Der Senator für Finanzen

Die Hansestadt Bremen

Der Senator für Finanzen · Rudolf-Hilferding-Platz 1 · 28195 Bremen

[redacted]

Auskunft erteilt
[redacted]
E-Mail
[redacted]
Datum und Zeichen
Ihres Schreibens
[redacted]
Mein Zeichen
(bitte bei Antwort angeben)
[redacted]

Bremen, 07.06.2023

Ihr Antrag nach dem Gesetz über die Freiheit des Zugangs zu Informationen für das Land Bremen: Alle Aufzeichnungen Koordinierungsstelle für IT-Standards (Referat 44) mit Bezug zur Registermodernisierung, beispielsweise Kommunikation (Briefe, Emails, etc), Gutachten, Stellungnahmen, Protokolle von Sitzungen, Vermerke zu Gesprächen und Abstimmungen [#278006]

Sehr geehrter [redacted]

aufgrund ihres Antrags vom 4.5.2023 auf Auskunft zu Dokumenten mit Bezug zur Registermodernisierung stellen wir folgende Dokumente zur Verfügung:

- **2018-09-30 TOOP D23 Architecture.pdf** Generic Federated OOP Architecture (3rd version)
- **2019-03_ITPLR-TOP17_Anlage1_Leitlinien-Modernisierung_Regis.pdf** Leitlinien für eine Modernisierung der Registerlandschaft
- **2019-03-12 Steimke Once Only Architektur.pdf** Bessere Verwaltungsleistungen durch Wiederverwendung vorhandener Daten
- **2019-06-12 MK Beschluss inkl. Anlage.pdf** Beschluss der Innenministerkonferenz im Rahmen der 210. Sitzung
- **2019-09-25_Registermodernisierung.pdf** Es bleibt schwierig Eine kurze Einführung zum Thema Registermodernisierung
- **2019-11-18 SDG.pdf** EU Anforderungen an die Digitalisierung von Verwaltungsverfahren
- **2020-01-10-Eckpunktepapier verfahrensübergreifender Identifikator.pdf** Vorschlag für eine mögliche Umsetzung der Anforderungen an die Registermodernisierung.
- **2020-25_Registermodernisierung_Eckpunkte.pdf** Eckpunkte für die Registermodernisierung

- **2021-05_Registermodernisierung.pdf** Registermodernisierung: Zielbild und Umsetzungsplanung
- **2021-25_Projektstrukturen.pdf** Projekt „Gesamtsteuerung Registermodernisierung“: Etablierung von Projektstrukturen
- 2021-35_Gesamtsteuerung_Projektbericht.pdf Projekt „Gesamtsteuerung Registermodernisierung“: Bericht zum Umsetzungsstand
- **2022-05-16-abschlussbericht-kosit.pdf** Bericht zur Erprobung Once-Only-Nachweisabruf mit dem Meldeportal Behörden des Landes NRW
- **2022-06_Bericht_Umsetzungsstand.pdf** Projekt „Gesamtsteuerung Registermodernisierung“: Bericht zum Umsetzungsstand
- **2022-22_RegMo_AL1_Bericht.pdf** Projekt „Gesamtsteuerung Registermodernisierung“: Bericht zum Umsetzungsstand
- **2022-22_RegMo_AL2_Reifegradmodell.pdf** Entscheidung zur Einführung eines Reifegradmodells für Nachweisabrufe und Ausrichtung des NOOTS auf Reifegrad D
- **2022-22_RegMo_AL3_Asynchrone_Prozesse.pdf** Entscheidung zur Unterstützung asynchroner Prozesse in der Architektur der Registermodernisierung
- **2022-22_RegMo_AL4_Nachweisabruf.pdf** Entwicklung eines allgemeinen Standards für den Nachweisabruf für die nationale Registermodernisierung
- **2022-22_RegMo_AL5_DSD.pdf** Aufbau eines nationalen Data Service Directory und Nutzung des europäischen Evidence Brokers
- **2022-22_RegMo_AL6_Registerdatennavigation.pdf** Entscheidung zur Umsetzung der Komponente Registerdatennavigation als zentralen Routing-Dienst (Routing As a Service) auf Grundlage des Deutschen Verwaltungsdiensteverzeichnis (DVDV) unter Wiederverwendung von Lösungsansätzen aus FIT-Connect

Mit freundlichen Grüßen

Im Auftrag

[redacted]

[redacted]

The Once-Only Principle Project

Generic Federated OOP Architecture

(3rd version)

Eric Grandry, Sander Fieten, Carmen Rotuna, Giovanni Paolo Sellitto, Jaak Tepandi, Ermo Täks, Dimitrios Zeginis

Submitted to the EC on 30/09/2018

Horizon 2020
The EU Framework Programme for Research and Innovation

PROJECT ACRONYM: TOOP

PROJECT FULL TITLE: The "Once-Only" Principle Project

H2020 Call: H2020-SC6-CO-CREATION-2016-2

H2020 Topic: CO-CREATION-05-2016 - Co-creation between public administrations: once-only principle

GRANT AGREEMENT n°: 737460

Generic Federated OOP Architecture (3rd version)

Deliverable Id:	D2.3
Deliverable Name:	Generic federated OOP architecture (3rd version)
Version:	V1.0
Status:	Final
Dissemination Level:	Public
Due date of deliverable:	M21 (September 2018)
Actual submission date:	30/09/2018
Work Package:	WP2
Organisation name of lead partner for this deliverable:	Tallinn University of Technology
Author(s):	Eric Grandry Sander Fieten Carmen Rotuna Giovanni Paolo Sellitto Jaak Tepandi Ermo Täks Dimitrios Zeginis
Partners contributing:	All beneficiaries

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Abstract:

The deliverable "D2.3. Generic Federated OOP Architecture (3rd version)" is the third official version of the generic federated Once-Only Principle (OOP) architecture. It develops further and extends the deliverables “D2.1. Generic federated OOP architecture (1st version)” (D2.1) and “D2.2. Generic federated OOP architecture (2nd version)” (D2.2).

The OOP architecture contributes to implementing OOP in public administrations and supports the interconnection and interoperability of national registries at the EU level. It is aligned with existing EU frameworks (EIRA, EIF) and aims to contribute to the implementation act of the forthcoming regulation about the Single Digital Gateway (SDGR). The OOP architecture uses the results of the e-SENS European Interoperability Reference Architecture. It provides support for developers of OOP projects and is based on the Connecting Europe Facility (CEF) Digital Service Infrastructures (DSIs), on the Building Blocks consolidated by the e-SENS project, and in justified cases, on new building blocks.

Compared to D2.2, this deliverable provides new Business Architecture, Information System Architecture, and Technology Architecture views. It is complemented with specific views addressing cross-cutting quality concerns, such as Security Architecture and Trust Architecture. The deliverable has also been further aligned with the existing EU interoperability frameworks, such as EIRA and EIF.

The Architecture Principles and Architecturally Significant Requirements constitute the Architecture Drivers and Decisions. The Stakeholders section present the goal model of TOOP architecture, its target users and use cases, as well as main stakeholders.

The deliverable D2.3 is comprised of a textual component and a wiki component. The current document is the textual component of D2.3. The wiki component is an architecture repository providing an in-depth content on the architecture views; it is available on the TOOP D2.3 documentation space in Confluence (please see the Glossary). The next official deliverable related to the generic federated OOP architecture is D2.4 (M30, due June 2019).

All web-links referred to in this deliverable are valid on the submission date of the deliverable.

This is a preliminary version of the deliverable, pending review and approval by the European Commission.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

Changes between D2.2 and D2.3

Modification	Details
Restructuring and reworking the methodology, architecture, and deliverable	The structure and all components of D2.2 have been reworked and updated in D2.3, new components have been added. The D2.3 provides new Business Architecture, Information System Architecture, and Technology Architecture views. It is complemented with new views addressing cross-cutting quality concerns, such as Security Architecture and Trust Architecture. The deliverable D2.3 comprises the textual component and the wiki component. The current document is the textual component of D2.3. The wiki component provides an in-depth content on the architecture views. It is available on the TOOP D2.3 documentation space in Confluence (please see the Glossary).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Table of contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

List of Figures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

List of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

List of Abbreviations

Acronym	Explanation
ABB	Architecture Building Block
ABR	Access to Base Registries
ADL	Architecture Description Language
AI	Artificial Intelligence
ASR	Architecturally Significant Requirements
AT	Automated Translation
BB	Building Block
BPMN	Business Process Model and Notation
BRIS	Business Registers Interconnection System
CCTF	Common Components Task Force
CEF	Connecting Europe Facility
CEF DSI	The DSI financed by CEF
D2.1	TOOP deliverable “D2.1. Generic federated OOP architecture (1st version)”
D2.2	TOOP deliverable “D2.2. Generic federated OOP architecture (2nd version)”
D2.3	TOOP deliverable “D2.3. Generic federated OOP architecture (3rd version)”
DC	Data Consumer
DP	Data Provider
DSI	Digital Service Infrastructure
EC	European Commission
eID	Electronic Identification
eIDAS	electronic Identification and Signature (EU regulation)
EIF	European Interoperability Framework
EIRA	European Interoperability Reference Architecture
EO	Economic Operator
EES	ETSI Rationalised Framework for Enhanced Security Services
IS	Information System
IT	Information Technology

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

JTF	Joint Technical Taskforce
JTG	WP3/WP2 Joint Technical Group
LSP	Large Scale Pilot
MA	Maritime Administration
IOP	Interoperability
OOP	Once-Only Principle
PA	Pilot Area
PKI	Public Key Infrastructure
PSC	Port State Control
SAT	Solution Architecture Template
SML	Service Metadata Locator
SBB	Solution Building Block
SDGR	Single Digital Gateway Regulation
TOOP	The Once-Only Principle Project
TOOPRA	The TOOP Reference Architecture
WP	Work Package

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Glossary

Term	Explanation
Application Architecture	A description of the structure and interaction of the applications as groups of capabilities that provide key business functions and manage the data assets (source: The Open Group 2011)
Architecture	Fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution (source: ISO/IEC 42010:2011)
Architecture description	An artefact used to express an architecture (source: ISO/IEC 42010:2011)
Architecture framework	Conventions, principles and practices for the description of architectures established within a specific domain of application and/or community of stakeholders (source: ISO/IEC 42010:2011)
Architecture view	An artefact expressing the architecture of a system from the perspective of specific system concerns (source: ISO/IEC 42010:2011)
Architecture viewpoint	An artefact establishing the conventions for the construction, interpretation and use of architecture views to frame specific system concerns (source: ISO/IEC 42010:2011)
Building Block	Represents a (potentially re-usable) component of business, IT, or architectural capability that can be combined with other building blocks to deliver architectures and solutions. Building blocks can be defined at various levels of detail, depending on what stage of architecture development has been reached. For instance, at an early stage, a building block can simply consist of a name or an outline description. Later on, a building block may be decomposed into multiple supporting building blocks and may be accompanied by a full specification. Building blocks can relate to "architectures" or "solutions". http://pubs.opengroup.org/architecture/togaf9-doc/arch/ (Ch.3)
Business Architecture	A description of the structure and interaction between the business strategy, organization, functions, business processes, and information needs (source: The Open Group 2011)
Competent Authority	'Competent authority' is a Member State body or authority established at either national, regional or local level with specific responsibilities relating to the information, procedures, assistance and problem-solving services.
Digital Service Infrastructure	CEF trans-European infrastructures based upon mature technical and organisational solutions, and aimed at supporting exchanges and collaboration with and within the public sector, across the EU
Evidence	`Evidence` means any document or data, including text or sound, visual or audiovisual recording, irrespective of the medium used, required issued by a competent authority to prove facts or compliance with requirements for procedures referred to in Article 2(2)(b). Source: SDGR, 14401/1/17 REV 1, Brussels, 28 November 2017
Information System Architecture	A description of the realization of the Business Architecture with IT components, and more specifically with the existing building blocks, as well as a description of the principles guiding the design of the IS architecture
Legal Entity	An association, corporation, partnership, proprietorship, trust, or individual that has legal standing in the eyes of law (http://www.businessdictionary.com/definition/legal-entity.html)
National registry	A data registry maintained by a Competent Authority

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Natural person	Please see "Person, Natural"
Once Only Principle	The public administrations should ensure that citizens and business supply the same information only once to a public administration
OOP architecture	A complex comprising the Generic Once Only Principle Reference Architecture and associated components, resulting from the TOOP project
OOP system	System based on the Once-Only Principle as applied in the TOOP project
Person, Legal	A legal person is a registered organization, having its registered office in a Member State. Reference: SDGR, 14401/1/17 REV 1, Brussels, 28 November 2017, Article 3(1)
Person, Natural	A natural person is a human, residing in a Member State. Reference: SDGR, 14401/1/17 REV 1, Brussels, 28 November 2017, Article 3(1)
Reference Architecture	Reference architectures are standardized architectures that provide a frame of reference for a specific domain, sector or field of interest (Proper and Lankhorst 2014). TOOPRA specific concern is the implementation of the OOP.
Scenario	One typical way in which a system is used or in which a user carries out some activity.
Technology Architecture	The Technology Architecture describes the logical software and hardware capabilities that are required to support the deployment of business, data, and application services. This includes IT infrastructure, middleware, networks, communications, processing, standards, etc. (source: The Open Group 2011)
TOOP D2.3 documentation space in Confluence	The space is provided on http://wiki.ds.unipi.gr/display/TOOPRA.
TOOP T2.1	TOOP Task 2.1, Federated Technical Architecture. T2.1 has a dual role. It is developing the TOOP Once Only Principle Reference Architecture, providing it in T2.1 deliverables. In parallel, T2.1 is prototyping, testing and participating in pilot implementations of the architecture, together with WP3, within the Common Components Task Force (CCTF) and in Joint Group Task Forces (JTF)
Use case	A specification of one type of interaction with a system. One use case may involve several scenarios (usually a main success scenario and alternative scenarios)
User	User is anyone who is a citizen of the Union, a natural person residing in a Member State or a legal person having its registered office in a Member State, and who accesses the information, the procedures, or the assistance or problem-solving services, referred to in Article 2(2), through the gateway. Reference: SDGR, 14401/1/17 REV 1, Brussels, 28 November 2017, Article 3(1)
User story	Informal description of one or more system features from the user perspective

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Executive Summary

The Once Only Principle states that "*the public administrations should ensure that citizens and business supply the same information only once to public administration*": it is one of the pillars of the strategy for the Digital Single Market and one of the basic principles of the EU eGovernment Action Plan 2016-2020.

The Once-Only Principle Project (TOOP) aims to explore, demonstrate, and enable the Once Only Principle.

The achievement of this objective is supported by implementing three once-only pilot projects (TOOP pilots), by developing a generic federated OOP architecture, and by exploring other aspects of OOP and its supporting infrastructure such as legal landscape, OOP drivers and barriers, and sustainability.

TOOP focus area within the Once Only Principle implementation is on information related to business activities and on cross-border sharing of this information. The primary concern of the TOOP Reference Architecture (TOOPRA) developed within this project is to support the application of TOOP in this focus area, although its wider usage is not excluded. It builds on analysis of the TOOP requirements, on the experience of previous Large Scale Pilot (LSP) projects, and on the know-how gained with implementation of the TOOP pilots. As the TOOP project is required to support the implementation of the Single Digital Gateway Regulation (SGDR), the architecture has been aligned with SDGR provisions.

The main political and legislative principles underlying the OOP architecture are stated in the Annex 2 of the European Interoperability Framework Implementation Strategy (European Commission 2017). One of the main technical principles for development of the OOP architecture is the reuse of existing frameworks and building blocks provided by CEF, e-SENS, and other initiatives. The TOOP generic federated OOP architecture relies on such frameworks, on the European Interoperability Reference Architecture (EIRA) (Chou et al. 2015), the CEF Building Blocks, and the e-SENS deliverable D6.6 "e-SENS European Interoperability Reference Architecture", among others.

The OOP architecture contributes to implementing OOP in public administrations and supports the interconnection and interoperability of national registries at the EU level. It is aligned with existing EU frameworks (EIRA, EIF), is aimed to contribute to the implementation act of the forthcoming regulation about the Single Digital Gateway (SDGR) and uses the results of the e-SENS European Interoperability Reference Architecture. It provides support for developers of OOP projects and is based on the Connecting Europe Facility (CEF) Digital Service Infrastructures (DSIs), on the Building Blocks consolidated by the e-SENS project, and in justified cases, on new building blocks.

The current deliverable is the third official version of the generic federated Once-Only Principle (OOP) architecture. It develops further and extends the deliverables "D2.1. Generic federated OOP architecture (1st version)" (D2.1) and "D2.2. Generic federated OOP architecture (2nd version)" (D2.2).

The deliverable D2.3 is comprised of a textual component and a wiki component. The current document is the textual component of D2.3. The wiki component is an architecture repository providing an in-depth content on the architecture views; it is available on the TOOP D2.3 documentation space in Confluence (see Glossary).

The architecture has been developed using an exploratory and agile approach, in cooperation with the TOOP pilots and other TOOP Work Packages (WPs) and tasks. Compared to D2.2, this deliverable provides new Business Architecture, Information System Architecture, and Technology Architecture views. It is complemented with specific views addressing cross-cutting quality concerns, such as Security Architecture and Trust Architecture.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

The Architecture Principles (APs) and Architecturally Significant Requirements (ASRs) constitute the Architecture Drivers and Decisions. The Stakeholders section present the goal model of TOOPRA, its target users and use cases, as well as main stakeholders.

This deliverable is a work in progress. The next official deliverable related to the generic federated OOP architecture is D2.4 (M30, due June 2019).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

1. Introduction

1.1. Scope and Objective of Deliverable

The Once Only Principle states that "*the public administrations should ensure that citizens and business supply the same information only once to public administration".*

The Once-Only Principle Project (TOOP) aims to explore, demonstrate, and enable the Once Only Principle. The achievement of this objective is supported by implementing three once-only pilot projects (TOOP pilots), by developing a generic federated OOP architecture, and by exploring other aspects of OOP and its supporting infrastructure such as legal landscape, OOP drivers and barriers, and sustainability.

TOOP focus area within the Once Only Principle implementation is on information related to business activities and on cross-border sharing of this information (Krimmer et al. 2017). The Generic Once-Only Principle Reference Architecture, developed within TOOP, relates primarily to applications in the TOOP focus area, although a wider usage is not excluded. It builds on the analysis of the TOOP requirements, on the experience of previous Large-Scale Pilot (LSP) projects, and on the know-how gained with implementation of the TOOP pilots. Due to the shift in the TOOP project focus requiring it to support implementation of the Single Digital Gateway Regulation - SGDR (European Union 2017), the current version of the OOP architecture has been aligned with SDGR provisions.

The current deliverable is the third official version of the generic federated Once-Only Principle (OOP) architecture. It develops further and extends the deliverables "D2.1. Generic federated OOP architecture (1st version)" (D2.1) and "D2.2. Generic federated OOP architecture (2nd version)" (D2.2).

The deliverable D2.3 comprises the textual component and the wiki component. The current document is the textual component of D2.3. The wiki component provides an in-depth content on the architecture views, cross-cutting concerns, stakeholders, and the architecture drivers and decisions, and is available on the TOOP D2.3 documentation space in Confluence (see Glossary).

The architecture has been developed using an exploratory and agile approach, in cooperation with the TOOP pilots and other TOOP Work Packages (WPs) and tasks. Compared to D2.2, this deliverable provides new Business Architecture, Information System Architecture, and Technology Architecture views. It is complemented with specific views addressing cross-cutting quality concerns, such as Security Architecture and Trust Architecture.

The Architecture Principles (AP) and Architecturally Significant Requirements (ASRs) constitute the Architecture Drivers and Decisions. The Stakeholders section present the goal model of TOOPRA, its target users and use cases, as well as main stakeholders.

This deliverable is a work in progress. The next official deliverable related to the generic federated OOP architecture is D2.4 (M30, June 2019).

1.2. WP2 General Objectives and Vision

According to (Krimmer et al. 2017), the benefits expected from the project are: a better-functioning digital single market, with increased customer satisfaction and a better image of public authorities, allowing to get:

- time savings,
- lowering the administrative burden and reducing costs for business,
- fulfilling legal obligations faster,
- improved service quality and administrative efficiency.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

WP2 approach aims to capture TOOP pilots results and add value by generalising and formalizing it for further use. WP2 is serving abovementioned goals through offering usable high-level views to capture enablers, barriers and principal design of developed technical solutions in one coherent documentation set. Due to the innovative nature of the project, the content and coverage of this set is highly experimental, subject to continuous development and might serve as a blueprint for developing similar cross-border solutions.

More specifically addressing the goals listed above, time savings for public authorities could be gained through following TOOP development patterns and Generic Architecture defined principles. Reduced administrative burden and costs can be achieved by using standard solution blocks, identified with help of Reference Architecture. Generic Architecture, Reference Architecture and standard solution blocks are designed in line with legal requirements. Improved service quality and efficiency is accessible through tested, mature, interconnected and interoperable TOOP standard building blocks.

The general objectives of TOOP WP2 (Technical Architecture, Legal and Governance Aspects) are to develop a generic, federated OOP architecture, to identify general legal barriers and drivers regarding privacy, confidentiality and consent needed for the implementation of OOP, to assess the possible impacts of the implementation of OOP in the pilots in WP3, as well as to define a sustainability plan for the maintenance of the architectures, building blocks and drivers/barriers after the end of the project.

The results of WP2 work represent the main technological innovation of TOOP: the generic federated OOP architecture that supports the interconnection and interoperability of national registries at the EU level - together with other investigations needed to generalize, extend, and sustain the TOOP results.

1.3. Methodology of Work

The methodology of work follows from TOOP aims and activities. This project implements three TOOP pilots, develops a generic federated OOP architecture, supports implementation of the Single Digital Gateway Regulation, and explores other aspects of OOP and its supporting infrastructure such as OOP drivers and barriers. The architecture described in this deliverable is qualified as a

- Generic Architecture and a
- Reference Architecture.

The architecture is generic, as it is designed by abstracting from domain specificities and identifying the common elements associated with the problem domain (the Once-Only Principle). It is part of an architecture continuum, as defined in The Open Group's Architecture Framework (TOGAF)[1] (The Open Group 2011), which allows to move from a generic architecture to a domain-specific and a pilot-specific architecture. TOGAF is chosen because it is open source and accessible for all the interested parties without additional costs, thus in coherence with European Commission strategy for internal use of Open Source Software (https://ec.europa.eu/info/departments/informatics/open-source-software-strategy_en).

TOGAF Architecture Development Method (ADM) is a proven Enterprise Architecture methodology, ensuring consistent standards, methods, and communication among Enterprise Architecture professionals. TOGAF 9.2 considers an "enterprise" to be any collection of organizations that have common goals (section 1.3). Given that TOOP aims to connect different governmental services originating from different EU member states, the Enterprise that TOOP has in scope is *a group of*

[1] http://www.opengroup.org/public/arch/p3/ec/ec_ac.htm

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

loosely linked independent governmental entities that collaborate to achieve common a goal, which is defined by OOP principles.

The architecture described in this deliverable is a Reference Architecture, as opposed to a solution architecture: Reference Architectures "capture the essence of existing architectures, and the vision of future needs and evolution to provide guidance to assist in developing new solution architectures" (Cloutier et al. 2010). Reference architectures are standardized architectures that provide a frame of reference for a particular domain, sector or field of interest (Proper and Lankhorst 2014): in the case of TOOPRA the main concern is supporting the OOP. Reference models or architectures provide a common vocabulary, reusable designs and industry best practices. They are not solution architectures, i.e. they are not implemented directly. Rather, they are used as a constraint for more concrete architectures. Typically, a reference architecture includes common architecture principles, patterns, building blocks and standards.

The TOOP Reference Architecture (TOOPRA) is developed in cooperation with the TOOP pilots and other TOOP Work Packages. The main pilot design activities are done in TOOP WP3, and more specifically in the Common Components Task Force (CCTF), which is responsible for designing the common components to be used in the pilots. TOOP T2.1 is prototyping, testing and participating in pilot implementations of the architecture together with WP3 within the CCTF and in Joint Group Task Forces (JTF). The TOOPRA builds on the know-how gained with designing the TOOP pilots and experience of previous Large Scale Pilots (LSP), especially the reusable building blocks constituting the Digital Service Infrastructure (DSI). The TOOPRA also contributes to the TOOP pilot design and to the modification and development of the DSI.

1.4. Relations to Internal TOOP Environment

The TOOP T2.1 members are simultaneously contributing to several parallel processes: developing further the architecture; delivering T2.1 deliverables in specified deadlines; participating within the WP3/WP2 Joint Technical Group (JTG), the Common Components Task Force (CCTF), and the Joint Technical Taskforces (JTF). The current deliverable presents the results of the architecture development process, evaluates and extends the pilot outcomes, exchanges best practice results with other WP2 tasks, and provides architecture-related support to WP3 within the scope of task T2.1.

Specific instantiations of the architecture are being implemented in development of the TOOP pilot projects in WP3. The architecture is partially based on the interaction between WP2 and WP3, on the questionnaire and information provided with respect to other tasks in WP2, and other sources. Maintaining and further development of the architecture will be planned by the Sustainability and Governance task of WP2.

Inputs to this deliverable were received from the EU official sources, from CEF Building Blocks, from deliverables and wikis of the e-SENS project, from TOOP WP3, from desk research, from architecture guidelines, frameworks, standards, and from other sources.

This architecture is aimed at guiding the designers and developers of pilot applications in WP3 and the stakeholders who will develop applications to support the interconnection and interoperability of national registries at the EU level and provide implementation of the Single Digital Gateway Regulation.

1.5. Relations to External TOOP Environment

This deliverable reports the results produced by TOOP WP2. These results represent the main technological innovation of TOOP - the generic federated OOP architecture. This architecture supports the interconnection and interoperability of national registries at the EU level. It is in line with existing EU frameworks (EIRA, EIF) and takes into account the e-SENS European Interoperability Reference

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Architecture. It provides input for SDGR implementation and is oriented towards reuse of the CEF DSIs and the Building Blocks consolidated by the e-SENS project.

1.6. Legal Issues

Several legal issues had to be clarified when writing the deliverable. These issues were related to European legislation, as well as to national legislation in Member States and Associated Countries that are participating in the WP3 pilots. The solutions found (see TOOP Deliverable D2.5, 2017) allowed to conclude that it is possible to build the generic federated OOP architecture in line with existing EU frameworks and Building Blocks such as the European Interoperability Framework, the European Interoperability Reference Architecture, the Single Digital Gateway Regulation, the CEF Building Blocks, and the e-SENS Building Blocks.

1.7. Structure of the Document

Introduction, the first chapter of this document, states the scope and objectives of the deliverable and the TOOP WP2, its methodology, relations to TOOP internal and external environments, and other issues.

The architecture design methodology, including its motivation, framework, process, and requirements analysis are analysed in the second chapter.

The third chapter presents the summary of the TOOP Reference Architecture, including three architecture views (Business Architecture, Information System Architecture, Technology Architecture), description of the architecture repository, and link to the architecture models.

The fourth chapter provides a set of the TOOP Reference Architecture life cycle management processes, with the aim of providing a better support to stakeholders, fostering user adoption of the architecture, and enhancing transparency of its change management.

The state of the cooperation of the TOOP Architecture team with other relevant EC Initiatives is presented in the fifth chapter.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

2. Architecture Design Methodology

The initial purpose of the OOP architecture was to aid development of specific information systems architectures supporting the Once-Only Principle. After SDGR was introduced in April 2017, the TOOP project was additionally given the task to provide input to the SDGR Implementing Act. This means that the architecture had to take into account new requirements emerging from SDGR.

The TOOPRA is therefore developed by combining top-down and bottom-up approaches:

- The Once-Only Principle and its legal environment, specifically the "SDGR draft", as well as the user requirements from the "Member States" (i.e. pilots), guide the design of the architecture;
- The existing frameworks and building blocks provided by "CEF DSI", e-SENS, and other initiatives, together with TOOP "Common Pilot Solution Architecture", are designed artefacts that are injected within the architecture where appropriate and support the design of the architecture.

The Figure 1 graphically represents this combined approach, including the expected outcomes of TOOPRA: on one hand it should be a blueprint for the OOP systems and the implementing acts based on SDGR, on the other hand it should contribute to both the pilot architecture and the DSI. Note that the TOOP "Common Pilot Solution Architecture" also interacts with the "Member States" and the "CEF DSI"; however, these interactions focus more on implementation aspects, while the interactions with the TOOPRA are on architectural aspects.

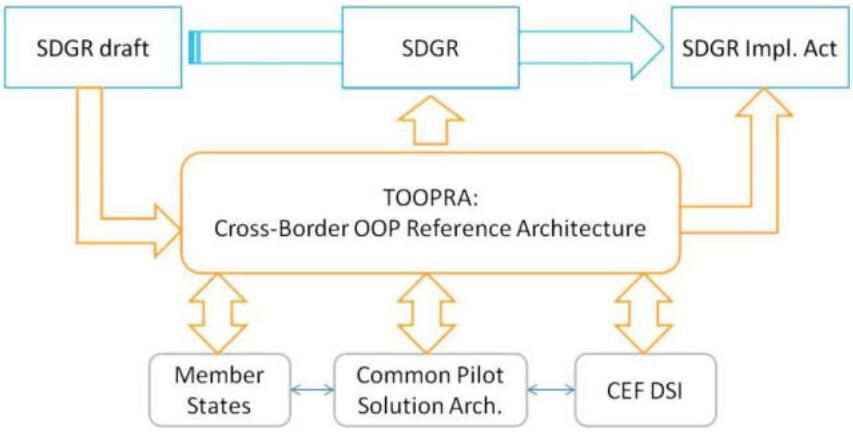


Figure 1: Context of TOOP Architecture Design

2.1.Architecture Development Motivation, Target Users, Use Cases

2.1.1. Architecture Development Motivation

The motivation behind architecture development is to share some best practices for cross-border solution development through high-level, architectural descriptions, laying the foundations for the future developments of the wide set of different high-quality cross-border solutions.

Administrations can benefit from the existence of a generic architecture since they can select solutions without reference to a vendor. The architectural model can be included in the technical specifications of a call for tender and this should reduce vendor lock in.

A generic architecture opens the market to a multiplicity of compliant solutions and to a multiplicity of vendors, lowering the entrance barriers for the SMEs and fostering competition. This should also

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

lower the prices of procuring an OOP service for administrations and improve quality of OOP services for citizens.

EC can benefit from the TOOPRA since the existence of a reference architecture should make the development process of an OOP service more effective and efficient.

The direct beneficiaries are the users of the architecture, which are a special category of stakeholders, since they are interested in the quality of the architecture but also in its usability and other architectural qualities.

Another approach is to classify beneficiaries according to the temporal aspects of their interest. Different interest groups are involved in different time periods, thus making unified approach even more challenging. For example, TOOP project managers are involved during TOOP project time; architects and developers focus on the outcome after the project has finished but before launching new cross-border services; businesses are involved after this period and so forth. Each of these interest groups has different expectations and requirements upon the project outcome.

Therefore, a simple separation is made to distinguish between wider TOOP project related interest groups (hereby classified as Stakeholders) from direct users of TOOP Reference architecture (TOOPRA target users).

2.1.2. Stakeholders

Architecture development motivation is presented from two viewpoints: stakeholders and users. Stakeholders do form a wider spectrum of all interest groups, whilst direct users of TOOP architecture are considered as target audience for using this document. Stakeholders are divided into next main groups.

Key roles and responsibilities within the project:

- **TOOP managers** are the people involved in planning and managing the project and ensuring smooth delivery of the project outcomes. Indirectly this group involves also EU top level officers, developing legislation regarding Single Digital Market Regulation and ensuring cross-border public data and services movement.
- **TOOP implementors** are persons directly responsible for planning and development of solutions enabling cross-border public data and services movement. This involves public officials, architects, analysts and developers, using TOOP project results as blueprint for creating forthcoming software solutions in similar scale.
- **Prospective service users** are citizens and business, going to use cross-border public data and services movement enabling software solutions. This is the main stakeholder's group for whom this initiative should serve, ensuring delivery of highly efficient and user-friendly software solutions in the close future.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

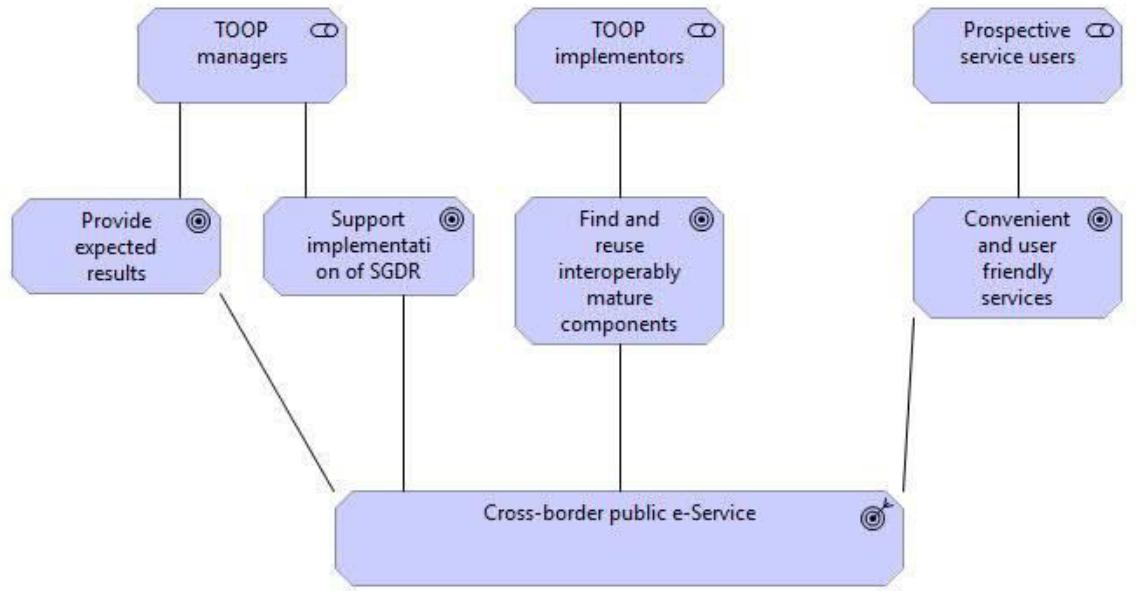


Figure 2: The TOOPRA goal model

2.1.3. TOOPRA target users

The target users of the architecture are the present and future developers of EU eGov services, which will benefit from the existence of a generic reference architecture TOOPRA in two ways:

1) they have a reference model that guides the selection of the relevant building blocks (architecture as a Solution Architectural Template)

2) they can test their solutions for compliance against architecture (architectural compliance).

In addition to the target users we should also consider the possible stakeholders, which are the people that can receive direct or indirect benefits from the existence of TOPRA.

A first list of stakeholders has been identified during the early phases of the project.

Target users do form a special group of stakeholders, holding specific interest toward TOOP Reference Architecture. The documentation, reflecting the development of different level and universal/reusable building blocks is expected to serve target users in multiple ways. The TOOP has the objective to support users in the following scenarios.

- Designing: accelerate the design EU wide software solutions that support the delivery of interoperable digital public services (across borders and sectors).
- Assessing: provide a reference model for comparing existing architectures in different Member States, to identify focal points for convergence and reuse.
- Communicating and sharing: help documenting the most salient interoperability elements of complex solutions and facilitate the sharing of (re)usable solutions.
- Discovering and reusing: ease the discovery and reuse of interoperability solutions.

The main categories of TOOP Reference Architecture users are as follows.

- **Architects,** Enterprise Architects as well as Solution Architects, that are responsible for the design of cross-border solution architectures.
- **Portfolio managers** responsible for maintaining the catalogue of assets related to the design and implementation of eGovernment solutions and for making investment decisions on these assets.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

- **Business analysts** responsible for assessing and to study the impact of changes in the (external) environment on IT systems.
- **Developers** responsible for design, development and implementation of software solutions for interoperable digital public services (across borders and sectors).

The TOOPRA users are involved in the following main use cases (Figure 3).

- Design and document cross-border solution Architectures architecture use case
- Compare cross-border solution architectures use case
- Create portfolio of solutions use case
- Manage portfolio of solutions use case
- Rationalise portfolio of solutions
- Support impact assessment on ICT use case
- Design, develop and implement

Detailed descriptions of the use cases, as well as a stakeholder list containing three levels of stakeholders are given in the TOOP D2.3 wiki component in Confluence.

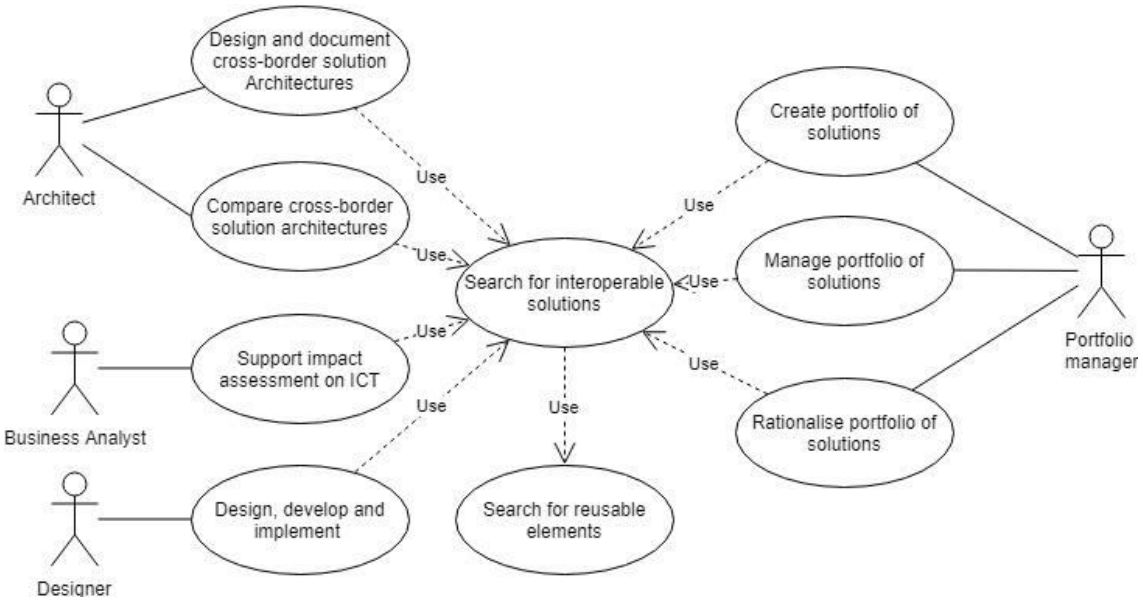


Figure 3: Target users and their use cases within the TOOPRA

2.2.Architecture Description Framework

An architecture description is an artefact describing the architecture for some system of interest. In ISO/IEC/IEEE 42010, system refers to man-made and natural systems, including software products and services and software-intensive systems.

Frameworks conforming to the standard often include processes, methods, tools and other practices beyond those specified above. The two most well-known examples of architecture frameworks are TOGAF and Zachman's information systems architecture framework[2] (Zachman 2008).

The TOOPRA description is organized along the following architecture views, adopted from TOGAF framework (illustrated in Figure 4): the business view (**Business Architecture**), concerned with the business operations of the TOOP system, the IS view (**IS Architecture**), concerned with the realization

[2] https://en.wikipedia.org/wiki/Zachman_Framework

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

of the business operations with information systems, and the technology view (**Technology Architecture**), concerned with the logical software and hardware capabilities that are required to support the IS architecture. They are complemented with specific views addressing cross-cutting quality concerns, such as security architecture and trust architecture. The architecture drivers and decisions comprise the architecture principles (AP) and architecturally significant requirements (ASRs). The stakeholders component presents the goal model of TOOPRA, its target users and use cases, as well as main stakeholders.

The domain model (the architecture domain definition and description) has been provided in the TOOP D2.2 deliverable. The environment and the context of the Once-Only domain affects the architecture by providing relevant knowledge and information that guides the design of the architecture. The political and legal environment, the pilot (and other relevant) requirements, as well as the architecture patterns and other elements of the architecture and design body of knowledge have been the main external elements considered in the TOOP architecture deliverables.

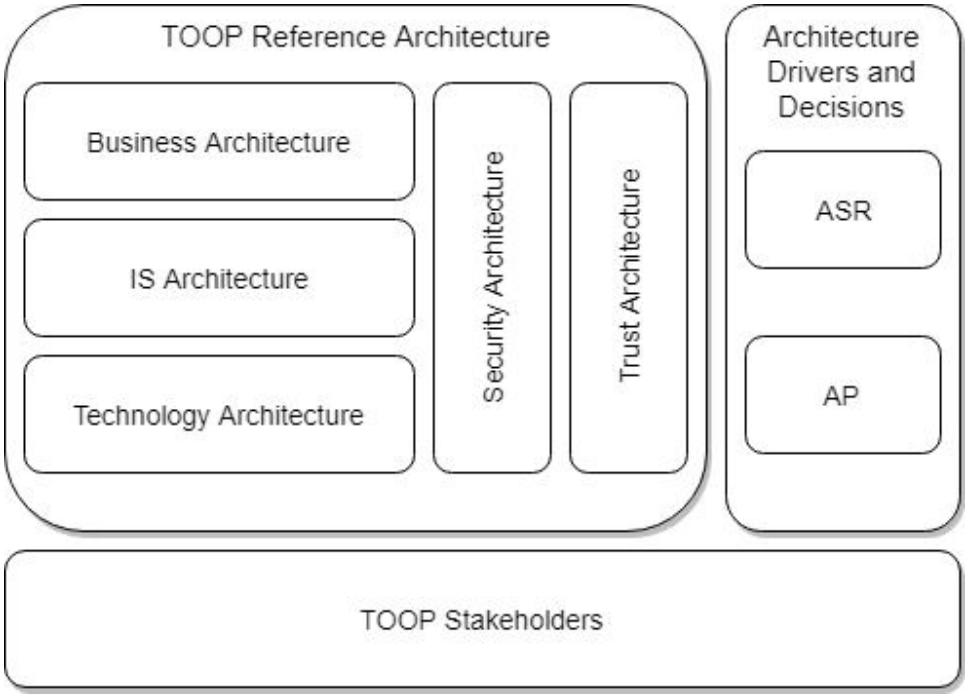


Figure 4: Generic Reference Architecture Description Framework

2.3.Architecture Design Process

Figure 5 shows the principal activities within the TOOP architecture development process, together with their outputs.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

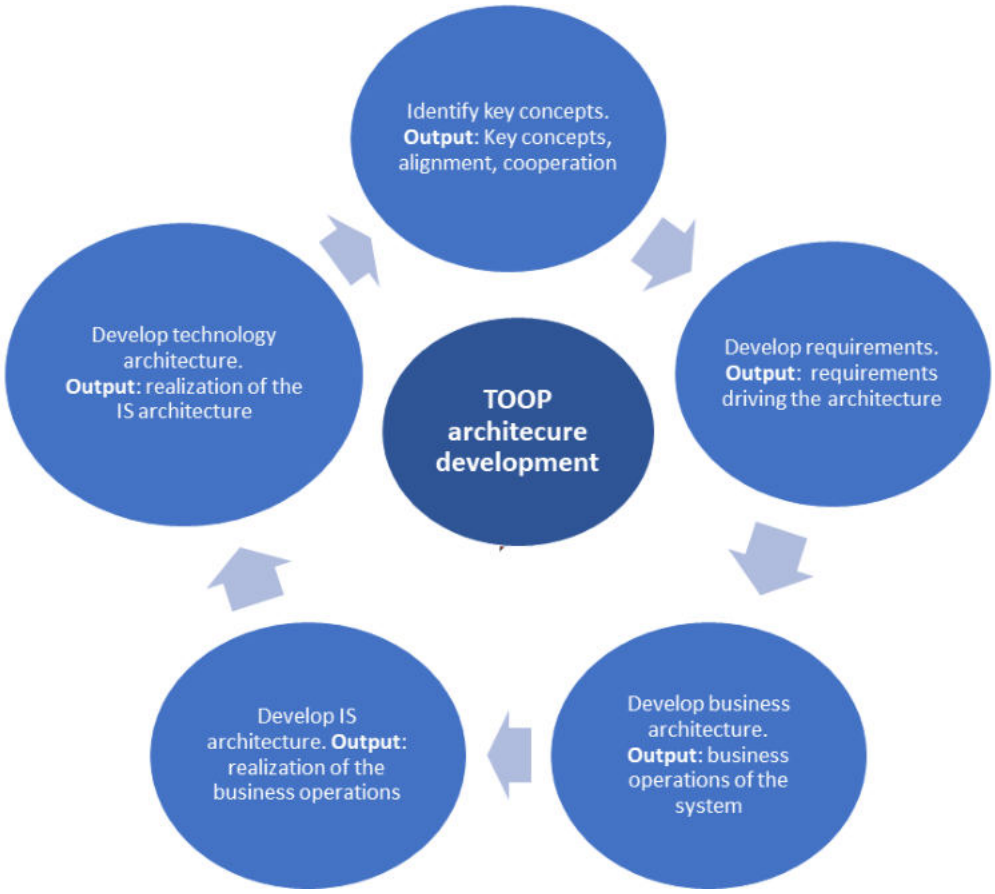


Figure 5: Activities within the TOOP architecture development process

The architecture deliverable development follows an incremental approach, involving four official versions (D1.1, D2.2, D2.3, D2.4) and two interim versions. The current document is the third official version and will be developed further in the next edition. To the reasonable extent, duplication of content from previous deliverable versions has been avoided in D2.3; however, in each consecutive version of the architecture deliverable, some components from the previous versions may be added, some components may be developed further or modified, and some components may be left unchanged.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

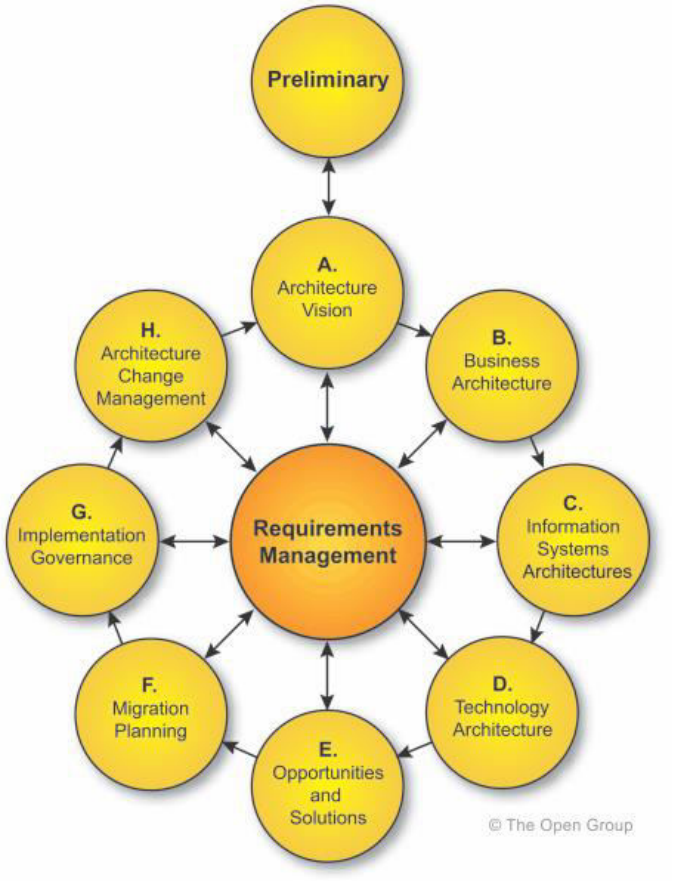


Figure 6: TOGAF Architecture Development Cycle

For the development process of the generic, federated OOP Architecture, the Architecture Development Method (ADM) of TOGAF9.1[3] was adopted. This methodology follows a cyclic approach towards the development of an architecture, its implementation and maintenance (see the figure). In the development of D2.3, a complete TOGAF ADM cycle was not adopted, since TOGAF does not mandate a complete cycle - the focus has been on phases from A to D. TOGAF was used as a methodology to improve the quality of the product (D2.3) with the aid of a structured reference process, therefore the selected TOGAF phases have not been reported in the deliverable. The deliverable was not intended as a TOGAF application exercise.

A mapping between the TOGAF steps and the D2.3 chapters loosely the following:

TOGAF Preliminary Phase --> D2.3 Introduction

TOGAF Phase A “Architecture Vision Phase” --> D2.3 Architecture Methodology

TOGAF PHASE B --> D2.3 3.1.1 Business Architecture

TOGAF PHASE C --> D2.3 3.1.2 Information Systems Architecture

TOGAF Phase D --> D2.3 3.1.3 Technology architecture

[3] http://pubs.opengroup.org/architecture/togaf9-doc/arch/

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

All these phases have involved some cycles through the TOGAF Requirement Management Phase. The E-H phases were applied in the selection and evolution of the existing Building Blocks from previous projects and CEF, but not in depth. These phases will lead the evolution of D2.3 into D2.4. In relation to the TOGAF architecture framework, Archimate3.0[4] specification has been used as an architecture description language (ADL).

2.4. Requirements Analysis

The requirements of interest in designing TOOP Reference Architecture are the **Architecturally Significant Requirements** (ASR's), i.e. "those requirements that have a measurable impact on a software system's architecture" (Chen, Babar, and Nuseibeh 2013). Significant is a key term in this definition and is ultimately measured by high cost of change in the designed architecture.

The ASR's are specified by referring to concepts and elements of the domain model: the requirements are indeed guiding the solution to be designed to solve the problem domain. ASR's will therefore refer to an actor/role's capability, as captured in the domain model.

Besides the ASR's, **architecture principles** are also captured: they are "underlying general rules and guidelines for the use and deployment of all IT resources and assets across the enterprise" (TOGAF). They reflect a level of consensus among the various elements of the enterprise and form the basis for making future architecture decisions.

A principle differs from a requirement by its scope: it is a general rule applied to any element of the designed architecture. Some architecture principles might be the source from which architecture requirements are derived. The architecture principles however remain key guidelines driving the architecture decisions and might be referred to at any stage of the architecture design (from business architecture to technology architecture).

Both the ASR's and the Architecture Principles are structured according the standard Software/System Product Quality Model (ISO/IEC 25010) and the related Data Quality Model (ISO/IEC 25020), both part of the Software Quality Requirements and Evaluation (SQuaRE) family of standards. Adopting a standard structure contributes to ensuring that all relevant architecture concerns are integrated and to identifying potential lack of expressed needs from the stakeholders: a relevant quality attribute that is not associated with any requirement might represent a gap in the requirements engineering process, seen from the viewpoint of the architect.

Table 1 identifies the relevant quality attributes in the context of TOOP: these are the concerns for which requirements and/or principles should be specified.

Table 1: Relevant Quality Attributes

Quality Attribute	Relevance and specific goals in TOOP
System Quality	
Functional Suitability	The domain model (actors/roles and collaboration model) is the baseline for the functional suitability dimension. It is complemented with functional requirements associated with the capabilities of each domain participant.

[4] http://pubs.opengroup.org/architecture/archimate3-doc/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Quality Attribute	Relevance and specific goals in TOOP
Performance Efficiency	The performance is mainly relevant from the **time-behaviour** perspective (i.e. the degree to which the response and processing times and throughput rates of a product or system, when performing its functions, meet requirements), associated with the end-to-end processing time of the user request. The **capacity** might also be relevant, in terms of size of data to exchange, as well as in terms of transaction **throughput**
Compatibility	The compatibility quality dimension is concerned with **interoperability**, from the perspective of both the exchange of information and the use of exchanged information. The **coexistence** attribute is relevant in terms of integration with existing MS systems and the compliance with the principle of subsidiarity.
Usability	The **operability** of the system is the main concern: it especially relates to the cross-border exchange. Moreover, **accessibility** is a compulsory requirement, especially in terms of European languages.
Reliability	The reliability is mainly concerned with the **availability** of the system, and specifically of the cross-border exchange.
Security	Security is a main concern in TOOP, as the system deals with the exchange of authenticated data and authorized access to the data. The requirements are associated with **confidentiality**, **integrity**, **availability (of the information)**, **nonrepudiation**, **accountability**, **auditability**, **authenticity/trustworthiness**, as well as **privacy**.
Maintainability	Although **modularity** and **reusability** are of paramount importance to ensure maintainability, they are not directly concerned with the architecture of the system (but with the detailed design of the solution).
Data Quality	
Accuracy	**Syntactic** and **semantic** accuracy of the exchanged data are particularly important in TOOP.
Completeness	The completeness of data cannot be guaranteed on the TOOP architecture level as the TOOP does not include the collection and validation of data about the data subject from the data owner.
Consistency	The consistency of data is ensured by the systems that the TOOP architecture relies on. TOOP in itself cannot therefore ensure the data consistency.
Credibility	The authenticity of data is a major concern in the cross-border exchange of evidence. TOOP should ensure that the authenticity is maintained during the exchange.
Currentness	Evidence can be updated during its lifecycle. The currentness of data is ensured by the systems that the TOOP architecture relies on. TOOP has to integrate this and provide a mechanism to ensure the use of current data.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

The ASR's and Architecture Principles specifications are the outcome of a standard requirements engineering process, composed of the following activities:

- Requirements inception
- Requirements analysis
- Requirements specifications
- Requirements validation

The activities are contextualized, both to the scope of the project and to the goal of designing a reference architecture (as opposed to an application architecture). The contextualized activities and their outcomes are described in the following sections.

2.4.1. Architecture Requirement Inception

During the inception phase, the needs of the stakeholders are captured: they are the baseline for the specifications of the requirements. In TOOP, the needs are issued from the following sources:

- The legal environment and specifically the draft SDGR;
- The interoperability principles and recommendations (extracted from the EIF);
- The pilot needs.

The needs of the stakeholders are captured by other WP and/or tasks. The main sources of these needs are:

- Legal principles and requirements (D2.5)
- Draft SDGR[5]
- EIF Principles and Recommendations[6]
- User requirements issued by each pilot and available on the pilot wiki[7]

2.4.2. Architecture Requirement Analysis

In this phase, the requirements from each source is analysed and its impact on the architecture is assessed. The result of this assessment might be that

- The requirement is not relevant in terms of architecture
- The requirement is either generalized or specialized in an architecture principle
- The requirement is generalized in an architecture requirement

Annex I of D2.2 describes the outcome of the legal framework analysis, while Annex II of D2.2 describes the outcome of the EIF analysis.

2.4.3. Architecture Principles Specifications

In this phase, the identified architecture principles are formulated and associated with the quality model. The specified architecture principles are traced back to their sources (e.g., 'EIF-04' refers to EIF Recommendation 4).

[5] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0256

[6] https://ec.europa.eu/isa2/eif_en

[7] http://wiki.ds.unipi.gr/display/TOOPPILOTS/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Table 2: Architecture Principles[8]

ID	Name	Description	Rationale	Quality attributes	Implications
PRINC-01	Open specifications and standards	To ensure technical interoperability, give preference to open specifications and standards in the design of the cross-border evidence exchange system, taking due account of the coverage of functional needs, maturity and market support and innovation	EIF-04 EIF-33	Reusability Interoperability	If a new component is to be designed, give preference to open specifications and standards
PRINC-02	Reusable solutions	Design TOOP Architecture as a Reference Architecture, which can be reused as a template to develop the various solutions architectures. Include the reuse of existing building blocks when relevant.	EIF-06	Reusability	Develop TOOP architecture as a reusable solution; reuse BB when possible
PRINC-06	Once Only Principle	Adhere to the Once Only Principle in the design of the Reference Architecture for SDGR	EIF-13	Operability	The Once Only Principle helps to meet the users' requirement to provide only the information that is absolutely necessary to obtain a given public service
PRINC-07	Standards and specifications process	Put in place processes to select relevant standards and specifications,	EIF-21	Interoperability	Standards and specifications are fundamental to interoperability.

[8] Numbering of Architecture Principles is kept from earlier iterations of the deliverable, however, some of the principles have been removed from the table.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

		evaluate them, monitor their implementation, check compliance and test their interoperability			Their management process needs to be established together with architecture development
PRINC-08	Standards and specifications selection	Use a structured, transparent, objective and common approach to assessing and selecting standards and specifications	EIF-22	Interoperability	A structured, transparent, objective and common approach to the standards and specifications process should be developed
PRINC-09	Interoperability agreements	Establish interoperability agreements in all layers, complemented by operational agreements and change management procedures	EIF-26	Interoperability	Interoperability agreements in all layers, complemented by operational agreements and change management procedures, are needed to implement TOOP architecture and should be foreseen
PRINC-10	Organisational relationships	Clarify and formalise organisational relationships between the participants in the Once-Only processes	EIF-29	Interoperability	Clarification and formalization of organisational relationships between stakeholders are needed to implement TOOP architecture and should be foreseen
PRINC-13	Infrastructure for European public services	Decide on a common scheme for interconnecting loosely coupled service components and put in place and maintain the	EIF-35	Interoperability	Infrastructure for establishing and maintaining European public services should be decided,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

		necessary infrastructure for establishing and maintaining European public services			developed, and put in place
PRINC-14	Reusable services and information sources	Develop a shared infrastructure of reusable services and information sources that can be used by all public administrations	EIF-36	Interoperability	The infrastructure for establishing and maintaining European public services should comprise reusable services and information sources that can be used by all public administrations
PRINC-15	eIDAS Trust Services	The TOOP architecture should use trust services according to the Regulation on eID and Trust Services as mechanisms that ensure secure and protected data exchange in public services	EIF-47	Security	Mechanisms are in place to ensure secure and protected data exchange in public services
PRINC-16	Data Minimization	The information exchanged between the participants of the system should be limited to the data required by the processing	Privacy-by-Design	Privacy	Privacy risks are reduced due to data minimization
PRINC-17	Purpose Limitation	The information exchanged between the participants of the system should only be used for the explicitly agreed purpose	Privacy-by-Design	Privacy	Privacy risks are reduced due to using information only for the explicitly agreed purpose
PRINC-18	Consent Management	When the consent of the user is	Privacy-by-Design	Privacy	Privacy risks are reduced due to

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

		necessary for data protection purposes, it shall be obtained in accordance with Regulation (EU) 2016/679 and Regulation (EU) 45/2001			obtaining the consent of the user where necessary
PRINC-19	Semantic Mediation	A guide to the terminology used and/or a glossary of relevant terms used in each base registry should be made available for both human and machine-readable information purposes. Develop interfaces with base registries and authoritative sources of information, publish the semantic and technical means and documentation needed for others to connect and reuse available information.	EIF 37-39	Interoperability	A shared representation of the information available in authoritative sources should be in place, both for human and machines

2.4.4. Architecture Requirements Specifications

In this phase, the identified requirements are formulated and associated with the quality model. The specified architecture requirements are traced back to their sources. The resources are:

- Pilot Areas, e.g. 'PA1.1-REQ-8' refers to TOOP Pilot Area 1.1 requirement REQ-8, 'PA2.1-DATA-2' refers to TOOP Pilot Area 2.1 requirement DATA-2.
- EIF recommendations e.g. ‘EIF-45’ refers to recommendation 45.
- SDGR e.g. 'SDGR.Art12.4' refers to draft SDGR article 12.4.
- Legal requirements from D2.5 e.g. ‘LEG-GA-03’ refers to Good administration requirement 3, ‘LEG-CTRL-02' refers to Control requirement 2.
- Principles from the previous section e.g. PRINC-18.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

Table 3: Architecture requirement specifications

ID	Description	Rationale	Quality attribute
ASR-FUNC-01	Data Consumer must be informed about the conditions and terms of use of the retrieved information	PA1.1-REQ-8 PA1.2-REQ-11 PA1.3-REQ-8	Functional Suitability
ASR-FUNC-02	Where the completion of a procedure requires a payment, users are able to pay any fees online through cross-border payment services, including, at a minimum, credit transfers or direct debits as specified in Regulation (EU) No 260/2012 of the European Parliament and of the Council	SDGR-Art.11.1.e EIF-45 PA1.1-REQ-18 PA1.2-REQ-21 PA1.3-REQ-18 PA2.1-BUSINESS-1 PA2.2-BUSINESS-1	Functional Suitability
ASR-FUNC-03	Data Consumer may use the system to send messages to the Data Provider	PA1.1-REQ-15 PA1.2-REQ-18 PA1.3-REQ-15	Functional Suitability
ASR-FUNC-04	Data Provider may provide data services for verification of specific conditions, i.e. DP replies True/False to specific statement.	PA2.1-PULL-1 PA2.2-PULL-1	Functional Suitability
ASR-PERF-01	DP should not unnecessarily delay the process of transmitting the Data to the DC	PA1.NiceToHave	Performance Efficiency
ASR-PERF-02	DP should communicate the expected level of service associated with the processing of the request for Data from the DC	EIF-19	Performance Efficiency
ASR-IOP-01	Data Consumer must be able to request Evidence about the User from Data Provider	SDGR.Art12.4 SDGR.Art12.2 PA1.1-REQ4 PA1.2-REQ-4 PA1.2-REQ-5 PA1.3-REQ-4	Compatibility Interoperability
ASR-IOP-02	Data Provider must be able to automatically process request for Evidence from Data Consumer	SDGR-Art12.2 PA1.1-REQ-7 PA1.2-REQ-9 PA1.2-REQ-10 PA1.3-REQ-7	Compatibility Interoperability

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

ASR-IOP-03	Data Provider must be able to transmit requested Evidence to Data Consumer	SDGR.Art12.2 PA1.1-REQ4 PA1.2-REQ-4 PA1.2-REQ-5 PA1.3-REQ-4	Compatibility Interoperability
ASR-IOP-04	Data Consumer must be able to unambiguously understand and automatically process Evidence retrieved from Data Provider	SDGR-Art12.2 PA1.1-REQ-9 PA1.2-REQ-12 PA1.3-REQ-9 PA2.1-DATA-2 PA2.2-DATA-2	Compatibility Interoperability
ASR-IOP-05	Data Consumer and Data Provider must be technically able to exchange information	SDGR-Art12.2 PA1.1-REQ-3 PA1.2-REQ-3 PA1.3-REQ-3	Compatibility Interoperability
ASR-COE-01	The Competent Authorities must be able to reuse existing national or EU infrastructure, including the BRIS infrastructure	PA1.1-REQ-19 PA1.2-REQ-22 PA1.3-REQ-19 PA2.1-ARCHITECTURE-1 PA2.2-ARCHITECTURE-1	Compatibility Coexistence
ASR-SEC-01	The transmission of an Evidence from DP to DC must guarantee the confidentiality of the exchanged Evidence	SDGR-Art12.2 PA1.1-REQ-16 PA1.1-REQ-17 PA1.2-REQ-19 PA1.2-REQ-20 PA1.3-REQ-16 PA1.3-REQ-17 PA2.1-SECURITY-3 PA2.2-SECURITY-3	Security
ASR-SEC-02	The transmission of an Evidence from DP to DC must guarantee the integrity of the exchanged Evidence	SDGR-Art12.2 PA1.1-REQ-16 PA1.1-REQ-17 PA1.2-REQ-19 PA1.2-REQ-20 PA1.3-REQ-16 PA1.3-REQ-17	Security

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

		PA2.1-SECURITY-3 PA2.2-SECURITY-3	
ASR-SEC-03	DC must be informed about the level of availability of Data provided by DP.	PA1.1-REQ-8 PA1.2-REQ-11 PA1.3-REQ-8	Security
ASR-SEC-04	The Evidence provided by DP must be available according to the legal requirements	EIF-27	Security
ASR-SEC-05	Data Consumer must ensure that the request for Evidence was initiated by the User, unless not legally required	SDGR.Art12.4	Security
ASR-SEC-06	Data Provider is responsible for transmitting the requested Evidence in accordance with the confidentiality and integrity requirements,	SDGR.Art12.4	Security
ASR-SEC-07	DP should not provide the evidence if the request does not conform to the legal requirements of DP	EIF-27	Security
ASR-SEC-08	If Data Provider cannot transmit any evidence, data provider must give reasons for this.	LEG-GA-03	Security
ASR-SEC-09	Appropriate audit and logging measures must be implemented to ensure that any exchange of evidence organised under the OOP can be verified by competent authorities in case of disputes (including the identification of the sending and receiving competent authorities, the time of the exchange, and the integrity/authenticity of the exchanged data itself).	LEG-CTRL-02	Security
ASR-SEC-10	Data Consumer must authenticate the *User* before requesting Evidence from Data Provider when authentication is required	PA1.1-REQ-1 PA1.2-REQ-1 PA1.2-REQ-2 PA1.3-REQ-1	Security
ASR-SEC-11	DC must identify the Data Subject associated with the User.	LEG-CTRL-01 PA1.1-REQ-2 PA1.2-REQ-2	Security
ASR-SEC-12	DP must validate that the User is authorized to retrieve information about the Data Subject	LEG-CTRL-01 PA1.1-REQ-2 PA1.2-REQ-2	Security

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

ASR-SEC-13	The participants to the Evidence exchange process must be identified, specifically DC and DP	PA2.1-SECURITY-1 PA2.2-SECURITY-1	Security
ASR-SEC-14	DP must verify that data consumer is an authorized digital public service before transmitting the required Evidence	PA2.1-SECURITY-2 PA2.2-SECURITY-2	Security
ASR-SEC-15	Data Consumer must be able to prove that the User explicitly requested the retrieval of Evidence from the Data Provider	SDGR.Art12.4 PA1.1-REQ-5 PA1.2-REQ-6 PA1.2-REQ-7 PA1.3-REQ-5	Security
ASR-SEC-16	Data Provider must be able to prove the reception of the transmitted Evidence by Data Consumer	PA1.1-REQ-11 PA1.2-REQ-14 PA1.3-REQ-11	Security
ASR-SEC-17	Data Consumer must be able to prove the reception of the Evidence request by Data Provider	PA1.1-REQ-10 PA1.2-REQ-13 PA1.3-REQ-10	Security
ASR-SEC-18	The Evidence transmitted by Data Provider to Data Consumer shall be limited to what has been requested	SDGR.Art12.6 PRINC-17	Security
ASR-SEC-19	The Evidence transmitted by the Data Provider to the Data Consumer shall only be used for the purpose of the procedure for which the evidence was exchanged	SDGR.Art12.6 PRINC-18	Security
ASR-SEC-20	When the consent of the user is necessary to retrieve Evidence from the Data Provider, it shall be obtained in accordance with Regulation (EU) 2016/679 and Regulation (EU) 45/2001	SDGR.Art12.6 PRINC-19	Security
ASR-SEC-21	Data provided by the Data Provider to the Data Consumer may not be provided by the Data Consumer to third parties, *except where third parties are required to achieve the communicated purpose, or unless it has been consented by the User*	LEG-GA-04 PA2.1-LEGAL-2 PA2.2-LEGAL-2 PRINC-18	Security
ASR-REL-01	The level of availability of the exchange process must comply with the legal requirements	EIF-27	Reliability
ASR-USA-01	It must be possible to operate the Evidence exchange process according to various deployment models: component on premise,	EIF-35	Usability

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

	service on premise, mutualized and centralized service		
ASR-ACC-05	The legal value and meaning of data should not be altered crossing a national border	PA2.1-DATA-1 PA2.2-DATA-1	Data Accuracy
ASR-CONS-01	The User has the possibility to preview the evidence to be used by the Data Consumer and to check the validity of the retrieved information	SDGR-Art12.2 PA1.1-REQ-6 PA1.2-REQ-8 PA1.3-REQ-6	Data Consistency
ASR-COMP-01	The User may be able to add information not provided by the data provider(s)	PA1.1-REQ-13 PA1.3-REQ-13	Data Completeness
ASR-CRED-01	The authenticity of the data transmitted by DP must be trusted by DC	EIF-37	Data Credibility
ASR-CURR-01	Data Consumer can subscribe to change events associated with the Data life cycle	PA2.1-PUSH-4 PA2.2-PUSH-4	Data Currentness
ASR-CURR-02	Modification of data are asynchronously notified, on a predefined schedule, to the Data Consumer that have subscribed to the notification service. A Data consumer has the possibility to unsubscribe to the notification service	PA2.1-PUSH-1 PA2.1-PUSH-2 PA2.1-PUSH-3 PA2.2-PUSH-1 PA2.2-PUSH-2 PA2.2-PUSH-3	Data Currentness

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

3. TOOP Reference Architecture

This chapter provides a short summary of the TOOP Reference Architecture. The main version of the architecture with detailed diagrams and explanations is available on the TOOP D2.3 documentation space in Confluence (please see the Glossary).

3.1. Architecture Description

The architecture is described along the business, information system and technology dimensions. It is complemented with specific views addressing cross-cutting quality concerns, such as Security Architecture and Trust Architecture.

3.1.1. Business Architecture

The business architecture is first addressed from the information processing viewpoint[9]. Figure 7 specifies the operational end-to-end processes of executing Once Only Principle as part of the delivery of a public eService. The business process is designed to meet the business requirements.

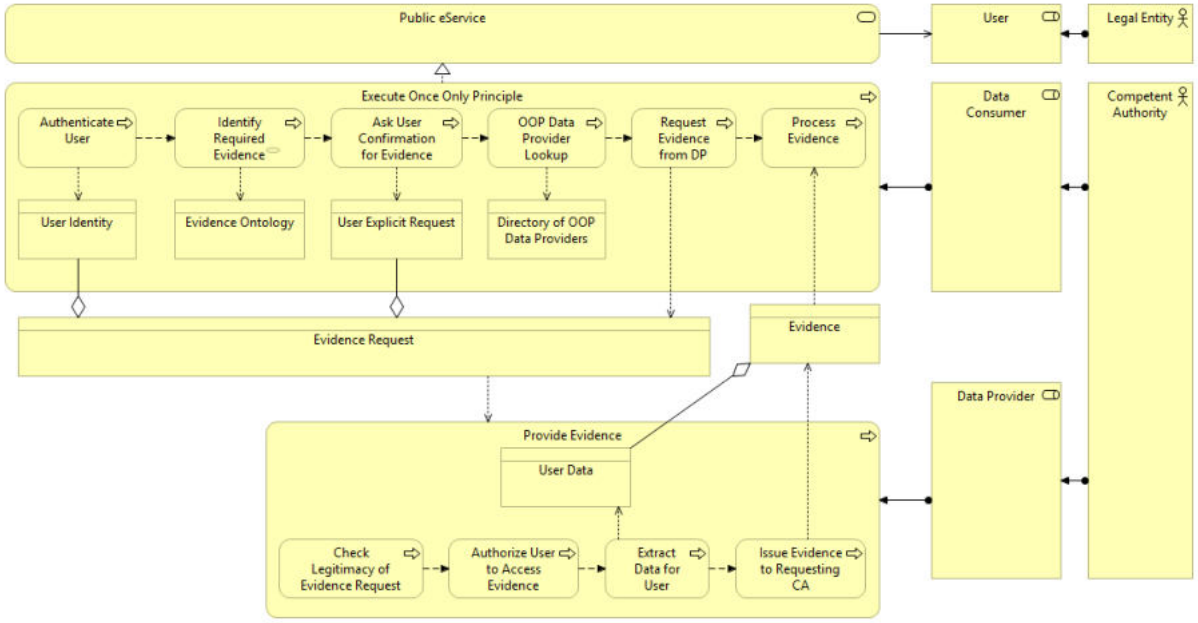


Figure 7: End-to-end Business Process

In Figure 8, a capability map is depicted, which represents the responsibilities of each business role involved in TOOP in terms of required business capabilities. It generically should be interpreted the following way: to participate in TOOP in the role of a Business Role, an organisation is required to deploy the Business Capabilities assigned to that business role.

[9] http://wiki.ds.unipi.gr/display/TOOPRA/Business+Architecture

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

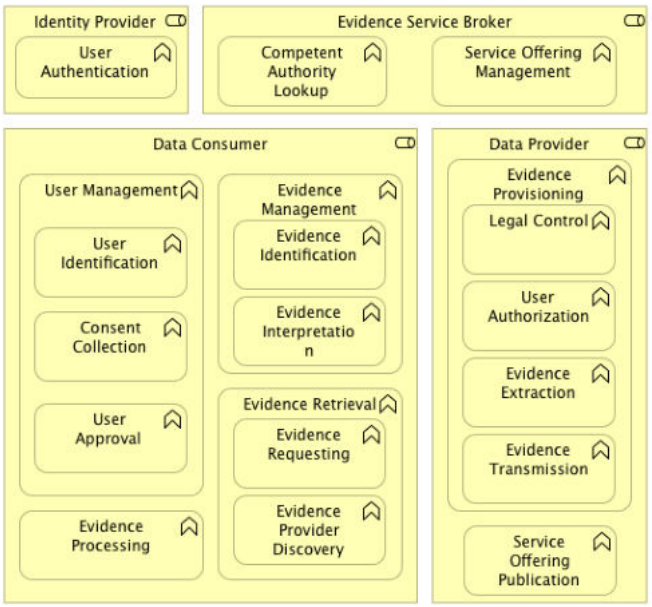


Figure 8: Capability Map

The Capability Map enables the participants to efficiently and easily identify the required business capabilities associated with the role they will play. It is also a valuable tool for architects and designers to support gap analysis when transitioning to TOOP.

Figure 9 specifies the Exchange of Business Information between the various roles participating in TOOP. It generically should be interpreted the following way: as part of a Business Capability deployed by a Business Role, an Exchange of Business Information takes place with another Business Role.

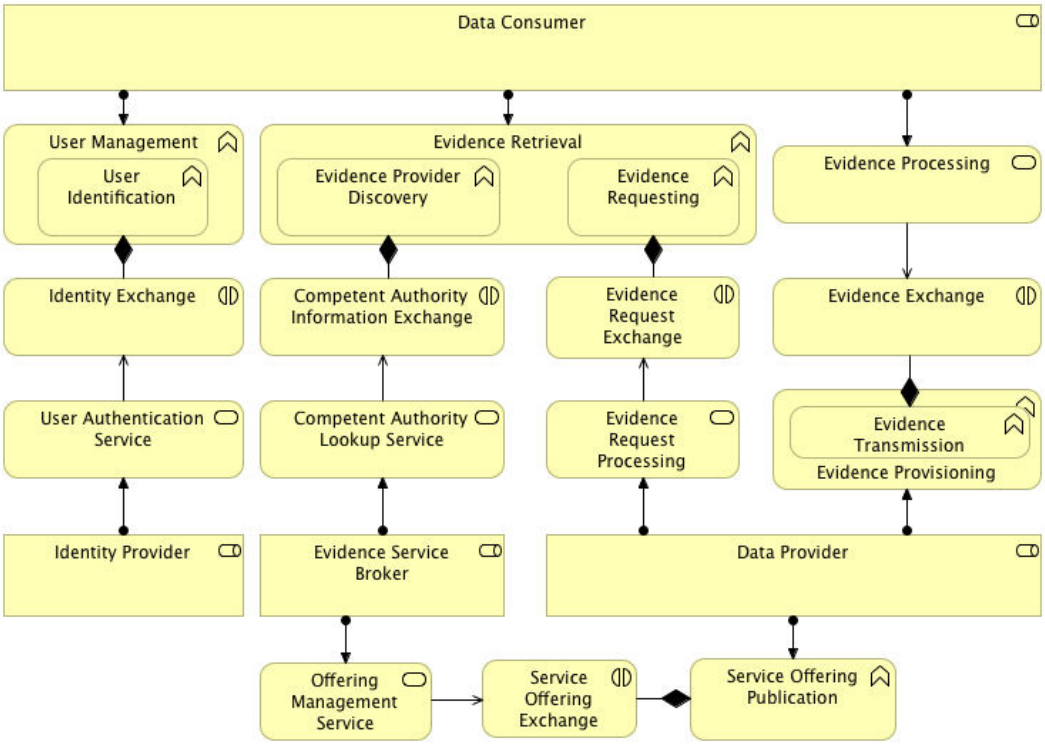


Figure 9: Exchange of Business Information

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

The Business Interactions diagram enables architects and designers to efficiently and easily identify the major organisational interoperability points, as each Exchange of Business Information requires to be addressed from an IOP perspective. In TOOP there are 4 main exchanges of business information:

- Identity Exchange, between Data Consumer and Identity Provider
- Competent Authority Information Exchange, between Data Consumer and Evidence Service Broker
- Evidence Request Exchange, between Data Consumer and Data Provider
- Evidence Exchange, between Data Provider and Data Consumer

3.1.2. Information System Architecture

The IS Architecture realizes the business capabilities through the use of application components and functionalities[10].

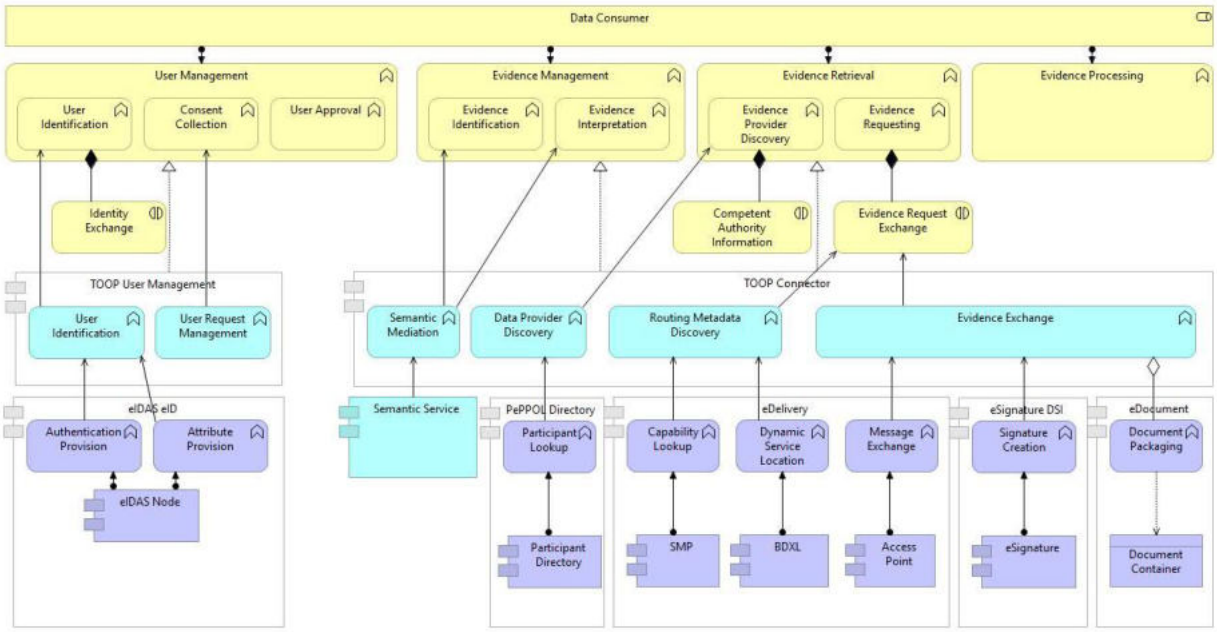


Figure 10 specifies how each DC operational capabilities are realized. The solution introduces 2 main components, encapsulating application functionalities:

- TOOP User Management component, responsible for all functionalities required to support user management in TOOP;
- TOOP Connector component, responsible for all functionalities required to actually exchange Evidence in TOOP.

[10] http://wiki.ds.unipi.gr/display/TOOPRA/IS+Architecture

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

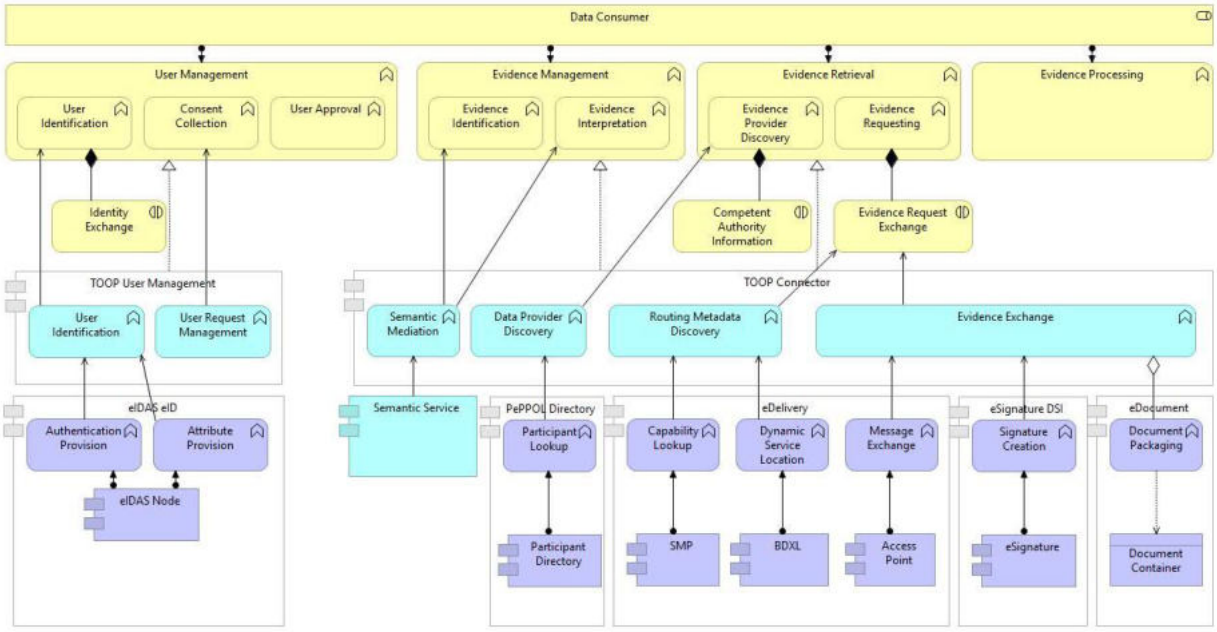


Figure 10: DC Operational Capabilities Realization

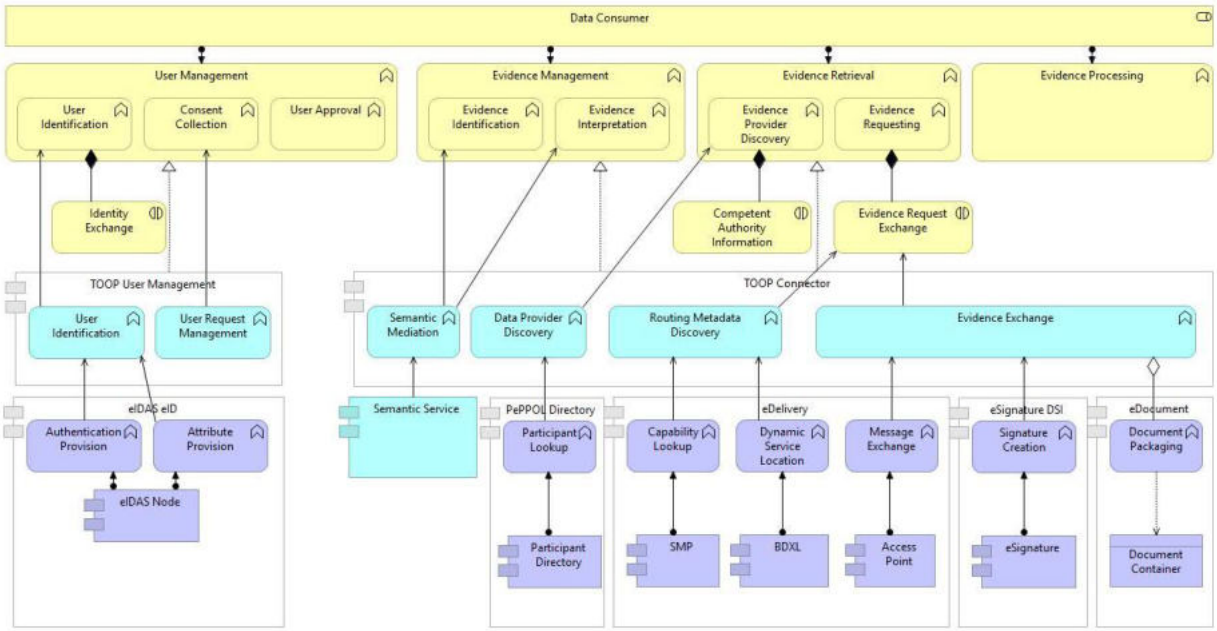


Figure 10 also specifies how the existing Building Blocks are leveraged to realize the required functionalities.

Figure 11 specifies how each DP operational capabilities are realized. The solution introduces the 2 main TOOP components, i.e. TOOP Connector and TOOP User Management.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

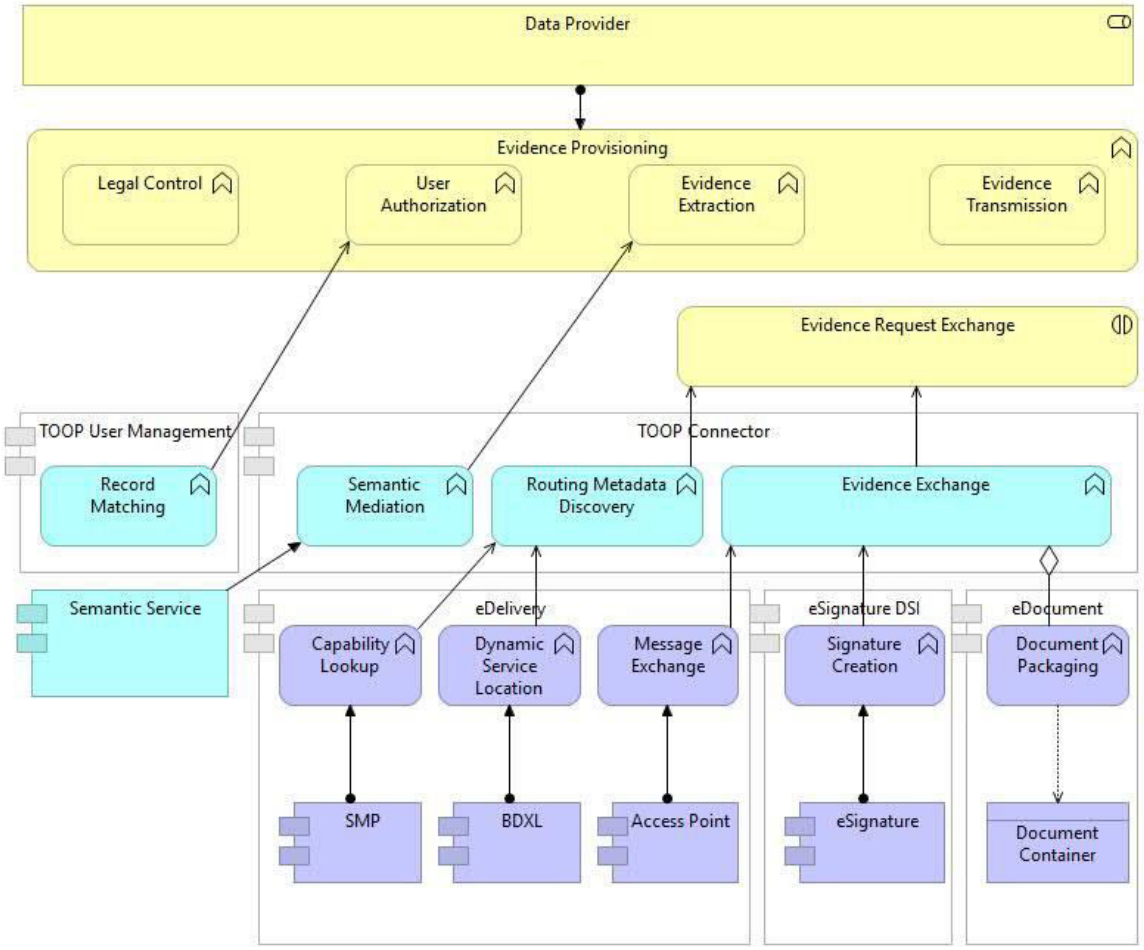


Figure 11: DP Operational Capabilities Realization

3.1.3. Technology Architecture

The Technology Architecture provides logical components and services that are required to support the deployment of business capabilities and application components described in the Information System Architecture[11]. It comprises both the European infrastructure components and the components within the MS responsibility. The components within the MS responsibility include the components maintained by the Member State and by its Competent Authorities.

TOOPRA is a reference architecture and therefore does not directly specify the deployment model. The current TOOP Technology Architecture model is available on the TOOP D2.3 documentation space in Confluence. It comprises two components:

- the Deployment Topologies view,
- the Network and Communication view.

Due to a wide variety of information systems that can be developed using the Technology Architecture, there is no fixed way of how to deploy TOOP services. In the Deployment Topologies view, three different deployment topologies are presented. The impact of different topologies on the business organization and governance is analysed with each deployment option. Each deployment topology

[11] http://wiki.ds.unipi.gr/display/TOOPRA/Technology+Architecture

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

comprises the central European infrastructure components, components deployed on the Member State level, and components deployed on a Competent Authority level.

The Network and Communication view focuses on how the system is implemented from the perspective of the communications engineer. It helps to assure that within the system, appropriate communications and networking services are developed and deployed by relevant stakeholders. From the Network and Communication perspective, a TOOP application uses the following components: communication networks in the Member States, TOOP central communications infrastructure, the eIDAS network[12], and the Internet.

The standards/protocols to be used are presented in the Information System Architecture view.

3.1.4. Cross-Cutting Concerns

The TOOP Reference Architecture Cross-Cutting Concerns comprise security architecture, trust architecture, and management aspects[13].

Information security and trust are overlapping, but not identical. The standard ISO/IEC 27000:2016 defines information security as preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, trustworthiness, accountability, non-repudiation, traceability, and reliability can be involved.

Trust establishment guarantees, that the origin and the destination of the data and documents are authentic (authenticity) and trustworthy (trustworthiness), and that data and documents are secured against any modification by untrusted parties (integrity) (Cofta 2007; Gaurav, Sarfaraz, and Singh 2014; Winslett 2003). Additional constituents of trust management - accountability, non-repudiation, traceability, and confidentiality as a component of trust management - can be supported by maintaining processing logs and other controls, encrypting data and documents during the transmission, etc.

The TOOP security architecture is based on the ISO/IEC 27000-series of standards. Based on ISO/IEC 27000:2016, the Security Architecture section of the TOOP D2.3 documentation space in Confluence proposes the notion of an Information Security Management System (ISMS), consisting of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization to protect its information assets. It describes the following steps needed to establish, monitor, maintain, and improve an ISMS:

- identify information assets;
- identify associated information security requirements;
- assess and treat information security risks;
- select and implement relevant controls to manage unacceptable risks;
- monitor, maintain and improve the effectiveness of ISMS.

The Trust Architecture section of the TOOP D2.3 documentation space in Confluence proposes similar steps with regard to trust establishment.

The Management Aspects concern two issues: governance of TOOPRA shared resources and principles of OOP project development. The shared resources include the central European infrastructure components providing the TOOP network management. The governance model of these resources will be provided by TOOP Task 2.5 Sustainability and Governance in its deliverable D2.13 Sustainability aspects of OOP. In the Management Aspects section, the second aspect - principles of OOP project

[12] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2018/01/15/EU+Login+Authentication+System+Connected+to+the+eIDAS+Network

[13] http://wiki.ds.unipi.gr/display/TOOPRA/Cross-Cutting+Concerns

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

development - is presented. It includes prerequisites and technical development activities of an OOP project.

3.2.Architecture Repository and the D2.3 wiki component

TOOP Reference Architecture is maintained in an architecture repository, which describes each architecture element in detail. The architecture repository can be accessed at http://wiki.ds.unipi.gr/display/TOOPRA. The structure of the repository is aligned with the architecture framework.

The architecture repository also represents the D2.3 wiki component in Confluence.

3.3.Architecture Models

According to ISO 42010, the views of TOOPRA are specified by models expressed in ArchiMate. The architecture models are maintained in a git repository at https://github.com/TOOP4EU/toop-goopra-models. The link to the repository is provided for information only, the repository itself is not part of the current deliverable.

The diagrams presented in this report and on the wiki are extracted from the models in the repository.

Most technical level diagrams of TOOP Reference Architecture use the default iconography of the ArchiMate language[14].

[14] http://pubs.opengroup.org/architecture/archimate3-doc/apdxa.html#_Toc489946151

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

4. Architecture Life Cycle Management

A set of Life Cycle management (LCM) processes has been defined, with the aim of providing simplified processes, a better support to stakeholders (including the CEF), fostering user adoption and transparency to the change management of TOOP Reference Architecture. The processes were designed in the spirit of ISO 20000, as a set of IT services provided to a customer. In this case, the customers are the stakeholders of TOOP Reference Architecture.

Independently of how the project receivers will manage TOOPRA life cycle after the hand-over, these IT services have been structured in a generic way and implemented in the JIRA platform, which will facilitate the transfer of support history and open issues to the CEF and other stakeholders.

4.1.1. Life Cycle Management Process

LCM services

The following IT LCM services are provided to TOOPRA LCM:

Table 4: LCM services

Service name	Meme
Support management	'Please perform this with the reference architecture
Change management	'I'd like a new feature to be added in the reference architecture'
Release management	'When will changes be accepted and available?'

Service design

The service design is summarized in Table 5.

Table 5: Service design

Service	Internal outcomes	Customer outcomes
Support Management	Task (work)	Report, info
Change management	Risk assessment, source code, deployable binary	Change acceptance/rejection
Release Management	Release plan	TOOPRA updated, release notes

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Service architecture

The service architecture can be summarized as per the figure below:

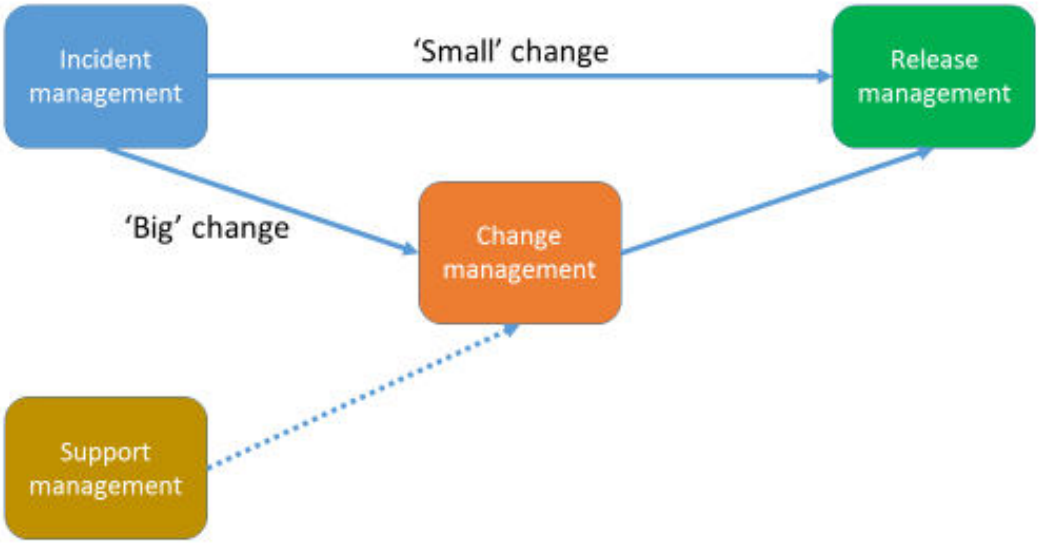


Figure 12: Service Architecture

Service strategy

The service strategy adopted is:

- Ticket/process based (JIRA)
- Make it easy to track progress and effort, consolidate PM's
- Keep it simple towards the customer, however
- Try to get 90% of info from the 1st interaction
- Simple workflows: only customer added-value activities
- CAB (Change Advisory Board) can support the Lead Architect with risk assessment and recommendations

To simplify the service implementation, the Release Management process is embedded in both Incident Management and Change Management processes, providing full history and transparency of changes (issue-to-production).

TOOPRA issues as per Table 6 are reported and tracked on the JIRA platform provided by TOOP partner University of Piraeus.

Table 6: JIRA Projects

Item	JIRA link
TOOPRA	http://jira.ds.unipi.gr/projects/TOOPRA/

4.1.2. TOOPRA Life cycle management

Change management process

The overall process for TOOPRA support includes the Lead Architect dispatching new opened issues to WP2 technical experts, which will do risk assessment and recommendation on change acceptance/rejection. The Architecture Board can be involved as Change Advisory Board (CAB) for complex changes. Typically, the experts discuss the matter as appropriate in JIRA itself and in case of

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

favourable opinion propose a change by editing private, next-release document pages in the TOOPRA Wiki[15]. The Lead Architect then picks up the ticket and continues through the embedded Release Management process.

Each ticket in TOOPRA JIRA is cross-linked to the corresponding page in the TOOPRA Confluence wiki, providing full history of changes and ease of navigation between the two platforms. The ticket also features a specific field to signal if public consultation is warranted. This is particularly useful to address issues that imply changes to existing standards used in TOOP, e.g. ETSI, providing full transparency.

Figure 13 depicts the Change Management workflow. On the lower left corner, there is the complementing state-machine.

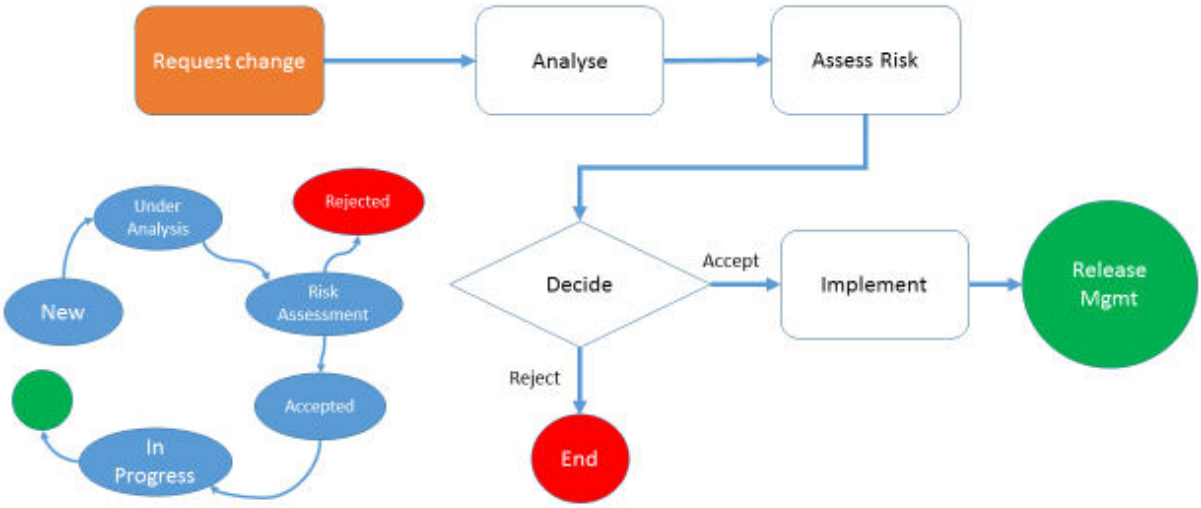


Figure 13: Change Management Process

Release management process

After the acceptance of a change request the Lead Architect eventually communicates the release plan to stakeholders, in the form of release notes for each regular release (e.g., monthly). For accepted changes, the process is closed when the changes are reflected in some published version of TOOPRA wiki.

By connecting JIRA and Confluence platforms, it is possible to relate tickets in JIRA to specific TOOPRA releases, whose content and versioning is managed in Confluence.

Figure 14 depicts the Release Management process workflow. By embedding this process in Change Management, no further JIRA workflow is needed. The embedding translates into adding three more states in the end of IM and CM issues/tickets.

Figure 14: Release Management Process

[15] http://wiki.ds.unipi.gr/display/TOOPRA/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Support management process

This process was designed to be very generic, to provide architecture support besides change requests.

Basically, the Lead Architect distributes the support request tickets to technical experts, who are expected to document discussions with the requester, peers, external organizations, etc. and ultimately fulfil the request.

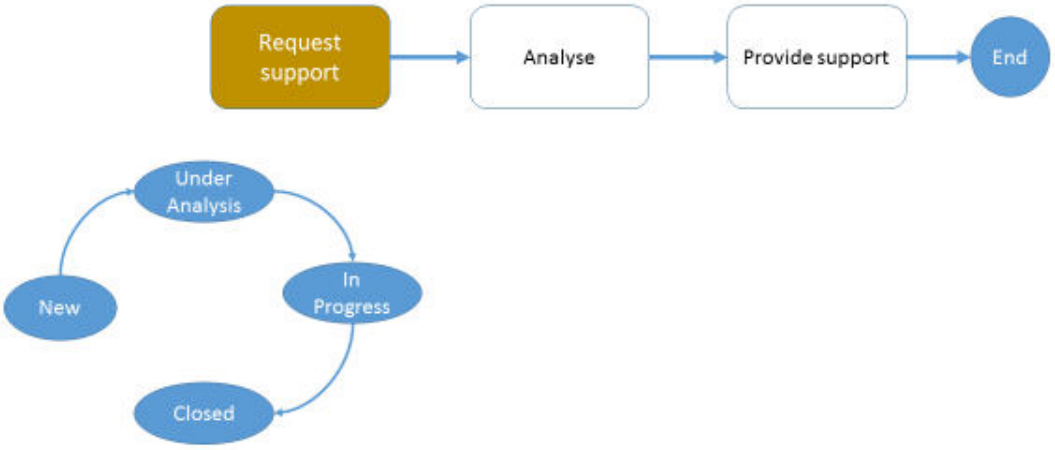


Figure 15: Support Management Process

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

5. Alignment and Cooperation with EC Initiatives

Besides the internal collaborations, TOOP Architecture team seeks to align and cooperate with other relevant EC Initiatives. This section summarizes the state of the cooperation.

5.1. EIRA

The TOOP Architecture team followed a one-day workshop by Raul Abril, which took place on 1 June 2018, to better understand the ins and outs of the European Interoperability Reference Architecture (EIRA).

The main result of the workshop was that EIRA and TOOPRA can coexist, as they complement each other. The primary concern of EIRA is to support interoperability of public services at an EU level, while TOOPRA is focused on supporting the OOP in cross-border exchange of documents and evidences. Synergies between the two architectures are evident, since they address different concerns of the same stakeholders. Public services can benefit from cross-border interoperability and from the application of the OOP.

5.2. Power and Mandates

Action 2016.12 of the ISA programme aims at creating a shared European data model for a cross-border interoperable representation of powers and mandates information. This representation will allow the seamless exchange of information about the powers and mandates of natural person when representing a legal person in the context of an eID exchange process.

Currently there is no shared European taxonomy about representation powers and mandates and this fact prevents powers/mandates information originated in one country from being directly machine processable in other. The TOOP project has proposed semantic mediation as a stop-a-gap measure for semantic interoperability in the exchange of this business information, but the development of an ontology for powers and mandates can streamline the overall process of identification and release of consent in TOOP transactions.

TOOP is a Stakeholder for this ISA action and an alignment meeting with ISA has been held in June 2018 in Brussels. TOOP can provide a valuable input to ISA and test the results of this action in the context of the Pilots. From an architecture point of view, the results of the Power and Mandates should integrate the Core Person and Core Business vocabularies with a common taxonomy for representation powers/mandates linked to legal entities, as these vocabularies are already part of the Core TOOP semantic model.

5.3. Access to Base Registries

A synergy and an alignment between TOOPRA and the ISA Action for Access to Base Registries (ABR) is desirable. Up to now some members of the TOOP architecture team and the CCTF have participated in the ABR seminars organized by ISA/Everis.

Base registries are part of the EIF conceptual model for integrated public services provision (source: Annex to EIF COM(2017) 134 final, Part 4). The conceptual model lays a basis for interoperability by design of European public services. To be interoperable, they should be designed in accordance with the proposed model.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

According to EIF, a base registry is *"a trusted and authoritative source of information under the management of some organization which can and should be digitally reused by others. Base registries are reliable sources of basic information on data items such as people, companies, vehicles, licences, buildings, locations and roads. This type of information constitutes the 'master data' for public administrations and European public service delivery. 'Authoritative' here means that a base registry is considered to be the 'source' of information, i.e. it shows the correct status, is up-to-date and is of the highest possible quality and integrity"*[16].

Based on this definition, Base Registries are a basic component of TOOP environment, even if their inner structure is not part of TOOPRA. In some sense, TOOPRA should represent the main model for a base registry framework in compliance to EIF, describing *"the agreements and infrastructure for operating base registries and the relationships with other entities*".

The following table reports the technical recommendations applicable to Base registries, as listed in the EIF Annex, part 4.

Table 7: EIF technical recommendations applicable to base registries

	EIF recommendation
Recommendation 37:	Make authoritative sources of information available to others while implementing access and control mechanisms to ensure security and privacy in accordance with the relevant legislation.
Recommendation 38:	Develop interfaces with base registries and authoritative sources of information, publish the semantic and technical means and documentation needed for others to connect and reuse available information.
Recommendation 39:	Match each base registry with appropriate metadata including the description of its content, service assurance and responsibilities, the type of master data it keeps, conditions of access and the relevant licences, terminology, a glossary, and information about any master data it uses from other base registries.
Recommendation 40:	Create and follow data quality assurance plans for base registries and related master data.

The ISA ABR action (Access to Base Registries) is aimed at assessing the needs for a Framework for Base Registry Access, based on best practices and all the different activities associated with master data management. One of their objectives is to create a base registry framework that 'describes the agreements and infrastructure for operating base registries and the relationships with other entities', as specified in the new version of the EIF.

Up to now, this action produced an overview of reusable solutions from EU countries in order to facilitate the interconnection and access to base registries, a factsheet of the state-of-affairs in the EU countries, as well as the EFTA countries has also been performed, covering both the individual base registry level, as well as the interconnection level and a series of webinars for the exchange and promotion of best practices among EU countries that aim at speeding up the development and overcoming problems that are being faced by developers.

[16] https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

As part of the action, they developed guidelines for public administrations, to make the base registries more accessible and efficiently connected, giving them the status of authentic source of data also in a cross-border exchange of information. The guidelines include recommendations and how-to on all interoperability aspects concerning base registries.

5.4. Catalogue of Services

The ISA action about the catalogue of services is aimed at defining a set of tools to create and manage machine-readable descriptions of public services. These descriptions should facilitate the discovery and fruition of services within and across national borders.

The catalogue of services is based on the Core Public Service Vocabulary Application Profile (CPSV-AP), which is a data model for harmonising the way public services are described on eGovernment portals.

Currently the service discovery in TOOP is based on the SML-SMP building block – a synergy between the two initiatives can benefit both parties.

5.5. SDG Common Architecture

The aim of this action is to provide the technical basis for the implementation of the future Single Digital Gateway Regulation[17]. The expected stakeholders of the action are Member States authorities (national, regional, local levels). The TOOP Reference Architecture deliverables are reviewed by the Beneficiary Managers of participating Member States which may potentially create synergies between the TOOP project and the SDG Common Architecture action.

5.6. CEF

The TOOP Architecture team has had several joint workshops involving CEF representatives. The TOOP Reference Architecture makes wide use of the main CEF Building Blocks[18].

[17] https://ec.europa.eu/isa2/actions/common-architecture-single-digital-gateway_en

[18] http://wiki.ds.unipi.gr/display/TOOPRA/.IS+Architecture+v2.3

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Conclusion and future actions

The current deliverable is the third official version of the generic federated Once-Only Principle (OOP) architecture. It develops further the previous architecture deliverable versions D2.1 and D2.2, providing the Business Architecture, Information System Architecture, and Technology Architecture views complemented with views addressing cross-cutting quality concerns, such as Security Architecture and Trust Architecture. The goal model, target users and use cases, as well as presentation of the main stakeholders describe driving forces behind the architecture. The requirements analysis comprises the Architecture Principles and Architecturally Significant Requirements. A set of the TOOP Reference Architecture life cycle management processes and the state of the cooperation of the TOOP Architecture team with other relevant EC Initiatives are provided.

The architecture is aligned with existing EU frameworks (EIRA, EIF), the Connecting Europe Facility (CEF) Digital Service Infrastructures (DSIs), and the building blocks consolidated by the e-SENS project.

The architecture contributes to implementing OOP in public administrations, supports the interconnection and interoperability of national registries at the EU level, and aims to contribute to the implementation act of the forthcoming regulation about the Single Digital Gateway (SDGR).

The deliverable comprises the textual component and the wiki component. The current document is the textual component of D2.3. The wiki component is an architecture repository providing an in-depth content on the architecture views.

This deliverable is a work in progress. The next official deliverable related to the generic federated OOP architecture is D2.4 (M30, June 2019), which will introduce additions to and improvements of this deliverable including:

- Manage requirements traceability on wiki. This includes a mapping between the requirements and the architecture views and components.
- Align the TOOP architecture with the needs and requirements that come from PA3: Maritime Pilot.
- Describe the main interfaces among the architecture building blocks and the way they communicate.
- Describe the standards and protocols to be used at the Technology Architecture.
- Elaborate the role of semantics in the TOOP architecture by defining the functionality and complementarity of “Semantic Mediation” and “Semantic Service” components.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

References

TOOP Deliverables

TOOP D2.1: Tepandi, J., Verhoosel, J.P.C., Zeginis, D., Wettergren, G., Dimitriou, J., Rotuna, C., Carabat, C., Albayrak, Ö., Yilmaz, E., Lampoltshammer, T., Täks, E., Prentza, A., Brandt, P., Kavassalis, P., Leontaridis, L., Streefkerk, J.W. (2017) Generic Federated OOP Architecture (1st version). Deliverable D2.1 of the TOOP project. Available at: http://toop.eu/sites/default/files/D21_Federated_OOP_Architecture.pdf.

TOOP D2.2: Eric Grandry, Paul Brandt, Jerry Dimitriou, Sander Fieten, Carmen Rotuna, Jaak Tepandi, Ermo Täks, Jack Verhoosel, Dimitrios Zeginis (2018) Generic Federated OOP Architecture (2nd version). Deliverable D2.2 of the TOOP project. Available at: http://toop.eu/sites/default/files/D22_Generic_Federated_OOP_Architecture_Final.pdf.

TOOP D2.5: Graux, H. (2017) Overview of legal landscape and regulations. Deliverable D2.5 of the TOOP project. Available at http://www.toop.eu/sites/default/files/D25_legal_landscape_and_regulations.pdf.

TOOP D2.6: Krimmer, R., Kalvet, T., Toots, M., Cepilovs, A. (2017) Position Paper on Definition of the "Once-Only" Principle and Situation in Europe. Deliverable D2.6 of the TOOP project. Available at: http://toop.eu/assets/custom/docs/TOOP_Position_Paper.pdf.

TOOP D2.7: Kalvet, T., Toots, M., Krimmer, R. (2017) Drivers and Barriers for OOP (1st version). Deliverable D2.7 of the TOOP project. Available at: http://toop.eu/sites/default/files/D27_Drivers_and_Barriers.pdf.

Other references

Board of Innovation. 2018. "The Broker." 2018. https://www.boardofinnovation.com/business-revenue-model-examples/the-broker/.

Chen, Lianping, Muhammad Ali Babar, and Bashar Nuseibeh. 2013. "Characterizing Architecturally Significant Requirements." IEEE Software 30 (2):38–45.

Chou, By Carol C H, By Carol C H Chou, Florida Digital Archive, Florida Digital Archive, Andrea Goethals, and Andrea Goethals. 2015. "An Introduction to the European Interoperability Reference Architecture v0.9.0 (EIRA)," 65.

Cleland-Huang, J., O. Gotel, and A. Zisman. 2011. Software and Systems Traceability. Springer, London.

Cleland-Huang, J., R. Settimi, E. Romanova, B. Berenbach, and S. Clark. 2007. "Best Practices for Automated Traceability." Computer 40 (6):27–35.

Cloutier, Robert, Gerrit Muller, Dinesh Verma, Roshanak Nilchiani, Eirik Hole, and Mary Bone. 2010. "The Concept of Reference Architectures." Systems Engineering 13 (1):14–27. https://doi.org/10.1002/sys.20129.

Cofta, P. 2007. Trust, Complexity and Control: Confidence in a Convergent World. Wiley.

e-SENS. 2015. "E-SENS SAT eDocument." http://wiki.ds.unipi.gr/display/ESENS/SAT+-+eDocument+-+0.6.0.

———. 2016. "eSENS D3.7. Sustainability Plans for E-SENS Building Blocks." https://www.esens.eu/sites/default/files/e-sens_d3.7.pdf.

ETSI. 2006. "Technical Specification XML Advanced Electronic Signatures and Infrastructure; ETSI TS 101 903 v1.3.2." http://uri.etsi.org/01903/v1.3.2/ts_101903v010302p.pdf.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

———. 2013. “ETSI TS 102 918 v1.3.1 (2013-06) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC).” http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf.

European Commission. 2016. “EU eGovernment Action Plan 2016-2020 - Accelerating the Digital Transformation of Government.” Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2016 (179):1–11. https://doi.org/10.1017/CBO9781107415324.004.

———. 2017. “European Interoperability Framework – Implementation Strategy.” Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, no. COM(2017) 134 final:9.

———. 2018a. “Digital Single Market.” 2018. https://ec.europa.eu/digital-single-market/.

———. 2018b. “eGovernment & Digital Public Services.” 2018. https://ec.europa.eu/digital-single-market/en/public-services-egovernment.

European Union. 2017. “Proposal for a Regulation of the European Parliament and the Council on Establishing a Single Digital Gateway to Provide Information, Procedures, Assistance and Problem Solving Services and Amending Regulation (EU) No 1024/2012, COM/2017/0256 Final - 2017.” 2017. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017%0APC0256.

Gaurav, R., M. Sarfaraz, and D. Singh. 2014. “Survey on Trust Establishment in Cloud Computing.” In The Next Generation Information Technology Summit (Confluence), 5th International Conference. Noida, India. IEEE.

Greefhorst, Danny, and Erik Proper. 2011. Architecture Principles The Cornerstones of Enterprise Architecture. Architecture Principles The Cornerstones of Enterprise Architecture. Vol. 6. https://doi.org/10.1007/978-3-642-20279-7.

GS1. 2012. “Standard Business Document Header (SBDH) Specification.” https://www.gs1.org/standard-business-document-header-sbdh.

Harris, Steve, and Andy Seaborne. 2013. “SPARQL 1.1 Query Language.”

Ian Sommerville. 2010. “Software Engineering (Ninth Edition).” In Software Engineering (Ninth Edition), 147–75.

ISA. 2014. “Guidelines for Public Administrations on E-Document Engineering Methods.” https://ec.europa.eu/isa2/sites/isa/files/miscellaneous/guidelines-for-public-administrations-on-e-document-engineering-methods-en.pdf.

ISA specification. 2012. “ISA Interoperability Solution for European Public Administration. ‘Core Vocabularies Specification: Core Business Vocabulary, Core Person Vocabulary, Core Location Vocabulary’. ISA Specification.”

———. 2013. “ISA Interoperability Solution for European Public Administration. “Core Public Service Vocabulary Specification“. ISA Specification.”

———. 2016. “ISA Interoperability Solution for European Public Administration. ‘Core Public Organisation Vocabulary v1.0.0’. ISA Specification.”

———. 2017. “ISA Interoperability Solution for European Public Administration. ‘Core Public Service Vocabulary Application Profile 2.1’. ISA Specification.”

ISA Specification. 2016. “ISA Interoperability Solution for European Public Administration. ‘Core Criterion and Core Evidence Vocabulary v1.0.0’. ISA Specification.”

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

Koehn, Philipp. 2010. “MOSES, Statistical Machine Translation System, User Manual and Code Guide.” Technical Report, 245. http://www.statmt.org/moses/manual/manual.pdf.

Koehn, Philipp, Hieu Hoang, Alexandra Birch, Chris Callison-Burch, Marcello Federico, Nicola Bertoldi, Brooke Cowan, et al. 2007. “Open Source Toolkit for Statistical Machine Translation.” In Proceedings of the 45th Annual Meeting of the Association for Computational Linguistics (ACL), 177–80. https://doi.org/10.3115/1557769.1557821.

Krimmer, Robert, Tarmo Kalvet, Maarja Toots, and Aleksandrs Cepilovs. 2017. “The Once-Only Principle Project Position Paper on Definition of OOP and Situation in Europe.”

Mason, S. 2012. Electronic Signatures in Law. Cambridge: Cambridge University Press.

Peffers, Ken, Tuure Tuunanen, Marcus A Rothenberger, and Samir Chatterjee. 2007. “A Design Science Research Methodology for Information Systems Research.” Source Journal of Management Information Systems 24 (3):45–77. https://doi.org/10.2753/MIS0742-1222240302.

Proper, Henderik A., and Marc M. Lankhorst. 2014. “Enterprise Architecture. Towards Essential Sensemaking.” Enterprise Modelling and Information Systems Architectures 9 (1):5–21. https://doi.org/10.1007/s40786-014-0002-7.

Publications Office of the European Union. 2017. “New European Interoperability Framework. Promoting Seamless Services and Data Flows for European Public Administrations” 2017:48. https://doi.org/10.2799/78681.

Zachman, John A. 2008. “The Concise Definition of The Zachman Framework.” Zachman International, Inc. 2008. https://www.zachman.com/about-the-zachman-framework.

Zhou, J. 2001. Non-Repudiation in Electronic Commerce. Artech House.

The Open Group. 2011. “TOGAF®, an Open Group Standard.” Open Group Standard. 2011.

Winslett, M. 2003. “An Introduction to Trust Negotiation.” In Lecture Notes in Computer Science, Vol 2692. Berlin, Heidelberg: Springer.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

Contributors

Name	Surname	Organisation	Country
Paul	Brandt	TNO, the Netherlands Organisation for applied scientific research	NL
Jerry	Dimitriou	University of Piraeus Research Center	GR
Evangelos	Kalampokis	Centre for Research and Technology Hellas (CERTH)	GR
Konstantinos	Tarabanis	Centre for Research and Technology Hellas (CERTH)	GR
Jack	Verhoosel	TNO, the Netherlands Organisation for applied scientific research	NL

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

SH Schleswig-Holstein
Der echte Norden

IT-Planungsrat
Digitale Zukunft gestalten

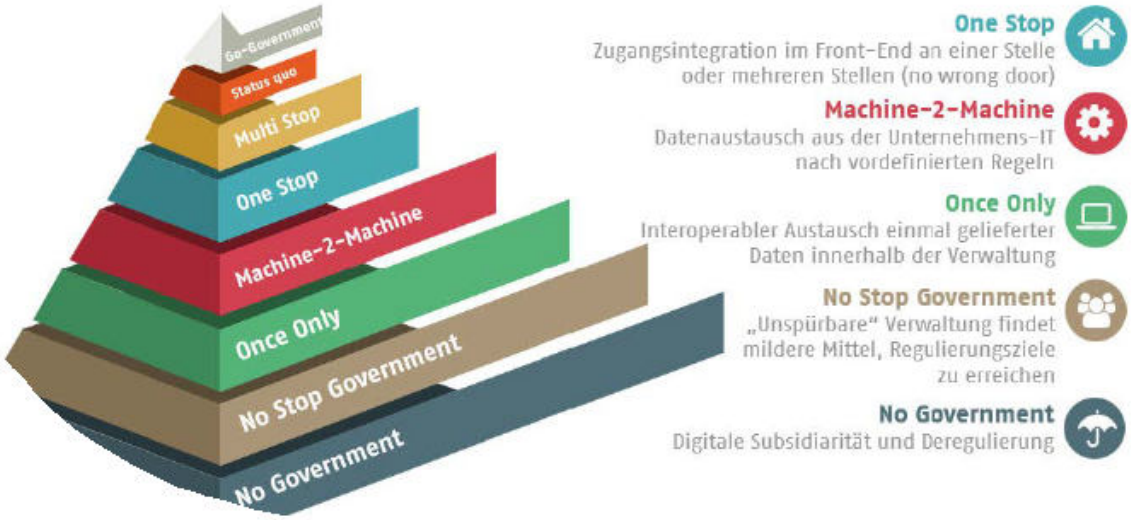
7. Fachkongress des IT-Planungsrats am 12./13. März 2019 in Lübeck

Karen Lahmann
Alexander Leder
Frank Steimke

Bessere Verwaltungsleistungen durch Wiederverwendung vorhandener Daten

Gänzlich vermieden werden kann der Kontakt zwischen Nutzer und Verwaltung, indem Daten genutzt werden, die bereits in der Verwaltung vorliegen. Hierfür hat sich vor dem Hintergrund der Datenschutz-Grundverordnung (DSGVO) sowie E-Government-Gesetzen in Bund und Ländern der Rechtsrahmen verändert (Martini & Wenzel, 2017). Demnach können mit dem Einverständnis der Nutzer in der Verwaltung gespeicherte Daten wiederverwendet und hierfür zwischen Behörden ausgetauscht werden. Dadurch müssen Bürgerinnen und Bürger sowie Unternehmen nicht immer wieder dieselben Angaben gegenüber Behörden machen, sondern nur ein einziges Mal (Once Only). Voraussetzung dafür ist allerdings die Modernisierung der disparaten deutschen Registerlandschaft.

Abbildung 7.1. Prinzipien der Umsetzung für das OZG

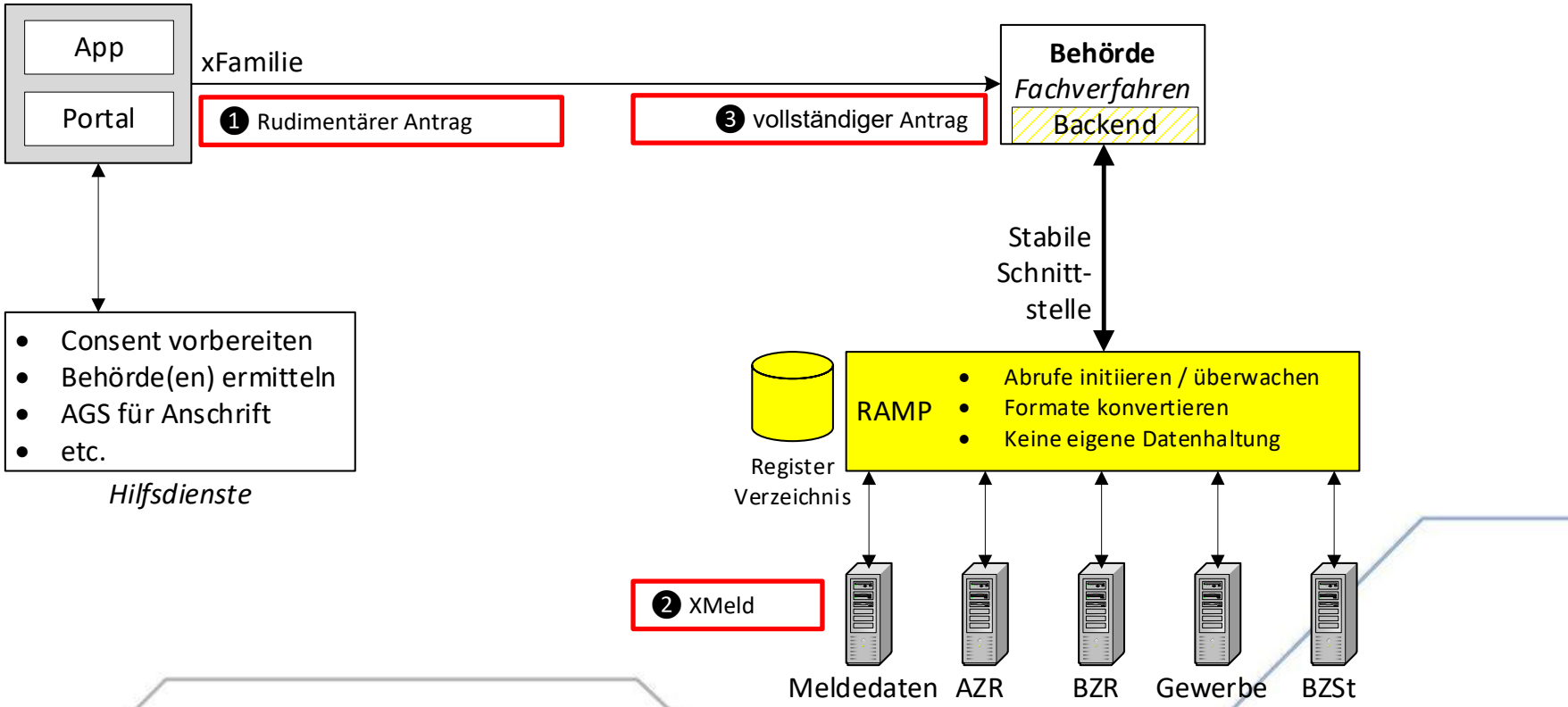


Realistisches Vorgehen

IT-Planungsrat
Digitale Zukunft gestalten

- Nicht alles neu planen
- Brücken bauen
- Bestehende Möglichkeiten nutzen
  - Technisch: bestehende Schnittstellen
  - Rechtlich: bestehende Auskunfts- und Übermittlungsverpflichtungen

Grundprinzip



Bedeutung einer Unterschrift

IT-Planungsrat
Digitale Zukunft gestalten

Name:	*Vom nPA*
Kind:	Vom Nutzer eingegeben
Anschrift:	
Familienstand:	
Kindschaftsverhältnis:	
Bankverbindung:	Vom Nutzer eingegeben
Staatsangehörigkeit:	
Gehalt:	
Inanspruchnahme:	Vom Nutzer eingegeben

Ich beantrage:

- ☐ Kindergeld
- ☐ Elterngeld
- ☐ Geburtsurkunde

(Elektronische) Unterschrift

Ich bestätige die Richtigkeit der von mir eingegebenen Daten

Vertrauen in hohe Datenqualität in Registern der Verwaltung und anderer Stellen

Basisregister im Sinne EIF

IT-Planungsrat
Digitale Zukunft gestalten

- Zuverlässige Quelle von Informationen
  - Daten sind vertrauenswürdig, authentisch und zuverlässig
  - aktuell mit größtmöglicher Qualität und Integrität
- Grundpfeiler für europäische öffentlicher Dienste
  - Daten sollen digital weiterverwendet werden
- Zuständigkeit einer einzelne Organisation
  - Erhebung, Verwendung, Aktualisierung Bewahrung von Informationen

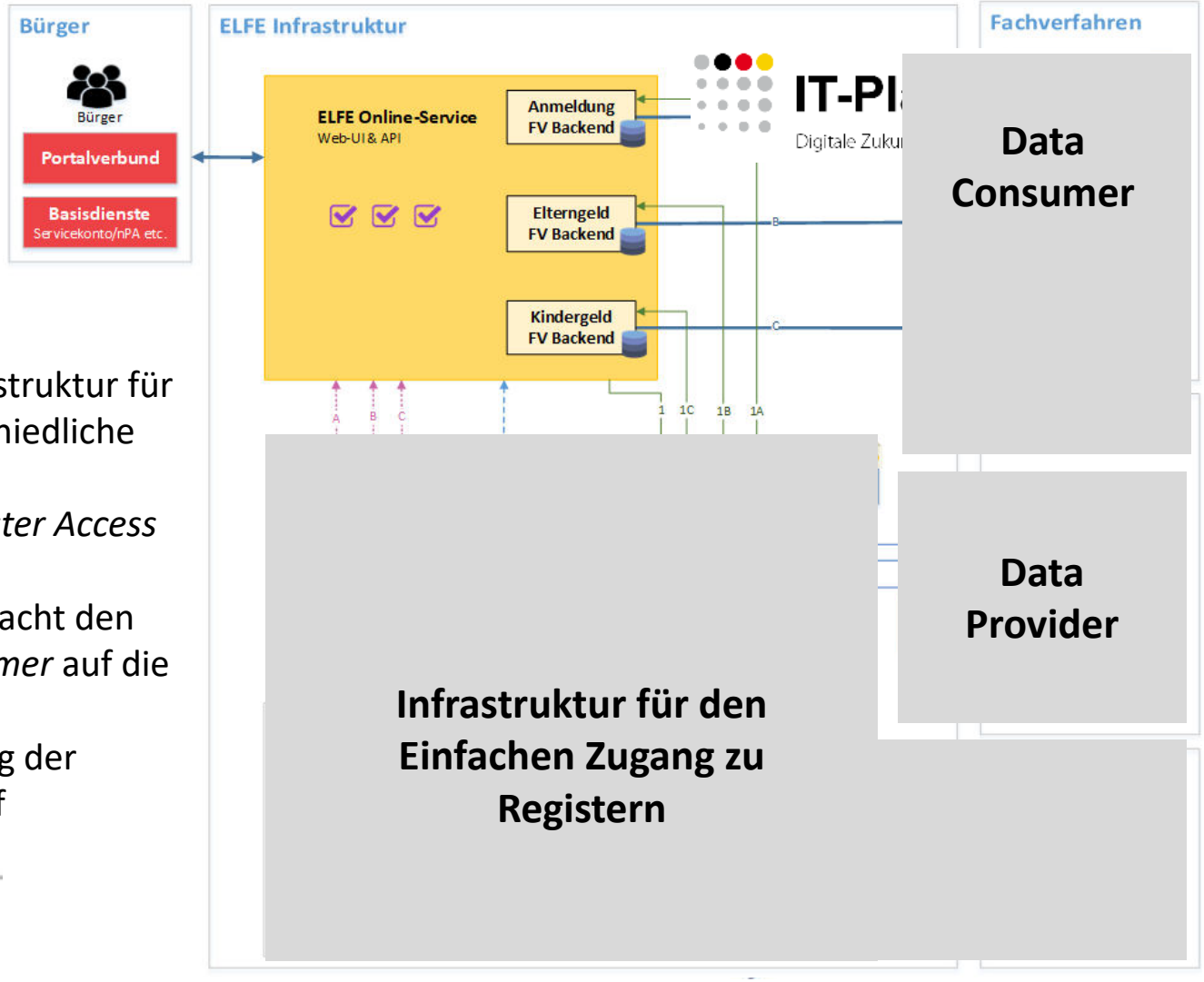
Nutzersicht / Behördensicht

IT-Planungsrat
Digitale Zukunft gestalten

- Eine Lebenslage …
  - … inhaltlich und rechtlich separate Vorgänge
- *Die Verwaltung* gibt es nicht [darf es nicht geben] …
  - … aber Behörden sollen zusammenarbeiten …

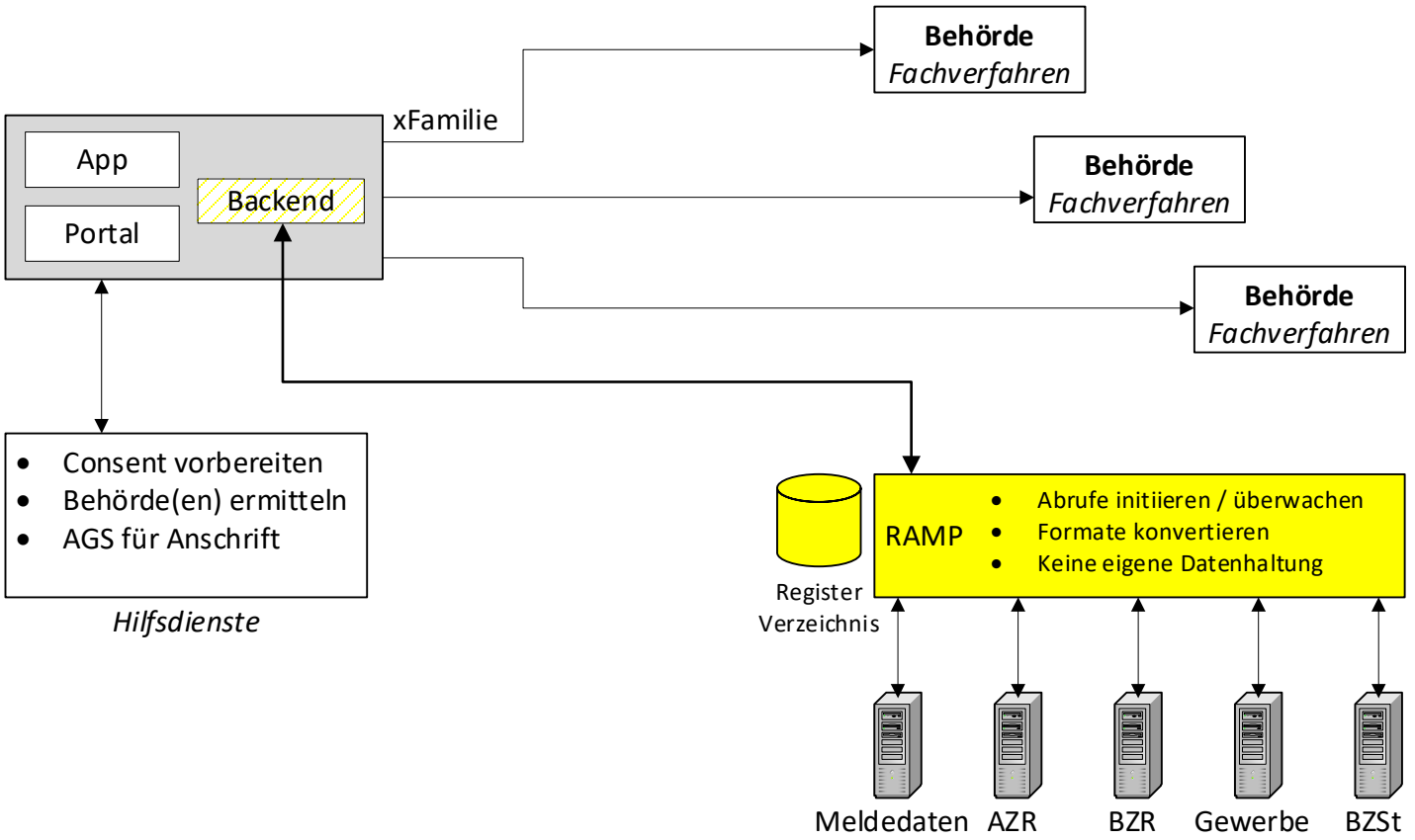
Bremer Architektur für ELFE

- Fachunabhängige Infrastruktur für den Zugriff auf unterschiedliche Register
- Prototype RAMP: *Register Access Management Proxy*
- Organisiert und vereinfacht den Zugriff der *Data Consumer* auf die *Data Provider*
- Organisiert Zustimmung der Nutzer zum Datenabruf



Alternatives Modell

IT-Planungsrat
Digitale Zukunft gestalten



Single Digital Gateway / TOOP

IT-Planungsrat
Digitale Zukunft gestalten

- Einfacher Zugang zu hochwertigen Informationen und effizienten Verfahren für Bürger und Unternehmen
- **Artikel 14:** Austausch von Nachweisen und Anwendung des Grundsatzes der einmaligen Erfassung („Once Only Principle“)
  - Die Kommission richtet ein technisches System für den automatisierten Austausch von Nachweisen **zwischen zuständigen Behörden** in verschiedenen Mitgliedstaaten ein.
- Technische Standards werden verbindlich festgelegt werden
- 21 Verwaltungsleistungen vollständig digital im SDG
  - Nachweis der Eintragung im Geburtenregister
  - Bestätigung der Meldung an der aktuellen Adresse
  - Meldung / Zulassung zur Ausübung einer Geschäftstätigkeit

Thesen

IT-Planungsrat
Digitale Zukunft gestalten

1. Wir brauchen eine fachunabhängige Architektur für den leichten Registerzugriff
2. Sie soll primär die Zugriffe für Behörden unterstützen
3. Sie erlaubt den pragmatischen Einstieg in die Registermodernisierung
4. Für den effizienten Zugriff auf Basisregister benötigen wir eine „Landkarte der Basisdaten und Basisregister“

IT-Planungsrat

Digitale Zukunft gestalten

Karen Lahmann, LAVA
Alexander Leder, Brandenburg
Frank Steimke, KoSIT

Leitlinien für eine Modernisierung der Registerlandschaft

Aus dem Koalitionsvertrag vom 12. März 2018 ergibt sich der Auftrag, die öffentlichen Register zu modernisieren und dafür die Vorschläge des Normenkontrollrates zu prüfen (Rn 2046f.).

I. Politische/strategische Ziele

Die Nutzung bereits vorhandener Daten bei der Verwaltung durch modernisierte und vernetzte Register ermöglicht **effizientes und wirtschaftliches Verwaltungshandeln** und **entlastet Bürger und Unternehmen**. Weitere Ziele sind:

- **Bessere Qualität der Verwaltungsarbeit.** Der Abruf verlässlicher Registerdaten verringert Zeitaufwand in der Verwaltung (nach Schätzung des NKR 59% Einsparung) und reduziert Verwaltungsfehler sowie Betrugsfälle (z.B. bei der Bewilligung von Sozialleistungen).
- **Stärkung des Datenschutzes**
- **Umstellung auf registerbasierten Bevölkerungszensus** (Forderung der EU). Das reduziert den Bürokratieaufwand (nach Schätzung des NKR 87% Einsparung).
- **Nutzerfreundliche Digitalisierung und Umsetzung des OZG ("Once Only").** Keine Papiernachweise der Antragsteller mehr, sondern Nutzung vorhandener Registerdaten (z.B. Einkommensdaten zur Berechnung von Elterngeld)

II. Maßnahmen

Gegenwärtig ist die Registerlandschaft dezentral strukturiert. Viele Register sind nicht miteinander verknüpft, so dass Daten nicht an die Behörden bzw. Register übermittelt werden können, die diese Daten zur Erfüllung ihrer Aufgaben benötigen. Daten werden mehrfach erfasst und es bestehen Inkonsistenzen. Um das zu ändern, brauchen wir:

- Die Schaffung eines **Kerndatensystems** - Ein dauerhaft eingerichteter zentraler Personenbestand ermöglicht die übergreifende Pflege von Personendaten.
- Die Einführung eines verfassungs- und datenschutzkonformen **Identifikators** unter Wahrung geeigneter Garantien für die Rechte und Freiheiten der Person ermöglicht das zuverlässige Auffinden von Datensätzen zu einer Person in verschiedenen Registern, ohne die bestehenden Register zu zentralisieren.
- Eine durchgängige **Interoperabilität und Ertüchtigung der Registerlandschaft** ermöglicht die Übermittlung der Daten zu einer Person aus verschiedenen Registern an die Behörden, die diese Daten zur Erfüllung ihrer Aufgaben benötigen sowie an die betroffene Person selbst.

Alle drei oben genannten Maßnahmen bewirken eine Verbesserung der Datenqualität (eindeutige Zuordnung, Vermeiden von Über- und Untererfassungen, Vollständigkeit der Informationen).

Die EU verlangt eine schnelle Einführung des Registerzensus; auch bei der nutzerfreundlichen Umsetzung des OZG drängt die Zeit. Es gilt daher, schon im Jahr

2019 Zielbild und Planung zu erarbeiten. Für die Realisierung von "Once Only" kommen die Anforderungen aus den Digitalisierungsprojekten zur OZG-Umsetzung.

III. Rahmenbedingungen

Die Registermodernisierung erfolgt nicht auf Kosten des Datenschutzes, sondern stärkt diesen durch:

- **Stärkung der Betroffenenrechte:** Berichtigungen, Auskünfte und Informationen über die Verwendung von Daten und ihre Nachvollziehbarkeit werden verbessert
- **Datensparsamkeit:** Verringerung der Nachweispflichten - durch bessere Nutzung bestehender Daten muss die Verwaltung nicht neu erheben und speichern.
- **Bessere Datenqualität**

IV. Governance

Registermodernisierung betrifft fast alle Verwaltungsbereiche. Die Ressorts sind daher ebenso einzubinden wie Länder einschließlich Kommunen. Fachliche Aspekte sind in den Fachministerkonferenzen zu behandeln, fachübergreifende Themen im IT-Planungsrat.

Bei dieser Ausgangslage muss das oberste Beschluss- und Steuerungsgremium die MPK sein.

Die Vorbereitung der MPK obliegt dem Bundeskanzleramt, ebenso wie die übergeordnete Koordinierung des Projekts und die politische Steuerung in die Ressorts und Fachministerkonferenzen hinein.

Die fachlichen Anforderungen an das Projekt werden überwiegend im Bereich des BMI, der IMK und des IT-PLR formuliert. Eine Projektstruktur im Bundesministerium des Innern, für Bau und Heimat übernimmt die fachliche Federführung und ist zentraler Ansprechpartner für die Klärung rechtlicher und inhaltlicher Fragen der Umsetzung.

Die Mitarbeit der Ressorts erfolgt über den IT-Rat und/oder fachliche Abstimmungsgremien.

Die Kommunen sind über die kommunalen Spitzenverbände einzubinden.

Das Statistische Bundesamt als Zensusbehörde sowie das Bundesverwaltungsamt als Kompetenzträger für Registerinfrastruktur sollen Teil der Projektorganisation sein. Dies gilt auch für FITKO als "Umsetzungsmuskel" des IT-Planungsrats sowie potenzieller Betreiber föderaler IT-Lösungen.

TOP 12: Verfahrensübergreifendes Identitätsmanagement als Teil der Registermodernisierung

Berichterstattung:	BMI
Hinweise:	MPK vom 24. bis 26.10.18 zu TOP 5
	IMK vom 28. bis 30.11.18 zu TOP 14
	AK I am 25./26.03.19 zu TOP 2
	AK II am 10./11.04.19 zu TOP 5
Veröffentlichung:	Freigabe Beschluss und Bericht
Az.:	V B 5.1/4

Beschluss:

1. Die IMK nimmt den "Vorschlag für die Verbesserung des Identitätsmanagements als Teil der Registermodernisierung" (Stand: 11.02.19) zur Kenntnis.

2. Sie bittet den BMI, auf dieser Grundlage die konzeptionellen Arbeiten unter Einbeziehung der Länder und der Koordinierungsstelle für IT-Standards (KoSIT) fortzuführen.

3. Die IMK bittet den BMI, ihr bis zur Herbstsitzung 2019 einen Zwischenbericht vorzulegen, der die erforderlichen Rechtsänderungen darstellt und Optionen für die fachliche und technische Realisierung eines registerübergreifenden Identitätsmanagement beinhaltet.

4. Sie bittet ihren Vorsitzenden, die MPK sowie den IT-Planungsrat über diesen Beschluss und den "Vorschlag für die Verbesserung des Identitätsmanagements als Teil der Registermodernisierung" zu informieren.

Bundesministerium des Innern, für Bau und Heimat

Berlin, den 11. Februar 2019

Vorschlag des Bundesministeriums des Innern, für Bau und Heimat zur Verbesserung des Identitätsmanagements als Teil der Registermodernisierung

Die Regierungschefinnen und Regierungschefs haben den Bund auf ihrer Jahreskonferenz vom 24. bis 26.10.18 gebeten, die Registermodernisierung unter Beteiligung der Länder umgehend zu starten und anschließend der Bundeskanzlerin und den Regierungschefinnen und Regierungschefs über den Stand zu berichten. Dieser Prozess ist initiiert.

Die Ständige Konferenz der Innenminister und -senatoren der Länder hat auf ihrer 209. Sitzung vom 28. bis 30.11.18 in Magdeburg zu TOP 14 folgenden Beschluss gefasst: „Davon ausgehend, dass verlässliche Angaben zur Identität von Personen die Grundlage für Verwaltungsleistungen darstellen, hält sie ein registerübergreifendes Identitätsmanagement und die Stärkung der Interoperabilität von Verwaltungsregistern in einer vernetzten Verwaltung für wesentliche Bestandteile einer Registermodernisierung.“ Die IMK hat bis zur Frühjahrssitzung 2019 um einen Vorschlag für die Verbesserung des Identitätsmanagements gebeten, der die Ausführungen zu TOP 5 "Digitalisierung der Verwaltung" der Jahreskonferenz der Regierungschefinnen und Regierungschefs der Länder vom 24. bis 26.10.18 berücksichtigt.

Im Koalitionsvertrag zwischen CDU, CSU und SPD für die 19. Legislaturperiode im Bund wurde vereinbart (Zeile 2001 ff): „Damit ermöglichen wir Behörden, Daten über gemeinsame Register und eindeutige, registerübergreifende Identifikationen zu verknüpfen („once only“-Prinzip). Wir werden die öffentlichen Register modernisieren und dafür die Vorschläge des Normenkontrollrates prüfen.“

Moderne Register sind nach dem Gutachten des Nationalen Normenkontrollrats *„Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren.“* vom Oktober 2017 das Fundament besserer Verwaltungsleistungen für Bürger und Unternehmen. Moderne Register sind essenziell für effiziente, bürger-

und unternehmensfreundliche digitale Angebote. Die Registerlandschaft der Innenverwaltung erfüllt die nötigen Anforderungen derzeit nicht. Es besteht Modernisierungsbedarf.

- Die immer stärkere Digitalisierung der Gesellschaft betrifft auch die Innenverwaltung. Unsere IT Verfahren und Register sind sowohl für die innere Sicherheit, als auch das ordnungsgemäße Handeln der gesamten öffentlichen Verwaltung und für die Digitalisierung von Verwaltungsleistungen unverzichtbar.
- Durch die gesetzliche Verpflichtung der öffentlichen Verwaltung zur Digitalisierung aller Verwaltungsleistungen einerseits und das Ziel der Nutzerfreundlichkeit andererseits ist die Herausforderung entstanden, mit einer angemessenen Informationsarchitektur und modernen Registern datensparsame und nutzerfreundliche Services zu bieten.
- Verlässliche Angaben zur Identität von Personen sind das Fundament aller Verwaltungsleistungen. Auch angesichts einer Vielzahl von Schutzsuchenden und Migranten brauchen wir neue, leistungsfähige Mechanismen für ein verfahrensübergreifendes Identitätsmanagement in einer vernetzen Welt.
- Zur Digitalisierung des EU Binnenmarktes wird die europäische Kommission ein einheitliches digitales Zugangstor einrichten, welches moderne Basisregister in Mitgliedsstaaten voraussetzt.

Die öffentliche Verwaltung braucht für alle Behörden eine verlässliche Datengrundlage in aufeinander abgestimmten Basisregistern, in denen die Daten stimmen und übereinstimmen. Dafür müssen Schwerpunkte neu gesetzt werden. Die Stärkung der Interoperabilität muss im Vordergrund stehen. Neue, verfahrensübergreifende Mechanismen zur sicheren Identifikation von Personen, welche die gesellschaftlichen Veränderungen der zunehmenden grenzüberschreitenden Mobilität und Migration angemessen berücksichtigen, sind erforderlich.

Da ein registerübergreifendes Identitätsmanagement und die Stärkung der Interoperabilität wesentlicher Bestandteil einer Registermodernisierung sind, beschließen wir auf Vorschlag des Bundesministeriums des Innern, für Bau und Heimat unter Beteili-

gung des IT-Planungsrates und der Vorsitzenden des AK I und des AK II die nachfolgenden Eckpunkte:

1. **Ein registerübergreifendes Identitätsmanagement einführen**

   Grunddaten zu einer Person sollen an einer zentralen Stelle gespeichert, in Abstimmung mit den Basisregistern auf Inkonsistenzen geprüft, verlässlich gepflegt, aktualisiert und bereitgestellt werden. Hierfür wollen wir ein Kerndatensystem schaffen, in dem die Grunddaten aller Personen mit Verwaltungskontakt in Deutschland gepflegt werden. Es wird zudem kenntlich gemacht, wie valide die Angaben zur Identität sind. Die Feststellung und Sicherung der Identität von Personen und die damit einhergehende Aufgabe zur Führung des Kerndatensystems soll eine eigenständige Aufgabe sein und einer eigenen Stelle zugeordnet werden.

   Eine eindeutige Zuordnung der Personalienidentität über alle Register hinweg ist herzustellen. Dies kann mithilfe eines Identifiers geschehen, der die Rechte und Freiheiten der betroffenen Personen nach Artikel 87 der Datenschutz-Grundverordnung wahrt. Der hierfür verwendete Identifier muss so verlässlich und robust sein, dass medienbruchfreie Prozessketten auch in komplexen Situationen stets auf der Grundlage eindeutiger Personenidentitäten operieren. Die bisherige redundante und z.T. widersprüchliche Speicherung der Daten in anderen Registern entfällt perspektivisch, weil an Stelle eigener Datenhaltung auf die Daten des Identitätsmanagements zurückgegriffen werden kann. Damit wird auch dem Grundsatz der Datensparsamkeit Rechnung getragen. Dafür wird ein datenschutzkonformer Mechanismus geschaffen, der die Zuordnung der Grunddaten zu den zugehörigen Datensätzen in Fachverfahren und -registern sicherstellt.

2. **Datensilos auflösen, „once-only-Prinzip auch für Behörden untereinander verwirklichen“ und registerbasierten Zensus ermöglichen**

   Derzeit sind Register meistens so organisiert, dass sie alle für den jeweiligen Fachbereich erforderlichen Daten enthalten und der Kreis der zugriffsberechtigten Behörden eng begrenzt ist. Dies führt zu einer vielfach redundanten und häufig widersprüchlichen und inkonsistenten Datenhaltung. Diese pflegeaufwändigen und damit unwirtschaftlichen Redundanzen sollten schrittweise aufgelöst werden. Jedes Datum sollte möglichst nur in einem Register der origi-

när zuständigen Behörde vorhanden sein und von dieser gepflegt werden. Im Gegenzug muss sichergestellt werden, dass alle Behörden die Daten, die sie für ihre Aufgabenerfüllung benötigen, schnell und unkompliziert erhalten können und dürfen. Einmal erhobene Informationen stehen im Rahmen eines Rechte- und Rollenkonzepts für alle weiteren relevanten Zwecke im Rahmen der rechtlichen Vorgaben zur Verfügung. Das Prinzip der Einmalerfassung und Mehrfachnutzung steigert die Akzeptanz und trägt zu einer signifikanten Verbesserung der Datenqualität bei. Dies verwirklicht auch im Verkehr zwischen Behörden das „once-only-Prinzip“. Dafür müssen die Rechtsgrundlagen, die Organisation und die Technik so weiterentwickelt werden, dass sie Durchlässigkeit und Datenweitergabe nicht nur erlauben, sondern fördern (Interoperabilität by Design). Die Empfehlungen zur Umsetzung des Europäischen Interoperabilitätsrahmens (EIF 2017) sollen geprüft werden.

Ein guter Ausgangspunkt für die nötige Weiterentwicklung in rechtlicher Hinsicht sind bestehende Regelungen, wonach die Daten eines Registers einer anderen öffentlichen Stelle insoweit zugänglich sind, als diese für die Erledigung einer eigenen Verwaltungsaufgabe erforderlich sind. In technischer Hinsicht ist der Informationsverbund der Innenverwaltung (der Standard XInneres mit den Modulen XMeld, XPersonenstand und XAusländer) weiter zu entwickeln.

Ein Identitätsmanagement für eine vernetzte Registerlandschaft ist ebenfalls erforderlich, um einen registerbasierten Zensus durchzuführen, der ab 2024 EU-weit verpflichtend und jährlich obligatorisch werden kann.

3. Aktualität und Qualität sowie Datensicherheit und Datenschutz gewährleisten

Die Registerlandschaft sollte so weiterentwickelt werden, dass sie eine hohe Qualität und Aktualität der Registerdaten (z.B. durch Prüfung auf Doubletten und Inkonsistenzen, Über- und Untererfassungen) sowie die Zugänglichkeit des Datenbestands für die nutzenden Behörden aller föderalen Ebenen aufgabenadäquat sicherstellt. Zugleich sollte ein hohes Maß an Datensicherheit (z.B. durch physisch verteilte Datenhaltung) und Datenverfügbarkeit gewährleistet sowie den datenschutzrechtlichen Vorgaben (insbesondere denjenigen der EU-Datenschutz-Grundverordnung) und den verfassungsrechtlichen Vor-

gaben (insbesondere derjenigen des Rechts auf informationelle Selbstbestimmung) entsprochen werden.

4. **Standardisierung auch in der Registerstruktur verwirklichen**

   Die Ergänzung von Daten, die aufgrund bundesrechtlicher Regelungen (konzeptionell oder tatsächlich) zentral vorgehalten werden, mit solchen, die aufgrund landesrechtlicher Regelungen in Registern von Ländern oder Kommunen gespeichert sind, soll durch rechtliche und technische Maßnahmen unterstützt werden. Dies erfordert eine durchdachte Architektur sowie einen umfassenden Standardisierungsansatz, der nicht (wie derzeit) nur die Datenübermittlung regelt, sondern auf Registerstrukturen ausgedehnt wird.

5. **Transparenz für die betroffenen Personen sicherstellen.**

   Die betroffenen Personen sollten im Rahmen ihres datenschutzrechtlichen Auskunftsrechts jederzeit auf einfache Weise feststellen können, welche Behörde zu welchem Zweck auf welche ihrer Daten zugegriffen hat. Dies kann z.B. durch Verbindung mit einem Nutzerkonto im Portalverbund nach dem OZG sichergestellt werden.

Koordinierungsstelle
für IT-Standards

Freie
Hansestadt
Bremen

Es bleibt schwierig

Eine kurze Einführung zum Thema Registermodernisierung

Frank Steimke| Koordinierungsstelle für IT-Standards (KoSIT)

12. XÖV Konferenz | 25. September 2019 | Bremen

Daten – Rohstoff und sensibles Gut

Daten sind der Treibstoff für Innovationen und neue Dienste.
Diese wollen wir ermöglichen

und gleichzeitig

den hohen und weltweit angesehenen Datenschutzstandard
Europas und Deutschlands halten.

Koalitionsvertrag zwischen CDU, CSU und SPD 19. Legislaturperiode

Aus dem Bericht des Normenkontrollrats (2017)

Koordinierungsstelle für IT-Standards

- Es besteht umfassender Modernisierungsbedarf
  - Zu viele Register, die Übersicht ist verloren gegangen
  - Administrative Zersplitterung
  - Gleiche oder ähnliche Daten werden mehrfach erhoben
  - Sie werden in diversen Registern gespeichert
  - Abgleiche und Qualitätschecks finden nicht statt
- Kern moderner Register sind gute Basisdaten, die nur einmal mitgeteilt werden müssen (Once Only)
  - Bei der originär zuständigen Behörde gespeichert
  - Qualitätsgesichert und stets aktuell
  - Leicht zugänglich (Befugnis vorausgesetzt)

Wer macht was ?

Koordinierungsstelle für IT-Standards

MPK und Bundesregierung

IT-Planungsrat

Koordinierungsprojekt (27. 6. 2019)

- Anforderungen identifizieren
- Architekturmodell
- Anforderungen an Rechtsänderungen
- Zielbild und Maßnahmenplanung

Abstimmung

Innenministerkonferenz

Beschluss 12. Juni 2019

- Identitätsmanagement
- Gesetzesentwurf
- Modernisierung der Register der IMK

Europäische Kommission

VERORDNUNG (EU) 2018/1724 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 2. Oktober 2018

über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012

- Innenministerkonferenz
- IT-Planungsrat
- EU-Kommission

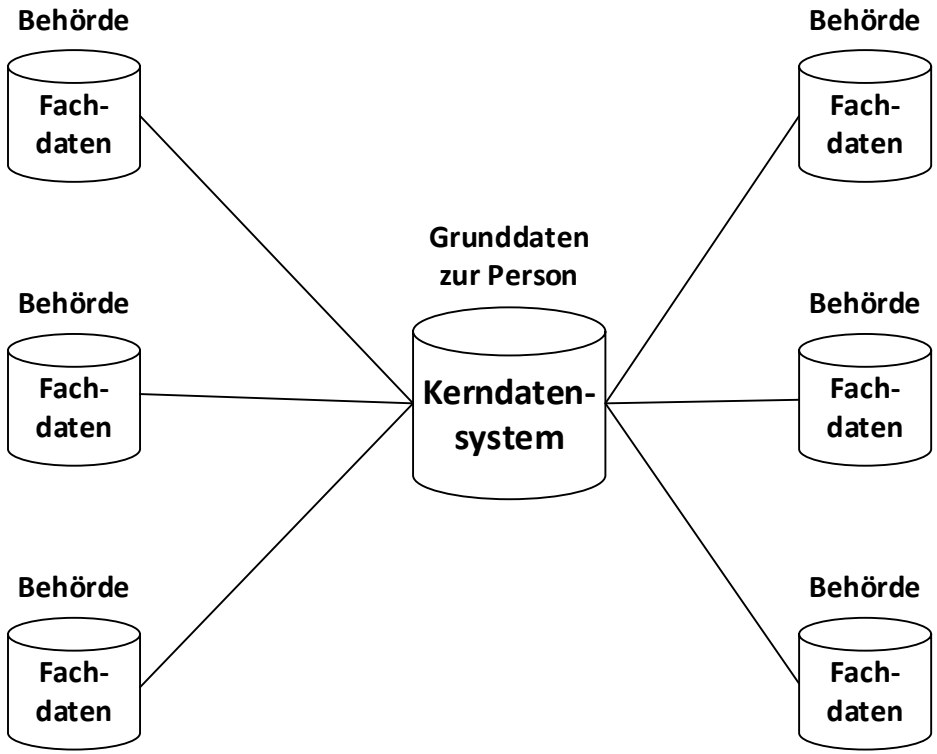
Identitätsmanagement und Modernisierung (IMK)

Koordinierungsstelle für IT-Standards

- **Datensilos auflösen, once-only-Prinzip auch für Behörden**
  - Daten möglichst nur bei der originär zuständigen Behörde speichern
  - Schneller und unkomplizierter Zugang (Berechtigung vorausgesetzt)
  - Datenweitergabe nicht nur erlauben, sondern fördern
- **Registerübergreifendes Identitätsmanagement einführen**
  - Kerndatensystem mit Grunddaten zur Person
  - Eindeutige Zuordnung der Personalienidentität über alle Register hinweg
  - Verlässlicher und robuster Identifier

Basisregister im Informationsverbund

Koordinierungsstelle für IT-Standards



- Daten werden konzeptionell nur an einer Stelle gespeichert
- **Eindeutige, stabile Identifikation der Datensätze im Verbund**

Datenschutzkonferenz (12. September 2019)

Koordinierungsstelle für IT-Standards

- Registermodernisierung muss die Nutzung einmal hinterlegter Daten erleichtern (Once Only Prinzip)

- Bessere Vernetzung birgt hohe Risiken für das Recht auf informationelle Selbstbestimmung
- Keine einheitlichen, verwaltungsübergreifende Identifikatoren
- Sektorspezifische Personenkennziffern kommen in Betracht

- Deutlich höheres Maß an Transparenz erforderlich (Datencockpit)

- Innenministerkonferenz
- IT-Planungsrat
- EU-Kommission

IT-Planungsrat
Architekturmodell: Fragestellungen

Koordinierungsstelle für IT-Standards

Tech-nisch	1 Identitäts-management	?	Wie werden Daten einer Person/einem Unternehmen zugeordnet?
	2 Zugangs-management	?	Wie gelangen die angefragten Daten zur anfragenden Stelle?
	3 Datenhaltung	?	Wo sind die Daten für Anwendungsfälle gespeichert?
	4 Schnittstellen-design	?	Welche Standards gelten für die Register, und welches "Design" liegt zu Grunde?
Organi-satorisch	5 Governance	?	Wer übernimmt die organisatorische Steuerung der Register und bestimmt somit die technische Dimension und Themen wie bspw. die Qualitätssicherung maßgeblich?
	6 Datenschutz	?	Wie und durch wen können die Anforderungen des Datenschutzes sichergestellt werden?

Quelle: BMI, Workshop 10. 9. 2019

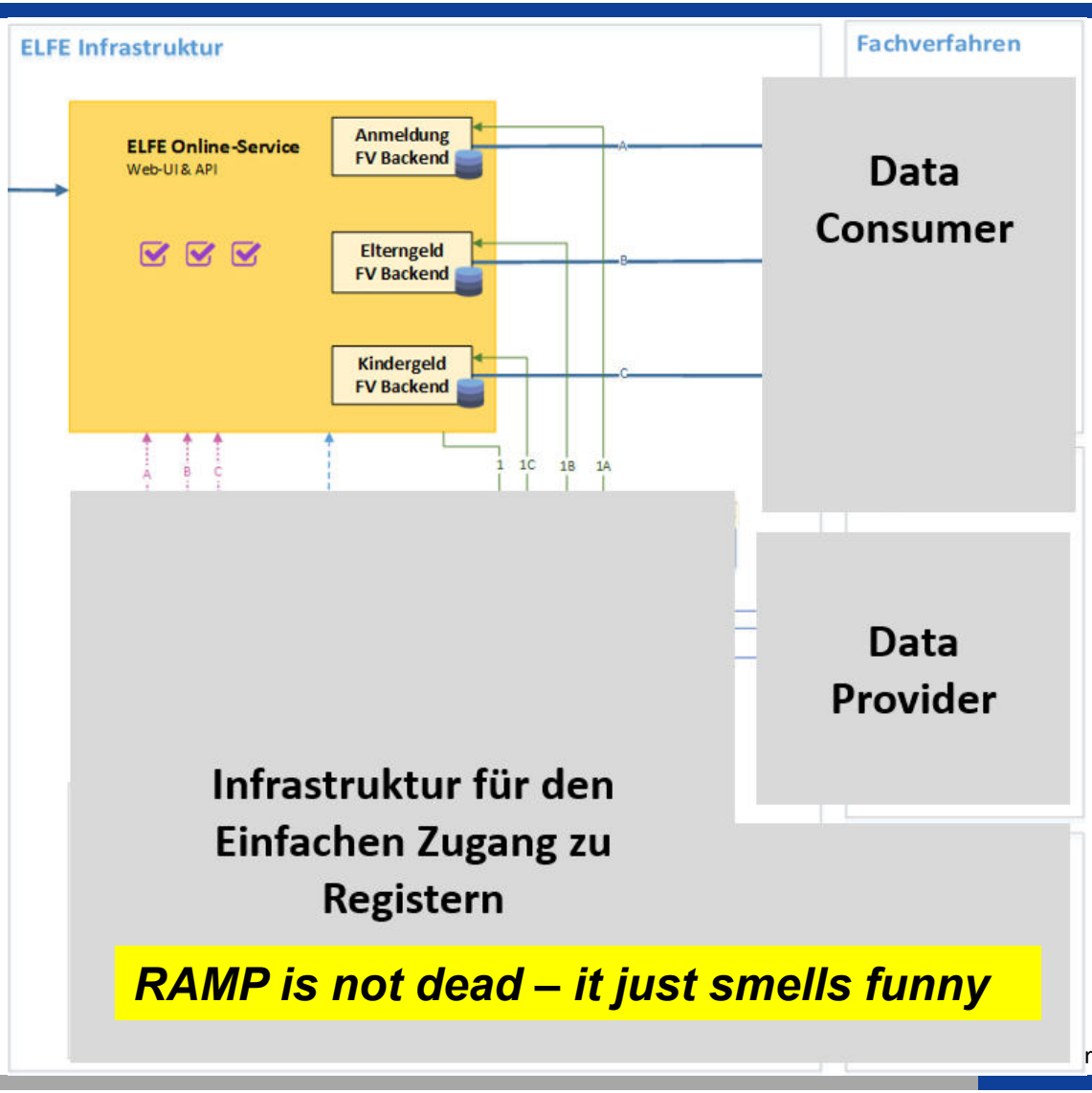
IT-Planungsrat: Zwischenstand nach Workshop

Koordinierungsstelle für IT-Standards

- Enge Registervernetzung auf Basis offener Standards
- Informationsverbund der IMK als Blaupause
- Brücken von XÖV zu anderen Verbünden erforderlich
  - Geodaten (Inspire)
  - Finanzverwaltung
  - Gesundheitswesen (Gematik)
  - *… und andere …*
  - *Arbeitgeber, Krankenkassen, Sozialversicherung*
  - *Kirchen*

XÖV-Konverter = Register Access Management Proxy (RAMP)

Koordinierungsstelle für IT-Standards



- Innenministerkonferenz
- IT-Planungsrat
- EU-Kommission

Die EU macht Druck …

Koordinierungsstelle für IT-Standards

- Single Digital Gateway Verordnung vom 2. 10. 2018
- 21 Verfahren vollständig digitalisiert anzubieten
  - Geburtsnachweis, Meldebestätigung, An- und Abmeldebestätigung, …
  - Anmeldung der Geschäftstätigkeit, Sozialversicherungs-Anmeldung, …
- Wir brauchen eine Infrastruktur für Once Only

Frist: Dezember 2023

… entwickelt aber auch Lösungen

Koordinierungsstelle
für IT-Standards

Based on the building blocks of former LSPs

The Once Only Principle

www.toop.eu

Fazit

Koordinierungsstelle für IT-Standards

- Dezentrale Registerstruktur bleibt – wird modernisiert
- Daten nur einmal speichern – bei der zuständigen Behörde
- Grunddaten zur Person an zentraler Stelle – Kerndatensystem
- Once Only ist übergreifendes Prinzip – OZG und SDG
- Register im Informationsverbund – Interoperability by Design
- Vernetzung auf Basis offener Standards – IMK als Blaupause
- Brücken bauen zwischen Verbünden – XÖV, eXtra, INSPIRE etc.
- Registerübergreifendes Identitätsmanagement – Identifier
- Mehr Vernetzung erfordert mehr Transparenz - Datencockpit
- EU fordert und fördert – SDG und TOOP

Es bleibt schwierig

Koordinierungsstelle
für IT-Standards

Freie
Hansestadt
Bremen

Vielen Dank für Ihre Aufmerksamkeit!

Frank Steimke| kosit (at) finanzen.bremen.de | www.xoev.de

EU Anforderungen an die Digitalisierung von Verwaltungsverfahren

gemäß EU Verordnung 2018/1724 zum Single Digital Gateway

Bundesministerium des Innern, für Bau und Heimat

Your Europe

Übersicht

Anforderungen an alle Online-Verfahren

1. Anzeige von Informationen zu Verfahren &zu Rechten und Pflichten in DEU
2. Erhebung statistischer Daten
3. Diskriminierungsfreie Datenfelder
4. Verpflichtendes ePayment
5. Barrierefreiheit (Web-Zugänglichkeit)
6. Einbindung SDG-Logo
7. Verpflichtende Nutzung von IMI zur Überprüfung elektronische Nachweise
8. Nutzerfeedback

Zusätzliche Anforderungen an spezifische Online-Verfahren:

9. Vollständige online Bereitstellung der Verfahren (inkl. EU-weites Once Only Prinzip)

Your Europe

I. Anforderungen an alle Online-Verwaltungsverfahren

1. Anzeige von Informationen vor Auslösen des Verfahrens:

a) Nutzerfreundliche Erstorientierung über Rechte, Pflichten in DEU.

„Wenn Sie ein Startup in Deutschland gründen wollen, sind folgende Regelungen und Vorschriften zu beachten: …“

- mindestens zu allen Themenbereichen des Annex I SDG-VO
- Inhalt gemäß Art. 9 SDG-VO
- in deutscher und englischer Sprache

  → *BVA Prozess; absehbar kein Handlungsbedarf für Länder & Kommunen*

b) **Leistungsbeschreibungen (= Informationen zu Verfahren)**

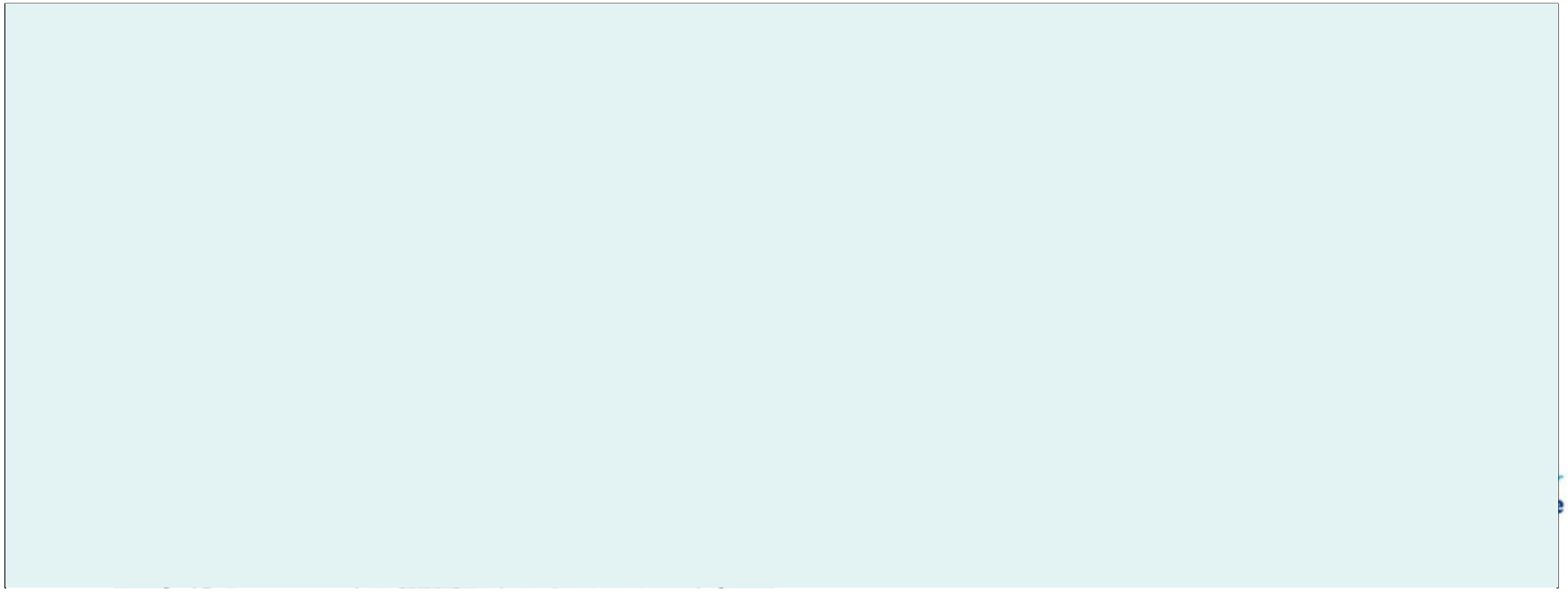
- mindestens zu allen Themenbereichen des Annex I SDG-VO
- Inhalt gemäß Art. 10 SDG-VO
- in deutscher und englischer Sprache

  → *FIM Leistungsbeschreibungen erfüllen die SDG-Kriterien*

Auf dem „Your Europe“ Portal verbleiben nur Informationen zu Rechten und Plfichten, die in der gesamten Europäischen Union gelten:

„Wenn Sie als Nicht EU Bürger/in die EU besuchen oder innerhalb der EU reisen wollen, benötigen Sie einen Reisepass, der […] und außerdem möglicherweise ein Visum“.

Weiterleitung in den Portalverbund



Mit Aufruf eines Online-Verfahrens:

2. Erhebung statistischer Daten (vgl. Art. 24 SDG-VO):

Für **Online-Verfahren der Mitgliedstaaten** – unter Wahrung der Anonymität der Nutzer – zu

- Anzahl,
- Herkunft,
- Art der Nutzer
- Nutzerpräferenzen und Nutzerpfade
- Benutzerfreundlichkeit,
- Auffindbarkeit,
- Qualität.

Anbieter von **Hilfs- und Problemlösungsdiensten** erheben in aggregierter Form

- die Anzahl, den Ursprung, den Gegenstand
- von Anfragen nach Hilfs- und Problemlösungsdiensten
- sowie deren Antwortzeiten

und tauschen sie aus.

Erster Entwurf des EU-Durchführungsrechtsakts

Informationen beruhen auf einem ersten Entwurf des Durchführungsrechtsakts der KOM – Änderungen vorbehalten

Übertragung zwei mal jährlich

(„Transmission biannually“)

Category of service	Data per page	Why do we need this?/ link with the SDGR
Procedures (online procedures in Annex I areas)	Number of users who identified themselves in the procedure portal/environment for the purpose of completing a procedure online	Which procedures are used most by users from other MSs? *(SDGR: data related to user preferences and accessibility of online procedures)*
	Number of [users/users from other MSs] who started a procedure (Annex I areas if online)	Which procedures are used most by users from other MSs? *(SDGR: data related to user preferences and accessibility of online procedures)*
	Number of [users/users from other MSs] who completed an online procedure [e.g. clicked on the “submit” button, received “confirmation of receipt”]	Which procedures could be completed by users from other MSs?; what is the ratio between the number of procedures launched and completed by users from other MSs? *(SDGR: data related to user preferences and to quality of procedures (fully online)*

3. Diskriminierungsfreie Datenfelder

Eingabefelder von Online-Verfahren müssen grundsätzlich Eingaben anderer EU Mitgliedstaaten ermöglichen (z.B. Telefonnummern, Anschriften, Postleitzahlen, Firmenbezeichnungen).

Vgl. Art. 13 Absatz 2 (b) i.V.m. Erwägungsgrund 18

4. Barrierefreiheit von Online-Angeboten

Die SDG-VO macht keine eigenen Vorgaben sondern verweist auf die Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates.

vgl. Art. 8 SDG-VO.

5. Verpflichtendes ePayment

- Anfallende Gebühren müssen online bezahlt werden können mittels EU-weit gängiger online Zahlungsmethoden ***(„weithin verfügbare grenzüberschreitende Zahlungs-dienste“)***

  → *Basiskomponente ePayBL stellt ein Bündel EU-weit gängiger Zahlungsmethoden zur Verfügung und erfüllt damit die SDG-Vorgabe (vgl. https://www.epaybl.de/)*

6. Einbindung des SDG-Logos

- in die über das SDG erreichbaren Webseiten der Mitgliedstaaten als Qualitätssiegel

7. Verpflichtende Nutzung von IMI

- zur Überprüfung EU-grenzüberschreitend übermittelter elektronischer Nachweise sofern diese nicht automatisiert mittels Registervernetzung übermittelt wurden

6. Nutzerfeedback

- zu den über das SDG erreichbaren **Online-Verfahren** der Mitgliedstaaten
- inkl. der Online-Verfahren der sog. Hilfs- und Problemlösungsdienste:
  - Einheitlicher Ansprechpartner
  - Produktinformationsstellen & Bauproduktinformationsstellen
  - Beratungszentren für Berufsqualifikation
  - Nationale Kontaktstellen grenzüberschreitende Gesundheitsversorgung
  - Europäisches Netz der Arbeitsvermittlungen EURES
  - Online Streitbeilegungsstellen

Erster Entwurf des EU-Durchführungsrechtsakts:

- **wenn Nutzer die ausgefüllte Beantragung abschicken und**
- **wenn Nutzer das Verfahren vor Einreichung abbrechen;**

Vgl. Punkt 1.3 des Entwurf des Durchführungsrechtsakts:

*"The user feedback mechanism should be integrated to the procedure in a way that it makes it easy for users to provide their feedback **if they fully completed and submitted** their application form and **if they abandoned the application** before submitting it. "*

Nutzerfeedback zu Online-Verfahren:

Informationen beruhen auf einem ersten Entwurf des Durchführungsrechtsakts der KOM – Änderungen vorbehalten

Detaillierte Feedbackmöglichkeit

Questions	Answers
Were the instructions for completing the procedure available in English?	YES/NO/I do not know
Was it easy to fill in the form/submit required information?	(star rating from 1 to 5)
Were you able to identify or authenticate yourself using your national eID or eSignature?	YES/NO/not relevant
Could you provide required evidence of compliance with applicable requirements in electronic format?	YES/NO/partly/not relevant
Were you able to pay any fees online?	(YES/NO/not applicable)
Would you like to make any specific comments?	Open text box

Gemäß Entwurf des Durchführungsrechtsaktes wird das Feedback

Informationen beruhen auf einem ersten Entwurf des Durchführungsrechtsakts der KOM – Änderungen vorbehalten

- automatisiert
- in Echtzeit
- direkt an die KOM
- inkl. der URL

übermittelt.

Falls eigenes Tool verwendet wird: Übermittlung muss auf Antworten zu Fragen der KOM beschränkt werden (*Vgl. Entwurf Durchführungsrechtsakt Part I, Punkt II.*)

II. Anforderungen an spezifische Online-Verwaltungsverfahren

Spezifische Anforderungen gelten **zusätzlich** für Verfahren im Geltungsbereich von:

- Annex II der SDG-VO
- Berufsanerkennungsrichtlinie (2005/36/EG),
- Dienstleistungsrichtlinie (2006/123/EG),
- Richtlinie über die öffentliche Auftragsvergabe (2014/24/EU),
- Richtlinie über die Vergabe von Aufträgen durch Auftraggeber im Bereich der Wasser-, Energie- und Verkehrsversorgung sowie der Postdienste (2014/25/EU).

9. Vollständige online-Bereitstellung (gemäß Art. 13 SDG-VO)

1. digitale Identifizierung gemäß eIDAS-VO
2. automatische digitale Empfangsbestätigung
3. online Abwicklung mittels Formular-Management-System *(kein PDF !)*
4. Nutzer können EU-grenzüberschreitend die automatisierte elektronische Übertragung von Nachweisen veranlassen
5. Nutzer können anderweitig notwendige Informationen digital übermitteln
6. digitale Signierung ist möglich
7. digitale endgültige Einreichung *(kein PDF !)*
8. digitale Verbescheidung oder Benachrichtigung über den Abschluss des Verfahrens

EU-grenzüberschreitende automatisierte Übertragung von Nachweisen:

- **nur auf ausdrückliches Ersuchen des Nutzers**
- Nutzer müssen die automatisiert zu übermittelten Nachweise **vorab einsehen** und entscheiden können, ob sie mit dem Austausch der Nachweise fortfahren oder nicht.
- nur **zweckgebunden** in dem erforderlichen Maß

  → vgl. Art. 14 SDG-VO

- Die **KOM wird Mitte 2021 ein technisches System** für die EU-weite grenzüberschreitende Registervernetzung bereitstellen und Durchführungsrechtsakt erlassen.

  → Nachweise müssen in dem von der EU vorzugegebenen technischen Format vorliegen

  → Entsprechende nachweisführende deutschen Register müssen an das technische System der KOM angeschlossen werden.

10. Ausnahmeregelung:

Eine Aussetzung der vollständigen online Bereitstellung ist nur für einzelne Schritte der online-Verfahren und nur vorübergehend in definierten Ausnahmefällen möglich und ggü. KOM und den anderen Mitgliedstaaten zu begründen (vgl. Art. 6 Abs. 3 SDG-VO).

Vielen Dank für Ihre Aufmerksamkeit !

Eckpunktepapier zum Einsatz eines verfahrensübergreifenden Identifiers - „4-Corner Modell“

Fassung vom 10.01.2020

Frank Steimke, KoSIT

1 Motivation und Begründung

2 Eigenschaften der Infrastruktur

2.1 Die sektorübergreifende Datenübermittlung erfolgt nicht direkt zwischen den beiden Behörden, sondern immer über Dritte Stellen

2.2 Die bei der sektorübergreifenden Datenübermittlung zu beteiligenden Dritten müssen öffentliche Stellen im Sinne des § 2 BDSG sein

2.3 Die an der Datenübermittlung zu beteiligenden Dritten haben die Aufgabe, die sektorübergreifenden Datenübermittlungen zu kontrollieren und zu protokollieren

2.4 Die Dritten Stellen kennen die Metadaten der Datenübermittlung, insbesondere kennen sie die Identität der Kommunikationspartner

2.5 Der Identifier ist nicht Bestandteil der Metadaten der Datenübermittlung

2.6 Die Dritten Stellen müssen ihre Aufgaben ohne Kenntnis des Nachrichteninhalts erbringen können

2.7 Die Vertraulichkeit der Datenübermittlung muss mindestens auf der Strecke zwischen den Transporteuren sichergestellt sein

2.8 Jede sektorübergreifende Datenübermittlung muss durch eine Dritte Stelle unter Angabe der Kommunikationspartner und dem Zweck hergestellt (vermittelt) werden

2.9 Einträge in den Verzeichnis- bzw. Vermittlungsdienst können nur durch öffentliche Stellen in einem offengelegten (transparenten) Prozess erfolgen

2.10 Alle zur Infrastruktur gehörenden Komponenten werden in einem offenen, von der öffentlichen Verwaltung kontrollierten Prozess betrieben und weiterentwickelt

3 Konkretisierung für die Innenverwaltung

1 Motivation und Begründung

Verlässliche Angaben zur Identität der betroffenen Person sind die Grundlage aller personenbezogenen Verwaltungsleistungen. Die öffentliche Verwaltung speichert Daten zu Personen auf der Basis entsprechender Befugnisse in elektronisch geführten Registern, die nach dem Prinzip der behördlichen Zuständigkeit fachlich und häufig auch geografisch dezentral organisiert sind. Bei der elektronischen Abwicklung von Verwaltungsverfahren muss die eindeutige Zuordnung von Datensätzen in Registern zur jeweils betroffenen Person gewährleistet werden. Die irrtümliche Zuordnung von Datensätzen zur falschen Person muss ebenso ausgeschlossen werden, wie die ergebnislose Suche trotz vorhandener Datensätze.

Für eine verlässliche Zuordnung von Datensätzen in Registern zur betroffenen Person dürfen in Teilbereichen der öffentlichen Verwaltung eindeutige Identifikatoren genutzt werden. Beispiele hierfür sind die Steuer-ID (§ 139 AO) und die AZR Nummer (§ 3 AZRG). Ihre Verwendung ist jeweils nur für bestimmte Geschäftsvorfälle zulässig.

Verfahrensübergreifend wird derzeit häufig eine Kombination von Stamm- bzw. Basisdaten der betroffenen Person für eine Identifikation herangezogen (Name, Angaben zur Geburt, aktuelle Anschrift). Dieser faktisch vorhandene „sprechende Identifikator“ weist sowohl funktionale als auch datenschutzrechtliche Mängel auf.

Vor diesem Hintergrund hat die IMK die Einführung eines registerübergreifenden Identitätsmanagements beschlossen (210. Sitzung im Juni 2019, TOP 12). Es soll ein Identitätsregister eingerichtet werden, in dem die Grunddaten aller Personen mit Verwaltungskontakt in Deutschland gepflegt werden. BMI schlägt vor, das Identitätsregister unter Nutzung der Steuer-ID-Datenbank des BZSt einzurichten. Eine eindeutige Zuordnung der Personalienidentität über alle Register der öffentlichen Verwaltung hinweg soll mithilfe eines Identifiers sichergestellt werden. BMI schlägt vor, hierfür die Steuer-ID oder einen davon abgeleiteten Identifikator zu verwenden. Dieser Identifier ist eine Kennziffer im Sinne des Artikel 87 DSGVO.

Im Zuge der Einführung eines Identifiers müssen aus verfassungsrechtlichen Gründen Maßnahmen ergriffen werden die verhindern, dass es durch eine unzulässige Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von umfassenden Persönlichkeitsprofilen kommen kann. Zugleich muss sichergestellt sein, dass rechtmäßige Datenübermittlungen uneingeschränkt möglich sind und zuverlässig funktionieren. Für jede Datenübermittlung bedarf es zunächst einer entsprechenden Rechtsgrundlage. In der nach dem Prinzip der behördlichen Zuständigkeit dezentral organisierten Registerlandschaft der öffentlichen Verwaltung ist die *Zusammenführung* von Daten gleichbedeutend mit der *Übermittlung* von Daten. Daher soll die unzulässige Zusammenführung einzelner Lebens- und Personaldaten, die zur Erstellung von Persönlichkeitsprofilen führen könnte, dadurch ausgeschlossen werden, dass Kontrolle über Datenübermittlungen zwischen Behörden ausgeübt wird.

Zu diesem Zweck sollen innerhalb der Behörden- bzw. Registerlandschaft der öffentlichen Verwaltung *Sektoren* anhand fachlicher Kriterien definiert werden, beispielsweise *Finanzen / Gesundheit / Arbeit und Soziales / Innenverwaltung*. Sektor-übergreifenden Datenübermittlungen, die den Identifier enthalten, dürfen nur über eine technische Infrastruktur erfolgen, die die erforderlichen Kontrollmöglichkeiten des Staates gewährleistet.

Auf diese Weise wird mittels rechtlicher und technischer Maßnahmen sichergestellt, dass Datenübermittlungen zwischen Sektoren stets nur in einem kontrollierten und überwachten Umfeld stattfinden können. Die unkontrollierte Zusammenführung von Daten aus unterschiedlichen Sektoren ist nicht möglich, so dass die Erstellung von Persönlichkeitsprofilen durch „den Staat“ bzw. eine Behörde wirksam verhindert wird.

2 Eigenschaften der Infrastruktur

Nachfolgend werden Eigenschaften einer Infrastruktur für Datenübermittlungen zwischen Behörden genannt, die erforderlich sind, um die notwendigen Kontrollfunktionen bei Datenübermittlungen zwischen Sektoren ausüben zu können.

Die Eigenschaften werden abstrakt und technikneutral beschrieben. Zur Erläuterung der Eigenschaften wird die konkrete Umsetzung in der Innenverwaltung herangezogen. Die dabei genannten, konkreten Standards bzw. Komponenten dienen nur der Illustration.

Sektor-übergreifende Datenübermittlungen zwischen Behörden, die den Identifier enthalten, sind nur zulässig, wenn sie über eine technische Infrastruktur mit den nachfolgend genannten Eigenschaften erfolgt:

2.1 Die Datenübermittlung erfolgt nicht direkt zwischen den beiden Behörden, sondern immer über Dritte Stellen

*Die beiden Stellen, zwischen denen auf der Basis bestehender Rechtsgrundlagen übermittelt werden, werden als **Autor** bzw. **Leser** bezeichnet. Die Daten dürfen nicht direkt zwischen diesen beiden Stellen ausgetauscht werden, sondern es müssen Dritte Stellen beteiligt sein, bei denen die nachfolgend dargestellten Kontrollfunktionen wahrgenommen werden können.*

In der Innenverwaltung ist dieses Prinzip durch den Im Auftrag des IT-Planungsrats von der KoSIT herausgegebene OSCI Transport Standard und die vom IT-Planungsrat bereitgestellte Anwendung „Governikus“ realisiert. Für die Herstellung einer Verbindung (Vermittlungsdienst) wird das vom Bund und den Ländern gemeinsam betriebene „Deutsche Verwaltungsdiensteverzeichnis DVDV 2“ genutzt. Die Infrastruktur der Innenverwaltung wird gebildet durch die abgestimmte Nutzung technischer Standards und geeigneter, von der öffentlichen Verwaltung betriebener Anwendungen.

Die rechtliche Verpflichtung zur Anwendung dieser Infrastruktur ist u. a. in §§ 2, 3 der 1. BMeldDÜV für die Übermittlung von Meldedaten festgelegt.

2.2 Die bei der Datenübermittlung zu beteiligenden Dritten müssen öffentliche Stellen im Sinne des § 2 BDSG sein

Der Betreiber des Vermittlungsdienstes und die für den Transport zuständigen Stellen müssen selbst der staatlichen Kontrolle unterliegen.

In der Innenverwaltung ist diese Bedingung nach unserem Kenntnisstand für alle Betreiber der OSCI-Intermediäre (Anwendung Governikus des IT-Planungsrats) und alle als Clearing- bzw. Vermittlungsstellen agierenden Organisationseinheiten ebenso gewährleistet, wie für alle Betreiber des Deutschen Verwaltungsdiensteverzeichnisses DVDV auf Bundes- und Landesebene.

2.3 Die an der Datenübermittlung zu beteiligenden Dritten haben die Aufgabe, die sektorübergreifenden Datenübermittlungen zu kontrollieren und zu protokollieren

*Es muss mindestens protokolliert werden: **Wer** übermittelt Daten **an Wen** aus welchem **Anlass** zu welchem **Zeitpunkt**.*

In der Innenverwaltung führen die am Transport beteiligten Stellen entsprechende Protokolle auf Basis des OSCI Laufzettels. Die konkreten Inhalte der Protokollangaben und die Aufbewahrungsfristen sind innerhalb der Innenverwaltung abgestimmt.

In der Innenverwaltung nehmen die Betreiber der OSCI Intermediäre eine zusätzliche, ursprünglich nicht vorgesehene Kontrollfunktion wahr: nach dem Erhalt einer Nachricht prüfen sie im Zusammenspiel mit dem Vermittlungsdienst DVDV, ob die Behördenkategorie des Absenders und der Anlass der Datenübermittlung zusammenpassen. Beispiel: wenn eine Nachricht aus Anlass einer Fortschreibung von Meldedaten gemäß § 23 BMG übermittelt wird, dann muss der Absender der Nachricht eine Behörde der Kategorie „Meldebehörde" sein. Andernfalls wird ein Fehler gemeldet, auf den entsprechend reagiert werden kann.

2.4 Die Dritten Stellen müssen ihre Aufgaben ohne Kenntnis des Nachrichteninhalts erbringen können

Sowohl die originären Aufgaben des sicheren Transports bzw. der Herstellung (Vermittlung) einer Verbindung, als auch die hier beschriebenen Kontroll- und Überwachungsfunktionen müssen die Dritten Stellen auch dann in vollem Umfang wahrnehmen können, wenn sie keine Kenntnis vom eigentlichen Nachrichteninhalt haben.

*Eine andere Formulierung dieser Eigenschaft lautet: Die Infrastruktur muss die Möglichkeit einer **Ende-zu-Ende Verschlüsselung** zwischen den beiden behördlichen Kommunikationspartnern (Autor und Leser) unterstützen.*

In der Innenverwaltung wird dieses Prinzip zunächst durch die Verwendung des OSCI Transport Standards realisiert. Dieser unterstützt die kryptografisch unterschiedliche Behandlung der Metadaten und der eigentlichen Inhaltsdaten, so dass der sichere Transport auch dann gewährleistet wird, wenn die Betreiber der OSCI Intermediäre keinerlei Kenntnis vom Nachrichteninhalt erlangen können.

Angesichts wachsender Anforderungen an die Infrastrukturen der öffentlichen Verwaltung wird dieses Prinzip durch den ebenfalls im Auftrag des IT-Planungsrats von der KoSIT herausgegebenen Standard XTA erweitert, und noch stärker auf die Anforderungen der als Transporteur agierenden Stellen angepasst.

2.5 Die Dritten Stellen kennen die Metadaten der Datenübermittlung, insbesondere kennen sie die Identität der Kommunikationspartner

*Die Identität der behördlichen Kommunikationspartner (**Autor** und **Leser**) soll durch Zertifikate nachgewiesen werden, die einer von der öffentlichen Verwaltung kontrollierten Publik Key Infrastructure (PKI) entstammen.*

2.6 Der Identifier ist nicht Bestandteil der Metadaten der Datenübermittlung

Durch diese Festlegung soll ausgeschlossen werden, dass Transporteure eine personenbezogene Profilbildung betreiben können, die über alle innerbehördlichen Datenübermittlungen zu einer bestimmten Person Auskunft geben könnte

2.7 Die Vertraulichkeit der Datenübermittlung wird mindestens auf der Strecke zwischen den Transporteuren durch eine hinreichende Verschlüsselung sichergestellt.

2.8 Jede sektorübergreifende Datenübermittlung muss durch eine Dritte Stelle unter Angabe der Kommunikationspartner und dem Zweck hergestellt (vermittelt) werden

Diese Dritte Stelle wird Vermittlungsdienst oder Verzeichnisdienst genannt. Sie versorgt die Transporteure mit den für den Transport erforderlichen Angaben (z. B. öffentlichen

Schlüsseln des Empfängers zwecks Gewährleistung der Vertraulichkeit durch Verschlüsselung).

Die Herstellung einer Verbindung ist nur dann möglich, wenn es für den angegebenen Zweck und die angegebenen Kommunikationspartner einen entsprechenden Eintrag im Vermittlungs- bzw. Verzeichnisdienst gibt. Anders ausgedrückt: Datenübermittlungen, für die keine Rechtsgrundlage angegeben werden kann, oder bei denen die Angaben zu Sender, Empfänger und Zweck nicht zueinander passen, können nicht vermittelt werden.

In der Innenverwaltung kommt für diese Zwecke das DVDV 2 zum Einsatz.

2.9 Einträge in den Verzeichnis- bzw. Vermittlungsdienst können nur durch öffentliche Stellen in einem offengelegten (transparenten) Prozess erfolgen

Die Tatsache, dass nur solche Datenübermittlungen vermittelt werden können, für die es einen hinsichtlich der Kommunikationspartner und dem Zweck passenden Eintrag gibt, ist für die Kontrollfunktionen entscheidend. Daher dürfen Eintragungen nur in einem kontrollierten Verfahren vorgenommen werden.

Nur die durch den Bund bzw. die Länder bestimmten „pflegenden Stellen" sind befugt, Einträge in das DVDV 2 vorzunehmen, welches in der Innenverwaltung als Vermittlungsdienst agiert. Dafür erforderliche Datenübermittlungen zwischen „pflegenden Stellen" und dem DVDV 2 sind ebenfalls durch OSCI-Transport gesichert. Dadurch werden unbefugte Manipulationen verhindert, gleichzeitig wird Nachvollziehbarkeit sichergestellt.

2.10 Alle zur Infrastruktur gehörenden Komponenten werden in einem offenen, von der öffentlichen Verwaltung kontrollierten Prozess betrieben und weiterentwickelt

Entsprechend der bisherigen Ausführungen gehören zur Infrastruktur folgende Anwendungen und Interoperabilitätsstandards:

- *Der Vermittlungs- bzw. Verzeichnisdienst. In der Innenverwaltung: DVDV 2*
- *Der oder die Transporteure. In der Innenverwaltung: die Betreiber der OSCI Intermediäre.*
- *Eine Public Key Infrastrukture (PKI) für den Nachweis der Identität der Kommunikationspartner*
- *Ein oder mehrere Standards für die Interoperabilität zwischen allen an der Datenübermittlung beteiligten Stellen der Infrastruktur. Diese müssen als offene Standards im Sinne der Free Software Foundation Europe e.V. (FSFE) betrieben werden.*

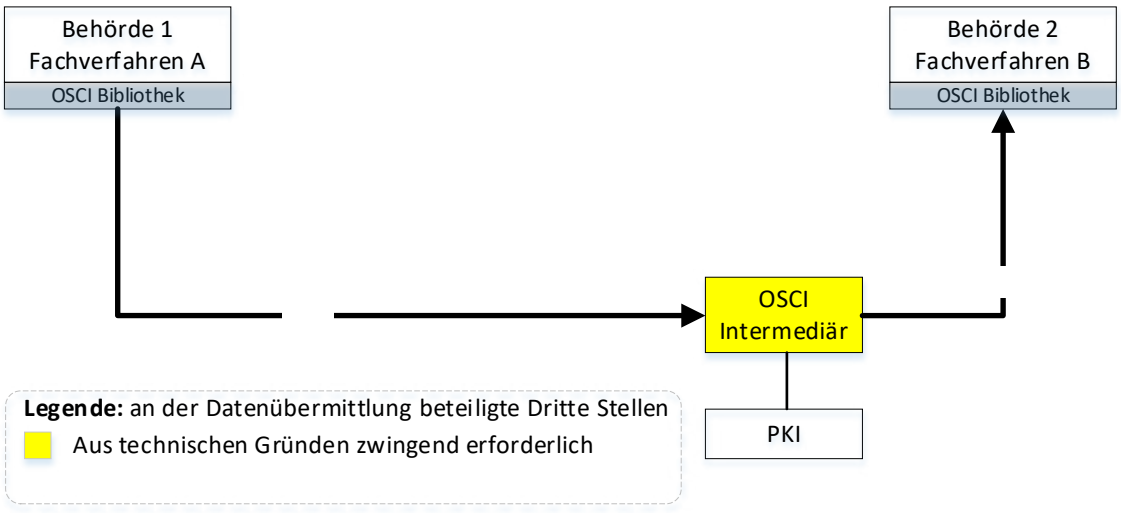
  In der Innenverwaltung sind dies die beiden im Auftrag des IT-Planungsrats herausgegebenen Standards OSCI-Transport und XTA.

Durch die Verpflichtung zur (Weiter-) Entwicklung aller zur Infrastruktur gehörenden Komponenten (Anwendungen und Standards) wird die notwendige Transparenz gewährleistet, die wiederum den Aufsichtsbehörden die Wahrnehmung ihrer Kontrollaufgaben ermöglicht.

3 Konkretisierung für die Innenverwaltung

Nachfolgend werden die allgemein gehaltenen, technikneutralen Anforderungen des Abschnitt 2 für die in der Innenverwaltung vorhandene Infrastruktur konkretisiert und erläutert. Sie basiert auf Standard OSCI Transport. Er wurde durch die OSCI-Leitstelle (Vorläufer der KoSIT) gemeinsam mit dem BSI entwickelt und im Jahr 2002 erstmalig veröffentlicht. Er ist fachunabhängig, das heißt, für die Datenübermittlung zwischen beliebigen Kommunikationspartnern innerhalb und außerhalb der öffentlichen Verwaltung geeignet. Er erfordert zwingend eine Infrastrukturkomponente, bei der kryptografische Funktionen gebündelt und Nachrichten aufbewahrt werden können (Intermediär). Betreiber der Intermediäre können ihre Aufgaben ohne Kenntnis der Inhaltsdaten wahrnehmen (Ende-zu-Ende Verschlüsselung). Dies ermöglicht den Betrieb von Intermediären durch zentrale Stellen. Das ursprüngliche Konzept (ca. 2005) ist in Abbildung 1 dargestellt.

Abbildung 1: Ursprüngliches Konzept für OSCI



Dieses Konzept erwies sich jedoch als nicht ausreichend, weil die Komplexität der Organisation der sicheren Datenübermittlung mit tausenden von Kommunikationspartnern auf der Ebene des Bundes, der Länder und vor allem aller Kommunen unterschätzt worden ist.

Die inzwischen tatsächlich vorhandene, in der Praxis bewährte Infrastruktur der Innenverwaltung ist dementsprechend komplexer. Sie ist Abbildung 4 in dargestellt. Sie wird in identischer bzw. sehr ähnlicher Form auch im Bereich der Übermittlung elektronischer Gewerbeanzeigen gemäß § 14 Absatz 8 GewO und im elektronischen Rechtsverkehr genutzt.

Verzeichnisdienst DVDV 2

Bei einer Vielzahl von Kommunikationspartnern ist eine zentrale Stelle erforderlich, die eine Übersicht über alle insgesamt angebotenen elektronischen Dienste führt. Hierfür wurde das Deutsche Verwaltungsdiensteverzeichnis DVDV eingeführt. Darin ist beispielsweise verzeichnet, welche technischen Kommunikationsparametern für die Behörde erforderlich sind, die den Dienst der Abruf von Meldedaten gemäß § 38 BMG für die Kommune Bremerhaven anbietet.

Nähere Informationen zum DVDV 2 und den aktuell eingetragenen Diensten sind auf der Webseite des ITZ Bund erhältlich [1, 2].

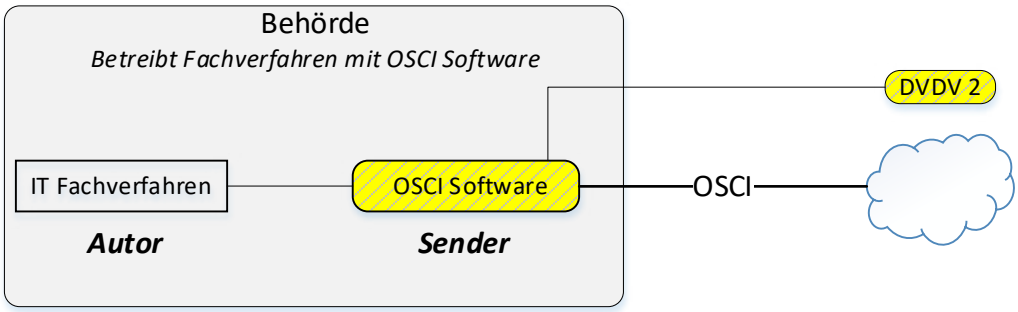
Organisation des sicheren Transports als eigenständige Aufgabe

Bei einer Vielzahl von Kommunikationsbeziehungen ist die Organisation des Nachrichtentransports eine komplexe Aufgabe. Sie beinhaltet den Umgang mit elektronischen Zertifikaten, die Identifikation und Behebung technischer Fehler, die Protokollierung etc.

Transportaufgaben wurden daher ausgelagert und eigenen Rollen zugewiesen. Diese werden als **Sender** bzw. **Empfänger** und zusammenfassend als **Transporteure** bezeichnet. Es gibt unterschiedliche Ausprägungen, die in Abbildung 2 und Abbildung 3 jeweils für die Rolle Sender dargestellt werden.

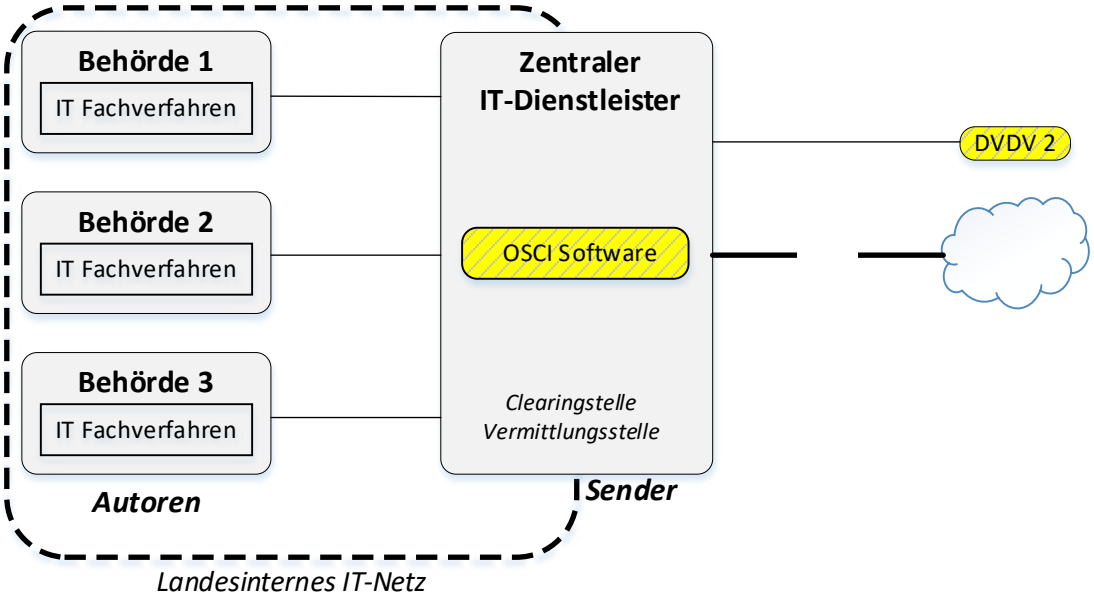
Es kann sich um eine spezielle Software handeln, die als Ergänzung eines IT-Fachverfahrens bereitgestellt wird, um die Datenübermittlung mit OSCI zu organisieren (teilweise als Kommunikationsserver bezeichnet). In diesem Fall agiert die Behörde, bei der das Fachverfahren betrieben wird, gleichzeitig als Transporteur (siehe Abbildung 2).

Abbildung 2: Anbindung mit OSCI Software (Kommunikationsserver)



Häufiger ist jedoch die Errichtung einer für ein Bundesland zentralen Clearing- oder Vermittlungsstelle (siehe § 2 Abs. 3 der 1. BMeldDÜV), bei der die Rolle des Transporteurs im Wege der Datenverarbeitung im Auftrag der angeschlossenen Fachbehörden wahrgenommen wird.

Abbildung 3: Clearing- bzw. Vermittlungsstellen



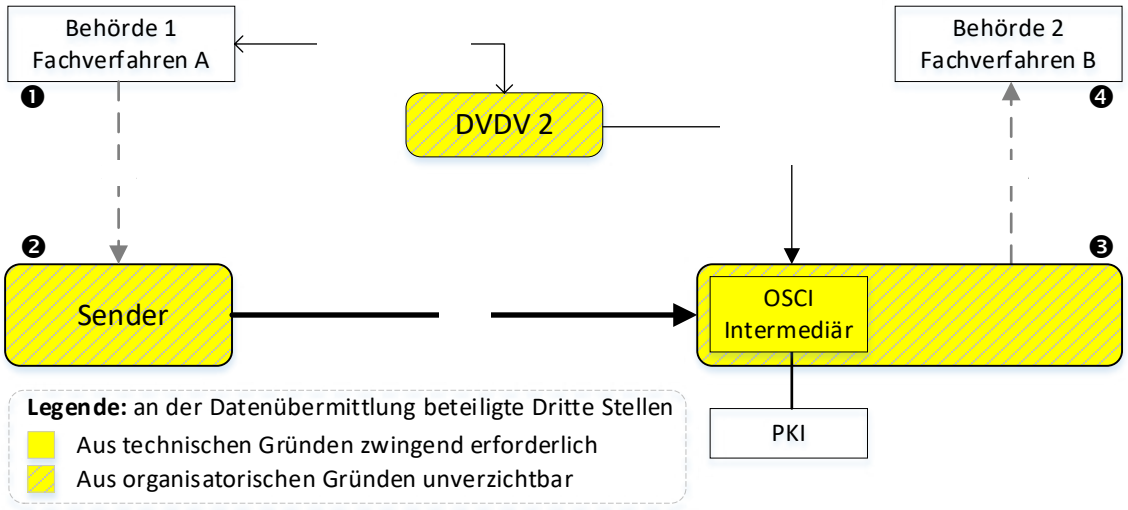
Die Betreiber der für die OSCI Infrastruktur zuständigen Clearingstellen haben sich selbstorganisiert zusammengeschlossen und tagen regelmäßig.

Unabhängig von der Art der Anbindung ergibt sich aufgrund der konzeptionellen Trennung der Aufgaben einer Fachbehörde, die als Autor bzw. Leser einer Fachnachricht agiert, und der

Organisation des sicheren Transport die in Abbildung 4 schematisch dargestellte Infrastruktur der Innenverwaltung. Sie ist seit 2007 ohne nennenswerte Störungen in Betrieb. Jährlich werden mehrere 100 Millionen Nachrichten übermittelt.

Solche Infrastrukturen werden als *4-Corner Modell* bezeichnet (die vier Ecken sind in Abbildung 4 gekennzeichnet). Nach unserem Kenntnisstand ist die Tatsache, dass die beim Transport zu beteiligenden Dritten Stellen ihre Aufgabe auch ohne Kenntnis des Nachrichteninhalts erbringen können, zumindest nicht selbstverständlich (ggfs. ein Alleinstellungsmerkmal).

Abbildung 4: Infrastruktur der Innenverwaltung (schematisch)



Dritte Stellen im Sinne des Eckpunktepapiers

Hinsichtlich der Aussagen des Eckpunktepapiers bedeutet das insbesondere, dass die als Transporteure agierenden Stellen (*„Sender“* und *„Empfänger“* in Abbildung 4 nicht aus technischen Gründen zwangsläufig mit dem Einsatz von OSCI verbunden sind. Dies wäre lediglich der OSCI Intermediär. In der Praxis ist aber deutlich geworden, dass die Organisation des sicheren Nachrichtenversands in einer flächendeckenden Infrastruktur der öffentlichen Verwaltung so komplex ist, dass er spezialisierten Rollen übertragen werden muss.

Dies sind meistens rechtlich eigenständige Organisationseinheiten, deren originäre Aufgabe darin besteht, im Auftrag angeschlossener IT-Fachverfahren die effiziente und verlässliche Datenübermittlung gemäß einschlägigen Rechtsgrundlagen sicherzustellen. Sofern ihnen im Rahmen der Einführung eines verfahrensübergreifenden Identifiers zusätzliche Kontrollaufgaben bei Sektor-übergreifenden Datenübermittlungen zugewiesen werden, sollte ggfs. ihre rechtliche Einordnung neu bestimmt werden.

Neben den Transporteuren kommt auch der Verzeichnisdienst DVDV 2 als *Dritte Stelle* zur Wahrnehmung von Kontrollfunktionen im Sinne des Eckpunktepapiers in Betracht.

Welche Lösung am besten geeignet ist, wird noch zu bestimmen sein, wenn

a) Klarheit über die „Sektoren“ hergestellt worden ist, an deren Grenzen Kontrollfunktionen eine Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen verhindern; und
b) Die dort erforderlichen Kontrollfunktionen näher bestimmt worden sind.

Weblinks

[1] DVDV bei ITZ Bund

[2] Übersicht der Dienste im DVDV

Eckpunkte für die Registermodernisierung

Bestehende Anforderungen, vorläufige Architekturskizze sowie sich daraus ergebende Maßnahmen im Rahmen des IT-Planungsratsprojekts Registermodernisierung

April 2020

Inhaltsverzeichnis

1. Kontext und Inhalte des Dokuments

I. Kernbotschaften

Kontext

Eine moderne Registerlandschaft mit automatisiertem und sicherem elektronischen Datenaustausch sowie hochqualitativer Datenhaltung zwischen beteiligten Registern ist Voraussetzung für die Digitalisierung der deutschen Verwaltung. Um das Gesamtvorhaben der Registermodernisierung zu unterstützen, wurden mehrere Vorhaben mit jeweils eigenem Fokus ins Leben gerufen:

- Das Koordinierungsprojekt Registermodernisierung seitens des IT-Planungsrats (IT-PLR)
- Das von der Innenministerkonferenz (IMK) initiierte Vorhaben zur Einführung eines registerübergreifenden Identitätsmanagements
- Das Vorhaben zur Reduktion von Statistikpflichten bei Unternehmen seitens der Wirtschaftsministerkonferenz (WiMiKo)
- Weitere ressortspezifische Digitalisierungs- und Harmonisierungsvorhaben wie etwa eJustice (Justiz) und Gematik (Gesundheitswesen).

Das vorliegende Dokument konsolidiert die aus zwei durchgeführten Workshops und dem daran anschließenden Austausch in Arbeitsgruppen ermittelten Anforderungen an das Gesamtvorhaben der Registermodernisierung und zeigt den aktuellen Erkenntnisstand zu möglichen Lösungsoptionen auf.

Das Dokument ist im Rahmen des Koordinierungsprojekts Registermodernisierung unter Federführung des Bundesministeriums des Innern, für Bau und Heimat (BMI) entstanden mit dem Ziel, die Entwicklungen vorhabenübergreifend zu bündeln, um das weitere Vorgehen abzustimmen und zu vereinfachen. Es gibt den Stand der Überlegungen zum April 2020 wieder, vorbehaltlich der weiteren Entwicklungen eines Gesetzesentwurfs zum registerübergreifenden Identitätsmanagements.

Anwendungsfälle und Zielbild

Die Registermodernisierung sollte nutzerorientiert gestaltet werden. Als Nutzer anzusehen sind in diesem Kontext Bürger und Unternehmen, ggf. weitere Dritte

sowie die Verwaltung einschließlich der statistischen Ämter im Rahmen der jeweiligen relevanten Anwendungsfälle. Als Anwendungsfälle wurden identifiziert:

- Die digitale „Once-only"-Umsetzung von Verwaltungsleistungen für Bürger und Unternehmen, teilweise EU-weit, im Rahmen des Onlinezugangsgesetzes (OZG) und der Single-Digital-Gateway-Verordnung (SDG-VO)
- Die registerbasierte Durchführung des Zensus (Registerzensus)
- Der automatisierte, zwischenbehördliche Datenaustausch über Verwaltungsbereiche hinweg und ggf. die Anbindung weiterer Akteure an existierende Datenbestände auf bestehenden bzw. zukünftigen Rechtsgrundlagen.

Das Zielbild einer modernisierten Registerlandschaft ergibt sich aus den zukünftigen Abläufen dieser drei Anwendungsfälle. Es beschreibt das Zusammenspiel der bestehenden (ggf. ergänzten) dezentralen Registerlandschaft mit neuen Komponenten, um - datenschutzkonform - vollständig digitale Verwaltungsleistungen medienbruchfrei zu ermöglichen, den Zensus vollständig und in hoher Qualität registerbasiert durchzuführen und Daten zwischen Behörden (insbesondere über Verwaltungsbereiche hinweg) einfach, effizient und ohne manuelle Interaktion auszutauschen. Ermöglicht wird dies neben technischen Entwicklungen durch rechtliche und organisatorische Anpassungen.

Anforderungen und Erfolgsfaktoren

Aus dem beschriebenen Zielbild ergeben sich vier zentrale Anforderungen für die Umsetzung des Vorhabens der Registermodernisierung:

- **Einführung eines registerübergreifenden Identitäts- und Qualitätsmanagements.** Eindeutige Zuordnung natürlicher Personen und Unternehmen; aktives Qualitätsmanagement über bestehende Datenbestände; Anbindung an föderale Integrationsbemühungen seitens der EU
- **Ermöglichung des Datenaustauschs zwischen allen zu beteiligenden Stellen auf rechtlicher Grundlage.** Ausbau von Schnittstellen und Standards; Anpassung der Transportwege; ggf. Erweiterung des Zugriffs- und Rechtemanagements

- **Unterstützung der datenhaltenden Behörden für eine Ertüchtigung der Datenhaltung in Registern und elektronisch geführten Datenbanken.** Erfüllung von Vollständigkeit, Qualität und Datensparsamkeit
- **Umsetzung gemäß datenschutzrechtlichen Vorgaben** und **mit Schutz vor Profilbildung.** Etablierung von Sicherheitsmaßnahmen, Nachvollziehbarkeit und Transparenz.

Außerdem sind für die Umsetzung vier unterstützende Erfolgsfaktoren relevant:

- **Fokus auf den Nutzen** und die Akzeptanz für Bürger, Unternehmen und die Verwaltung
- **Inkrementelle Weiterentwicklung** der Bestandsarchitektur
- **Zukunftssicherheit und Flexibilität** für Anpassungen.
- **Berücksichtigung** der Vorgaben und Angebote der EU-Kommission

Aktueller Stand der Lösungsoptionen und zu klärende Fragen

Alle Anforderungen werden derzeit im Rahmen der einzelnen Vorhaben bearbeitet. Zu vielen Anforderungen liegen bereits Lösungsoptionen in unterschiedlichen Reifegraden vor. Die technisch-konzeptionellen Vorschläge sollen stets rechtlich und organisatorisch begleitet werden, da diese Themenfelder erfahrungsgemäß mindestens ebenso relevant für eine nachhaltige Lösung sind. Bei allen Lösungsoptionen wird darauf geachtet, dass die Arbeiten externer Dienstleister produkt- und dienstleisterneutral erfolgen. Ziel ist, dass konzipierte Lösungen, konzeptionelle Ausarbeitungen oder Vorbereitungen für alle Dienstleister in Bund und Ländern anschlussfähig sind. Der aktuelle Stand der jeweiligen Diskussion sowie die vorrangig zu klärenden Fragen werden im Dokument entlang der Anforderungen beschrieben.

- **Anforderungen an das Identitäts- und Qualitätsmanagement.** Die Analyse und Konzeption verschiedener Lösungsmodelle für ein Identitätsmanagement für Personen ist abgeschlossen. Die Grundentscheidung für ein Gestaltungsmodell ist noch nicht erfolgt. Die Ausgestaltung eines registerübergreifenden Identitätsmanagements bestimmt wesentlich die Rahmenbedingungen für die weitere Registermodernisierung. Parallel dazu erarbeitet das Bundesministerium für Wirtschaft und Energie (BMWi) derzeit ein Umsetzungskonzept für die

Einführung eines Basisregisters für Unternehmensstammdaten verbunden mit einer bundeseinheitlichen Wirtschaftsnummer. Sowohl im Falle personenbezogener Identifikatoren als auch im Bereich der Unternehmen ist die Anbindung an ein EU-weites Identitätsmanagement zunächst offen.

- **Anforderungen an den Datenaustausch.** Grundlegende Erkenntnisse zur Ausgestaltung neu zu schaffender Architektur und Schnittstellen liegen vor. Innerhalb einzelner Verwaltungsbereiche (etwa Inneres sowie Arbeit und Soziales) besteht bereits ein hoher Grad an Interoperabilität, daher erscheint die systematische Entwicklung von Verbindungen zwischen bestehenden Informationsverbünden als ein aussichtsreicher Weg zu einer schnellen Umsetzung. Hierfür werden neben technischen auch rechtliche und organisatorische Fragestellungen zu adressieren sein.

- **Anforderungen an die Datenhaltung.** Erste Analysen hinsichtlich der einzubeziehenden Register und elektronisch geführten Datenbanken sind Gegenstand der aktuellen Arbeiten im Koordinierungsprojekt. Im weiteren Verlauf wird zunächst eine Festlegung der Anforderungen an „moderne Register“ und anschließend eine detaillierte Übersicht der anzubindenden Register inklusive der jeweiligen technischen Standards und Fähigkeiten („Landkarte“) zu erstellen sein, um den Ertüchtigungsbedarf abzuschätzen. Die Konzeption der Basisdatenhaltung sowohl für Personen- als auch für Unternehmen wurde begonnen und wird jeweils unter Federführung des BMI sowie des BMWi erarbeitet. Darüber hinaus müssen neue Register aufgebaut werden, z. B. ein Gebäude- und Wohnungsregister und ein statistisches Bildungsregister. Die Sicherstellung einer befähigten Datenhaltung liegt in der Verantwortung der datenhaltenden Behörden; das Koordinierungsprojekt kann diese unterstützen, indem es Anforderungen zur Datenhaltung spezifiziert. Vorschläge für verbesserte Nutzungsmöglichkeiten für bereits in der Verwaltung vorhandenen Daten erarbeitet und ggf. übergreifende technische Lösungen konzipiert und betreut.

- **Anforderungen an die Datensicherheit/Schutz vor Profilbildung.** Mit dem 4-Corner-Prinzip wurde eine bereits etablierte und getestete Sicherungsmaßnahme für den sektorüberschreitenden Datenaustausch zwischen öffentlichen Stellen vorgeschlagen, über die im Vergleich möglicher Alternativen für

die Umsetzung eines registerübergreifenden Identitätsmanagements entschieden wird. Der nötige Ertüchtigungsbedarf, vor allem außerhalb der Innenverwaltung, muss ermittelt werden. Es wird erwogen, die existierende Protokollierung an mehreren Stellen der Architektur zu erweitern, um eine Nachvollziehbarkeit der Datenaustausche sicherzustellen. Zudem wird im derzeitigen Entwurf des BMI für ein Registermodernisierungsgesetz ein Datencockpit beschrieben, welches in Zusammenhang mit der OZG-Umsetzung Transparenz über erfolgte Datenaustausche ermöglichen soll. Zu klären wird sein, wie eine nutzerorientierte und gleichzeitig in datenschutzkonforme und dabei insbesondere auch datensparsame Ausgestaltung möglich wird.

Übergreifend wird deutlich, dass die bestehende Architektur der Registerlandschaft einer deutlichen Stärkung der Interoperabilität bedarf, was insbesondere die Weiterentwicklung bestehender und ggfs. neu zu schaffender Architekturkomponenten miteinschließt. Aus dem bisherigen Diskussionsstand wird in diesem Dokument eine erste übergreifende Architekturskizze entwickelt, die das mögliche Zusammenspiel der einzelnen Elemente auf konzeptionellem Niveau beschreibt.

Abgeleitete Maßnahmen im Koordinierungsprojekt

Das Koordinierungsprojekt Registermodernisierung hat folgende Arbeitspakete als nächste Schritte definiert:

- Übergreifende Steuerung und Konzeption
- Vervollständigung der Übersicht zu den Anforderungen
- Architekturmodell
- Recht
- Governance und Organisation
- Sicherstellen sichtbarer Erfolge

Das Koordinierungsprojekt wird in einem ersten Schritt sowohl einen „Blueprint“ für die Gesamtkonzeption erstellen als auch im Rahmen von punktuellen Erprobungen frühzeitig testen, wie vorrangige Maßnahmen erfolgreich umgesetzt werden können. Hierzu werden bis Ende 2020 die Ergebnisse aus den Arbeitspaketen konsolidiert und in Berichtsform an den IT-PLR übermittelt. Darüber hinaus soll die weitere Umsetzung begleitet werden.

II. Kontext der Registermodernisierung

Eine moderne Registerlandschaft mit automatisiertem und sicherem elektronischen Datenaustausch auch über Verwaltungsbereiche hinweg zwischen beteiligten Registern sowie hochqualitativer und datenschutzkonformer Datenhaltung innerhalb dieser ist Voraussetzung für die Digitalisierung der deutschen Verwaltung. Innerhalb einzelner Verwaltungsbereiche[1] besteht oftmals bereits ein effizienter und großvolumiger automatisierter Datenaustausch, wohingegen im Rahmen der weiteren Arbeiten eine größere Harmonisierung zwischen den Verwaltungsbereichen angestrebt werden sollte. Neben der noch stärkeren Digitalisierung von Verwaltungsprozessen schaffen Digitalisierungsvorhaben der Europäischen Kommission wie die SDG-Verordnung und auch die Datenschutz-Grundverordnung weitere Erfordernisse für eine Modernisierung. Der IT-PLR hat daher in seiner 29. Sitzung am 27.06.2019 das Koordinierungsprojekt Registermodernisierung mit folgenden Aufgaben ins Leben gerufen[2]:

- Identifizierung der Anforderungen an eine Registermodernisierung
- Erstellung eines Architekturmodells für eine Registerlandschaft auf der Basis vernetzter Register
- Erfassung der Anforderungen für gesetzliche Änderungen
- Erstellung eines Zielbilds und einer Maßnahmenplanung.

Grundsätzlich ergeben sich derzeit drei zentrale Anwendungsfälle, die Anforderungen an die Registermodernisierung stellen:

1. Die digitale „Once-only"-Abwicklung von Verwaltungsleistungen für Bürger[3] und Unternehmen, teilweise EU-weit, gemäß OZG und SDG-VO[4]

[1] Beispiele sind u.a. Finanzwesen, Steuerautomation, Gemeinsame Grundsätze der Träger im Sozialbereich für SGB (z.B. Rente, BA, Krankenkassen), Innenverwaltung, Gesundheitswesen (Gematik) sowie Justiz (eJustice)

[2] https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2019/Sitzung_29.html?pos=5

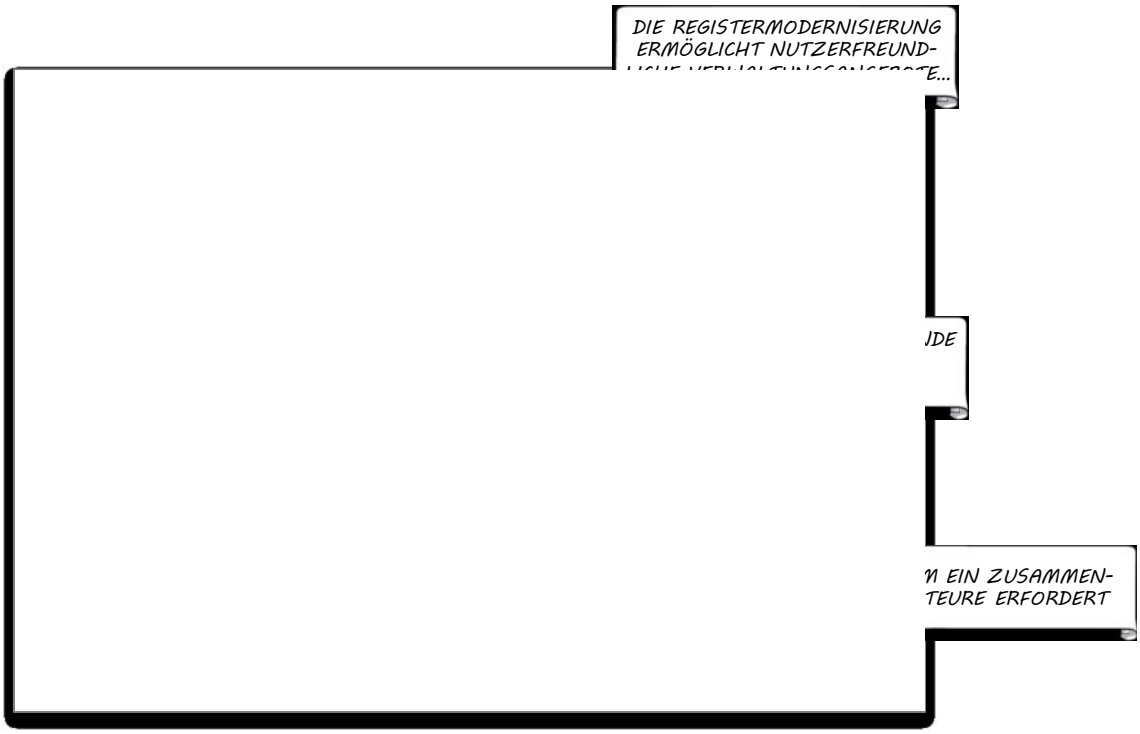
[3] Im Sinne einer besseren Lesbarkeit beschränkt sich das Dokument im Folgenden bei der Nennung von Personen, Berufen, Positionen und Titeln auf die männliche Form, ohne damit die weibliche ausschließen zu wollen.

[4] Ermöglichung ausgewählter „Once-only"-Leistungen bis Ende 2023; https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018R1724&from=EN

2. Die registerbasierte Durchführung des Zensus (Registerzensus)[5]
3. Der datenschutzkonforme automatisierte, zwischenbehördliche Datenaustausch auf rechtlicher Grundlage.

Die Registermodernisierung ist somit ein umfassendes Vorhaben und erfordert die Einbindung aller Ressorts und aller föderalen Ebenen sowie ggf. weiterer Dritter. Im Rahmen des Koordinierungsprojekts wurde im September bzw. Dezember 2019 in zwei Workshops die sinnbildliche Visualisierung als „gemeinsamer Bebauungsplan“ gewählt (siehe Abbildung 1), die ausdetailliert auch als Fold-Out beiliegt (siehe separate Datei).

Abbildung 1: Visualisierung des Zielbilds für die Registermodernisierung



[5] Hier z.B. Erfüllung von Anforderungen der EU – jährliche Übermittlung kleinräumiger Bevölkerungszahlen ab 2024 (Ergebnisprotokoll Workshop Koordinierungsprojekt September 2019, S. 22)

III. Struktur dieses Dokuments

Kapitel 2 beschreibt vertieft die drei genannten Anwendungsfälle für die Registermodernisierung und bietet einen Überblick über bestehende Festlegungen, die im Rahmen des Koordinierungsprojekts Registermodernisierung aufgegriffen werden. Aus den Anwendungsfällen ergibt sich das Zielbild der Registermodernisierung.

Kapitel 3 leitet aus den Erläuterungen in Kapitel 2 übergreifende Anforderungen und Erfolgsfaktoren für die Registermodernisierung ab.

Kapitel 4 erläutert den aktuellen Diskussionsstand zu Lösungsvorschlägen entlang der ermittelten Anforderungen, unterschieden nach bereits entwickelten Konzepten und Ideen und noch zu klärenden Themen. Eine vorläufige Architekturskizze zur Registermodernisierung veranschaulicht die Gesamtheit der aktuell diskutierten technischen Lösungsvorschläge.

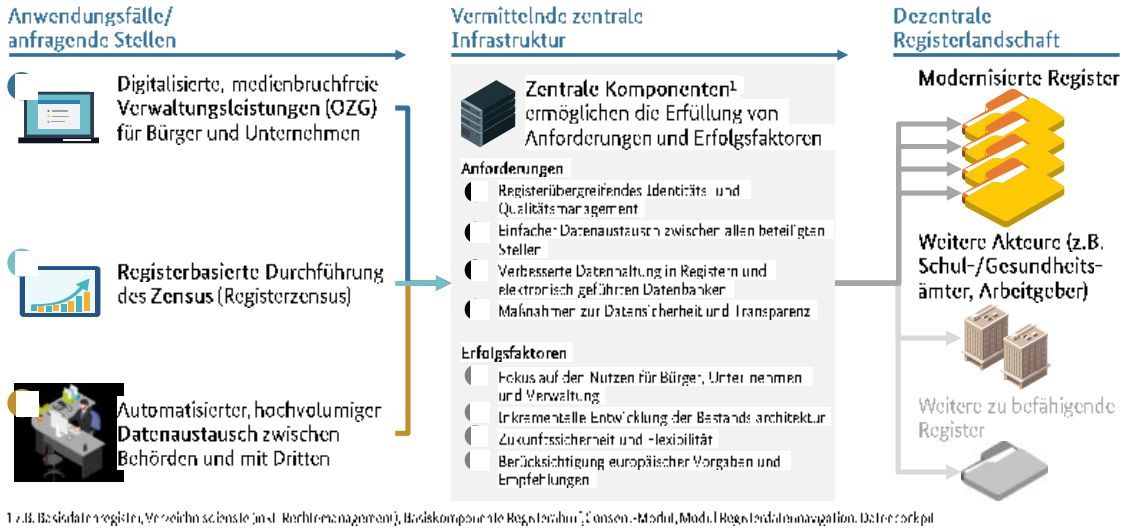
Kapitel 5 definiert anhand der Anforderungen und Lösungsansätze geeignete Maßnahmenpakete technischer, rechtlicher oder organisatorischer Natur. Diese werden ergänzt durch Steuerungsmaßnahmen und spezifische Maßnahmen zur frühen Umsetzung (d.h. bis Ende 2020) von punktuellen Erprobungen. Abschließend zeigt das Kapitel die nächsten Schritte auf.

2. Zielbild und Anwendungsfälle der Registermodernisierung

I. Beschreibung der drei relevanten Anwendungsfälle einer modernisierten Registerlandschaft

Die Registermodernisierung ist ein umfangreiches und technisch komplexes Vorhaben mit Auswirkungen auf eine Vielzahl von Akteuren auf EU-, Bundes-, Landes- und kommunaler Ebene und ggf. weiterer Dritter. Aus der Beschreibung der relevanten drei Anwendungsfälle ergibt sich ein gesamthaftes Bild zu den derzeitigen Anforderungen der Registermodernisierung (siehe Abbildung 2).

Abbildung 2: Gesamtkontext der Registermodernisierung – erste übergreifende Architekturskizze für die drei relevanten Anwendungsfälle



1 z.B. Basisdatenregister, Verzeichnisdienste (inkl. Rechtemanagement), Bidirektionale Registerbrücke, Zensus-Modul, Modul Registerdatenmanagement, Datenexzerpt

1. Anwendungsfall: digitale „Once-only"-Abwicklung von Verwaltungsleistungen für Bürger und Unternehmen

Aktueller Stand der Diskussion

Im Rahmen der Umsetzung des OZG[6] sowie des Single Digital Gateway (SDG)[7] der EU werden aktuell alle dafür geeigneten Verwaltungskontakte digitalisiert. Bürger und Unternehmen sollen zukünftig sämtliche Leistungen nutzerfreundlich auch elektronisch abwickeln können. Dabei soll der Grundsatz der einmaligen Erfassung („Once-only"-

[6] OZG online: https://www.gesetze-im-internet.de/ozg/BJNR313800017.html

[7] Ermöglichung ausgewählter „Once-only"-Leistungen bis Ende 2023; https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018R1724&from=EN

Prinzip) auch für Behörden untereinander umgesetzt werden[8] – d.h. Bürger oder Unternehmen sollen ihre Daten jeweils nur einmal an den Staat übermitteln müssen. Bereits durch eine Behörde gespeicherte Daten – z.B. der Familienstand oder eine Eheurkunde – werden dann bei weiteren Anträgen mit Einverständnis der Betroffenen aus den datenhaltenden Registern abgerufen, so dass die Antragstellung einfach und medienbruchfrei erfolgen kann.

Zielbild

Im Zielbild können alle relevanten Verwaltungsleistungen auch online durch Bürger bzw. Unternehmen beantragt bzw. möglichst auch auf digitalem Wege erbracht werden. Im Rahmen der Abwicklung der Onlineleistung erfolgt eine Identifikation in einem Nutzerkonto (Bürger- bzw. Unternehmenskonto) auf verschiedenen Vertrauensniveaus; im Vertrauensniveau „hoch" mittels eID, im Vertrauensniveau „niedrig" z.B. mit Benutzername/Passwort. Der Antragsprozess selbst ist medienbruchfrei und dem „Once-only"-Prinzip folgend gestaltet. Alle im Antrag benötigten Daten, die bereits in der Verwaltung vorliegen, können auf Wunsch des Bürgers aus den jeweils originär zuständigen Registern abgerufen werden. Das gilt auch für Nachweise, z.B. Urkunden. Die entsprechenden Datenfelder werden mittels Registerabruf vorbefüllt. Zudem wird sichergestellt, dass alle Behörden die Daten, die sie für ihre Aufgabenerfüllung benötigen, schnell und unkompliziert erhalten können und dürfen. Einmal erhobene Informationen stehen im Rahmen eines Rechte- und Rollenkonzepts für alle weiteren berechtigte Zwecke im Rahmen der rechtlichen Vorgaben zur Verfügung. Diese konsequente „Once-only"-Abwicklung von Anträgen ermöglicht eine signifikante Zeitersparnis seitens des Antragstellers und erspart in vielen Fällen den Weg zum Amt.

2. Anwendungsfall: registerbasierte Durchführung des Zensus (Registerzensus)

Aktueller Stand der Diskussion

In Deutschland sind die Statistischen Ämter des Bundes und der Länder mit der regelmäßigen Durchführung des Zensus und der Bevölkerungsstatistiken beauftragt. Alle zehn Jahre erfolgt zur Erfüllung von Anforderungen auf EU- sowie auf nationaler Ebene ein Zensus mit Erhebungen zu demografischen Merkmalen der Bevölkerung, zum Bildungsstand, zur Arbeitsmarktbeteiligung, zu Haushalts- und Familienangaben, zum

[8] Vgl. hierzu für die Bundesverwaltung: Digitalisierungsprogramm OZG Bund – Reifegradmodell

Gebäude- und Wohnungsbestand sowie zu den Wohnverhältnissen der Bevölkerung. Aufgrund neuer EU-Anforderungen müssen schon vor der regulären Zensusrunde im Jahr 2031 voraussichtlich ab 2024 jährlich geokodierte Bevölkerungszahlen übermittelt werden. Dies kann mit dem derzeitigen System nicht umgesetzt werden. Im bisherigen Zensusmodell werden zur Korrektur der Fehlerfassungen in den Melderegistern sowie zur Ermittlung von Merkmalen, die nicht in Registern vorhanden sind, persönliche Befragungen von stichprobenartig ausgewählten Haushalten vorgenommen sowie eine Erhebung bei allen Eigentümerinnen und Eigentümern von Gebäuden und Wohnungen durchgeführt. Dieses Vorgehen ist zum einen sehr aufwändig und kostenintensiv und bedeutet zum anderen eine zusätzliche Belastung für die zu befragenden Personen. Künftig soll der Zensus registerbasiert ohne ergänzende Befragungen durchgeführt werden (Registerzensus). Hierfür sind vor allem Voraussetzungen hinsichtlich der Datengrundlagen, der Datenqualität in den zugrunde liegenden Registern sowie der Möglichkeiten zur Zuordnung von Registereinträgen zu erfüllen.[9] Dazu wird aktuell geplant, die notwendigen fachlichen, rechtlichen und technischen Voraussetzungen für die Ermittlung, Qualitätssicherung und Zuordnung der Registerdaten (perspektivisch mittels Personenidentifiern sowie mit Gebäude- und Wohnungsnummern) zu schaffen und ggf. neue Register aufzubauen, um Datenlücken zu schließen.

Zielbild

Im Zielbild werden die für den Zensus benötigten Daten gemeinsam mit den in den Ursprungsregistern vorhandenen Identifiern zu Personen und zu Gebäuden und Wohnungen an die Statistik übermittelt, womit innerhalb der Statistik eine eineindeutige Zuordnung von z.B. Basisdaten zu Personen, Daten zur Arbeitsmarktbeteiligung und zu Bildungsabschlüssen sowie die Bildung von Haushalten und ihre Verknüpfung mit Wohnungen möglich wird. Die arbeits- und kostenintensiven Haushaltsbefragungen können somit entfallen. Die Übermittlung der Personendaten kann nach Vorliegen eines Identifiers pseudonymisiert erfolgen. Die Einzeldaten unterliegen weiterhin dem Statistikgeheimnis, eine Auswertung findet nur auf aggregierter Ebene statt. Ein neu geschaffenes statistisches Bildungsregister und ein Gebäude- und Wohnungsregister komplettieren die Datenlage. Die Prüfung der Angaben aus den Melderegistern auf Über-

[9] Anforderungen und Perspektiven auf dem Weg zu einem künftigen Registerzensus, Statistisches Bundesamt, Sonderheft Zensus 2021, 2019

und Untererfassungen erfolgt unter anderem durch Nutzung des „Lebenszeichenansatzes“[10] und wird durch ein vorgesehenes Datenmerkmal in den Basisdaten (z.B. letzter Verwaltungskontakt) unterstützt.

3. Anwendungsfall: zwischenbehördlicher Datenaustausch und ggf. Anbindung weiterer Dritter

Aktueller Stand der Diskussion

Es besteht ein intensiver Datenaustausch auf rechtlicher Grundlage zwischen Behörden untereinander und teilweise zwischen Behörden und berechtigten Akteuren aus der Privatwirtschaft. Besonders Austausche über Verwaltungsbereiche (etwa Inneres, Arbeit und Soziales, Gesundheit) hinweg verlaufen oftmals zeitaufwendig und umständlich. Auf Grund fehlender eindeutiger Zuordnung vieler Datensätze sind aufwendige manuelle Prüfungen unter Zuhilfenahme eines „Datenkranzes“ (z.B. Vor- und Nachname, Geburtsdatum und -ort) erforderlich. Daher besteht ein Bedarf an zuverlässigen, automatisierten und reibungslosen Datenübertragungen. Als weiterer Aspekt ist zu beleuchten, inwiefern redundante Datenhaltungen in den Fachregistern mit den neu gewonnenen Möglichkeiten der sicheren Zuordnung aufgelöst werden können. Daneben zählen zu diesem Anwendungsfall alle bisherigen und zukünftigen Übermittlungsbedarfe auf rechtlicher Grundlage ohne Verbindung zu einer konkreten Verwaltungsleistung.

Zielbild

Im Zielbild könnte ein automatisierter Datenaustausch zwischen berechtigten Stellen ohne manuelle Interaktion erfolgen. Die beteiligten Register könnten die angefragten Datensätze eineindeutig mittels eines registerübergreifenden Identitätsmanagements zuordnen; es wäre keine manuelle Überprüfung der Ergebnisse (z.B. von Personen gleichen Namens) nötig. Zudem könnten – vorbehaltlich rechtlicher Grundlagen und auf Basis ihrer jeweiligen Berechtigungen – deutlich mehr beteiligte Stellen miteinander kommunizieren. Die rechtliche Zulässigkeit des Datenaustauschs würde mittels geeigneter Sicherheits-maßnahmen sichergestellt, und entstehende Datenaustausche würden protokolliert. Die Basisdaten einer Person könnten direkt von einer zentral vorhaltenden Stelle durch berechtigte Behörden in hoher Qualität abgerufen werden. Für andere Datenpunkte ist geklärt, welche Register originär zuständig sind. Langfristig könnten die Systeme in den

beteiligten Stellen mit einem deutlich reduzierten Datensatz arbeiten – nämlich mit denjenigen Daten, für die die Stelle originär zuständig ist. Dafür bedarf es einer Stärkung der Interoperabilität der beteiligten IT-Verfahren auf allen Ebenen (rechtlich, organisatorisch, semantisch und technisch) und der Etablierung von „IT-Brücken“ zwischen bestehenden Informationsverbünden unter der Maßgabe einer übergreifenden „Interoperabilitäts-Governance“.

II. Bestehende Festlegungen zum Thema Registermodernisierung

Eine Reihe unterschiedlicher Gremien hat Beschlüsse zur Ausgestaltung der Registermodernisierung gefasst und relevante Rahmenbedingungen für diese festgelegt:

MPKs vom 06.06. und 05.12.2019

Die MPK befasste sich sowohl mit der Digitalisierung der Verwaltung als auch mit Leitlinien für eine Modernisierung der Registerlandschaft. Hierbei wurde die Empfehlung ausgesprochen, verbesserte Voraussetzungen für die Durchführung des Zensus ab 2024 zu schaffen, eine frühzeitige Beteiligung des BMI, des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) und der Datenschutzbeauftragten des Bundes und der Länder sicherzustellen und Vorarbeiten der ressortübergreifenden BLAG zur Reduzierung von Statistikpflichten zum Basisregister für Unternehmen mit bundeseinheitlicher Wirtschaftsnummer zu befürworten.[11]

IMK vom 12. bis 14.06.2019[12] und IMK vom 04. bis 06.12.2019[13], TOP 32

Die IMK hat in ihrem Beschluss vom Juni 2019 das BMI mit konzeptionellen Arbeiten zur Verbesserung des Identitätsmanagements durch die Einführung eines Identitätsregisters als Teil der Registermodernisierung beauftragt und dabei die Länder einzubinden. Sie hat fünf für die Registermodernisierung zentrale Aufgabenbereiche identifiziert:

---

[11] http://www.landtag.ltsh.de/infothek/wahl19/unterrichtungen/00100/unterrichtung-19-00151.pdf

[12] Vgl. Sammlung der zur Veröffentlichung freigegebenen Beschlüsse der 211. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder vom 04. bis 06.12.2019 in Lübeck, TOP 32.

[13] Vgl. Zwischenbericht für die Innenministerkonferenz vom 04. bis 06.12.2019, BMI – Referat V II 2, Berichtsdatum: 01.09.2019.

1) Ein registerübergreifendes Identitätsmanagement einführen

2) Datensilos auflösen, „Once-only-Prinzip auch für Behörden untereinander verwirklichen“ und registerbasierten Zensus ermöglichen

3) Aktualität und Qualität sowie Datensicherheit und Datenschutz gewährleisten

4) Standardisierung auch in der Registerstruktur verwirklichen

5) Transparenz für die betroffenen Personen sicherstellen

Der entsprechende Abschlussbericht wurde ausgearbeitet, mit der Bund-Länder-AG Registerübergreifendes Identitätsmanagement abgestimmt und soll der IMK im Juni 2020 vorgelegt werden. Er befasst sich im Wesentlichen mit den für Ziffer 1 erforderlichen Maßnahmen.

Wirtschaftsministerkonferenz vom 25. bis 26.06.2019

Laut WiMiKo ergibt sich der Arbeitsauftrag zur Registermodernisierung als wesentlicher Aspekt für die Umsetzung eines Servicekontos für Unternehmen – zur Koordinierung der nationalen Initiativen (z.B. im Koordinierungsprojekt Registermodernisierung, IMK und Bund-Länder-AG (BLAG) zur Reduktion von Statistikpflichten) unter Berücksichtigung der europäischen Rahmenbedingungen.

Abschlussbericht der BLAG „Abbau von Statistikpflichten“ vom 02.10.2019

Von der BLAG wurden zur Reduzierung von Statistikpflichten[14] Vorschläge aus den Bereichen Modernisierung und Digitalisierung der Statistik sowie Reduzierung von Belastungen erarbeitet. Für die Modernisierung werden ein Basisregister für Unternehmensstammdaten in Verbindung mit einer bundeseinheitlichen Wirtschaftsnummer und eine Erweiterung oder Ergänzung der Verwaltungsdaten-Informationsplattform (VIP) vorgeschlagen. Ziel ist die bürokratische Entlastung und Vermeidung von wiederholten behördlichen Auskunftsersuchen durch Schaffung eines Unternehmensstammdatenbestands in einem Basisregister. Für die Digitalisierung werden verschiedene Potenziale benannt, wie die Datengenerierung über Big-Data-Analyse oder

[14] Abschlussbericht der ressortübergreifenden Bund-Länder-Arbeitsgruppe zur Reduzierung von Statistikpflichten, https://www.bmwi.de/Redaktion/DE/Downloads/A/abschlussbericht-reduzierung-von-statistikpflichten.pdf?__blob=publicationFile&v=6

Datennutzung in gewerblichen Zusammenhängen. Für viele Branchen wird über den Statistikabbau im engeren Sinne berichtet.

IT-PLR-Sitzungen vom 12.03. und vom 27.06.2019

In der 28. Sitzung hat der IT-PLR bereits das Koordinierungsprojekt Registermodernisierung eingerichtet – unter Federführung des Bundes, Hamburgs und Bayerns sowie unter Einbeziehung der Koordinierungsstelle für IT-Standards (KoSIT), des Aufbaustabs Föderale IT-Kooperation (FITKO) und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Laut Fachkongress des IT-PLR 2018 gibt es mehrere Kernanliegen der Modernisierung im Sinne von Anwendungsfall 1: die Information und Hilfe für Bürger und Unternehmen sowie den Zugang zu ausgewählten Verfahren. Diese sind direkte Bestandteile der Digitalisierung des Leistungsantrags.[15]

In der 29. Sitzung fasste der IT-PLR[16] Beschlüsse zur Registermodernisierung[17], mit denen unter anderem der Auftrag an das Koordinierungsprojekt Registermodernisierung nachgeschärft wurde. Demnach gehören zu den Aufgaben insbesondere die Identifizierung der Anforderungen, die Erstellung eines Architekturmodells, die Erfassung der Anforderungen für gesetzliche Änderungen und die Erstellung eines Zielbilds und einer Maßnahmenplanung (siehe oben).[18]

[15] Fachkongress des IT-Planungsrats 2018 am 16./17.04. in Weimar, „Single Digital Gateway der EU", Vortrag des BMI

[16] Auf Grundlage des am 01.08.2009 in Kraft getretenen Gesetzes zur Änderung des Grundgesetzes (Art. 91c) beschlossen (https://www.it-planungsrat.de/DE/ITPlanungsrat/RechtlicheGrundlagen/rechtliche_grundlagen_node.html)

[17] Sammlung der Beschlüsse einsehbar unter https://www.it-planungsrat.de/DE/ITPlanungsrat/OZG-Umsetzung/OZG_Umsetzung_node.html

[18] https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2019/Sitzung_29.html?pos=5

SDG-VO der EU vom 02.10.2018

EU-weit sollen das OOP (Once Only Principle)[19] als Anforderung aus der EU-Verordnung 2018/1724 zum SDG (ergänzend zur erfolgenden Umsetzung von OZG[20]) mittels vereinheitlichter Anlaufstellen den Verwaltungsaufwand senken.[21] Aus der SDG-Verordnung ergeben sich die Anforderungen, dass bis Ende 2020 die Verwaltungsportale aller Mitgliedstaaten in dem übergreifenden EU-Portal gebündelt werden und auf allen EU-Sprachen durchsuchbar sein sollen. Zusätzlich muss die elektronische Übertragung von Nachweisen im Zusammenhang mit vollständig online abzuwickelnden Verfahren bis Ende 2023 sichergestellt werden. Die Umsetzung für den grenzübergreifenden Austausch auf einem technisch automatisierten System soll die Leistungsgerechtigkeit durch den Austausch von Nachweisdaten durch Datenübermittlungen steigern. Gleichzeitig werden die Bürger entlastet, da Daten nur einmalig abgefragt werden sollen. Auch das Anmelden und Durchsetzen von Ansprüchen wird für die Bürger und Unternehmen durch „Once only" vereinfacht, während für Behörden dem Leistungsmissbrauch durch Nutzung von Falschidentitäten vorgebeugt werden kann. Das zugehörige Projekt „The Once Only Principle Project" (TOOP) und Nachfolger erarbeiten Referenzarchitekturen und ggf. -implementierungen für ein föderal übergreifendes System mit Fokus auf Unternehmen. Die Connecting Europe Facility stellt „Building Blocks" zur Verfügung, von denen einige bereits erfolgreich in Deutschland umgesetzt worden sind (beispielsweise eDelivery für die Umsetzung der Verordnungen des Bundes und der Länder zur elektronischen Rechnungsstellung). Sie erarbeitet eine Referenzarchitektur[22] für die supranationale „Once-only"-Abwicklung von Verwaltungsanträgen und Nachweiserbringungen.

---

[19] Der eGovernment-Aktionsplan 2016-2020 beschreibt das Once Only Principle (OOP), nach dem die Verwaltung sicherstellen soll, dass Bürger und Unternehmen gleiche Daten der Verwaltung nur einmalig übermitteln müssen (siehe https://ec.europa.eu/digital-single-market/en/news/communication-eu-egovernment-action-plan-2016-2020-accelerating-digital-transformation)

[20] Anforderungen an die EU-grenzüberschreitende Online-Identifizierung aus eIDAS-Verordnung Nr. (EU) 910/2014, Informationen zur Barrierefreiheit aus Richtlinie (EU) 2016/2102 und dem Übereinkommen der Vereinten Nationen über die Rechte von Menschen mit Behinderungen

[21] https://cordis.europa.eu/article/id/386894-cutting-the-bureaucratic-red-tape-using-the-once-only-principle/de

[22] OOP Technical System – Architecture Blueprint; Explanatory Note; 2020; Connecting Europe Facility

3. Anforderungen und Erfolgsfaktoren der Registermodernisierung

Aus den vorangehend beschriebenen Anwendungsfällen lassen sich übergreifende Anforderungen für die Registermodernisierung sowie Erfolgsfaktoren für deren Umsetzung ableiten. Diese sind als technikoffene Grundprinzipien zu verstehen, welche einen Rahmen für die Entwicklung technikgebundener Lösungsoptionen bieten sollen. Die dargelegten Einschätzungen beziehen sich auf die Ergebnisdokumentation zweier Workshops (September und Dezember 2019) im Rahmen des Koordinierungsprojekts Registermodernisierung sowie der laufenden Arbeit des Koordinierungsprojekts und seiner Unterarbeitsgruppe Architekturmodell.

I. Anforderungen an die Registermodernisierung

a. Registerübergreifendes Identitäts- und Qualitätsmanagement

In einer modernisierten Registerlandschaft müssen einander zugehörige Datensätze – etwa diejenigen, die sich auf die gleiche Person oder das gleiche Unternehmen beziehen – **eineindeutig einander zuzuordnen sein (Anforderung 1 an das Identitätsmanagement).** Hierfür ist es hilfreich, dass alle betrachteten Register eindeutige Identifier führen.

Das Identitätsmanagement soll zudem ein **aktives Qualitätsmanagement (Anforderung 2 an das Identitätsmanagement)** der Daten ermöglichen, da durch die oben beschriebene Zuordnung Inkonsistenzen deutlich leichter und automatisiert erkennbar sind. Hierfür ist es nötig, solche Inkonsistenzen zu erkennen und erforderliche Korrekturen zügig in allen beteiligten Registern zu veranlassen. Daneben sollten bestehende und etablierte Qualitätssicherungsprozesse der Register sollten soweit wie möglich genutzt werden. Zudem soll aus Datensätzen anhand eines möglichen Validitätswertes, die Verlässlichkeit, mit der die Übereinstimmung eines Personenbasisdatensatzes im Identitätsregister mit den wahren personenidentifizierenden Basisdaten einer Person angenommen werden kann, deutlich werden.

Schließlich sollte ein Identitätsmanagement kompatibel zu **Integrationsbemühungen seitens der EU (Anforderung 3 an das Identitätsmanagement)** (SDG-VO) gestaltet werden, die eine Anbindung an Identifier oder Registersysteme anderer Mitgliedsstaaten ermöglichen sollen.

b. Einfacher Datenaustausch zwischen allen beteiligten Stellen

Damit die zu beteiligenden Register und elektronisch geführten Datenbanken automatisiert Daten austauschen können, müssen bestehende **Schnittstellen und Standards** mit dem Ziel der Konvergenz weiterentwickelt werden **(Anforderung 1 an den Datenaustausch)**. Barrieren, die einer Interoperabilität entgegenstehen, sind abzubauen. Die Anbindung an entstehende EU-weite Standards im Rahmen von SDG ist zu berücksichtigen und umzusetzen.

Ebenso müssen die zu verwendenden **Transportwege (Anforderung 2 an den Datenaustausch)** zwischen einzelnen Akteuren geschaffen bzw. ertüchtigt werden, sofern zuvor eine rechtliche Grundlage eingerichtet und im heutigen Zustand noch keine technisch nutzbare Verbindung bestehen sollte. Dabei ist eine Verfügbarkeit der Daten in Echtzeit zumindest im Anwendungsfall 1 erforderlich.[23]

Eine Erweiterung und Ertüchtigung eines **Zugriffs- und Rechtemanagements (Anforderung 3 an den Datenaustausch)** ist als Querschnittsthema für das Gesamtvorhaben Registermodernisierung anzusehen. Die verbesserte Zuordnungsfähigkeit von Datensätzen muss mit einer entsprechenden hochwertigen Steuerung und Kontrolle der Datenaustausche einhergehen. Dafür bedarf es insbesondere der Transparenz der Zugriffsrechte für Behörden, die grundsätzlich durch die jeweils wahrzunehmenden Aufgaben festgelegt sind, und mittels infrastruktureller Maßnahmen umgesetzt werden sollen.

Prinzipiell sind drei unterschiedliche Fälle zu betrachten:

1. Die Kontrolle von Datenaustauschen auf Basis bestehender rechtlicher Grundlagen und Befugnisse für einen automatischen Austausch

2. Die Kontrolle von Datenaustauschen zum Abruf von Inhaltsdaten oder Nachweisen bei Online-Verwaltungsanträgen mit zusätzlicher Einwilligung des Bürgers

3. Die eineindeutige Identifikation von Bürgern oder Unternehmen im Nutzerkonto oder im Datencockpit.

[23] Ergebnisprotokoll Workshop Koordinierungsprojekt September 2019, S. 27

c. Verbesserte Datenhaltung in Registern und elektronisch geführten Datenbeständen

Alle Daten, die auf gesetzlicher Grundlage oder mit Einwilligung des Bürgers und der Bürgerin auch außerhalb des originären Zwecks benötigt werden, sollten in einem Register oder einem elektronisch geführten Datenbestand für berechtigte Stellen vorgehalten werden, , um **Vollständigkeit (Anforderung 1 an die Datenhaltung)** in der Datenhaltung zu erreichen, wobei ein hohes Maß an Datensicherheit gewährleistet sein muss,. Dafür sind zunächst die Anforderungen an „moderne Register" weiter abzustimmen und die Anforderungen an diese festzulegen, um anschließend den jeweiligen Modernisierungsbedarf objektiv bestimmen zu können. Bisher nicht vorhandene Register (insbesondere ein Gebäude- und Wohnungsregister) sollten zeitnah aufgebaut werden. Bei einem solchen Aufbau ist darauf zu achten, dass dieser von Beginn an interoperabel zur modernisierten Registerlandschaft erfolgt.

Die **Qualität (Anforderung 2 an die Datenhaltung)** der Daten (d.h. Validität, Konsistenz und Aktualität) soll in einer modernisierten Registerlandschaft deutlich über dem bisherigen Niveau liegen. Die Zuordnung einzelner Datenpunkte (z.B. Datum der Eheschließung) zu einem originär zuständigen Register ermöglicht die Definition so genannter „Leitregister". Zum anderen ermöglicht die registerübergreifende Zuordnung von Datensätzen die automatisierte Aufdeckung von Dateninkonsistenzen, die wiederum in einem von zentraler Stelle koordinierten Prozess zügig aufgelöst werden sollen.

d. Maßnahmen zur Datensicherheit und Transparenz

Die verbesserte und automatisierte Zuordnung von Registerdaten aus unterschiedlichen Verwaltungsbereichen darf eine unzulässige Zusammenführung von personenbezogenen Daten nicht zulassen. In einer modernisierten Registerlandschaft sind laut Einschätzung der Datenschutzkonferenz[24] entsprechende **Sicherungsmaßnahmen (Anforderung 1 an den Datenschutz)** zu etablieren, die auf wirksame technische und organisatorische Weise sicherstellen, dass Datenübermittlungen unterbunden werden, die bereits die Möglichkeit einer umfassenden Katalogisierung von Bürgerinnen und Bürgern durch den Staat, die das Persönlichkeitsrecht gefährdet, beinhalten.

---

[24] Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, 12.09.2019

Für eine **Nachvollziehbarkeit (Anforderung 2 an den Datenschutz)** und Kontrolle der beschriebenen Sicherungsmaßnahmen sind. die bestehenden Mechanismen der Protokollierung der vorgenommenen Datenaustausche zwischen Registern auszubauen. Diese kann im Verdachtsfall einen Missbrauch erhärten oder entkräften.

Zudem wird aktuell davon ausgegangen, dass eine erhöhte **Transparenz (Anforderung 3 an den Datenschutz)** für den Bürger über erfolgte Datenaustausche hilfreich ist, um diesem in einer modernisierten Registerlandschaft Einsichtnahme und ggf. Kontrolle über die Verwendung der eigenen personenbezogenen Daten zu ermöglichen und das Vertrauen in die digitalisierte Verwaltung zu stärken.

II. Erfolgsfaktoren für die Umsetzung

a. Fokus auf den Nutzen für Bürger, Unternehmen und die Verwaltung

Oberste Priorität bei der Konzeption und Umsetzung der Registermodernisierung sollte der Nutzwert für Bürger, Unternehmen und die Verwaltung haben. Daher ist darauf zu achten, nutzerorientiert vorzugehen und die Architektur entsprechend zu gestalten, dass ein echter Mehrwert für die Nutzer eines solchen Systems entsteht. Für Bürger und Unternehmen ist bei der Abwicklung von Verwaltungsverfahren vorrangig eine Entlastung bei der Beibringung von Nachweisen maßgeblich. Für die Statistik soll die aufwands- und kostenintensive Erhebung von Daten entfallen und zugleich die erforderliche hohe die Qualität des Zensus sichergestellt werden. Für die Verwaltung soll der automatisierte Datenaustausch eine spürbare Verbesserung in der effizienten und effektiven Zusammenarbeit bewirken. Außerdem sollten geeignete Pilotvorhaben (einzelne OZG-Leistungen und Architekturkomponenten) identifiziert werden, die möglichst bereits vor Fertigstellung des Gesamtvorhabens in regional oder funktional eingeschränktem Rahmen gestartet werden können. Diese können zur Verdeutlichung der zu erwartenden Vorteile dienen und das modernisierte Architekturmodell einem ersten Praxistest unterziehen.

b. Inkrementelle Weiterentwicklung der Bestandsarchitektur

Die dezentral organisierte deutsche Registerlandschaft soll erhalten bleiben.[25] Für die zügige Umsetzung der Registermodernisierung ist die Weiternutzung der bestehenden, etablierten

[25] Eckpunkte zum registerübergreifenden Identitätsmanagement; Digitalkabinett (11.11.2019) als Teil der Registermodernisierung

Infrastruktur von Vorteil. Da sich in der Vergangenheit je Verwaltungsbereich unterschiedliche Kommunikations- und Datenstandards herausgebildet haben, ist von deren Fortbestand und einer Verbindung durch geeignete „Übersetzungsstellen“ (Gateways) auszugehen. Dadurch kann die Registermodernisierung schneller umgesetzt und die Unterstützung aller Akteure sichergestellt werden.

c. Zukunftssicherheit und Flexibilität für Anpassungen

Allgemein soll die Registermodernisierung auf dem Prinzip der Nachhaltigkeit entwickelt werden und nicht nur vorfallbezogene Lösungen bieten, sondern eine Gesamtbetrachtung und Harmonisierung der Anforderungen aus unterschiedlichen Sachverhalten ermöglichen.[26] Das bedeutet insbesondere, dass entwickelte technische Lösungen möglichst umfassend und wiederverwendbar gestaltet werden sollen; Arbeiten sollen produkt- und dienstleisterneutral erfolgen. Es wird sichergestellt, dass konzipierte Lösungen, konzeptionelle Ausarbeitungen und Vorbereitungen für alle Dienstleister in Bund und Ländern anschlussfähig und nachnutzbar sind. Die modernisierte Registerlandschaft sollte auch flexibel gestaltet sein, um unter anderem neue Register einzubinden, Austausche gemäß veränderten rechtlichen Grundlagen anders zu reglementieren und sich an die in Entwicklung befindlichen technischen Vorgaben seitens der EU anzupassen.

d. Berücksichtigung europäischer Vorgaben und Empfehlungen

Die europäische Kommission betreibt systematisch die Errichtung einer grenzüberschreitenden Vernetzung relevanter IT-Verfahren. Die Mitgliedsstaaten müssen die entsprechenden Verordnungen (beispielsweise zu elektronischen Rechnungen, zur Datenübermittlung zwischen den Trägern der Sozialversicherung oder zur Errichtung eines Single Digital Gateway) innerhalb der entsprechenden Fristen umsetzen. Die Kommission unterstützt die Mitgliedsstaaten durch das Europäische Interoperabilitätsrahmenwerk (EIF), die Bereitstellung von Infrastrukturkomponenten (CEF Building Blocks) sowie darauf aufbauende Projekte und Initiativen. Deren angemessene Berücksichtigung sichert nicht nur die Anschlussfähigkeit an die technischen Systeme der EU, sondern trägt auch zur Wirtschaftlichkeit der Umsetzung bei, und ist insoweit ein Erfolgsfaktor für die Registermodernisierung in Deutschland.

[26] Ergebnisprotokoll Workshop Koordinierungsprojekt September 2019, S. 28

4. Aktueller Stand der Diskussion und Lösungsskizze der Registermodernisierung

Nachfolgend werden die derzeit innerhalb des Koordinierungsprojektes diskutierten technischen, rechtlichen und organisatorischen Lösungsvorschläge hinsichtlich der genannten Anforderungen beschrieben. Die im weiteren Verlauf vorrangig zu klärenden Fragestellungen sind jeweils gesondert ausgewiesen. Zur vereinfachten Einordnung der benannten technischen Sachverhalte und Architekturkomponenten ist eine vorläufige Architekturskizze der Gesamtarchitektur als Fold-out beigefügt. Diese hat zum derzeitigen Stand der Diskussion jedoch illustrativen Charakter und soll insbesondere nicht den Lösungsraum zukünftiger technischer Diskussionen einschränken.

I. Stand der Diskussion zu den Anforderungen an das Identitäts- und Qualitätsmanagement

1. Eineindeutige Zuordnung von Datensätzen über Register hinweg

Um Datensätze verschiedener Register eineindeutig einander zuzuordnen, sollen ein oder mehrere registerübergreifende Identifier eingeführt werden. Dabei ist zu unterscheiden zwischen Personen- und Unternehmensidentifiern, deren Einführung jeweils aktuell vorbereitet wird.

Für die Einführung eines Personenidentifiers wird auf Bundesebene unter Federführung des BMI ein Gesetzentwurf abgestimmt, der die Nutzung der bereits existierenden Steuer-ID in den jeweiligen Fachregistern sowie Qualitätssicherungsmaßnahmen für die Basisdaten natürlicher Personen vorsieht.

Für die Schaffung eines Unternehmensidentifiers ist analog zum Personenidentifier die Einführung einer bundeseinheitlichen, „nicht sprechenden“ Wirtschaftsnummer geplant. Diese soll mit weiteren Basisdaten in einem „Basisregister für Unternehmensstammdaten“ gespeichert werden. Register mit Unternehmensbezug sollen mittels des gemeinsamen Identifiers untereinander und mit dem Basisregister Daten automatisiert austauschen können, insbesondere auch im Bereich der amtlichen Statistik (hier dürfen aufgrund des Rückspielverbots jedoch keine Daten aus der amtlichen Statistik in das Basisregister fließen). Dies wird auch die anfallenden Statistikpflichten reduzieren. Zusätzlich ist ein „Unternehmensportal“ als Frontend für digitale Verwaltungsleistungen geplant. Die Einbeziehung

von Personenunternehmen macht es erforderlich, den Unternehmensidentifier datenschutzrechtlich ebenfalls nach den Vorgaben der Datenschutz-Grundverordnung zu behandeln.[27]

Auf Grund der Schnittmengen zwischen den beiden Vorhaben strebt das Koordinierungsprojekt an, auf konzeptioneller und technischer Ebene erworbene Erkenntnisse zu koordinieren, um ein abgestimmtes und ggf. technisch harmonisiertes Vorgehen auch bei zeitlich unterschiedlichen Umsetzungen anzustreben.

Für den Registerzensus ist es erforderlich, Gebäude- und Wohnungsnummern einzuführen. Diese sollen über das Gebäude- und Wohnungsregister werden. Darüber hinaus unterstützen die Gebäude- und Wohnungsnummern die eindeutige Identifizierung von Gebäuden und Wohnungen.

Zu klärende Fragen: Für die Einführung eines oder mehrerer Personenidentifier wird eine politische Entscheidung im Gesetzesvorhaben zum registerübergreifenden Identitätsmanagement bezüglich des umzusetzenden Modells (zentrale oder bereichsspezifische ID, technische Vorkehrungen zur Datensicherheit) zeitnah angestrebt. Weiterhin wird für die weitere Ausgestaltung zu klären sein, ob und in welcher Art und Weise eine Authentifizierung bzw. Identifikation der Bürger (z.B. mittels eID) mit dem Identifier verbunden wird.

Sowohl für Personen- als auch Unternehmensidentifier wird zu klären sein, welche Zuständigkeiten hinsichtlich Daten- und Gestaltungshoheit vorliegen werden. Ebenso wird die Berücksichtigung des Datenschutzes entlang der weiteren Gestaltung erforderlich sein, besonders bezüglich der Frage, ob für den Unternehmensidentifier geringere datenschutzrechtliche Anforderungen bestehen. Zudem werden die Anforderungen und deren Umsetzung hinsichtlich der Interoperabilität der beiden Identifier zu prüfen sein. Bei der Entwicklung eines Unternehmensportals sollten mögliche Schnittstellen zum Portalverbund geprüft und genutzt werden.

[27] Ergebnisprotokoll Workshop Koordinierungsprojekt Dezember 2019, S. 29

2. Erkennung von Inkonsistenzen und aktives Qualitätsmanagement

Ein wichtiger Vorteil eines registerübergreifenden Identitätsmanagements wird es sein, deutlich einfacher als heutzutage Dateninkonsistenzen bei den personenbezogenen Basisdaten zwischen Fachregistern aufzudecken (etwa unterschiedliche Meldeadressen in Datensätzen zur gleichen Person) und eine entsprechende Korrektur zu koordinieren. Hierzu soll jeweils eine zentrale Stelle mit einem entsprechenden Qualitätssicherungsteam befähigt werden, solche Fälle nachzuverfolgen und die Korrektur fehlerhafter Einträge in den betroffenen Registern zu erwirken. Diese Aufgabe sollte durch eine Registermodernisierungsbehörde wahrgenommen werden.

Speziell für den Anwendungsfall Registerzensus besteht unter anderem Regelungsbedarf bezüglich der Zuordnung von Registereinträgen sowie der Nutzung des Personenidentifiers, sobald dieser eingeführt wurde (siehe Kapitel 3.I.a. und 4.I.1.). Damit der Registerzensus hochqualitativ durchgeführt werden kann, ist es wichtig, dass bestehende Zuordnungen sowie die Ergebnisse von Qualitätssicherungsmaßnahmen, z. B. in den Basisdaten zu Personen in einer modernisierten Registerlandschaft auch für die Zwecke der Statistik nutzbar gemacht werden können. Darüber hinaus muss der neue bzw. die neuen Personenidentifier in die erforderlichen Register eingeführt werden. Dabei ist sichergestellt, dass nur aggregierte Ergebnisse den Raum der Statistik verlassen dürfen. Ein weiteres Anliegen einer Neuregelung ist es, die Qualität der bestehenden Datenplattform des StBA zu technischen, rechtlichen und organisatorischen Informationen der relevanten Register – der Verwaltungsinformationsplattform (VIP) – durch eine Berichtspflicht seitens der registerführenden Stellen zu stärken (siehe Kapitel 4.III.3).

Zu klärende Fragen: Die Ausgestaltung der zentralen Qualitätssicherungsverfahren und das Zusammenspiel zwischen der verantwortlichen Stelle und den Fachregistern bedarf einer rechtlichen Regelung.

Neben der bisherigen Plattform VIP des StBA bzw. aufsetzend auf dieser wäre es für die Gesamtkonzeption von Vorteil, wenn die Informationen zusätzlich in maschinenlesbarer Form einer Architekturkomponente „Registerdatennavigation“ zugespielt werden (siehe Kapitel 4.III.3). Hinsichtlich der Durchführung eines Registerzensus ist zu beantworten, wo die beschriebene Informationsstelle im finalen Ausbauzustand verortet wird.

3. Anbindung an ein Identitätsmanagement der EU

Aus der SDG-VO ergibt sich unter anderem die Vorgabe, ausgewählte Verwaltungsleistungen EU-weit unter Beachtung des Grundsatzes der einmaligen Erfassung abzubilden. Zudem soll ein supranationales Identitätsmanagement eingeführt werden, welches die Verarbeitung von Personenidentifiern aus Mitgliedsstaaten erlaubt. Im Rahmen der Projekte TOOP (Fokus auf Unternehmen) sowie Once Only Principle (OOP) Blueprint[28] wird eine Referenzarchitektur und ggf. -implementierung erarbeitet, welche im Fortgang der Registermodernisierung technisch berücksichtigt werden sollte. Hierbei ist vorgesehen, dass auf nationaler Ebene ein eIDAS-Node einzurichten ist, der die technische Anbindung des Identitätsmanagements an Mitgliedsstaaten ermöglicht. Ein entsprechender Node wird bereits derzeit beim Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem ITZ Bund unter anderem zur Erfüllung der sich hinsichtlich der e-Rechnung[29] ergebenden Anforderungen aufgesetzt. Weiterhin sind ein oder mehrere eDelivery-Nodes einzurichten, die den eigentlichen Datenaustausch mit entsprechenden Nodes anderer Mitgliedsstaaten durchführen. Der Austausch zwischen eDelivery-Nodes erfolgt dabei nach dem 4-Corner-Prinzip. Weitere Komponenten sind auf EU-Ebene geplant (Criterion and Evidence Type Rule Base, Registry of Authorities, Data Service Directory, Semantic Mapping); für diese kann eine Zulieferung von Informationen erforderlich sein.

Zu klärende Fragen: Bisher noch nicht bekannt ist, in welcher Architektur die Anbindung an EU-weite Systeme erfolgen wird (z.B. Einrichtung einer „Kopfstelle", also eines eIDAS-Nodes und eines oder mehrerer eDelivery-Nodes). Bei der Entwicklung von Architekturkomponenten (siehe weitere Anforderungen) sollte jeweils geprüft werden, inwiefern diese auch EU-weit interoperabel gestaltet werden können bzw. müssen. Weiterhin ist die datenschutzgerechte Ausgestaltung deutscher Personenidentifier, die in den Mitgliedstaaten genutzt werden, festzulegen. Die Prüfung und ggf. die Nutzung bestehender Referenzimplementierungen seitens TOOP und OOP Blueprint sollten vorrangig erfolgen.

---

[28] OOP Technical System – Architecture Blueprint; Explanatory Note; 2020; Connecting Europe Facility

[29] In Zusammenhang mit Pan-European Public Procurement OnLine (PEPPOL); https://peppol.eu/

II. Stand der Diskussion zu den Anforderungen an den Datenaustausch

1. Aufbau von Schnittstellen und Definition von Standards

Die deutsche Verwaltungs- und Registerlandschaft ist stark heterogen geprägt. Konsolidierungen verwendeter Übertragungs- und Datenstandards fanden innerhalb einzelner „Verwaltungsbereiche“ statt (etwa OSCI/XÖV im Innenbereich, eXTra im Arbeits- und Sozialbereich), aber nur in begrenztem Maße über Verwaltungsbereiche hinweg. Bereiche technischer Ähnlichkeit entsprechen oftmals Ressortzuschnitten. Eine modernisierte Registerlandschaft sollte entweder harmonisierte Standards speziell für Datenabrufe einsetzen oder aber auf entsprechende Übersetzungsstellen (sog. „Gateways“) zurückgreifen, die für den Endnutzer (z.B. Fachverfahren, Bürgerportale) möglichst unsichtbar im Hintergrund agieren sollten. Eine domänenübergreifende Harmonisierung der Standards und anderer Interoperabilitätsmechanismen in den bestehenden Informationsverbünden für ganz Deutschland ist nicht realistisch, zudem würde bereits der Versuch eine deutlich verlängerte Umsetzungszeit des Gesamtvorhabens Registermodernisierung bedingen.

Daher basieren die konzeptionellen Arbeiten der UAG Architekturmodell darauf, dass eine Architekturkomponente konzeptioniert werden soll, die Abrufe seitens der anfragenden Stellen vereinheitlicht und die angefragten Register über die jeweils dort verwendeten Standards adressiert („Basiskomponente Registerabruf“). Die in Registern verwendeten Standards sollten hinsichtlich ihrer Eignung geprüft und ggf. aktualisiert werden.[30] Neben dem Abruf reiner Registerdaten soll zusätzlich ein Abruf von Nachweisen (z.B. Geburtsurkunde) möglich sein – dies sowohl in maschinenlesbarer Form (etwa als signiertes XML-Dokument) als auch als menschenlesbares Dokument (etwa als signiertes PDF/A-Dokument). Die Nutzung der beschriebenen Komponente wird derzeit hauptsächlich im Kontext des Anwendungsfalls 1, der digitalen „Once only“-Abwicklung von Verwaltungsleistungen, diskutiert, könnte jedoch Relevanz für andere Anwendungsfälle besitzen, insbesondere die Kommunikation zwischen Behörden und anderen Stellen (Anwendungsfall 3).

Für Neuentwicklungen innerhalb der Architektur, also auch ggf. neu aufzubauende Registersollten nach Möglichkeit bestehende Standards genutzt werden. Neben der Nutzbarkeit, einfachen Implementierung und der Zugänglichkeit zu den Daten und der

[30] Ergebnisprotokoll Workshop Koordinierungsprojekt Dezember 2019, S. 19

Dokumentation sollten ebenfalls die Zertifizierung, dauerhafte Pflegezuständigkeit und die Adaptierbarkeit für fachliche Spezifika gegeben sein. Eine Interoperabilität mit EU-weiten Standards sollte erklärtes Ziel der Neuentwicklungen und Erweiterungen sein. Übergreifend ist eine enge Abstimmung des Koordinierungsprojekts mit der KG Portalverbund, insbesondere deren AG Standards und Schnittstellen, sicherzustellen.

Zu klärende Fragen: Es wird eine Grundsatzentscheidung erfolgen müssen, ob eine Harmonisierung bestehender Standards oder eine Übersetzung dieser ineinander erfolgen soll. Dafür wird zu ermitteln sein, wie viele relevante Standards betrachtet werden, wie hoch die erwarteten Anpassungsaufwände und wie hoch das jeweilige Sicherheitsniveau zu bewerten ist. In jedem Fall muss eine Festlegung auf „Leitstandards" erfolgen, die z.B. neu entstehende Architekturkomponenten (siehe unten) als internen Standard nutzen. Diese Leitstandards würden dann entweder in allen Verwaltungsbereichen eingeführt oder alternativ würden mittels Gateways Übersetzungen aus dem Leitstandard in die lokal genutzten Standards ermöglicht. Hierbei ist zu identifizieren, inwiefern solche übersetzenden Bausteine (etwa die Basiskomponente Registerabruf) durch ihre zentrale Positionierung innerhalb vieler Datenflüsse nicht selbst zu einem datenschutzrechtlichen Risiko würden. Es wird zu erwägen sein, ob dezentrale Gateways direkt an den Fachregistern dieses Risiko vermindern können.

Wie vorangehend beschrieben, ist zu klären, ob sich die Nutzung der Komponente nur auf Datenabrufe im Rahmen der digitalen Antragstellung auf Verwaltungsleistungen beziehen soll oder ob die gleiche Funktionalität auch Abrufen seitens statistischer Stellen (Anwendungsfall 2) sowie Abrufen in der zwischenbehördlichen Kommunikation (Anwendungsfall 3) zugutekommen kann. Unklar ist bisher, ob die Entwicklung eines generischen (fachunabhängigen) Standards speziell für „Once-Only-Datenabrufe" sinnvoll ist, der sich auf eine automatisiert auswertbare „Registerlandkarte" von Verzeichnissen für Daten und Services abstützen kann. Weiterhin zu klären ist, ob und in welchem Ausmaß die Nutzung „dritter Stellen" als Intermediäre im Sinne des 4-Corner-Prinzips bei der Nutzung der Komponente erforderlich ist. Für die Basiskomponente Registerabruf und alle weiteren Komponenten ist zudem zu entscheiden, ob diese als eigenständige technische Lösungen entwickelt werden sollen oder ob eine Bündelung der jeweiligen Funktionalitäten im Rahmen einer gesamthaften technischen Implementierung oder eine Nutzung von Referenzimplementierungen im Rahmen von TOOP bzw. des OOP Blueprints möglich ist.

2. Ertüchtigung der verwendeten Transportwege

Für eine erhöhte Interoperabilität der bestehenden Register und elektronisch geführten Datenbanken wird die Infrastruktur des Datenaustauschs, also auch die Anbindung datenführender Stellen an das Verbindungsnetz stellenweise erweitert werden müssen. Ziel ist es, die Zugänglichkeit der vorhandenen Daten mit hoher Performance und großer zeitlicher Verfügbarkeit (minimale Ausfallzeiten) sicherzustellen. Der insofern vereinfachte Datenaustausch in einer modernisierten Registerlandschaft kann mit zusätzlichen Risiken einhergehen, die es zu adressieren gilt. Im Fall personenbezogener Daten ist mittels geeigneter technischer und organisatorischer Sicherungsmaßnahmen eine unzulässige Zusammenführung im Sinne einer Profilbildung wirksam zu unterbinden. Möglicherweise könnten bestehende Infrastrukturen, die dem so genannten 4-Corner-Prinzip folgen, eine Sicherungsmaßnahme darstellen[31]. Hier erfolgt eine logische Trennung zwischen Autor und Leser einer Datenübermittlung (Corner 1 und 4, meist Fachverfahren) von Sender und Empfänger (Corner 2 und 3, meist Intermediäre), die den eigentlichen Versand einer Datenübermittlung durchführen. Die Intermediäre können als dritte Stellen als neutrale Instanz das Vorliegen einer rechtlichen Grundlage der bereichsübergreifenden Übermittlung sicherstellen, z.B. unter Nutzung eines Verwaltungsdienstes (etwa Deutsches Verwaltungsdiensteverzeichnis (DVDV)), der eine „Wächterfunktion“ ausübt. Solche Infrastrukturen sind unter anderem schon in Teilen der Innenverwaltung, der Justiz sowie in den Bereichen Arbeit und Soziales vorhanden und auf europäischer Ebene bekannt.[32] Für eine Anbindung an einen sicheren europäischen Datenaustausch wird die Errichtung eines oder mehrerer eDelivery-Nodes erforderlich sein (siehe Kapitel 4.I.3), was ggf. durch eine Erweiterung bestehender Intermediäre gelöst werden könnte. Über die Sicherungsmaßnahmen hinaus ist die rechtskonforme physische Anbindung der einzelnen Akteure ggf. via Verbindungsnetz sicherzustellen.

Zu klärende Fragen: Der Kenntnisstand über die Verbreitung von Infrastrukturen, die dem 4-Corner-Prinzip folgen, in anderen Verwaltungsbereichen sowie über die ggf. erforderlichen Schritte zur Ertüchtigung dieser Verwaltungsbereiche ist zu erweitern. Die Anforderungen an die Anbindung an einen europaweiten Datenaustausch sollten geprüft werden, u.a. dahingehend, ob einer oder mehrere eDelivery-Nodes zu errichten sind und ob

---

[31] Eckpunktepapier zum Einsatz eines verfahrensübergreifenden Identifiers („4-Corner Modell“), KoSIT (10.01.2020)

[32] Z.B. OSCI, eXTra, PEPPOL

diese Erweiterungen von Intermediären oder Neuentwicklungen darstellen sollen. Außerdem ist zu prüfen, inwiefern Vorgaben seitens des Netzgesetzes (IT-NetzG) auf neu zu schaffenden Verbindungen innerhalb des Verbindungsnetzes bestehen.

3. Etablierung eines erweiterten Zugriffs- und Rechtemanagements

Wie in den Anforderungen in Kapitel 3 beschrieben, sind für ein Zugriffs- und Rechtemanagement für Datenaustausche selbst, aber auch für den Zugriff auf ein solches System drei Aspekte relevant, die gesondert beschrieben werden:

1. **Datenaustausch auf bestehenden Rechtsgrundlagen.** Zu errichtende steuernde Stellen, z.B. Intermediäre im 4-Corner-Prinzip, müssen anhand von Zugriffslisten und / oder Informationen der Public-Key Infrastrukturen automatisiert Datenaustausche bei vorhandener rechtlicher Grundlage technisch zulassen oder bei fehlender rechtlicher Grundlage abbrechen. Grundlage der Entscheidung sollen die der Behörde eingeräumten Befugnisse sein, d. h. insbesondere die Frage, ob ein Datenabruf der abrufenden Behörde generell von der Befugnis gedeckt ist. Die Pflege solcher Listen bzw. der PKI muss in der Hoheit einiger weniger oder nur einer autorisierten Stelle liegen, die Schreibzugriff besitzt. Änderungen der Listen werden dann erforderlich, wenn sich gesetzliche Rahmenbedingungen ändern. Eine solche Struktur liegt mit dem DVDV in Version 2 bereits vor, wodurch sich eine Weiternutzung anbietet. Da das Zugriffsmanagement aber nicht im Fokus der bisherigen Entwicklung des DVDV stand, ist davon auszugehen, dass weitere Anpassungen erforderlich sein werden.

   Es ist zu erwarten, dass in einer modernisierten Registerlandschaft Datenaustausche zwischen deutlich mehr beteiligten Akteuren stattfinden werden, als dies heute der Fall ist. Somit stellt sich aus rechtlicher Sicht die Frage, in welcher Detailtiefe diese Austausche jeweils gesetzlich geregelt werden müssen – d.h. jeweils unter Angabe der beteiligten Stellen sowie exakter Nennung der ausgetauschten Datenfelder. Die Möglichkeit einer einfacheren und flexibleren Lösung im Rahmen einer übergreifenden gesetzlichen Regelung, die die Grundprinzipien solcher Austausche bestimmt und aus der sich die Berechtigung im Einzelfall ableitet sollte diskutiert werden.

2. **Datenaustausche zum Abruf von Inhaltsdaten oder Nachweisen bei Online-Verwaltungsleistungsanträgen mit Einwilligung des Bürgers**. In einer modernisierten Registerlandschaft sind zusätzlich zu heute schon technisch möglichen und rechtlich reglementierten Abrufen viele weitere Abrufe denkbar und sinnvoll. Für all diejenigen Abrufe, die im Interesse des Bürgers vorgenommen werden, um ihm nur eine einmalige

Erfassung der entsprechenden Daten zu ermöglichen, wird es zusätzlich nötig sein, die Einwilligung des Bürgers einzuholen und nachvollziehbar zu protokollieren. Nur mit erfolgter Einwilligung dürften solche Abrufe zu Stande kommen. Zu diesem Zweck wird aktuell diskutiert, eine weitere Architekturkomponente, das Consent-Modul, zu entwickeln. Hierüber können Einwilligungen erteilt (und diese ggf. zeitlich beschränkt) werden; das Consent-Modul speichert sie und macht sie maschinenlesbar und verschlüsselt abrufbar (etwa als signiertes XML-Dokument). Eine zusätzliche Funktionalität soll darin bestehen, einen „Consent-Dialog" bereitzustellen: ein in einen digitalen Antrag auf Verwaltungsleistungen eingebundenes Formular in standardisierter Form, welches etwa aufzeigt, welche Register für welche Datenfelder angefragt werden sollen und dem Nutzer z.B. durch Markierung von „Checkboxen" die Abgabe der Zustimmungen ermöglicht. Ebenso sollte eine Einsicht des Bürgers in die erteilten Einwilligungen möglich sein, inklusive einer Möglichkeit, diese zu verändern oder zu widerrufen. Die Nutzung der beschriebenen Komponente wird derzeit hauptsächlich im Kontext des Anwendungsfalls 1, der digitalen „Once-only"-Abwicklung von Verwaltungsleistungen, diskutiert, könnte jedoch Relevanz für weitere Anwendungsfälle besitzen.

3. **Identifizierung und Authentifizierung im System.** Das OZG gibt mit den in § 3 Absatz 2 geregelten Nutzerkonten bereits eine Lösung für die elektronische Identifizierung und Authentifizierung vor, die in Entsprechung des Konzepts der eIDAS-Verordnung je nach Sensibilität der betreffenden Daten verschiedene Sicherheitsniveaus für den Nachweis der Identität vorschreibt (vgl. auch § 8 Satz 1 OGZ). Die Spannbreite reicht vom einfachen Login mit einem Benutzernamen und einem Passwort (Sicherheitsniveau „niedrig"), über die geplante Nutzung von z.B. ELSTER-Zertifikaten (Sicherheitsniveau „substantiell") bis hin zur eID-Funktion des neuen Personalausweises, des elektronischen Aufenthaltstitels oder der eID-Karte (Sicherheitsniveau „hoch"). Bei entsprechendem Sicherheitsniveau der Authentifizierung kann in einer modernisierten Registerlandschaft die eineindeutige Zuordnung des sich über ein Nutzerkonto authentifizierenden Nutzers zu einem Personen- oder Unternehmensidentifier gewährleistet werden. Bei der Beantragung von Unternehmensleistungen (sowie analog für weitere Organisationen, etwa Vereine) ist sicherzustellen, dass diese nur durch berechtigte authentifizierte Mitarbeiter erfolgen.

Zu klärende Fragen: Offene Fragen bezüglich dieser Anforderung bestehen vornehmlich bezüglich zwei der dargestellten Aspekte:

1. **Datenaustausch auf bestehenden Rechtsgrundlagen.** Zu klären ist im Falle der Nutzung des DVDV als steuernde Stelle für Zugriffsrechte, inwiefern die existierende Architektur erweitert werden muss, um den erhöhten Anforderungen einer modernisierten Registerlandschaft zu genügen. Grundsätzlich ist zu entscheiden, ob ein ertüchtigtes DVDV das Zugriffs- und Rechtemanagement für alle Verwaltungsbereiche vermitteln soll oder ob weitere technische Lösungen für andere Bereiche (weiter)entwickelt werden sollen. Hierfür ist zu ermitteln, in welcher Form und in welcher Komplexität andere Verwaltungsbereiche bereits eigene Lösungen für ein Zugriffs- und Rechtemanagement betreiben. Ebenfalls wird zu klären sein, in welcher Hoheit der Schreibzugriff auf die erwähnten Zugriffslisten liegen wird.

   Aus rechtlicher Sicht ist vorab die prinzipielle Möglichkeit einer gesamthaften gesetzlichen Regelung erlaubter Datenaustausche zu prüfen. Falls diese besteht, sollte eine nachfolgende Analyse der voraussichtlichen Zahl und Detailtiefe zu regelnder zukünftiger Austausche anschließen, um abzuschätzen, inwiefern eine solche Regelung Zeit, Kosten und Komplexität in der weiteren Gesetzgebung einsparen kann und wie mit den bestehenden rechtlichen Regelungen umgegangen werden soll. Außerdem muss in diesem Fall eine Konzeption zugrunde zu legender Grundprinzipien erfolgen, die hinreichend flexibel gegenüber zukünftigen Anwendungsfällen sind und gleichzeitig eine hohe Sicherheit gegenüber Datenmissbrauch und unzulässiger Profilbildung von Bürgern garantieren. Vor allem müssen die Erfordernisse des Datenschutzrechts eingehalten werden; dies ist umfassend zu prüfen.

2. **Identifizierung und Authentifizierung im System.** Es stellen sich insbesondere folgende Kernfragen:

   - Wie kann zwischen den Identitäts-/Stammdaten, die über Nutzerkonten aus einem elektronischen Identifizierungsmittel übermittelt werden, und dem zu einem Nutzer (privat handelnde natürliche Person oder Unternehmen) gehörenden Personen- oder Unternehmensidentifier eine eineindeutige Verbindung hergestellt werden? Die aktuellen Planungen des BMI sehen nicht vor, dass der Personenidentifier bis an den Nutzer herangetragen wird, also etwa auf dem Personalausweis zu speichern ist, um den ausgestalteten Personenidentifier von einer problematischen vollwertigen Personenkennziffer abzugrenzen. Somit ist zu klären, ob und wie eine automatisierte Zuordnung des Nutzerkontos zum Identifier zuverlässig ermöglicht werden kann und ob diese

Zuordnung ggf. auf Grund datenschutzrechtlicher Erfordernisse nur temporär bestehen darf.

- Was ist bei der Identifikation und Authentifikation EU-ausländischer Personen und Unternehmen zu beachten?

III. Stand der Diskussion zu den Anforderungen an die Datenhaltung

Die vollständige, hochqualitative und sparsame Datenhaltung in Registern und elektronisch geführten Datenbanken ist ein relevanter Aspekt für das Gelingen des Gesamtvorhabens der Registermodernisierung. Allerdings obliegt die Erfüllung dieser Anforderungen den datenhaltenden Behörden selbst. Das Koordinierungsprojekt Registermodernisierung kann diese unterstützen, indem es Anforderungen zur Datenhaltung spezifiziert, Vorschläge für verbesserte Nutzungsmöglichkeiten für bereits in der Verwaltung vorhandenen Daten erarbeitet und ggf. übergreifende technische Lösungen konzipiert und betreut.

1. Einzubindende Register und Erweiterung der Registerlandschaft, um alle benötigten Daten vorzuhalten

Für eine möglichst breite Abdeckung der genannten Anwendungsfälle sollten Register und elektronisch geführte Datenbanken möglichst umfassend Teil der Registermodernisierung sein, d.h. insofern ertüchtigt, um eineindeutig und automatisiert mit anderen Akteuren in der vorzusehenden IT-Infrastruktur kommunizieren zu können. Hierzu muss spezifiziert werden, welche technischen Anforderungen an „moderne Register" bestehen und welche vorrangig modernisiert werden sollen. In einer ersten Aufwandsschätzung für ein registerübergreifendes Identitätsmanagement wurden – mit dem Fokus auf Personendaten – 26 Registertypen als vorrangig für eine Modernisierung bzw. Einbindung in eine modernisierte Registerlandschaft erachtet. Basis der zugrundeliegenden Analyse bildeten dabei die „Top 10"-Register aus dem entsprechenden Gutachten des NKR[33], für den Registerzensus erforderliche Register sowie für bereits hinsichtlich erforderlicher Registerschnittstellen untersuchte OZG-Leistungen erforderliche Register (zum Abruf vorhandener Daten gemäß „once only"). Eine deutlich erweiterte und detailliertere Vorgehensweise, z.B. hinsichtlich unternehmensrelevanter Register, kann die Basis für das Gesamtvorhaben der Registermodernisierung liefern. Im Einzelfall sollte jedoch abgewogen werden, ob der Nutzen eine ggf. kosten- und zeitintensive Ertüchtigung rechtfertigt, insbesondere bei Registern, die nur mit wenigen Stellen in Kontakt treten oder Einträge gewöhnlich nicht aktualisieren.

Aktuell liegen für den Registerzensus nicht alle benötigten Daten bereits in Registern oder elektronisch geführten Datenbanken vor. Derzeit fehlen ein Gebäude- und Wohnungs-

[33] NKR: „Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren." (Oktober 2017)

register sowie ein statistisches Bildungsregister, die für die Durchführung eines Registerzensus benötigt werden.[34] Für die Errichtung solcher Register können wiederum weitere Datenquellen benötigt werden, etwa von Schulträgern für ein zu schaffendes Bildungsregister. Eine Einbindung von Geodaten ist insbesondere für die jährliche geokodierte Gewinnung der Bevölkerungszahlen ab 2024 erforderlich, wofür das statistische Anschriftenregister nach § 13 Absatz 2 Bundesstatistikgesetz weiterentwickelt wird. Zur Ermöglichung georeferenzierender Verwaltungsleistungen wurde die GDI-DE[35] als zentrale Geokomponente geschaffen, die die weitere Harmonisierung in diesem Bereich vorantreibt.

Zu klärende Fragen: Eine abgestimmte Sicht auf die kurz-, mittel- und langfristig anzubindenden Register im Rahmen der Registermodernisierung sollte vorrangig erarbeitet werden. Die getroffene Auswahl wird starken Einfluss darauf haben, wie lange die Registermodernisierung insgesamt andauern wird und wie viele Kommunikations- und Datenstandards zu betrachten sind. Die Erstellung einer detaillierten Übersicht über vorhandene Register und elektronisch geführte Datenbanken, inklusive vorhandener technischer Gegebenheiten (unter anderem verwendete Fachverfahren), ist hierfür als Grundlage anzusehen. Zudem gilt es, Transparenz darüber herzustellen, welche relevanten Daten insbesondere für den Registerzensus noch nicht in Registerform vorliegen, so dass ein Aufbau solcher Register erwogen werden kann. Ebenso wird zu klären sein, welche z.B. kommunalen Nutzer einer modernisierten Registerlandschaft und ggf. weitere Dritte betrachtet werden müssen und in welcher Form Anpassungen bei diesen erforderlich werden.

2. Sicherstellung der Qualität der Datensätze

Um sicherzustellen, dass die in den Registern hinterlegten personenbezogenen Basisdaten stets hochqualitativ sind (frei von Dubletten und Schreibfehlern sowie Adresse, Geburtsdatum etc. auf aktuellem Stand) und Über- und Untererfassungen zu bereinigen, ist einerseits vorgesehen, Qualitätssicherungsprozesse in der basisdatenregisterführenden Stelle einzurichten, die auf Korrekturen in Kontakt mit den registerführenden Stellen hinwirkt und andererseits eine perspektivische Löschung der dezentral gespeicherten personenbezogenen Basisdaten anstrebt, um diese durch die im Basisdatenregister

[34] Quelle: Ergebnisprotokoll Workshop Koordinierungsprojekt September 2019, S. 22, „Anforderungen an Registermodernisierung“

[35] GDI-DE: Eckpunktepapier zur Berücksichtigung von Geodaten und Geodateninfrastrukturen bei der Umsetzung des Onlinezugangsgesetzes (OZG), 14.02.2020

vorhandenen Datenfelder zu ersetzen. Dieses zentrale Qualitätsmanagement ist in Kapitel 4.I.2 detailliert beschrieben, wohingegen sich dieser Abschnitt mit entsprechenden Aufgaben der registerführenden Stellen selbst befasst. Die Abgleiche sollten weitestgehend automatisiert erfolgen können.

Zu klärende Fragen: Zur Sicherstellung der Qualität der Datensätze bedarf es einer Regelung, welche Stelle im Verlauf einer Datenkorrektur die Datenhoheit übernimmt (siehe Kapitel 4.I.2). Weiterhin ist zu prüfen, ob die vorhandenen Ressourcen für diese Aufgabe bei allen registerführenden Stellen ausreichend dimensioniert sind.

3. Datenminimierung

Zum einen die zentrale Speicherung von **Basisdaten**, zum anderen die Schaffung einer Architekturkomponente „**Registerdatennavigation**“, die als maschinenlesbare Landkarte für Registerdaten dienen soll. Beide Bausteine können es mittelfristig ermöglichen, „Leitregister“ je Datenfeld zu definieren und eine **Bereinigung** der jeweiligen mehrfach vorgehaltenen Daten in anderen Registern durchzuführen. Hierbei kann ein **Fallbeispiel** aus der Überarbeitung des Datenaustauschs beim AZR als Referenz dienen. Die genannten Themen werden im Folgenden detailliert beschrieben.

1. Die Speicherung von **Basisdaten** (z.B. Meldeadresse, Geburtsdatum und -ort) an einer zentralen Anfragestelle könnte einen Großteil der Datenaustausche – die sich meist ausschließlich auf solche Basisdaten beziehen – vereinfachen. Außerdem könnte diese Stelle einfacher als bisher eine koordinierende und leitende Rolle bei der Verbesserung der Datenqualität einnehmen (siehe oben). Die Steuer-ID-Datenbank der BZSt betreibt bereits heute eine ähnliche zentrale Basisdatenspeicherung, ist allerdings nur für rechtlich eng begrenzte Zwecke nutzbar. In einer modernisierten Registerlandschaft hätte ggf. jede Stelle mit Bedarf an Personendaten Zugriff auf diese Basisdaten.

   Auch für Unternehmensdaten soll ein „Stammregister“ eingeführt werden, welches sich aus mehreren Quellregistern speist und eine zentrale Vorhaltung relevanter Daten ermöglicht. Bei der nun beginnenden Konzeption und Umsetzung kann eine Abstimmung mit laufenden Entwicklungen bei der zentralen Haltung von Personenbasisdaten förderlich sein.

Zu klärende Fragen: Bei der Entwicklung eines „Stammregisters“ für Unternehmensdaten ist zu erwägen, inwiefern eine konzeptionelle und technische Harmonisierung mit Entwicklungen einer solchen zentralen Stelle für Personenbasisdaten hilfreich und möglich ist.

2. In der bisherigen Diskussion wurde deutlich, dass es einer zentralen Datenbank als Navigator in der Registerlandschaft („Modul **Registerdatennavigation**“) bedarf. Ein solches Modul sollte auf der bestehenden Datenbasis des VIP des StBA (siehe rechtliche Anforderung) aufbauen und um ein maschinenlesbares Format erweitern. Nach Möglichkeit sollen Empfehlungen der EU-Kommission für die Beschreibung von Datenkatalogen berücksichtigt werden. Eine rechtliche Regelung innerhalb des Bundesstatistikgesetzes für eine VIP für Statistikzwecke wird aktuell erarbeitet, wird aber im bisherigen Planungsrahmen nicht allein die Aufgaben des Moduls erfüllen können. Das StBA entwickelt derzeit aufbauend auf den bestehenden Prototypen die Pilotanwendung einer öffentlich zugänglichen webbasierten Plattform. Der zunächst für Zwecke der amtlichen Statistik entwickelte Pilot soll bereits im ersten Quartal 2021 zur Verfügung stehen. Im Sinne einer nachhaltigen Pflege sollen Verwaltungsstellen des Bundes und die nach Landesrecht für die Wahrnehmung der Aufgaben der öffentlichen Verwaltung zuständigen Stellen auf Anforderung Angaben über Herkunft, Struktur, Inhalt und andere Metadaten übermitteln. Nach den Vorgaben der BLAG zur Reduzierung von Statistikpflichten ist sie bewusst offen gehalten für den Ausbau zu einem übergreifenden Datenkatalog der öffentlichen Verwaltung (DaKa). Die Entwicklung eines über Statistikzwecke hinausgehenden Moduls sollte in jedem Fall eng abgestimmt mit dem Vorhaben des StBA erfolgen. Die Leitfrage hinter der Nutzung des Moduls Registerdatennavigation ist: „In welchem Register finde ich welche Daten originär?“. Da bei Abfragen der Registerdatennavigation keinerlei Inhalts-, sondern nur Metadaten verwendet werden und insbesondere kein Personenbezug nötig sein wird, kann das Modul vermutlich ohne oder mit relativ einfachen Zugangsbeschränkungen umgesetzt werden. Die beschriebene Datenbank kann vermutlich auch die Anforderungen erfüllen, die seitens BLAG zur Reduzierung von Statistikpflichten im Unternehmensbereich aufgestellt wurden. Daher ist ein koordiniertes Vorgehen bei der Entwicklung anzuraten. Ziel kann es sein, beide Vorhaben mittels derselben Datenbank zu erfüllen.

Zu klärende Fragen: Die Konzeption des Moduls Registerdatennavigation hat erst begonnen. In Bezug auf die laufende Weiterentwicklung der VIP des StBA ist zunächst zu klären, inwiefern die für die amtliche Statistik etablierte Plattform als Grundlage dienen und erweitert werden kann. Es ist in der Konzeption der Architektur zur Registermodernisierung noch nicht entschieden, nach welchem Kommunikations- und Datenstandard Abrufe bei diesem Modul gestaltet werden. Informationen über die für bestimmte Daten originär zuständigen Behörden müssen in verwaltungsöffentlichen Verzeichnisdiensten analog dem DVDV für Dienste veröffentlicht werden, um einen möglichst einfachen Zugang zu den Daten für alle berechtigten Behörden sicherzustellen. Ebenso ist noch nicht entschieden, in welcher Zuständigkeit und welcher technischen Umsetzung inklusive Sicherheitsstandards das Modul entwickelt werden soll. Die Zusammenfassung mit einer oder mehreren anderen in der Entwicklung befindlichen Komponenten sollte geprüft werden. Zudem ist zu erarbeiten, ob die Nutzung des Moduls mittelfristig verpflichtend werden soll, was ein wichtiger Schritt zur Bereinigung von Registern hinsichtlich doppelt vorgehaltener Daten sein kann (siehe unten). Außerdem sind die Anforderungen seitens Personen- und Unternehmensdaten miteinander abzugleichen und hinsichtlich einer gemeinsamen Entwicklung des Moduls Registerdatennavigation zu prüfen.

3. Bei vorhandener zentraler Vorhaltung von Basisdaten sowie einer funktionsfähigen Architekturkomponente Registerdatennavigation wird grundsätzlich eine **Bereinigung** von Registern und elektronisch geführten Datenbanken möglich. Hierbei müsste im Detail untersucht werden, welche Daten sich für eine Bereinigung eignen. So könnten z.B. alle Daten, die zur Kontaktaufnahme mit Bürgern benötigt werden (z.B. Name, Anschrift), als nicht bereinigungsfähig angesehen werden. Die Möglichkeit einer Bereinigung würde außerdem stark davon abhängen, inwiefern Zwischenspeicherung von Daten technisch und rechtlich möglich bleibt bzw. ob auf eine Zwischenspeicherung bei hinreichend verfügbaren und schnellen Datenübertragungskanälen verzichtet werden kann.

4. Die kürzlich abgeschlossene Überarbeitung des Datenaustauschs zu aufenthalts- und asylrechtlichen Zwecken kann als **Fallbeispiel**[36] genannt werden. Rechtliche

[36] Bericht der Steuerungsgruppe XInneres zu Auswirkungen der Digitalisierung des Ausländerwesens auf XInneres (Stand: 28.02.2017)

und technische Veränderungen wurden untersucht, um zu beurteilen, wie eine Integration von Daten aus dem Kerndatensystem des AZR in das Informationssystem der Innenverwaltung gelingen kann. Ziel war es, eine verlässliche Datenübermittlung der benötigten Daten sicherzustellen und gleichzeitig die rechtlichen, organisatorischen und technischen Voraussetzungen zu schaffen, um Ländern und Kommunen effizientes Handeln durch konsistente Daten zu ermöglichen. Bei einer von der Projektgruppe zur Digitalisierung des Asylverfahrens (PG DAS) entwickelten Lösung findet auf konzeptioneller Ebene keine redundante Datenhaltung statt. Im Bedarfsfall wird das Datum der letzten Veränderung im AZR erfragt; nur bei Änderungen werden Daten übermittelt. Dieses Verfahren nutzt die temporäre Vorhaltung von Daten (Caching), um den zügigen Abruf sicherzustellen. Es gewährleistet sowohl die Qualität als auch die Aktualität, z.B. für statistische Auswertungen, Berichte, Prognosen und Controlling. Es verwirklicht allerdings (noch) nicht die tatsächliche Löschung redundanter Daten.

IV. Stand der Diskussion zu den Anforderungen an die Datensicherheit

1. Errichtung geeigneter Sicherungsmaßnahmen

In einer modernisierten Registerlandschaft muss sichergestellt sein, dass keine unzulässige Profilbildung erfolgen kann und dass eine sichere Übertragung aller Daten gegeben ist. Dazu sind zusätzliche Sicherungsmaßnahmen vorgesehen, wie z.B. die Datenübermittlung zwischen verschiedenen Verwaltungsbereichen über das 4-Corner-Prinzip. Die Funktionsweise ist oben bereits beschrieben.

Zu klärende Fragen: Die konzeptionellen Vorschläge zu möglichen Sicherungsmaßnahmen sind weiter auszuarbeiten und aus verfassungs- und datenschutzrechtlicher Sicht zu bewerten. Diese Einschätzung ist im Nachgang entsprechend in die weitere Ausgestaltung der Architektur einzubinden. Außerdem ist zu klären, wie die Implementierung der Sicherungsmaßnahmen und deren Kontrolle wahrgenommen werden soll, z.B. der Intermediäre und ob neu einzurichtende Architekturkomponenten ebenfalls an ein 4-Corner-Prinzip oder an andere Sicherungsmaßnahmen angebunden werden und wie dies technisch ausgestaltet werden kann.

2. Sicherstellung der Nachvollziehbarkeit (z.B. mittels Protokollierung)

Um die Rechtmäßigkeit und Verhältnismäßigkeit erfolgter Datenaustausche zuverlässig zu kontrollieren ist geplant, die durchgeführten Datenaustausche nachvollziehbar zu protokollieren und bei Verwaltungsverfahren den Bürgern in einem speziellen Onlinedienst, dem Datencockpit, zur Einsichtnahme zur Verfügung zu stellen. Die Protokollierung müsste derart erfolgen, dass nachprüfbar ist, welche Stellen wann zu welchem Zweck mit wem welche Daten ausgetauscht haben. In jedem Fall müssen die relevanten Metadaten einer Kommunikation erfasst werden, d.h., wer (anfragende Stelle) mit wem (angefragte Stelle) wann (Zeitstempel) und zu welchem Zweck (rechtliche Grundlage) über wen oder was (Identifier von Personen oder Unternehmen) Daten ausgetauscht hat. Die derzeitige Infrastruktur beinhaltet bereits eine Protokollierung an mehreren Stellen, nämlich bei beteiligten Fachverfahren, Intermediären, Clearing-Stellen, Verzeichnisdiensten und Registern selbst. Diese müssten aber harmonisiert und ggf. technisch ertüchtigt werden, um den hohen Ansprüchen an Datenaustausche in einer modernisierten Registerlandschaft gerecht zu werden. In den aktuellen, dem 4-Corner-Prinzip folgenden Systemen haben die transportierenden Stellen i.d.R. (Intermediären und Clearing-Stellen) keine Kenntnis über den Inhalt oder die betreffenden Personen des Datenaustauschs. Sie müssten gegebenenfalls dahingehend angepasst werden, die verwendeten Identifier als Metadaten zu klassifizieren.

Zu klärende Fragen: Es wird zu entscheiden sein, welche Datenfelder minimal an welchen Stellen in welcher Form protokolliert werden müssen. Des Weiteren ist zu klären, ob über die Metadaten hinaus auch die fachlichen Inhaltsdaten eines solchen Austauschs protokolliert werden müssen. Relevant ist in diesem Kontext eine Entscheidung darüber, ob die verwendeten Identifier in einem Datenaustausch als Metadaten klassifiziert werden können. Dies bedingt das Ausmaß der zu beteiligenden protokollierenden Stellen (siehe oben). Generell muss geprüft werden, ob der Transparenzgewinn durch das Datencockpit den Verlust an Datensicherheit bei der Offenlegung von Metadaten bei solchen Stellen rechtfertigt, die bisher keine Kenntnis von diesen Daten hatten.

3. Aufbau von Transparenz (z.B. mittels Datencockpit)

Für eine dem Bürger zugängliche Einsichtnahme in solche Protokolle (siehe oben) wird im Rahmen der OZG-Umsetzung ein Datencockpit konzipiert. Dieser als sog. „Digitalisierungslabor“ unter Einbindung von Nutzern sowie Datenschützern aus Bund und Ländern gemeinsam erarbeitete Dienst soll erfolgte Datenaustausche für den Nutzer

transparent machen. Nach dem Stand der Abstimmung soll das Datencockpit den Nutzer darüber Auskunft geben können, welche Datenaustausche im Rahmen von Verwaltungsverfahren zu seiner Person stattgefunden haben sowie welche Daten über ihn in einzelnen Registern gespeichert sind. In Klärung ist momentan noch, in welchem Umfang das Datencockpit zur Bereitstellung dieser Funktionen selbst Daten speichern muss. Diskutiert werden hier das sog. Quellenmodell (das Datencockpit ist nach dem Login immer leer, alle Informationen zu Datenaustauschen werden aus allen in Frage kommenden dezentralen Registern als „Quellen" immer wieder neu angefragt und nach der Sitzung gelöscht) und das sog. Mischmodell (das Datencockpit speichert zumindest minimale Metadaten über die erfolgen Datenaustausche – z.B. bereitstellendes Register und Zeitpunkt - so dass weitere Informationen gezielt dort für die Sitzung nachgeladen werden können). Um eine gemeinsame Entscheidung hierzu herbeizuführen, werden im nächsten Schritt beide Modelle im Hinblick auf Nutzerorientierung, technische Machbarkeit sowie (datenschutz-)rechtliche Bewertung gegenübergestellt. Begleitend hierzu wird gegenwärtig die Referenzimplementierung des Datencockpits in gemeinsamer Federführung von Bremen und Bund/BMI geplant. Als erste Anwendungsfälle sollen hier die zur Umsetzung der Lebenslage „Geburt" aus dem ELFE-Projekt geplanten Datenaustausche prototypisch umgesetzt werden und so – der bisherigen agilen Arbeitsweise folgend – die konzeptionellen Festlegungen zum Datencockpit validiert und ggf. fortgeschrieben werden.

Zu klärende Fragen: Für die Entwicklung und Anbindung des Datencockpits ist zu klären, welche Daten (z.B. nur Metadaten und wenn ja, welche Metadaten) angezeigt werden. Bei Nutzung eines Zwischenspeichers für Austausche im Datencockpit ist zu vermeiden, dass dieser selbst zu einem Datenschutzrisiko wird, da in ihm zumindest Metadaten aus unterschiedlichen Verwaltungsbereichen zusammenlaufen würden. Dies ist als übergreifendes Spannungsfeld zu betrachten, da ein Einbruch ins Datencockpit zu einer Profilbildung führen könnte. Weiterhin ist zu entscheiden, ob auch Inhaltsdaten per Anfrage im Datencockpit abgerufen werden können und ob diese in das Datencockpit geliefert oder dem Bürger auf separatem Weg zugestellt würden. Ebenso ist zu spezifizieren, welche Anwendungsfälle ein Datencockpit umfassen soll.

V. Tabellarische Übersicht über den aktuellen Diskussionsstand und zu klärende Fragen je Anforderung

Tabelle 1: Übersicht über den bisherigen Diskussionsstand und zu klärende Fragen je Anforderung

Stand der Diskussion zu den Anforderungen an das Identitäts- und Qualitätsmanagement

	Bisheriger Diskussionsstand	Fragen, die noch zu klären sind
Eineindeutige Zuordnung von Datensätzen über Register hinweg	▪ Es wird Personen- und Unternehmensidentifier geben ▪ Unternehmensidentifier mit „nicht sprechender" Wirtschaftsnummer geplant ▪ Einführung von Gebäude- und Wohnungsnummern für Registerzensus erforderlich ▪ Koordinierung der Erkenntnisse angestrebt	▪ Entscheidung zur weiteren Ausgestaltung des Personenidentifiers ▪ Wie wird die Identifikation für den Personenidentifier gestaltet? ▪ Welche Zuständigkeiten bestehen hinsichtlich Daten- und Gestaltungshoheit? ▪ Wie wird der Datenschutz berücksichtigt? ▪ Kann das Unternehmensportal von Synergien zum Portalverbund profitieren?
Erkennung von Inkonsistenzen und aktives Qualitätsmanagement	▪ Zentrale Stelle soll mit Qualitätssicherungsteam ausgestattet werden ▪ Dieses soll Dateninkonsistenzen zwischen Fachregistern aufdecken ▪ Statistikgeheimnis bleibt in Kraft ▪ Qualität der Verwaltungsdatenplattform soll durch technische Befähigung und Berichtspflicht registerführender Stellen steigen ▪ Registerzensusvorbereitungsgesetz (geokodierte Bevölkerungszahlen) bis Ende 2020 vorgesehen	▪ Rechtliche Regelung des Qualitätssicherungsteams und des Qualitätsprozesses ▪ Verortung einer zentralen Informationsstelle zu klären
Anbindung an ein Identitätsmanagement der EU	▪ Ausgewählte Verwaltungsleistungen sollen EU-weit „once only" abgebildet werden ▪ Supranationales Identitätsmanagement soll gewährleistet werden ▪ Technisch wird ein eIDAS-Node einzurichten sein sowie ein oder mehrere eDelivery-Nodes ▪ Mögliche Zulieferung von Informationen an weitere Komponenten auf EU-Ebene	▪ Welche Anforderungen der Interoperabilität bestehen zu EU-weiten Systemen und wie werden diese adressiert? ▪ Wie wird die technische Ausgestaltung der Anbindung an EU-weite Systeme erfolgen (z.B. „Kopfstelle")? ▪ Was ist datenschutzrechtlich bei Nutzung des Personenidentifiers in Mitgliedsstaaten zu beachten?

Stand der Diskussion zu den Anforderungen an den Datenaustausch

	Bisheriger Diskussionsstand	Fragen, die noch zu klären sind
Aufbau von Schnittstellen und Definition von Standards	▪ Verwaltungslandschaft innerhalb einzelner Verwaltungsbereiche mit relativ harmonisierten Schnittstellen, allerdings nur begrenzte Harmonisierung zwischen Bereichen ▪ Entweder vereinheitlichte Standards oder Übersetzungsstellen notwendig ▪ Zentrale Architekturkomponente geplant („Basiskomponente Registerabruf") ▪ XFall, ein XÖV-konformer Standard, als Kommunikationsstandard zur Komponente geplant	▪ Wird eine Harmonisierung bestehender Standards oder eine Übersetzung zwischen Standards erfolgen? ▪ Welcher Standard ist ggf. der „Leitstandard"? ▪ Welche Anwendungsfälle werden durch die Basiskomponente beantwortet? ▪ Welche Standards werden in der Kommunikation mit den angefragten Registern unterstützt? ▪ Ist bei der Basiskomponente und anderen Komponenten auch die Nutzung von Intermediären im 4-Corner-Prinzip erforderlich? ▪ Werden Komponenten eigenständig oder gebündelt nach Funktionalitäten technisch umgesetzt? ▪ Können Referenzimplementierungen seitens EU für die Entwicklung von Architekturkomponenten genutzt werden?
Ertüchtigung der verwendeten Transportwege	▪ Errichtung von geeigneten technischen und organisatorischen Sicherungsmaßnahmen erforderlich ▪ Verbot einer Profilbildung über verschiedene Verwaltungsbereiche hinweg ▪ 4-Corner-Prinzip als mögliche Sicherungsmaßnahme identifiziert ▪ Netzgesetz gibt den Rahmen für physische Austauschkanäle vor	▪ Wie weit ist das 4-Corner-Prinzip verbreitet? ▪ Welche Anforderungen bestehen an den europaweiten Datenaustausch? ▪ Können Intermediäre die Funktion von eDelivery-Nodes übernehmen? ▪ Welche Vorgaben bestehen zur Nutzung des Verbindungsnetzes?
Etablierung eines erweiterten Zugriffs- und Rechtemanagements	▪ Anpassungen des bestehenden Rechte- und Zugriffsmanagements erforderlich ▪ Mögliche Ertüchtigung des bestehenden Rechtemanagements (z.B. beim DVDV) für Datenaustausch auf bestehenden rechtlichen Grundlagen ▪ Aufbau eines Consent-Moduls für das Management mit Einwilligungen von Bürgern zu weiteren Austauschen auf rechtlicher Grundlage sowie Bereitstellung eines „Consent-Dialogs" für Verwaltungsanträge ▪ Authentifizierung im System gemäß den Entwicklungen im Nutzerkonto und Portalverbund	▪ Ist es möglich, Datenaustausche gesamthaft rechtlich zu beschreiben? ▪ Wie wird die Bestandsarchitektur (z.B. des DVDV) erweitert? ▪ Soll das DVDV das Zugriffs- und Rechtemanagement für alle Verwaltungsbereiche verwalten? ▪ Welche Form und Komplexität haben Zugriffs- und Rechtemanagement anderer Verwaltungsbereiche? ▪ Wer wird die Hoheit des Schreibzugriffs auf die Zugriffslisten wahrnehmen? ▪ In welcher Form erfolgen Speicherung, Abruf und Einsicht in die Daten des Consent-Moduls? ▪ Wie und an welcher Stelle wird der Login im Nutzerkonto mit dem Personenidentifier verknüpft?

Stand der Diskussion zu den Anforderungen an die Datenhaltung

	Bisheriger Diskussionsstand	Fragen, die noch zu klären sind
Einzubindende Register und Erweiterung der Registerlandschaft	▪ Registermodernisierung umfasst möglichst viele Register und elektronisch geführte Datenbanken ▪ Priorisierung der Modernisierung nötig: vorläufige Liste von 26 vorrangig relevanten Registern liegt vor ▪ Aufbau weiterer Register insb. für Registerzensus erforderlich, z.B. Bildungs-, Gebäude- sowie Wohnungsregister	▪ Welche Register werden kurz-, mittel- und langfristig angebunden? ▪ Welche relevanten Daten liegen nicht in Registerform vor? ▪ Welche weiteren Nutzer gibt es? ▪ Welche Anpassungen sind bei weiteren Nutzern (z.B. kommunalen Akteuren) erforderlich?
Sicherstellung der Qualität der Datensätze	▪ Registerführende Stellen (insbesondere diejenigen mit Bürgerkontakt) melden Änderungen an eine zentrale Stelle ▪ Registerführende Stellen pflegen Änderungsanträge seitens zentraler Stelle im eigenen Datenbestand ein ▪ Änderungsanträge sollen weitestgehend automatisiert verarbeitet werden	▪ Welche Stelle übernimmt im Verlauf einer Datenkorrektur die Datenhoheit? ▪ Werden Verantwortlichkeiten bei jeder registerführenden Stelle benannt? ▪ Sind die entsprechenden Ressourcen bei registerführenden Stellen vorhanden? ▪ Welche rechtliche Grundlage benötigen die Melde- und Änderungspflichten?
Befähigung zur Datenminimierung	▪ Zentrale Speicherung von Basisdaten zu Personen ▪ Modul „Registerdatennavigation" geplant: Übersicht, welche Daten in welchem Register originär vorliegen ▪ Bestehende Datenbasis VIP des StBA wird derzeit ausgebaut und kann ggf. als Vorleistung für das Navigationsmodul dienen ▪ „Stammregister" für Unternehmensdaten soll eingeführt werden ▪ Arbeiten zum Datenaustausch im AZR können als Fallbeispiel für Datensparsamkeit dienen	▪ Kann ein „Stammregister" für Unternehmen von einer Harmonisierung mit einer entsprechenden Stelle für Personenbasisdaten profitieren? ▪ Inwiefern kann VIP des StBA bei der Entwicklung des Navigationsmoduls als Vorleistung dienen? ▪ Welchen Kommunikations- und Datenstandard nutzt das Navigationsmodul? ▪ Ist die Löschung von Basisdaten in den dezentralen Registern nachfolgend verpflichtend?

Stand der Diskussion zu den Anforderungen an die Datensicherheit

	Bisheriger Diskussionsstand	Fragen, die noch zu klären sind
Errichtung geeigneter Sicherungs-maßnahmen	▪ Datensicherheit bei der Zuordnung von Registerdaten muss durch Errichtung zusätzlicher Sicherungsmaßnahmen weiter verstärkt werden ▪ Mögliche Sicherungsmaßnahme ist der Datentransport mittels 4-Corner-Prinzip	▪ Wie bewertet die Datenschutzkonferenz die vorgeschlagenen Sicherungsmaßnahmen? ▪ Welche Instanz kontrolliert die Intermediäre? ▪ Ist eine Anbindung via 4-Corner-Prinzip auch für die neuen Architektur-komponenten erforderlich?
Sicherstellung der Nachvollziehbarkeit (z.B. mittels Protokollierung)	▪ Protokollierung kontrolliert Rechtmäßigkeit und Verhältnismäßigkeit erfolgter Datenaustausche ▪ Datencockpit schafft Transparenz für Bürger darüber, welche Stellen wann, zu welchem Zweck und mit wem welche Daten ausgetauscht haben ▪ Protokollierung bei Intermediären erfasst nur Metadaten der Kommunikation ▪ Bisherige Protokollierung muss harmonisiert werden und Identifier ggf. als Metadaten klassifizieren ▪ Alternative Protokollierung auch in Registern und Fachverfahren mit Personenbezug	▪ Welche Datenpunkte werden wo und in welcher Form protokolliert? ▪ Werden außer Metadaten auch die fachlichen Inhaltsdaten des Austauschs protokolliert? ▪ Können Identifier als Metadaten klassifiziert werden?
Aufbau von Transparenz (z.B. mittels Datencockpit)	▪ Einsichtnahme der Bürger in Datenaustausche erwünscht ▪ Dafür notwendiges Modul Datencockpit wird in sog. „Digitalisierungslabor“ erarbeitet ▪ Metadaten werden entweder als Verweis im Datencockpit vorgehalten („Mischmodell“) oder direkt von den registerführenden Stellen abgerufen („Quellenmodell“) ▪ Erste Anwendungsfälle im Prototyp sollen Datenaustausche zur Lebenslage „Geburt“ im ELFE-Projekt sein	▪ Welche Daten werden im Datencockpit angezeigt? ▪ Welches Risiko birgt ein Einbruch ins Datencockpit für die Profilbildung? ▪ Werden Metadaten vorgehalten oder abgerufen? ▪ Werden die Inhaltsdaten ins Datencockpit geliefert oder dem Bürger auf separatem Weg zugestellt? ▪ Welche Anwendungsfälle soll das Datencockpit umfassen?

5. Umsetzungsplan und nächste Schritte

Das Koordinierungsprojekt hat einen initialen Maßnahmenplan entwickelt, der entlang von sechs Themenblöcken folgende Arbeitspakete spezifiziert (siehe Abbildung): Neben der übergreifenden Steuerung und Konzeption (1) sollen Anforderungen (2) definiert, das Architekturmodell (3) entworfen, die rechtlichen Rahmenbedingungen (4) inklusive notwendiger Gesetzesänderungen festgelegt sowie ein abgestimmtes Verständnis der Governance und Organisation (5) erreicht werden. Abschließend sollen anhand von punktuellen Erprobungen frühzeitige Erfolge erzielt und somit spürbarer Mehrwert für die Nutzer erzielt werden (6).

Diese Arbeitspakete werden in enger Koordination mit allen Stakeholdern (u.a. Bundeskanzleramt, FITKO, KoSIT, BMWi, BVA, StBA, Vertreter der Länder und Kommunen, KG Portalverbund) bearbeitet und mit den Vorhaben zum Unternehmensidentifier und zum Personenidentifier abgestimmt.

Die Arbeitspakete müssen zugleich zeitnah an die Ergebnisse des Gesetzesvorhabens angepasst werden und insbesondere die sich daraus ergebenden Anforderungen synchronisieren.

Das Koordinierungsprojekt wird in einem ersten Schritt sowohl einen „Blueprint“ für die Gesamtkonzeption erstellen als auch den frühzeitigen Erfolg und spürbaren Mehrwert einzelner vorrangiger Maßnahmen und Komponenten sicherstellen. Hierzu werden bis Ende 2020 die Ergebnisse aus den Arbeitspaketen konsolidiert und in Berichtsform an den IT-PLR übermittelt. Darüber hinaus soll die weitere Umsetzung begleitet werden. Ergebnisse der Arbeitspakete 1 bis 5 werden Konzeptpapiere („Blueprints“) für die Umsetzung des Vorhabens sein, während in Arbeitspaket 6 bereits einzelne Module implementiert bzw. einzelne „Once-only“-Anwendungen ermöglicht werden sollen.

Abbildung 3: Maßnahmen im Rahmen des Koordinierungsprojekts Registermodernisierung

Aufgaben und Inhalte des Koordinierungsprojekts Registermodernisierung

Arbeitspakete		Ziel	Aufgaben
Übergreifende Steuerung und Konzeption		Ressort- und organisationsübergreifend abgestimmtes Vorgehen und Gesamtkonzept zur Registermodernisierung	1.1 Etablierung der Programmstruktur inkl. relevanter Formate 1.2 Einrichtung zusätzlicher UAGs (insb. Recht und Governance) 1.3 Erarbeitung eines Zielbilds und Gesamtkonzeption 1.4 Kontinuierliche Berichterstattung gegenüber den Auftraggebern sowie Vorbereitung der Beschlussfassung
Vorantreiben der inhaltlichen und konzeptionellen Arbeiten	Anforderungen	Sicherstellung der Berücksichtigung aller Anforderungen (insb. nationale und EU-seitige Pflichtanforderungen) sowie Schätzung von Kosten und Aufwand	2.1 Vervollständigung der ermittelten Anforderungen insb. im Hinblick auf EU-seitige Anforderungen 2.2 [Aufwands- und Kostenschätzung Einführung Identifier[1]] 2.3 Aufwandsschätzung für die Modernisierung der Register 2.4 Aufwandsschätzungsmodell für Länder und Kommunen
	Architektur-Modell	Kohärentes Architekturmodell für eine moderne Registerlandschaft in Deutschland	3.1 Entwicklung einer Architektur-Skizze; Fokus insb. auf a Landkarte der zu verknüpfenden und führenden Register inkl. fachlicher Priorisierung b Zugangsmanagement und Mechanismen zum Datenaustausch und -abruf c Architektonische Einordnung verschiedener Infrastrukturkomponenten (z.B. Daten-Cockpit, Basiskomponente Registerabruf, Consent-Modul, etc.) und Schnittstellen 3.2 [Entwicklung von Lösungen für registerübergreifendes Identitätsmanagement[1]]
	Recht	Einheitliches Vorgehen bei notwendigen Gesetzänderungen, um rechtskreisübergreifende Registervernetzung zu ermöglichen	4.1 Prüfung der modernisierten Gesamtarchitektur 4.2 Grundsatzprüfung der Regelungsinhalte bei gesetzlichen Vorhaben 4.3 Bearbeitung allgemeiner rechtlicher Fragen der Registermodernisierung sowie legislativer Forderungen 4.4 [Gesetzentwürfe für Identitätsmanagement/ Registerzensusvorbereitungsgesetz]
	Governance und Organisation	Abgestimmtes Verständnis zur Governance für eine modernisierte Registerlandschaft	5.1 Ermittlung der grundlegenden Aufgaben zur Organisation der Registerlandschaft 5.2 Erarbeitung von Optionen zu Verantwortlichkeiten unter Berücksichtigung bestehender Regelungen 5.3 [Governance Bearbeitung im laufenden Betrieb]
Sicherstellen sichtbarer Erfolge		Sichtbare Erfolge der Registermodernisierung u.a. im Kontext der OZG-Umsetzung	6.1 Identifizierung und ggf. Umsetzung von geeigneten Pilotprojekten a Zusammenführen von Anforderungen aus der Praxis der Umsetzung von "Once-Only" im Rahmen laufender Labore des OZG-Programms mit einer modernisierten Registerlandschaft (durch Neupilotierung oder Analyse bereits laufender OZG-Pilotprojekte) b Modellierung und Praxisabgleich ausgewählter Pilotprojekte von Fachverfahren in einer modernisierten Registerarchitektur 6.2 Begleitung und ggf. Anstoß relevanter Infrastruktur-Module

1 Teil des IMK-Vorhabens bearbeitet durch BMI VII 2

1. Übergreifende Steuerung und Konzeption

Für den übergreifenden Projekterfolg ist es essenziell, die Programmstruktur mit allen relevanten Akteuren abzustimmen und Kernverantwortlichkeiten abzuklären. Insbesondere muss das Format (z.B. Workshops) der Zusammenarbeit zwischen den unterschiedlichen Akteuren abgestimmt werden. Die Steuerung erfolgt in vier Teilen:

- **1.1 Etablierung der Programmstruktur inklusive relevanter Formate**
  Die Akteure stimmen dazu Formate sowie technische und zeitliche Möglichkeiten ab. Arbeitsgruppen, Lenkungskreise und weitere Termine werden terminiert, geplant und nachbereitet. Das bewährte Workshop-Format wird als regelmäßiger Interaktionspunkt mit einer breiteren Stakeholdergruppe genutzt.

- **1.2 Einrichtung zusätzlicher UAGs**
  Zusätzlich zur Unterarbeitsgruppe (UAG) Architekturmodell sollen UAGs die organisatorischen und regulatorischen Fragen strukturieren und Lösungen ausarbeiten. Daher werden die UAGs Recht und Governance eingerichtet und Aufgabensteckbriefe erstellt. Die erarbeiteten Erkenntnisse werden in die Gesamtkonzeption eingebunden.

- **1.3 Erarbeitung eines Zielbilds und einer Gesamtkonzeption**
  Ein für alle Stakeholder einsehbares Eckpunktepapier (das vorliegende Dokument) stellt einen Konsens zu den derzeitigen Anforderungen an die Registermodernisierung, die technische Konzeption und alle erforderlichen Maßnahmen sicher. Des Weiteren umfasst diese Maßnahme die fortlaufende enge Abstimmung mit den Vorhaben zum Personen- bzw. Unternehmensidentifier sowie der KG Portalverbund.

- **1.4 Berichterstattung an Auftraggeber und Vorbereitung der Beschlussfassung**
  Erarbeitete Ergebnisse werden regelmäßig an die auftraggebenden Gremien (z.B. IT-PLR, IMK, ggf. MPK) übermittelt. Nach Abschluss der Konzeptionsphase wird die Beschlussfassung für den IT-PLR vorbereitet und übersandt.

2. Vervollständigung der Übersicht zu den Anforderungen

Die Ermittlung und Synthese der Anforderungen an die Modernisierung der Registerlandschaft ist essenziell für die effiziente und effektive Architekturentwicklung.

- **2.1 Vervollständigung der nationalen und EU-seitigen Anforderungen**
  Nationale (unter anderem Vorgaben eines registerübergreifenden Identitäts-

managements, Zielbild einer medienbruchfreien und nutzerfreundlichen Verwaltungsdigitalisierung, Registerzensus, Datencockpit, Statistikpflichten der Unternehmen) und europäische Anforderungen (unter anderem TOOP, Routing zwischen Registern, SDG) müssen erfüllt und übersichtlich dargestellt werden. Bereits vorhandene Strukturen sowie organisatorische, inhaltliche und technische Vorarbeiten sind einzubeziehen.

- **[2.2 Aufwands- und Kostenschätzung für die Einführung des Identifiers]**
  Die Einführung von registerübergreifenden Identifiern ist Kernbestandteil der Registermodernisierung. Die zeitlichen und finanziellen Ressourcen, die für die Umsetzung dieser Modelle anfallen, und die verfassungsrechtliche Bewertung sind dabei relevant für die ganzheitliche Einschätzung und Auswahl.
  Dieses Thema wird im Rahmen des IMK-Vorhabens zum Personenidentifier bearbeitet.

- **2.3 Aufwandsschätzung für die Modernisierung der Register**
  Über die Einführung des Identifiers hinaus ist mit weiteren Aufwänden zu rechnen (z.B. Aufbau von Schnittstellen oder Ertüchtigung von Registern). Diese werden für die weitere Verwendung im Projekt quantitativ abgeschätzt.

- **2.4 Aufwandsschätzung für Länder und Kommunen**
  Auf Grund der Komplexität des föderalen Systems wird die Aufwandsschätzung für Länder und Kommunen gesondert betrachtet.

3. Architekturmodell

Für die technische Entwicklung der Registermodernisierung (Architekturmodell) sind vier Maßnahmen geplant. Die Entwicklung von Architekturkomponenten erfolgt außerhalb des Koordinierungsprojektes Registermodernisierung; dieses prüft lediglich die architektonische Konzeption und Verortung in einer modernisierten Registerlandschaft.

- **3.1 Landkarte der zu verknüpfenden und führenden Register**
  Erstellung einer menschen- und maschinenlesbaren Landkarte für Registerdaten und deren jeweilige technische Befähigung. Diese ermöglicht die Planung vorzunehmender Ertüchtigungen. Die Landkarte soll alle zu beteiligenden Register identifizieren und priorisieren, insbesondere Personen- und Unternehmensdaten (ggf. weitere, wie z.B. Geodaten). Im laufenden Betrieb kann die Landkarte der Architekturkomponente Registerdatennavigation zugutekommen. So erleichtert diese das Auffinden der Daten

in den originären Registern, verbessert die Datenqualität und ermöglicht eine mögliche Bereinigung von mehrfach vorgehaltenen Daten.

- **3.2 Zugangsmanagement und Mechanismen zum Datenaustausch und -abruf**
  Die konzeptionellen Grundlagen für Authentifizierung, Adressierung und Rechtverwaltung in den Registern und der Mechanismus zum Datenaustausch und -abruf sollen im Abgleich mit bestehenden europäischen Vorleistungen und Architekturskizzen geschaffen werden.

- **3.3 Einordnung der Infrastrukturkomponenten und Schnittstellen**
  Für alle Infrastrukturkomponenten (Datencockpit, Basiskomponente Registerabruf, Consent-Modul, Registerdatennavigation etc.) sollen die technischen Voraussetzungen und jeweiligen Interdependenzen detailliert werden.

- [**3.4 Entwicklung des registerübergreifendes Identitätsmanagements**]
  Einer detaillierten Aufwandsschätzung des gewählten Modells für die Register-modernisierung folgt die Gesetzgebung. Anforderungen, die sich spezifisch aus den Eckpunkten des gewählten Modells ergeben (z.B. Datencockpit, hinsichtlich zentraler Haltung von Basisdaten und Anpassungen beim Verzeichnisdienst), werden in das Gesamtprojekt integriert.
  Die Einführung erfolgt in einem separaten Vorhaben.

4. Recht

Ziel ist es, eine rechtliche Prüfung der Gesamtarchitektur und ihrer einzelnen Komponenten zu erarbeiten. Dafür sollen abgestimmte Grundsatzentscheidungen unter Einbezug aller Akteure definiert werden. Außerdem ist eine laufende Begleitung der sichtbaren Erfolge (siehe Maßnahmenpaket 6) vorgesehen. Das Arbeitspaket Recht wird in vier Teilthemen bearbeitet:

- **4.1 Prüfung der modernisierten Gesamtarchitektur**
  Rechtliche Prüfung der modernisierten Gesamtarchitektur und ihrer einzelnen Komponenten.

- **4.2 Grundsatzprüfung der Regelungsinhalte bei gesetzlichen Vorhaben**
  Einigung innerhalb der UAG Recht auf Arbeitsprinzipien sowie Prüfung auf Eckpunkte der möglichen rechtlichen Anpassungen. Eine Klärung des allgemeinen Ansatzes bei rechtlichen Änderungen zu Datenaustauschen soll vorbereitet werden; untersucht

werden soll auch die Machbarkeit einer einheitlichen im Gegensatz zu einer Einzelfallregelung für Datenübermittlungen.

- **4.3 Bearbeitung allgemeiner rechtlicher Fragen sowie legislativer Forderungen**
  Diese Maßnahme bewertet die vorgeschlagenen strukturellen Sicherungsmaßnahmen, beurteilt die Sicherheit hinsichtlich möglicher Datenschutzrisiken und begleitet fortlaufend die technische Entwicklung hinsichtlich möglicher rechtlicher Fragestellungen. Auch soll die Verknüpfung modernisierter Register mit einem Datencockpit rechtlich analysiert werden. Zudem sollen mögliche punktuelle Erprobungen rechtlich geprüft und begleitet werden.

- [**4.4 Gesetzentwürfe für Identitätsmanagement/Registerzensus**]
  Schaffung einer sicheren Rechtsgrundlage für die Registermodernisierung über die in Entwicklung befindlichen Gesetzentwürfe für Identitätsmanagement und zum Registerzensus.
  Dieses Thema wird im Rahmen des IMK-Vorhabens zum Personenidentifier sowie im Rahmen der Arbeit des BMI zum Registerzensus bearbeitet.

5. Governance und Organisation

Für die erfolgreiche Organisation der Registermodernisierung muss übergreifend ermittelt werden, welche Verantwortlichkeiten existieren und zukünftig festgeschrieben werden sollen. Außerdem ist eine laufende Begleitung der sichtbaren Erfolge (siehe Maßnahmenpaket 6) vorgesehen.

- **5.1 Ermittlung der Grundlagen zur Organisation der Registerlandschaft**
  Es wird erarbeitet, welche Rollen in der Registermodernisierung basierend auf den zu erfüllenden Aufgaben neu anfallen und nach welchen Prinzipien Verantwortlichkeiten definiert und identifiziert werden sollen. Zudem wird eine Kommunikation der dezentralen Register untereinander bei Nutzung eines neuen zentralen Identifiers analysiert.

- **5.2 Erarbeitung von Optionen der Verantwortlichkeiten**
  Identifizierten Rollen werden mögliche Verantwortungsprofile im Sinne eines Zuständigkeitskonzepts einer modernisierten Registerlandschaft zugeordnet. Dabei ist auch der genaue Aufgabenumfang zu beschreiben, den sowohl eine Registermodernisierungsbehörde als auch die Behörden mit Verwaltungsregistern im Hinblick auf die

Nutzbarmachung des Identifiers und innerhalb des Transformationsprozess der Registerlandschaft übernehmen müssen.

- **5.3 Governance sicherstellen im laufenden Betrieb**
  Um mögliche weitere benötigte neue Rollen zu identifizieren, wird eine Delta-Analyse zwischen einmaliger Umsetzung und laufendem Betrieb durchgeführt. Sollten hier weitere Bedarfe anfallen, müssen ggf. weitere Verantwortlichkeiten ermittelt werden.

6. Sicherstellen sichtbarer Erfolge

Einzelne OZG-Leistungen und Architekturkomponenten sollen hinsichtlich einer frühen Umsetzung geprüft und geplant werden. Dies ermöglicht das frühzeitige Erkennen von möglichem Nachbesserungsbedarf sowie die erhöhte Sichtbarkeit von Verbesserungen für die Nutzer der Registermodernisierung. Hierbei wird sichergestellt, dass keine Einzelsysteme entwickelt werden, sondern die weitere Umsetzung mittels modularer Gestaltung an vorhandene Vorleistungen anknüpfen kann.

- **6.1 Identifizierung und ggf. Umsetzung von geeigneten punktuellen Erprobungen**
  Mögliche unter dem Gesichtspunkt von „once only“ zu verwirklichende OZG-Leistungen werden auf Grundlage von Analysen (z.B. Anzahl anzubindender Register, Sichtbarkeit, Praktikabilität) priorisiert und bewertet. Nachfolgend wird eine Feinplanung der für die Umsetzung nötigen Schritte erstellt und durch die UAGs begleitet. Zudem sollen Pilotprojekte in Fachverfahren in einer modernisierten Registerlandschaft identifiziert und modelliert werden.

- **6.2 Begleitung und ggf. Anstoß der relevanten Infrastruktur**
  Es werden mögliche funktionell oder räumlich eingegrenzte Anwendungsgebiete für eine frühzeitige Inbetriebnahme neuer Komponenten identifiziert. Zeitleisten bis zur Umsetzung werden definiert und eine agile Umsetzung hin zu einem nutzbaren Prototyp begleitet.

Abkürzungsverzeichnis

AsylbLG	Asylbewerberleistungsgesetz
AZR	Ausländerzentralregister
BAföG	Bundesausbildungsförderungsgesetz
BDSG	Bundesdatenschutzgesetz
beBPo	besonderes elektronisches Behördenpostfach
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BLAG	Bund-Länder-AG
BMF	Bundesministerium der Finanzen
BMI	Bundesministerium des Innern, für Bau und Heimat
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BZSt	Bundeszentralamt für Steuern
Ct.	Eurocent
IDM	Identitätsmanagement
DE4A	Digital Europe for All
DVDV	Deutsches Verwaltungsdiensteverzeichnis
DVDV2	Deutsches Verwaltungsdiensteverzeichnis (Version 2)
ELStAM	Elektronische Lohnsteuerabzugsmerkmale
EU	Europäische Union
EUR	Euro
eXTra	XML-basiertes Transportverfahren
FIM	Föderales Informations-Management
FITKO	Föderale IT-Kooperation
FV	Fachverfahren
GDI-DE	Geodateninfrastruktur Deutschland
ID	Identifikator
IDNr./IdNr.	Identifikationsnummer aus dem Datensatz der BZSt
IMK	Innenministerkonferenz
IT	Informationstechnik
IT-PLR	IT-Planungsrat
KBA	Kraftfahrtbundesamt

KfZ	Kraftfahrzeug
KoSIT	Koordinierungsstelle für IT-Standards
MAV	Maschinelles Anfrageverfahren
Mio.	Millionen
MPK	Ministerpräsidentenkonferenz
NKR	Normenkontrollrat
OSCI	Online Services Computer Interface
OZG	Onlinezugangsgesetz
RV	Rentenversicherung
SDG	Single Digital Gateway
SDG-VO	Single-Digital-Gateway-Verordnung
StBA	Statistisches Bundesamt
TOOP	The Once-Only Principle Project
TOP	Tagesordnungspunkt
UUID	Universally Unique Identifier
VIP	Verwaltungsdaten-Informationsplattform
WiMiKo	Wirtschaftsministerkonferenz
XMeld	XML-Fachstandard im Meldewesen
XÖV	XML- Fachstandard in der öffentlichen Verwaltung
XTA	XML-Fachstandard

Registermodernisierung: Zielbild und Umsetzungsplanung

Januar 2021

Inhaltsverzeichnis

1. Kernbotschaften

Um ein systematisches Vorgehen bei der Modernisierung der deutschen Registerlandschaft sicherzustellen, richtete der IT-Planungsrat (IT-PLR) das „Koordinierungsprojekt Registermodernisierung“ ein.[1] Das Koordinierungsprojekt wurde damit beauftragt, ein Zielbild und eine Maßnahmenplanung für eine modernisierte Registerlandschaft zu entwickeln, welches hiermit vorgelegt wird.

Nutzenversprechen für Bürger[2], Unternehmen und Verwaltung:
Registermodernisierung – die digitale Zukunft wird real

Die Nutzbarmachung von in Registern gespeicherten Daten durch eine konzertierte Modernisierung der deutschen Registerlandschaft ist Voraussetzung für jegliche nachhaltige Digitalisierung der deutschen Verwaltung. Nur durch die einfache, sichere und nachhaltige Nutzbarmachung von Registerdaten kann eine digitale Handlungsfähigkeit des deutschen Staates langfristig sichergestellt werden. Eine moderne Registerlandschaft stiftet Mehrwert für Bürger und Unternehmen und fördert zugleich eine effiziente digitale Verwaltung durch:

a) einfache, digitale Once-Only-Verwaltungsleistungen, sodass Bürger und Unternehmen ihre Daten nur einmal übermitteln müssen

b) einen aufwandsarmen und aktuellen registerbasierten Zensus, sodass arbeits-, zeit- und kostenintensive Haushaltsbefragungen entfallen

c) einen effizienten und sicheren zwischenbehördlichen Datenaustausch, bei dem manuelle Überprüfungen überflüssig werden

d) eine hohe Anschlussfähigkeit an das europäische technische System, damit EU-Bürger und Unternehmen Verwaltungsverfahren auch grenzüberschreitend online abwickeln können

e) eine Basis für wissenschaftliche Untersuchungen als Beitrag zum Design und der Bewertung politischer Maßnahmen und damit für eine moderne, evidenzbasierte Politik

f) einen hohen Datenschutzstandard und erweiterte Transparenz durch die konsequente Umsetzung von „Privacy by Design“ [3].

Elemente einer modernisierten Registerlandschaft

[1] Entscheidung 2019/23 – Registermodernisierung, 29. Sitzung am 27.06.2019, siehe https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2019/Sitzung_29.html?pos=5 (zuletzt abgerufen am 27.01.2021).
[2] Im Folgenden wird aus Gründen der besseren Lesbarkeit ausschließlich die männliche Form benutzt.
[3] Privacy by Design, Art. 25 DSGVO „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“.

Technische Architektur: Herzstück der modernen Registerlandschaft ist die technische Architektur. Diese soll, soweit möglich und zweckmäßig, auf der Basis der bestehenden Anwendungen und Standards des IT-Planungsrats errichtet werden. Sie muss gemäß den vorgesehenen rechtlichen Vorgaben des Registermodernisierungsgesetzes (RegMoG[4]) erweitert werden und sowohl die Umsetzung von „Once Only" in Deutschland als auch den Anschluss an das europäische Once-Only-System sicherstellen. Die bedarfsgerechte Erweiterung der technischen Infrastruktur umfasst beispielsweise ein zentrales Verzeichnis für Nachweistypen und Schnittstellen für die Anschlussfähigkeit bestehender Register. Bei der Weiterentwicklung soll die Stärkung der Interoperabilität innerhalb Deutschlands sowie die Konvergenz zu europäischen Technologien im Vordergrund stehen.

Weiterentwicklung und Aufbau von Registern: Neben der technischen Architektur sollen auch die Register selbst weiterentwickelt werden, um sicherzustellen, dass sie Mindestanforderungen an Anschlussfähigkeit und Datenmanagement genügen. Dafür sollen von Seiten des Bundes sowohl technische und methodische Unterstützung bereitgestellt als auch Anreize geschaffen werden, um registerführende Stellen bei notwendigen Weiterentwicklungen bestmöglich zu unterstützen. Auch die Wissenschaft mit ihren Expertisen, insbesondere in Hinsicht auf Datenqualität und die Potenziale von Registerdaten, soll dabei einbezogen werden. Von insgesamt mehr als 375 Registern wurden im IDNrG 56 Register benannt, die für die Umsetzung des Onlinezugangsgesetzes (OZG) eine vorrangige Rolle spielen. Unter Berücksichtigung der beschriebenen Anwendungsfälle wurden daraus sowie aus für Unternehmen relevanten Registern 18 „Top-Register" identifiziert, deren Datenbestände prioritär für „Once-Only" nutzbar gemacht werden sollten. Neben der Ertüchtigung bestehender Register gilt es zudem, Möglichkeiten für den Aufbau neuer Register zu prüfen, insbesondere eines Gebäude- und Wohnungsregisters und eines Bildungsregisters.[5] Bei der Planung und Umsetzung des registerbasierten Zensus sowie bei der Prüfung neuer Register, wie z. B. dem Bildungsregister, sollte die Wissenschaft frühzeitig eingebunden werden.

Rechtliche Grundlagen: Eine nachhaltige Registermodernisierung kann nur gelingen, wenn die verfassungs-, verwaltungs- und datenschutzrechtlichen Rahmenbedingungen von Beginn an mitgedacht werden. Aus rechtlicher Sicht kommt es bei der Registermodernisierung daher vor allem auf die Sicherstellung eines hohen Datenschutzniveaus bei gleichzeitiger Verbesserung der Transparenz für Bürger und Unternehmen an. Beides stärkt das Vertrauen der Bürger und Unternehmen in die öffentliche Verwaltung und bildet das Fundament für die

[4] In diesem Zielbild wird das Registermodernisierungsgesetz in der Fassung vom 11.11.2020 zitiert (BT-Drs. 19/24226), zum aktuellen Stand siehe http://dipbt.bundestag.de/extrakt/ba/WP19/2678/267861.html.
[5] vgl. MPK-Beschluss zu Leitlinien für eine modernisierte Registerlandschaft vom 5. Dezember 2019

Akzeptanz staatlicher E-Government-Angebote. Rechtliche Grundvoraussetzung ist, dass jede Datenverarbeitung nur bei Vorliegen einer Rechtsgrundlage erfolgen darf. Es bleibt dem Fachrecht vorbehalten, über die Ausgestaltung gesetzlicher Verarbeitungsbefugnisse zu befinden. Die zur Ermöglichung neuer Datenaustauschverbindungen notwendigen Anpassungen und Ergänzungen von Fachgesetzen können per Artikelgesetz in einem Omnibusverfahren durchgeführt werden. Unabhängig von diesen Überlegungen sollte eine Änderung des E-Government-Rechts eingehend geprüft werden.

Governance: Zur nachhaltigen Weiterentwicklung einer modernen, interoperablen Registerlandschaft müssen Organisationsstrukturen in einer zukunftsweisenden Governance so gestaltet sein, dass unterschiedliche Verwaltungsbereiche und -ebenen jederzeit effektiv zusammenarbeiten können. Um die Nutzenversprechen entsprechend des Zielbilds zu realisieren, müssen Aufgabenfelder und Zuständigkeiten sowie Entscheidungs-, Änderungs- und Kontrollprozesse klar festgelegt und Akteure mandatiert sein. Dabei sollen Dopplungen mit bereits bestehenden Strukturen vermieden werden, insbesondere beim Aufbau organisatorischer Anforderungen unter Berücksichtigung europäischer Vorgaben zur Umsetzung eines Once-Only-Rahmenwerks (u. a. SDG-VO).

Umsetzungsplanung

Das beschriebene Zielbild soll im Rahmen eines Modernisierungsprogramms über einen Zeitraum von fünf Jahren umgesetzt werden. Es gilt, zügig wahrnehmbare Entlastungseffekte für Bürger, Unternehmen und die Verwaltung zu schaffen. Dies spiegelt sich in der Umsetzungsplanung wider. Das geplante Programm umfasst drei Phasen: 1) Erprobung und Umsetzungsvorbereitung (Proof of Concept; bis Ende 2021), 2) Weitestgehende Umsetzung der technischen Architektur, rechtlicher Grundlagen und der Governance (bis Ende 2023) und 3) Aufnahme des laufenden Betriebs und Anschluss priorisierter Register (bis Ende 2025).

Im Jahr 2021 sollen wesentliche Elemente des Zielbilds erprobt und die Umsetzung vorbereitet werden. Das umfasst die Erprobung und Konzeption der technischen Architektur (Funktionalitäten, Standards und Methoden), die Weiterentwicklung und den Aufbau von Registern, die Evaluation relevanter Rechtsfragen und die Ausgestaltung der übergreifenden Governance. Dazu soll ein "Steuerungsprojekt Registermodernisierung" unter Federführung des Bundesministeriums des Innern, für Bau und Heimat (BMI) sowie der Länder Bayern und Hamburg eingerichtet werden, welches ab Mitte 2021 alle relevanten Arbeiten im Sinne eines Multiprojektmanagements steuert und die notwendige inhaltliche Koordination mit assoziierten Vorhaben sicherstellt.

2. Kontext

Die Digitalisierung der Verwaltung birgt gewaltige Potenziale für Bürger, Unternehmen und die Verwaltung selbst. Voraussetzung für eine erfolgreiche Digitalisierung ist eine moderne Registerlandschaft – sie sollte Verwaltungsdaten in hoher Qualität und Verfügbarkeit bereitstellen und einen einfachen, sicheren elektronischen Datenaustausch unter Einhaltung höchster Datenschutzstandards ermöglichen.

Entsprechend hohe Anforderungen an die Modernisierung der Registerlandschaft stellen sowohl nationale Digitalisierungsvorhaben wie das OZG und der registerbasierte Zensus als auch die SDG-VO[6] und die DSGVO[7] des Europäischen Parlaments und des Rats der Europäischen Union.

Um ein systematisches Vorgehen bei der Modernisierung der deutschen Registerlandschaft sicherzustellen, richtete der IT-PLR das „Koordinierungsprojekt Registermodernisierung" unter Federführung des Bundesministeriums des Innern, für Bau und Heimat (BMI) sowie der Länder Bayern und Hamburg sowie unter Einbeziehung der Koordinierungsstelle für IT-Standards (KoSIT), des Aufbaustabs Föderale IT-Kooperation (FITKO), und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) ein. Das Koordinierungsprojekt wurde damit beauftragt, ein Zielbild und eine Umsetzungsplanung für eine modernisierte Registerlandschaft unter der Maßgabe zu entwickeln, den Nutzen für Bürger, Unternehmen und Verwaltung zügig und spürbar zu erhöhen.

3. Zielbild der Registermodernisierung

Das Zielbild der Registermodernisierung umfasst ein klares Nutzenversprechen für Bürger, Unternehmen und Verwaltung (3.1) sowie die Beschreibung wesentlicher Elemente einer modernen Registerlandschaft (3.2).

3.1 Nutzenversprechen für Bürger, Unternehmen und Verwaltung: Registermodernisierung – die digitale Zukunft wird real

Eine moderne Registerlandschaft stiftet Mehrwert für Bürger und Unternehmen und fördert zugleich eine effiziente, digitale Verwaltung. Mit einem geschätzten jährlichen Gesamtnutzen von 6,3 Mrd. EUR zuzüglich weiterer 0,6 Mrd. EUR pro Zensus birgt die Digitalisierung von Verwaltungsleistungen auf Basis einer modernen Registerlandschaft

[6] VERORDNUNG (EU) 2018/1724 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012, Single Digital Gateway-Verordnung, siehe unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018R1724&from=EN (zuletzt abgerufen am 02.12.2020).

[7] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), siehe unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679 (zuletzt abgerufen am 02.12.2020).

enormes Potenzial.[8] Auch langfristig ist die einfache und sichere Nutzbarmachung von in Registern gespeicherten Daten Voraussetzung für jegliche Digitalisierung der deutschen Verwaltung. Sechs Anwendungsfälle stehen dabei im Fokus: a) einfache, digitale Once-Only-Verwaltungsleistungen, b) ein aufwandsarmer und aktueller registerbasierter Zensus, c) ein effizienter und sicherer zwischenbehördlicher Datenaustausch, d) eine hohe Anschlussfähigkeit an das europäische technische System (SDG-VO), e) eine datenschutzkonforme Sekundärnutzung geeigneter Registerdaten durch die Wissenschaft, sowie f) ein hoher Datenschutzstandard durch erweiterte Transparenz und Protokollierung des Datenaustausches.

Abbildung 1: Nutzenversprechen der Registermodernisierung

a) Einfache, digitale Once-Only-Verwaltungsleistungen: Auf Basis einer modernisierten Registerlandschaft sollen alle relevanten Verwaltungsleistungen für Bürger und Unternehmen digital beantragt und auch digital erbracht werden können. Hierbei soll das Once-Only-Prinzip verwirklicht werden. Das Prinzip impliziert auf Seiten des Bürgers und der Unternehmen, dass diese der Verwaltung ihre Daten jeweils nur einmal übermitteln müssen. Die Verwaltung soll also auf Wunsch des betroffenen Bürgers auf bereits vorhandene, auch bei anderen öffentlichen Stellen liegende Daten zurückgreifen, anstatt sie beim Bürger (erneut) anzufordern. Derzeit sind Register meist so organisiert, dass alle für den jeweiligen Fachbereich erforderlichen Daten vorgehalten werden und der Kreis der zugriffsberechtigten Behörden eng begrenzt ist. In Zukunft soll sichergestellt werden, dass alle Behörden die Daten, die sie für ihre Aufgabenerfüllung benötigen, schnell und unkompliziert erhalten können und dürfen – bei gleichzeitig strikter Beachtung der

[8] NKR: „Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren." (Oktober 2017).

datenschutzrechtlichen Zulässigkeitsbestimmungen und wirksamer Verhinderung einer unzulässigen Bildung von Persönlichkeitsprofilen. Dies erfordert neben technischen, rechtlichen und organisatorischen Voraussetzungen auch eine Erweiterung des Selbstverständnisses der registerführenden Stellen als „Datenhüter“ um die Rolle des „Datenbereitstellers“. Damit einher geht die Chance, die Prozesse analoger Fachverfahren auf den Prüfstand zu stellen und ggf. Anpassungen für den digitalen Prozess vorzunehmen.

b) Aufwandsarmer und aktueller registerbasierter Zensus: Die Modernisierung der Registerlandschaft soll auch die Grundlage für einen registerbasierten Zensus legen. Laut Vorgaben der EU müssen voraussichtlich ab dem Jahr 2024 – also schon vor dem nächsten "regulären" Zensus 2031 – jährlich geokodierte Bevölkerungszahlen übermittelt werden. Die dazu benötigten Daten sollen künftig registerbasiert erhoben werden. Arbeits-, zeit- und kostenintensive Haushaltsbefragungen könnten damit weitestgehend entfallen.

c) Effizienter und sicherer zwischenbehördlicher Datenaustausch: Schon heute gibt es einen intensiven Datenaustausch zwischen Behörden. Besonders beim Austausch zwischen verschiedenen Verwaltungsbereichen besteht jedoch Verbesserungsbedarf. Ein registerübergreifendes Identitätsmanagement ist in der Lage, zukünftig eine eindeutige Zuordnung angefragter Datensätze und einen zuverlässigen, automatisierten Datenaustausch zwischen berechtigten Stellen in direktem Zusammenhang mit Verwaltungsleistungen nach dem OZG zu ermöglichen. Zudem könnten – vorbehaltlich rechtlicher Grundlagen und entsprechend ihrer jeweiligen Berechtigungen – deutlich mehr beteiligte Stellen auf Basis einheitlicher und sicherer Standards miteinander kommunizieren.

d) Hohe Anschlussfähigkeit an das europäische technische System (SDG-VO): Durch die Weiterentwicklung relevanter Register, die Ertüchtigung der technischen Infrastruktur, sowie die Herstellung einer rechtlichen und organisatorischen Anschlussfähigkeit an das europäische technische System wird sichergestellt, dass ausgewählte Verwaltungsverfahren grenzüberschreitend für EU-Bürger und Unternehmen so bereitgestellt werden, dass sie vollständig medienbruchfrei online abgewickelt werden können. Analog zu dem zuvor dargestellten Punkt a) bedeutet dies, dass Bürger und Unternehmen auch grenzüberschreitend der Verwaltung ihre Daten jeweils nur einmal übermitteln müssen (europäisches Once-Only-Prinzip).

e) Sekundärnutzung der Registerdaten durch die Wissenschaft: Registerdaten haben auch für die Wissenschaft ein hohes Potenzial. Forschung auf Basis von Registerdaten kann wichtige Erkenntnisse über gesellschaftliche und wirtschaftliche Zusammenhänge generieren und damit die politische Entscheidungsfindung evidenzbasiert unterstützen (vgl. auch Erwägungsgrund 157 der DSGVO). Die Registermodernisierung verbessert die Grundlagen für eine datenschutzkonform auszugestaltende, registerdatenbasierte Forschung in Deutschland. Durch eine verbesserte Datenbereitstellung wird nicht nur

datengestützte Forschung und Stichprobenziehung in Deutschland ermöglicht, auch internationale Vergleiche ließen sich besser durchführen.

f) Hoher Datenschutzstandard und erweiterte Transparenz: Im Zuge der Registermodernisierung soll „Privacy by Design" konsequent verfolgt werden. Durch geeignete technische und organisatorische Maßnahmen sollen Datenschutzgrundsätze umgesetzt, das Recht auf informationelle Selbstbestimmung effektiv geschützt und die Rechte der von der Verarbeitung ihrer Daten Betroffenen gestärkt werden. Bürger sollen auf Knopfdruck digital und damit nutzerfreundlicher als bisher in einem Datencockpit Transparenz darüber erhalten können, welche ihrer Daten zwischen Behörden ausgetauscht wurden. Die Gefahr einer unzulässigen Profilbildung über personenbezogene Daten aus den verschiedenen Registern soll rechtlich und technisch wirksam nach dem jeweiligen Stand der Technik ausgeschlossen werden, u. a. durch strenge, gesetzlich festgelegte Zweckbindungen und konsequente technische Trennung. Zudem soll durch die eindeutige Zuordnung von Datensätzen zur richtigen Person bzw. zum richtigen Unternehmen künftig die Notwendigkeit manueller Abgleiche von Trefferlisten entfallen – und damit auch die Möglichkeit des Zugriffs auf Daten unbeteiligter Dritter aufgrund fehlerhafter Identifikation.

3.2 Elemente einer modernisierten Registerlandschaft

Um die beschriebenen Anwendungsfälle erfolgreich umzusetzen, braucht es vier wesentliche Elemente: 1) eine interoperable und sichere technische Architektur, 2) anschlussfähige Register auf Seiten der registerführenden Stellen, 3) rechtliche Rahmenbedingungen für einen sicheren und datenschutzkonformen Datenaustausch einschließlich bedarfsgerechter Zugangsmöglichkeiten für die Wissenschaft, sowie 4) eine zukunftsweisende Governance.

3.2.1 Technische Architektur

Herzstück der modernen Registerlandschaft ist eine interoperable und sichere technische Architektur, die insbesondere auf bestehenden Anwendungen und Standards des IT-Planungsrats aufbaut und diese sinnvoll ergänzt, um dem breiten Anforderungsspektrum der föderalen Registerlandschaft gerecht zu werden. Durch die Entwicklung neuer Funktionalitäten müssen sowohl die Umsetzung von „Once Only" in Deutschland als auch der Anschluss an das europäische Once-Only-System sichergestellt werden. Dabei soll die föderal-dezentrale Datenhaltung erhalten bleiben. In Summe soll gewährleistet werden, dass die Anforderungen des RegMoG[9] erfüllt und Reifegrad 4 des OZG[10], also die Once-Only-Beantragung von digitalen Verwaltungsleistungen[11], erreicht werden. Dafür gilt es auch,

[9] BT-Drs. 19/24226, zum aktuellen Stand siehe http://dipbt.bundestag.de/extrakt/ba/WP19/2678/267861.html.
[10] Quelle: https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/info-ozg/info-reifegradmodell/info-reifegradmodell-node.html.
[11] Auch bei analoger Beantragung soll das technische System eine Once-Only-Nachweiserbringung sicherstellen.

durch technische, organisatorische und möglicherweise gesetzliche Vorgaben sowie eine entsprechende Unterstützung den Anschluss bestehender Register an die technische Architektur sicherzustellen.

Bedarfsgerechte Erweiterung der bewährten technischen Infrastruktur

Bereits heute kommen verschiedene technische Komponenten zum Einsatz, um einen sicheren und effizienten Datenaustausch zu gewährleisten. Die Umsetzung von „Once Only" erfordert jedoch neue technische Funktionalitäten. Für deren Umsetzung bedarf es teilweise der Erweiterung bestehender Komponenten, in anderen Fällen müssen Anwendungen neu entwickelt und in bestehende Architekturen integriert werden. Grundsätzlich soll der Weiterentwicklung bestehender Lösungen Vorrang vor der Neuentwicklung zusätzlicher Komponenten gewährt werden.

- **Vertraulichkeit des Datenaustauschs**: Der Bund und die Länder haben in den vergangenen Jahren bereits Vermittlungsstellen für die sichere Datenübermittlung im Informationsverbund der Innenverwaltung errichtet (4-Corner-Modell). Diese sollen künftig auch dann zum Einsatz kommen, wenn Daten unter Nutzung der Identifikationsnummer zwischen öffentlichen Stellen verschiedener Verwaltungsbereiche ausgetauscht werden. Sie helfen Vertraulichkeit und Integrität beim Datenaustausch sicherzustellen, indem sie als unabhängige Intermediäre zwischen Absender und Empfänger einer Nachricht vermitteln, ohne Einblick in den Nachrichteninhalt selbst zu erhalten. Durch die Protokollierung von Metadaten (u. a. Absender, Empfänger, Grund der Datenübermittlung, Zeitstempel) verschafft dieses System Transparenz über die Datenflüsse und somit zusätzliche Kontrollmöglichkeiten zur Gewährleistung der Einhaltung datenschutzrechtlicher Anforderungen, z. B. der wirksamen Vermeidung von Profilbildung (Anforderung zur Umsetzung des RegMoG)[12].
- **Identifizierung, Authentisierung, Ende-zu-Ende-Verschlüsselung**: Zur Identifizierung und Authentisierung abrufender Behörden oder Behördenmitarbeiter (Data Consumer) kann die bestehende Public-Key-Infrastructure der Verwaltung (V-PKI) genutzt werden, sofern sie um relevante neue Zertifikate und Schlüssel erweitert wird. Das Verzeichnis digitaler Zertifikate und kryptografischer Schlüssel dient der Absicherung des elektronischen Datenaustausches und ermöglicht eine Ende-zu-Ende-Verschlüsselung. Diese soll möglichst flächendeckend zum Einsatz kommen. Insbesondere der Austausch von Daten unter Nutzung der Identifikationsnummer zwischen öffentlichen Stellen verschiedener Verwaltungsbereiche muss durchgehend verschlüsselt in gesicherten Verfahren erfolgen (Anforderung zur Umsetzung des RegMoG). Es ist zu prüfen, ob durch die Umsetzung der SDG-VO künftig weitere Anforderungen zu erfüllen sind.

[12] Vgl. § 9 Abs. 1 IDNrGE.

- **Zentrales Verzeichnis für Nachweistypen**: Bei Once-Only-Datenabfragen muss die jeweils originär zuständige Behörde für ein Datum anhand eines zentralen Verzeichnisses für Nachweistypen ermittelt und eine entsprechende Navigation dahin eingeleitet werden. Eine Verpflichtung für registerführende Stellen zur Identifikation von originären Nachweisen erforderliche Metadaten aller von ihnen geführten Datenbestände zu melden, könnte dazu beitragen, die Transparenz und Funktionalität der deutschen Registerlandschaft nachhaltig zu erhöhen und Inkonsistenzen aufzudecken. Es ist abzuwägen, ob ein solches Verzeichnis sowie eine mögliche Registerdatennavigation über die Erweiterung des deutschen Verwaltungsdiensteverzeichnisses (DVDV), die Verwaltungsdaten-Informationsplattform (VIP), die nach dem IDNrG zu erstellende Registerlandkarte oder eine gänzlich neue Komponente umgesetzt wird.
- **Anschlussfähigkeit bestehender Register:** Bestehende Register müssen an die technische Architektur angeschlossen werden. Dafür müssen fachübergreifend kompatible Schnittstellen angeboten werden. Als Angebot an registerführende Stellen können Komponenten zur Übersetzung von Datenstandards dabei helfen, eine Anschlussfähigkeit herzustellen. Das Bundesverwaltungsamt setzt bereits heute auf sogenannte Service Gateways, um die eigenen Register zu vernetzen. Im OZG-Themenfeld Querschnitt wird die Basiskomponente Nachweisabruf entwickelt, die OZG-Leistungen einen einheitlichen Zugriff auf wichtige Registerleistungen ermöglichen soll. Diese Technologien sollen als optionale Komponenten genutzt werden können, soweit ein entsprechender Bedarf besteht. Noch nicht vollständig digital erfasste Register sollen langfristig digitalisiert werden, um einen Anschluss an die technische Architektur zu ermöglichen. Dabei ist eine Orientierung an den international anerkannten FAIR-Kriterien (Findable, Accessible, Interoperable, Reusable) denkbar. Diese Kriterien implizieren keine generelle öffentliche Zugänglichkeit der Daten. Die Registerdaten sollten jedoch nicht nur maschinenlesbar bereitgestellt, sondern auch durch entsprechende einheitliche Metadaten für Bürger, Unternehmen, Wissenschaft und Verwaltung einfacher nutzbar gemacht werden.

Entwicklung neuer Funktionalitäten zur Vervollständigung des Once-Only-Systems in Deutschland

Weiterhin erfordert die erfolgreiche und zügige Umsetzung von Once-Only-Funktionalitäten, die nicht durch eine Erweiterung bestehender Komponenten umgesetzt werden können, die Entwicklung neuer Komponenten.

- **Optimiertes Identitätsmanagement:** Die Einführungen der Steueridentifikationsnummer als bereichsübergreifendes Ordnungsmerkmal für Personen (zentraler Bestandteil des RegMoG) sowie einer bundeseinheitlichen Wirtschaftsnummer als bereichsübergreifendes Ordnungsmerkmal für Unternehmen schaffen die Grundlage für ein registerübergreifendes Identitätsmanagement. Verantwortliche Stellen können

Basisdaten[13] von Personen und Unternehmen auf Inkonsistenzen prüfen, verlässlich pflegen und bereitstellen.

- **Erhöhung von Transparenz**: Den Bürgern sollen Informationen darüber, welche Daten zur eigenen Person ausgetauscht wurden, zur Verfügung gestellt werden. Diese Transparenz ist eine wichtige Voraussetzung für die Akzeptanz von Once-Only-Verwaltungsprozessen auf Seiten der Bürger. Mehr Transparenz auf Knopfdruck schafft ein „Datencockpit", das als neue zentrale Komponente konzipiert werden soll und Informationen über erfolgte Datenaustausche bereitstellt (Anforderung zur Umsetzung des RegMoG)[14]. Ein weiterer Ausbau der Funktionalitäten des Datencockpits wird projektbegleitend evaluiert.
- **Nachweis der Datenübermittlungserlaubnis**: Dies soll eine neue Komponente, das sog. „Consent-Modul", ermöglichen. Diese Komponente kann als deutscher Beitrag in den bei der Europäischen Kommission derzeit laufenden Entwicklungsprozess eines technischen Systems für grenzüberschreitende Once-Only-Austausche eingebracht werden.
- **Einheitlicher Datenstandard**: Zentraler Bestandteil der Once-Only-Architektur ist ein fachunabhängiger, einheitlicher (generischer), hochstabiler IT-Standard für den Abruf von Nachweisen aus Registern. Dieser ist eine Ergänzung zu bestehenden Fachstandards wie XÖV und XSozial, die komplexe fachspezifische Prozesse unterstützen und weiterhin notwendig sein werden. Einen solchen Once-Only-Standard gilt es unter Berücksichtigung von europäischen Vorgaben neu zu entwickeln und zu erproben.
- **Unterstützung der Antragsstellung und Nachweiserbringung durch „Once Only"**: Zur konkreten Einbindung von der Verwaltung bereits vorliegenden Daten in Online-Antragsverfahren im Sinne von „Once Only" gibt es verschiedene Möglichkeiten. Zum einen können Registerdaten auf Wunsch des Nutzers zur automatischen Vorbefüllung von Online-Anträgen bzw. zur Ergänzung von Nachweisen während des Antragsprozesses verwendet werden, sodass der Nutzer den vollständig ausgefüllten Antrag einschließlich der Nachweise selbst absenden kann. Diese Variante ist kurzfristig eingeschränkt auf jene Register, die bereits heute Daten ausreichend schnell zur Verfügung stellen können sowie die Daten aus der eID-Funktion des Personalausweises, des Aufenthaltstitels, der eID-Karte, und aus den Nutzer-/Service- bzw. Unternehmenskonten. Sie soll langfristig jedoch vermehrt ermöglicht werden. Zum anderen kann die Ergänzung des Online-Antrags bzw. die Ergänzung von Nachweisen nach Absenden (des unvollständigen Antrags) durch die für das Verwaltungsverfahren zuständige Behörde erfolgen, wenn dies vom Antragsteller gewünscht wird; entsprechendes gilt auch für die Fälle, in denen bereits nach den Vorschriften des Verfahrensrechts ein unmittelbarer

[13] Die zur Identifizierung einer natürlichen Person erforderlichen personenbezogenen Daten sind die Basisdaten, vgl. § 4 Abs. 2 IDNrGE.
[14] Artikel 2 Nummer 2 § 10 OZG-E des Entwurfs des RegMoG.

Austausch von Nachweisen zwischen Behörden erforderlich ist (z.B. aus Gründen des Fälschungsschutzes). Wenn auf diese Weise alle für den Antrag notwendigen Nachweise eingeholt worden sind, soll dem Antragsteller die Möglichkeit eingeräumt werden, diese zu sichten und zu entscheiden, ob sein Antrag auf dieser Basis bearbeitet wird oder ob der Prozess insgesamt abgebrochen werden soll. Im Unterschied zum automatisierten Vorbefüllen von Formularen im Moment der Antragstellung funktioniert diese Lösung kurzfristig auch mit solchen Registern, deren Antwortzeitverhalten ein automatisiertes Vorbefüllen gegenwärtig noch nicht zulassen. Die Entscheidung für die konkrete Ausgestaltung des Once-Only-Prozesses soll aus der Perspektive der Nutzerorientierung und -akzeptanz in Abstimmung mit den Fachprojekten erfolgen, in denen die verschiedenen OZG-Leistungen umgesetzt werden.

- **Schnittstellen zu OZG-Fachverfahren und OZG-Portalen**: Damit Fachverfahren und Portale im OZG-Kontext den Datenaustausch nutzen können, benötigen diese standardisierte Schnittstellen. Über diese Schnittstellen muss nicht nur die Kommunikation in Richtung des Anwenders erfolgen, es müssen auch benötigte Sitzungsinformationen, z. B. Anmeldestatus, Identitäten und Berechtigungen übermittelt werden können.

Once-Only-Datenkette

Die notwendigen Komponenten lassen sich vereinfacht in einer Once-Only-Datenkette darstellen. Die beschriebenen Komponenten und deren Zusammenspiel soll im Jahr 2021 in der Praxis erprobt und evaluiert werden.

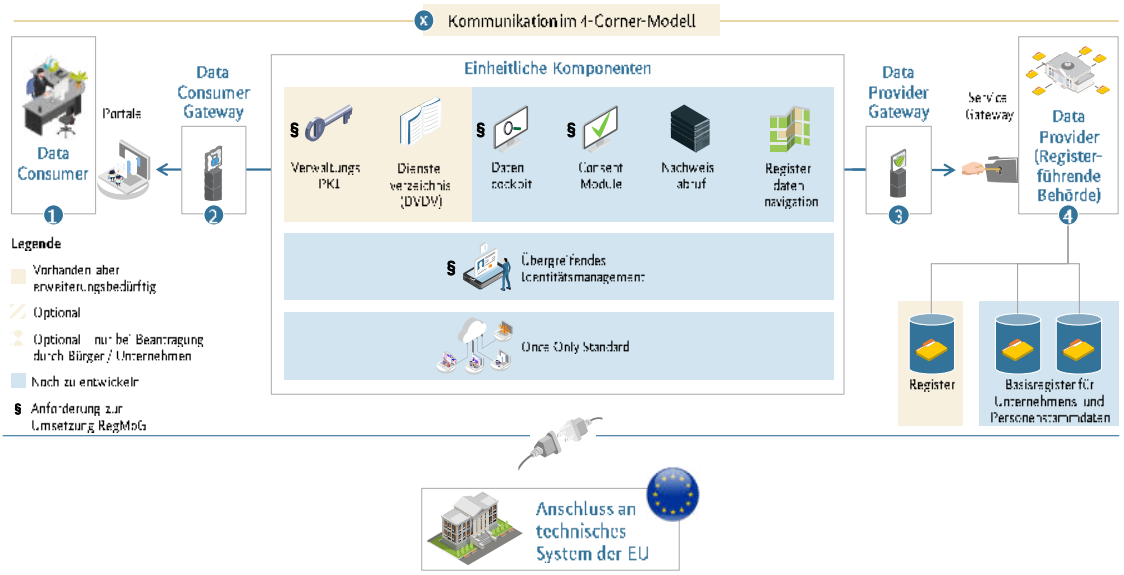


Abbildung 2: Vereinfachte Darstellung des Architekturmodells als Datenkette zur Umsetzung von „Once Only“ in Deutschland

Die technische Anschlussfähigkeit an die IT-Architektur der EU soll durch die Integration europäischer Infrastrukturkomponenten (z. B. Evidence Broker, Data Service Directory, Routing Info Discovery Service und Registry of Authority) gewährleistet werden. Die genaue

Festlegung der technischen Funktionalitäten liegt in der Zuständigkeit der EU-Kommission und befindet sich noch in Abstimmung.

3.2.2 Weiterentwicklung von Registern

Neben der technischen Architektur müssen auch die Register selbst für die digitale Zukunft bestmöglich aufgestellt sein. Als Register werden in diesem Kontext alle Datenbestände bzw. systematischen Sammlungen von Informationen bezeichnet, die der Erbringung von Verwaltungsleistungen dienen.[15] In Deutschland existieren in diesem Sinne mehr als 375 Register.[16] Die dort gespeicherten Daten bilden die Basis für die digitale Verwaltung.

Verlässlichkeit durch bundeseinheitliche Anschlussbedingungen

Im Zielbild soll sichergestellt sein, dass alle relevanten Register Mindestanforderungen an Anschlussfähigkeit und Datenmanagement genügen, um erfolgreich im Rahmen der technischen Architektur zu funktionieren. Öffentliche Stellen, die relevante Register führen, benötigen Planungssicherheit hinsichtlich der Bedingungen, unter denen sie in das technische System für „Once Only" integriert werden können. Zur Gewährleistung der Interoperabilität im bundesweiten Informationsverbund sollen daher die Anforderungen zu Form und Verfahren des Abrufs von Nachweisen – vorausgesetzt rechtlicher Zulässigkeit – verbindlich vorgegeben werden. Diesbezüglich kann eine Orientierung an den Regelungen der Verordnungen des Bundes für die Übermittlung von Meldedaten erfolgen (1. BMeldDÜV und 2. BMeldDÜV), mit denen die Schnittstellen für alle angeschlossenen Verfahren festgelegt sind. Von Seiten des Bundes sollen sowohl technische und methodische Unterstützung bereitgestellt als auch Anreize geschaffen werden, um registerführende Stellen bei den notwendigen Weiterentwicklungen bestmöglich zu unterstützen.

Für die registerführenden Behörden sollen verbindliche Vorgaben entwickelt werden, deren Umsetzung für eine optimale Nachnutzung ihrer Nachweise im Rahmen geltenden Rechts erforderlich sind. Beispielsweise ist absehbar, dass sie eine stets aktuelle Beschreibung der bei ihnen erhältlichen Nachweise in abgestimmten Formaten veröffentlichen müssen, um damit sowohl die Planung der Umsetzung von OZG-Leistungen zu befördern als auch die zentralen Verzeichnisdienste zu befüllen. Für entsprechende Regelungen zur Transparenz, aber auch viele andere Aspekte, bietet das „Europäische Interoperabilitätsrahmenwerk"[17] (EIF) wertvolle Anhaltspunkte, die einer Konkretisierung für die Anwendung in Deutschland bedürfen (siehe Annex: Leitprinzipien der Registermodernisierung).

[15] Vgl. zum Begriff des Registers Shirvani, Das Phänomen des Registers: Begriff, Typologie, unions- und verfassungsrechtliche Implikationen, in Brinkmann/Schmoeckel, Registerwesen, Grundlagen, Rechtfertigung, Potentiale, 2020, S. 53.
[16] Mehrfach vorkommende Register auf Landes- und kommunaler Ebene sowie Register, die von einzelnen Einrichtungen geführt werden, wurden nur einfach gezählt.
[17] https://ec.europa.eu/isa2/eif_en.

Weiterentwicklung bestehender Register mit Fokus auf die Anwendungsfälle

Von den über 375 Registern wurden im IDNrG bereits 56 Register benannt, in die eine bereichsübergreifende Identifikationsnummer als übergreifendes Ordnungsmerkmal für natürliche Personen eingespeichert werden soll[18]. Auch bei der Weiterentwicklung der Registerlandschaft im Sinne der beschriebenen Anwendungsfälle spielen diese 56 Register aufgrund ihrer besonderen Bedeutung für die Umsetzung des OZG eine vorrangige Rolle.

Im Sinne einer systematischen Priorisierung sollte der Fokus in einem ersten Schritt auf den Registern liegen, die eine mögliche Funktion als Datendrehscheibe[19] einnehmen können und für insgesamt vier Vorhaben besonders relevant sind: die Umsetzung von OZG-Leistungen, die Durchführung des Registerzensus, eine sichere und effiziente Gestaltung des zwischenbehördlichen Datenaustauschs sowie die europäische Vernetzung im Rahmen der SDG-VO. Von den 56 Registern des IDNrG sowie für Unternehmen relevanten Registern wurden in diesem Sinne 18 „Top-Register" identifiziert (s. Anhang 3), für welche die notwendigen Anforderungen an Anschlussfähigkeit und Datenmanagement prioritär sichergestellt werden sollen.

Um ein zielgerichtetes Vorgehen zu ermöglichen, wurden Anforderungen an Anschlussfähigkeit und Datenmanagement entwickelt, die als Ansatzpunkt für eine systematische Analyse von Registern sowie die Ableitung von individualisierten Maßnahmen je Register dienen können. Dabei gilt es, die spezifischen Rahmenbedingungen der jeweiligen Register zu berücksichtigen – denn Register dienen unterschiedlichen Zwecken, beruhen auf unterschiedlichen gesetzlichen Grundlagen und sind aus vielerlei Gründen unterschiedlich aufgebaut.

Anforderungen an die Anschlussfähigkeit

Basierend auf Empfehlungen der Europäischen Kommission lassen sich die Anforderungen an die Anschlussfähigkeit (Interoperabilität) von Registern in vier Dimensionen unterteilen (detaillierte Beschreibung in Anhang 1):

- **Rechtliche Anforderungen**: Automatisierte Datenabfragen sollten stets für alle berechtigten Nutzer rechtlich möglich sein.
- **Organisatorische Anforderungen**: Registerführende Stellen sollten als „Data Provider" agieren. Im Sinne eines Service-Anbieters ermöglichen sie einen einfachen, sicheren, und verlässlichen Zugriff auf ihre Daten.
- **Semantische Anforderungen**: Daten, Dienste und Zugriffsmechanismen sollten transparent, standardisiert und öffentlich beschrieben sein.

[18] Außerdem werden in der Gesetzesbegründung zum RegMoG, genauer in der Begründung zur Anlage 1 des IDNrG, weitere Register genannt, die gegebenenfalls zu einem späteren Zeitpunkt in die Anlage des Gesetzes aufgenommen werden sollen, z. B. das Handelsregister, siehe BT-Drs. 19/24226, S. 77.

[19] Dedizierte Stelle innerhalb eines Bereichs, an der besonders viele Daten zusammenlaufen und ausgetauscht werden, bspw. Rentenversicherung im Bereich Soziales oder Melderegister im Bereich Inneres.

- **Technische Anforderungen**: Eine sichere Anbindung an Vermittlungsstellen und eine stabile, generische Once-Only-Schnittstelle sollten die Interoperabilität technisch sicherstellen. Datensätze sollten sich auch in der behördenübergreifenden Kommunikation eindeutig zuordnen lassen.

Anforderungen an das Datenmanagement

Auch an das Datenmanagement der Register bestehen Anforderungen in vier Dimensionen (detaillierte Beschreibung in Anhang 2):

- **Anforderungen an die Datenerfassung**: Die Datenerfassung sollte weitestgehend automatisiert erfolgen. Neue Datenquellen sollten über standardisierte Schnittstellen einfach und unmittelbar angebunden werden können.
- **Anforderungen an die Datenspeicherung**: Die Datenspeicherung sollte ausschließlich digital erfolgen, die Speicherung elektronischer Dokumente erlauben und eine Verlaufsdarstellung der Registerdaten (falls fachlich sinnvoll und rechtlich zulässig) ermöglichen.
- **Anforderungen an die Datenverantwortlichkeit**: Rollen und Zuständigkeiten sowie eindeutige Datensicherheitsstandards sollten klar definiert sein.
- **Anforderungen an die Datenqualität**: Daten sollten, je nach Erfordernis, zu jeder Zeit genau, aktuell, konsistent und zugänglich sein.

Neue Register

Neben der Ertüchtigung bestehender Register ist zu prüfen, inwiefern durch den Aufbau neuer Register Lücken in der Registerlandschaft zu schließen sind, um so die Umsetzung der wesentlichen Anwendungsfälle zu ermöglichen.[20] Dabei sind auch die spezifischen Anforderungen zur Umsetzung des Registerzensus und von Verwaltungsleistungen für Unternehmen zu beachten. Bei einer Entwicklung dieser neuen Register (s. Kapitel 4) sind die beschriebenen Anforderungen an Anschlussfähigkeit und Datenmanagement von Anfang an konsequent zu beachten. Außerdem sollten Erfahrungen und bekannte Methoden aus dem Aufbau bestehender Register, z. B. in Form der Registerfactory, einbezogen werden.

Eine bessere Vernetzung von bestehenden und neuen Registern sowie eine höhere Transparenz über das Vorhandensein und die Verortung von Registerdaten könnte langfristig zur Konsolidierung und systematischeren Gliederung der Registerlandschaft beitragen. So könnten Basisdatenbestände in Beziehung gesetzt, Lücken geschlossen und Redundanzen behoben werden.

[20] Vgl. MPK-Beschluss zu Leitlinien für eine modernisierte Registerlandschaft vom 5. Dezember 2019

3.2.3 Rechtliche Grundlagen

Eine nachhaltige Registermodernisierung kann nur gelingen, wenn die verfassungs-, verwaltungs- und datenschutzrechtlichen Rahmenbedingungen von Beginn an mitgedacht werden. Aus rechtlicher Sicht kommt es daher vor allem auf die Sicherstellung eines hohen Datenschutzniveaus unter Verbesserung der Transparenz für Bürger und Unternehmen an. Beides stärkt das Vertrauen der Bürger und Unternehmen in die öffentliche Verwaltung und bildet das Fundament für die Akzeptanz staatlicher E-Government-Angebote. Rechtliche Grundvoraussetzung ist, dass jede Datenverarbeitung nur bei Vorliegen einer Rechtsgrundlage erfolgen darf. Dies gilt unabhängig davon, ob der Staat die Daten zu Zwecken der Eingriffs- oder Leistungsverwaltung[21] erhebt und mit Blick auf die Umsetzung des Once-Only-Prinzips auch unabhängig davon, ob personenbezogene Daten direkt bei dem Betroffenen erhoben oder aus einem Register abgerufen werden.

Als Rechtsgrundlage kommen für Behörden dabei grundsätzlich zwei Instrumente in Betracht: nationale, gesetzliche Rechtsgrundlagen[22] oder die in der DSGVO legaldefinierte Einwilligung[23]. Für den Bereich der Eingriffsverwaltung kommt die Einholung einer Einwilligung als Rechtsgrundlage, u. a. wegen der fehlenden Freiwilligkeit ihrer Erteilung, von vornherein nicht in Betracht. Im Bereich der Leistungsverwaltung kommt die Einholung einer Einwilligung als Rechtsgrundlage nur dann in Betracht, wenn insbesondere das Vorliegen von Freiwilligkeit zu bejahen ist (siehe auch den Erwägungsgrund 43 der DSGVO). Der Bürger muss eine echte Wahlmöglichkeit haben, also auch ohne Nachteile auf die Erteilung der Einwilligung verzichten können (siehe Erwägungsgrund 42 Satz 5 der DSGVO). Für den Anwendungsfall (a) „Einfache, digitale Once-Only-Verwaltungsleistungen“ bedeutet dies, dass der Weg, die Leistung analog zu beantragen, weiterhin offenstehen muss und nicht zusätzlich erschwert werden darf (z. B. durch hohe Kosten). Nur in diesem Fall kann die Einwilligung zur zwischenbehördlichen Nachweisbeschaffung freiwillig erteilt werden.

Im Bürger-Staat-Verhältnis empfiehlt es sich sowohl in der Eingriffs- als auch in der Leistungsverwaltung, Datenverarbeitungen nur auf Grundlage gesetzlicher Verarbeitungsbefugnisse durchzuführen. Dies entspricht den verfassungs- und datenschutzrechtlichen Vorgaben, wonach – insbesondere mit Blick auf den sog. Bestimmtheitsgrundsatz[24] und den

---

[21] Bezeichnung für die Bereiche der staatlichen Exekutive, die durch Gebote oder Verbote oder durch die Festlegung von Pflichten und Beschränkungen in Freiheitsrechte des Einzelnen eingreifen (z. B. im Polizeirecht), im Unterschied zur Leistungsverwaltung (z. B. im Sozialhilferecht).

[22] Vgl. Art. 6 Abs. 1 UAbs. 1 lit c) oder e), Abs. 3 DSGVO, der für die Mitgliedstaaten die Möglichkeit zur Schaffung nationaler Regelungen vorsieht.

[23] Siehe Art. 4 Nr. 11 DSGVO i. V. m. Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO, bzw. im Falle besonderer Kategorien Art. 9 Abs. 2 lit. a) DSGVO.

[24] Der sog. Bestimmtheitsgrundsatz legt einen strengen Maßstab an die Verwendung unbestimmter Rechtsbegriffe, von Generalklauseln und Ermessensermächtigungen. Danach muss gewährleistet bleiben, dass das Handeln der Verwaltung messbar und in gewissem Ausmaße für den Bürger voraussehbar und berechenbar ist sowie dass eine Gerichtskontrolle ermöglicht wird (vgl. BVerfGE 110, 33, 53 ff.; 108, 186, 235; 103, 332, 384).

Vorbehalt des Gesetzes (auch Parlamentsvorbehalt oder Wesentlichkeitstheorie[25]) – der Staat möglichst spezifisch die Umstände und Voraussetzungen eines Grundrechtseingriffs regeln muss. Eine Datenverarbeitung stellt auch im Bereich der Leistungsverwaltung einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar.

Auch zur Umsetzung des Once-Only-Prinzips, d. h. in der Leistungsverwaltung, sollte daher in der Regel nicht auf die Einwilligung als Rechtsgrundlage, sondern auf gesetzliche Rechtsgrundlagen zurückgegriffen werden.[26] Gesetzliche Rechtsgrundlagen für den automatisierten Once-Only-Datenaustausch müssen zumindest in der Leistungsverwaltung in aller Regel erst noch im Fachrecht normiert werden (siehe z. B. das Digitale-Familienleistungen-Gesetz[27]).

Kombination aus gesetzlicher Rechtsgrundlage und Einwilligung als Tatbestandsmerkmal

Soweit die Einholung einer Einwilligung in der Leistungsverwaltung im Einzelfall als Rechtsgrundlage dienen kann, ist auch eine Kombination aus gesetzlicher Rechtsgrundlage und Einwilligung denkbar. Dies kann durch kumulative Aufnahme der Einwilligung in den Tatbestand der gesetzlichen Rechtsgrundlage als Tatbestandsmerkmal erfolgen.

Die Aufnahme einer Einwilligung als zusätzliches Tatbestandsmerkmal ist insbesondere im hier vorliegenden Once-Only-Kontext zu befürworten.[28] So kann im Sinne digitaler Souveränität sichergestellt werden, dass die Entscheidungshoheit über die eigenen Daten sowie über die Art und Weise der Nachweiserbringung beim Bürger verbleibt.[29] Die Datenerhebung auf Basis gesetzlicher Rechtsgrundlage mit inkorporierter Einwilligung als Tatbestandsmerkmal stellt auch in verfassungsrechtlicher Hinsicht einen milderen Eingriff in das auf Recht informationelle Selbstbestimmung gegenüber einer solchen allein aufgrund gesetzlicher Rechtsgrundlage dar[30].

---

[25] Der Vorbehalt des Gesetzes stellt einerseits auf die Transparenz und Vorhersehbarkeit des staatlichen Handelns ab und gibt andererseits – ähnlich wie die Wesentlichkeitstheorie - vor, dass das Parlament als das einzige unmittelbar demokratisch legitimierte Staatsorgan sich nicht seiner Aufgabe entziehen darf, die grundlegenden Entscheidungen für das Gemeinwesen zu treffen (vgl. BVerfGE 47, 46, 78).

[26] Vgl. Art. 6 Abs. 1 UAbs. 1 lit. c) oder e), Abs. 3, 4 DSGVO.

[27] Digitale-Familienleistungen-Gesetz vom 03.12.2020 - Bundesgesetzblatt Teil I 2020 Nr. 59 09.12.2020 S. 2668.

[28] Auch im Bereich der Leistungsverwaltung kann es zweckmäßig sein, den Once-Only-Datenaustausch auch unabhängig von einer Willensäußerung des Bürgers oder des Unternehmens zu ermöglichen. Denkbar ist das z. B. in Fällen, in denen der *Validität* und *Vollständigkeit* der Daten eine besonders hohe Bedeutung zukommt, etwa wenn das Manipulationsrisiko bzgl. einzureichender Nachweise (empirisch) besonders hoch ist und / oder die bewirkten finanziellen Schäden besonders hoch wären (vgl. z. B. auch § 23 Abs. 1 Nr. 2 BDSG).

[29] D. h. im Ergebnis zur Entfaltung des Grundrechts auf informationelle Selbstbestimmung, hergeleitet durch das BVerfG aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.

[30] Vgl. u. m.w.N Kühling/Klar/Sackmann, Datenschutzrecht, 4. Auflage 2018, Rdnr. 492; vgl. auch Rdnr. 288 zur Herleitung aus Art. 8 der Grundrechtecharta.

Rechtsgrundlage und Norm[31]	**Besonderheiten, Hinweise**
Einwilligung Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO	<u>Voraussetzungen des Art. 7 DSGVO müssen vorliegen:</u> • Informiertheit des Betroffenen, insbesondere über Art, Umfang, Dauer und Zwecke der Datenverarbeitung • Freiwilligkeit (s. auch unten) • Gewährleistung der Widerruflichkeit („so einfach wie die Erteilung“, Art. 7 Abs. 3 S. 4 DSGVO) • Nachweisbarkeit einer Einwilligungserklärung Mit Widerruf der Einwilligung entfällt die Rechtsgrundlage – die Datenverarbeitung wird damit für die Zukunft unzulässig.
Gesetzliche Rechtsgrundlage, die das Vorliegen einer Einwilligung tatbestandlich erfordert Art. 6 Abs. 1 UAbs. 1 lit. e), Abs. 3 DSGVO i.V.m. der jeweiligen gesetzlichen Rechtsgrundlage	Hinsichtlich des (zusätzlichen) Tatbestandsmerkmals der Einwilligung gilt das oben Ausgeführte entsprechend. Mit Widerruf der Einwilligung entfällt eine (tragende) Voraussetzung der *gesetzlichen* Rechtsgrundlage – die Datenverarbeitung wird damit für die Zukunft unzulässig.

Tabelle 1: Übersicht über Rechtsgrundlagen und Normen

Fazit: Es bleibt dem Fachrecht vorbehalten über die Ausgestaltung gesetzlicher Verarbeitungsbefugnisse zu befinden. Zur Umsetzung des Once-Only-Prinzips wird empfohlen, die Einwilligung als Tatbestandsmerkmal in der gesetzlichen Rechtsgrundlage vorzusehen. Die hierfür notwendigen fachgesetzlichen Verarbeitungsbefugnisse können per Artikelgesetz in einem Omnibusverfahren novelliert werden.[32]

Mögliche Generalklausel zur Umsetzung des Once-Only-Prinzips?

Unabhängig von diesen Überlegungen sollte eine Änderung des E-Government-Rechts eingehender geprüft werden. Eine zentrale Frage hierbei lautet: Ist eine gesetzliche Änderung außerhalb des Fachrechts zur Umsetzung einer Once-Only-basierten E-Government-Strategie (insbesondere § 5 Abs. 2 EGovG betreffend) unter strenger Wahrung der Verfassungsmäßigkeit, insbesondere mit Blick auf das Bestimmtheitsprinzip und die Wesentlichkeitstheorie, rechtlich möglich und im Sinne einer effizienten Registermodernisierung hilfreich? Vor diesem Hintergrund ist eine Generalklausel, die allgemein die Voraussetzungen eines Once-Only-Datenaustauschs außerhalb des Fachrechts regelt, äußerst kritisch zu beleuchten. Dabei ist zu beachten, dass das Fachrecht ohnehin in den allermeisten Fällen novelliert werden muss, um Once-Only-Datenaustausche zu ermöglichen, und daher der Mehrwert einer solchen Generalklausel fraglich erscheint.

Weitere Prüfvorhaben: Verantwortlichkeit für den Betrieb des technischen Systems und Möglichkeit einer gesetzlichen Anschlussverpflichtung für registerführende Stellen

Um einen reibungslosen dauerhaften Betrieb des zu errichtenden technischen Systems sicherzustellen, soll frühzeitig geprüft werden, welche Akteure für diese Aufgabe in Frage

[31] Vorbehaltlich besonderer Anforderungen bei der Verarbeitung besonderer Kategorien personenbezogener Daten, vgl. Art. 9 Abs. 1, 2 DSGVO sowie § 35 Abs. 1 SGB I.
[32] Beispiel: Digitale-Familienleistungen-Gesetz, aaO.

kommen (z. B. der Bund). Um den größtmöglichen Nutzen der Registermodernisierung zu entfalten, wird eine hohe Anschlussquote an die technische Architektur derjenigen Behörden angestrebt, die relevante Register führen. Dies soll durch ein umfassendes Unterstützungsangebot seitens des Bundes gefördert werden. Ob und in welcher Form darüber hinaus eine rechtlich verbindliche Regelung möglich und zweckmäßig wäre, gilt es rechtlich zu evaluieren.

Einschätzung zu europäischen Vorgaben

Nach Art. 14 SDG-VO errichtet die EU-Kommission zusammen mit den Mitgliedstaaten ein technisches System für den grenzüberschreitenden automatisierten Austausch von Nachweisen unter Berücksichtigung des Once-Only-Prinzips. Dieses System muss insbesondere die Ausstellung von Nachweisen auf ausdrücklichen Wunsch des Nutzers ermöglichen (Art. 14 Abs. 3 SDG-VO). Kommission und Mitgliedstaaten verhandeln zwar noch über die datenschutzrechtlichen Implikationen dieses Verordnungsartikels; er ist aber dahingehend zu verstehen, dass mit ihm noch keine Rechtsgrundlage für eine Datenübermittlung zwischen den Behörden geschaffen wurde, sondern diese sich aus der DSGVO bzw. dem nationalen Recht ergeben muss.[33] Art. 14 SDG -VO gibt jedenfalls den Grundsatz vor, dass der Nutzer das technische System verwenden kann, aber nicht muss, sofern das Unionsrecht oder das Recht eines Mitgliedstaats nichts Gegenläufiges regeln. Die Zielarchitektur sollte demnach in folgender Hinsicht flexibel ausgestaltet werden: Zum einen soll sie einen Datenaustausch ermöglichen, sofern und soweit dieser vom Nutzer gewünscht wird („auf ausdrückliches Ersuchen")[34], zum anderen, wenn ein zwischenbehördlicher Datenaustausch aufgrund gesetzlicher Rechtsgrundlage vorgesehen ist.

3.2.4 Governance

Die öffentliche Verwaltung kann ohne eine leistungsfähige, robuste und verlässliche technische Infrastruktur zur Datenübermittlung zwischen und mit Behörden nicht mehr funktionieren. Schon heute werden zwischen öffentlichen Stellen in Deutschland jedes Jahr mehrere Milliarden Nachrichten elektronisch ausgetauscht. Mit der vollumfänglichen Umsetzung des OZG, dem Umstieg auf elektronische Rechnungen, dem registerbasierten Zensus und der Umsetzung des Once-Only-Prinzips in Deutschland und Europa wird es zu einer Vervielfachung dieser Zahlen kommen. Die Sicherstellung eines möglichst störungsfreien Betriebs der Infrastruktur in ihrer Gesamtheit beim Bund, den Ländern und den Kommunen ist daher für die öffentliche Verwaltung Deutschlands entscheidend. Sie muss nach den Grundsätzen der Robustheit, Verlässlichkeit und Übersichtlichkeit betrieben werden.

[33] Dies ergibt sich aus dem Austausch zwischen der Kommission und den Mitgliedstaaten.
[34] Vgl. Art. 14 Abs. 4 SDG-VO.

Eine moderne, interoperable Registerlandschaft benötigt daher eine übergreifende Governance. Denn die fortlaufende Gewährleistung von sicherer Interoperabilität ist Voraussetzung für die Umsetzung bereits identifizierter wie auch künftiger Anwendungsfälle – und damit für die Realisierung von Mehrwert für Bürger, Unternehmen, Wissenschaft und Verwaltung. Interoperabilität wird regelmäßig von Änderungen im Umfeld beeinträchtigt, durch neue rechtliche Vorschriften etwa oder neue technische Entwicklungen. Organisationsstrukturen müssen daher so gestaltet sein, dass unterschiedliche Verwaltungsbereiche und -ebenen jederzeit effektiv zusammenarbeiten können. Dazu müssen Aufgabenfelder und Zuständigkeiten sowie Entscheidungs-, Änderungs- und Kontrollprozesse klar festgelegt sein – sowohl im innerdeutschen als auch im europäischen Kontext.

Bei der Umsetzung der künftigen Governance sollen bestehende Strukturen sinnhaft ergänzt werden – ein sehr komplexes Vorhaben, das mehrere Jahre in Anspruch nehmen wird. Die hier dargelegten Ausarbeitungen müssen inhaltlich fortgeführt werden. In einem ersten Schritt wurden die folgenden, teils neuen Aufgaben definiert, die sich in strategische und operative Aufgabenbereiche unterteilen lassen (s. Abbildung 3).

Abbildung 3: Übersicht strategischer und operativer Aufgaben

Strategische Aufgaben umfassen richtungsweisende Entscheidungen, die von hoher Bedeutung für die gesamte Registerlandschaft sind.

- **Strategisch-politische Entscheidungsfindung**: Als oberste Instanz trifft der IT-Planungsrat (IT-PLR) bereichsübergreifende, richtungsweisende, strategisch-politische Entscheidungen zur Interoperabilität. Dabei sollen Fachministerkonferenzen (FMKs) und die Ministerpräsidentenkonferenz (MPK) bedarfsgerecht einbezogen werden.
- **Strategische Steuerung und Koordination**: Die Umsetzung richtungsweisender Entscheidungen muss unter Einbindung aller relevanten Ressorts und Akteure gesteuert werden. Je nach Natur eines Vorhabens sollte ein entsprechendes Gremium eingerichtet

werden, z. B. ein Lenkungskreis mit Vertretern aus mehreren Ressorts und Ländern. Dieser ist dem IT-Planungsrat, einer FMK oder der MPK verpflichtet und besitzt Steuerungsbefugnis für nachgelagerte Instanzen. Dem Lenkungskreis obliegt die anwendungsbezogene Ermittlung und Verknüpfung von Interoperabilitätsinitiativen auf Bundes- und Landesebene.

- **Koordinierung von EU-Angelegenheiten**: Die deutsche Verwaltung ist nicht nur gefordert dauerhaft europäische Vorgaben zu berücksichtigen, sie muss auch die Vertretung deutscher Interessen in den Partizipationsformaten der EU-Kommission sicherstellen. Ferner gilt es, die Konformität der in Deutschland entwickelten Infrastruktur mit europäischen Vorgaben, z. B. durch Verordnungen und Richtlinien, zu gewähren. Eine Koordinierungsstelle für EU-Angelegenheiten könnte die jeweils zuständigen Stellen, z.B. den nationalen SDG-Koordinator, in der Verwaltung bei der Wahrnehmung dieser Aufgaben unterstützen.
- **Proaktive Einbindung des Datenschutzes und der IT-Sicherheit**: Verantwortliche für den Datenschutz und die IT-Sicherheit sollen konsequent von Anfang an proaktiv einbezogen werden. So lässt sich von vornherein sicherstellen, dass technische und organisatorische Maßnahmen datenschutzkonform und sicher umgesetzt werden.

Operative Aufgaben umfassen die Grundlagen für die konkrete Zusammenarbeit der verschiedenen Akteure.

- **Operative Planung und Koordinierung**: Die operative Zusammenarbeit mehrerer Verwaltungsorganisationen funktioniert nur dann effektiv, wenn alle Beteiligten eine gemeinsame Vorstellung von Zielen, Zeitspannen und Prioritäten haben. Eine Anlaufstelle für Interoperabilität soll für eine übergreifende Planung, Koordinierung, Leitung und Qualitätssicherung von Vorhaben zur Herstellung und Förderung von Interoperabilität zuständig sein.
- **Ganzheitliche Steuerung und Weiterentwicklung des technischen Systems**: Das Zusammenwirken der am technischen System beteiligten Akteure hängt derzeit allein von deren Kooperationsbereitschaft und -fähigkeit ab. In Zukunft soll eine Anlaufstelle für das technische System – sowohl das bestehende System als auch notwendige Erweiterungen – über die Kompetenz verfügen, Vorgaben bezüglich der Partizipation im System zu machen, z. B. Anschlussbedingungen für alle Nutzer sowie Service-Level-Agreements (SLAs) festzulegen und die Nutzung des Once-Only-Standards vorzugeben. In Summe müssen technische Komponenten, Methoden und Standards koordiniert betrachtet und weiterentwickelt werden.
- **Umfassendes Informationsmanagement:** Eine moderne Registerlandschaft lebt von Transparenz. Das Schaffen von Transparenz soll künftig koordinierter vorangetrieben werden, z. B. von einer Anlaufstelle für Informationsmanagement. Dazu gehören die Aufbereitung und Pflege von relevanten Statistiken sowie die Erstellung und Weiterentwicklung der Übersicht über alle Register. Schließlich muss durch geeignete

Qualitätssicherungsmaßnahmen eine für die Nutzungszwecke jeweils ausreichende Datenqualität gewährleistet werden (z. B. im Hinblick auf Mehrfachfälle sowie Über- und Untererfassungen).

- **Proaktive Einbindung der Wissenschaft**: Bei der Planung und Umsetzung der Registermodernisierung kann die Wissenschaft wichtige Impulse, bspw. zur Verbesserung der Datenqualität und Entwicklung von Nutzungsperspektiven im Kontext einer evidenzbasierten Politik, geben und sollte daher proaktiv eingebunden werden.

In einem nächsten Schritt muss geprüft werden, welche Akteure für die Ausübung der beschriebenen Aufgaben in Frage kommen und wie die Zusammenarbeit effizient und zielgerichtet gestaltet werden kann. Dabei sollten Dopplungen mit bereits bestehenden Strukturen vermieden werden. Ein Austausch zu Strukturen und Erfahrungen vergleichbarer Großprojekte wird als sinnvoll erachtet und angestrebt (z. B. Pan-European Public Procurement OnLine (PEPPOL)).[35]

4. Umsetzungsplanung

Das beschriebene Zielbild soll im Rahmen eines Modernisierungsprogramms über einen Zeitraum von fünf Jahren umgesetzt werden. Es gilt, zügig wahrnehmbare Entlastungseffekte und Potenziale für Bürger, Unternehmen und Verwaltung zu schaffen. Dies spiegelt sich in der Umsetzungsplanung wider. Das geplante Programm umfasst drei Phasen: 1) Erprobung und Umsetzungsvorbereitung (Proof of Concept; bis Ende 2021), 2) Weitestgehende Umsetzung des technischen Systems, rechtlicher Grundlagen und der Governance (bis Ende 2023), sowie 3) Aufnahme des laufenden Betriebs und Anschluss priorisierter Register (bis Ende 2025). Dabei müssen gesetzliche Vorgaben sowie zeitliche und inhaltliche Abhängigkeiten von assoziierten Vorhaben der Verwaltungsdigitalisierung berücksichtigt und nach Möglichkeit ein gemeinsames oder zumindest koordiniertes Vorgehen angestrebt werden:

- Bis Ende 2021: Verabschiedung eines Gesetzesentwurfs zur Einführung eines Basisregisters für Unternehmensstammdaten in Verbindung mit einer bundeseinheitlichen Wirtschaftsnummer
- Bis Ende 2022: Vollumfängliche Umsetzung des OZG[36]

[35] PEPPOL verfolgt das Ziel der Standardisierung grenzüberschreitender, elektronisch unterstützter öffentlicher Vergabeverfahren innerhalb der Europäischen Union.
[36] https://www.bmi.bund.de/DE/themen/moderne-verwaltung/verwaltungsmodernisierung/onlinezugangsgesetz/onlinezugangsgesetz-node.html.

- Bis Ende 2023: Vollumfängliche Umsetzung der SDG-VO[37] (Bekanntgabe verpflichtender Anschlussbedingungen für die Mitgliedsstaaten mittels Durchführungsrechtsakten bis Mitte 2021)
- Ende 2024: Beginn jährlicher, registerbasierter Ermittlung der Bevölkerungszahlen
- RegMoG: Umsetzung bis fünf Jahre nach Inkrafttreten durch Bestätigung der technischen Voraussetzungen für den Betrieb nach dem Identifikationsnummerngesetz durch das BMI[38]

Es ergibt sich folgende übergreifende zeitliche Planung (detaillierte Maßnahmen- und Umsetzungsplanung in Anhang 4):

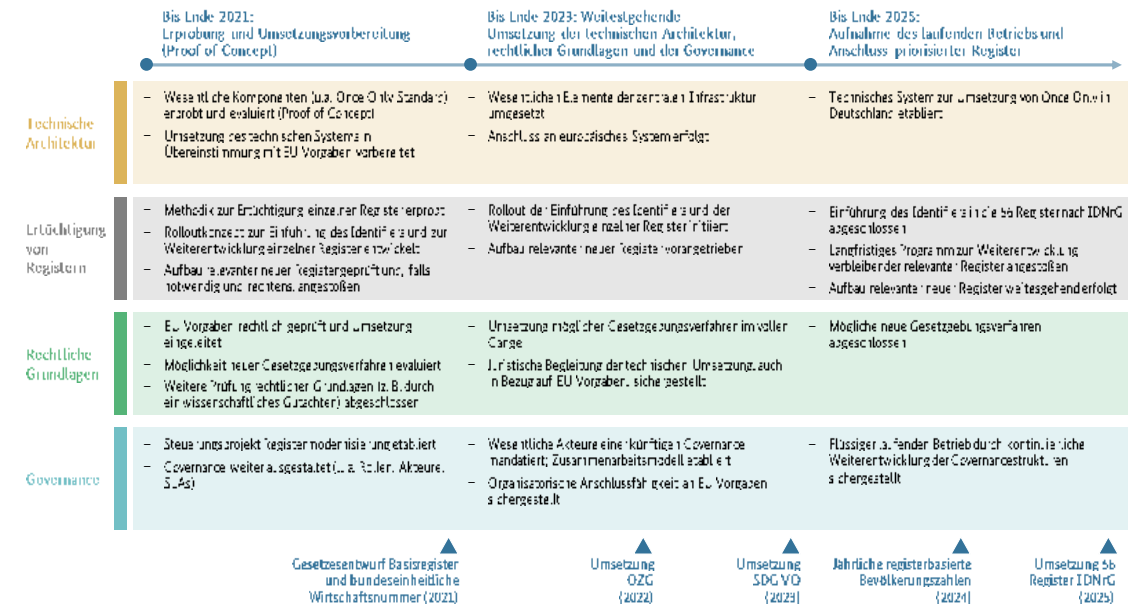


Abbildung 4: Übergreifende, vereinfachte Umsetzungsplanung

1.) Erprobung und Umsetzungsvorbereitung (Proof of Concept): Bis Ende 2021 werden wesentliche Komponenten der technischen Architektur erprobt und evaluiert, sowie deren Umsetzung vorbereitet. Dabei wird eine enge Abstimmung mit relevanten assoziierten Vorhaben erfolgen. Anforderungen an Anschlussfähigkeit und Datenmanagement für relevante Register werden gefestigt und kommuniziert. Eine Methodik zur Ertüchtigung relevanter Register wird gemeinsam mit registerführenden Stellen erprobt, um für die weitere Umsetzung bestmögliche Unterstützung anbieten zu können. Bei der Weiterentwicklung von Registern wird eine enge Verzahnung mit der Umsetzung der Personenidentifikationsnummer und entsprechenden Roll-Out-Planungen angestrebt. Parallel wird der Aufbau wesentlicher neuer Register vorangetrieben. Die entwickelten rechtlichen Empfehlungen werden evaluiert und um weitere Empfehlungen ergänzt (z. B.

[37] https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/info-sdg/sdg-anforderungen/sdg-anforderungen-node.html.
[38] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/registermodernisierungsgesetz.html.

durch ein Rechtsgutachten); die Erprobung der technischen Infrastruktur wird weiterhin rechtlich begleitet. Zudem werden die Notwendigkeit möglicher Gesetzesvorhaben evaluiert und entsprechende Eckdaten erarbeitet. Die Durchführungsrechtsakte der EU werden bewertet und für die weitere Umsetzung berücksichtigt. Für die Etablierung einer künftigen Governance werden die notwendigen Handlungsfelder mit entsprechenden Akteuren und Interaktionsmodi hinterlegt. In Summe kann spätestens ab 2022 mit der Umsetzung der technischen, rechtlichen und organisatorischen Maßnahmen begonnen werden.

2.) Weitestgehende Umsetzung der technischen Architektur, rechtlicher Grundlagen und der Governance: Bis Ende 2023 sollen alle wesentlichen Elemente der zentralen Infrastruktur umgesetzt und funktionstüchtig sein. Die Umsetzung des OZG und der SDG-VO wurden erfolgreich abgeschlossen. Die Einführungen von Personenidentifikationsnummer und bundeseinheitlicher Wirtschaftsnummer sind in vollem Gange, der Aufbau dazugehöriger Register ist entscheidend vorangetrieben. Die relevantesten Register (insbesondere für OZG-Leistungen und SDG-Verwaltungsverfahren) folgen den entwickelten Standards. Juristische Prüfungen sind abgeschlossen und mögliche Anpassungsbedarfe in Gesetzgebungsverfahren abgeschlossen oder angestoßen. Wesentliche Akteure einer künftigen Governance sind mandatiert und ein Zusammenarbeitsmodell etabliert.

3.) Aufnahme des laufenden Betriebs und Anschluss priorisierter Register: Bis Ende 2025 soll die Registermodernisierung im Wesentlichen abgeschlossen sein. Das technische System zur Umsetzung von „Once Only" in Deutschland ist etabliert, der Anschluss an die zentrale Infrastruktur flächendeckend (bzw. wo sinnvoll) sichergestellt. Alle relevanten Register folgen den etablierten Standards, die nachhaltige Ertüchtigung der gesamten Registerlandschaft ist angestoßen. Rechtliche Grundlagen sind klargestellt und wo nötig präzisiert. Die entwickelte Governance sorgt für einen sicheren laufenden Betrieb und die kontinuierliche Weiterentwicklung der Registerlandschaft.

Vertiefung Phase 1: Erprobung und Umsetzungsvorbereitung (Proof of Concept)

Im Jahr 2021 sollen wesentliche Elemente des Zielbilds erprobt und die Umsetzung vorbereitet werden. Dazu soll ein „Steuerungsprojekt Registermodernisierung" unter Federführung des BMI sowie der Länder Bayern und Hamburg eingerichtet werden, welches ab Mitte 2021 alle relevanten Arbeiten im Sinne eines Multiprojektmanagements steuert und die notwendige inhaltliche Koordination mit assoziierten Vorhaben sicherstellt. In diesem Zuge sollen auch die Definition von messbaren Kriterien zur Zielerfüllung und der Aufbau eines umfassenden Erfolgscontrollings erfolgen.

Technische Architektur: Grundsätzlich soll sich das Vorgehen zum Aufbau der technischen Architektur in Deutschland am Vorgehen der EU-Kommission orientieren. Die technische Architektur sowie Standards und Methoden werden durch das Steuerungsprojekt

koordiniert konzipiert und – in Anlehnung an die Abstimmung mit den Mitgliedstaaten der EU – mit relevanten Behörden diskutiert. Im Jahr 2021 werden relevante Komponenten der geplanten technischen Infrastruktur erprobt und evaluiert bzw. weiterentwickelt, um eine Umsetzung ab 2022 vorzubereiten. Zwecks Datenaustausch über verschiedene Bereiche hinweg sollen insbesondere ein fachübergreifender Once-Only-Standard und Service Gateways erprobt werden. Eine mögliche Erprobung der Registervernetzung anhand ausgewählter OZG-Leistungen durch die Integration entsprechender OZG-Fachportale mit der technischen Architektur kann dazu beitragen, die Funktionalität aus Nutzersicht zu beleuchten. Weitere wesentliche Bestandteile für den Datenaustausch über Verwaltungsbereiche hinweg, wie das sogenannte 4-Corner-Modell, werden weiterentwickelt.

Ertüchtigung von Registern: Zur systematischen Weiterentwicklung relevanter Register wird eine Methodik zum Anschluss an die technische Architektur und zur Sicherstellung der Anforderungen an das Datenmanagement zusammen mit registerführenden Stellen erprobt. Dadurch soll eine bedarfsgerechte Unterstützung für registerführende Behörden angeboten werden können. Die Weiterentwicklung der Register sollte gemeinsam mit der Umsetzung der Personenidentifikationsnummer geplant und ein synchronisiertes Vorgehen sichergestellt werden. Parallel gilt es, den Aufbau relevanter neuer Register unter Beachtung der Anforderungen an moderne Data Provider voranzutreiben bzw. zu prüfen. Dazu gehören insbesondere:

- Ein Bildungsregister und ein Gebäude- und Wohnungsregister[39] für vielfältige Nutzungszwecke im Bereich der Planung und des Verwaltungsvollzugs sowie für die registerbasierte Durchführung des Zensus
- Ein Anschriftenregister als Referenzdatenbestand zur eindeutigen Zuordnung der offiziell vergebenen Anschriften
- Basisregister für Unternehmensstammdaten in Verbindung mit der Einführung einer bundeseinheitlichen Wirtschaftsnummer sowie ggf. ein separates W-IdNr-Register im Zuge der Einführung einer Wirtschaftsidentifikationsnummer

Als weitere wichtige aufzubauende Register sind das e-ID-Karte-Register (nach eIDKG) und das Wettbewerbsregister (nach WregG) in Betracht. Das Modernisierungsprogramm stellt sicher, dass ein Wissens- und Erfahrungstransfer stattfindet. Die Wissenschaft kann in diesem Prozess unterstützen und sowohl Impulse für die Weiterentwicklung bestehender als auch für die Prüfung und den Aufbau neuer Register geben.

Rechtliche Grundlagen: Im Zuge des Aufbaus des technischen Systems werden relevante Rechtsfragen weiter evaluiert, ggf. unter Zuhilfenahme eines wissenschaftlichen Gutachtens. Gleichzeitig gilt es, die Vorgaben der europäischen Kommission zu prüfen und ihre Umsetzung in Deutschland zu begleiten. Außerdem wird im Jahr 2021 geprüft, ob und inwiefern in den Folgejahren im Zuge der weiteren Registermodernisierung neue

[39] Vorbehaltlich möglicher Anpassungen durch (Ressort-)Abstimmungen zum entsprechenden Gesetzesentwurf.

Gesetzgebungsverfahren eingeleitet werden müssen – z. B. ein Artikelgesetz zur Anpassung von Fachgesetzen und eine gesetzliche Anschlussverpflichtung an das technische System für registerführende Behörden.

Governance: Das Steuerungsprojekt Registermodernisierung ist im Sinne eines Multiprojektmanagements etabliert. Die übergreifende Governance für die modernisierte Registerlandschaft wird im Jahr 2021 weiter ausgestaltet. Dazu gehört u. a. Akteure für die Erfüllung vordefinierter Aufgaben zu benennen und zu mandatieren. Auf diese Weise kann sukzessive der dauerhafte Betrieb entsprechend der neuen Governance aufgenommen werden. Neue Vorgaben der EU-Kommission sind dabei fortlaufend zu berücksichtigen.

Annex: Leitprinzipien der Registermodernisierung

Am 23. März 2017 veröffentlichte die Europäische Kommission Leitlinien für digitale öffentliche Dienste, den „Europäischen Interoperabilitätsrahmen“ (EIF). Dieser Rahmen soll den Mitgliedsstaaten helfen, bei der Verwaltungsdigitalisierung einen gemeinsamen Ansatz zu verfolgen und die grenzüberschreitende Interoperabilität fördern. Die Europäische Kommission empfiehlt allen Mitgliedsstaaten die Festlegung eines Rahmenwerks zur Förderung der Interoperabilität auf nationaler Ebene.

Ausgehend von dieser Empfehlung der EU-Kommission wurden Leitprinzipien in fünf Dimensionen (übergreifend, semantisch, technisch, organisatorisch und rechtlich) entwickelt, die bei der Errichtung und dem Betrieb des technischen Systems für „Once Only“ in Deutschland genutzt werden können. Gleichzeitig können sie als Orientierungshilfe für die Harmonisierung von Digitalisierungs- und Modernisierungsvorhaben der deutschen Verwaltung genutzt werden. Als möglicher Nukleus eines „Nationalen Interoperabilitätsrahmens“ (NIF) sollen die Leitprinzipien kontinuierlich weiterentwickelt werden, bspw. durch den Einbezug von Erfahrungen assoziierter Digitalisierungsvorhaben. Adressaten können Akteure auf Bundes-, Landes- und Kommunalebene sein, die in Definition, Design, Entwicklung und Umsetzung von digitalen Verwaltungsangeboten eingebunden sind.

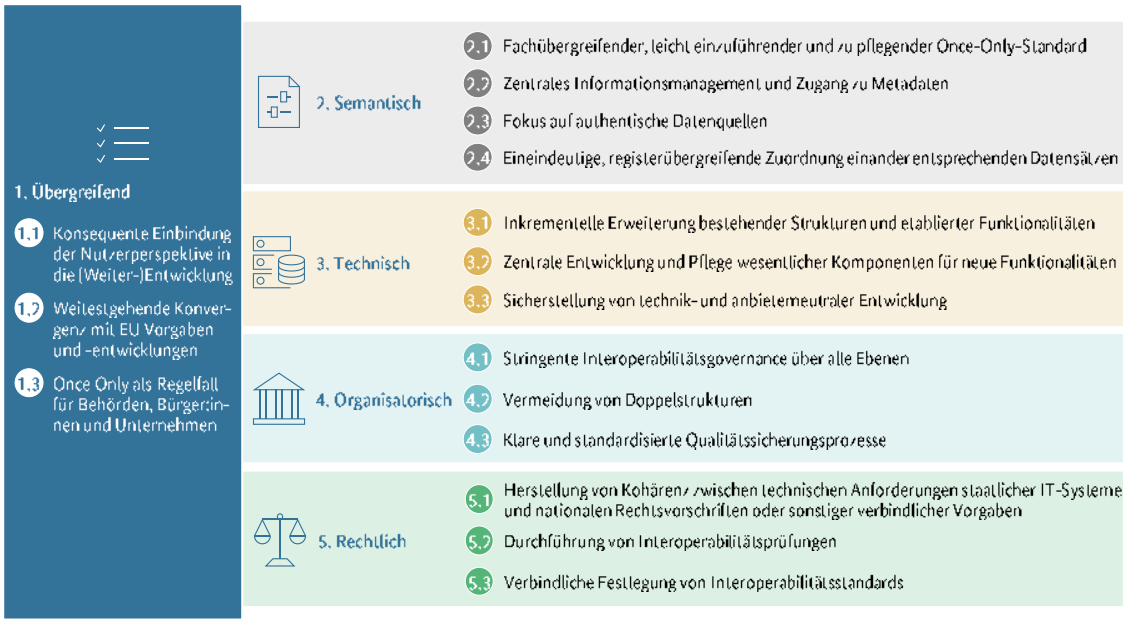


Abbildung 5: Leitprinzipien der Registermodernisierung

1 Übergreifende Leitprinzipien

Die übergreifenden Leitprinzipien geben einen richtungsweisenden Rahmen für die Anwendung der weiteren Leitprinzipien vor.

1.1 Konsequente Einbindung der Nutzerperspektive in die (Weiter-)Entwicklung

Jede Maßnahme soll daran gemessen werden, inwieweit sie einen spürbaren, pragmatischen Mehrwert für die Nutzer – Bürger, Unternehmen und Behörden – schafft.

1.2 Weitestgehende Konvergenz mit EU-Vorgaben und -entwicklungen

Die Errichtung eines technischen Systems zur Umsetzung von „Once Only“ in Deutschland soll sich, soweit möglich und sinnvoll, am Vorgehen der EU orientieren.

1.3 „Once Only“ als Regelfall für Behörden, Bürger und Unternehmen

Die Registerlandschaft soll sämtliche Daten erfassen und berechtigten Nutzern sollen bereits erhobene Daten datenschutzkonform möglichst leicht zur Wiederverwendung zugänglich gemacht werden.

2 Semantische Leitprinzipien

Die semantischen Leitprinzipien beinhalten wortwörtlich die Voraussetzungen dafür, dass beim Datenaustausch in der „selben Sprache“ gesprochen werden kann.

2.1 Fachübergreifender, leicht einzuführender und zu pflegender Once-Only-Standard

Ein übergreifender, offener und hochstabiler Standard zum Once-Only-Datenaustausch über alle Verwaltungsbereiche hinweg soll entwickelt werden.

2.2 Zentrales Informationsmanagement und Zugang zu Metadaten

Ein maschinenlesbares und zentrales Informationsmanagement soll transparent machen, welche Daten in welchen Registern vorhanden sind und an welcher Stelle sie in höchster Qualität vorliegen. Das Informationsmanagement soll zudem vermerken, welches Register für den jeweiligen Datenpunkt originär zuständig ist.

2.3 Fokus auf authentische Datenquellen

An das technische System sollen primär authentische Datenquellen der öffentlichen Verwaltung angeschlossen werden. Eine Ausweitung auf authentische Datenquellen Dritter (z. B. Notare oder Arbeitgeber) ist denkbar, bedarf allerdings einer rechtlichen Prüfung.

2.4 Eineindeutige, registerübergreifende Zuordnung einander entsprechender Datensätze

Datensätze interoperabler Register sollen einander mittels eineindeutiger persistenter Identifier unzweifelhaft zuordenbar sein – insbesondere über Verwaltungsbereiche hinweg.

3 Technische Leitprinzipien

Die technischen Leitprinzipien betonen vor allem Wirtschaftlichkeits- und Nutzenaspekte.

3.1 Inkrementelle Erweiterung bestehender Strukturen und Weiterentwicklung etablierter Funktionalitäten

Vorleistungen sollen mit Blick auf eine wirtschaftliche Umsetzung bestmöglich weitergenutzt und -entwickelt werden.

3.2 Zentrale Entwicklung und Pflege wesentlicher Komponenten für neue Funktionalitäten

Zentral entwickelte und gepflegte, modulare Komponenten sollen den einzelnen Akteuren als Standardbausteine zur Modernisierung angeboten werden. Sie fügen sich idealerweise nahtlos in bestehende, dezentrale Strukturen ein und ermöglichen registerführenden Behörden so die Zuschaltung neuer Funktionalitäten.

3.3 Sicherstellung von technik- und anbieterneutraler Entwicklung

Im Sinne von Wirtschaftlichkeit und Offenheit für die besten und innovativsten Lösungen soll bei der Entwicklung des technischen Systems Neutralität hinsichtlich Technologie- und Anbieterauswahl sichergestellt werden.

4 Organisatorische Leitprinzipien

Die organisatorischen Leitprinzipien setzen den Rahmen für den Betrieb einer modernisierten Registerlandschaft.

4.1 Stringente Interoperabilitätsgovernance über alle Ebenen

Eine Interoperabilitätsgovernance soll alle föderalen Ebenen bis zum Bund abdecken und insbesondere Brücken zwischen bislang heterogen gesteuerten Bereichen der Registerlandschaft schlagen.

4.2 Vermeidung von Doppelstrukturen

Bei der Umsetzung der künftigen Governance sollen bestehende Strukturen sinnhaft ergänzt werden, ohne Doppelstrukturen zu schaffen.

4.3 Klare, standardisierte Qualitätssicherungsprozesse

Klare, standardisierte Qualitätssicherungsprozesse ermöglichen es, Dateninkonsistenzen zügig und einheitlich aufzulösen sowie festzulegen, welcher Datensatz als Referenz genutzt wird.

5 Rechtliche Leitprinzipien bzw. rechtliche Interoperabilitätsmaßnahmen

Rechtliche Leitprinzipien im Sinne des EIF sollen dazu beitragen, dass staatliche Stellen, deren Handeln von verschiedenen rechtlichen Rahmenbedingungen, Grundsätzen und Strategien geleitet wird, befähigt werden, zusammenzuarbeiten. Dies kann auf nationaler Ebene nur unter Berücksichtigung genau dieser rechtlichen Rahmenbedingungen gelingen. Danach sind rechtliche Leitprinzipien dem deutschen Rechtssystem fernab der

grundgesetzlich festgelegten Staatsstrukturprinzipien[40], die wiederum mehr sind als bloße Leitprinzipien, fremd. Gleichwohl kann das Ziel rechtlicher Interoperabilität durch einen koordinierten Ansatz folgender rechtlicher Interoperabilitätsmaßnahmen gefördert werden.

5.1 Herstellung von Kohärenz zwischen technischen Anforderungen staatlicher IT-Systeme und nationalen Rechtsvorschriften und sonstiger verbindlicher Vorgaben

Durch den regelmäßigen Abgleich von technischen Anforderungen und nationalen Rechtsvorschriften sowie sonstiger verbindlicher Vorgaben kann die technisch-rechtliche Interoperabilität gefördert werden, indem rechtliche Rahmenbedingungen an technische Weiterentwicklungen angepasst werden.

5.2 Durchführung von Interoperabilitätsprüfungen

Die Durchführung von Interoperabilitätsprüfungen hinsichtlich etwaiger Unterschiede zwischen technischen Gegebenheiten des Bundes und der Länder kann der Identifikation rechtlicher Hemmnisse und daraus ableitbarer (gesetzlicher) Regelungsbedarfe dienen und auf diese Art die technisch-rechtliche Interoperabilität fördern.

5.3 Verbindliche Festlegung von Interoperabilitätsstandards

Die verbindliche Festlegung und Weiterentwicklung von Interoperabilitätsstandards, die ebenenübergreifend für Bund und Länder gelten, kann die technisch-rechtliche Interoperabilität fördern.

[40] Zu den Staatsstrukturprinzipien aus Art. 20 GG zählen das Demokratieprinzip (Art. 20 Abs. 1, Abs. 2 GG), das Rechtsstaatsprinzip (Art. 20 Abs. 2 S. 2, Abs. 3 GG), das Bundesstaatsprinzip (Art. 20 Abs. 1 GG), das republikanische Prinzip (Art. 20 Abs. 1 GG) sowie das Sozialstaatsprinzip (Art. 20 Abs. 1 GG). Daneben existiert als sog. Staatsziel auch das Umweltstaatsprinzip aus Art. 20a GG. Siehe dazu z. B. BeckOK GG/Huster/Rux, 44. Ed. 15.8.2020, GG Art. 20, 20a.

Anhang

Anhang 1

Anforderungen an die Anschlussfähigkeit einzelner Register

Dimension	Anforderung	Nicht erfüllt	Teilweise erfüllt	Voll erfüllt
Rechtlich: Einheitliche Grundprinzipien	1.1. Automatisierte Datenabrufe für alle Nutzer mit fachlichem Bedarf möglich	Keine automatisierten Datenabrufe möglich	[illegible]	Vollständige Anbindung und Verfügbarkeit für automatisierten Datenabruf
	1.2. Authentisierung datenabrufender Behörden mittels zentraler Dienste umgesetzt	Kein einheitliches Verfahren für die Authentisierung öffentlicher Stellen	Teilweise Umsetzung der zentralen Dienste für die Authentisierung	[illegible]
Organisatorisch: Data Provider als verlässlicher, gut erreichbarer Dienstleister	2.1. Durchgehende Verfügbarkeit von Registerdaten ist grundsätzlich sichergestellt	[illegible]	[illegible]	[illegible]
	2.2. Die Komplexität aus Nutzerperspektive wird durch Maßnahmen aktiv reduziert	[illegible]	[illegible]	[illegible]
	2.3. Verlässliche Prozesse und nutzerorientiertes Änderungsmanagement wird durchgesetzt	[illegible]	[illegible]	[illegible]
Semantisch: Transparenz über gehaltene Daten und Dienste	3.1 Gehaltene Daten werden transparent, standardisiert und öffentlich beschrieben	[illegible]	[illegible]	[illegible]
	3.2. Angebotene Dienste werden verständlich, standardisiert und öffentlich beschrieben	[illegible]	[illegible]	[illegible]
	3.3. Zugriffsmechanismen für Datenaustausch werden standardisiert und öffentlich beschrieben	[illegible]	[illegible]	[illegible]
	3.4. Gehaltene Inhaltsdaten und deren Nutzung sind zur eigenen Person/Unternehmen einsehbar	[illegible]	[illegible]	[illegible]
Technisch: Sichere, neutrale Lösungen	4.1. Sichere Anbindung an Vermittlungsstellen ist eingerichtet	[illegible]	[illegible]	[illegible]
	4.2. Generische und stabile (Once-Only) Schnittstelle ist vorhanden	[illegible]	[illegible]	[illegible]
	4.3. Technikoffene IT-Standards werden für alle Datenaustausche genutzt	[illegible]	[illegible]	[illegible]
	4.4. Datensätze können eindeutig denjenigen aus anderen Registern zugeordnet werden	[illegible]	[illegible]	[illegible]

Abbildung 6: Anforderungen an die Anschlussfähigkeit einzelner Register

Anhang 2

Anforderungen an das Datenmanagement einzelner Register

Dimension	Anforderung	Nicht erfüllt	Teilweise erfüllt	Voll erfüllt
Datenerfassung	1.1. Dezentral erfasste Daten werden unmittelbar ins Register eingespielt (Push)/ durch das Register zusammengeführt (Pull)	[illegible]	[illegible]	[illegible]
	1.2. Anbindung neuer Datenquellen ist durch standardisierte Schnittstellen einfach möglich	[illegible]	[illegible]	[illegible]
Datenspeicherung	2.1. Daten werden ausschließlich digital gespeichert	[illegible]	[illegible]	Alle Daten werden digital gespeichert
	2.2. Verlaufsdarstellung der Speichersachverhalte ist möglich	[illegible]	[illegible]	[illegible]
	2.3. Das Register ermöglicht bei relevanten Datensätzen die Zuspeicherung von Dokumenten	[illegible]	[illegible]	[illegible]
Datenverantwortlichkeit	3.1. Klare Zuständigkeiten und Definition verantwortlicher Akteure und Rollen	[illegible]	[illegible]	[illegible]
	3.2. Es gibt zentrale Datenerhebungsstandards für registerführende Stellen	[illegible]	[illegible]	[illegible]
	3.3. Klare Datensicherheitsstandards	[illegible]	[illegible]	[illegible]
	3.4. Gesetzliche Grundlage	[illegible]	[illegible]	[illegible]
Datenqualität	4.1. Registerdaten sind genau und zuverlässig	[illegible]	[illegible]	[illegible]
	4.2. Registerdaten sind aktuell	[illegible]	[illegible]	[illegible]
	4.3. Registerdaten sind konsistent	[illegible]	[illegible]	[illegible]
	4.4. Registerdaten sind zugänglich und klar	[illegible]	[illegible]	[illegible]

Abbildung 7: Anforderungen an das Datenmanagement einzelner Register

Anhang 3: 18 „Top-Register“ der Registermodernisierung

Bereich	**Register**
Inneres	Melderegister
	Passregister
	Personalausweisregister
	Personenstandsregister
	Ausländerzentralregister
Finanzen	Identifikationsnummernregister
	Daten der Finanzverwaltungen der Länder
Justiz	Bundeszentralregister
	Gewerbezentralregister
Arbeit & Soziales	Bei der Bundesagentur für Arbeit systematisch geführte personenbezogene Datenbestände nach dem Dritten Buch Sozialgesetzbuch
	Betriebedaten der Bundesagentur für Arbeit
	Stammsatzdatei der Datenstelle der Rentenversicherung gemäß § 150 des Sechsten Buches Sozialgesetzbuch
	Versichertenkonten der Rentenversicherungsträger gemäß § 149 des Sechsten Buches Sozialgesetzbuch
	Versichertenverzeichnisse der Krankenkassen
	Zentrales Unternehmerverzeichnis der gesetzlichen Unfallversicherung
Bildung	Bei den allgemeinbildenden und beruflichen Schulen, Schulbehörden, Bildungseinrichtungen nach § 2 des Hochschulstatistikgesetzes systematisch geführte personenbezogene Datenbestände zu Bildungsteilnehmenden
Wirtschaft	Verzeichnis der gemäß § 14 der Gewerbeordnung angezeigten Gewerbebetriebe
Verkehr	Zentrales Fahrzeugregister

Anhang 4: Detaillierte Umsetzungsplanung (2021-2025)(1/2)

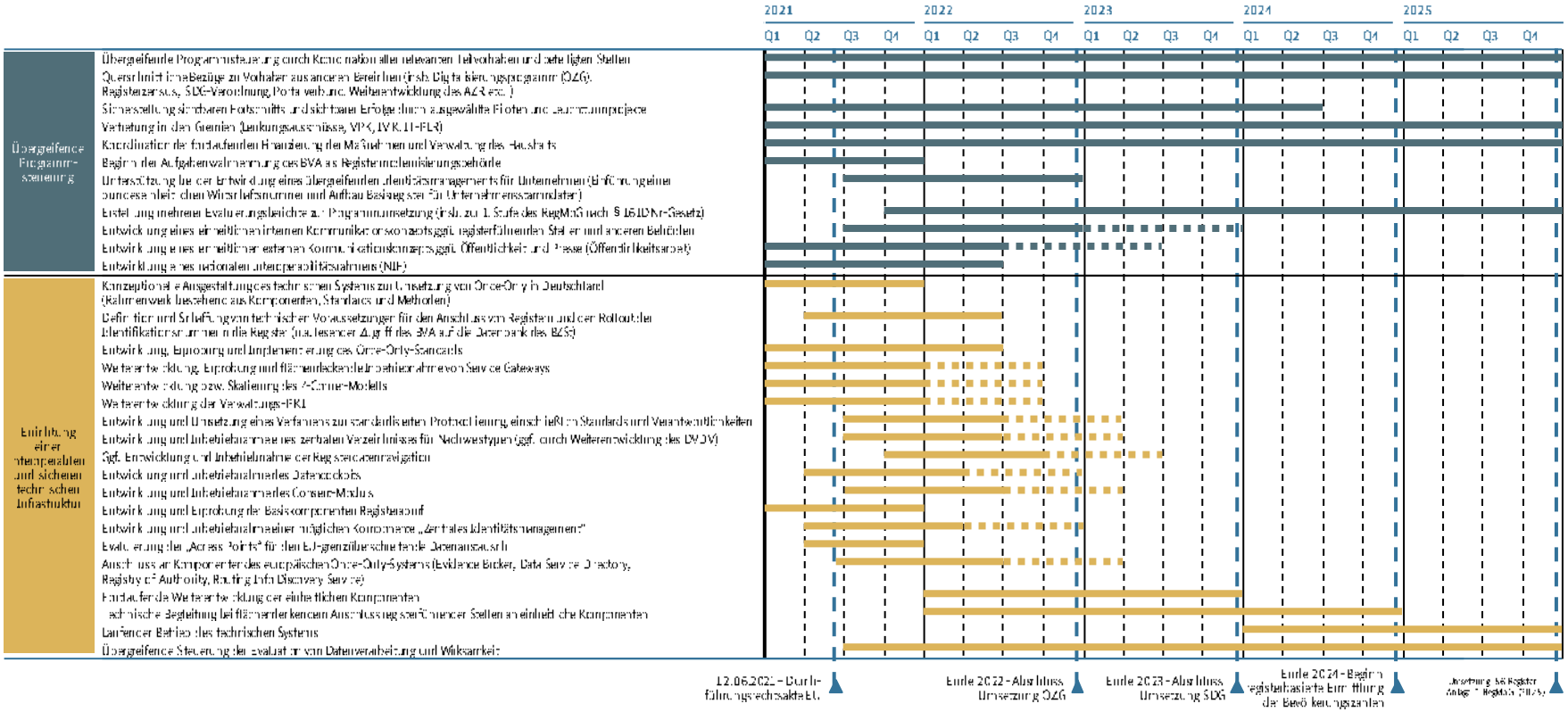


Abbildung 8: Detaillierte Umsetzungsplanung – Teil 1 von 2

Anhang 4: Detaillierte Umsetzungsplanung (2021-2025)(2/2)

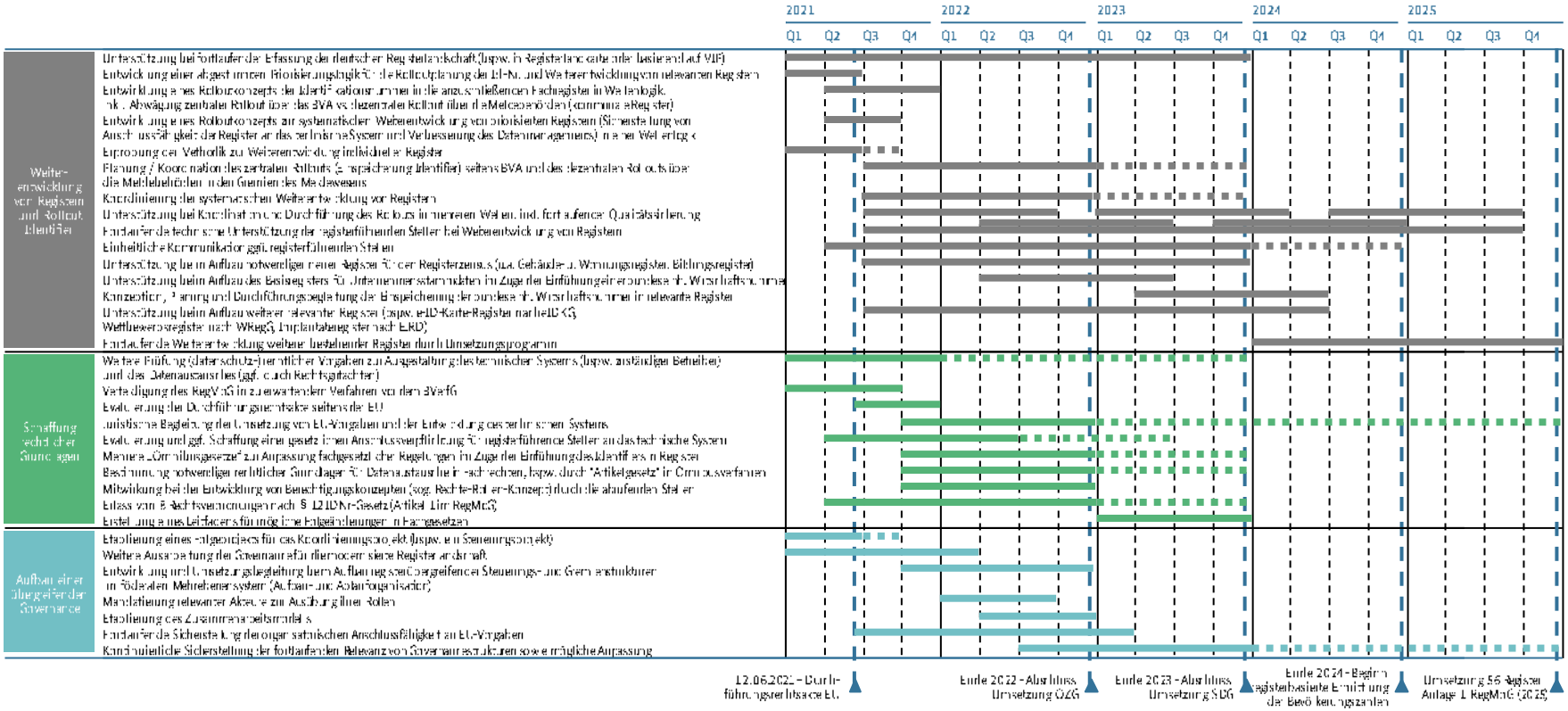


Abbildung 9: Detaillierte Umsetzungsplanung – Teil 2 von 2

Abkürzungsverzeichnis

BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BMeldDÜV	Verordnung zur Durchführung von regelmäßigen Datenübermittlungen zwischen Meldebehörden
BMI	Bundesministerium des Innern, für Bau und Heimat
DSGVO	Datenschutz-Grundverordnung
DVDV	Deutsches Verwaltungsdiensteverzeichnis
EIF	Europäischer Interoperabilitätsrahmen
EU	Europäische Union
EUR	Euro
FITKO	Föderale IT-Kooperation
FMK	Fachministerkonferenz
IDNrG	Identifikationsnummerngesetz
IT	Informationstechnik
IT-PLR	IT-Planungsrat
KoSIT	Koordinierungsstelle für IT-Standards
Mrd.	Milliarden
NIF	Nationaler Interoperabilitätsrahmen
MPK	Ministerpräsidentenkonferenz
NKR	Nationaler Normenkontrollrat
OZG	Onlinezugangsgesetz
RegMoG	Registermodernisierungsgesetz
SDG	Single Digital Gateway
SDG-VO	Single-Digital-Gateway-Verordnung
SLA	Service-Level-Agreement
VIP	Verwaltungsinformationsplattform
V-PKI	Public Key Infrastructure der Verwaltung
XSozial	XML-Fachstandard im Bereich Soziales
XÖV	XML- Fachstandard in der öffentlichen Verwaltung

Abbildungsverzeichnis

Tabellenverzeichnis

Projekt „Gesamtsteuerung Registermodernisierung“: Etablierung von Projektstrukturen

Mai 2021

Inhaltsverzeichnis

1. Kernbotschaften

Der IT-Planungsrat hat am 17. März 2021 das vom Koordinierungsprojekt Registermodernisierung erarbeitete Zielbild der Registermodernisierung beschlossen. Der im Zielbild vorgeschlagenen Vorgehensweise zur Umsetzung wurde zugestimmt.[1] Der Chef des Bundeskanzleramtes und die Chefinnen und Chefs der Staats- und Senatskanzleien der Länder haben am 6. Mai 2021 der Bundeskanzlerin und den Regierungschefinnen und Regierungschefs der Länder empfohlen, die Vorlage des Zielbildes zu begrüßen und den IT-Planungsrat zu bitten, eine koordinierte Umsetzung einzuleiten.

Um eine konzertierte Umsetzung der Registermodernisierung zu ermöglichen und die im Zielbild abgegebenen Nutzenversprechen für Bürger[2], Unternehmen und die Verwaltung einzuhalten, wurde das Koordinierungsprojekt vom IT-Planungsrat gebeten, einen **Vorschlag zur Einrichtung des Projektes „Gesamtsteuerung Registermodernisierung“** zu erarbeiten, welcher in diesem Dokument dargestellt wird.

Projekt „Gesamtsteuerung Registermodernisierung“

Um ein systematisches und schlüssiges Vorgehen bei der Modernisierung der deutschen Registerlandschaft sicherzustellen, richtet der IT-Planungsrat das Bund-Länder-Projekt „Gesamtsteuerung Registermodernisierung“ unter Federführung des Bundes (Bundesministeriums des Innern, für Bau und Heimat (BMI)) sowie der Länder Bayern und Hamburg ein. Es soll im Rahmen eines übergreifenden Programmmanagements die im Zielbild beschriebene ressort- und ebenenübergreifende Umsetzung aller Teilprojekte der Registermodernisierung vorantreiben. Die Gesamtsteuerung hat sicherzustellen, dass die Teilprojekte synergetisch auf die Erreichung der Nutzenversprechen gegenüber Bürgern und der Wirtschaft hinarbeiten. Dabei sollen bestehende bereichs- und ebenenübergreifende Strukturen wie z. B. aus der Umsetzung des Onlinezugangsgesetzes (OZG) berücksichtigt werden.

Kernstrukturen des Projektes „Gesamtsteuerung Registermodernisierung“

Entsprechend des FIT-Vorgehensmodells ist der IT-Planungsrat Projekteigentümer, die Federführer oder von ihnen beauftragte Akteure sind Projektmanager. Die Projektleitung liegt bei der aus den drei Federführern bestehenden Leitung der Transformationseinheit (siehe Kapitel 4.1). Ein durch die Federführer einzurichtender Lenkungskreis „Gesamtsteuerung Registermodernisierung“ trifft strategische

[1] Entscheidung 2021/05 – Registermodernisierung, 34. Sitzung des IT-Planungsrats vom 17. März 2021, siehe unter https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2021/Sitzung_34.html?pos=5, (zuletzt abgerufen am 14.05.2021).
[2] Im Folgenden wird aus Gründen der besseren Lesbarkeit ausschließlich die männliche Form benutzt.

Entscheidungen soweit diese nicht dem IT-Planungsrat oder anderen Gremien vorbehalten sind.

Um eine bereichs- und ebenenübergreifende Umsetzung sicherzustellen, wird eine **Bund-Länder-Transformationseinheit** eingerichtet, um die übergreifende Programmsteuerung wahrzunehmen. Die Transformationseinheit wird durch die Federführer des Projektes geleitet und durch die Koordinierungsstelle für IT-Standards (KoSIT) sowie das Bundesverwaltungsamt (BVA) als Registermodernisierungsbehörde unterstützt. In ihr werden die operativen Aufgaben der übergreifenden Programmsteuerung gebündelt. Die Transformationseinheit soll durch eine gezielte inhaltliche und methodische Unterstützung sowie ein konsequentes Programmmanagement die erfolgreiche Umsetzung aller Teilprojekte sicherstellen. Dafür werden vorerst zehn Aufgabenbereiche definiert: 1) Leitung der Transformationseinheit, 2) Zielsetzung und Veränderungsstrategie, 3) „Master of Ceremony" und Wissensmanagement, 4) Priorisierung und Steuerung von Teilprojekten, 5) Programmcontrolling, Risikomanagement und Qualitätssicherung, 6) Governance des laufenden Betriebs 7) Kommunikation, Change-Management und Stakeholdermanagement, 8) Haushaltsplanung und Finanzierung, 9) Übergreifende Strukturen / Kontaktstelle Kompetenzteams, sowie 10) Gremienkoordination Registermodernisierung.

Einbettung in bestehende Gremienstrukturen sowie Schaffung neuer Gremien und Formate

Für den Erfolg ist eine umfängliche und koordinierte Einbettung des Projektes „Gesamtsteuerung Registermodernisierung" in die bestehenden Gremienstrukturen – den IT-Planungsrat (IT-PLR), die Konferenz des Chefs des Bundeskanzleramts mit den Chefinnen und Chefs der Staats- und Senatskanzleien der Länder (ChefBK/CdSK), die Fachministerkonferenzen der deutschen Länder (FMK) sowie die Ministerpräsidentenkonferenz (MPK) – unabdingbar.

Außerdem bedarf es der Schaffung von übergreifenden Projektstrukturen, Austauschformaten und Foren zur Erfüllung relevanter Funktionen wie z. B. die Förderung von Informations-, Erfahrungs- und Wissensaustausch, den Zufluss innovativer Ideen, die Identifikation und Hebung von Synergien, die Nutzung vorhandener Expertise sowie die Möglichkeit direkter und indirekter Steuerung von Teilprojekten. Die zu schaffenden Strukturen sind dabei auch explizit als Angebot für Akteure zu verstehen, die an der Umsetzung von Teilprojekten der Registermodernisierung beteiligt oder von ihr betroffen sind.

Der hier vorgelegte Vorschlag zum Aufbau der Kernstrukturen des Projektes „Gesamtsteuerung Registermodernisierung" unter dem Dach des IT-Planungsrates soll

einen zügigen und zielgerichteten Start der Registermodernisierung ermöglichen und so zu einer schnellen Generierung von spürbarem Nutzen im Sinne des Zielbild beitragen.

2. Kontext

Die Digitalisierung der Verwaltung birgt gewaltige Potenziale für Bürger, Unternehmen und die Verwaltung selbst. Voraussetzung für eine erfolgreiche Digitalisierung ist eine moderne Registerlandschaft – sie sollte Verwaltungsdaten in hoher Qualität und Verfügbarkeit bereitstellen und einen einfachen, sicheren elektronischen Datenaustausch unter Einhaltung höchster Datenschutzstandards ermöglichen. Eine moderne Registerlandschaft ist somit kein Selbstzweck, sondern eine Voraussetzung für die erfolgreiche Verwaltungsdigitalisierung, die es zügig zu schaffen gilt.

Das vom Koordinierungsprojekt Registermodernisierung im Jahr 2020 unter Federführung des Bundes, Hamburgs und Bayerns sowie unter Einbeziehung der Koordinierungsstelle für IT-Standards (KoSIT), des Aufbaustabs Föderale IT-Kooperation (FITKO) und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) erarbeitete Zielbild der Registermodernisierung wurde im März 2021 vom IT-Planungsrat beschlossen. Der im Zielbild vorgeschlagenen Vorgehensweise zur Umsetzung wurde zugestimmt. Somit liegt erstmals ein gesamthafter Fahrplan für die Modernisierung der deutschen Registerlandschaft vor.

Um diesen umzusetzen und die im Zielbild abgegebenen Nutzenversprechen für Bürger, Unternehmen und die Verwaltung einzuhalten, wurde das Koordinierungsprojekt vom IT-Planungsrat gebeten, einen **Vorschlag zur Einrichtung des Projektes „Gesamtsteuerung Registermodernisierung“** zu erarbeiten. Das Projekt soll die ressort- und ebenenübergreifende Umsetzung des Gesamtvorhabens gewährleisten.

Nachstehend wird daher ein Vorschlag zum Aufbau von Kernstrukturen eines Projektes „Gesamtsteuerung Registermodernisierung“ unter dem Dach des IT-Planungsrates vorgelegt. Das FIT-Vorgehensmodell wurde dabei berücksichtigt.

3. Projekt „Gesamtsteuerung Registermodernisierung“

Das Projekt „Gesamtsteuerung Registermodernisierung“ soll im Rahmen eines übergreifenden Programmmanagements die im Zielbild beschriebene ressort- und ebenenübergreifende Umsetzung aller Teilprojekte der Registermodernisierung vorantreiben. Es steuert und unterstützt die Teilprojekte der Registermodernisierung u. a. durch

- Definition der rechtlichen, technischen und organisatorischen Rahmenbedingungen der Registermodernisierung auf Basis des Zielbildes (u. a. durch Festlegung von inhaltlichen und prozessualen Projektstandards),
- Herbeiführung von operativen und strategischen Entscheidungen,
- Abstimmung von fachlichen und zeitlichen Planungen, Koordination von Abhängigkeiten und Identifizierung von Synergieeffekten zwischen den einzelnen Teilprojekten und mit anderen Vorhaben (z. B. der Umsetzung des OZG),

- Aufbau eines übergreifenden Programmcontrollings,
- Unterstützung der Teilprojekte durch Expertise (z. B. Kompetenzteams) und agilitätsbefördernde Umsetzungsformate (z. B. Innovationssprints),
- Durchführung von Aufwandsschätzungen und einer koordinierten Mittelbeantragung sowie eines Finanzcontrollings unter Beachtung der finanzverfassungs-rechtlichen Rahmenbedingungen,
- Sicherstellung der Berücksichtigung von Anschlussfähigkeit an europäische Vorgaben (insb. Art. 14 SDG-Verordnung[3]),
- Sicherstellung der Berücksichtigung von Besonderheiten und spezifischen Anforderungen des bereichsspezifischen Rechts (z. B. im Bereich des Sozialrechts),
- Beratung der Teilprojekte bei der datenschutzkonformen Umsetzung von Modernisierungsmaßnahmen,
- Sicherstellung der Berücksichtigung der spezifischen Anforderungen der amtlichen Statistik und insbesondere des Registerzensus mit dem Ziel einer möglichst umfassenden, datenschutzkonformen Nutzung von Verwaltungsdaten
- Systematische Kommunikation der Vorhaben und der Mehrwerte der Registermodernisierung sowie Einbringen der Anforderungen der Registermodernisierung in andere Vorhaben.

Die Gesamtsteuerung hat sicherzustellen, dass die Teilprojekte synergetisch auf die Erreichung der Nutzenversprechen gegenüber Bürgern und der Wirtschaft hinarbeiten. Innerhalb eines durch die Gesamtsteuerung mittels einheitlicher Projektstandards definierten Modernisierungsrahmens liegt bei den Teilprojekten die Verantwortung für die Erreichung ihrer Projektziele sowie die Etablierung geeigneter Einzelprojektstrukturen und -ressourcen. Die Gesamtsteuerung unterstützt priorisierte Teilprojekte u. a. mit der Herbeiführung von Entscheidungen in ressort- und ebenenübergreifenden Gremien sowie der Bereitstellung umsetzungsbefördernder Formate und Expertise.

Dafür gilt es u. a. das Gesamtaufgabenportfolio der Registermodernisierung zu erfassen, jegliche Umsetzungsvorhaben zu klassifizieren sowie Projektstrukturen zu schaffen, die eine erfolgreiche Verzahnung, Koordination und Steuerung dieser Vorhaben und die Vernetzung mit anderen Vorhaben ermöglichen. Außerdem soll in mehreren Stufen und über mehrere Jahre die Umsetzung der Registermodernisierung koordinierend und steuernd sowie strategisch und kommunikativ begleitet werden. Dabei sind die im Bereich der Registermodernisierung relevanten Stakeholder aus Bund, Ländern und Kommunen sowie der Wirtschaft und aus Wissenschaft und Forschung einzubinden. Insbesondere soll die Gesamtsteuerung durch eine enge Einbindung registerführender Behörden sicherstellen,

[3] VERORDNUNG (EU) 2018/1724 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012, Single Digital Gateway-Verordnung, siehe unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018R1724&from=EN (zuletzt abgerufen am 28.04.2021).

dass die Registermodernisierung von einer breiten und innovationsfreudigen „Fach-Community“ getragen wird.

3.1 Federführung des Projektes „Gesamtsteuerung Registermodernisierung“

Um ein systematisches und schlüssiges Vorgehen bei der Modernisierung der deutschen Registerlandschaft sicherzustellen, richtet der IT-PLR das Bund-Länder-Projekt „Gesamtsteuerung Registermodernisierung“ unter Federführung des Bundes (BMI) sowie der Länder Bayern und Hamburg ein. Auf Grund des beträchtlichen Umfangs des Gesamtvorhabens Registermodernisierung sowie der bereichs- und ebenenübergreifenden Relevanz besteht die Möglichkeit, die Federführerschaft im Projektverlauf zu erweitern. Im weiteren Verlauf gilt es, die Ausgestaltung der jeweiligen Rollen der Federführer – ggf. durch Abschluss einer entsprechenden Verwaltungsvereinbarung – festzulegen. Die FITKO, die KoSIT sowie das BVA als Registermodernisierungsbehörde werden auf Grund ihrer fachlichen Relevanz und Expertise bei der Leitung des Projektes „Gesamtsteuerung Registermodernisierung“ und einzelnen Teilprojekten eng eingebunden. Die fachgerechte Einbindung des Statistischen Bundesamtes (Destatis) sowie des Bayerischen Landesamtes für Statistik als Vertreter der Statistischen Ämter der Länder im Zuge der Einführung des Registerzensus als Anwendungsfall der Registermodernisierung (siehe Zielbild Registermodernisierung) wird sichergestellt.

3.2 Aufgabenspektrum des Projektes „Gesamtsteuerung Registermodernisierung“

Im Gesamtkontext Registermodernisierung ergibt sich ein weitreichendes Aufgabenportfolio mit etlichen inhaltlich und strukturell eng verzahnten Vorhaben. Den Kern der nachhaltigen Modernisierung der deutschen Registerlandschaft bilden die vier im Zielbild Registermodernisierung beschriebenen wesentlichen Elemente: 1) eine interoperable und sichere technische Architektur, 2) anschlussfähige Register auf Seiten der registerführenden Stellen, 3) rechtliche Rahmenbedingungen für einen sicheren und datenschutzkonformen Datenaustausch einschließlich bedarfsgerechter Zugangsmöglichkeiten für die Wissenschaft, sowie 4) eine zukunftsweisende Governance.

Jedes dieser vier Elemente umfasst eine Vielzahl von Teilprojekten, die von verschiedenen Akteuren über alle Verwaltungsebenen und -bereiche hinweg vorangetrieben werden müssen. So gilt es bei der Errichtung einer interoperablen und sicheren technischen Infrastruktur unter anderem ein Once-Only-Rahmenwerk mit Komponenten, Standards und Methoden für Deutschland zu schaffen, die Anschlussfähigkeit an das europäische Once-Only-System nach Art. 14 der SDG-Verordnung herzustellen, bewährte Anwendungen und Standards wie das deutsche Verwaltungsdiensteverzeichnis (DVDV) weiterzuentwickeln sowie neue Komponenten wie das Datenschutzcockpit zu entwickeln.

Im Zuge der Weiterentwicklung bestehender sowie bei der Prüfung des Aufbaus neuer Register gemäß dem Zielbild Registermodernisierung gilt es z. B. das Registermodernisierungsgesetz (RegMoG), insb. die Einspeicherung der Personenidentifikationsnummer in die im Identifikationsnummerngesetz (IDNrG) genannten Register, umzusetzen, einheitliche Anschlussbedingungen für registerführende Stellen in technischer, organisatorischer und rechtlicher Hinsicht zu bestimmen, ein nachhaltiges und umfassendes Registerertüchtigungsprogramm zu schaffen, sowie gegebenenfalls bedarfsgerecht und basierend auf gesetzlichen Grundlagen neue Register zu entwickeln. Darüber hinaus müssen verlässliche rechtliche Rahmenbedingungen für den Datenaustausch geschaffen sowie fachgesetzliche Regelungen angepasst werden. Zudem gilt es verwaltungsbereichsübergreifende Organisationsstrukturen zu schaffen, um auch langfristig ein zielführendes Zusammenspiel aller Beteiligten sicherzustellen.

Neben diesen inhärenten Teilprojekten im Sinne des Zielbildes Registermodernisierung bestehen etliche weitere inhaltlich-verwandte Vorhaben, die im Gesamtkontext der Verwaltungsdigitalisierung betrachtet werden müssen, wie z. B. die Umsetzung des Onlinezugangsgesetzes (Leistungsdigitalisierung und die Errichtung des Portalverbunds), die Durchführung des Registerzensus sowie einzelne (Pilot-) Vorhaben wie das Föderale Informationsmanagement (FIM) und „Einfach Leistungen für Eltern“ (ELFE). Insbesondere die bereichs- und ebenenübergreifende Umsetzung des OZG ist bei der Ausgestaltung der Umsetzung der Registermodernisierung zu berücksichtigen, um bestehende Strukturen und Erfahrungswerte gewinnbringend zu nutzen sowie Synergien zu heben (z. B. bei der technischen Umsetzung, einer flächendeckenden Kommunikation sowie der Priorisierung von Teilprojekten). So sollte das Projekt „Gesamtsteuerung Registermodernisierung“ vertreten durch die Transformationseinheit (siehe Kapitel 4.1) an bestehenden Austauschformaten der OZG-Umsetzung teilnehmen, während konkrete OZG-Umsetzungsvorhaben, insb. bei der Umsetzung von OZG-Reifegrad 4 („Once Only“), in Steuerungs- und Austauschformaten der Registermodernisierung, wie dem Projekteboard (siehe Kapitel 4.3), einbezogen werden sollten. Insbesondere die Umsetzung von OZG-Leistungen im Reifegrad 4 als zentraler Anwendungsfall des Zielbildes Registermodernisierung soll prioritär berücksichtigt werden. Eine enge Verzahnung der beiden Großvorhaben ist für den Gesamterfolg essenziell.

Eine aufeinander abgestimmte und somit auch effektive sowie wirtschaftliche Umsetzung all dieser Vorhaben kann nur durch eine übergreifende Programmsteuerung und die konsistente Ausübung von Projektmanagementtätigkeiten unter stetiger Berücksichtigung relevanter Schnittstellen sichergestellt werden. Dazu gehören u. a. die Weiterentwicklung der Strategien zur Zielerreichung im Bereich Registermodernisierung, die Einbettung des Projektes in relevante politische Gremienstrukturen, die Einführung von Steuerungs-, Kontroll- und Risikomanagementmechanismen und -werkzeugen, ein umfassendes Stakeholdermanagement, eine vorausschauende Haushaltsplanung und Finanzierung

sowie die Entwicklung von internen und externen Kommunikationsstrategien und -konzepten.

Zur Ausübung der steuernden Projektmanagementtätigkeiten soll eine Bund-Länder-Transformationseinheit unter Leitung der Federführer (Bayern, Hamburg, Bund: BMI) eingerichtet werden (s. Kapitel 4.1).

3.3 Ressourcenbedarfe

Bei der Registermodernisierung handelt es sich nach Einschätzung des Nationalen Normenkontrollrates (NKR) um ein in der Dimension mit der Umsetzung des Onlinezugangsgesetzes vergleichbares Vorhaben.[4] Dabei ist die Registermodernisierung eine Investition in die Zukunft der deutschen Verwaltungsdigitalisierung, die mit einem Gesamtnutzen von ca. 6,3 Mrd. EUR pro Jahr enormes Entlastungspotential für Bürger, Wirtschaft und die Verwaltung bietet.[5] Die Registermodernisierung ermöglicht mit der Realisierung des Once-Only-Prinzips (OZG-Reifegrad 4) durchgehend medienbruchfreie Antrags- und Bearbeitungsprozesse bei OZG-Leistungen. Um diese Entlastungspotentiale zu realisieren werden laut Schätzung des NKR einmalige Investitionskosten i. H. v. ca. 2,5 Mrd. EUR anfallen. Europarechtlich ist Deutschland zudem zum Anschluss an ein EU-weites Once-Only-System bis Dezember 2023 verpflichtet (Art. 14 SDG-Verordnung).

Eine prioritäre Aufgabe des Projektes „Gesamtsteuerung Registermodernisierung“ wird es somit auch sein, die zur Umsetzung des Zielbildes Registermodernisierung bis 2025 entstehenden Aufwände ebenengenau zu ermitteln. Damit sollen Finanzierungsbedarfe frühzeitig erkannt sowie Bund und Ländern die Möglichkeit gegeben werden, diese bei der Haushaltsplanung zu berücksichtigen.

Für die Umstellungsaufwände im Bereich des Bundes stehen – insb. für die Umsetzung des Registermodernisierungsgesetzes – Mittel in Höhe von insgesamt bis zu 300 Mio. EUR gemäß Nummer 40 des Konjunktur- und Krisenbewältigungspakets der Bundesregierung vom 3. Juni 2020 zur Verfügung. Für den Anschluss an OZG-Leistungen und die Bereitstellung technischer Schnittstellen können zudem Mittel aus der Ziffer 41 des Konjunktur- und Krisenbewältigungspakets in Anspruch genommen werden. Die zur Umsetzung des Zielbildes Registermodernisierung erforderlichen Mittelbedarfe können nicht allein aus dem Konjunktur- und Krisenbewältigungspaket der Bundesregierung gedeckt werden.

Deshalb bedarf es für den hier vorgeschlagenen Aufbau föderaler Steuerungsstrukturen eines Projektbudgets des IT-Planungsrates. Dabei gilt es insbesondere die für den Aufbau

[4] NKR (2020), Monitor Digitale Verwaltung #4: https://www.normenkontrollrat.bund.de/resource/blob/72494/1783152/14635b15fe7f6902039abcd653de6c61/20200909-monitordigitaleverwaltung-4-data.pdf

[5] NKR (2017): Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren, Register modernisieren: https://www.normenkontrollrat.bund.de/nkr-de/homepage/erweiterte-suche/mehr-leistung-fuer-buerger-und-unternehmen-726194

und den Betrieb der Transformationseinheit bis 2025 befristet entstehenden Ressourcenbedarfe zu decken. Es wird daher vorgeschlagen, dass die Federführer auf Basis einer Aufwandsschätzung dem IT-Planungsrat bei seiner Herbstsitzung 2021 einen mit der FITKO abgestimmten Entscheidungsvorschlag zur weiteren Finanzierung des Projektes „Gesamtsteuerung Registermodernisierung“ unterbreiten.

4. Kernstrukturen des Projektes „Gesamtsteuerung Registermodernisierung“

Entsprechend des FIT-Vorgehensmodells sind folgende Kernstrukturen vorgesehen: Projekteigentümer ist der IT-Planungsrat, die Federführer oder von diesen beauftragte Akteure sind Projektmanager. Die Projektleitung liegt bei der aus den Federführern bestehenden Leitung der Transformationseinheit. Ein durch die Federführer einzurichtender Lenkungskreis „Gesamtsteuerung Registermodernisierung“ trifft strategische Entscheidungen soweit diese nicht dem IT-Planungsrat oder oder anderen Gremien vorbehalten sind.

Das Gesamtvorhaben Registermodernisierung umfasst nahezu alle Ressorts und föderalen Ebenen in einer Vielzahl an verzahnten Teilprojekten. Als ebenenübergreifendes Großvorhaben kann die Registermodernisierung nur unter enger Beteiligung aller relevanten Stakeholder erfolgreich umgesetzt werden. Dafür bedarf es im Nukleus einer **schlagkräftigen Projektorganisation**, die das Gesamtvorhaben strategisch betrachtet sowie operativ koordiniert und steuert. Im Kern des Projektes „Gesamtsteuerung Registermodernisierung“ soll daher eine **Bund-Länder-Transformationseinheit** stehen und die übergreifende Programmsteuerung wahrnehmen.

4.1 Einrichtung einer Bund-Länder-Transformationseinheit

Die Transformationseinheit wird durch die Federführer des Projektes geleitet. In ihr werden die operativen Aufgaben der übergreifenden Programmsteuerung gebündelt. Die Transformationseinheit soll durch eine gezielte inhaltliche und methodische Unterstützung sowie ein konsequentes Programmmanagement die erfolgreiche Umsetzung aller Teilprojekte sicherstellen. Sie agiert als inhaltlicher Vordenker und Sparringpartner, definiert Ziele, entwickelt die Veränderungsstrategie weiter und hilft dabei diese zu operationalisieren. Sie unterstützt die konsistente Erreichung der gesetzten Ziele, indem sie adäquate Kontroll- und Steuerungsmechanismen entwickelt und etabliert, relevante Stakeholder rechtzeitig und im richtigen Ausmaß einbindet und Verantwortlichkeiten einfordert.

Außerdem obliegt es der Transformationseinheit inhaltliche und zeitliche Interdependenzen zwischen Teilprojekten zu erkennen und einen entsprechenden Austausch zu fördern. Sie fungiert als zentrale Wissensstelle in Bezug auf den

Projektfortschritt und stellt eine ausreichende Transparenz für eine faktenbasierte Entscheidungsfindung sicher.

Es obliegt der Transformationseinheit weitere notwendige Projektstrukturen, Formate und Foren zu schaffen. Für den Erfolg des Großvorhabens ist es entscheidend, dass die Transformationseinheit zügig und mit hinreichender personeller Untersetzung aufgebaut wird.

Zur Ausübung aller relevanten übergreifenden Projektmanagementtätigkeiten soll die Bund-Länder-Transformationseinheit entlang von vorerst **zehn übergreifenden Aufgabenbereichen** aufgebaut werden. Die personelle Besetzung der einzelnen Bereiche wird zwischen allen drei Federführern – BMI, Hamburg und Bayern – abgestimmt und aufgabenorientiert fortlaufend angepasst. Grundsätzlich können die Federführer Aufgaben in sämtlichen Bereichen der Transformationseinheit wahrnehmen. Eine Bereichsleitung stellt die kohärente Aufgabenwahrnehmung innerhalb des Bereiches sicher. Außerdem können die einzelnen Federführer die Wahrnehmung ihnen obliegender Aufgabenbereiche anderen staatlichen Akteuren übertragen.

Abbildung 1: Übergreifende Aufgabenbereiche der Bund-Länder-Transformationseinheit Registermodernisierung

- **Leitung der Transformationseinheit:** Zur Sicherstellung einer abgestimmten Vorgehensweise über alle zehn Aufgabenbereiche hinweg, insb. bei Aufgabenbereichen mit inhaltlichen Schnittstellen wie z. B. der Umsetzungssteuerung und dem Programmcontrolling, bedarf es einer übergreifenden Leitung und Steuerung der Transformationseinheit. Diese wird durch die Federführer des Projektes (Bayern, Hamburg, Bund) wahrgenommen. Die Federführer benennen jeweils eine Person nebst Vertretung, die diese Leitungsaufgabe wahrnimmt. Die übergreifende Leitung der Transformationseinheit ist gegenüber den einzelnen Aufgabenbereichen der Einheit fachlich weisungsbefugt.

- **Zielsetzung und Veränderungsstrategie:** Die Registermodernisierung wird über Jahre hinweg eins der prägendsten Vorhaben der Verwaltungsdigitalisierung sein. Die Ansprüche von Bürgern, Unternehmen und der Verwaltung können sich rapide ändern, heutige Technologien in fünf Jahren veraltet sein. Um sich nicht auf bestehende Strukturen und ursprüngliche Planungen zu versteifen, sondern die notwendige Offenheit für Neuerungen zu bewahren und auch nachhaltig die im Zielbild beschriebenen Nutzenversprechen zu erreichen, muss eine stetige Überprüfung und Weiterentwicklung der übergreifenden Veränderungsstrategie vorgenommen werden. Es gilt, bestehende Ansätze regelmäßig zu hinterfragen und Innovationen zu beleuchten, um relevante Trends frühzeitig zu erkennen und falls sinnhaft aufzugreifen. Außerdem sollte die übergreifende zeitliche Umsetzungsplanung aller Teilprojekte (Masterplanmanagement) regelmäßig überprüft und bei Bedarf an neue Gegebenheiten angepasst werden.
- „**Master of Ceremony" und Wissensmanagement:** Die Transformationseinheit muss durch regelmäßige zielführende Austausche der federführenden Akteure geprägt sein, um eine gesamthafte Umsetzungskoordination und -steuerung zu gewährleisten. Dafür gilt es relevante Formate innerhalb der Transformationseinheit zu etablieren sowie Möglichkeiten für eine systematische anlassbezogene Integration von weiteren Akteuren zu schaffen. Darüber hinaus sollte ein Wissensmanagementansatz entwickelt werden, um Konsistenz sicherzustellen und die interne und externe Kommunikation zu befähigen.
- **Priorisierung und Steuerung von Teilprojekten**: Der Transformationseinheit obliegt im Rahmen ihrer Zuständigkeiten (im Einvernehmen mit den jeweiligen Teilprojektverantwortlichen) die Aufgabe der zeitlichen und inhaltlichen Priorisierung von Teilprojekten der Registermodernisierung sowie die Identifikation und Beschleunigung möglicher Piloten. Es gilt zu unterscheiden zwischen 1.) Teilprojekten der Registermodernisierung, also Umsetzungsvorhaben im Sinne des Zielbildes Registermodernisierung und 2.) assoziierten Vorhaben, also inhaltlich-verwandten Vorhaben im Gesamtkontext Verwaltungsdigitalisierung, die auch im Kontext Registermodernisierung relevant sind. Die Gesamtverantwortung für den Umsetzungserfolg der Teilprojekte der Registermodernisierung (Kategorie 1) trägt in letzter Instanz als Projekteigentümer der IT-Planungsrat. Den Federführern als Projektmanagern der Gesamtsteuerung obliegt es, den Umsetzungserfolg aller Teilprojekte durch eine strategische Steuerung sowie eine operative Unterstützung sicherzustellen. Zur fortlaufenden Steuerung der Teilprojekte gilt es adäquate Steuerungswerkzeuge zu entwickeln und zu etablieren sowie eine enge Verzahnung mit dem Projektcontrolling sicherzustellen. Durch diesen Aufgabenbereich ist auch sicherzustellen, dass die im Zielbild genannten 18 „Top-Register" priorisiert modernisiert, Synergien mit OZG-Umsetzungsvorhaben, insb. in Bezug auf die Erreichung des OZG-Reifegrads 4 („Once Only") gezielt gehoben und Anforderungen

aus dem Anwendungsfall Registerzensus berücksichtigt werden. Insbesondere bei der Modernisierung der 18 „Top-Register“ sollte eine enge Verzahnung mit entsprechenden OZG-Umsetzungsprojekten (z. B. in Form von Laboren) sichergestellt werden. Durch die Verfügbarmachung von Registerdaten für relevante OZG-Leistungen im Sinne von „Once Only“ kann zügig spürbarer Mehrwert für Bürger und Unternehmen geschaffen werden. Bestehende Umsetzungsstrukturen wie z. B. die Wahrnehmung der Federführung eines OZG-Umsetzungsvorhabens durch ein Land können so für die Modernisierung entsprechender Register synergetisch genutzt werden. Innerhalb des durch die Gesamtsteuerung mittels einheitlicher Projektstandards und strategischer Vorgaben definierten Modernisierungsrahmens wird die Verantwortung für die Erreichung ihrer Projektziele weitestgehend auf die Teilprojekte der Registermodernisierung übertragen. Bei Bedarf sollen Teilprojekte anlassbezogen auch operativ unterstützt werden, z. B. wenn durch die Verzögerung eines Vorhabens eine Verzögerung oder Gefährdung anderer Teilprojekte droht. Die Steuerung der Teilprojekte erfolgt in der Regel bilateral (mit den in den Teilprojekten verantwortlichen Stellen). Es sollen jedoch auch teilprojektübergreifende Steuerungs- und Austauschformate geschaffen werden, die eine übergreifende Steuerung und Koordination ermöglichen (siehe z. B. „Projekteboard“, Kapitel 4.3). Dieser Aufgabenbereich wird durch den Federführer Bund (BMI) geleitet, der auch das neu einzurichtende „Projekteboard“ verantwortet. In das Projekteboard sollen bedarfsgerecht auch assoziierte Vorhaben (Kategorie 2) eingebunden werden, um einen konstruktiven Austausch mit relevanten, inhaltlich-verwandten Umsetzungsvorhaben sicherzustellen. Denn auch jene Vorhaben, deren Steuerung und Umsetzung nicht direkt dem Projekt „Gesamtsteuerung Registermodernisierung“ obliegen, müssen übergreifend einbezogen werden, um eine konzertierte Verwaltungsdigitalisierung und Modernisierung der deutschen Registerlandschaft zu ermöglichen. Das BVA als Registermodernisierungsbehörde soll den Aufgabenbereich operativ unterstützen.

- **Programmcontrolling, Risikomanagement und Qualitätssicherung:** Basierend auf den entwickelten übergreifenden Zielen und Veränderungsstrategien sowie den konkreten Priorisierungs- und Steuerungsmechanismen gilt es Controlling-Werkzeuge und -berichte zu erarbeiten und ein fortlaufendes Projektcontrolling zu etablieren. Im Zuge des Controllings gilt es außerdem einen Risikomanagementansatz zu entwickeln sowie eine Qualitätssicherung vorzunehmen. Durch einen regelmäßigen Abgleich von Umsetzungskonzepten und -fortschritten mit der übergreifenden Veränderungsstrategie und entsprechenden Zielen kann ein Fokus auf die Erfüllung der Nutzenversprechen der Registermodernisierung sichergestellt werden. Zur Sicherstellung einer engen Verzahnung mit dem Bereich „Priorisierung und Steuerung“ wird dieser Bereich ebenfalls vom Bund (BMI) geleitet und durch das BVA operativ unterstützt.

- **Governance des laufenden Betriebs:** Eine moderne, interoperable Registerlandschaft benötigt eine übergreifende Governance, die einen möglichst störungsfreien Betrieb der technischen Infrastruktur in ihrer Gesamtheit beim Bund, den Ländern und den Kommunen sicherstellt. Der Transformationseinheit obliegt die Definition von Strukturen, Prozessen und Werkzeugen, die einen nachhaltigen störungsfreien Betrieb ermöglichen. Dazu gehören z. B. verbindliche Prozesse im Anforderungsmanagement sowie einschlägige Service Level Agreements.
- **Kommunikation, Change-Management und Stakeholdermanagement**: Das Gesamtvorhaben Registermodernisierung bedarf einer breiten Zustimmung und eines Mitwirkens aller relevanten Stakeholder auf allen Ebenen. Um diese sicherzustellen, sollte sowohl das Vorhaben als solches als insb. auch der Mehrwert der Registermodernisierung regelmäßig und breit kommuniziert werden. Für die zielführende Mitwirkung insb. der registerführenden Stellen wird es essenziell sein, Transparenz über Anforderungen der Registermodernisierung und entsprechende Unterstützungsangebote zu schaffen. Beispielsweise bedarf es zielgruppenorientierter, auch über die Fachöffentlichkeit hinausweisender Kommunikationsformate (Bürger/ Wirtschaft/ Verwaltung) sowie einer Kontakt- und Informationsstelle („Single Point of Contact“) für Registerbehörden, Anforderungsgeber und weitere Stakeholder. Es gilt, interne und externe Kommunikationsstrategien und -konzepte zu entwickeln, relevante Inhalte aufzubereiten und adressatengerecht zu kommunizieren, z. B. durch die Erstellung von FAQs oder die Einrichtung einer Website zur Registermodernisierung. Im Sinne eines gesamthaften Change-Management-Ansatzes sollen die fortlaufenden Veränderungen der Strukturen der deutschen Registerlandschaft an die sich wandelnden Rahmenbedingungen organisationsübergreifend begleitet werden. Die Analyse der Stakeholder-Landschaft sowie die Schaffung von regelmäßigen Austauschformaten kann ein wesentlicher Treiber für den Umsetzungserfolg werden. Dieser Bereich wird durch einen Federführer geleitet und durch das BVA als Registermodernisierungsbehörde operativ unterstützt.
- **Haushaltsplanung und Finanzierung:** Zur vorrausschauenden Sicherstellung der Finanzierung des Gesamtvorhabens muss eine Aufwandsschätzung der Mittelbedarfe zur Umsetzung des Zielbildes (s. Kapitel 3.3) sowie eine koordinierte Beantragung von Haushaltsmitteln aus allen relevanten Töpfen erfolgen. Dafür soll ein durch den Federführer Bund (BMI) geleiteter Bereich – das „Finanzierungsbüro“ – innerhalb der Transformationseinheit eingerichtet werden. Diesem soll auch die Durchführung des Finanzcontrollings sowie die Berichterstattung im Zuge vom Finanzmittelerhalt obliegen.
- **Übergreifende Strukturen / Kontaktstelle Kompetenzteams:** Um eine ressort- und ebenenübergreifende Einbindung aller relevanten Akteure und Teilprojekte zu gewährleisten, bedarf es der Schaffung von übergreifenden Projektstrukturen,

Austauschformaten und Foren (s. Kapitel 4.3). Die Transformationseinheit ist zuständig für die Konzeption, Entwicklung und Etablierung relevanter übergreifender Strukturen sowie initiativen- und zeitpunktbezogener Austauschformate. Der Bereich „Übergreifende Strukturen“ ist auch Kontaktstelle der Transformationseinheit für die Teamleitungen der Kompetenzteams (s. Kapitel 4.3.) und unterstützt diese bei der Teamorganisation.

- **Gremienkoordination Registermodernisierung:** Die Transformationseinheit soll als zentrale Anlaufstelle für alle relevanten Gremien sowie Umsetzungsbeteiligte im Kontext der Registermodernisierung dienen. Um eine umfassende Einbettung in relevante Gremienstrukturen sowie die zielführende Vorbereitung, Koordination und Abstimmung im Vorfeld zu Gremiensitzung zu gewährleisten, soll eine dedizierte Gremienkoordinationsstelle eingerichtet werden. Im Zuge des Aufbaus dieses Bereiches wird auch geprüft, ob und in welchem Umfang die FITKO Aufgaben der Gremienkoordination in dem Projekt übernehmen kann.

4.2 Einbettung des Projektes „Gesamtsteuerung Registermodernisierung“ in die politische Gremienstruktur

Für den Erfolg der gesamthaften Umsetzung der Modernisierung der deutschen Registerlandschaft ist eine umfängliche und koordinierte Einbettung des Projektes „Gesamtsteuerung Registermodernisierung“ in die bestehenden Gremienstrukturen – den IT-Planungsrat (IT-PLR), die Konferenz des Chefs des Bundeskanzleramts mit den Chefinnen und Chefs der Staats- und Senatskanzleien der Länder (ChefBK/CdSK), die Fachministerkonferenzen der deutschen Länder (FMK) sowie die Ministerpräsidentenkonferenz (MPK) – unabdingbar. Nur durch die Einbindung aller relevanten Gremien und Akteure können eine ressort- und ebenenübergreifende Umsetzung sichergestellt, Legitimation erzielt und die notwendige Effizienz und Effektivität von Entscheidungsfindungsprozessen erreicht werden. Um eine zielgerichtete und kurzfristige Steuerung des Projektes zu ermöglichen, wird außerdem ein Lenkungskreis neu eingerichtet. Die Koordination aller relevanten Gremienstrukturen erfolgt über die Stelle „Gremienkoordination Registermodernisierung“ der Transformationseinheit (s. Kapitel 4.1).

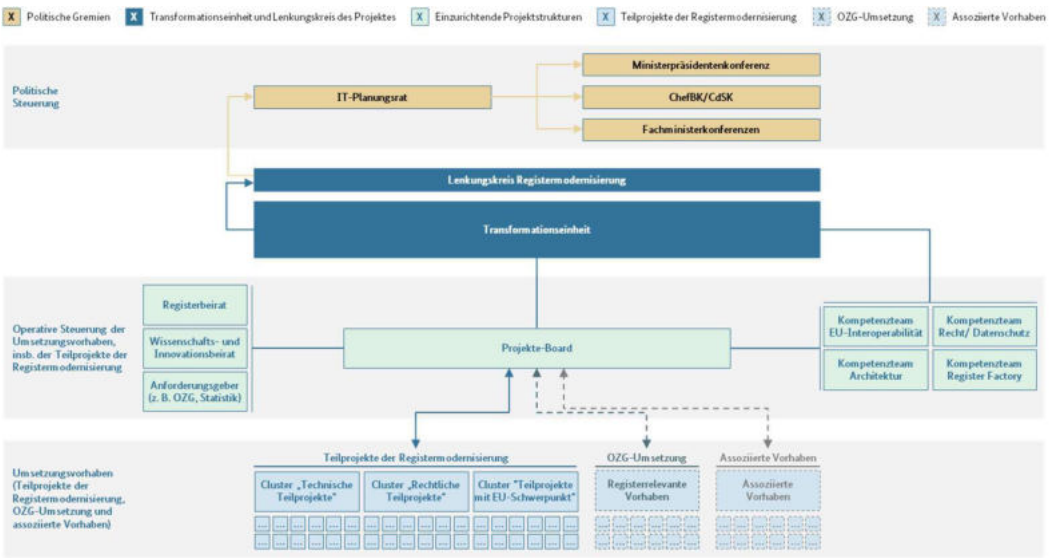


Abbildung 2: Schematische Abbildung der Projektstrukturen des Projektes „Gesamtsteuerung Registermodernisierung" (siehe auch Anhang 1)

4.2.1 Einrichtung neuer projekteigener Gremien

Die Einrichtung projekteigener Gremien dient der zielgerichteten und kurzfristigen Entscheidungsfindung sowie der regelmäßigen Kontrolle des Gesamtprojektfortschritts. Durch eine höhere Tagungsfrequenz und die Möglichkeit von anlassbezogenen Sitzungen kann eine engere Steuerung gewährleistet werden. Außerdem kann die Einbeziehung von übergreifenden Gremien wie dem IT-Planungsrat so zielgerichtet vorbereitet werden.

- **Lenkungskreis Registermodernisierung:** Gemäß dem FIT-Vorgehensmodell wird ein Lenkungskreis des Projektes eingerichtet. Im Lenkungskreis sollten auf Abteilungsleitungsebene die Federführer des Projektes (Bayern, Hamburg, Bund: BMI), der jeweilige Vorsitz des IT-Planungsrates (soweit nicht mit der Federführung identisch) sowie der Präsident des Bundesverwaltungsamtes (Register-modernisierungsbehörde) vertreten sein. Vertreter weiterer Ressorts aus Bund und Ländern sowie der Fachministerkonferenzen sind entscheidungsbezogen einzubinden. In beratender Funktion sollten Vertreter kommunaler Spitzenverbände, des BfDI und des Vorsitzes der Datenschutzkonferenz (DSK), der FITKO sowie die Leitung der Transformationseinheit und die Vorsitzenden des Registerbeirats und des Wissenschafts- und Innovationsbeirats (s. Kapitel 4.3) mitwirken. Der Lenkungskreis steuert die Transformationseinheit und die Kompetenzteams des Projektes. Gegenüber den Teilprojekten der Registermodernisierung stellt der Lenkungskreis durch Steuerungsentscheidungen sicher, dass auf Basis des Zielbildes eine auf die Realisierung der Nutzenversprechen fokussierte Umsetzung erfolgt. Hierfür definiert der Lenkungskreis beispielsweise Projektstandards für die Teilprojekte der Registermodernisierung, die dem IT-Planungsrat zur Zustimmung vorgelegt werden. Der Lenkungskreis gibt sich eine Geschäftsordnung, in der auch die Frage des Vorsitzes

geregelt wird. Das Gremium wird durch die Gremienkoordination der Transformationseinheit als Geschäftsstelle unterstützt. Der Lenkungskreis berichtet dem IT-Planungsrat und legt diesem strategische Richtungsentscheidungen zur Beschlussfassung vor. Entsprechende Beschlussvorlagen werden über die Federführer des Projektes im üblichen Verfahren in den IT-Planungsrat (Vorbefassung Abteilungsleitungsrunde) eingebracht.

- **Ggf. Einrichtung Fachgremium Registermodernisierung beim IT-Planungsrat**: Im Zuge des Aufbaus der Projektstrukturen ist zu prüfen, inwieweit auch die Einrichtung eines Fachgremiums „Registermodernisierung" beim IT-Planungsrat angezeigt ist. Das Gremium könnte der kontinuierlichen Einbindung der Länder auf Arbeitsebene sowie ggf. auch der Fachministerkonferenzen dienen. Der Lenkungskreis Registermodernisierung wird dem IT-Planungsrat über die Federführer zum Ergebnis der Prüfung berichten und ggf. einen Vorschlag zur Einrichtung eines solchen Gremiums unterbreiten.

4.2.2 Einbettung in bestehende Gremienstrukturen

Die Einbettung der Projektstrukturen in die bestehenden Gremienstrukturen soll insbesondere die Einbeziehung aller relevanten Akteure gewährleisten – sowohl ressortübergreifend als auch über alle föderalen Ebenen hinweg. Die Registermodernisierung wird in Deutschland über Jahre hinweg eines der bedeutendsten Vorhaben im Gesamtkontext Verwaltungsdigitalisierung sein, weshalb die Sicherstellung einer Kenntnis bei relevanten Akteuren sowie die durch sie ausgesprochene Legitimation von zentraler Bedeutung sein wird.

- **IT-Planungsrat**: Dem IT-Planungsrat als Auftraggeber des Projektes „Gesamtsteuerung Registermodernisierung" obliegen die Grundsatzentscheidungen, wie u. a. der Beschluss über die Struktur des Projektes und die Benennung der verschiedenen Beteiligten inklusive ihrer Verantwortlichkeiten und Entscheidungsbefugnisse. Der IT-Planungsrat entscheidet sowohl über wichtige Richtungsentscheidungen als auch über die Festlegungen von wesentlichen Standards. Außerdem beschließt er über die jeweiligen Zwischenergebnisse. Es ist beabsichtigt, dem IT-Planungsrat durch die Einführung eines regelmäßigen Tagesordnungspunktes bei seinen Sitzungen über den Umsetzungsstand zu berichten.
- **Konferenz des Chefs des Bundeskanzleramts mit den Chefinnen und Chefs der Staats- und Senatskanzleien der Länder (ChefBK/CdSK)**: Der IT-Planungsrat bezieht die Besprechung ChefBK/CdSK bei wesentlichen Richtungsentscheidungen übergeordneter Natur mit ein, um eine erweiterte politische Legitimation im Bund-Länder-Kontext ressort- und ebenenübergreifend herbeizuführen. Dadurch werden die Entscheidungen zum Projekt „Gesamtsteuerung Registermodernisierung" auf eine breite Basis gestellt.

- **Fachministerkonferenzen (FMK)**: Viele FMK haben Digitalisierungsstrategien für ihren jeweiligen Zuständigkeitsbereich entwickelt und in länderübergreifenden Informationsverbünden umgesetzt. Da der Anschluss dieser Informationsverbünde an die neu zu errichtende fachübergreifende Once-Only-Architektur geplant und umgesetzt werden muss, ist die Einbeziehung der FMK für den Erfolg der Registermodernisierung unverzichtbar. Dafür werden von den FMK benannte Vertreter auf Arbeitsebene direkt in die Kompetenzteams und das Projekteboard eingebunden, sodass bereits auf dieser Ebene eine fachliche Begleitung und Absicherung der Entscheidungen erfolgt. Die Gremienkoordination der Transformationseinheit trägt daneben dafür Sorge, dass die FMK über den IT-Planungsrat auch auf Leitungs- bzw. Vorsitzebene beteiligt werden, sofern politisch relevante Entscheidungen in den Zuständigkeitsbereich einer oder mehrerer FMK fallen. Entscheidungen der Fachministerkonferenzen werden im Vorfeld strategischer Richtungsentscheidungen des Projektes eingeholt.
- **Ministerpräsidentenkonferenzen (MPK)**: Die Ministerpräsidentenkonferenz wird bei Entscheidungen übergeordneter Natur beteiligt, sofern eine politische Entscheidung auf oberster Ebene erforderlich ist. In der MPK sollen Richtungsentscheidungen von überragender strategischer Bedeutung für die Registermodernisierung in Deutschland getroffen werden.

4.3 Einrichtung weiterer Projektstrukturen

Um eine koordinierte Umsetzung aller relevanten Vorhaben sicherzustellen, wird es nicht reichen, eine zentrale Transformationseinheit ins Leben zu rufen und relevante Gremien einzubinden. Es bedarf der Schaffung von übergreifenden Projektstrukturen, Austauschformaten und Foren für Teilprojekte der Registermodernisierung, assoziierten Vorhaben im Gesamtkontext Verwaltungsdigitalisierung, sowie weitere relevante und interessierte Stakeholder. Solche Strukturen, Formate und Foren können mannigfaltige Funktionen erfüllen – z. B. die Förderung von Informations-, Erfahrungs- und Wissensaustausch, den Zufluss von innovativen und neuartigen Ideen, die Identifikation und Hebung von Synergien, die Nutzung von vorhandener Expertise sowie auch die Möglichkeit direkter und indirekter Steuerung von Vorhaben durch die Nutzung von Controlling-Werkzeugen und die Schaffung von Transparenz. Die avisierten Strukturen sind explizit als Angebot für Akteure gedacht, die an der Umsetzung von Teilprojekten der Registermodernisierung beteiligt oder von ihr betroffen sind. Im weiteren Projektverlauf sollen die Strukturen evaluiert und weiterentwickelt sowie um weitere vielversprechende Formate ergänzt werden. In einem ersten Schritt gilt es die Kompetenzteams EU-Interoperabilität, Architektur, Register Factory und Recht/ Datenschutz, das Projekteboard, den Registerbeirat sowie den Wissenschafts- und Innovationsbeirat zu konzipieren und zu etablieren.

- **Kompetenzteam EU-Interoperabilität (Art. 14 SDG-VO[6]):** Die Umsetzung des Zielbildes Registermodernisierung wird auch von europäischen Anforderungen und Synergiepotentialen geprägt. Das Kompetenzteam begleitet die Teilprojekte der Registermodernisierung dabei, die auf europäischer Ebene entwickelten Interoperabilitätsanforderungen zu erfüllen. Insbesondere begleitet das Kompetenzteam die Umsetzung des Art. 14 SDG-VO, der die Mitgliedstaaten verpflichtet, die Anschlussfähigkeit an ein europäisches System zur Umsetzung des Once-Only-Prinzips sicherzustellen (sog. „Once-Only-Technical-System"[7]). Im Auftrag des nationalen SDG-Koordinators und unter Beteiligung der Bundesressorts, der SDG-Koordinatoren der Länder sowie des Registerbeirats klärt das Kompetenzteam relevante Architektur- und Rechtsfragen unter anlassbezogener Beteiligung der Kompetenzteams Architektur und Recht/ Datenschutz. Die FITKO wird beteiligt. Somit unterstützt das Kompetenzteam den nationalen SDG-Koordinator bei der Wahrnehmung seiner Aufgaben. Zugleich unterstützt das Kompetenzteam zuständige Stellen dabei, die Vertretung deutscher Interessen im Bereich der Register in Partizipationsformaten auf EU-Ebene sicherzustellen. Das Kompetenzteam behält den Überblick über europäische Interoperabilitätsinitiativen und Projekte im Bereich Register-modernisierung (z. B. „Once Only Large Scale Pilot DE4A"), trägt zur Netzwerkbildung und zum Praxisaustausch auf europäischer Ebene bei und vermittelt den Teilprojekten Ansprechpartner auf EU-Ebene oder in anderen Mitgliedstaaten. Damit kann Deutschland die Erfahrungen und innovativen Ansätzen anderer Mitgliedstaaten berücksichtigen und zugleich aktiv zur europäischen Interoperabilitätsbeförderung beitragen.
- **Kompetenzteam Architektur**: Im Kompetenzteam Architektur werden die verschiedenen Aspekte der technischen Architektur des neu zu errichtenden Systems für die Umsetzung von „Once Only" zusammengeführt. Das Kompetenzteam sichert deren Konsistenz im Gesamtzusammenhang und bereitet Beschlussvorlagen für die Entscheidungsgremien des Projektes vor. Verbindliche Rahmenbedingungen sind neben dem Zielbild das RegMoG und Art. 14 der SDG-Verordnung. Bestehende Produkte und Standards des IT-Planungsrats sollen vorrangig verwendet und bei Bedarf sinnvoll ergänzt bzw. angepasst werden. Das Kompetenzteam formuliert Anforderungen an die Governance für Betriebsaspekte des technischen Systems. Es wird durch das BVA als Registermodernisierungsbehörde organisiert Die FITKO wird eingebunden. Das BVA wird durch die KoSIT insbesondere im Bereich europäischer Anforderungen (u. a. Europäischer Interoperabilitätsrahmen (EIF), SDG-VO) sowie der

[6] VERORDNUNG (EU) 2018/1724 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012, Single Digital Gateway-Verordnung, siehe unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018R1724&from=EN (zuletzt abgerufen am 02.12.2020).

[7] Die technischen und operativen Spezifikationen des technischen Systems legt die Kommission in einer Durchführungsverordnung auf Grundlage von Art. 14 Abs. 9 SDG-VO bis zum 21.06.21 fest.

Implikationen des RegMoG (u. a. konsistente Weiterentwicklung des XÖV-Rahmenwerks) unterstützt. Die Beteiligung weiterer Stellen ist bedarfsgerecht zu klären, wobei eine personelle Kontinuität von hoher Relevanz ist.

- **Kompetenzteam Register Factory:** Die Register Factory ist ein in der Praxis bewährter Standard des BVA zur effizienten Bereitstellung von Registern. Sie basiert auf einer leistungsfähigen, offenen Architekturplattform und umfasst standardisierte Konzepte, Bausteine und Werkzeuge für alle typischen Anforderungen an ein Register. Bei der Bereitstellung eines neuen Registers können diese vorgefertigten Elemente angepasst und in eine standardisierte Plattform integriert werden, sodass lediglich fachspezifische Anforderungen neu zu entwickeln sind. Dadurch können Register deutlich schneller und wirtschaftlicher umgesetzt werden. Die Register Factory wurde bereits durch andere Behörden erfolgreich eingesetzt und steht in weiten Teilen auch als Open-Source-Lösung zur Verfügung. Um die Bereitstellung neuer Register zu unterstützen und langfristig die technologische Heterogenität der Registerlandschaft zu reduzieren, soll die Register Factory an das neu zu errichtende System für „Once Only“ angepasst und ihre Nutzung erleichtert werden. Dabei sollen sowohl Anforderungen aus der Registermodernisierung als auch aus der Umsetzung des Onlinezugangsgesetzes Beachtung finden. Das Kompetenzteam soll die Anforderungen für die Weiterentwicklung und breitere Nutzung der Register Factory erheben und in die Umsetzung bringen sowie ein Beratungs- und Unterstützungsangebot für interessierte registerführende Stellen bereitstellen.
- **Kompetenzteam Recht/ Datenschutz:** Das neu einzurichtende Kompetenzteam Recht/ Datenschutz soll im Projekt „Gesamtsteuerung Registermodernisierung“ als zentrale Anlaufstelle für rechtliche Fragen fungieren. Kerntätigkeit ist die Zurverfügungstellung von rechtlicher Expertise und die Unterstützung von Umsetzungsprojekten. Das Kompetenzteam Recht/ Datenschutz besteht aus einem festen „Kernteam Recht“, dessen Leitung sich aus den Federführern zusammensetzt. Das Kernteam übernimmt die dauerhafte Organisation und Verwaltung bei der Beantwortung von Rechtsfragen, legt das Verfahren fest und steht im regelmäßigen Austausch mit der Steuerung der Transformationseinheit. Eine ressortübergreifende Expertenrunde wird zur Beantwortung der jeweiligen Frage oder eines Fragenkomplexes vom Kernteam einberufen. Bei Fragen mit datenschutzrechtlichem Schwerpunkt sind zum Beispiel der BfDI und die DSK beratend einzubinden. Die Ergebnisse werden regelmäßig dem Lenkungskreis Registermodernisierung vorgelegt, der auch über die Vorlage bei weiteren betroffenen Gremien (IT-PLR, FMK, u.a.) entscheidet.
- **Projekteboard**: Das von der Transformationseinheit einzurichtende Projekteboard soll primär als regelmäßiges Steuerungs- und Austauschformat für die Teilprojekte der Registermodernisierung dienen. Es soll den Teilprojekten einen niedrigschwelligen Raum für Impulse, Innovationen und interdisziplinären Austausch bieten. Daneben

dient es der Transformationseinheit auch zur Herstellung von Transparenz über den Projektfortschritt sowie der Identifikation von Abhängigkeiten mit anderen Teilprojekten. Die Detailprozesse der Steuerung der Projekte durch die Transformationseinheit und das Projekteboard sind noch festzulegen. Als institutionalisiertes Format soll das Projektboard der Transformationseinheit auch dazu dienen, übergreifende strategische Steuerungsentscheidungen zu kommunizieren und mit den Teilprojekten zu diskutieren. So sollen z. B. die von der Transformationseinheit im Einvernehmen mit dem IT-Planungsrat zu definierenden Projektstandards im Projekteboard vermittelt und nachgehalten werden. Die Teilprojekte der Registermodernisierung werden durch das Projekteboard durch die Transformationseinheit, die Kompetenzteams sowie die Beiräte (Registerbeirat, Wissenschafts- und Innovationsbeirat) mit Expertise, Entscheidungsherbeiführung bei teilprojektübergreifenden Aspekten der Registermodernisierung (Gremienkoordination) sowie bedarfsgerechten Unterstützungsangeboten begleitet. Auch Anforderungsgeber wie das OZG und die amtliche Statistik (z. B. im Zuge der Umsetzung des Registerzensus) sowie weitere assoziierte Vorhaben, die im Gesamtkontext Verwaltungsdigitalisierung Schnittstellen zur Registermodernisierung haben, sollen bedarfsgerecht eingebunden werden und am Austausch teilhaben. Bei großen inhaltlichen Überschneidungen, wie insb. bei der Umsetzung des Onlinezugangsgesetzes, soll eine regelmäßige Teilnahme relevanter Umsetzungsvorhaben sichergestellt werden. Die Teilprojekte der Registermodernisierung sollen im weiteren Projektverlauf – z. B. analog zu den im Zielbild Registermodernisierung benannten zentralen Elementen – in Kategorien bzw. Cluster eingeteilt werden. Zunächst sollen die Cluster „Technische Teilprojekte“ (u. a. technische Architektur und Register, insb. (Weiter-) Entwicklung der im Zielbild genannten technischen Komponenten sowie der 18 „Top-Register“), „Rechtliche Teilprojekte“ (u. a. Gesetzgebungsverfahren und fachrechtliche Regelungen) sowie „Teilprojekte mit EU-Schwerpunkt“ (insb. übergreifende Umsetzung Art. 14 SDG-VO und grenzüberschreitende Angelegenheiten) gebildet werden. Aus ihrer Zugehörigkeit zu einem Cluster folgt, von welchem Bereich der Transformationseinheit bzw. von welchem Kompetenzteam ein Teilprojekt federführend begleitet wird. Außerdem können Steuerungs- und Austauschformate durch die Bildung von thematischen Clustern bedarfsgerechter gestaltet werden. So soll das Projekteboard ein Forum bieten für verschiedene standardisierte und anlassbezogene Formate. Als standardisierte Formate sollen z. B. ein Komponentenboard und eine Registerwerkbank (beide Cluster Technik), europäische Netzwerk-Sessions (Cluster EU-Angelegenheiten) sowie regelmäßige Innovationssprints und interdisziplinäre Labore (beide Cluster-übergreifend) angeboten werden. Die Detaillierung, Formalisierung und Institutionalisierung der Steuerungs- und Austauschformate hat im weiteren Projektverlauf zu erfolgen. Über die Zuordnung der Teilprojekte entscheidet der

Lenkungskreis im Einvernehmen mit dem jeweiligen Projektauftraggeber (z. B. Bundes- oder Landesressort). Dem IT-Planungsrat wird regelmäßig darüber berichtet, welche Projekte durch die Gesamtsteuerung gesteuert werden und welche assoziierten Vorhaben koordinierend begleitet werden.

- **Registerbeirat:** Die Umsetzung der mit dem Gesamtvorhaben verbundenen Veränderungen wird die registerführenden Stellen vor erhebliche Herausforderungen stellen. Daher ist es im Sinne der Kommunikation sowie des Wissens- und Veränderungsmanagements wichtig, sie von vornherein in das Vorhaben einzubeziehen und ihnen eine „Stimme" zu geben. Gleichzeitig ist eine Beratung durch die registerführenden Stellen unverzichtbar, um Anforderungen und Handlungsalternativen zu bewerten sowie gut und schnell umsetzbare Lösungsalternativen zu ermitteln. Der Registerbeirat soll diese Aufgabe als unabhängiges Gremium wahrnehmen, das Register aus der Bundes- und Landesverwaltung, dem kommunalen Bereich sowie weiterer betroffener Körperschaften repräsentiert. Der Vorsitz wird gewählt. Der Registerbeirat nimmt am Projekteboard teil und tagt vierteljährlich, bei Bedarf anlassbezogen. Er bestimmt die Themen selbst, berät zu an ihn adressierten Fragestellungen und kann auch zu weiteren operativen und strategischen Anliegen der Registermodernisierung Position beziehen.
- **Wissenschafts- und Innovationsbeirat**: Der Wissenschafts- und Innovationsbeirat berät den Lenkungskreis und die Transformationseinheit als unabhängiges Gremium und bringt Erkenntnisse aus der Wissenschaft, Forschung und Wirtschaft ein. Die konkrete Benennung von „Akteuren aus Wissenschaft, Forschung und Wirtschaft" erfolgt durch den Lenkungskreis in Abstimmung mit dem Bundesministerium für Bildung und Forschung (BMBF) und dem Bundesministerium für Wirtschaft und Energie (BMWi). Die Anzahl der Mitglieder beträgt ca. 12 und ist interdisziplinär und divers aufgestellt (Sachverstand diverser Fachrichtungen aus Wissenschaft und Praxis durch Akteure aus der freien Wirtschaft, Start-Ups, Innovatoren, etc.). Der Vorsitz wird gewählt. Der Wissenschafts- und Innovationsbeirat nimmt am Projekteboard teil und tagt vierteljährlich, bei Bedarf anlassbezogen. Er bestimmt die Themen selbst, gibt im Projekteboard umsetzungsbefördernde Impulse und kann auch zu weiteren operativen und strategischen Anliegen der Registermodernisierung Position beziehen. Er soll Innovationspotentiale erkennen und fördern und ist an der Schnittstelle zwischen den Teilprojekten der Registermodernisierung und assoziierten Vorhaben angesiedelt.

5. Ausblick auf Weiterentwicklung des Projektes „Gesamtsteuerung Registermodernisierung"

Der hiermit vorgelegte Vorschlag zum Aufbau der Kernstrukturen des Projektes „Gesamtsteuerung Registermodernisierung" unter dem Dach des IT-Planungsrates soll einen zügigen und zielgerichteten Start der ganzheitlichen Umsetzung der

Registermodernisierung ermöglichen und so zu einer schnellen Generierung von spürbarem Nutzen im Sinne des Zielbild beitragen. Das Gesamtvorhaben Registermodernisierung ist durch eine Vielzahl von Teilprojekten mit unterschiedlichen Zeitschienen und Wirkungskreisen geprägt – die Anforderungen an übergreifende Steuerungsstrukturen werden sich im Laufe der Jahre wandeln und müssen stetig evaluiert und bei Bedarf angepasst werden. Dieser Vorschlag soll also auch den Grundstein legen für eine bedarfsgerechte Weiterentwicklung der Strukturen unter Berücksichtigung aller relevanten Akteure und den sich wandelnden Anforderungen an die Registermodernisierung. Die Einführung der Bund-Länder-Transformationseinheit soll dabei eine ressort- und ebenenübergreifende Perspektive gewährleisten. Wie im Zielbild Registermodernisierung beschrieben, sollen die Projektstrukturen außerdem langfristig in eine nachhaltige Governance der deutschen Registerlandschaft überführt werden. Die hierin beschriebenen Gremien und Strukturen sollen in Summe sicherstellen, dass dabei auch langfristig alle relevanten Perspektiven betrachtet werden.

Anhang

Anhang 1: Schematische Abbildung der Projektstrukturen des Projektes „Gesamtsteuerung Registermodernisierung“

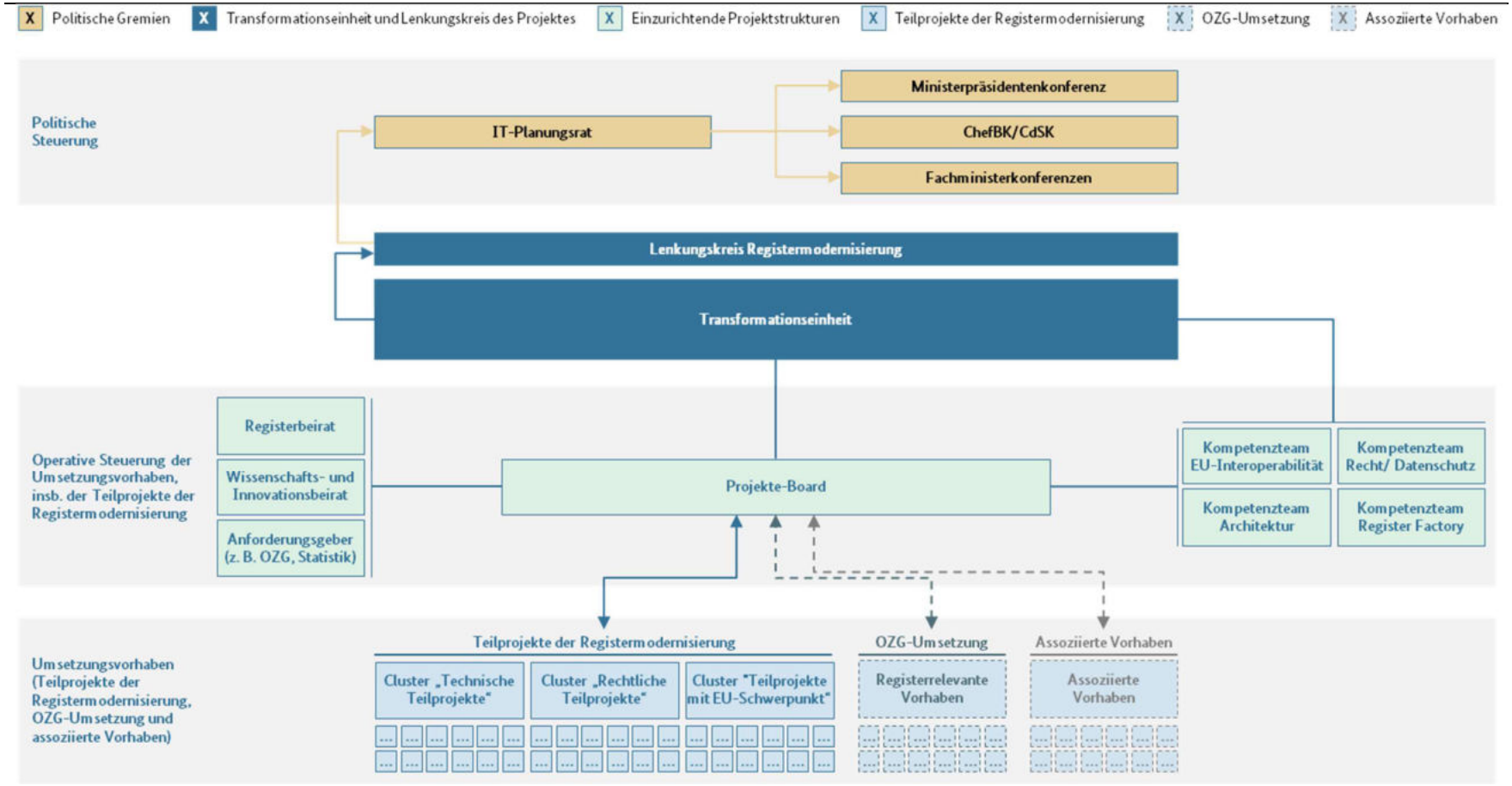


Abbildung 3: Schematische Abbildung der Projektstrukturen des Projektes „Gesamtsteuerung Registermodernisierung" (Großabbildung)

Abkürzungsverzeichnis

BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BMBF	Bundesministerium für Bildung und Forschung
BMI	Bundesministerium des Innern, für Bau und Heimat
BMWi	Bundesministerium für Wirtschaft und Energie
Destatis	Statistisches Bundesamt
DSK	Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder / „Datenschutzkonferenz“
DVDV	Deutsches Verwaltungsdiensteverzeichnis
EU	Europäische Union
EUR	Euro
FITKO	Föderale IT-Kooperation
FMK	Fachministerkonferenzen
IDNrG	Identifikationsnummerngesetz
IT	Informationstechnik
IT-PLR	IT-Planungsrat
KoSIT	Koordinierungsstelle für IT-Standards
Mio.	Millionen
Mrd.	Milliarden
MPK	Ministerpräsidentenkonferenz
NKR	Nationaler Normenkontrollrat
OZG	Onlinezugangsgesetz
RegMoG	Registermodernisierungsgesetz
SDG	Single Digital Gateway
SDG-VO	Single-Digital-Gateway-Verordnung

Abbildungsverzeichnis

Projekt „Gesamtsteuerung Registermodernisierung“: Bericht zum Umsetzungsstand

Oktober 2021

Inhaltsverzeichnis

Kernbotschaften

Der IT-Planungsrat hat am 17. März 2021 das vom Koordinierungsprojekt Registermodernisierung erarbeitete Zielbild der Registermodernisierung beschlossen. Um eine konzertierte Umsetzung der Registermodernisierung zu ermöglichen, wurde im IT-Planungsrat im Juni 2021 die Einrichtung des Projektes „Gesamtsteuerung Registermodernisierung" beschlossen. Unter Federführung des Bundes (Bundesministerium des Innern, für Bau und Heimat (BMI)) sowie der Länder Baden-Württemberg, Bayern, Hamburg und Nordrhein-Westfalen soll im Rahmen eines übergreifenden Programmmanagements die Umsetzung aller Teilprojekte der Registermodernisierung vorangetrieben werden.

Mit der Aufnahme der neuen Federführer Baden-Württemberg und Nordrhein-Westfalen ist das Steuerungsprojekt erfolgreich gestartet und in die inhaltliche Arbeit eingestiegen:

- Definition konkreter Ziele 2021 zur Aufnahme der Arbeit in den Bereichen Architektur, Weiterentwicklung von Registern, rechtliche Grundlagen und Governance (Kontroll- und Steuerungsstrukturen)
- Aufbau der Steuerungsprojekte mit Fokus auf Etablierung der Transformationseinheit, Aufbau der Kompetenzteams sowie Aufsetzen des Lenkungskreises und Projekteboards
- Definition bereits laufender Teilprojekte und assoziierter Vorhaben zur Integration in das Gesamtprogramm zur Registermodernisierung
- Identifikation konkreter Pilotvorhaben zur Erprobung der Zielarchitektur der Registermodernisierung und Evaluierung weiterer möglicher Piloten
- Integration der nationalen Umsetzung von Art. 14 der SDG-VO in die Gesamtsteuerung Registermodernisierung, u.a. durch Aufbau des Kompetenzteams EU-Interoperabilität unter Federführung der KoSIT

Um die Gesamtsteuerung des Projektes sicherzustellen, sind erforderliche Ressourcen auf Seiten der Federführer und Unterstützer vorzusehen. Gemäß Beschluss 2021/25 des IT-Planungsrates soll hierfür ein Budget zur Programmsteuerung vorgesehen werden. Die mit dem Aufbau und Betrieb der Gesamtsteuerung verbundenen Aufwände werden derzeit im Kreis der Federführer geschätzt und validiert. Die entsprechende Finanzierung für die Aufwände der Gesamtsteuerung der Registermodernisierung für 2021 und 2022 soll aus vorhandenen Mitteln des Digitalisierungsbudgets erfolgen. Eine validierte und begründete Übersicht der anfallenden Aufwände ist im nächsten Schritt

durch die Federführer zu erstellen und ein entsprechender Projektantrag bei der FITKO einzureichen.

Insgesamt fallen für die Umsetzung der Registermodernisierung als Gesamtvorhaben auf Ebene Bund, Länder und Kommunen zudem erhebliche Aufwände – erste Schätzungen beziffern diese auf ca. 2,9 Mrd. € – an, die über die reine Umsetzung der Anforderungen des RegMoG hinausgehen. Um Bund und Länder auch bei der Haushaltsvorsorge hinsichtlich dieser Aufwände zu unterstützen, wurde ein erstes Aufwandsschätzmodell (ASM) entwickelt, das im nächsten Schritt im Bund-Länder-Kreis unter Einbeziehung kommunaler Expertise weiter zu validieren ist.

1. Kontext

Mit dem im März 2021 vom IT-Planungsrat beschlossenen Zielbild der Registermodernisierung und dem im Mai 2021 vom IT-Planungsrat eingerichteten Projekt „Gesamtsteuerung Registermodernisierung“ unter Federführung des Bundes (BMI) sowie der Länder Baden-Württemberg, Bayern, Hamburg und Nordrhein-Westfalen wurden wesentliche Grundlagen für eine konzertierte Umsetzung der Registermodernisierung gelegt.

Nachstehend wird der aktuelle Umsetzungsstand des Vorhabens dargelegt sowie wesentliche Eckpfeiler mit Bezug auf die Aktivitäten bis Jahresende sowie die Schritte zur Validierung einer Schätzung des Finanzierungsbedarfs umrissen.

2. Umsetzungsstand Projekt „Gesamtsteuerung Registermodernisierung“

Das Projekt „Gesamtsteuerung Registermodernisierung“ strebt im Sinne eines übergreifenden Programmmanagements an, die im Zielbild beschriebene ressort- und ebenenübergreifende Umsetzung aller Teilprojekte der Registermodernisierung konzertiert voranzubringen. Unter Federführung des BMI sowie der Länder Baden-Württemberg, Bayern, Hamburg und Nordrhein-Westfalen stellt die Gesamtsteuerung die Realisierung des Zielbildes sicher. Der aktuelle Projektstand wird im Nachfolgenden vorgestellt.

2.1 Projektziele 2021

Den Kern des Gesamtprogramms bilden die vier im Zielbild Registermodernisierung beschriebenen Elemente: 1) eine interoperable und sichere technische Architektur, 2) anschlussfähige Register auf Seiten der registerführenden Stellen, 3) rechtliche Rahmenbedingungen für einen sicheren und datenschutzkonformen Datenaustausch, sowie 4) eine zukunftsweisende Governance (Kontroll- und Steuerungsstrukturen im laufenden Betrieb). Um ein zielgerichtetes Vorgehen zum Start der Umsetzung des Zielbildes Registermodernisierung sicherzustellen wurden die wesentlichen Ziele für 2021 und eine arbeitsteilige Aufgabenwahrnehmung unter den Federführern bis Jahresende definiert. Die Ziele orientieren sich dabei an den vier Säulen des Zielbildes, welche durch eine zusätzliche übergreifende Dimension ergänzt werden.

Die Ziele werden jeweils im Tandem aus Bund (BMI) und einem der federführenden Länder verantwortet. Zudem unterstützen die Koordinierungsstelle für IT-Standards (KoSIT) sowie das Bundesverwaltungsamt (BVA) als Registermodernisierungsbehörde die Arbeit, beispielsweise durch die Übernahme der Leitung einzelner Kompetenzteams (vgl. 3.3.1). Je Ziel wurden konkrete Schritte definiert, die durch die verantwortlichen Federführer und operativ durch die Kompetenzteams bearbeitet werden.

Durch die seitens der Federführer initiierten Maßnahmen sollen insbesondere bei den folgenden Schwerpunkten des Zielbildes wesentliche Fortschritte erzielt werden:

- **Architektur:** Initiierung eines Validierungsprozesses zum Architekturzielbild der Registermodernisierung inklusive der Rollen und dem Zusammenspiel der Komponenten auf Basis erster Pilotierungserfahrungen, Initiierung der Umsetzung von Komponenten sowie Definition des Vorgehens zur Anbindung an das europäische Once-Only-Technical-System (OOTS)
- **Weiterentwicklung von Registern:** Definition des Vorgehens und Grobplanung der Weiterentwicklung von Registern (Einspielung Identifikationsnummer, Anschluss an Once-Only-Komponenten und weiterführende Modernisierung von Registern) sowie Erprobungsaktivitäten bei ausgewählten Top-18-Registern
- **Rechtliche Grundlagen:** Klärung rechtlicher Fragestellungen im Zusammenhang mit dem OOTS, rechtliche Begleitung des Pilotvorhabens im Melderecht sowie Entwicklung eines Vorgehensmodells zum ressort- und länderübergreifenden Screening von Rechtsänderungsbedarfen mit Blick auf Once-Only im Fachrecht
- **Governance:** Etablierung der Steuerungsstrukturen des Projektes inkl. der Teilprojekte sowie Aufbau des übergreifenden Programmcontrollings
- **Übergreifend:** Abschätzung des Finanzierungsbedarfs für den Aufbau und Betrieb des Steuerungsprojektes sowie Validierung eines Aufwandsschätzmodells zur Ermittlung der Gesamt-Finanzierungsbedarfe im Bereich Registermodernisierung, übergreifende Kommunikation und Stakeholdermanagement, Etablierung eines vernetzten Wissensmanagements, Erstellung eines Grobkonzepts zur Registerlandkarte sowie Identifizierung von Schnittstellen und Betroffenheiten zwischen der Registermodernisierung und SDG sowie OZG

2.2 Aufbau von Steuerungsstrukturen

Die im 35. IT-PLR beschlossenen Projektstrukturen werden derzeit aktiv durch das Steuerungsprojekt etabliert.

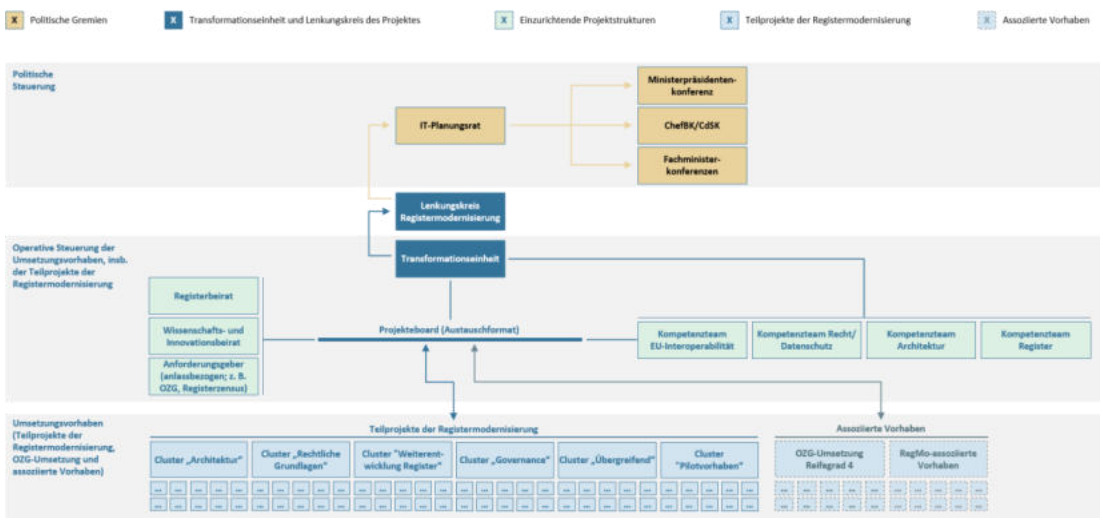


Abbildung 1: Schematische Abbildung der Projektstrukturen des Projektes „Gesamtsteuerung Registermodernisierung" (siehe auch Anhang 1)

Im Kern des Projektes „Gesamtsteuerung Registermodernisierung" steht die **Bund-Länder-Transformationseinheit**, welche die übergreifende Programmsteuerung wahrnimmt. Die Transformationseinheit fand sich im Juli 2021 erstmalig unter Beteiligung aller Federführer im Rahmen einer Auftaktveranstaltung zusammen und tagt seither kontinuierlich im 2-wöchigen Rhythmus. Im Rahmen der vereinbarten Aufgabenbereiche wurde zudem die inhaltliche Arbeit an konkreten Zielen in einem Tandem BMI und federführendem Land begonnen (z.B. im Bereich Governance, Kommunikation). Für das übergreifende Programmcontrolling, das operativ durch das BVA unterstützt wird, liegt ein erstes Konzept vor. Dieses wird derzeit operationalisiert und hiernach in ein kontinuierliches Programmcontrolling überführt.

Als Gremium für übergreifende Programmentscheidungen wird zudem der **Lenkungskreis Registermodernisierung** aufgebaut. Die konstituierende Sitzung des Lenkungskreises ist nach erfolgter Benennung der stimmberechtigten und beratenden Mitglieder für den Oktober 2021 geplant. Ein erstes Vorbereitungstreffen der stimmberechtigten Mitglieder soll im September 2021 stattfinden.

Das **Projekteboard** wird als zentrale Austauschplattform für die Teilprojekte der Registermodernisierung etabliert. Im ersten Schritt wurden hierzu bereits laufende Teilprojekte und assoziierte Vorhaben der Registermodernisierung identifiziert, die zu einem ersten Auftakt voraussichtlich im September eingeladen werden (vgl. 3.3.2). In einem weiteren Schritt wird das Format des Projekteboards verstetigt und das Vorgehen zum Anschluss bereits identifizierter Teilprojekte in das Programmmanagement definiert. Die Liste bestehender Teilprojekte wird nach erfolgter Finalisierung durch den Lenkungskreis

in seiner konstituierenden Sitzung beschlossen sowie dem IT-PLR in seiner nächsten Sitzung vorgelegt.

Um eine koordinierte Umsetzung aller relevanten Vorhaben sicherzustellen und fachliche Expertise zu übergreifenden Fragestellungen der Registermodernisierung zu bündeln, werden vier **Kompetenzteams** (KT) aufgebaut: das KT EU-Interoperabilität unter Leitung der KoSIT, das KT Architektur unter der Leitung des BVA, das KT Recht/ Datenschutz unter der Leitung des BMI und des Landes Bayern, sowie das KT Register unter der Leitung des BVA.

2.3 Integration der Teilprojekte

Auf Bundes- und Landesebene sind bereits viele Vorhaben in der Umsetzung, die einen Beitrag zur Umsetzung des Zielbildes Registermodernisierung erbringen und in das Gesamtprogramm integriert werden sollen. Hierzu wurden in einem ersten Schritt bereits laufende Teilprojekte sowie assoziierte Vorhaben identifiziert, die direkte Bezugspunkte zur Umsetzung des Zielbilds der Registermodernisierung aufweisen oder eine inhaltlich relevante Schnittstelle zum Gesamtprogramm darstellen. Im Rahmen einer ersten Auftaktveranstaltung des Projekteboards werden diese Teilprojekte und Vorhaben im nächsten Schritt zu einem übergreifenden Austausch eingeladen (vgl. 2.1).

In einem nächsten Schritt erfolgt die Definition des Vorgehens zum Anschluss der laufenden Teilprojekte an das Gesamtprogramm. Damit ist auch die Aufnahme eines kontinuierlichen Programmcontrollings verbunden. Auf dieser Basis wird Transparenz hergestellt, wie sich die Teilprojekte in die Umsetzungsplanung des Zielbildes Registermodernisierung einfügen. Ausgehend vom Zielbild der Registermodernisierung erfolgt zudem eine Ableitung, welche zusätzlichen Teilprojekte für eine erfolgreiche Umsetzung noch zu initiieren und in das Gesamtprogramm zu integrieren sind.

2.4 Pilotierungsvorhaben

Um frühzeitig erste Erfahrungen zur praktischen Umsetzung des Zielbildes der Registermodernisierung zu erhalten, werden im Rahmen von Pilotierungsvorhaben einzelne Komponenten der Once-Only-Datenkette konkret erprobt. Die Erkenntnisse aus den Piloten zahlen dabei auf drei wesentliche Bereiche ein: (1) Umsetzung relevanter Leistungen des Onlinezugangsgesetzes im Reifegrad 4, (2) Umsetzungsvorbereitung des RegMoG mit Blick auf den Aufbau des Basisdatenregisters und die Einspeicherung der einheitlichen

Identifikationsnummer sowie (3) Validierung der Once-Only-Architektur und somit des Zielbildes der Registermodernisierung.

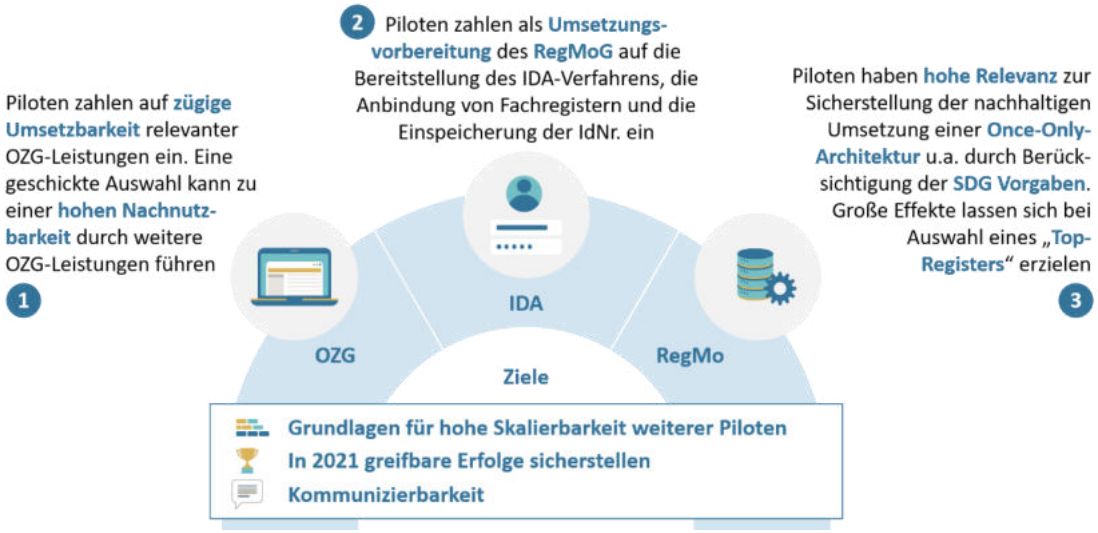


Abbildung 2: Zielsetzung der Pilotvorhaben der Registermodernisierung (siehe auch Anhang 2)

Um dieses zu erreichen, wurden drei Module definiert, die im Rahmen der Pilotvorhaben adressiert werden sollen:

1) **Pilotierung der Einspielung der ID-Nr.:** Einspielung der Identifikationsnummer in das jeweilige Register inklusive Schaffung der technischen Vorrausetzungen

2) **Erprobung ausgewählter Once-Only-Komponenten:** Anschluss des Registers an ausgewählte Once-Only-Komponenten wie z.B. Single-Digital-Gateway, Consent-Modul, Nachweisabruf

3) **Registerweiterentwicklung:** Modernisierung auf vier Dimensionen (rechtliche, organisatorische, semantische und technische Interoperabilität), um Register gesamtheitlich anschlussfähig für zukünftige digitale Anforderungen zu machen

In einem ersten Schritt wurden laufende bzw. vor einer Initiierung stehende Pilotvorhaben identifiziert, deren Ziel die Erprobung von Komponenten der Zielarchitektur anhand konkreter Vorhaben ist. So finden beispielsweise technische Erprobungen statt, wie sich europäische Once-Only-Anforderungen in der deutschen Registerlandschaft umsetzen ließen. Zudem wird derzeit eine deutsche Beteiligung an einem europäischen „Large Scale Pilot“ (DE4A) auf EU-Ebene geprüft. Auch hinsichtlich der Einspeicherung der ID-Nr. nach dem IDNrG wurden seitens des BVA technische Erprobungsaktivitäten gestartet.

In einem weiteren Schritt werden aktuell zusätzliche Kandidaten für Pilotregister aus dem Kreis der OZG-nutzungsträchtigen Top-18-Register des Zielbildes evaluiert, um im Kontext der oben erläuterten Module weitere Pilotvorhaben bis Jahresende zu initiieren.

2.5 Umsetzung Art. 14 SDG-Verordnung

Gemäß Art. 14 Abs. 9 SDG-VO hat die Europäische Kommission (KOM) einen Durchführungsrechtsakt zu erlassen, um die technischen und operativen Spezifikationen für das technische System, dem Once-Only-Technical-System (OOTS) nach Art. 14 SDG-VO festzulegen. Das OOTS soll den automatisierten Austausch von Nachweisen zwischen zuständigen Behörden in verschiedenen Mitgliedstaaten ermöglichen. Zuletzt am 04.06.2021 übermittelte die KOM eine überarbeitete Fassung des Entwurfs einer Durchführungsverordnung (DVO) nach Art. 14 Abs. 9 SDG-VO. Die in der SDG-VO vorgesehene Frist - 12.06.2021 - zum Erlass der DVO ist abgelaufen. Die Abstimmung ist nun für den Herbst 2021 vorgesehen. Grund dafür ist die Einleitung eines Kontrollverfahrens seitens des Rats nach Art. 11 der Komitologie-VO (VERORDNUNG (EU) Nr. 182/2011). Die Mitgliedstaaten, einschließlich Deutschland, gehen davon aus, dass die KOM ihre Kompetenzen überschreitet („ultra-vires"-Problematik). Am 14.07.2021 übermittelte die KOM die „Technical Design Documents" zum OOTS. Nach Analyse dieser Dokumente werden die Verhandlungen bilateral mit der KOM fortgeführt.

Mit der Überarbeitung der eIDAS-Verordnung und der geplanten Einführung einer EUid-Brieftasche (European Digital Identity Wallets) gibt es eine enge Verknüpfung zum OOTS. Eine Zusammenarbeit bei der Entwicklung von Standards für Arten von Beweismitteln/elektronische[n] Attribute[n] ist zu prüfen, auch um Doppelarbeit zu vermeiden.

Im Rahmen der Erarbeitung der DVO wurden eine Reihe wichtiger deutscher Forderungen aufgenommen, die auch im letzten Entwurf weiterhin erfüllt sind, wie z. B. die Berücksichtigung der föderalen Registerlandschaft und einheitliche Standards für die Protokollierung bei allen Systemteilnehmern.

Weiterhin gibt es große Herausforderungen bei der Umsetzung von Art. 14 der SDG-VO: Einige Mitgliedstaaten verweisen aufgrund der Infrastrukturvoraussetzungen auf absehbare Probleme bei der Umsetzung. Wenn sich diese Befürchtungen bewahrheiten, könnte der eigentliche, gesamteuropäische Mehrwert des Systems nicht erreicht werden, für den alle Mitgliedstaaten erfolgreich angebunden werden müssen.

Daneben gilt es zu klären, welche Rechtsänderungsbedarfe im Zuge der Umsetzung von Art. 14 der SDG-VO notwendig sind. In Anbetracht der komplexen Anforderungen an das OOTS, der heterogenen nationalen und internationalen Registerlandschaft und der verspäteten Veröffentlichung der o. g. DVO erscheint dazu die zeitliche Umsetzungsfrist ausgesprochen ambitioniert.

Aufgrund der großen Herausforderung ist es wichtig, dass die nationale Umsetzung von Art. 14 der SDG-VO in die Gesamtsteuerung Registermodernisierung integriert wird. Das den bisherigen Prozess mit technischer Expertise begleitende Team wird daher unter der Federführung der KoSIT in das Kompetenzteam EU-Interoperabilität überführt und sichert so die Konsistenz der Umsetzung des Zielbildes in Bezug auf europäische Anforderungen und Synergiepotentiale. Rechtliche Fragen werden im Kompetenzteam Recht/Datenschutz behandelt. Die Länder werden weiterhin im Rahmen der SDG-Koordination in die Umsetzung dieses europäischen Vorhabens eng eingebunden.

3. Ressourcenbedarfe / Aufwandsschätzmodell

Als Kernprojekt der deutschen Verwaltungsdigitalisierung ist die Registermodernisierung laut Nationalem Normenkontrollrat (NKR) in seiner Dimension mit dem Onlinezugangsgesetz vergleichbar.[1] Im Rahmen der in der 34. Sitzung des IT-Planungsrates beschlossenen Umsetzung des Zielbildes der Registermodernisierung bis 2025 werden daher erhebliche Aufwände auf allen Verwaltungsebenen anfallen. Für eine frühzeitige Berücksichtigung bei der Haushaltsplanung gilt es die Aufwände für Bund und Länder bestmöglich zu ermitteln, um so die notwendige Finanzierung im Rahmen verfügbarer Haushaltsmittel sicherzustellen. Da die Umsetzung des Zielbildes der Registermodernisierung bis 2025 deutlich über die reine Umsetzung des RegMoG hinausgeht, bedarf es für das Gesamtvorhaben Registermodernisierung weiterführender zu erwirtschaftender Ressourcen. Die derzeit aus Ziffer 40 des Konjunkturpaketes zur Verfügung gestellten Mittel zur Umsetzung des RegMoG stellen daher nur einen Teil der Haushaltsvorsorge dar.

Grundsätzlich sind hierbei zwei Ressourcenbedarfe zu unterscheiden, welche im Folgenden nach einer Beschreibung der Ausgangslage zur Finanzierung (vgl. 3.1) näher erläutert werden. Zum einen sind die Aufwände auf Seiten Bund und federführender Länder zum Aufbau und zum Betrieb des Steuerungsprojektes Registermodernisierung maßgeblich (vgl. 3.2). Zum anderen sind die darüberhinausgehenden Aufwände auf Bundes- und Landes-/Kommunalebene einzuplanen, die für die umfangreichen Umsetzungsaufgaben des Gesamtvorhabens Registermodernisierung bis Ende 2025 anfallen (vgl. 3.3).

3.1 Ausganglage zur Finanzierung

Das dem derzeitigen Steuerungsprojekt Registermodernisierung vorausgegangene Koordinierungsprojekt Registermodernisierung wurde als Bund-Länder-Projekt des IT-Planungsrates damit beauftragt, die Konzeption einer bundesweiten Architektur für die Registermodernisierung zu erarbeiten. Als solches wurde das Koordinierungsprojekt durch ein eigenes Budget im Rahmen des Digitalisierungsbudgets 2020 des IT-Planungsrates

[1] NKR (2020), Monitor Digitale Verwaltung #4: https://www.normenkontrollrat.bund.de/resource/blob/72494/1783152/14635b15fe7f6902039abcd653de6c61/20200909-monitordigitaleverwaltung-4-data.pdf

finanziert. Mit dem Mitte 2020 verabschiedeten Konjunkturpaket wurden der Registermodernisierung als wichtige Säule der Digitalisierung der gesamten Verwaltung in Bund, Ländern und Kommunen 300 Mio. EUR zur Finanzierung bereitgestellt. Als Folge dessen beschloss der IT-Planungsrat in seiner 34. Sitzung (Beschluss 2021/01), dass eine Abgrenzung zwischen Digitalisierungsbudget und Konjunkturpaket vorzunehmen ist.

Mit dem Beschluss zur Einrichtung des Projektes "Gesamtsteuerung Registermodernisierung" in der 35. Sitzung des IT-Planungsrates wurde beschlossen, dass für das Gesamtvorhaben Registermodernisierung ein Budget zur Programmsteuerung des IT-Planungsrates vorzusehen ist (Beschluss 2021/25). Dabei ist das Steuerungsprojekt als Bund-Länder-Projekt des IT-Planungsrates mit der Aufgabe betraut, die Realisierung des Zielbildes Registermodernisierung entsprechend der beschlossenen Umsetzungsplanung (Entscheidung IT-PLR Nr. 2021/05) zu steuern. Das zu realisierende Zielbild geht dabei weit über die Anforderungen des RegMoG hinaus und bedarf einer weiteren Finanzierung im Rahmen verfügbarer Haushaltsmittel, welche sowohl den Aufbau und Betrieb des Steuerungsprojektes an sich (vgl. 3.2) als auch die Umsetzung der Registermodernisierung insgesamt im Sinne des Zielbildes betrifft (vgl. 3.3).

3.2 Ressourcenbedarfe für Aufbau und Betrieb des Steuerungsprojektes

Damit das Steuerungsprojekt Registermodernisierung eine erfolgreiche Gesamtsteuerung für die Registermodernisierung gewährleisten kann, sind für den Aufbau und den Betrieb der vorgesehenen Steuerungsstrukturen (vgl. Abschnitt 2.2) notwendige Projektressourcen auf Seiten der Federführer vorzusehen. Nur so kann eine übergreifende Programmsteuerung (via Lenkungskreis und Transformationseinheit) sowie ein effektiver Wissensaufbau und -transfer im Projekt (via Projekteboard und Kompetenzteams) gewährleistet werden.

Gemäß der Beschlusslage des IT-Planungsrates (Beschluss 2021/25) ist für die Gesamtsteuerung Registermodernisierung ein Budget zur Programmsteuerung vorzusehen. Die mit dem Aufbau und Betrieb des Steuerungsprojektes verbundenen Aufwände werden derzeit im Kreis der Federführer für die Jahre 2021 und 2022 geschätzt und validiert, wobei die Aufwände für den Aufbau der Steuerungsstrukturen in 2021 voraussichtlich unter den Aufwänden des vollen Betriebes des Steuerungsprojektes liegen werden. In Abstimmung zwischen den Federführern und der FITKO wurde hierzu als Finanzierungsvorschlag für die Jahre 2021 und 2022 eine Mittelbereitstellung aus vorhandenen Mitteln des Digitalisierungsbudgets ausgearbeitet. Eine validierte und begründete Übersicht der anfallenden Aufwände ist im nächsten Schritt durch die Federführer zu erstellen und ein entsprechender Projektantrag bei der FITKO einzureichen. Mit der Finanzierung des Projektes über Mittel aus dem Digitalisierungsbudget unterliegt das Projekt auch den entsprechenden Regularien für die Durchführung von Projekten des Digitalisierungsbudgets.

3.3 Ressourcenbedarfe zur Umsetzung des Gesamtvorhabens Registermodernisierung (Aufwandsschätzmodell)

Wie eingangs dargelegt, sind für die Umsetzung des Zielbildes der Registermodernisierung erhebliche Aufwände auf Seiten Bund, Ländern und Kommunen zu erwarten, die über die bisher im RegMoG veranschlagten Aufwände hinausgehen. Das Koordinierungsprojekt Registermodernisierung hat ein erstes Aufwandsschätzmodell (ASM) entwickelt, welches die einmaligen und jährlichen Aufwände im Rahmen der Registermodernisierung in Gänze schätzen soll. Das ASM deckt dabei sowohl die Aufwände ab, die im Rahmen der Umsetzung der Anforderungen des RegMoG zu erwarten sind, als auch darüberhinausgehende Aufwände für die weitere Realisierung des Zielbildes Registermodernisierung (bspw. Umsetzung des Architekturzielbildes zur Realisierung des Once Only-Prinzips). Demnach werden die einmaligen gesamtstaatlichen Aufwände auf 1,9 Mrd. EUR bis 2,3 Mrd. EUR geschätzt wohingegen sich die laufenden Aufwände bis einschließlich 2025 in Summe auf ca. 0,6 Mrd. EUR bis 1,1 Mrd. EUR belaufen. Im nächsten Schritt sind diese ersten Schätzungen zu validieren.

3.2.1 Vorstellung des Aufwandsschätzmodells

Das ASM ist ein Hilfsmittel, um Aufwände im Zusammenhang mit der Umsetzung der Registermodernisierung abzuschätzen. Es konsolidiert eine Vielzahl von bestehenden Daten bzw. Schätzungen, die aus belegten Quellen stammen (z.B. Statistiken des StBA, Leitfäden zu Erfüllungsaufwänden des BMF, durchgeführte Wirtschaftlichkeitsuntersuchungen), und ergänzt diese, wo nötig, um weitere Annahmen, die zunächst durch das Koordinierungsprojekt Registermodernisierung getroffen und nun durch das Gesamtsteuerungsprojekt Registermodernisierung beim Vorhandensein neuer Erkenntnisse aktualisiert wurden.

Um eine Aufwandschätzung der Registermodernisierung als Gesamtvorhaben zu ermöglichen, folgt das ASM einer einheitlichen Strukturlogik. Alle Aufwände werden entsprechend ihrer inhaltlichen Klassifizierung innerhalb der Registermodernisierung einer von sieben Aufwandskategorien zugeordnet. Die Aufwandskategorien unterteilen sich in (1) technische Architektur, (2) Anschluss an das technische System, (3) bestehende Register, (4) wesentliche neue Register, (5) Personenidentifikationsnummer, (6) Unternehmensidentifikationsnummer und (7) registerübergreifende Umsetzungsstrukturen. Innerhalb der einzelnen Kategorien setzen sich die Aufwände aus insgesamt 54 Aufwandstreibern zusammen. Die Aufwände der einzelnen Treiber können dabei entweder auf Bundesebene, Landesebene oder beiden Ebenen anfallen. Je Aufwandstreiber wird zudem in zwei Aufwandsarten unterschieden – einmalige und jährliche Aufwände. Dabei wird für alle Aufwände immer eine Spanne „von“ „bis“ inkl. einem zur Berechnung verwendetem Wert innerhalb der Spanne verwendet.

Als zeitliche Dimension wird innerhalb des ASM ein Umsetzungszeitraum von bis zu 5 Jahren in Betracht gezogen, da der Umsetzungszeitraum der Registermodernisierung laut

Zielbild von 2021 bis 2025 verlaufen soll. In diesem Zeitraum soll möglichst die Aufnahme des laufenden Betriebs und der Anschluss der priorisierten Register erfolgen. Auf dieser Basis wird je Aufwandstreiber die Anzahl an Jahren im Betrachtungszeitraum in denen jährliche (laufende) Aufwände anfallen abhängig von dem geschätzten Datum der Inbetriebnahme bzw. Fertigstellung der Umsetzung eines Aufwandstreibers geschätzt. Alle zeitlichen Werte werden ebenfalls in einer Spanne „von" „bis" inkl. einem zur Berechnung verwendetem Wert innerhalb der Spanne angegeben.

Zusammenfassend berücksichtigt das ASM für die Berechnung von Aufwänden je Kategorie und Aufwandstreiber immer sowohl einmalige als auch jährliche Aufwände sowie den Zeitpunkt der Inbetriebnahme bzw. Fertigstellung der Umsetzung eines Aufwandstreibers entsprechend der daraus resultierenden Anzahl an Jahren im laufenden Betrieb innerhalb des Betrachtungszeitraums bis 2025.

Das ASM ermöglicht es im Zuge des weiteren Vorgehens alle Aufwandsannahmen kontinuierlich weiterzuentwickeln und entsprechend an neue Faktenlagen anzupassen. Ausgangspunkt für die einzelnen Werte sind bestehende Schätzungen aus den unterschiedlichen bereits existierenden Quellen zur Registermodernisierung (z.B. Gesetzen, WiBe). In einzelnen Fällen hat das Koordinierungsprojekt abweichende bzw. aktuellere Einschätzungen vorgenommen. Zudem wurden Einschätzungen für Aufwandstreiber vorgenommen, für die bisher keine Schätzungen vorlagen. Die Kombination dieser beiden als Inputs getroffenen Annahmen bildet die Grundlage (den Basisfall) für das ASM. Darüber hinaus ermöglicht das ASM abweichende Annahmen für alle Aufwandstreiber zu treffen. Diese abweichenden Werte werden vom ASM automatisch für alle Berechnungen innerhalb des Modells anstelle der im Basisfall getroffenen Schätzungen bzw. Annahmen berücksichtigt. Somit ermöglicht das ASM jederzeit auf neue Erkenntnisse im Rahmen der Registermodernisierung einzugehen und die entsprechenden Implikationen für die Gesamtaufwände für Bund, Länder und verschiedene Aufwandstreiber zu berücksichtigen.

3.2.2 Erste Ergebnisse der initialen Aufwandschätzung

Laut ASM beträgt der Gesamtaufwand für die Registermodernisierung im Betrachtungszeitraum von 2021 bis 2025 nach aktuellem Kenntnisstand ca. 2,9 Mrd. EUR (zwischen 2,5 Mrd. EUR und 3,4 Mrd. EUR). Davon fallen im Betrachtungszeitraum ca. drei Viertel aller Aufwände einmalig und ca. ein Viertel aller Aufwände als Summe der jährlichen Aufwände an. Insgesamt sind die einmaligen Aufwände ca. 8-mal so hoch wie die jährlichen Aufwände. Dies ist bedingt durch die hohe Dezentralität der deutschen Registerlandschaft, die den einmaligen Anschluss an das technische System und die Weiterentwicklung einer Vielzahl von Registern auf Landes- oder Kommunalebene mit sich bringt. Innerhalb der Einmalaufwände entfallen ca. die Hälfte auf die Weiterentwicklung bestehender Register und deren Anschluss an das technische System.

Auf Basis von vorläufigen Annahmen ergibt sich dieser ersten Schätzung nach, dass ca. zwei Drittel der Gesamtaufwände auf Landes- und Kommunalebene im Betrachtungszeitraum

anfallen. Folglich ist ca. ein Drittel der Gesamtaufwände im gleichen Zeitraum auf Bundesebene zu verorten. Der deutlich höhere Aufwandsanteil auf Landes- und Kommunalebene ist ebenfalls auf die hohe Dezentralität der deutschen Registerlandschaft zurückzuführen.

Die Aufwände des ASM sind im Weiteren zu validieren. Das bestehende ASM könnte nach erfolgreicher Validierung als Beitrag zu haushaltsbegründenden Unterlagen für Bund und Länder dienen. Um dies zu ermöglich, ist auf Basis des validierten ASM im nächsten Schritt eine Konkretisierung dahingehend zu treffen, welche Aufwände bereits durch bestehende Ressourcen finanziert sind und für welche Aufwände eine darüberhinausgehende Finanzierung erforderlich ist. Die hierdurch vorgenommene Schätzung eines weiterführenden Finanzierungsbedarfs könnte bund- sowie länderseitig haushaltsbegründenden Unterlage in kommende Haushaltsaufstellungsverfahren eingebracht werden. Haushaltsverhandlungen auf Bundesebene werden hierdurch nicht präjudiziert.

Anhang

Anhang 1: Projektstrukturen des Projektes „Gesamtsteuerung Registermodernisierung“

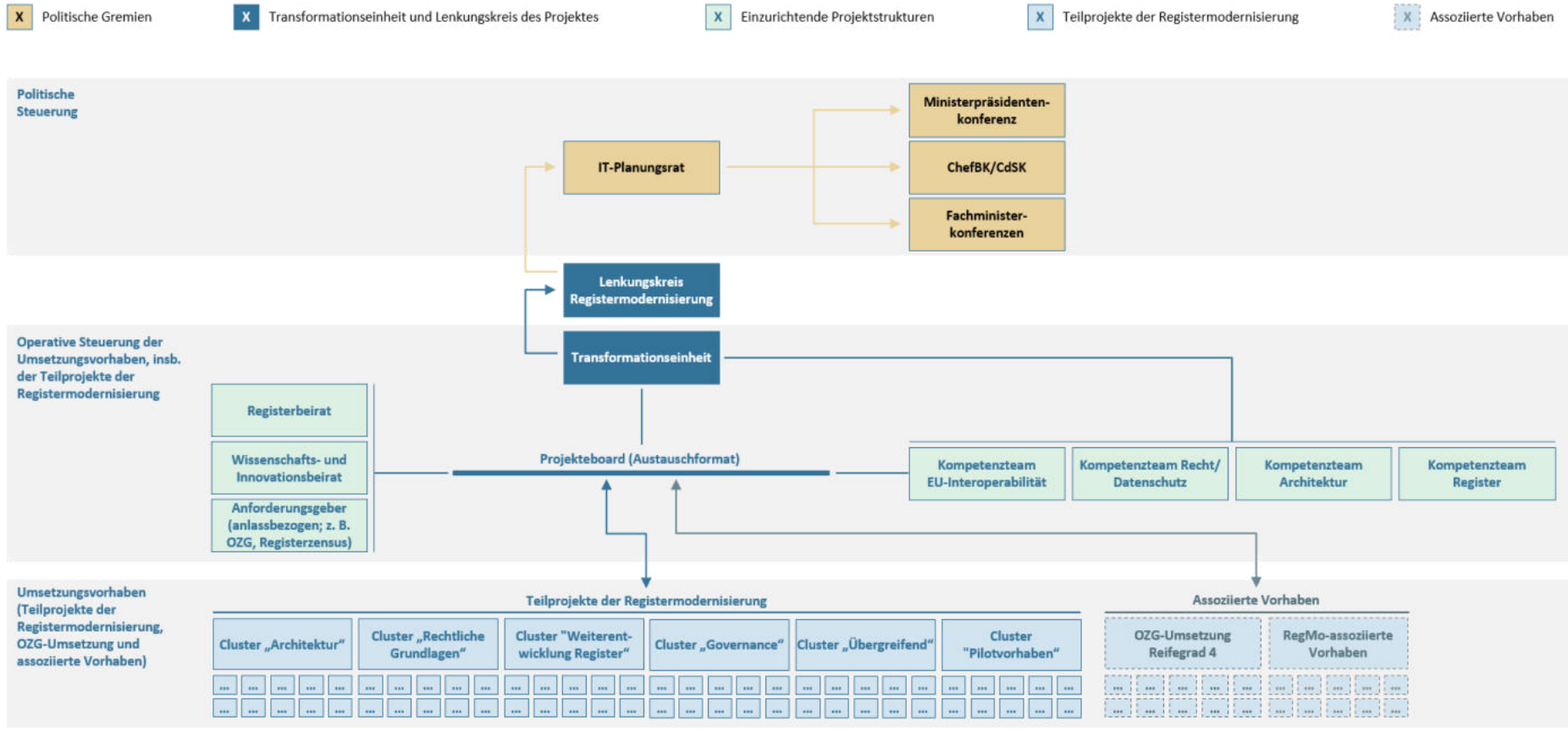


Abbildung 3: Schematische Abbildung der Projektstrukturen des Projektes „Gesamtsteuerung Registermodernisierung“ (Großabbildung)

Anhang 2: Zielsetzung der Pilotierung

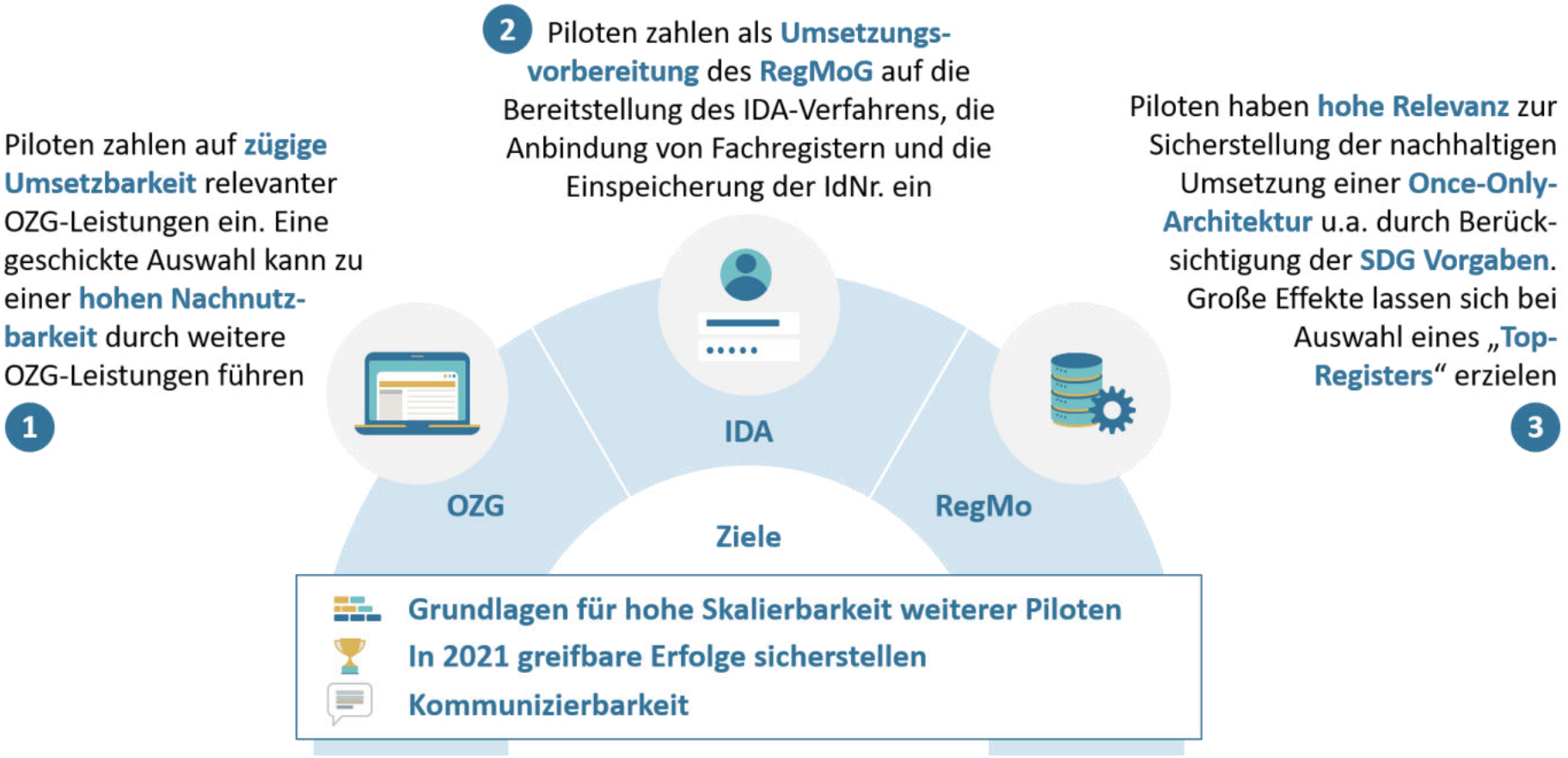


Abbildung 4: Zielsetzung der Pilotvorhaben der Registermodernisierung (Großabbildung)

Abkürzungsverzeichnis

ASM	Aufwandsschätzmodell
BMI	Bundesministerium des Innern, für Bau und Heimat
BVA	Bundesverwaltungsamt
DE4A	Digital Europe for All
DVO	Durchführungsverordnung
eIDAS	electronic IDentification, Authentication and trust Services
EUR	Euro
FITKO	Föderale IT-Kooperation
IDNrG	Identifikationsnummerngesetz
IT-PLR	IT-Planungsrat
KOM	Europäische Kommission
KoSIT	Koordinierungsstelle für IT-Standards
KT	Kompetenzteam
Mio.	Millionen
Mrd.	Milliarden
NKR	Nationaler Normenkontrollrat
OOTS	Once-Only-Technical System
OZG	Onlinezugangsgesetz
RegMoG	Registermodernisierungsgesetz
SDG	Single Digital Gateway
SDG-VO	SDG-Verordnung
WiBe	Wirtschaftlichkeitsberechnung

Abbildungsverzeichnis

Erprobung Once-Only-Nachweisabruf mit dem Meldeportal Behörden des Landes NRW

Abschlussbericht zum Erprobungsprojekt 7 im Gesamtvorhaben Registermodernisierung des IT-Planungsrats

Koordinierungsstelle für IT-Standards (KoSIT)

Veröffentlicht 16.5.2022

Erprobung Once-Only-Nachweisabruf mit dem Meldeportal Behörden des Landes NRW

Koordinierungsstelle für IT-Standards (KoSIT)

Veröffentlicht 16.5.2022

Zusammenfassung

Im Rahmen des Gesamtvorhabens „Registermodernisierung“ des IT-Planungsrats wurden im Jahr 2021 mehrere Erprobungsprojekte durchgeführt. Dieser Abschlussbericht dokumentiert das Erprobungsprojekt 7, welches bis Ende 2021 unter Federführung der KoSIT mit dem Meldeportal Behörden des Landes NRW durchgeführt wurde.

Im Projekt wurde in Form eines *Proof of Concept (PoC)* gezeigt, dass das Meldeportal Behörden mit einer Schnittstelle ausgestattet werden kann, die den technischen Vorgaben der EU-Kommission für den Anschluss an das technische System entspricht, welches gemäß Artikel 14 der SDG Verordnung errichtet werden soll (OOTS). Über eine entsprechende Schnittstelle könnten Nachweise von allen nordrhein-westfälischen Meldebehörden mit dem von der EU-Kommission dafür vorgesehenen Standard abgerufen werden. Nach derzeitigem Kenntnisstand sind dafür keine Schnittstellenänderungen bei den IT-Verfahren der kommunalen Meldebehörden notwendig. Dem liegt allerdings eine Auffassung zur rechtlichen und fachlichen Einordnung des Meldeportal Behörden zugrunde, die einer näheren Analyse und Bestätigung bedarf (siehe Abschnitt 1.9).

Eine zentrale Rahmenbedingung war die Übertragbarkeit auf das nationale technische System (NOOTS) und nationales Recht, insbesondere das Identifikationsnummerngesetz (IdNrG). Da das von der EU-Kommission vorgesehene Transportprotokoll AS4 CEF eDelivery derzeit keine Ende-zu-Ende Sicherheit unterstützt, erfüllt es die Anforderungen des IdNrG nicht. Im Projekt wurde daher der Standard OSCI des IT-Planungsrats eingesetzt. Durch den Einsatz des Standards XTA des IT-Planungsrats konnte eine weitgehende Unabhängigkeit vom Transportprotokoll erreicht werden, so dass die Möglichkeit des Einsatzes europäischer Lösungen proaktiv befördert wird, wenn diese den nationalen Anforderungen in vollem Umfang entsprechen.

Alle Ergebnisse stehen unter dem Vorbehalt, dass die EU-Kommission weit hinter dem eigenen Zeitplan zurückbleibt und bisher lediglich Entwürfe rechtlicher und technischer Vorgaben veröffentlicht hat. Ein Abgleich mit verbindlichen Anschlussbedingungen konnte daher im Projekt leider nicht erfolgen.

Versionsgeschichte		
Version 1.0	16.5.2022	KoSIT
Initiale Fassung		

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Liste der Beispiele

Kapitel 1. Übersicht und zentrale Ergebnisse

1.1. Management Summary

Im Rahmen des Gesamtvorhabens „Registermodernisierung“ des IT-Planungsrats wurden im Jahr 2021 mehrere Erprobungsprojekte durchgeführt. Dieser Abschlussbericht dokumentiert das Erprobungsprojekt 7, welches bis Ende 2021 unter Federführung der KoSIT mit dem Meldeportal Behörden des Landes NRW durchgeführt wurde.

Das Meldeportal Behörden wird vom Kommunalen Rechenzentrun Niederrhein (KRZN) betrieben. Es ist gemäß landesrechtlicher Vorgaben die zentrale Stelle für alle Auskünfte zu Meldedaten für Behörden des Landes NRW. Es werden jährlich über 40 Millionen Auskünfte aus Melderegistern für Behörden erteilt. Im Projekt wurde in Form eines Proof of Concept (PoC)zumindest grundsätzlich gezeigt, dass das Meldeportal Behörden um eine zusätzliche Schnittstelle in dem Format erweitert werden kann, welches die EU-Kommission für Nachweisabrufe im technischem System gemäß Artikel 14 der SDG Verordnung 2018/1724 vorgeben wird. Dem lag die Überlegung zugrunde, dass durch den Anschluss des Meldeportal Behörden an das technische System alle nordrhein-westfälischen Meldebehörden angeschlossen sind, ohne dass es dafür einer Änderung bei den Fachverfahren der kommunalen Meldebehörden bedarf[1]. Und da das Meldeportal Behörden Teil eines Verbunds der Meldedatenportale aller Bundesländer ist, könnten möglicherweise sogar alle bundesdeutschen Meldebehörden durch den einen, zentralen Anschluss an einem einzigen Meldeportal erledigt werden. Bei aller Vorsicht hinsichtlich der Aussagekraft eines auf einen einzigen Anwendungsfall bezogenen *Proof of Concept* kann man zumindest feststellen, dass keine eindeutigen Gegenargumente gefunden wurden, so dass es sich auf jeden Fall lohnt, die Idee weiter zu verfolgen. Dieser Interpretation liegt allerdings eine Auffassung zur rechtlichen und fachlichen Einordnung des Meldeportal Behörden zugrunde, die einer näheren Analyse und Bestätigung bedarf (siehe Abschnitt 1.9). Die Erprobung hat außerdem geholfen die Praxistauglichkeit der von der EU vorgeschlagenen Lösungsansätze besser einschätzen zu können und die Rahmenbedingungen für den Aufbau eines technischen Systems für Once Only in Deutschland zu schärfen.

Dabei war zu berücksichtigen, dass das von der EU-Kommission vorgesehene Transportprotokoll AS4 CEF eDelivery die gemäß § 7 IdNrG unter bestimmten Bedingungen zwingend erforderliche Ende-zu-Ende Sicherheit zunächst nicht unterstützen wird. Deshalb ist im Erprobungsprojekt der Standard OSCI des IT-Planungsrats als Basis für das nationale Once Only System angenommen worden, der sich unter anderem im Informationsverbund aller kommunal geführten Register der Innenverwaltung ebenso wie im elektronischen Rechtsverkehr seit vielen Jahren bewährt hat. Da aber davon auszugehen ist, dass sich auch der europäische Standard technisch weiterentwickeln wird, so dass die notwendigen Ende-zu-Ende Sicherheitsmechanismen zukünftig zumindest als Option zur Verfügung stehen werden, wurde geprüft, ob der Standard XTA 2 des IT-Planungsrats zu einer weitgehenden Unabhängigkeit vom Transportprotokoll führen kann, um somit die Möglichkeiten eines Einsatzes europäischer Standards proaktiv zu verbessern (siehe Abbildung 1.8).

Die positiven Ergebnisse des Pilotvorhabens haben zu einer raschen Festlegung der technischen Verfahren der Datenübermittlung an und durch die Registermodernisierungsbehörde geführt: Dass die Verordnung zu XBasisdaten (XBasisdatenV) vom 28. März 2022 unter anderem festlegt, dass als Transportstandards XTA 2 in Verbindung mit OSCI-Transport in der jeweils aktuellen Fassung oder andere in XBasisdaten genannte Standards oder Schnittstellen zu verwenden sind, ist sicherlich auch darin begründet, dass genau diese Kombination in dem hier dokumentierten Projekt intensiv untersucht worden ist. Im Projekt wurde aber auch deutlich, dass die Umsetzung der Ende-zu-Ende Sicherheit mit XTA und OSCI derzeit noch unnötig kompliziert ist, so dass Nachbesserungen in Bereichen der Dokumentation, der Anwendungen und Bibliotheken des IT-Planungsrats sowie der Testmöglichkeiten geboten sind. Diese Erkenntnisse sind inzwischen durch einen vom Land NRW initiierten Praxistest bestätigt worden.

Unabhängig vom Transportstandard wurde das von der EU-Kommission definierte *Evidence Exchange Model (EDM)* untersucht. Es legt einen generischen (fachunabhängigen) Standard für den Abruf von Nachweisen für natürliche oder juristische Personen fest. Es unterscheidet sich erheblich von etablierten XÖV Standards, gleichwohl konnte die Abbildung auf XMeld erfolgreich umgesetzt werden. Damit wurde gezeigt, dass das

[1]Dabei sind jedoch zusätzliche Anforderungen aufgrund der Verpflichtung zum Anschluss an das Datenschutzcockpit nicht berücksichtigt.

EDM der EU-Kommission eine geeignete Grundlage für den im Zielbild der Registermodernisierung postulierten „Einheitlicher Datenstandard“ ist.

Das Projekt hat zudem zu einer Fortentwicklung des Core Vocabulary (CV) der EU-Kommission beigetragen. Die Erprobung zeigte auf, dass rechtliche Vorgaben zur Speicherung des Geburtsdatums mit der bisherigen Fassung der Core Vocabularies nicht in allen Fällen umsetzbar waren. Unsere Erkenntnisse sind bei der Fortentwicklung berücksichtigt worden (siehe Issue 17 des Core Person Vocabulary). Außerdem wurde deutlich, dass technische Vorgaben der eIDAS Verordnung nicht mit personenstandsrechtlichen Vorgaben zur Eintragung des Geschlechts von Personen übereinstimmen. Das BMI hat insoweit Erkenntnisse des Erprobungsprojekts in die Expertengruppe zur Fortentwicklung der eIDAS Verordnung eingebracht.

Neben den üblichen technischen Schwierigkeiten und der ebenfalls nicht überraschenden Feststellung, dass die Komplexität der Aufgabenstellung zunächst erheblich unterschätzt worden war, so dass der Ressourcenbedarf jederzeit deutlich über den tatsächlich gegebenen Möglichkeiten lag, war das größte Problem der dramatische Zeitverzug der EU Gremien bei der Abstimmung verbindlicher Vorgaben mit den Mitgliedsstaaten. “By 12 June 2021, the Commission shall adopt implementing acts to set out the technical and operational specifications of the technical system necessary for the implementation of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2)” — dies ist die eindeutige Vorgabe des Artikel 14 Absatz 9 der SDG Verordnung. Aber ein politischer Streit zwischen der Kommission und Mitgliedsstaaten verhinderte das Zustandekommen des Durchführungsrechtsakts während der gesamten Projektlaufzeit. Zum Zeitpunkt der Veröffentlichung dieses Abschlussberichts Anfang Mai 2022 liegt er immer noch nicht vor.

Für das Erprobungsprojekt hatte dies erhebliche negative Konsequenzen. Die im SDG Vorhaben eingerichteten *working packages* wurden faktisch eingestellt, so dass die Abstimmung mit technischen Experten insbesondere im *WP 7* nicht mehr möglich war. Zudem fehlten dringend benötigte, technische Artefakte, zu denen insbesondere das finale XML Schema für den EDM-basierten Datenaustausch zählen. Um überhaupt arbeitsfähig zu sein, musste Ersatz aus teilweise dubiosen Quellen genutzt werden. Die Suche nach Ansprechpartnern und einigermaßen verlässlichem Material hat sehr viel Zeit und Energie beansprucht.

Vor diesem Hintergrund konnten keine finalen Ergebnisse erzielt werden. Alle technischen Lösungen stehen notwendigerweise unter dem Vorbehalt, dass sie mit verbindlichen Vorgaben der EU abgeglichen werden müssen, nachdem der Durchführungsrechtsakt abgestimmt, und die Abstimmungen zwischen Experten auf europäischer Ebene wieder aufgenommen worden sind.

1.2. Zentrale Begriffe und Abkürzungen

Dem Vorhaben standen verschiedene Quellen aus dem SDG Kontext zur Verfügung. Neben der SDG Verordnung und ersten Entwürfen des Implementig Act und der Technical Design Documents (TDD) waren dies insbesondere die Ergebnisse des Vorprojekts TOOP. Mit Ausnahme der SDG Verordnung, die in allen Mitgliedssprachen veröffentlicht worden ist, liegen alle anderen Dokumente ausschließlich in englischer Sprache vor. Zudem nutzen sie für zentrale Konzepte unterschiedliche Bezeichnungen. So wird etwa die öffentliche Stelle, die einen Nachweis bei einer anderen öffentlichen Stelle abruft, in TOOP als “Data Consumer” bezeichnet, während SDG-Dokumente sie als “Evidence Requester” bezeichnen. Dies war für unser Vorhaben hinderlich, zumal auch eine Übersetzung in die deutsche Sprache angestrebt wurde, die rechtlich zumindest akzeptabel sein sollte.

Tabelle 1.1 erläutert zentrale Begriffe, die in diesem Dokument verwendet werden.

Tabelle 1.1. Abkürzungsverzeichnis und Glossar

AGS	Amtlicher Gemeindeschlüssel	Der Amtliche Gemeindeschlüssel ist ein 8-stelliger Schlüssel zur eindeutigen Identifizierung einer Gemeinde mit den Bestandteilen: Bundesland (2 Stellen), Regierungsbezirk (1 Stelle), Kreis (2 Stellen) und Gemeinde (3 Stellen).

		Er wird vom Statistischen Bundesamt herausgegeben und ist in dem hier dargestellten Projekt unerlässlich für die Ermittlung der Meldebehörde, die einen Nachweis zur betroffenen Person ausstellen kann.
AS4	AS4 Profile of ebMS 3.0	Eine OASIS Standard für die sichere Datenübermittlung. Er wird von der EU Kommission in einer bestimmten Ausprägung für die grenzüberschreitenden Datenübermittlung im OOTS vorgeschrieben werden.
CEF eDelivery	Connecting Europe Facility: eDelivery	Die „Connecting Europe Facility (CEF)“ ist ein zentrales EU-Förderinstrument zur Finanzierung von Infrastrukturinvestitionen in Europa. Für den Bereich CEF Digital stehen insgesamt rd. 2 Mrd. Euro bis 2027 zur Verfügung. Gefördert wird der Ausbau hochleistungsfähiger digitaler Infrastruktur in Europa. Grundlage für das Förderprogramm ist die CEF2-Verordnung. [Quelle: Internetpräsenz des BMDV] Im Rahmen dieses Programms werden Bausteine - „building blocks“ entwickelt und den Mitgliedsstaaten zur Verfügung gestellt: „to promote the adoption of the same open standards and technical specifications, by the different sectors of the Union, for the most basic & common functionalities of any sectorial project/ platform.“ eDelivery ist ein CEF Baustein für eine „Messaging Infrastructure based on the 4-Corner Model“. CEF eDelivery wird in einer Präsentation der EU Kommission genauer dargestellt.
competent authority	Eine competent authority im Sinne des Artikel 3 Nr. 4 der SDG Verordnung ist eine *zuständige Behörde*: jede Stelle oder Behörde eines Mitgliedstaats auf nationaler, regionaler oder lokaler Ebene mit bestimmten Zuständigkeiten für die unter die SDG-Verordnung fallenden Informationen, Verfahren, Hilfs- und Problemlösungsdienste.	
CV	Core Vocabulary	Die EU Kommission gibt unter dem Namen “Core Vocabulary” eine Reihe von einfachen, wiederverwendbaren und erweiterbaren Datenmodellen für oft benötigte Informationsobjekte wie *Name*,, *Anschrift*, *Geburtsangaben* etc. heraus. Derzeit gibt es Core Vocabularies für • Business • Location • Person • Public Service • Public Organisation • Criterion and Evidence Core Vocabularies bilden die Grundbausteine für strukturierte Nachweise, die für den Daten-

		austausch im OOTS modelliert und vom Evidence Provider zur Verfügung gestellt werden.
Data Service	Data Service means a technical service through which an evidence provider handles the evidence requests and dispatches evidence	
DC	Data Consumer	Ein Synonym für *Evidence Requester*, welches im TOOP Projekt genutzt worden ist.
DP	Data Provider	Ein Synonym für *Evidence Provider*, welches im TOOP Projekt genutzt worden ist.
DSD	Data Service Directory	Eine zentrale technische Komponente des OOTS, in der verzeichnet ist, welche Behörden für welche Nachweistypen zuständig sind.
DVDV	Deutsches Verwaltungsdiensteverzeichnis	Ein Verzeichnis der elektronischen Dienste, die von Behörden der öffentlichen Verwaltung angeboten werden. Das Diensteverzeichnis ist eine föderale Anwendung des IT-Planungsrats. Es wurde 2007 zunächst für das elektronische Melderegister entwickelt und im Oktober 2019 von der neuen, flexibleren Version DVDV 2.0 abgelöst. Etwa 30.000 Fachverfahren bundesweit sind derzeit in dem Verzeichnis registriert. *[Quelle: ITZ Bund]*
EDM	Exchange Data Model	Part IV der Technical Design Documents beschreibt Prozesse, Standards und Datenstrukturen für den Austausch von Nachweisen zwischen den beiden betroffenen Behörden. Das EDM ist die Grundlage für den generischen Standard zum Abruf von Nachweisen im nationalen Kontext, der im Projekt Registermodernisierung entwickelt werden soll.
eIDAS	electronic IDentification, Authentication and trust Services	Verordnung 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt.
EP	Evidence Provider	Ein Evidence Provider ist eine „competent authority“, die rechtmäßig Nachweise an andere Behörden (Evidence Requester) übermittelt. In diesem Dokument übersetzt als „übermittelnde Stelle“.
ER	Evidence Requester	Ein Evidence Requester ist eine „competent authority“, die Nachweise für ihre Aufgabenwahrnehmung benötigt, und diese bei dem zuständigen Evidence Provider abruft. In diesem Dokument übersetzt als „abrufende Stelle“.
IdNrG	Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung (Identifikationsnummerngesetz)	Das IdNrG ist das Stammgesetz des Registermodernisierungsgesetzes (RegMoG).
Intermediary Platform	A technical solution through which evidence providers or evidence requesters connect to the common services referred to in Article 4(1) or to evidence providers or	

	evidence requesters from other Member States. [Quelle: SDG Implementing Regulation. Proposal vom März 2022]	
KoSIT Validator	Es handelt sich um eine Software zur automatisierten Prüfung von XML Dokumenten gegen Strukturvorgaben (in XSD Schema) und Geschäftsregeln (in Schematron formuliert) mit der Möglichkeit, bei festgestellen Abweichungen Handlungsempfehlungen zu geben. In seiner 23. Sitzung hat der IT-Planungsrat mit Beschluss 2017/22 (6a) die KoSIT im Rahmen des Betriebs des Standards XRechnung mit der „dauerhaften Bereitstellung eines Moduls zur Konformitätsprüfung elektronischer Rechnungen als offene Referenzimplementierung sowie aller zugehöriger Artefakte “beauftragt. Im Rahmen dieser Beauftragung wurde die Software entwickelt, die als KoSIT Validator unentgeltlich und quelloffen zur Verfügung steht. Sie wird inzwischen nicht nur für elektronische Rechnungen, sondern weitere Fachstandards wie XUnternehmen intensiv genutzt. Im Eprobungsprojekt wurde sie im Meldeportal Behörden genutzt um die simulierten Nachweisabrufe auf Konformität mit SDG-Vorgaben, aber auch nationalen Vorgaben zu prüfen.	
KRZN	Kommunales Rechenzentrum Niederrhein	Betreiber des Meldeportal Behörden für das Land NRW
MG NRW	Meldegesetz NRW	Online veröffentlicht im Justizportal des Landes NRW. § 7 MG NRW legt das das Meldeportal Behörden als zentrale Stelle für den automatisierten Abruf durch Behörden fest.
NOOTS	Nationales Once Only technical System	Gemäß des vom IT-Planungsrat beschlossenen Zielbilds Registermodernisierung wird ein nationales technisches System für den Austausch von Nachweisen und Anwendung des Grundsatzes der einmaligen Erfassung innerhalb der öffentlichen Verwaltung Deutschlands errichtet. Das NOOTS muss an das OOTS angeschlossen werden, damit deutsche Behörden, die mit den NOOTS verbunden sind, mittelbar auch an das OOTS angebunden sind. Dies ist eine Voraussetzung für die Erfüllung der Verpflichtungen aus der SDG Verordnung.
OASIS	Organization for the Advancement of Structured Information Standards	Eine internationale, nicht-gewinnorientierte Organisation, die sich mit der Weiterentwicklung von E-Business- und Webservice-Standards beschäftigt.
OOTS	Once Only Technical System	Die Europäische Kommission wird gemäß Artikel 14 der SDG Verordnung das Once Only Technical System errichten. Es handelt sich um ein technisches System für den grenzüberschreitenden automatisierten Austausch von Nachweisen und Anwendung des Grundsatzes der einmaligen Erfassung (“Once Only Principle”)
OSCI	Online Services Computer Interface	OSCI ist der Protokollstandard für die einheitliche Übermittlung von Nachrichten in der IT-Infrastruktur für Fachverfahren der Verwaltung. Er wird von der KoSIT für den IT-Planungsrat herausgegeben.

		Die OSCI-Spezifikation bildet verwaltungsspezifische, fachunabhängige Anforderungen an eine sichere, rechtsverbindliche sowie robuste und nachvollziehbare Datenübertragung ab.
PoC	Proof of Concept	Überprüfung der prinzipielle Durchführbarkeit eines Vorhabens anhand von Prototypen, ohne den Anspruch, dass diese anschließend izu einem Produkt weiterentwickelt werden können.
RegRep v4	OASIS ebXML RegRep Version 4.0	Ein OASIS Standard für ebXML **Reg**istry-**Rep**ository. Publiziert vom OASIS ebXML Registry TC (Fassung vom 25. Januar 2012).
Schematron	Schematron ist eine Technologie zur Formulierung von Geschäftsregeln mit der Möglichkeit, dass strukturierte Nachweise im XML Format automatisiert daraufhin überprüft werden können, ob die Geschäftsregeln eingehalten werden. Es handelt sich um einen ISO Standard („ISO/IEC 19757-3:2020 Information technology — Document Schema Definition Languages (DSDL) — Part 3: Rule-based validation using Schematron“). Im Rahmen der Registermodernisierung wird Schematron zusammen mit XSD Schema genutzt, um Nachweisabrufe auf formale Korrektheit zu prüfen (siehe Abschnitt 4.7).	
SDG	Single Digital Gateway	Ein digitales Zugangstor zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten auf europäischer Ebene. Begründet durch die SDG-Verordnung 2018/1724 vom 2. Oktober 2018.
SOAP	Simple Object Access Protocol	Ein Netzwerkprotokoll, mit dessen Hilfe Daten zwischen Systemen ausgetauscht und Remote Procedure Calls durchgeführt werden können. SOAP ist ein industrieller Standard des World Wide Web Consortiums (W3C). *[Quelle: Wikipedia]* XTA und OSCI basieren auf SOAP.
TDD	Technical Design Documents	Konkrete technische Beschreibung des OOTS und der verbindlichen Vorgaben zur Anbindung von Behörden an das OOTS. Die TDD werden durch SDG Projektgremien in einem nicht-öffentlichen Verfahren erstellt. In unregelmäßigen Abständen werden Entwürfe zwecks Abstimmung mit den Mitgliedsstaaten veröffentlicht.
TOOP	The Once Only Principle	TOOP wurde im Januar 2017 als eine Initiative von rund 50 Organisationen aus 20 EU-Mitgliedstaaten und assoziierten Ländern ins Leben gerufen. Das Hauptziel von TOOP war die Erforschung und Demonstration des Once Only Prinzips in einem grenzüberschreitenden, europaweiten Maßstab. Das Projekt endete am 31. März 2021. Es ist unter toop.eu dokumentiert.

		Die TOOP Solution Architecture war eine der wichtigsten Informationsquellen für das Erprobungsprojekt mit dem Meldeportal Behörden.
XML Schema	Eine Technologie zur Beschreibung der erwarteten Struktur von XML Dokumenten durch ein Strukturschema, definiert durch das W3C in der XML Schema Definition Language (XSD) Mit marktüblichen Technologien kann geprüft werden, ob ein XML Dokument den Strukturvorgaben eines XML Schema entspricht.	
XTA2	XÖV Transport Adapter Version 2	XTA standardisiert fachübergreifend den Anschluss von Fachverfahren an die Übermittlungsinfrastruktur der Verwaltung. Hierfür definiert XTA die erforderlichen fachunabhängigen Nachrichten, Nachrichtenmerkmale, Transportvorgaben und Berichtsstrukturen. Die Nutzung dieses Standards generiert auch in sicheren Netzen Mehrwerte, z. B. Ende-zu-Ende-Sicherheit und -Adressierung oder auch Nachweise zur Integrität der Nachrichten, die durch die Netzebene allein nicht abgedeckt werden.

1.3. Motivation

Die europäische Kommission wird gemäß Artikel 14 der Verordnung 2018/1724 ein technisches System für den grenzüberschreitenden automatisierten Austausch von Nachweisen und Anwendung des Grundsatzes der einmaligen Erfassung errichten. Deutsche Behörden müssen bis Ende 2023 an dieses Once Only technical System (OOTS) angeschlossen werden. Einerseits in der Rolle des *Evidence Providers*, also registerführender Behörden, deren Daten in Form elektronischer Nachweise zukünftig auch von Behörden im europäischen Ausland abgerufen werden können. Andererseits in der Rolle des *Evidence Requesters*, also einer Behörde die Nachweise zur Bearbeitung von Anträgen benötigt, und diese zukünftig auch von zuständigen Behörden im europäischen Ausland abrufen kann.

Für den Anschluss betroffener Behörden wird die europäische Kommission den Mitgliedsstaaten in Ergänzung der SDG-Verordnung präzise Vorgaben machen:

- In Form eines verbindlichen Durchführungsrechtsakts (“Implementing Regulation”), welche die Komponenten des OOTS und die Rechte und Pflichten der Mitgliedsstaaten zu deren Nutzung konkretisiert;
- In Form der *Technical Design Documents* (TDD) mit der technischen Konkretisierung hinsichtlich der zu nutzenden IT-Standards und der Anschlussmechanismen. Obwohl die TDD auf der Basis europäischen Rechts formal nicht bindend sind, haben sie gleichwohl zur Gewährleistung der Interoperabilität im OOTS einen verbindlichen Charakter.

Zum Zeitpunkt der Durchführung lagen sowohl die Implementing Regulation, als auch die Technical Design Documents lediglich in Entwurfsfassungen vor.[2]Dennoch galten mindestens folgende Annahmen über die technischen Vorgaben als gesichert:

1. Die Kommission wird generische Mechanismen für den Nachweisabruf vorgeben, die auf dem OASIS Standard RegRep v4 in Kombination mit eIDAS Token für die jeweils betroffene Person bzw. das betroffene Unternehmen basieren. Die Mechanismen sind im Teil iv: „Exchange Data Model (EDM)“ der TDD detailliert beschrieben.

   Im Zielbild der Registermodernisierung vom Januar 2021 war ebenfalls ein generischer Abrufstandard als Ziel formuliert worden[3]. Insofern war ein wesentlichen Erkenntnisinteresses des Pilotprojekts die Prüfung

[2]Dies ist zum Zeitpunkt der Finalisierung dieses Abschlussberichts, Mitte Mai 2022, leider immer noch der Fall.
[3]Einheitlicher Datenstandard, Abschnitt 3.2.1 „Technische Architektur“, Seite 10 des Zielbildes vom Januar 2021. Vom IT-Planungsrat mit der Entscheidung 2021/05 beschlossen.

des von der EU-Kommission in Teil iv der TDD vorgegebenen Exchange Data Model hinsichtlich seiner Eignung als „Einheitlicher Datenstandard“ im Sinne des Zielbildes vom Januar 2021.

2. Die Kommission wird zur Gewährleistung der sicheren Datenübermittlung zwischen Behörden verschiedener Mitgliedsstaaten den Standard AS4 CEF eDelivery vorgeben. Die Details sind ebenfalls in den TDD festgelegt. Es war bekannt, dass die *High level architecture* des OOTS kein Ende-zu-Ende Sicherheit unterstützen wird.

   Diese ist nicht konform zu nationalen Recht, denn § 7 Abs. 2 IdNrG fordert die Ende-zu-Ende Sicherheit zwischen Behörden unterschiedlicher Verwaltungsbereiche bei Einsatz der Identifikationsnummer. Insofern war klar, dass für die sichere Übermittlung von Nachrichten zwischen der abrufenden Stelle (Evidence Requester) und der übermittelnden Stelle (Evidence Provider) in Deutschland eine andere als die von der EU-Kommission zu erwartende Vorgabe gefunden werden muss.

   Das vom IT-Planungsrat beschlossene Zielbild vom Januar 2021 trifft in Abschnitt 3.2.1 (Seite 7) folgende Aussage: „Herzstück der modernen Registerlandschaft ist eine interoperable und sichere technische Architektur, die insbesondere auf bestehenden Anwendungen und Standards des IT-Planungsrats aufbaut und diese sinnvoll ergänzt, um dem breiten Anforderungsspektrum der föderalen Registerlandschaft gerecht zu werden“. Zu den Standards des IT-Planungsrats gehört insbesondere OSCI. Zudem sind die technikneutralen Vorgaben zu Datenübermittlungen in § 7 IdNrG ausweislich der Gesetzesbegründung wesentlich durch die in großen Teilen der Innenverwaltung vorhandene Infrastruktur motiviert, die auf dem Standard OSCI des IT-Planungsrats basiert.

   Insofern war ein weiteres, wesentliches Erkenntnisinteresse des Pilotprojekts die Prüfung der Frage, ob ein sicherer Datenaustausch zwischen der abrufenden Stelle (Evidence Requester) und übermittelnder Stelle (Evidence Provider) auf der Grundlage des Standards OSCI konform zu den Vorgaben des IdNrG mit Ende-zu-Ende Sicherheit erfolgen kann.

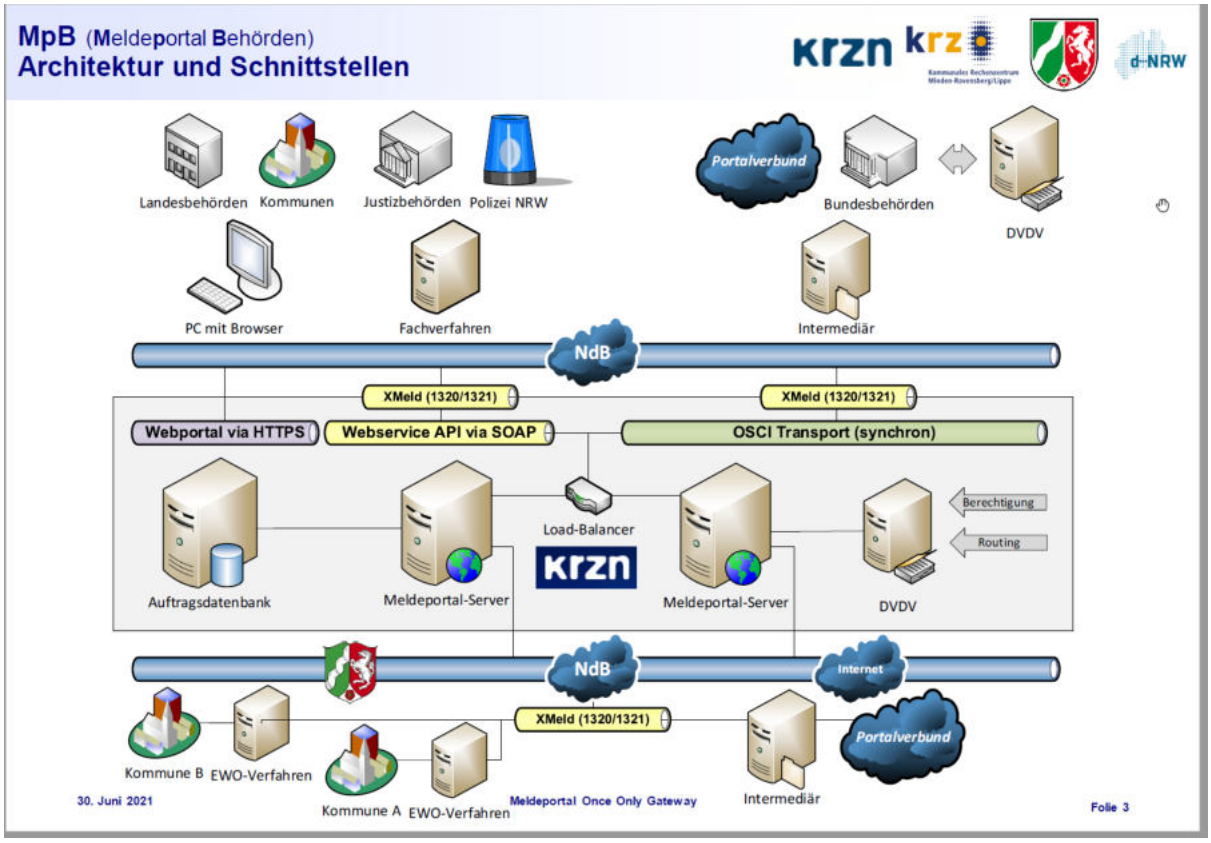
Die zu erwartenden Vorgaben der EU-Kommission betreffen in Deutschland Behörden, die in der Regel in nationale Informationsverbünde integriert sind. Dies ist beispielsweise für Meldebehörden der Fall. Sie sind aufgrund von Übermittlungsverordnungen des Bundes, also nationales Rechts, Bestandteil eines Informationsverbunden die auf den IT-Standards XInneres/XMeld und OSCI-Transport basieren. Zukünftig müssen sie außerdem an das OOTS der EU-Kommission angeschlossen werden, in denen ganz andere Anschlussbedingungen gelten.

Das Meldeportal Behörden des Landes NRW

Grundsätzlich könnten Meldebehörden direkt an das OOTS angeschlossen werden. Sinnvoller scheint aber die Alternative über eine spezialisierte Organisationseinheit, die unter anderem die Aufgabe hat, den Anschluss vieler Meldebehörden an das OOTS zu bündeln und die dabei entstehenden Aufgaben der Interoperabilität unterschiedlicher technischer Systeme zentral zu managen.

Das Kommunale Rechenzentrum Niederrhein (KRZN) betreibt für das Land NRW dessen „Meldeportal Behörden“. Dieses ist aufgrund des § 7 des Meldegesetzes für das Land Nordrhein-Westfalen (MG NRW) die zentrale Stelle für den automatisierten Abruf durch öffentliche Stellen des Landes NRW. Das *Meldeportal Behörden* unterstützt derzeit bereits unterschiedliche Schnittstellenformate für die Behörden, die Meldedaten abrufen wollen. Alle Meldebehörden des Landes NRW sind mittels des XÖV Standards XInneres / XMeld an das *Meldeportal Behörden* angebunden, das heißt, alle nach außen angebotenen Schnittstellen werden auf XMeld abgebildet (siehe Abbildung 1.1). Das Nordrhein-westfälische Portal ist in einem Portalverbund des Meldewesens wiederum mit den Portalen anderer Bundesländer vernetzt, so dass dem Grunde nach Abrufe von Meldedaten aus dem gesamten Bundesgebiet möglich sind. Im Jahr 2020 waren ca. 96.000 aktive Nutzer registriert, und es wurden knapp 43 Millionen Abrufe von Meldedaten bearbeitet.

Abbildung 1.1. Funktionsweise des Meldeportal Behörden in NRW



Das Meldeportal Behörden des Landes NRW bietet den abrufenden Behörden unterschiedliche Abrufschnittstellen, die alle auf XInneres / XMeld abgebildet werden. Im Pilotvorhaben 7 wurde gezeigt, dass eine Erweiterung um eine zusätzliche Schnittstelle nach den Vorgaben der EU-Kommission für SDG Nachweisabrufe grundsätzlich möglich ist.

Zusammenfassung des Erkenntnisinteresses

Insoweit kann die Aufgabenstellung des Pilotprojekts 7 wie folgt zusammengefasst werden: es war zu prüfen, ob das vom KRZN betriebene „Meldeportal Behörden“ um eine weitere Schnittstelle ergänzt werden kann, so dass

A. Nachweise von allen Meldebehörden des Landes NRW abgerufen werden können, ohne dass es einer Veränderung der Schnittstelle zwischen dem Meldeportal Behörden und den Meldebehörden bedarf (diese basiert unverändert auf XMeld);

B. Die Syntax und Semantik der Nachrichten zum Abruf beim Meldeportal Behörden durch Teil IV: Evidence Exchange der TDD bestimmt wird, weil dies nach derzeitigem Kenntnisstand die verbindliche Vorgabe für den Nachweisabruf im OOTS gemäß Artikel 14 der SDG Verordnung werden wird;

C. Die sichere Übermittlung der Nachrichten zum Nachweisabruf und dessen Übermittlung abweichend von den Vorgaben der EU-Kommission mit dem Standard OSCI des IT-Planungsrats erfolgt, weil nur so die Vorgabe zur Ende-zu-Ende Sicherheit gemäß § 7 IdNrG bei Datenübermittlungen im NOOTS erfüllt werden können, und weil dies der Vorgabe zur Verwendung von Standards des IT-Planungsrats aus dem Zielbild vom Januar 2021 entspricht.

Zu diesem Dokument: Um Risiken in einem Umfeld vielfach neuer Technologien und Infrastrukturmerkmale einzugrenzen, wurde im Erprobungsprojekt ein Durchstich des Nachweisabrufs von der Nachweisanforderung

(Evidence Requester, ER) bis zur Nachweislieferung (Evidence Provider, EP) umgesetzt, der die Vorgaben aufnimmt und beispielhaft umsetzt. Fragestellungen und Ergebnisse aus dem Durchstich werden evaluiert. Es wird gefragt, inwieweit die Ergebnisse verallgemeinert werden können und welcher Handlungsbedarf resultiert.

Praktische Fragen und Themen der Erprobung

- Passen die (durch die SDG-Umsetzung vorgesehenen) **eIDAS Identitätsparameter** in der Praxis auf den OZG-Nachweisabruf?
- Wie ist die durch das RegMoG geforderte **E2E-Sicherheit** im Rahmen einer **4-Corner-Infrastruktur** technisch umsetzbar?
- Wie können dabei die einzusetzenden **Transportprotokolle** (insbesondere OASIS AS4 und OSCI-Transport) entkoppelt werden von der technischen Anbindung der Online Services (ER) und registerführenden Behörden (EP)?
- Lässt sich der Standard XTA-Webservice in diesem Zusammenhang als **Mechanismus der Entkopplung** von beispielsweise Corner 1 und Corner 2 einsetzen?
- Wie würde in der Praxis im Rahmen einer **Kopfstellen-Architektur** ein dynamisches Routing funktionieren (= Adressierung der zuständigen Meldebehörde durch die Kopfstelle)?
- Wie kann im Rahmen einer Kopfstellen-Architektur **ein Once Only Format** (abgeleitet aus dem IA der SDG-VO-Umsetzung) mit den etablierten Formaten der Kopfstellen-Domäne (hier: XMeld) zusammenspielen?

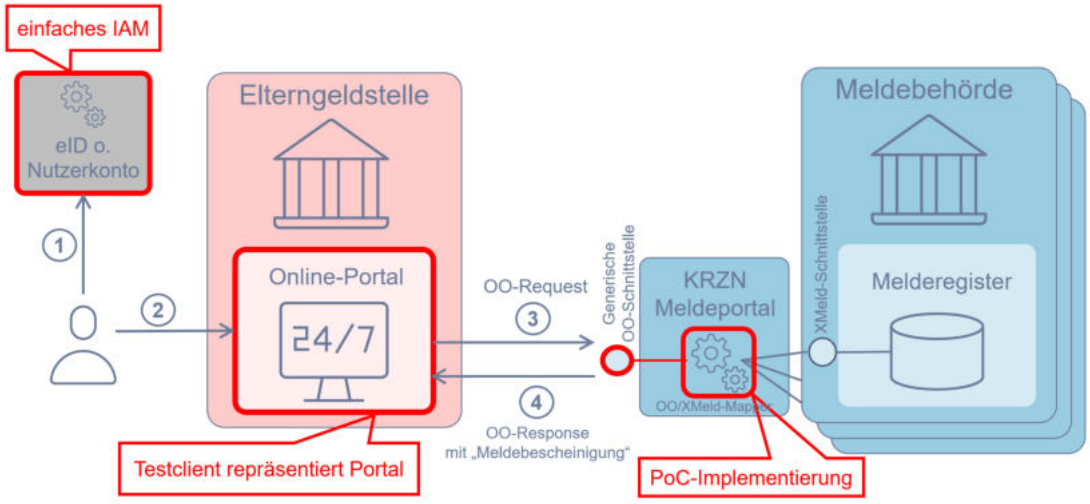
1.4. Proof of Concept

Hier wird beschrieben, wie das dem Erprobungsprojekt zugrundeliegende fachliche Szenario durch die Umsetzung in einem Proof of Concept (PoC) abgebildet wird. In dem unten dargestellten Diagramm sind das Gesamtszenario mit den realisierten Durchstich-Komponenten skizziert: Ein fiktives Verwaltungsportal („Online-Dienst“) fordert im Rahmen einer Verwaltungsleistung als Nachweis eine Meldebescheinigung gemäß § 18a BMG für den Antragsteller über eine generische Once Only Schnittstelle von der zuständigen Meldebehörde an.

Das Verwaltungsportal und dessen Online-Dienst wird im PoC durch eine einfache Webapplikation („Testclient") repräsentiert. Dieser Testclient bedient die Once Only Schnittstelle, die als PoC-Implementierung vom KRZN-Meldeportal bereitgestellt wird. Bestandteil der Schnittstellenimplementierung ist eine Komponente, die den Once-Only-Request auf eine XMeld-konforme Datenabrufnachricht abbildet ("OO/XMeld-Mapper“) und durch das KRZN-Meldeportal an das zuständige Melderegisterverfahren leitet. Die auf diesem Weg erhaltene XMeld-Antwort wird als Nachweis in die generische OO-Antwortnachricht transformiert und an den Testclient zurück geliefert.

Die in realen Szenarien vom Antragsteller durchzuführende Identifizierung mittels eIDAS bzw. Online-Ausweisfunktion (eID) wird im PoC ersetzt durch eine Authentifizierung an einer gebräuchlichen Standardkomponente für Identitätsmanagement (Keycloak). Die Komponente ist im PoC so angepasst worden, dass sie im Zuge der Authentifizierung Attribute zum Nutzer (Antragsteller) liefert, die hinsichtlich Format und Inhalt denen von eID exakt entsprechen.

Abbildung 1.2. Übersicht zum Proof of Concept



1.5. Ebenen der Nachrichtenstrukturen

Zu den Eckpunkten für den PoC zählt, dass auch nationale Once-Only-Abfragen sich an dem Stand der Vorgaben zur EU-SDG-Umsetzung (Technical Design Documents (TDD) for the Implementation of the Once Only Technical System (OOTS)) orientieren. Insbesondere gilt dies für die `Request` und `Response` Nachrichtenformate, die in den TDD spezifiziert sind. Ein Augenmerk bei der PoC-Implementierung war, die Handhabung mit diesen komplexen Strukturen zu erproben und zu erleichtern.

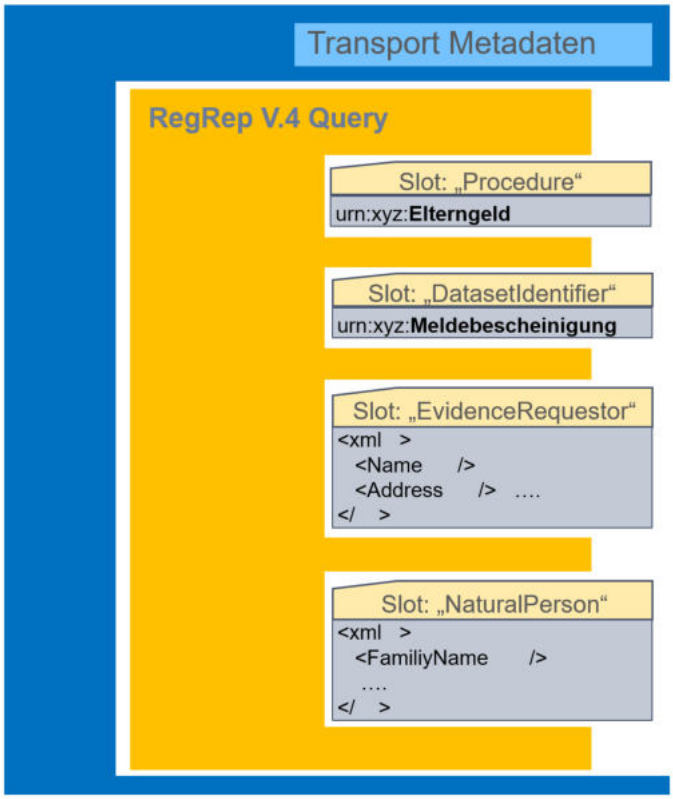
Die TDD geben die `QueryRequest` und `QueryResponse` Nachrichtenformate aus der OASIS RegRep Spezifikation vor. Drei verschiedene Spezifikationen bauen aufeinander auf und sind für die Konstruktion dieser Request- und Response-Strukturen zu berücksichtigen:

- **OASIS ebXML RegRep V.4, Part 2: Services and Protocols (ebRS)** Diese Spezifikation definiert das Schema der äußeren Nachrichtenstruktur, die im Wesentlichen als Container für die „Slots" dienen. Slot kennzeichnen bei ebXML RegRep einen Property-Mechanismus, bei dem beliebige Werte (XML-Strukturen) an Schlüsselnamen gebunden werden können.

- **Data Exchange Model zur Once-Only-Schnittstelle des OOTS** Dabei handelt es sich um eine Profilierung der RegRep-Query-Schnittstelle der EU-SDG-Arbeitsgruppe. Es werden obligatorische und optionale Slots mit dessen Semantik, Schlüsselnamen und Wertebelegung definiert.

- **Vocabulary-Schemata** Die Schemata für konkrete Slot-Werte bilden die unterste Ebene. Im Rahmen des PoC sind sowohl Schemata aus Core Vocabularies (ISA CV 1.1 beta) als auch eigene Schemata, die an CV orientiert sind und diese fachlich erweitern.

Abbildung 1.3. Schematische Darstellung einer Request nachricht im EDM



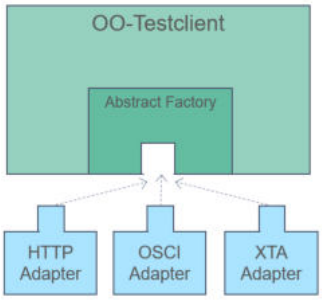
Die Konstruktion und das Parsen der Nachrichten wurde im PoC durch eine selbst entwickelte Bibliothek unterstützt, die von Details zu verwendeten Schemata und deren Versionen abstrahiert. Vor dem Hintergrund der nicht finalen Spezifikationen zum OO-Standard der SDG-EU-Umsetzung war ein Ziel des PoC, eine Abstraktion von den konkreten Nachrichtenausprägungen zu erproben. So konnte z.B. nachgewiesen werden, dass ohne Änderungen des Testclient-Quellcodes zwischen unterschiedlichen Versionen verwendeter Core-Vocabulary-Schemata zur Laufzeit gewechselt werden konnte.

1.6. Transport-Agnostik

In Übereinstimmung mit dem Architekturmodell galt es, den Nachrichtenaustausch zur Once-Only-Abfrage vom verwendeten Transportprotokoll zu abstrahieren. Die PoC-Implementierung sollte daher explizit die Protokollunabhängigkeit unterstützen und in der Architektur sichtbar ausweisen. Über das Transportprotokoll hinaus sollte auch die Kommunikationstopolgie von einem schlichten 2-Corner hin zu einem 4-Corner-Modell realisiert werden.

Dazu sind bei den exemplarischen *Evidence Requester* und *Evidence Provider* Implementierungen die Nachrichtenverarbeitung (Erzeugung und Auswertung) klar entkoppelt von Transportaufgaben (Senden und Empfangen). Diese Entkopplung erfolgte teilweise mittels gängiger Entwurfsmuster wie z.B. *Abstract Factory*, um verschiedene Transportimplementierungen (HTTP, XTA mit OSCI, optional XTA mit AS4) der PoC-Implementierung, die den *Evidence Requester* repräsentiert (OO-Testclient) transparent und austauschbar bereitzustellen.

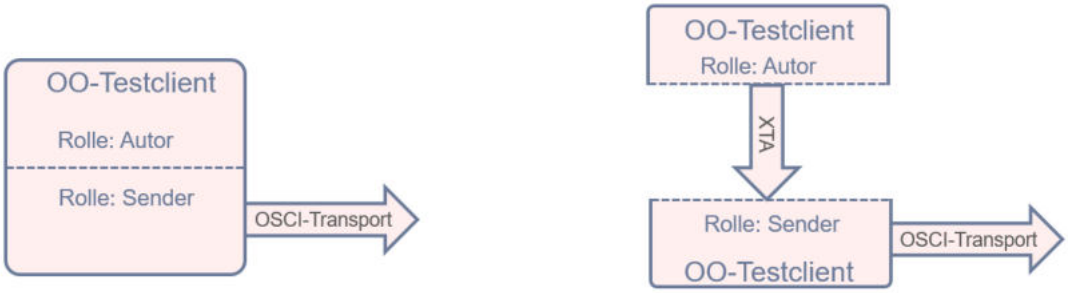
Abbildung 1.4. Testclient



Im Zuge der Iterationen der PoC-Implementierung sind nicht nur die unterstützten Transportprotokolle austauschbar erweitert (HTTP, OSCI), sondern auch die Kommunikationstopologie und die damit zugrundeliegende Systemarchitektur fortentwickelt worden. In den ersten Ausbaustufen erfolgte der Nachweisaustausch ausschließlich über eine 2-Corner-Architektur, d.h. der Testclient realisierte die logischen Rollen „Autor" und "Sender“ innerhalb einer Komponente (*Hinweis*: Die detaillierte technische Architektur des Testclients sieht zwar generell eine Trennung in Frontend- und Backendkomponente vor, die jedoch auf einer abstrakteren Architekturebene eine logische Komponente im Sinne eines Kommunikationsknotens („Corner“) repräsentieren).

Für die Topologieänderung von 2- auf 4-Corner ist der Testclient aufgetrennt worden in zwei physische Komponenten (Kommunikationsknoten). Zwischen diesen Komponenten erfolgte die Kommunikation mittels XTA, dabei wurde die Senderkomponente („XTA-Server") durch den "Governikus COM Despina“ realisiert. Dieses Auftrennen des Testclients ist im Diagramm illustriert.

Abbildung 1.5. Komponenten des Testclient



Gegenstand der Erprobung war, den Testclient beliebig zwischen Protokoll und Topologie auch zur Laufzeit wechseln lassen zu können, um so die Abstraktionsfähigkeit zu demonstrieren und nachzuweisen.

1.7. Ende-zu-Ende-Sicherheit

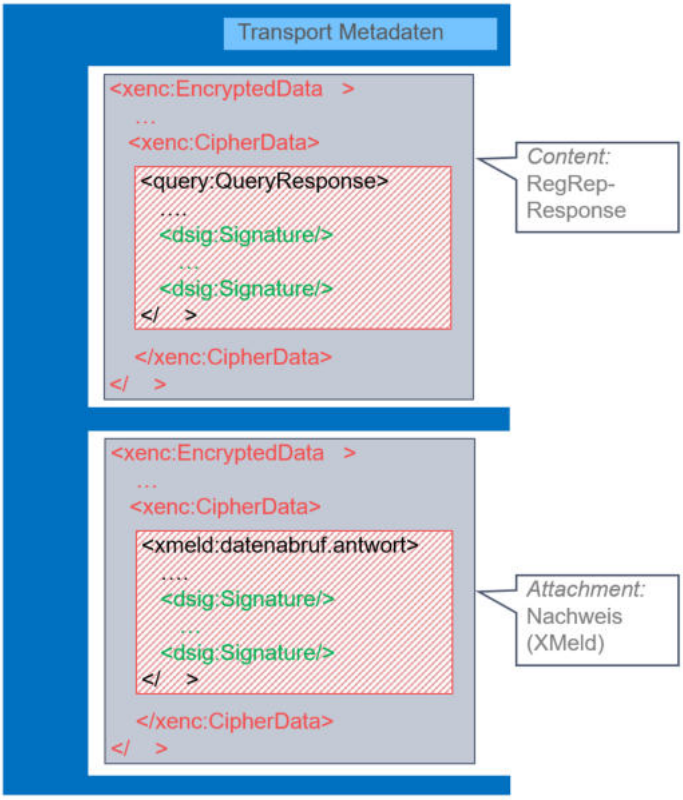
Die Technical Design Documents für das OOTS sehen für die Once Only Schnittstelle keine Mechanismen für eine Ende-zu-Ende-Sicherheit (E2E) vor, d.h. auf Ebene von Corner 1 (*Evidence-Requester*) und Corner 4 (*Evidence-Provider*) erfolgt weder eine Verschlüsselung der Nachrichten noch eine digitale Signatur. Gemäß TDD sind lediglich auf Ebene Corner 2 und 3 (zwischen den *eDelivery Access Points*) Verschlüsselung und Signatur gefordert.

Es war Gegenstand des PoC, im Durchstich sowohl eine Ende-zu-Ende-Verschlüsselung als auch eine digitale Signatur unter Berücksichtigung der Transportagnostik zu realisieren. Der PoC sollte ein mögliches Muster für eine nationale Once Only Schnittstellenspezifikation erproben, das trotz Austauschbarkeit der alternativen Protokolle OSCI und AS4 CEF eDeliverry zwischen den Corner 2 und 3 dennoch die E2E-Sicherheit gestattet.

Es sind daher Container-Formate für Signatur und Verschlüsselung zu verwenden, die nicht an Transportprotokolle bzw. deren Spezifikationen gebunden sind. Die Wahl fiel auf die W3C-Standards *XML Encryption* und *XML Digital Signature,* die beide auch innerhalb von OSCI-Transport und eDelivery AS4 Verwendung finden.

Alle XML-basierten Request- und Response-Nachrichten (RegRep-QueryRequest, RegRep-QueryResponse sowie der Nachweis in Form einer XMeld-Antwort) werden vom Testclient und der prototypischen OO-Schnittestellenimplentierung des KRZN-Meldeportals zunächst digital signiert und anschließend für den Leser (Corner 4) verschlüsselt. Die Signatur ist jeweils als sogenannte „Enveloped Signature“ ausgeführt worden, d.h. das XML-Signaturelement ist eingeschlossen in dem fachlichen XML-Dokument. Alle so signierten und verschlüsselten Nachrichten bzw. Nachweise sind XML-Dokumente mit dem Wurzelelement `EncryptedData` aus XML-Encryption.

Abbildung 1.6. Kryptografische Elemente bei der Übermittlung von Nachweisen



In Übereinstimmung mit den TDD zur SDG-EU-Umsetzung wurde auch im PoC der Nachweis als Attachment einer Antwortnachricht übermittelt, während die Metainformationen zum OO-Response in den RegRep-QueryResponse als direkter Content gepackt wurde. Dabei wurden beide Antwortbestandteile im PoC (QueryResponse und Nachweis) jeweils separat signiert und verschlüsselt. Eine übergreifende Signatur beider Bestandteile, die Metainformationen und Nachweis kryptographisch bindet, wäre sicher angemessener und wünschenswert. Dies ist aus Aufwandsgründen im PoC nicht erfolgt, sollte aber in einer realen Spezifikation wohl berücksichtigt werden.

1.8. Abbildung auf XMeld

Der PoC-Durchstich sollte praktisch erproben, ob ein über die generische Once Only Schnittstelle angefragter Nachweistyp „Meldebescheinigung“ abbildbar ist auf die existierenden XMeld-Schnittstellen der Melderegisterfachverfahren. Konkret ist die Nachricht `xmeld:datenabrufe.suchanfrage.1320` vom Meldeportal Behörden zur zuständigen kommunalen Meldebehörde verwendet worden, um die Nachweisdaten aus dem Register zu lesen. In Gegenrichtung wurde die korrespondierende `xmeld:datenabrufe.antwort.1321` als Nachweis genutzt, der unverändert als Anhang (Attachement) der EDM *Response* Nachricht beigefügt wurde.

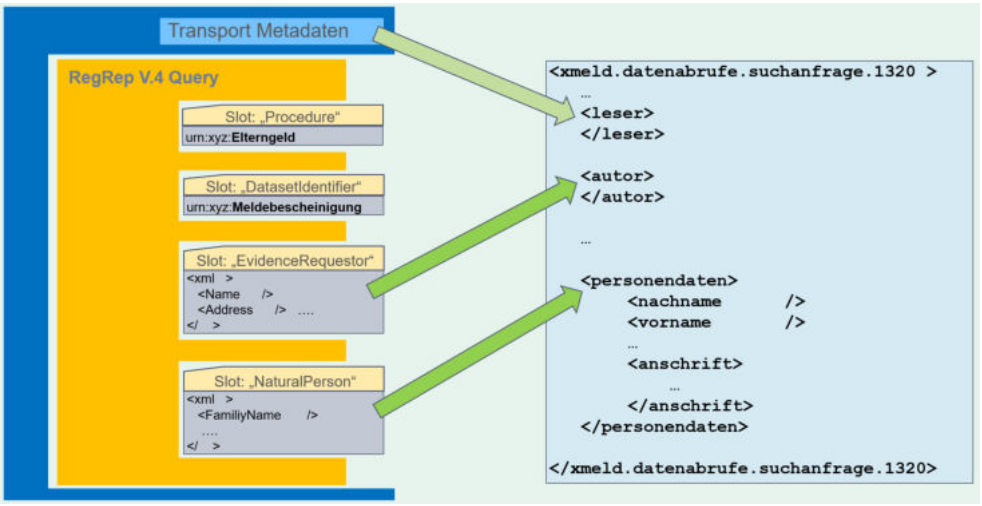
Die Transformation von den generischen OO-Anfragenachricht auf die XMeld-Suchanfrage 1320 ist über XSLT-Skripte realisiert worden. Die Abbildung vom ReqRep-Query-Request und dessen obligatorischen Slot-Einträgen war fast vollständig definierbar. Lediglich die in der XMeld-Suchanfrage obligatorischen Daten zum Leser (hier:

der *Evidence-Provider*, also das Melderegister) ist nicht enthalten im generischen OO-Request. Hintergrund ist , dass das EDM im OOTS davon ausgeht, dass dem *Evidence-Requester* selbst zum Zeitpunkt der Anfrage der zuständige *Evidence-Provider* noch gar nicht bekannt ist und erst durch zentrale Services und eine DSD Verzeichnisabfrage ermittelt wird (“Routing as a Service”).

In der PoC-Implementierung sind die Daten in der XMeld-Anfragenachricht zum Leser durch einen prototypisch umgesetzten AGS-Router ermittelt worden: Aufgrund der Angaben im OO-Request zum Subject (Postleitzahl und Wohnort der betroffenen Person) ist mittels AGS-Router der AGS und damit der Zuständigkeitsbereich der zu adressierenden Meldebehörde ermittelt und in die XMeld-Leser-Datenstruktur geschrieben worden.

In einer realen 4-Corner-Implementierung mit Ende-zu-Ende-Verschlüsselung könnte es ggfs. erforderlich werden, die Adressierungsinformationen zum *Evidence-Provider* (entspricht hier XMeld-Leser) auf Ebene der Transportnachricht (Corner 2/3 Kommunikation) zu übermitteln. Das wäre vermutlich dann der Fall, wenn man die Haltung einnimmt, dass das Meldeportal Behörden lediglich eine *intermediary platform* ist, während die für die betroffene Person zuständige Meldebehörde der Evidence Provider ist. Denn in diesem Fall hätte das Meldeportal Behörden als Corner 3 (Kopfstelle oder Provider-Gateway) keinen Zugriff auf die verschlüsselte OO-Anfragenachricht und den darin enthaltenen Subject-Daten. Vielmehr müssten die vom *Evidence-Requester* (Corner 1) durch Verzeichnisabfragen ermittelten Daten zum *Evidence-Provider* auch auf der Strecke Corner 2/3 transportiert werden - z.B. als SOAP-Header (OSCI) oder MessageProperties (eDelivery AS4). In diesem Fall könnte das Meldeportal Behörden wegen der Verschlüsselung keine Transformation auf das XMeld Format durchführen, so dass die jeweils zuständige kommunale Meldebehörde mit einer zusätzlichen Schnittstelle für den generischen Abrufstandard ausgestattet werden müsste.

Abbildung 1.7. Schematische Darstellung der Abbildung von EDM auf XMeld



1.9. Zusammenfassung der Ergebnisse

Das in 2020 erarbeitete Architekturmodell sowie weitere im Laufe des Erprobungsprojekts identifizierte Eckpunkte gaben den grundsätzlichen konzeptionellen Rahmen für die Realisierung eines Durchstichs als Proof of Concept (PoC) vor. Die für die Architektur des PoC eingesetzten Prinzipien und Muster werden in den folgenden Abschnitten präzise beschrieben. Es werden dabei Erkenntnisse formuliert, die in der Auseinandersetzung mit der OO-Architektur des Nachweisabrufs erarbeitet wurden.

Hinsichtlich des in Abschnitt 1.3 formulierten Erkenntnisinteresses können die Ergebnisse des Pilotprojektes 7 wie folgt zusammengefasst werden:

A. Das Meldeportal Behörden des Landes NRW konnte —zumindest im Rahmen des *Prooof of Concept* —mit einer zusätzlichen Schnittstelle für Nachweisabrufe gemäß der von Seiten der EU-Kommission zu erwartenden Vorgaben ausgestattet werden. Damit könnten Nachweise von daran angeschlossenen Behörden mit Mechanismen des SDG Evidence Exchange abgerufen werden, ohne dass es dafür Veränderungen an bestehenden Schnittstellen zwischen dem Meldeportal und den kommunalen Meldebehörden bedarf.

Ob dieses Ergebnis als Grundlage einer generellen Handlungsempfehlung für eine schnelle und wirtschaftliche Umsetzung der Registermodernisierung tauglich ist, hängt jedoch von der rechtlichen und fachlichen Würdigung des Meldeportal Behörden ab. Diese Fragestellung konnte im Rahmen des Erprobungsprojektes lediglich identifiziert, aber nicht abschließend untersucht werden. Zwei Positionen scheinen plausibel:

I. Da das Meldeportal Behörden gemäß des Nordrhein-Westfälischen Meldegesetzes als „zentrale Stelle für den automatisierten Abruf [von Meldedaten] durch öffentliche Stellen“ bestimmt ist, scheint die Annahme berechtigt, dass es sich dabei um den *Evidence Provider* im Sinne der OOTS Architektur handelt, denn dieser ist definiert als „ a competent authority … that lawfully issues structured or unstructured evidence“. In diesem Fall sind die kommunalen Meldebehörden zumindest aus Sicht des europäischen OOTS *out of scope*. Zudem könnte das Meldeportal Behörden auch in rechtlicher Hinsicht als „übermittelnde Stelle“ angenommen werden. Die Vorgaben des § 7 Abs. 2 IdNrG zur Datenübermittlung zwischen öffentlichen Stellen bezieht sich dann auf die Strecke zwischen einer abrufenden Behörde (dem Evidence Requester) und dem Meldeportal Behörden.

   Bei dieser Sichtweise bedarf es - ohne Berücksichtigung der Anforderungen des Artikel 2 RegMoG zum Datenschutzcockpit - keiner Anpassung der Schnittstellen kommunaler Meldebehörden.

II. Alternativ kann das Meldeportal Behörden als „intermediary platform“ im Sinne des SDG Durchführungsrechtsakts verstanden werden: “a technical solution through which evidence providers or evidence requesters connect … to evidence providers or evidence requesters from other Member States”. Bei dieser Sichtweise wäre der Evidence Provider die jeweils für die betroffene Person zuständige kommunale Meldebehörde. Hinsichtlich der nationalen Gesetzgebung könnte das bedeuten, dass die Vorgaben des § 7 Abs. 2 IdNrG sich auf die Strecke zwischen einer abrufenden Behörde (dem Evidence Requester) und der zuständigen Meldebehörde beziehen.

   Dies könnte möglicherweise dazu führen, dass rechtliche Vorgaben eine Ende-zu-Ende Verschlüsselung im nationalen Kontext auf der Strecke zwischen der abrufenden Behörde und der kommunalen Meldebehörde erfordern. In diesem Falle könnte das Meldeportal Behörden den Service der Konvertierung zwischen dem generischen Abrufstandard und dem XMeld Standard nicht anbieten, denn dies setzt den Zugriff auf Inhaltsdaten zwingend voraus. Dies würde unvermeidlich dazu führen, dass es notwendig wird, sämtliche IT-Verfahren der kommunalen Meldebehörden mit einer zusätzlichen Schnittstelle gemäß der Schnittstellenvorgaben des OOTS der Europäischen Kommission auszustatten.

Wegen der damit verbundenen fachrechtlichen Aspekte, und der weitreichenden Folgen einer Bewertung wird empfohlen, dass die Analyse nicht ausschließlich durch die Gremien des Projekts „Registermodernisierung“ erfolgt, sondern dass sie eng mit den jeweils fachrechtlich zuständigen Stellen abgestimmt wird. Im konkreten Beispiel sollten es Arbeitsgruppen der Melderechtsreferenten des Bundes und der Länder sein, analoge Fragestellungen wird es aber auch in anderen fachlichen Domänen geben.

Innerhalb des Erprobungsprojektes gab es keine einheitliche Einschätzung in dieser Frage. Allerdings wurden zwei relevante Hinweise gegeben, die beide eher die erste der Alternativen nahelegen (Meldeportal Behörden als Evidence Provider):

- Die klare Aufgabenzuweisung einer zentralen Stelle für alle Auskünfte zu Meldebehörden durch das Meldegesetz des Landes NRW spricht eher gegen die Sichtweise einer „technical solution“ und mehr für „ a competent authority that lawfully issues evidences“;

- Das Meldeportal Behörden ist Teil eines Verbunds von Behörden auf Landesebene, die jeweils die Aufgabe haben, Auskünfte zu Meldedaten zu bündeln um die Komplexität der dahinter liegenden Landschaft kommunaler Meldebehörden zu verbergen. Die meisten dieser Behörden in anderen Bundesländern als NRW sind als Spiegelregister ausgeführt, das heißt, dass sie im eigenen Datenbestand über Nachweise verfügen (während das Meldeportal Behörden in NRW den jeweiligen Nachweis im Moment des Abrufs von der zuständigen Meldebehörde besorgt).

B. Die Syntax und Semantik der in *Part IV: Evidence Exchange* der TDD beschriebenen Nachrichten konnte grundsätzlich auf die für den Abruf von Meldedaten bundesweit verbindlichen XMeld-Nachrichten 1320 und 1321 abgebildet werden. Dies ist ein wichtiges positives Indiz für die Eignung des von Seiten der EU-Kommission voraussichtlich vorgegebenen Standards für den *Evidence Exchange* als „Einheitlicher Daten-

standard“ im Sinne des vom IT-Planungsrat beschlossenen Zielbilds der Registermodernisierung vom Januar 2021.

Der größte konzeptionelle Unterschied war in einem Bereich festzustellen, der streng genommen nicht dem Standard für den Nachweisabruf zuzurechnen ist, sondern der„High level Architecture“ des Gesamtsystems, nämlich dem „Routing as a Service“.

XMeld Nachrichten für den zwischenbehördlichen Bereich sind stets so aufgebaut, dass sie im „Nachrichtenkopf“ Angaben zu beiden an der Datenübermittlung beteiligten Behörden enthalten. Dies entspricht der Analogie eines klassischen Briefes, der auf dem Briefumschlag Angaben zum Absender enthalten soll, und Angaben zum Empfänger enthalten muss. Ohne Angaben zum Empfänger kann die Nachricht nicht zugestellt werden.

Im Unterschied dazu enthält eine Nachweisabruf in EDM Syntax nur Angaben zur abrufenden Stelle (dem *EvidenceRequester)* und zum benötigten Nachweistyp, aber keine Angaben zur übermittelnden Stelle, weil es Aufgabe des Data Service Directory (DSD) ist, anhand des Nachweistyps und ggfs. weiterer Angaben die dafür originär zuständige Behörde zu ermitteln.

Dieser konzeptionelle Unterschied des Routings zwischen XÖV Standards in bewährten und weit verbreiteten Informationsverbünden der öffentlichen Verwaltung Deutschlands einerseits, und dem von Seiten der EU konzipierten technischen System gemäß Artikel 14 der SDG Verordnung andererseits war im Pilotprojekt unerwartet. Die Auseinandersetzung mit diesem Sachverhalt hat zu einem deutlich besseren Verständnis des Dienstes „Routing as a Service“ im OOTS geführt, und wird sich außerdem auf die Konzeption von „Kopfstellen“ auswirken.

Darüber hinaus hat die intensive Auseinandersetzung mit dem von Seiten der EU-Kommission vorgesehenen Nachrichtenformat zu wichtigen Erkenntnis hinsichtlich der Validierung der Nachrichten geführt, also der Konformität zu Geschäftsregeln, die auch aus nationalen Vorgaben resultieren können. So gibt es beispielsweise in Verordnungen des Bundes Vorgaben zum Zeichensatz, der bei der Übermittlung von Meldedaten zwingend zu beachten sind, die aber keine Entsprechung in den Geschäftsregeln des OOTS haben. Es konnte nachgewiesen werden, dass die von der KoSIT im Auftrag des IT-Planungsrats herausgegebene Anwendung „Validator“ gut geeignet ist, sowohl die Vorgaben des OOTS, als auch ergänzende Regeln aus bundes- oder landesrechtlichen Vorgaben zu prüfen.

C. Die grundsätzliche Eignung der Standards OSCI und XTA für eine Datenübermittlung zwischen abrufender und übermittelnder Behörde gemäß der Anforderungen des IdNrG an eine Ende-zu-Ende Sicherheit konnte nachgewiesen werden, obwohl Konfigurationsprobleme im PoC einer reibungslose Demonstration entgegenstanden. Insbesondere haben die Ergebnisse des Pilotprojektes die Überzeugung bestätigt und verstärkt, dass XTA 2 das Mittel der Wahl ist, um im 4-Corner Modell möglichst unabhängig von dem Zwischen den Cornern 2 und 3 verwendeten Transportprotokoll zu werden. Diese Erkenntnis ist von hoher Relevanz, weil absehbar ist, dass der nationale Standard OSCI des IT-Planungsrats mittelfristig zumindest in bestimmten Teilbereichen der nationalen Infrastruktur von europäischen Standards auf der Basis von AS4 ersetzt oder ergänzt werden könnte, wenn funktionale und sicherheitstechnische Ebenbürtigkeit festgestellt werden kann (siehe Abbildung 1.8).

Abbildung 1.8. XTA für Unabhängigkeit von Transportstandards

Die Nutzung von XTA 2 führt zu einer weitgehenden Unabhängigkeit vom Transportprotokoll, und unterstützt somit die Möglichkeit eines verstärkten Einsatzes des europäischen Transportstandards AS4 CEF eDelivery

Das Pilotvorhaben hat aber auch deutlich gemacht, dass die Umsetzung der Ende-zu-Ende Sicherheit mit XTA und OSCI derzeit noch mühsam und aufwändig ist. Für eine massenhafte Umsetzung im Kontext der Registermodernisierung bedarf es deutlicher Verbesserungen im Bereich der Dokumentation, beispielsweise durch Klarstellungen und Präzisierungen zur Nutzung der Standards im 4-Corner Modell, aber auch *Best-Practices* und Handlungsleitfäden. Es bleibt zu prüfen, ob Optimierungen in der OSCI-Bibliothek des IT-Planungsrats und ggfs. auch weitergehende Maßnahmen im Sinne umfangreicher Referenzimplementierungen zur einfacheren Umsetzung der Ende-zu-Ende Sicherheit in einer Infrastruktur für die Registermodernisierung beitragen können. [4]

[4] In die gleiche Richung gehen Erkenntnisse eines vom Land NRW initiierten Praxistests für den Einsatz von XTA und OSCI für die Übermittlung von Sozialdaten, über dessen Ergebnisse zur 38. Sitzung des IT-Planungsrats berichtet werden wird. Siehe Ziffer 4 des Beschlusses 2022/03.

Kapitel 2. Rahmenbedingungen

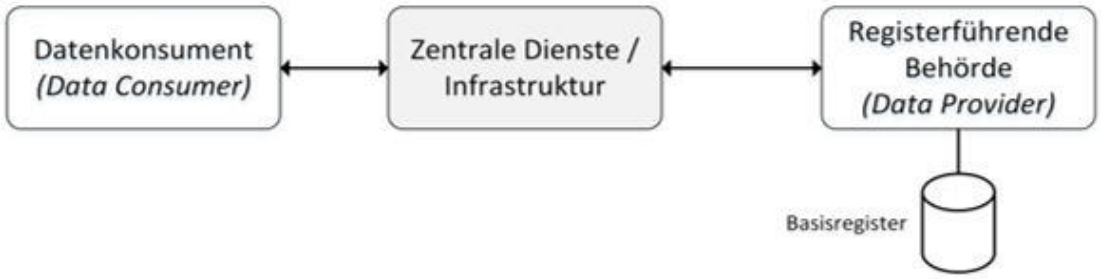
2.1. Prämissen aus dem Architekturmodell von 2020

Die wichtigsten Prämissen für die technische Umsetzung der Registermodernisierung gingen Ende 2020 aus den Abstimmungen der UAG Architekturmodell von 2019/20 hervor.

Zu diesen Prämissen zählten:

- Die Registermodernisierung ist ein **Infrastrukturprojekt**, welches einerseits in der Bereitstellung einer (zentralen) Infrastruktur für den Zugriff auf Registerdaten besteht und andererseits in der Anbindung von auszuwählenden (Basis)Registern und Datenquellen (Lieferanten von Daten) an diese Infrastruktur. Sinn der Anstrengung ist der Nutzen für Datenkonsumenten, unter denen zuallererst die OZG-Umsetzung mit ihren Qualitätszielen zu nennen ist.

Abbildung 2.1. Infrastruktur und nutzenden Komponenten



- Die **Bereitstellung der benötigten Infrastruktur** startet nicht bei Null, sondern soll geleistet werden, indem die seit 2006 sukzessive aufgebaute länderübergreifenden Messaging Infrastruktur (Anwendungen und Standards des IT-Planungsrats) weiterentwickelt wird. Am Betrieb dieser Infrastruktur sind Bund, Länder und eine Vielzahl von technischen IT-Dienstleistern beteiligt.

- Die **Umsetzung der SDG-Verordnung** in Deutschland (EU-übergreifender Nachweisabruf), die eine bestimmte technische Architektur vorgibt, soll anschlussfähig an diese modernisierte Infrastruktur realisiert werden. In die Umsetzung der RegMo in Deutschland gehen also die EU-Vorgaben ein.

- Die Anforderungen für die Umsetzung der RegMo in Deutschland (Nachweisabruf DE-DE im Rahmen der OZG-Umsetzung) gehen aber weiter. Sie ergeben sich aus dem RegMoG und formulieren in besonderem Maße Anforderungen an den Schutz personenbezogener Daten.

  - **bereichsübergreifende** Datenkommunikation ist über **neutrale Vermittlungsstellen** durchzuführen

  - dafür ist eine vollwertige Ende-zu-Ende-Sicherheit im Rahmen einer 4-Corner-Infrastruktur zu schaffen, die in bisherigen Infrastrukturen (eDelivery, OSCI-XTA) nur ansatzweise realisiert worden ist[1]

  - außerdem wird für nutzerbezogene Datentransparenz ein Datenschutzcockpit bereitgestellt

- **Generischer Once Only Standard**. Für die möglichst weitgehende Entlastung der Datenkonsumenten (deren Bedürfnisse als Nutzer priorisiert sind) wird ein Datenformat für den Nachweisabruf benötigt, das einsatzfähig ist unabhängig von der Fachlichkeit, der ein gegebener Nachweistyp zugeordnet ist (Nachweistyp Meldebescheinigung gemäß Bundesmeldegesetz des Innenressorts; Nachweistyp Privatführungszeugnis gemäß Bundeszentralregistergetz der Justiz).

Quellen:

[1]Nach unserem kenntnisstand ist das in der BSI TR-03123 beschriebene XML-Datenaustauschformat für hoheitliche Dokumente (XhD) das einzige, welches die Ende-zu-Ende Verschüsselung zwischen den beiden jeweils beteiligten Behörden verbindlich vorgibt.

- Architekturmodell von 2020 (Autor Frank Steimke, diskutiert und abgestimmt in der UAG Architekturmodell des Kooperationsprojekts Registermodernisierung)
- Zielbild für die Umsetzung der Registermodernisierung (im März 2021 vom IT-Planungsrat beschlossen)

2.2. Ziele der Erprobung

2.2.1. Motive der Erprobung (Stand Ende 2020)

Eine Reihe von Fragen und Risiken, die Ende 2020 erkannt werden, legen eine praxisnahe Erprobung in 2021 nahe.

Die von der EU-KOM vorgesehenen Komponenten eines Once Only Rahmenwerks unterscheiden sich grundlegend von den technischen Lösungen, die das XÖV Rahmenwerk prägen. Es liegen bisher keine Erfahrung mit der Praxistauglichkeit dieser Komponenten und den zu ihrer Anwendung erforderlichen Tools vor.

Sinn und Zweck der Erprobung in Pilotprojekt 7

Die Erprobung soll helfen, die Praxistauglichkeit der von der EU vorgeschlagenen Lösungsansätze besser einschätzen zu können und die Rahmenbedingungen für den Aufbau eines technischen System für Once Only in Deutschland zu schärfen.

Gespräche in den einschlägigen EU Work Packages WP 2, WP 4 und WP 7 des Projektes zur Umsetzung der SDG Verordnung in 2020 zeigen, dass dort alles andere als eine vollständige Sicherheit zum Zusammenspiel der ins Auge gefassten Komponenten und Technologien erreicht ist.

Vor diesem Hintergrund wird für das Pilotprojekt 7 eine *schrittweise Erprobung* für den Nachweisabruf mit wenigen Basisregistern vorgeschlagen.

Als Rahmenbedingungen für die Erprobung wurden im Dezember 2020 die folgenden Prämissen formuliert:

- Die Erprobung ist ein zeitlich befristetes Teilprojekt im Rahmen des Steuerungsprojektes Registermodernisierung. Es umfasst die Aktivitäten für die festgelegten Nachweise sowie Querschnittaufgaben.
- Die Erprobung hat primär die neuen Technologien und Methoden im Fokus, soll aber auch bestimmte rechtliche Aspekte berücksichtigen.
- Die Erprobung findet im kleinen Kreis mit ausgewählten Partnern im nationalen Kontext statt.
- Es soll ein Durchstich für den Abruf von Nachweisen gemäß Once Only Rahmenwerk entwickelt werden.
- Das Ziel der Erprobung besteht darin, Erfahrungen mit den neuen Technologien zu sammeln und Empfehlungen für die Anwendung in der Fläche zu entwickeln. Es ist nicht zu erwarten, dass am Ende der Erprobung einsatzfähige Produkte (Piloten) entstehen.
- Die Erprobung erfolgt primär für den Einsatz im nationalen Kontext (Once Only als Voraussetzung für OZG Verwaltungsleistungen gemäß Reifegrad 4).
- Da es noch keine finalen Vorgaben für die SDG Architektur gibt, sollen auch Lösungsansätze und Technologien des EU-Projektes DE4A geprüft werden.
- Bei der Auswahl der Geschäftsvorfälle und Nachweise soll die OZG Priorisierung und die Relevanz für die SDG Verordnung berücksichtigt werden.

2.2.2. Gegenstände von Pilotprojekt 7

Das Pilotprojekt 7 des Steuerungsprojektes Registermodernisierung des IT-Planungsrat erprobt Lösungsansätze für die technische Umsetzung der Registermodernisierung gemäß Zielbild.

Diese Lösungsansätze beziehen sich einerseits auf Infrastrukturthemen:

- 4-Corner-Modell und E2E-Sicherheit / für die rechtskonforme Umsetzung des Registermodernisierungsgesetzes
- Kopfstellen-Architektur / für den effizienten Zugang zu Domänen nachweisliefernder Stellen
- Entkopplung der Evidence Provider und Evidence Requester von den zu verwendenden Transporttechnologien / für die effiziente Umsetzung der Remote-Kommunikation innerhalb Deutschlands einerseits und im Austausch mit anderen Mitgliedsstaaten der EU andererseits

Andererseits sind für den Einsatz vorgesehene Technologien zu Nachrichten- und Datenformaten zu erproben, die im Zusammenhang der EU-Vorgaben sowie nationalen Rahmenbedingungen zu definieren bzw. zu konkretisieren sind

- OASIS RegRep4 / durch die EU vorgegebenes Format für die Request-Response-Syntax des Nachweisabrufs (Kommunikation zwischen Evidence Requester und Evidence Provider)
- EU ISA^2 Core Vocabularies / für die EU-übergreifend einheitliche Beschreibung der betroffenen Personen, ihrer Anschriften usw.
- XTA-Webservice / für die Anbindung der Evidence Requester und Evidence Provider an die Messaging Infrastruktur
- OSCI-Transport bzw. OASIS AS4 als Technologie bzw. Format für die Remote-Nachrichtenkommunikation

Besondere Fragestellungen der Interaktion der nationalen und internationalen Ebene

- Funktioniert eine Kopplung europäischer und deutscher Nachrichtenformate? Die Kopfstellen-Architektur bietet die Chance, die SDG-konformen Anfragen in domänenspezifische Formate (hier das in Deutschland etablierte XMeld) zu konvertieren und so die nachweisliefernden Stellen (hier Meldebehörden) zu entlasten.
- Welche Rechtsgrundlagen regeln das Verhalten der Nachweislieferanten in Deutschland? Die Meldebehörden in Deutschland sind auf Datenabrufe und Auskünfte nach definierten Passagen des deutschen Melderechts (BMG) eingestellt und bieten entsprechende Dienste an. Es ist zu prüfen, ob sich diese für die SDG-konforme Nachweislieferung nachnutzen lassen.

2.2.3. Ziele der Durchstichumsetzung in 2021

In direktem Zusammenhang mit der Durchstich-Entwicklung werden die Fragestellungen der Erprobung verfolgt. Dabei sind die Ergebnisse aus dem Durchstich zu evaluieren. Es ist zu fragen, inwieweit sie verallgemeinert werden können und welcher Handlungsbedarf ggf. resultiert.

Im Zusammenhang der Durchstichentwicklung lassen sich eine Reihe von Fragen praxisnah beantworten:

- Passen die (durch die SDG-Umsetzung vorgesehenen) eIDAS Identitätsparameter in der Praxis auf den OZG-Nachweisabruf?
- Wie ist die durch das RegMoG geforderte E2E-Sicherheit im Rahmen einer 4-Corner-Infrastruktur technisch umsetzbar?
- Wie können dabei die einzusetzenden Transportprotokolle (insbesondere OASIS AS4 und OSCI-Transport) entkoppelt werden von der technischen Anbindung der Online Services (Evidence Requester) und registerführenden Behörden (Evidence Provider)?
- Lässt sich der Standard XTA-Webservice in diesem Zusammenhang als Mechanismus der Entkopplung von beispielsweise Corner 1 und Corner 2 einsetzen?
- Wie würde in der Praxis im Rahmen einer Kopfstellen-Architektur ein dynamisches Routing funktionieren (= Adressierung der zuständigen Meldebehörde durch die Kopfstelle)?

- Wie kann im Rahmen einer Kopfstellen-Architektur ein Once Only Format (abgeleitet aus dem IA der SDG-VO-Umsetzung) mit den etablierten Formaten der Kopfstellen-Domäne (hier: XMeld) zusammenspielen?

Quellen

Erprobung eines Once Only Rahmenwerks. Zur Vorbereitung eines technischen Systems für Once Only in Deutschland; Frank Steimke, KoSIT (Fassung vom 08.10.2020

2.3. Fachliches Szenario für die Erprobung

2.3.1. Anwendungsfall Nachweisabruf - Meldebescheinigung

Für die Erprobung wird ein gut verstandener Anwendungsfall ausgewählt, der hier strukturiert beschrieben wird. Es werden die Gründe erläutert, warum er sich als Gegenstand der Erprobung eignet.

Beim kommunalen Melderegister handelt es sich um ein amtliches Verzeichnis, in dem jeder Einwohner der Kommune mit seiner aktuellen Anschrift registriert ist. Die Meldebescheinigung dient dazu, Meldedaten einer Person amtlich zu belegen bzw. zu übermitteln.

Die Melderegisterauskunft kann in einfacher Form von öffentlichen und privaten Stellen, oder in erweiterter Form nur von öffentlichen Stellen angefordert und vom zuständigen Einwohnermeldeamt erteilt werden. Daneben kann vom zuständigen Einwohnermeldeamt eine amtliche Meldebestätigung sowie eine Bescheinigung des Wohnsitzes ausgestellt werden.

Tabelle 2.1. Bezug zur OZG Verwaltungsleistung

OZG Verwaltungsleistung	**Themenfeld 6:** OZG-Querschnittsleistungen.
	Themenbereich 6.1: Querschnitt Bürger.
	Nr. der Verwaltungsleistung: 10559 Meldebestätigung und -registerauskunft.
	Federführung Themenfeld: BMI und Berlin (Umsetzung)
SDG Verfahren und Nachweis (Annex II)	**Verfahren:** Requesting Proof of Residence (Beantragung eines Wohnsitznachweises)
	Nachweis: Confirmation of registration at the current address (Bestätigung der Meldung an der aktuellen Adresse)
Basisregister	Melderegister gemäß § 3 BMG
Registerführende Behörde (Data Provider)	**Meldebehörde** gemäß § 1 BMG. Die Zuständigkeit der Meldebehörde ergibt sich auf der Ebene von Gemeinden nach dem Regionalprinzip. Ein **Portal** für Meldedaten gemäß § 49 Abs. 3 BMG (ggfs. in Verbindung mit der Portalverordnung - PortalV).
Abrufende Stellen (Data Consumer)	a) **Behörden:** Zunächst soll der Abruf durch öffentliche Stellen betrachtet werden, die Meldedaten zur Wahrnehmung ihrer jeweiligen Aufgaben benötigen (automatisierter Abruf gemäß §38, 39 BMG), weil dies für die Umsetzung von Once Only im OZG Kontext eine besonders hohe Relevanz hat. b) **Private:** Ggfs. kann in einem zweiten Schritt die einfache Melderegisterauskunft gemäß § 49 BMG zum Zweck der Bestätigung der Meldung an der aktuellen Adresse im nationalen Kontext zur Vorbereitung des Verfahrens nach Artikel 6 Absatz 1 der SDG Verordnung erprobt werden
Rechtsgrundlagen	• § 18 BMG: Meldebescheinigung bzw. der neue § 18a: Meldedatensatz zum Abruf

	• § 38, §39 BMG Datenübermittlungen zwischen öffentlichen Stellen / Automatisierter Abruf für Once Only zwischen Behörden, in Verbindung mit der BMeldDAV.
Relevanz	Die OZG Verwaltungsleistung hat eine besonders hohe Relevanz für die OZG Umsetzung, weil die Bestätigung der vom Antragsteller gemachten Angaben häufig als **Voraussetzung für andere Verwaltungsleitungen** gilt. Durch eine Once Only Realisierung können Bürger davon entlastet werden, selbst eine Meldebescheinigung besorgen und dem jeweiligen Antrag beifügen zu müssen.
Begründung für die Auswahl dieser Nachweise	• Hohe Relevanz für OZG und SDG, weil (die Bestätigung von) Meldedaten häufig als Grundlage anderer OZG Verwaltungsleistungen benötigt wird. Insbesondere sind Melderegister Register mit OZG Relevanz gemäß Anlage IDNrG.Semantische Beschreibung der Nachweise liegt vor (DSMeld, XMeld). Die Vorgehensweise und Praxistauglichkeit der Abbildung auf ISA Core Vocabulary (Person, Location) kann überprüft werden. • Der Abruf von Meldedaten ist im XÖV-Standard XInneres / XMeld realisiert. Es liegen viele Erfahrungen aus der Praxis vor. Die Umsetzung in einem Once Only Rahmenwerk ermöglicht daher die Möglichkeit des Vergleichs beider Lösungen (insbesondere mit Blick auf Anforderungen gemäß Abschnitt 1.4). • Aufgrund der dezentralen Registerlandschaft im Meldewesen kann die Ermittlung des zuständigen Data Providers nicht allein aufgrund der Bezeichnung des gewünschten Nachweises erfolgen. Es müssen zusätzliche Angaben herangezogen werden (AGS der Gemeinde, in der die betroffene Person gemeldet ist). Ein geeignetes Verfahren dafür muss auch mit der EU-KOM vereinbart werden (Issue in WP 7). • Im Rahmen der Erprobung können prototypisch Erweiterungen der Anwendung DVDV 2 für diesen Zweck entworfen und geprüft werden. • Erkenntnisse der Erprobung werden relativ leicht auf Datenabrufe aus anderen Registern des Informationsverbunds der Innenverwaltung übertragbar sein. • Insbesondere ist die Übertragbarkeit von Erkenntnissen auf den automatisierten Datenabruf bei der Registermodernisierungsbehörde gemäß § 6 IdNrG zu erwarten.
Partner für Erprobung	KRZN Niederrhein als Entwickler und Betreiber de Meldeportal Behörden, an das die kommunalen Meldebehörden des Landes NRW angebunden sind

Quellen

- *Erprobung eines Once Only Rahmenwerks. Zur Vorbereitung eines technischen Systems für Once Only in Deutschland*; Frank Steimke, KoSIT, Fassung vom 08.10.2020 (gekürzt)

2.4. Methode: Vorgehen im Erprobungsprojekt

2.4.1. Entwicklung Durchstich (Proof of Concept)

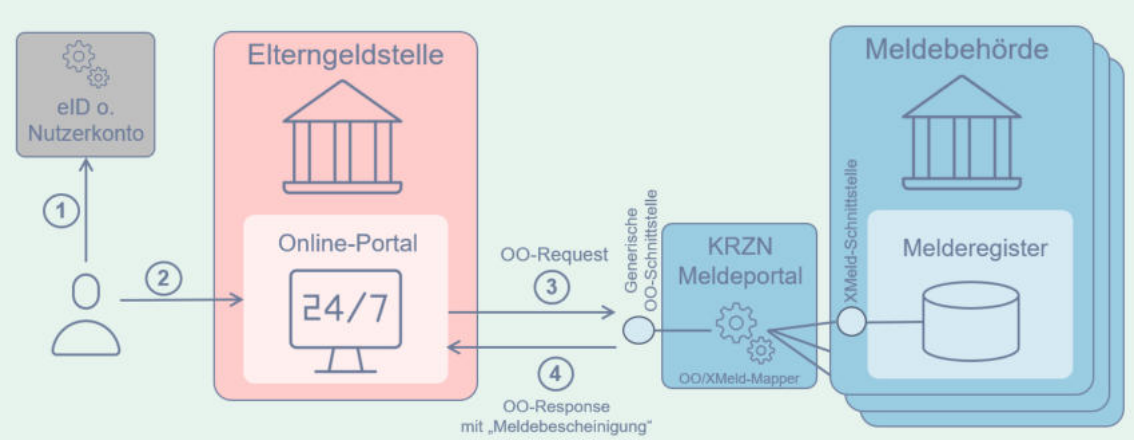
Der Arbeitsmodus für die Erprobung wurde so gewählt, dass Softwareentwicklung und konzeptionelle Ansätze parallel verfolgt werden und ineinandergreifen.

Für den Nachweisabruf war ein Durchstich als Proof of Concept zu entwickeln:

- Ein Testclient ruft - basierend auf definierten Identitäts- und Abrufkriterien - Nachweise vom NRW-Meldeportal ab (reales Testsystem aus Meldeportal-Softwarekomponenten und angebundenen Testregistern der kommunalen Meldebehörden in NRW).
- Schrittweise waren die zu erprobenden Komponenten und Technologien für den Abruf einzubauen, welche da sind OO-Standard für die Datenstrukturen aus Request- und Response-Nachrichten, E2E-Sicherheit, OSCI-Kommunikation und XTA-Entkopplung.

In Abbildung 2.2 werden Komponenten des Durchstichs auf das zu erprobende Fachszenario gemappt.

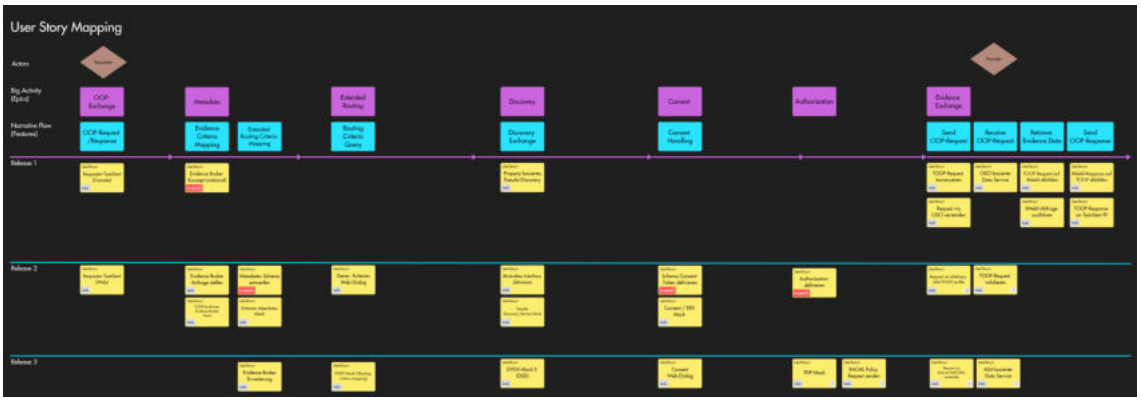
Abbildung 2.2. Fachliches Szenario



2.4.2. Iteratives Vorgehen

Ein Story Mapping regelte die Iterationen der Durchstich-Entwicklung.

Abbildung 2.3. Storymap des Pilotvorhabens



Werkstatt-Termine in April und Juni 2021 gaben die Möglichkeit zur Vernetzung

- im Steuerungsprojekt werden die Arbeiten aus Pilotprojekt 7 sichtbar gemacht
- Fragestellungen und Anforderungen aus anderen Bereichen des Steuerungsprojekts können an Pilotprojekt 7 herangetragen und durch dieses als Input aufgenommen werden

Abbildung 2.4. Agenda des zweiten „Blick in die Werkstatt“ Termins

IT-PLR Projekt Registermodernisierung

Erprobung Once-Only-Abruf mit dem NRW-Meldeportal

Der zweite Blick in die Werkstatt **30.06.2021 10:00 – 15:00 h**

Webkonferenz

1. **Überblick über die Lage aus Sicht BMI**
   a. Stand der Gesamtsteuerung und der Pilotierungsvorhaben
   b. Stand der Arbeiten zum SDG-VO Durchführungsrechtsakt
2. **Erprobung Architektur der OO-Abfrage – Stand der Arbeiten**
   a. Kommunikation einer Nachweis-Anfrage vom Antragsportal zum Meldeportal
   b. Kopfstelle Meldeportal: Validierung, XMeld-Transformation und Beantwortung der Anfrage
   c. Umsetzung der Once-Only-Nachrichten: Leistungen und Fallstricke
3. **Praktische Erkenntnisse und Zusammenhänge**
   a. Berührungspunkte mit dem beschlossenen RegMo-Zielbild
   b. Auswirkungen der Beschlusslage zur SDG-Umsetzung
   c. Blick auf die Once-Only-Umsetzung in Österreich
4. **Ausblick und Abschluss**
   a. Themen für den nächsten Werkstatt-Termin
   b. Blitzlicht

Kapitel 3. Umsetzung des Proof of Concept

Das fachliche Szenario, welches der PoC umsetzt, wird im Abschnitt Fachliches Szenario für die Erprobung beschrieben. Die PoC-Komponenten wurden folgendermaßen auf die Partner des Pilotprojekts 7 verteilt:

- **Evidence Requester** | Der Testclient für den Nachweisabruf simuliert den Online-Service einer Elterngeldstelle und war zu realisieren durch Dataport.
- **Evidence Provider** | Der Evidence-Provider war das Testsystem des (realen) Meldeportals des Landes NRW. Die Verbindung wurde vom KRZN realisiert durch Umsetzung eines OnceOnly Gateways zu diesem Meldeportal.
- **E2E-Verschlüsselung** | Zur durchgehend einheitlichen technologieunabhängigen E2E-Verschlüsselung wurde durch Dataport eine Kryptobibliothek umgesetzt.
- **RegRep4-Library** | Request-Response-Formate des Nachweisabrufs wurden in Form einer Bibliothek auf Basis der EU-Vorgaben (Standard OASIS RegRep4) ebenfalls von Dataport umgesetzt.
- **Once Only Standard** | Die inhaltlichen Formate für die Nachweisanforderung wurden durch die KoSIT entwickelt in Form des Versuchs der Spezifikation eines Once Only Standards (auf Basis der EU-Vorgaben in Bezug auf zu verwendende Datentypen aus den Core Vocabularies).

Komponenten und technische Rahmenbedingungen

- Es wurden für Entwicklung und Test jeweils die Firmen-PCs im Home Office eingesetzt.
- Für die Internet Verbindung wurde jeweils das private DSL verwendet.
- Gestellt wurden von Governikus Infrastrukturkomponenten: ein Intermediär für den Transport via OSCI / XTA-Server COM Despina für die XTA-Anbindung von Evidence Requester und Evidence Provider an die Transportinfrastruktur
- Der Evidence Provider wurde auf Basis des vom KRZN betriebenen Meldeportals des Landes NRW in einer Testumgebung mit Test-Datensätzen umgesetzt.
- Die von Governikus betriebene OSCI-Bibliothek wurde im Rahmen der Entwicklung verwendet.

Für die Datenkommunikation zwischen Evidence Requester und Evidence Provider wurden verschiedene Transport-Technologien erprobt:

- **HTTP POST:** Einfache direkte Kommunikation zwischen Evidence Requester und Evidence Provider
- **OSCI-Transport:** Kommunikation des Evidence Requesters mit dem Evidence Provider synchron per OSCI-Transport über einen OSCI-Intermediär
- **XTA-Webservice:** Anbindung des Evidence Requesters an einen Transport-Zugangspunkt/Anschluss A1, der die Kommunikation mit dem Evidence Provider (bzw. dessen Zugangspunkt/Anschluss A2 gemäß den Vorgaben des genutzten Transportprotokoll übernimmt (A1 und A2 kommunizieren synchron via OSCI-Transport, die angestrebte AS4-Datenübermittlung konnte nicht verprobt werden, da seitens EU-OOTS noch keine Festlegung des zu verwendenden AS4 profile vorlag und somit kein AS4-Netzwerk)

3.1. Leistungsumfang des PoC

Die wichtigsten Punkte der geplanten und zum großen Teil umgesetzten Merkmale des PoC

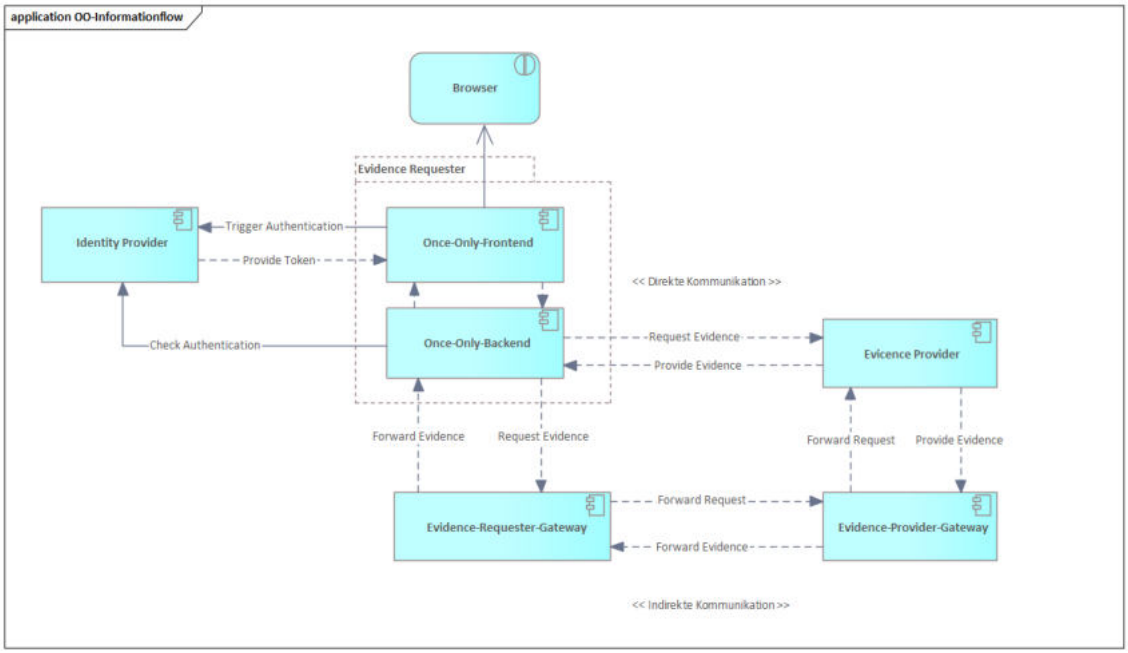
- Testclient arbeitet auf Basis der **eIDAS Identitätsparameter**
- Datenübermittlung unter Anwendung von **E2E-Verschlüsselung** per im Rahmen der PoC-Umsetzung entwickelten Kryptobibliothek

- Entkopplung von Corner 1 und Corner 2 per XTA-WS (Einbindung XTA-Server als Knoten C2)
- dynamisches **AGS-Routing** im Once Only Gateway des Meldeportals (= Adressierung der zuständigen Meldebehörde)
- (nur teilweise umgesetzt:) C3/C4-Entkopplung per XTA-WS: XTA-Anbindung des Once Only Gateways des Meldeportals als Knoten C4 (über COM Despina als Knoten C3)
- **Once Only Response** mit Evidence (in diesem Fall angeforderter Nachweis in Form einer XMeld-Nachrichteninstanz) als Attachment

3.2. Technische Architektur

Die Kommunikation der Komponenten und die verwendete Transporttechnik ist in Abbildung 3.1 dargestellt. Im Anschluss werden die einzelnen Technologien und Strukturen im Detail beschrieben.

Abbildung 3.1. Übersicht über Komponenten



Im Diagramm wird der Informationsfluss der Komponenten beschrieben: Einstiegspunkt in den Informationsfluss ist der *Browser* der Person, die den Nachweis anfordert. Über ein *Frontend* können die Parameter für die Anfrage des Nachweises eingesehen und angepasst werden. Die Authentifikation über den *Identity Provider* ist tokenbasiert. Im *Once-Only-Backend* werden die Personendaten aus diesem Token gezogen und können nicht im Frontend modifiziert werden.

Es wird sowohl die direkte Kommunikation als auch die indirekte Kommunikation dargestellt.

- Bei der direkten Kommunikation fordert der *Evidence Requester* direkt beim *Evidence Provider* den Nachweis an und erhält diesen entsprechend.
- Bei der indirekten Kommunikation wird der Request über das *Evidence-Requester-Gateway* weitergeleitet und der Evidence ebenfalls über das Gateway zurückgesendet.

3.2.1. Evidence Requester und Identity Provider

3.2.1.1. Technologie

Der Evidence Requester wird repräsentiert durch ein Angular Frontend (Version 12.1.1) und zwei Java-Backends (openjdk Version 11.0.13). Der Identity-Provider ist durch einen Keycloak (Version 12.0.4) realisiert.

Sowohl das Frontend, als auch die Backends haben eine Integration für den Identity-Provider und können ohne Authentifizierung nicht regelgerecht verwendet werden. Die Java-Backends verwenden das Framework Spring, welches 2021 laut jetbrains und stackoverflow eines der meistverwendeten und beliebtesten Java-Frameworks ist.

3.2.1.2. Architektur Testclient-Backend und Kommunikation

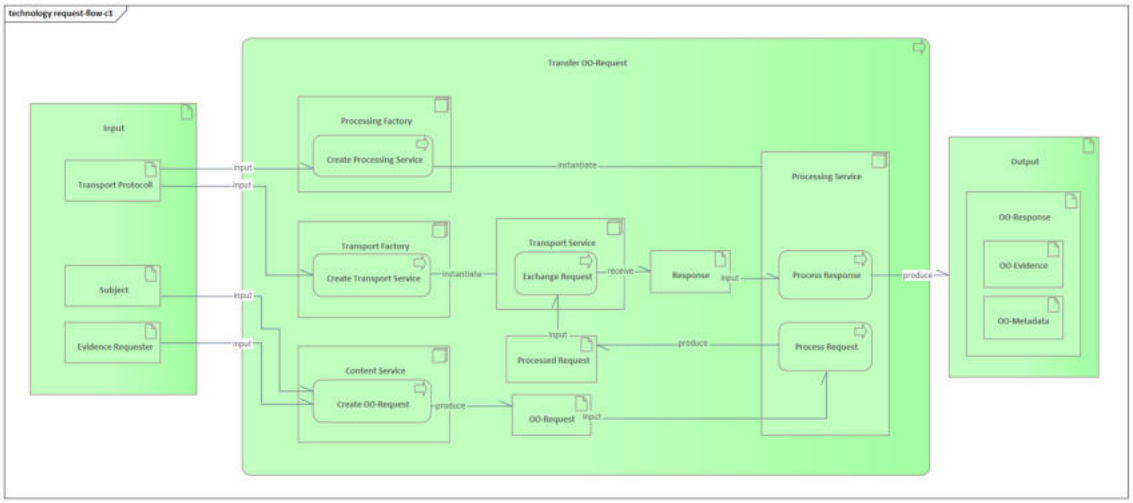
Ein wichtiges Paradigma bei der Umsetzung des Backends war *Transportagnostizität*. Der Transportweg soll vom Request entkoppelt werden und so leicht austauschbar sein. Hierfür wurde eine Factory angelegt, welche zum gegebenen Transportprotokoll den passenden Transport Service erstellt. Die Übergabe des Transportprotokolls kann vom Client gesteuert werden (in der Praxis liegt die Festlegung des Transportweges nicht beim User). Ferner wurde eine Bibliothek angelegt, welche aus den gegebenen Subject- und Evidence-Requester-Daten einen Once Only Request für den Anwendungsfall der Meldebescheinigung erzeugt.

Beim ersten Java-Backend liegt der Fokus darauf, eine erfolgreiche Kommunikation direkt über Http Post (https) mit dem Evidence Provider durchzuführen. Alternativ wurde für die Kommunikation OSCI-Transport eingesetzt.

Als nächster Schritt sollte die Kommunikation mit einer Ende zu Ende Verschlüsselung stattfinden (Anforderung aus IDNrG). Im diesem Zuge entstand ein zweites Backend mit einer überarbeiteten Architektur, welche es erleichtert, verschieden kryptographische Methoden bzw. Bibliotheken einzusetzen.

Die Erstellung des Requests, seine Vor- und Nachbearbeitung, sowie der Einsatz unterschiedlicher Transportformen ist im folgenden Diagramm beschrieben. Der Ablauf für das erste Backend ist im Anhang zu finden.

Abbildung 3.2. Erstellung und Übermittlung eines Request



Der Input besteht im Wesentlichen aus den Daten des Evidence Requesters, den Daten des Subjects, sowie dem gewünschten Transport Protokoll.

Die Daten des Subjects werden in der Praxis aus dem Token des Identity-Providers bezogen. Zur Vereinfachung wurde in dieser Darstellung auf diesen Schritt verzichtet. Zwar wählt im Allgemeinen der User nicht das Transport Protokoll aus, für die Erprobung war diese Herangehensweise jedoch sehr praktisch. Die dadurch entstandene Abstraktion kann auf die Praxis übertragen werden, um einem Backend unterschiedliche Transportformen zu ermöglichen. Für die Umsetzung des Transportservices für OSCI wurde die Bibliothek von

Governikus für OSCI 1.2 in der Version 2.1.0 unter https://www.governikus.de/osci-bibliothek/ verwendet. Für die Umsetzung des Transportservices für XTA wurde der XTA Beispielcode für XTA 2 Version 3 aus dem Bereich *Nicht-normative Hilfsmittel zu XTA 2 Version 3* unter https://www.xoev.de/downloads-2316#XTA verwendet.

Der Input wird an die REST Schnittstelle übergeben. Dort wird zunächst der pasende Service für den Transport, sowie der passende Service für die Verarbeitung der Nachricht bereitgestellt und der Once-Only-Request erstellt. Der Request wird dann mit dem Content Service verarbeitet, u.a. geschieht hier eine Verschlüsselung und eine Signatur. Der vorbereitete Request wird dann vom Transport Service synchron versendet und die Antwort passend vom Content Service entschlüsselt und verarbeitet. Der Output enthält den angefordertern Nachweis, welcher an den Client zurückgegeben wird. Der Transportweg der Nachricht wird in diesem Diagramm nur durch die *Exchange Request* Methode dargestellt. Eine detailliertere Darstellung kann am Ende des Abschnitts eingesehen werden.

3.2.2. Evidence Provider und Evidence Provider Gateway

3.2.2.1. Technologie

Der Evidence Provider wird im Erprobungsprojekt durch das Meldeportal für Behörden NRW repräsentiert.

Für die Anbindung an die Once-Only-Architektur wurde im Rahmen der Erprobung ein prototypisches Modul (*Meldeportal OnceOnly Gateway*, siehe unten) implementiert.

Dieses Modul basiert auf den folgenden Technologien:

- Java Web Application (Oracle JDK)
- Deployment auf Apache Tomcat
- Auszug externe Bibliotheken: SAXON (XML-Verarbeitung), Bouncy Castle (JCE), OSCI-Bibliothek, KoSIT-Validator, projektinterne Krypto-Bibliothek
- integrierte Unterstützung für Clusterbetrieb, Hot-Deployment und Hochverfügbarkeit

Das Gateway-Modul ist dem Meldeportal für Behörden NRW vorgeschaltet und kommunziert über SOAP/XML mit der offiziellen XML-API des Meldeportals. Die Erprobung wird ausschließlich auf Testsystemen und -umfeldern durchgeführt.

3.2.2.2. Architektur Meldeportal Once Only Gateway

Dieses für die Erprobung speziell implementierte Modul enthält verschiedene experimentelle Schnittstellen. Die unterschiedlichen Schnittstellen dienen der Erprobung der verschiedenen Transportformen HTTP-Post, OSCI-Transport (mit integrierter und mit manueller Verschlüsselung / Signatur) und XTA. Für die Umsetzung der OSCI-Transport-Schnittstelle wurde die Bibliothek von Governikus für OSCI 1.2 in der Version 2.1.0 unter https://www.governikus.de/osci-bibliothek/ verwendet.

Zur Realisierung des Moduls werden verschiedene Komponenten eingesetzt:

Der **KoSIT Validator** (https://github.com/itplr-kosit/validator) prüft und validiert eingehende Anfragen.

AGS-Router im Kontext der XMeld-Transformation. Das Erprobungsprojekt zielt darauf ab, die bereits bestehende Messaging Infrastruktur im Meldewesen weiter- bzw. mitzunutzen. Der TOOP-Request wird hierfür durch das Meldeportal Once Only Gateway in eine Nachricht (1320) aus dem Standard OSCI XMeld umgewandelt (es wurde die XMeld-Version 2.4.5 vom 31.01.2021 verwendet). Zur Adressierung einer Meldebehörde über XMeld ist ein amtlicher Gemeindeschlüssel erforderlich. Ein solcher AGS ist jedoch in der verwendeten Struktur für TOOP-Requests nicht enthalten und muss daher ermittelt werden, bevor die benötigte XMeld-Nachrichteninstanz erstellt werden kann.

- Im Erprobungsprojekt wurde dafür die prototypische Komponente „AGS-Router“ implementiert, die ausgehend aus den Informationen aus dem TOOP-Request den korrekten AGS der Ziel-Meldebehörde ermittelt.

Der Prototyp wertet für diese Zuordnung lediglich die Postleitzahl und den Ortsnamen aus und ermittelt damit anhand einer statischen Tabelle den AGS (Beispiel: Postleitzahl 47652, Ortsname Weeze => AGS 05154064).

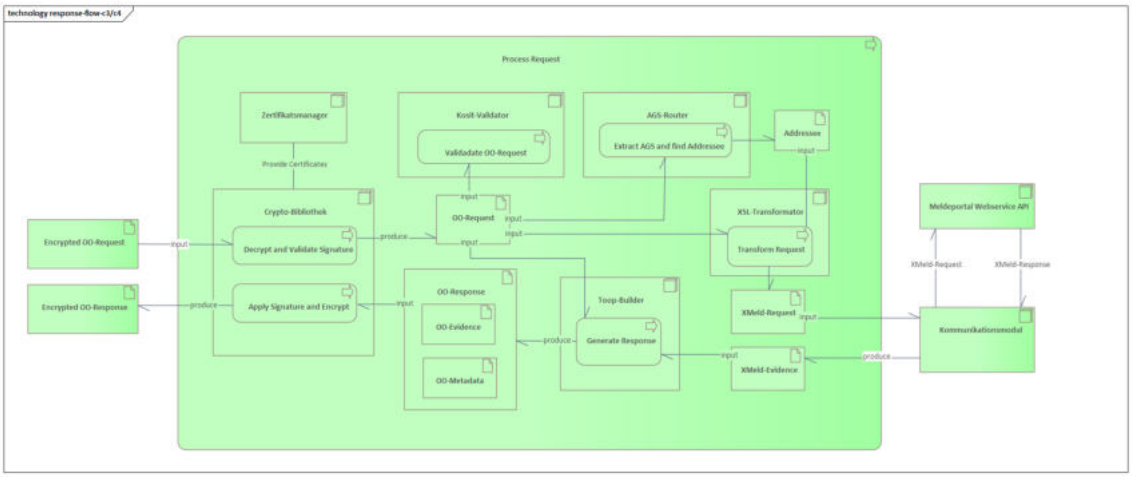
- In einem produktiven Szenario ist dieser Routing-Prozess erheblich komplexer - hier müssen zusätzlich Straßen, Hausnummern und ggf. Zusatzangaben berücksichtigt werden. In bestimmten Szenarien wäre es eventuell sogar erforderlich, historische Daten mit zu berücksichtigen (z.B. bei erfolgter Umbenennung von Straßen oder Neustrukturierung von Gebieten). Die Zuordnung obliegt daher einer gewissen Dynamik und müsste regelmäßig aktualisiert werden.

- Das AGS-Routing könnte sowohl als zentraler Service als auch als fester Bestandteil der Umwandlung eines TOOP-Request in eine XMeld-Nachricht realisiert werden.

Der **XSL-Transformator** überführt den Once-Only-Request in einen XMeld-Request. Dieser Request wird dann an die offizielle Schnittstelle (Webservice API) des Meldeportals für Behörden NRW weitergeleitet. Ein Kommunikationsmodul regelt die Kommunikation mit der Schnittstelle des Meldeportals. Dieses Modul beinhaltet die Authentifizierung gegenüber der Webservice API, sowie spezielle Sicherheitsuntermodule. Eine im Rahmen der Erprobung implementierte Krypto-Bibliothek ist für die Entschlüsselung des Once-Only-Requests und die Verschlüsselung des Once-Only-Response, sowie für die Signaturprüfung und Signaturerstellung verantwortlich. Dieselbe Biblilothek kommt auch im Once-Only -Backend des Evidence Requesters (s.o.) zum Einsatz.

Das folgende Diagramm beschreibt die Verarbeitung des Once-Only-Requests im Evidence Provider, sowie die Erstellung des Once-Only-Responce aus dem Request und dem Evidence des Meldeportals.

Abbildung 3.3. Verarbeitung von Request und Response im Meldeportal Behörden



3.2.2.3. Ende-zu-Ende Verschlüsselung und Rollenmodell

Betrachtet man dieses Modul als den *Evidence Provider*, so nimmt dieser die Position des Kommunikationsknotens C4 im 4-Corner Modell ein. Betrachtet man das Modul als *Provider Gateway*, so ist es der Kommunikationsknoten C3. In diesem Fall ist das Meldeportal als Ganzes der Evidence Provider.

Eine Ende-zu-Ende Verschlüsselung vom Evidence Requester bis zur kommunalen Meldebehörde ist bei dieser Betrachtung ohne eine Anpassung der Schnittstelle des Meldeportals nicht möglich, da das Meldeportal Behörden die Entschlüsselung vornehmen muss, um eine genaue Addressierung an das Meldeportal zu erreichen (Bestimmung der im XMeld-Standard zwingend erforderlichen Ziel-AGS durch die Routing-Komponente). Darüber hinaus bildet das Meldeportal Behörden den *Request* im EDM-Format auf einen XMeld 1320 Nachricht ab, und die XMeld 1321 Antwortnachricht auf einen *Response* im EDM Format.

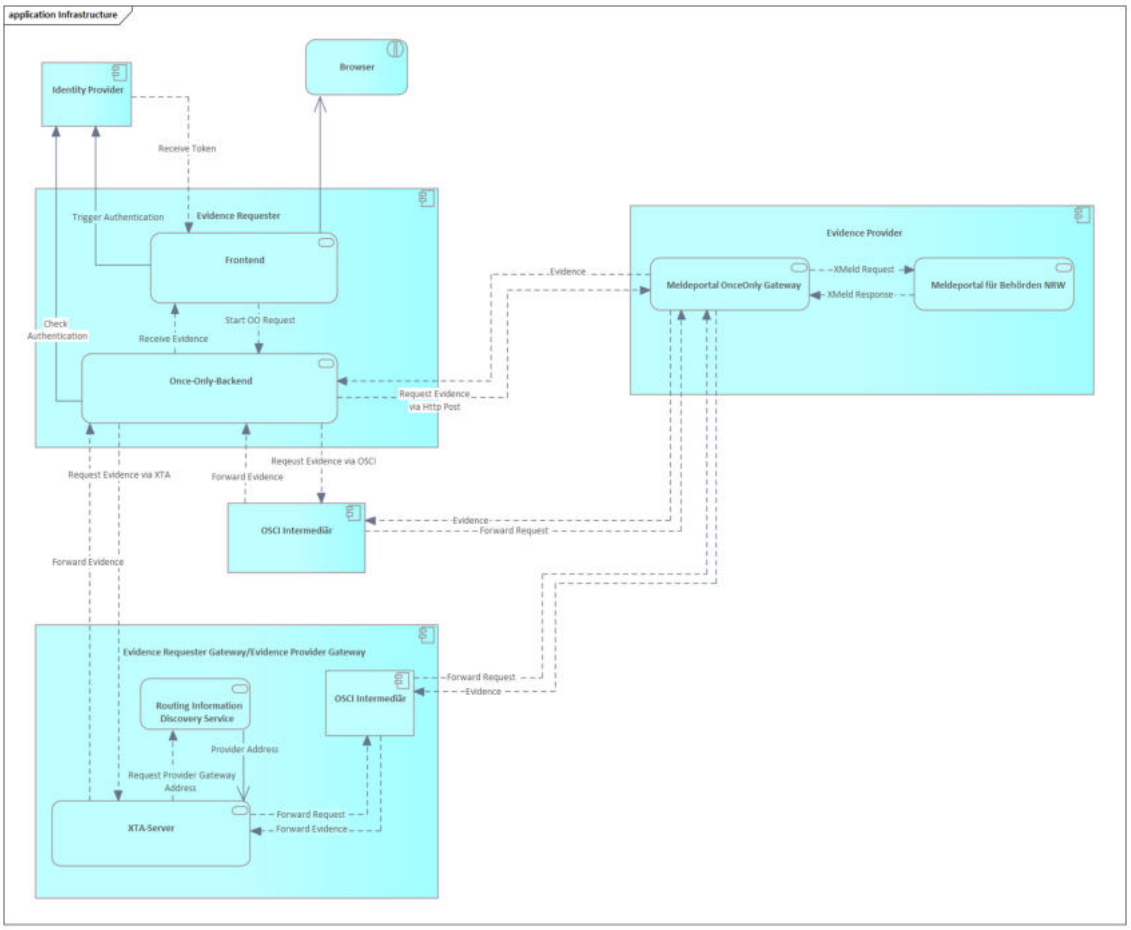
3.2.3. Gateways für Evidence Requester und Provider

Für die Kommunikation über OSCI-Transport wurde ein Governikus Test-Intermediär verwendet, welcher die Anfrage des Evidence Requester dem Meldeportal OnceOnly Gateway zustellt.

Der XTA-Server wurde durch das Governikus-Produkt COM Despina realisiert.

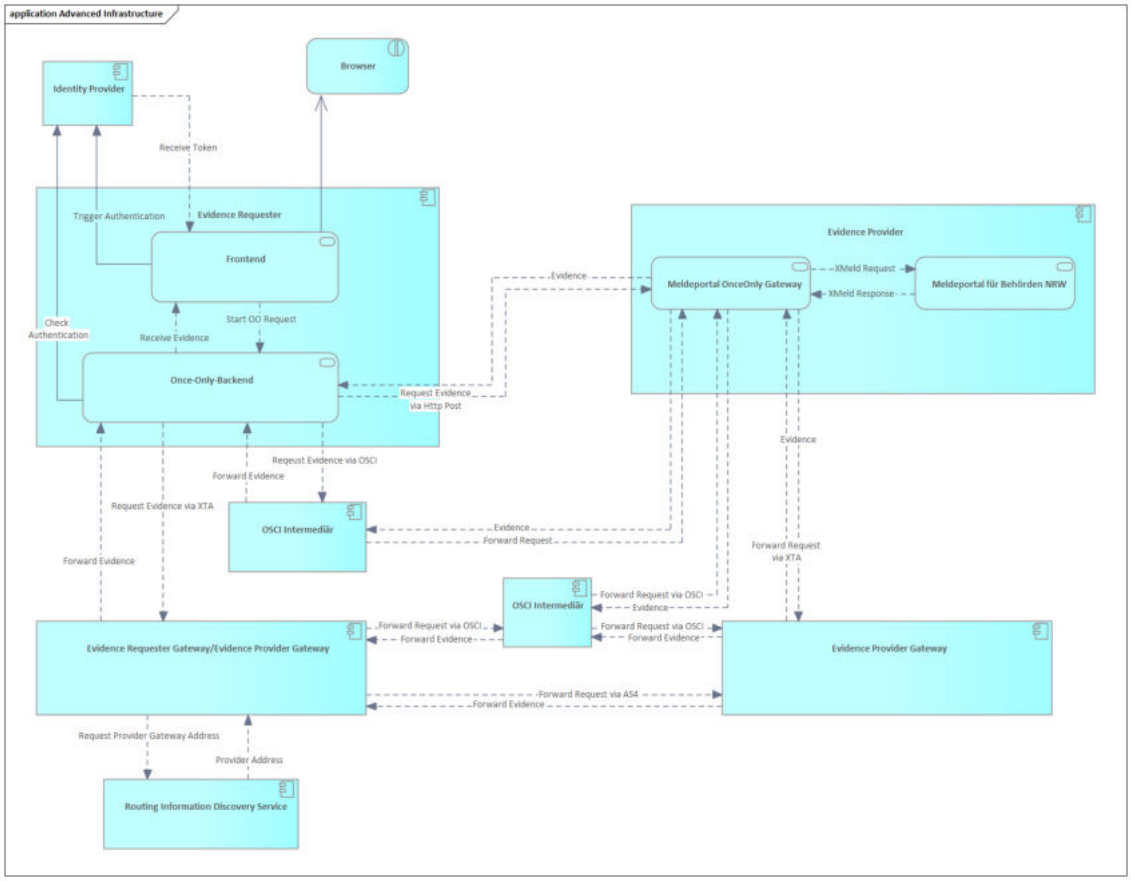
Das folgende Diagramm beschreibt den vollständigen Informationsfluss.

Abbildung 3.4. Vollständiger Informationsfluss



In diesem Diagramm wird das Evidence-Requester-Gateway nicht spezifisch dargestellt. Im HTTP-Post-Szenario erfolgt die Kommunikation direkt und es gibt diese Rolle nicht. Andernfalls übernehmen in diesem Diagramm das XTA-Backend oder der OSCI Intermediär diese Rolle. Einen einzelnen Evidence-Provider gibt es in dieser Umsetzung nicht. Dafür war eine weiterer XTA-Infrastruktur geplant. Die vollständige Architektur beschreibt das folgende Diagramm.

Abbildung 3.5. Vollständige Architektur



3.3. Fehlermanagement

3.3.1. Fehlermanagement in OASIS RegRep V.4

OASIS RegRep V.4 (genauer: die RegRep-Service-Spezifikation ebRS) definiert einen generischen Mechanismus, wie ein RegRep-Service Fehlersituationen kommuniziert:

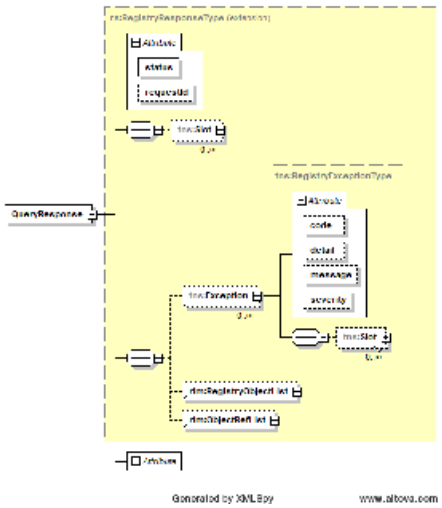
Im XML-Schema zu ebRS ist ein komplexer Typ sowie ein entsprechendes Element „RegistryException“ zur Beschreibung allgemeiner Fehlersituationen definiert. Das Element enthält

- die zwei verpflichtenden XML-Attribute `message` und `severity`
- sowie die zwei optionalen Attribute `code` und `detail`.

Innerhalb des RegRep-Response-Nachricht (hier speziell: QueryResponse) kann ein RegistryException-Element enthalten sein: Bei Warnungen ergänzend zum eigentlichen Payload (RegistryObjectList), bei echten Fehlern ohne weiteren Payload.

Es gibt keine Vorgaben oder Standardwerte für das code-Attribut, welches ohnehin optional ist. Da der Exception-Typ vom generischen Typ „RegistryExceptionType“ abgeleitet ist, könnten theoretisch optional beliebige Slots sämtlicher Datentypen in die Exception eingefügt werden, um komplexe, ergänzende Fehlerinformationen zu transportieren.

Abbildung 3.6. Exceptions im RegistryResponseType



3.3.2. Klassifizierung von Exceptions

Als Mechanismus zur Klassifizierung von Fehlersituationen sieht RegRep vor, Ableitungen (Extensions) des allgemeinen RegistryExceptionTyps vorzunehmen. RegRep definiert selbst innerhalb der verschiedenen RegRep-Schemata (RIM, RS, Query, Lifecycle) 13 kanonische Subtypen. Keiner dieser vordefinierten Subtypen ergänzt die Basis-Exception um Datenelemente, d.h. dass lediglich die Typspezifikation selbst als Klassifizierung dient, ohne spezifischere Fehlermetadaten strukturiert zu definieren.

Applikationen sind frei, eigene Subtypen zu definieren - diese ggf. dann auch mit strukturellen Erweiterungen.

Da die RegRep-Schemata lediglich die Typen und keine Elemente zu den Subexceptions definieren, muss der Subtype in der XML-Instanz mittels xsi:type spezifiziert werden. Die 13 kanonischen Exception-Subtypen sind in Table 3.1 dargestellt.

Table 3.1. Definierte Exceptions

XSD Element Name	Description
AuthenticationException	Generated by server when a client sends a request with authentication credentials and the authentication fails for any reason.
AuthorizationException	Generated by server when a client sends a request to the server for which it is not authorized.
CatalogingException	Generated by server when a problem is encountered during the processing of a CatalogObjectsRequest.
InvalidRequestException	Generated by server when a client sends a request that is syntactically or semantically invalid.
ObjectExistsException	Generated by the server when a SubmitObjectsRequest attempts to create an object with the same id as an existing object and the mode is “CreateOnly”.
ObjectNotFoundException	Generated by the server when a QueryRequest expects an object but it is not found in server.
QueryException	Generated by server when when a problem is encountered during the processing of a QueryRequest.
QuotaExceededException	Generated by server when a a request exceeds a server specific quota for the client.
ReferencesExistException	Generated by server when a RemoveObjectRequest attempts to remove a RegistryObject while references to it still exist.

XSD Element Name	Description
TimeoutException	Generated by server when a the processing of a request exceeds a server specific timeout period.
UnresolvedReferenceException	Generated by the server when a request references an object that cannot be resolved within the request or to an existing object in the server.
UnsupportedCapabilityException	Generated by server when when a request attempts to use an optional feature or capability that the server does not support.
ValidationException	Generated by server when a problem is encountered during the processing of a ValidateObjectsRequest.

3.3.3. Fehlerebenen im Kontext der Once Only Schnittstelle

Die von RegRep V.4 definierten Fehlerklassen haben den sehr generellen fachlichen Kontext der OASIS-Spezifikation (Lifecycle-Operationen auf Registries und Repositories) zum Hintergrund. Bezogen auf den speziellen Kontext einer OO-Nachweisabfrage sind die Fehlerklassen nur eingeschränkt anwendbar oder sind teilweise von der Spezifikation abweichend zu interpretieren.

Im Zuge der Durchstichimplementierung zum Proof-of-Concept sind unterschiedliche Ebenen von Fehlern identifiziert worden, die zum Teil auf eigene Exception-Subtypen abgebildet werden sollten. Die Technical Design Documents (TDD) der EU-SDG-Umsetzung machen aktuell dazu keine Vorgaben, sondern verweisen auf die allgemeinen Fehler von RegRe V.4 (s.o.). Folgende Fehlerebenen im OO-Kontext und mögliche Repräsentationen wurden erkannt:

1. **Transportschicht** Auf Fehler der Transportebene (vornehmlich Corner 2/3), die entweder die Technologie OSCI oder eDelivery/AS4 betreffen, kann auch nur konform zum jeweiligen Transportstandard reagiert werden. Eine Abbildung auf RegRep-Nachrichtenebene ist nicht möglich.

2. **Authentifizierung und Autorisierung** Unabhängig von der konkreten Form der Umsetzung zur Authentifizierung und Autorisierung sieht RegRep dedizierte Exception-Subtypen für diese Fehlersituationen vor, die auch im OO-Kontext sinnvoll nutzbar sind.

3. **Validierung** Die Validierung von Request und Response kann auf unterschiedlichen Ebenen fehlschlagen:

   a. Die generische RegRep-Nachricht selbst ist nicht schemakonform.

   b. Die OO-Profilierung der RegRep-Slots (generischer Property-Mechanismus) ist verletzt (fehlende verpflichtende Slots).

   c. Die Slot-Werte gemäß Profilierung sind nicht schemakonform. In einer etwas freieren Auslegung kann für alle Validierungsebenen die RegRep Fehlerklasse ValidationException dafür verwendet werden.

4. **Routing** Für OO-Requests, für die auf Basis der Adressierungsdaten zum Evidence-Provider (z.B. der AGS) kein zugehöriges Register ermittelt werden kann, wäre eine eigene Fehlerklasse mit ergänzenden Fehlerdaten sinnvoll.

5. **Interne Fehler** Allgemeine interne Fehler können auf allen Ebenen auftreten. Es ist sicherheitstechnisch zu bewerten, ob eine Rückmeldung mindestens der auslösenden Fehlerebene erfolgen kann.

In der PoC-Implementierung ist die identifizierte Ebenenklassifizierung nicht umgesetzt worden. Stattdessen sind Fehler der Ebenen 2 bis 5 lediglich in Form von Fehlertexten (message-Attribut innerhalb des QueryException-Subtyps) ausgedrückt worden. Ein späteres Fehlermanagement-Konzept sollte auch die Fortentwicklung Technical Design Documents (TDD) einbeziehen.

Des Weiteren sollte ein späteres Konzept die generelle Typisierung von Fehlern vorsehen, die ausdrückt, ob die Fehlersituation ursächlich durch ein Fehlverhalten des Requesters (Client) ausgelöst ist oder im Rahmen der Verarbeitung auf Seiten des Providers (Server) verortet ist. Ebenfalls wäre es sinnvoll, auszudrücken, ob eine

ggf. kurzzeitige Störung oder ein systematischer Fehler vorliegt. Dies könnte den Requester Informationen zur Reaktion auf den Fehler an die Hand geben.

3.4. Ergebnisse der PoC-Umsetzung

Es wurde ein PoC erstellt, um die Merkmale der technischen Umsetzung des Nachweisabrufs zu erproben.

Der Fokus der Durchstich-Implementierung liegt auf Strukturmerkmalen der Umsetzung einer vom RegMoG geforderten Infrastruktur sowie auf den für die SDG-Umsetzung vorgegebenen Formaten für den Nachweisabruf:

- Anforderungen des RegMoG an die Infrastruktur: Datenübermittlung in einer 4-Corner-Infrastruktur unter Anwendung von E2E-Verschlüsselung
- Vorgaben der EU für den SDG-Nachweisabruf: Generische Once Only Datenformate für die Request/Response-Struktur des Abrufs.

3.4.1. 4-Corner-Infrastruktur

Es wurde die E2E-Verschlüsselung auf der Basis einer für diesen Zweck entwickelten Kryptobibliothek durchgeführt und gezeigt, wie die Nachweisanfrage vor Übergabe an die Infrastruktur verschlüsselt werden kann (Verschlüsselung durch C1 für C4). Es wurden dafür kryptografische Mechanismen eingesetzt, die an der Strecke C1/C2 einsetzbar sind, ohne dass die Technologie der Datenübermittlung zwischen C2 und C3 an der Stelle bekannt sein muss (Transportagnostik).

Es wurde die Entkopplung der zwischen den Access Points eingesetzten Messaging Technologie von der Art der Anbindung von Evidence Requester und Evidence Provider an die Access Points demonstriert. Die C1/C2-Entkopplung wurde unter Verwendung der XTA-Webservice-Schnittstelle in der Version 2.1.1 umgesetzt (Einbindung des XTA-Servers COM Despina als Knoten C2). Dies ist dieselbe XTA-Version, die für den Informationsverbund der Meldebehörden seit einigen Jahren länderübergreifend im Einsatz ist. Entsprechend wurde die C3/C4-Entkopplung vorbereitet (unter Verwendung des XTA-Servers an der Position C3. Für die Kommunikation von C2 an C3 stehen dann alternativ die Webservice-Formate OSCI-Transport und AS4 zur Verfügung, ohne dass dies in der Anbindung von C1 an C2 (bzw. von C4 an C3) bekannt sein muss. Im PoC wird OSCI-Transport eingesetzt.

3.4.2. Leistungen und Grenzen der Umsetzung im PoC

Die technische Machbarkeit der XTA-Entkopplung wurde gezeigt. Sie wurde exemplarisch im Rahmen der C1/C2-Entkopplung implementiert. Für die C3/C4-Entkopplung wurde sie im KRZN-Meldeportal softwaretechnisch entsprechend kodiert. Wegen Begrenzungen der zur Verfügung stehenden Testinfrastruktur konnte die vollständige Strecke der XTA-Entkopplung zur Projektlaufzeit nicht mehr getestet werden bzw. deren Lauffähigkeit nicht dauerhaft reproduziert werden.

3.4.2.1. Begrenzungen der Testinfrastruktur

Es wurde eine Testumgebung benötigt, die für die C1-C2-Kommunikation einen XTA-Service bereitstellt, dann an eine OSCI-Infrastruktur die Requests als synchrone OSCI-Nachricht übergibt und die Responses von C3 bzw. C4 zurückgibt.

Innerhalb der Dataport-Infrastruktur konnte ein derartiger Service (mit voller Flexibilität in den zu variierenden Konfigurationen) nicht bereitgestellt werden. Daher wurde auf eine seitens Governikus bereitgestellte Testinstanz gesetzt. Der Aufruf dieser Testinstanz aus der Dataport-Infrastruktur (Test-Client-System) gestaltete sich mit Aufschalten der XTA-Funktionalität schwieriger als erwartet. Eine stabile Verbindung konnte nur ohne Verwendung eines Proxy realisiert werden. Anders ließ sich die Testinstanz des zur Verfügung gestellten Governikus COM Despina XTA-Service nicht ansprechen, um die abgesicherte Webservice-Schnittstelle zu konnektieren.

In der regulären Dataport-Infrastruktur sind jedoch entsprechende Proxies fest eingebaut. Daher wurde bei den Testdurchläufen per privatem Internet-Zugang (DSL) der Entwickler gearbeitet und mussten häufig wechselnde IP-Adressen der Client-Rechner in Kauf genommen werden.

Diese Begrenzung der Testinfrastruktur machte sich erst negativ bemerkbar, als der XTA-Server COM Despina in die Datenkommunikation eingebaut wurde. Diese Testinstanz reagiert nur auf externe Requests von fest konfigurierten IP-Adressen als festes Merkmal der bereitgestellten Governikus-Testinfrastruktur, die für reguläre XTA-Tests innerhalb eines Netzwerkes konzipiert ist. Dies - zusammen mit der Konfiguration von Firewall und weiteren Parametern der Testinfrastruktur - führten zum Ergebnis, dass keine auf Dauer lauffähige Testkonfiguration im Zusammenspiel Test-Client (Dataport) mit Testinfrastruktur (Governikus) realisierbar war.

Zwischenzeitlich (Nov/Dez 2021) konnte trotz dieser Schwierigkeiten die C1/C2-Entkopplung via COM Despina erfolgreich getestet werden. In Jan/Feb 2022 konnte auch diese C1/C2-Entkopplung wg. der genannten Konfigurationsprobleme nicht mehr reproduziert werden. Aus denselben Gründen konnte in Jan/Feb 2022 die durch KRZN (schon im Nov 2021 in Java) umgesetzte C3/C4-Entkopplung nicht getestet werden.

Sind Fehler gemacht worden? Zu lange entstand für die Leitung des AP 3.1 der Eindruck, dass die Probleme in der Entwicklung auf Defizite in der Koordination zurückzuführen sind. Erst in Feb 2022 wurde sichtbar, dass die Wurzel des Problems in bestimmten nicht änderbaren Rahmenbedingungen der verwendeten Testinfrastruktur bestand.

Auf einem anderen Blatt stehen die praktischen Erkenntnisse im Rahmen der Umsetzung der XTA-Schnittstellen und der XTA-Kommunikation mit COM-Despina. Sie sind valide und werden im Abschnitt 4.8 dokumentiert. Es wird eine Unterstützung für Entwickler von XTA-Schnittstellen benötigt, die ähnlich aufgestellt ist wie die in der Messaging Infrastruktur des IT-Planungsrat bewährte OSCI-1.2-Bibliothek. Die KoSIT bietet bisher Beispielcode für einen XTA-Client an, was hilfreich, aber allein nicht ausreichend ist. Weitere Erkenntnisse betreffen das Thema XTA-Konformität. Hier ist im Dienste der Umsetzung einer E2E-Verschlüsselung nachzubessern.

Kapitel 4. Erkenntnisse zu Architektur und Komponenten

4.1. Fachliche Bewertung des Szenarios

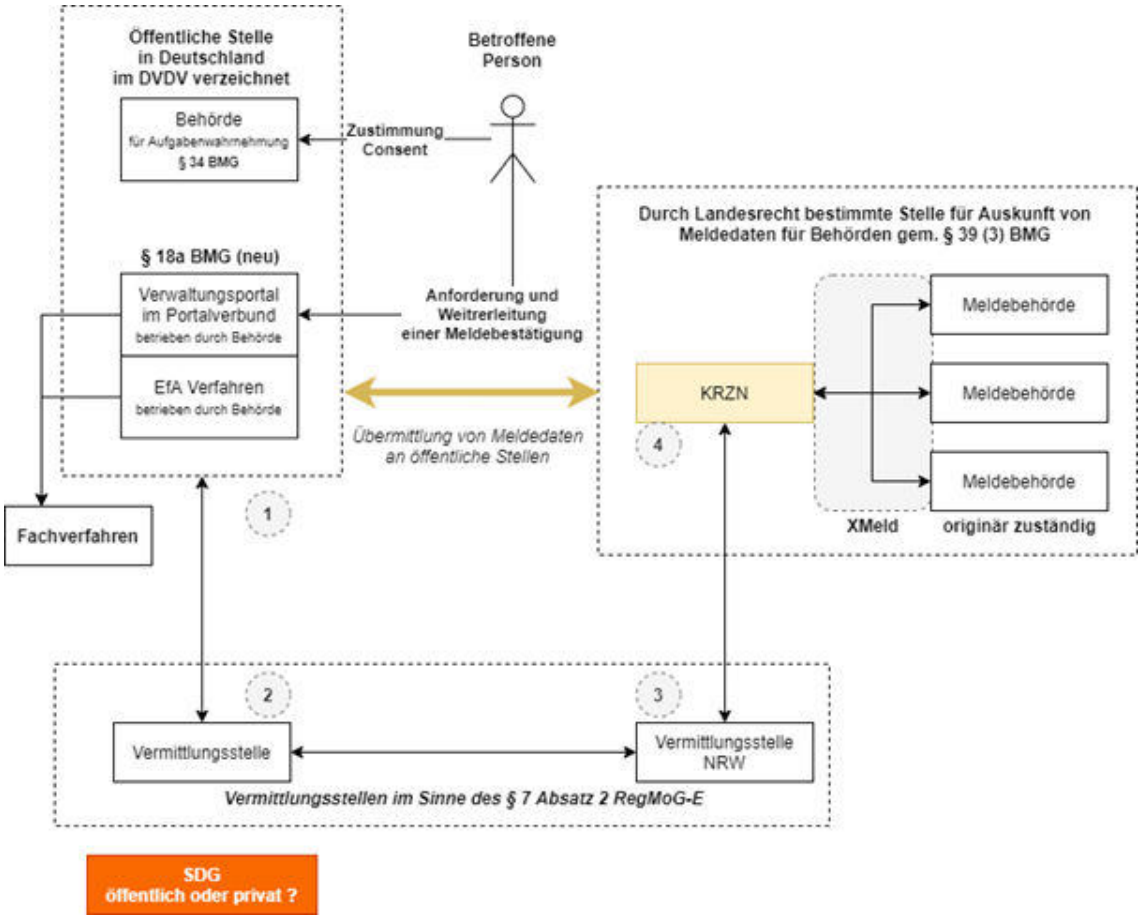
Der für das Erprobungsprojekt ausgewählte Anwendungsfall ist in Abbildung 4.1 beschrieben.

Im Rahmen seiner Umsetzung wird die technische Architektur des Nachweisabrufs erprobt. Andererseits ist der Anwendungsfall mit seinen Rechtsgrundlagen auch Gegenstand der rechtlich-fachlichen Diskussion. Wie ist der Nachweisabruf im Falle des Nachweistyps Meldebescheinigung rechtlich zu unterlegen?

Sollte er durch eine Generalklausel definiert und legitimiert werden, die sich auf alle für umgesetzte OZG-Leistungen benötigten Nachweisabrufe bezieht?

Wenn eine solche Generalklausel nicht in Aussicht ist, wäre der Nachweisabruf Meldebescheinigung auf Basis des Fachrechts des Einwohnerwesens zu deuten? Diese Analyse wird in der Abbildung visualisiert und auf dieser Seite durchgeführt.

Abbildung 4.1. Fachlichkeit im PoC



Besondere Eigenschaften des Anwendungsfalls

Das Pilotprojekt 7 bezieht sich auf genau einen der 21 geforderten SDG-Nachweistypen (siehe SDG-VO Anhang II)

- Der Fall ist relativ einfach, was die Auffindbarkeit des zuständigen Evidence Providers betrifft. Das liegt daran, dass der Nutzer die Lokalisierung des für die abzurufende Nachweisinstanz zuständigen Registers unterstützen kann. Ich weiß, wo ich wohne und also, welche Kommune für die Ausstellung meiner Meldebescheinigung zuständig ist.

- Außerdem hat der Anwendungsfall die Eigenschaft, dass Nutzer und betroffene Person des Nachweises (evidence subject) identisch sind („ich rufe eine Meldebescheinigung für mich ab“).

Die genannten beiden Eigenschaften sind zu berücksichtigen bei der Auswertung der Erkenntnisse.

Rechtliche Deutung des Anwendungsfalls: Behördenabruf vs. User-Abruf

Der benötigte Nachweis gemäß SDG Verordnung ist die „*Bestätigung der Meldung an der aktuellen Adresse*“. Diese wird der betroffenen Person zur Verfügung gestellt, also einer privaten Stelle. Dazu bedient sich die betroffene Person des Technischen Systems SDG-OOTS. Und hat gegenüber der anfragenden „competent authority“ erklärt, exakt zu diesem Zwecke das technisch System nutzen zu wollen. Gewissermaßen autorisiert die betroffene Person einen elektronischen Abruf, bleibt allerdings als Initiator immer in der Rolle desjenigen Akteurs, der nach Bereitstellung der Nachweise die weitere Verwendung auf Seiten der abfragenden Stelle frei gibt oder eben auch ablehnt. Da das KRZN derzeit nur Behörden als Kunden hat, muss festgelegt werden, wer mit wem auf welcher Rechtsgrundlage Daten austauschen darf, und wie der Ablauf sein kann. Eine Meldebestätigung wird für die betroffene Person nur einmal, unmittelbar nach der Anmeldung ausgestellt. Dem Nachweis Dritten gegenüber dient die Meldebescheinigung, die mehrfach ausgestellt werden kann (§ 18). Für den Abruf einer Meldebescheinigung als OZG Leistung liegt der Entwurf der XMeld-Nachrichten 1700, 1701 vor (final in XMeld Version 3.0 vom 31.07.2021). Eine Meldebestätigung wird ausgestellt *für die betroffene Person*.

Das KRZN-Meldeportal bietet aber keine Abrufmöglichkeiten für private Stellen an, sondern ausschließlich für Behörden. Daher müssen der Ablauf und der Erprobungsgegenstand geklärt werden:

A. Entweder handelt es sich um eine **Auskunft an öffentliche Stellen** gemäß 34 BMG (vgl. die obenstehende Abbildung) mit einem Datenumfang entsprechend einer Meldebescheinigung.

   - Die betroffene Person stimmt zu, dass die für die Verwaltungsleistung zuständige Behörde die Meldedaten abrufen darf. Ein entsprechender *Consent* muss vorliegen.

   - Die Behörde ruft gemäß § 34 BMG Daten ab und nutzt dafür den generischen Standard für Nachweisabrufe. Die Meldebehörde erteilt eine Auskunft in Form eines im *Once Only* Rahmenwerk definierten Nachweises an eine Behörde.

   - Es handelt sich um den klassischen Fall des Abrufs von Meldedaten durch eine Behörde, die diese Daten für die Wahrnehmung ihrer Aufgabe benötigt (das ist die Bearbeitung des eigentlichen Antrags, für den u. a. eine Meldebestätigung erforderlich ist).

B. Oder der während der Projektlaufzeit neu geschaffenen § 18a BMG wird einschlägig: (vgl. Abbildung 4.1): „Die Meldebehörde stellt **der betroffenen Person** auf deren Antrag die Meldedaten … zum Zweck der Weiterleitung in einer elektronischen Verwaltungsleistung gem. OZG im Wege des automatisierten Abrufs bereit. Hierzu hat die meldepflichtige Person die in § 18 Absatz 1 Satz 2 genannten Daten zu übermitteln. Die Meldedaten werden als unveränderbarer maschinenlesbarer Datensatz (Meldedatensatz) bereitgestellt. Aus dem Meldedatensatz muss der Zeitpunkt des Abrufs erkennbar sein.“

   - Die betroffene Person nimmt einen Dienst in Anspruch, der auf einem öffentlich-rechtlichen Verwaltungsportal betrieben wird, oder der als EfA Dienst von einer Behörde angeboten wird. Der Dienst erlaubt ihr die Anforderung einer Meldebescheinigung zwecks Weiterleitung an eine Behörde gemäß § 18a BMG-E.

   - Die öffentliche rechtliche Stelle, die das Verwaltungsportal oder den EfA Dienst betreibt, ruft Daten bei der Meldebehörde ab. Hierfür nutzt sie den neuen Once Only Standard.

- Die Meldebehörde übermittelt einen unveränderlichen Meldedatensatz in Form eines im *Once Only* Rahmenwerk definierten Nachweises an diese öffentlich-rechtliche Stelle.

- Der Dienst erlaubt der betroffenen Person, den Nachweis zusammen mit dem im Dienst erstelten Antrag an die für die OZG Verwaltungsleistung zuständige Behörde weiterzuleiten.

Zusammenfassung und Schlussfolgerung

- Entweder ruft eine Behörde Daten gemäß § 34 BMG ab, weil sie diese für die Wahrnehmung ihrer Aufgabe (nämlich die Bearbeitung der beantragten OZG Leistung) benötigt, und ihr eine Einwilligung der betroffenen Person vorliegt;

- Oder die betroffene Person nimmt einen Dienst eines Verwaltungsportals oder einen EfA Dienst in Anspruch, in dessen Rahmen unter anderem eine elektronische Meldebescheinigung für die Zwecke der Weiterleitung an ein (in diesem Bild nur angedeutetes) Fachverfahren erstellt wird.

Conclusio: In beiden Fälle ist die abrufende Stelle eine öffentliche Stelle im Inland, die im DVDV verzeichnet ist.

Als Quelle verwendet: Artikel Frank Steimke, *Erprobung Oncy Only Methoden und Standards durch KRZN*, vom 08.02.2021 (überarbeitet)

4.2. Transport Mechanismen

Auf dieser Seite wird die Diskussion zur Transport Technologie geführt, die im Architekturmodell eingeführt wurden. Die Diskussion dreht sich um die Anforderung, den Nachrichtenaustausch zur Once-Only-Abfrage vom verwendeten Transportprotokoll zu abstrahieren.

4.2.1. Message Exchange Protocol

Gegenstand ist die folgende Empfehlung aus dem Architekturmodell: „ Als Protokoll für die Remote-Datenkommunikation sind die auf Webservice-Technologie basierenden Standards OSCI-Transport bzw. OASIS AS4 vorzusehen.“ In einer 4-Corner-Infrastruktur, wie in der Abbildung unten dargestellt, betrifft diese Empfehlung die Interaktion von Access Point zu Access Point (= Interaktion der Knoten C2 und C3).

In welchem Kontext ist OSCI-Transport, in welchem OASIS AS4 einzusetzen?

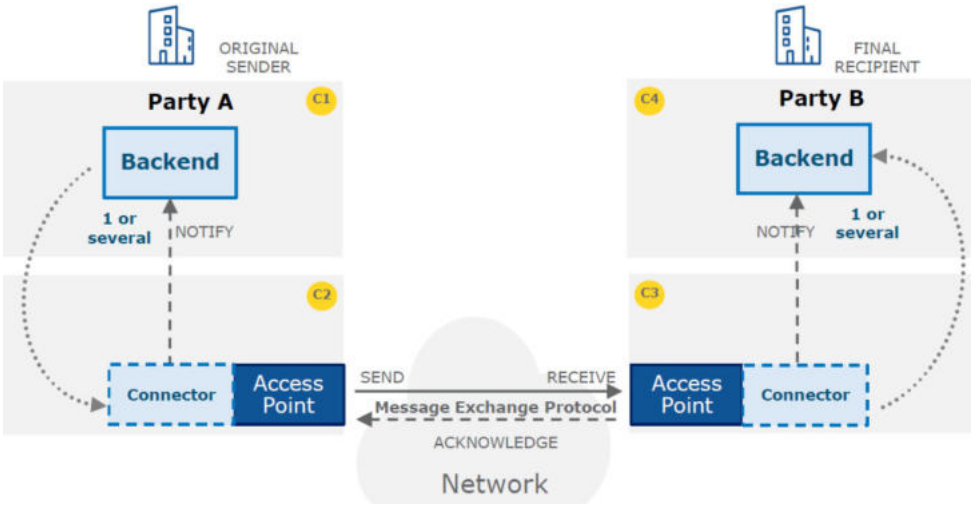
- OSCI-Transport ist die Empfehlung für den nationalen Nachweisabruf (DE von DE). OSCI ist der Standard der Wahl für die länder- bzw. bereichsübergreifende Nachrichtenkommunikation innerhalb Deutschlands. Dafür ist eine Infrastruktur etabliert und in Betrieb, auf die aufgesetzt werden kann. Das passt zum Zielbild der RegMo-Umsetzung in DE, welches vorgibt, dass vorhandene Infrastruktur weiterzuentwickeln ist, nicht auf der grünen Wiese eine neue Infrastruktur definiert und umgesetzt werden soll. Zu beachten ist hierbei das im jeweiligen Fachszenario präzise festgelegte Transportprofil für die OSCI-Kommunikation, so dass Struktur und Syntax der Transportnachricht einheitlich umgesetzt und interpretiert bzw. entschlüsselt werden kann. Im Kontext des Meldewesen wird auf XInneres referenziert, das für die OSCI-Kommunikation relevante Parametrisierungen des OSCI-Protokolls vornimmt.

  Zudem unterstützt OSCI die Ende-zu-Ende Sicherheit gemäß § 7 (2) IdNrG.

- OASIS AS4 ist vorgegeben für den internationalen Nachweisabruf im Rahmen der SDG-Umsetzung: Im OOTS der EU für die SDG-Umsetzung (vgl. Technical Design Documents) ist als Protokoll für die Nachrichtenkommunikation zwischen den Knoten C2 und C3 der Standard AS4 gesetzt. Allerdings gilt es, auch bei Verwendung von AS4 das jeweils genutzte Profil festzulegen, so dass die Konfiguration und Parametrisierung einheitlich für die beteiligten Systemkomponenten und Akteure umgesetzt wird. Das im Kontext der SDG-Umsetzung angestrebte Profil soll eDelivery AS4 profile sein, welches im Rahmen der CEF Building Blocks für den interoperablen grenzüberschreitenden Nachrichtentransport erarbeitet und spezifiziert wurde. Inwieweit eine Harmonisierung mit dem im OpenPeppol-Netzwerk präzisierten Peppol AS4 profile umgesetzt wird, muss beobachtet werden. Prinzipiell sollten alle zur Abbildung von OASIS AS4 Spezifikation realisierten

Access Points der Corner 2 und 3 auch weiter konkretisierende Profilierungen des Basisprotokolls umsetzen können

Abbildung 4.2. 4-Corner Modell in AS4



4.2.2. Entkopplung vom Messaging Protocol

Ausgehend vom Architekturmodell der Registermodernisierung sollen die deutschen Online Services (ER) und die deutschen registerführenden Verfahren (Evidence Provider) möglichst neutral und einheitlich in die Messaging Infrastruktur eingebunden werden.

Die Art ihrer technischen Anbindung per Standard XTA bietet die Chance, sie abzukoppeln von Variationen der Technologie für die Remote Nachrichtenkommunikation zwischen den Access Point.

> **Entkoppelung mittels XTA 2**
>
> Die XTA-Webservice-Schnittstelle ist ein passender Mechanismus zur Entkopplung der Knoten C1 und C4 vom zwischen den Access Points eingesetzten Messaging Protocol (siehe Abbildung 1.8).

In der 4-Corner-Infrastruktur ist also XTA als Mechanismus attraktiv für die Anbindung von Evidence Requester und Evidence Provider an die technische Infrastruktur. In der obigen Abbildung entspricht das der Anbindung der Backend-Knoten C1 bzw. C4 an die Access Points C2 bzw. C3.

4.2.3. Folgerung zum Transport-Binding

Es folgt, dass die Protokolle der C2/C3-Kommunikation durch ein Binding zu unterstützen sind, welches die benötigten Transformationen definiert, die die Knoten C2 und C3 leisten müssen.

- Ein Knoten **C2** nimmt Metadaten und Content im Format XTA von C1 entgegen und steht vor der Aufgabe, an einen Knoten C3 per OSCI oder alternativ AS4 versenden. Dasselbe gilt für die andere Kommunikationsrichtung (C3 per OSCI oder AS4 an **C2** und von dort per XTA an C1).
- Ein Knoten **C3** nimmt Metadaten und Content im Format XTA von C4 entgegen und leitet an einen Knoten C2 per OSCI oder alternativ AS4 versenden. Entsprechend für die andere Kommunikationsrichtung: C2 per OSCI oder AS4 an **C3** und von dort per XTA an C4).

> **Spezifikation des Transport-Binding**
>
> Pro Protokoll der Remote-Nachrichtenkommunikation (OSCI bzw. AS4) ist ein Transport Binding zu definieren. Das Transport Binding muss kompatibel sein mit den Anforderungen der E2E-Sicherheit.

Die Container für Metadaten und Content der Protokolle OSCI und AS4 sind nicht a priori deckungsgleich mit dem XTA-Format. Also wird pro Protokoll eine Transformationsvorschrift („Transport Binding“) benötigt, die den Transport über dieses Protokoll unterstützt.

Das Transport-Binding muss dabei so definiert werden, dass die Anforderungen der E2E-Sicherheit berücksichtigt werden.

Die Transformationsvorschrift XTA→OSCI wird als *XTA-OSCI-Binding* bezeichnet, die Transformationsvorschrift XTA→AS4 als *XTA-AS4-Binding*.

Eine vergleichende Betrachtung des Themas wird durchgeführt im Abschnitt 5.2.

4.3. Syntax und Payload des Nachweisabrufs

4.3.1. Request-Response Strukturen im Format OASIS-RegRep v4

Qua Vorgabe aus den Technical Desing Documents (TDD) der SDG-Umsetzung ist OASIS-RegRep v4 als Format für Nachweisabrufe durch die EU vorgegeben.

Auswahl und Anwendung von RegRep v4

RegRep v4 war nicht das Wunschformat unter Aspekten der Einfachheit und Nachvollziehbarkeit. Das Format hat sich dennoch als anwendbar erwiesen. Es wurde eine Java-Bibliothek entwickelt, um die benötigte Funktionalität zu kapseln. Diese Bibliothek konnte dann von den Evidence Requester- und Evidence Provider-Komponenten des PC ohne größere Probleme eingesetzt werden, um den Reqests eine Grundstruktur zu geben bzw. diese Struktur zu dekodieren.

4.3.2. Per Slot-Mechanismus eingebundene Datentypen des Payloads

RegRep-4 definiert eine Request-Response-Syntax für Abrufe, in dem bezeichnete Slots für die Einbindung von Objekten vorgesehen sind. Jeder Slot steht dabei für einen einzubindenden Inhalt (Payload).

Beispiele für eingebundenen Payload im Request sind: die Identität des Data Consumers, Identität der betroffenen Person, Zeitstempel der Abfrage, Art der angeforderten Daten bzw. des angeforderten Nachweistyps usw. Entsprechend wird die gelieferte Nachweisinstanz in der Response ebenfalls über den Slot-Mechanismus eingebunden.

Für jeden Slot, der in der Nachrichteninstanz Payloaddaten enthalten soll, sind im Rahmen der RegRep4-Syntax die Datentypen anzugeben, die in dem Slot zugelassen bzw. gefordert sind.

Anwendung des Slot-Mechanismus von RegRep v4

Der Slot-Mechanismus hat sich als umsetzbar erwiesen, wenn er auch kompliziert ist. Im Rahmen der vorgegebenen TDDs ist allerdings schwer erkennbar, welche Inhalte pro Slot vorgesehen sind. Anwender der TDD sollten für diesen Zweck mit ausdrücklichen Anleitungen unterstützt werden, wie sie in einer Spezifikation des Once Only Standards enthalten sein sollen.

4.3.3. Slot-Mechanismus & Payload-Validierung

Für die Kontrolle der erstellten bzw. zu lesenden Nachrichteninstanzen werden - wie immer - Validierungsmechanismen benötigt; für die datentechnische Auswertung und für die fachlich-rechtliche Kontrolle des übermittelten oder zu übermittelnden Inhalts.

Dies bedeutet in Bezug auf RegRep4-Dokumente: Zu validieren in einer Nachrichteninstanz sind die Datenobjekte, die den Slots zugeordnet sind, außerdem ist zu prüfen, dass die Datenobjekte jeweils dem richtigen Slot zugeordnet sind.

Es kann hier also nicht eine vollständige XML-Nachrichteninstanz gegen ein XML-Schema validiert werden, wie das in XÖV-Fachstandards der typische Validierungsmechanismus ist.

Vielmehr sind Abschnitte von XML-Bäumen zu prüfen gegen ein Set von Vorschriften, die Struktur und Gehalt referenzierter Objekte betreffen. Für diese Art der Validierungsanforderung eignet sich die XML-Technologie ISO Schematron, die in der Erprobung erfolgreich zum Einsatz kam.

Validierung per Schematron

Zur Validierung von Nachrichteninstanzen wurde die Technologie ISO-Schematron erfolgreich angewendet. Sie ergänzt die Validierung gegen XSD Schemate um die Möglichkeit der Prüfung gegen Geschäftsregel.

Die von der KoSIT im Auftrag des IT-Planungsrats herausgegebene Anwendung „Validator“ konnte im Meldeportal Behörden erfolgreich für notwendige Validierungsaufgaben auf der Basis von XSD Strukturvorgaben und Schematron Geschäftsregeln eingesetzt werden

4.3.4. Fachübergreifende Objekte: Einbindung von ISA2 Core-Vocabulary

Für die Spezifikation der Abruf-Queries wurden so weit wie möglich auf ISA^2 Core-Vocabulary basierende Datentypen eingesetzt. Dies geschah konform mit den Vorgaben der TDD.

In einigen Fällen weichen die für SDG-Abrufe definierten OO-Formate ab von denen, die für den OZG-Nachweisabruf im Rahmen der OZG-Umsetzung benötigt werden.

Aufgefallen sind in diesem Zusammenhang beispielsweise die folgenden Schwierigkeiten:

- **Unvollständiges Geburtsdatum**. Für ein unvollständig bekanntes Geburtsdatum fehlt in den Core Vocabularies der Europäischen Kommission eine passende Datenstruktur. In XÖV-Fachstandards, die in Deutschland angewendet werden, sind passende Datentypen für diesen Zweck enthalten.

  Dieser Sachverhalt wurde als Issue Nr. 17 bei der Weiterentwicklung der Core Vocabularies eingebracht. Basierend auf Ergebnissen des Erprobungsprojekts wurde am 7. Oktober 2021 der konkrete Vorschlag unterbreitet, den Datentyp `Date` zukünftig so zu modellieren, dass er für die Speicherung von Angaben zur Geburt gemäß des nationalen Fachrechts der Innenverwaltung geeignet ist. Mit Erfolg: “During the webinar of 02/12/2021 it was agreed to create a datatype Date as union of xs:date, xs:gYearMonth and xs:gYear”.

- **AGS-Daten**. Angaben zum Amtlichen Gemeindeschlüssel im Zusammenhang des zuständigen EPs müssen in den Request eingetragen werden, so dass das zuständige Register in DE gefunden werden kann. Im erprobten Anwendungsfall war für diese Angabe aber keine Position im Request erkennbar. Das Problem wurde sichtbar, als Daten in den Domänen-Fachstandard zu konvertieren waren, der die Angabe des AGS der zuständigen Behörde zwingend erfordert. Das Problem war in der vorliegenden Konstellation (Nachweistyp Meldebescheinigung) lösbar: aus der Anschrift der betroffenen Person konnte der AGS des zuständigen Evidence Provider abgeleitet werden. Das würde so aber schon für den Nachweistyp Geburtsurkunde nicht funktionieren, ist also nicht als allgemeingültige Regel generalisierbar.

- **Full Address**. Der CV-Datentyp full address wird gemäß TDD für die Formatierung der Anschrift der betroffenen Person angeboten. Er enthält die Angaben zu einer Anschrift in unstrukturierter Form (nicht aufgeteilt in einzelne definierte Elemente). Das stellt ein Problem für alle Kontexte des Datenabrufs dar, in denen ein Datenatz maschinell identifiziert werden muss und die Abfrage durchgehend medienbruchfrei zu prozessieren ist. Dieses Problem ist nicht auf DE beschränkt und betrifft auch nicht nur die Fachlichkeit Meldewesen.

4.3.5. Aufgabe der Spezifikation eines OO-Standards

Der Nachweisabruf gemäß SDG-VO soll allein auf Basis der TDD umsetzbar sein; wenigstens ist dies ein Ziel der TDD-Bereitstellung durch die EU. Warum ist es dann notwendig, einen Once Only Standard im Detail zu spezifizieren?

Die Spezifikation eines OO-Standards dient einerseits lediglich der Verbesserung von Qualität und Nachvollziehbarkeit für die SDG-VO-Umsetzung. Das wird im Rahmen der Umsetzung durch eine Vielzahl von Online-Services und Registerverfahren von Vorteil sein.

Darüberhinaus bietet das Format „OO-Standard“ aber auch die Möglichkeit, dass die Formate für den Nachweisabruf im Rahmen der OZG-Umsetzung methodisch auf entsprechende Weise spezifiziert und vorgegeben werden können (Synergieeffekt).

Andere MS planen nicht die Entwicklung eines OO-Standards, sondern lösen das Problem durch z.B. die zentrale Bereitstellung einer Software („SDG-Konnektor“), die die TDD-Schnittstellen umsetzt und die lokalen Online-Services oder Registerverfahren von dieser Notwendigkeit entlastet.

Ein OO-Standard kann unterschiedlich umfangreich definiert werden. Entweder spezfiziert er nur das Delta zu den TDD (Profilierung der TDD). Oder er bietet eine umfassende Darstellung, die auch den Gehalt der TDD reproduziert (geschlossene Spezifikation)

Bewertung: Das Ziel sollte die möglichst problemlose Umsetzbarkeit für die Hersteller von IT-Verfahren in DE sein, dafür scheint die Bereitstellung einer geschlossenen Spezifikation wesentlich zu helfen.

4.4. 4-Corner Infrastruktur & E2E-Sicherheit

4.4.1. Anforderungen an die Umsetzung von E2E-Sicherheit

Um echte E2E-Sicherheit im Rahmen der 4-Corner-Infrastruktur zu spezifizieren, müssen die folgenden Anforderungen umgesetzt werden.

Transport-Agnostik der Endpunkte

Data Consumer und Data Provider (die Endpunkte der Transaktionen im Rahmen des Nachweisabrufs) sind durch eine geeignete Anbindung an die Access Points vom Transportprotokoll zu entkoppeln (dafür steht der Standard XTA zur Verfügung). Auf der Basis der so umgesetzten Transport-Agnostik der Endpunkte ist die Infrastruktur in ihrer Gesamtheit deutlich leichter zu steuern und zu warten.

Binding für jedes verwendete Transport-Protokoll

Ein Transport-Bindung muss spezifiziert werden für alle zwischen der Access Points (C2 und C3) eingesetzten Protokolle (aktuell OSCI-Transport und AS4 in der Planung). Das Binding definiert die Transformation der Abfrageformate über die Access Points.

E2E-Sicherheit und Container-Strukturen

Um E2E-Sicherheit in der 4-Corner-Infrastruktur zu realisieren, muss Knoten C1 den Payload für Knoten C4 verschlüsseln. Daher muss C1 vor Übergabe der Objekte an Knoten C2 auf das Verschlüsselungszertifikat von C4 zugreifen. Als Voraussetzung davon muss C1 die Identität von C4 bekannt sein.

Es müssen durch die gesamte Infrastruktur die Objekte so über die Nachrichten-Formate (XTA, OSCI, AS4) prozessiert werden, dass das benötige Set an Metadaten für die Prozessierung durch die Transportknoten zugänglich ist (nicht vor ihnen durch unzugängliche Verschlüsselung verborgen).

Dafür sind die passenden Mechanismen und die nötigen Container-Strukturen der Nachrichtenformate zu spezifizieren. Diese Spezifikation sollte als Bestandteil in die Auslieferungsgegenstände des OO-Standards aufgenommen werden.

Die Änderungs- bzw. Erweiterungsbedarf, der daraus mit Blick auf die Standards und Komponenten XTA, DVDV, Data Consumer Gateway u.a. resultiert, ist in dem Rahmen dann ebenfalls aufzunehmen und zu verarbeiten.

4.4.2. Container und Mechanismen für die E2E-Nachrichtenprozessierung an den Kommunikationsknoten

Welche Container und welche Mechanismen sind betroffen und was ist zu beachten?

OSCI-Transport

Der Content-Container mit Attachments wäre zu signieren und zu verschlüsseln. Nachteil ist, dass er so auf das Protokoll OSCI-Transport-Kontext eingeschränkt bleibt. So entsteht die Idee, für den gegebenen Zweck einen Content-Container zu verwenden und über XTA zu versenden, so dass er durch den Knoten C2 in eine OSCI-Nachricht eingehängt werden kann.

Das funktioniert (wenn auch prinzipiell lösbar) in der Praxis aber nicht , weil das entsprechende Serialisierungsformat nicht definiert ist, es müsste dann als Erweiterung der OSCI-Spezifikation definiert werden. Zurzeit sind dafür keine Mechanismen vorhanden.

Ohnehin ist dieser Ansatz für echte Transport-Agnostik nicht geeignet.

Ansatz auf der Basis der Standards XML-Signature und XML-Encryption

Dieser Ansatz ist besser, wenn auch Nachteile vorhanden sind.

Abstrakte Message Parts sind zu definieren:

- Mit Blick auf die **Response** ist ein Part für die Nachweisinstanz zu definieren und ein zweiter Part für die RegRep4-Response mit den enthaltenen Metadaten (einschließlich der Referenz auf die Nachweisinstanz).
- Beim **Request** taucht das Problem nicht auf, weil dort nur ein Objekt (die Metadaten) verarbeitet werden muss.

Im Falle der Response sind die beiden Objekte separat zu verschlüsseln und zu signieren (so wird es in der Kryptobibliiothek der Durchstich-Umsetzung gemacht). Alternativ wäre dies auch als Bündel möglich, so ; dass die Objekte gemeinsam signiert werden können.

Verschlüsselungszertifikat des Lesers

Entscheidende Herausforderung für die E2E-Sicherheit ist, dass das Verschlüsselungszertifikat des Lesers verfügbar sein muss.

Dies bedeutet, dass der Leser dem Kommunikationsknoten C1 bzw. ggf. C2 bekannt sein muss, Es wäre hilfreich, wenn C1 von der Aufgabe entlastet werden könnte, das Verschlüsselungszertifikat des Lesers zu ermitteln bzw. abzurufen.

Es liegt nahe, dass C2 diese Aufgabe übernimmt, also die DVDV-Abfrage im Dienste von C1 durchführt, also diese Anforderung entsprechend wegkapselt, so dass im Anschluss das Verschlüsselungs- und das Signatur-Zertifikat bei C1 landet.

Dies sollte aber nicht als Verschlüsselungsservice des XTA-Servers umgesetzt werden , sonst wird C2 zum Hauptakteur und E2E zur leeren Bezeichnung. Das wäre also keine E2E-Sicherheit, die den Namen verdient. Diese Aufgabe sollte also in der Verantwortung der Fachbehörde (Online-Dienst) verbleiben, auch wenn die Fachbehörde mit ihren Anwendungen ggf. wiederum vom selben IT-Dienstleister gehostet wird.

XTA- und OSCI-bezogene Aspekte des OO-Standards

Im Standard XTA muss das Handling so beschrieben werden, dass der XTA-Server die Objekte entgegennehmen und auf die C2/C3-Strecke schicken kann, für die Kontexte, in denen dieser Mechanismus für E2E-Sicherheit verwendet wird

In der OSCI-Spezifikation ist keine entsprechende Anpassungen nötig.

Diese Verwendung wäre aber nicht eingegrenzt auf XTA-Schnittstellen, sie ist auch mit anderen Protokollen handhabbar.

Zuständigkeit für das Routing zum Leser

Diese Zuständigkeit soll bei C2 liegen, so dass C1 entlastet wird.

Der Mechanismus sollte in der Theorie sein: C1 übermittelt die nötigen Angaben über den Leser an C2. Diese werden im nächsten Schritt von C3 gelesen (C3 steht in engem Zusammenhang mit C4).

Lösung im Transport-Binding für OSCI: In OSCI sollte dafür ein ergänzender SOAP-Header (nur Gegenstand der Transportverschlüsselung) spezifiziert werden, der in der Adressierung von C3 eingesetzt wird.

Lösung im Transport-Binding für AS/4: Eine entsprechende Ergänzung der AS4-Spezifikation ist nicht nötig, weil die Funktionaltitä von Haus aus abgedeckt wird.

Erkenntnisse aus der Erprobung 2001

- Die Anforderung der E2E-Sicherheit wurden besser verstanden und konkreter kommuniziert.
- Die Problemlage wurde herausgearbeitet und die Hindernisse identifiziert.
- Ideen für Lösungsansätze wurden entwickelt. Diese sind jetzt reif für eine Umsetzung als Teil des geplanten OO-Standards.

Besser verstandene Prämissen für eine Infrastruktur, die den Namen 4-Corner verdient

Vor dem Hintergrund des RegMoG ist die 4-Corner-Infrastruktur mit E2E-Sicherheit von entscheidender Bedeutung. Im Vergleich dazu ist sie für eDelivery generell kein großes Thema, weil die E2-E-Sicherheit dort nicht zu den Anforderungen zählt.

Strukturmerkmale einer echten 4-Corner-Infrastruktur sind klar zu definieren und festzuhalten. Eine entsprechende Definition ist in den OO-Standard bzw. einen angehängten Teil prinzipiellen Charakters aufzunehmen. Die Dokumentation zu eDelivery (weniger die eDelivery-Spezifikationen selber) kann dabei helfen.

Merkmale einer 4-Corner-Infrastruktur

Die Entitäten C1 bis C4 müssen eigene Kommunikationsknoten sein, d.h. Kommunikationsinstanzen mit eigener Betriebsverantwortung. Es ist zwar nicht ausgeschlossen, dass zwei Knoten in der Dienstleistung desselben Rechenzentrums umgesetzt werden (z.B. derselbe Hosting-Dienstleister), sie müssen dann aber innerhalb dieses Rahmens separater Betriebsverantwortung unterliegen.

C3 hat eine besondere Aufgabe im Rahmen dieser Infrastruktur. Sie ist auch dann als separate Aufgabe zu leisten, wenn C3 zusammen mit C4 (Beispiel KRZN) in demselben Rechenzentrum angesiedelt ist.

4-Corner macht nur Sinn in einer Mandantenstruktur (nicht wenn es reine 1:1-Beziehung Fachbehörde und IT-DL gibt), dann ist auch Feinrouting notwendig (innerhalb der Mandanten von C3; also muss C3 versorgt werden mit lesbaren Informationen für dieses Routing (im entsprechenden Header).

Quellen

- https://documentation.init.de/display/ROOE/2021-10-12+JF
- https://projekte.kosit.org/once-only/oo-erprobung/-/issues/41#note_82773

4.5. Kopfstellen-Infrastruktur im Erprobungsprojekt

4.5.1. Das Kommunikationsszenario der Erprobung als 4-Corner-Szenario

Im Registermodernisierungsgesetz (RegMoG) und den Überlegungen der UAG Architekturmodell von 2020 wird das 4-Corner Modell zugrunde gelegt. Wo ist das KRZN-Meldeportal, welches im erprobten Szenario angesprochen wird, einzuordnen?

Im Beschluss der IMK zur Registermodernisierung im Innenressort von 12.06.2019 heißt es: *„Jedes Datum sollte [zukünftig] möglichst nur in einem Register der **originär zuständigen Behörde** vorhanden sein und von dieser gepflegt werden.“* Die für Meldedaten „originär zuständige Behörde“ in diesem Sinne ist die Meldebehörde der Kommune, in der die betroffene Person mit ihrer Hauptwohnung gemeldet ist.

In RegMoG wird das 4C-Modell gefordert*: „Datenübermittlungen zwischen Behorden verschiedener Bereiche erfolgen über **Vermittlungsstellen** verschlüsselt in gesicherten Verfahren. Vermittlungsstellen sind für den sicheren, verlässlichen und nachvollziehbaren Transport elektronischer Nachrichten zuständig und müssen diese Aufgabe **ohne Kenntnis der Nachrichteninhalte** erbringen können. Sie kontrollieren und protokollieren abstrakt die Übermittlungsberechtigung.“*

Zum Geschäftsmodell des KRZN-Meldeportals gehört die Wandlung zwischen XMeld und anderen Formaten für die Kunden. Genau diese Fähigkeit wurd auch bei der Erprobung eingesetzt. Es ist klar, dass diese Aufgabe nicht *ohne Kenntnis der Inhaltsdaten* erbracht werden kann. Damit ist auch klar, dass KRZN keine Vermittlungsstelle im Sinne im genannten Sinne ist.

4.5.2. Position des KRZN-Meldeportals in der 4-Corner-Infrastruktur

Vorläufige Einschätzung: Das KRZN-Meldeportal ist weder die originär für die Meldedaten zuständige Stelle, noch eine Vermittlungsstelle im Sinne des RegMoG, sondern es ist gemäß Bundesmeldegesetzt (§ 39 (3) BMG) die in NRW durch Landesrecht bestimmte Stelle die *sicherstellt, dass Meldedaten [durch andere Behörden] über das Internet oder über das Verbindungsnetz des Bundes und der Länder abgerufen werden können.* Diese Funktion wird nachfolgend als **Auskunft gebende Stelle** bezeichnet (dieser *Auskunft gebenden Stelle* in NRW entsprechen in den anderen Bundesländern die Meldedaten-Spiegelregister).

Hinweis: die Rechtsgrundlage in NRW regelt ausschließlich die Auskunft an öffentliche Stellen. Dem entsprechend hat KRZN derzeit ausschließlich Behörden als „Kunden“ *(Data Consumer)*.

Die Rollen der beteiligten Stellen sind in der Abbildung dargestellt. Die Inlandsbehörden, die die Daten anfordern, die Meldebehörden, die als originäre Quellen die Daten liefern und das KRZN-Meldeportal, das den Dienst der Auskunft gebenden Stelle anbietet.

Abbildung 4.3. Position des KRZN-Meldeportals in der 4-Corner-Infrastruktur

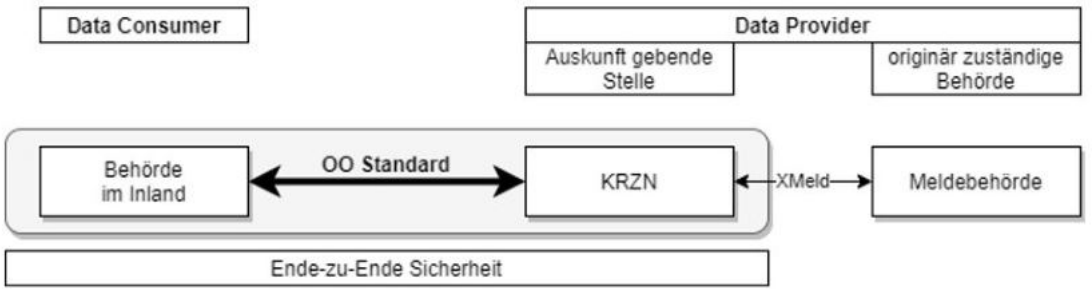


Abbildung - Rollen der beteiligten Stellen im nationalen Kontext

4.5.3. Fazit zur Kopfstellen-Infrastruktur im 4-Corner-Modell

Insgesamt ergibt sich im 4 Corner Modell

- Die **Data Consumer** befinden sich naturgemäß auf der Position **Corner-1**
- Meldeportal-KRZN füllt gemeinsam mit den Meldebehörden die Position **Corner-4** aus
- Die Ende-zu-Ende Kommunikation findet fachlich gemäß OO-Standard statt.
- Als E2E-Sicherheit wird sie durch die oben genannten Vermittlungsstellen technisch umgesetzt.

Quelle: Frank Steimke, *Erprobung Oncy Only Methoden und Standards durch KRZN*, vom 08.02.2021 (gekürzt)

4.6. SDG-Infrastruktur mit nationalen Kopfstellen

4.6.1. Leistungen einer domänenspezifischen Kopfstelle (bspw. Meldeportal NRW)

Adaptierung. Ein bestehendes Dienst-Portfolio wird für neue Dienstnutzer bzw. neue technische Vertriebswege erschlossen. Die Kopfstelle bietet zu den Diensten einen neuen Zugang an, ohne dass bei den registerführenden Behörden (Evidence Provider) Aufwände oder Änderungsbedarf entsteht (Legacy-Schnittstelle kann leisten).

Routing. Die Kopfstelle leistet unterstützendes Routing in einer dezentralen Infrastruktur, indem sie den für die Diensterbringung zuständigen Evidence Provider ermittelt und seine Dienstleistung anfordert.

4.6.2. Kritische Anmerkungen zur Übertragbarkeit

4-C-Infrastruktur

Das Meldeportal Behörden nimmt in der Rolle einer Kopfstelle als Knoten C4 an den Transaktionen teil. Sie zählt somit SDG-seitig als Evidence Provider. Dies ist für den cross-border Nachweisabruf sinnvoll. Zudem erscheint es auch ohne die spezifische „SDG Sichtweise “nicht unplausibel, eine durch Landesrecht für Auskünfte zu Meldedaten bestimmte öffentliche Stelle als „Evidence Provider“ zu verstehen, denn im Entwurf der Implementing Regulation ist dieser Terminus wie folgt definiert: “‘evidence provider’ means a competent authority as referred to in Article 14(2) of Regulation (EU) 2018/1724 that lawfully issues structured or unstructured evidence”. Gleichwohl ist unstrittig, dass zumindest in NRW die Nachweise die Nachweise nicht beim Meldeportal Behörden, sondern bei der jeweils zuständigen kommunalen Meldebehörde vorliegen. Ob insoweit mit dem im PoC realisierten Szenario die Anforderungen des § 7 Abs. 2 IdNrG vollumfänglich erfüllt werden können bliebe einer juristischen Prüfung vorbehalten, welche die Zielsetzung des Pilotvorhabens 7 weit übersteigt.

Transformation.

Die Umsetzung von neutralen Nachweisabfragen auf die domänenspezifische XMeld-Schnittstelle ist nur für solche Domänen übertragbar, in denen ein dömänenspezifischer Fachstandard vorgegeben oder zumindest faktisch etabliert ist. Ausweislich Tabelle 4.1 ist dies für fast alle der im Zielbild genannten TOP 18 Register der Fall.

Tabelle 4.1. Domänenspezifische Standards für TOP 18 Register

Bereich	Register	Domänenspazifischer Standard
Inneres	Melderegister	XInneres / XMeld

Bereich	Register	Domänenspazifischer Standard
	Passregister	XInneres / XPass Wird derzeit entwickelt gemäß Beschlusslage der IMK und des AK I
	Personalausweisregister	
	Personenstandsregister	XInneres / XPersonenstand sowie XPersonenstandregister
	Ausländerzentralregister	XInneres / XAusländer
Finanzen	Identifikationsnummernregister	XBasisdaten
	Daten der Finanzverwaltungen der Länder	IT Standards des KONSENS Verbunds der Finanzverwaltung
Justiz	Bundeszentralregister	XBFJ
	Gewerbezentralregister	
Arbeit & Soziales	Bei der Bundesagentur für Arbeit systematisch geführte personenbezogene Datenbestände nach dem Dritten Buch Sozialgesetzbuch	XSozial (in Entwicklung durch NRW) Zudem wahrscheinlich IT Standards gemäß der Gemeinsamen Grundsätze Technik des § 95 SGB IV (Prüfung erforderlich)
	Betriebedaten der Bundesagentur für Arbeit	
	Stammsatzdatei der Datenstelle der Rentenversicherung gemäß § 150 des Sechsten Buches Sozialgesetzbuch	
	Versichertenkonten der Rentenversicherungsträger gemäß § 149 des Sechsten Buches Sozialgesetzbuch	
	Versichertenverzeichnisse der Krankenkassen	
	Zentrales Unternehmerverzeichnis der gesetzlichen Unfallversicherung	
Bildung	Bei den allgemeinbildenden und beruflichen Schulen, Schulbehörden, Bildungseinrichtungen nach § 2 des Hochschulstatistikgesetzes systematisch geführte personen- bezogene Datenbestände zu Bildungsteilnehmenden	XHochschule (in Entwicklung)
Wirtschaft	Verzeichnis der gemäß § 14 der Gewerbeordnung angezeigten Gewerbebetriebe	XUnternehmen
Verkehr	Zentrales Fahrzeugregister	XKFZ

Gleichwohl gibt es sicherlich fachliche Domänen, in denen es bisher noch keinen domänenspazifischen IT-Standard gibt, und in denen die registerführenden Stellen folglich die OO-Schnittstelle implementieren müssen. Es stellt sich die Frage, warum dann nicht gleich durchgehend auf OO-Mechanismen aufgesetzt werden sollte, statt innerhalb bestimmter Domänen auf Transformationsleistungen einer Kopfstelle zu setzen. Es konnte im Erprobungsprojekt nur rudimentär untersucht werden, welchen Unterschied es machen würde, wenn die OO-Anfrage direkt an die zuständige MB gesteuert würde (über Dienste der Registermodernisierungsbehörde, unter Verwendung zentrale Verzeichnisdienste oder auf einem anderen Wege).

Routing-Mechanismus

Das im Erprobungsprojekt umgesetzte Routing durch die Kopfstelle funktioniert nur zufällig. Es macht sich den Umstand zunutze, dass aus der Anschrift der betroffenen Person der Nachweisabfrage (Subject) die für die Nachweiserbringung zuständige registerführende Behörde ermittelt werden kann. Aus dem Subject

werden dabei also durch die Kopfstelle Informationen für das Routing entnommen. Das ist offensichtlich nicht übertragbar auf andere Domänen.

Insofern bedarf es voraussichtlich eines Erweiterungsmechanismus um zuätzliche Attribute abzufragen, die für das Routing der Nachrichten erforderlich sind. Diese Erkenntnis korrespondiert mit einer entsprechenden Anforderung von deutscher Seite an die *High Level Architecture* und das EDM im SDG Kontext.[1]

4.6.3. Weitere Beobachtungen

Angaben zum Evidence Provider qua EU-Vorgaben. In der RegRep4-Datenstruktur sind keine separaten Angaben - kein Slot - für die Benennung des Evidence Provider vorgesehen (Slot nur enthalten für die Benennung des Evidence Requester). Es wird offenbar auf die Einträge von DE im DSD gesetzt, also auf die Verwendung zentraler Verzeichnisdienste, um den Evidence Provider zu ermitteln. Sobald der Evidence Provider identifiziert wurde (Schritt 1), lässt sich der Request an diesen Adressaten versenden (Schritt 2). Sofern im nationalen Kontext eine Ende-zu-Ende Verschlüsselung erfolgen soll oder muss, muss vorher der öffentliche Schlüssel des Evidence Provider ermittelt werden, damit die Nachricht für ihn verschlüsselt werden kann.

Vergleich mit Routing per DVDV. Der OOTS Mechanismus sieht die Ermittlung des Evidence Provider auf Basis einer DSD-Abfrage vor (Ermittlung der zuständigen Stelle). Diese Funktionalität kommt in der DVDV-Infrastruktur nicht vor. Eine DVDV-Abfrage fragt zu einer gegebenen zu adressierenden Stelle (deren ID muss also bekannt sein, z.B. „Meldebehörde der Stadt Iserlohn" oder "Meldebehörde, die zuständig ist für den Postleitzahlenbereich xxxxx“) bestimmte technische Erreichbarkeits- und Kommunikationsparameter ab. — *Hinweis:* dieses Thema ist mit der Lenkungskreis-Vorlage „Entscheidung zur Umsetzung der Komponente Registerdatennavigation als zentralen Routing-Dienst (Routing As a Service) auf Grundlage des Deutschen Verwaltungsdienstverzeichnis (DVDV) unter Wiederverwendung von Lösungsansätzen aus FIT-Connect“ aufgenommen worden. Darin wird perspektivisch der Aufbau eines zentralen Zuständigkeitsverzeichnis der Deutschen Verwaltung (DVZV) als Ergänzung des DVDV vorgeschlagen.

Angaben zum Subject im Evidence Request. Im Rahmen der Erprobung stellte sich die Frage „auf welcher Basis kann die Kopfstelle den für diesen Request zuständigen Evidence Provider ermitteln und adressieren“? Es ergibt sich ein Zusammenhang zum Thema Extended Routing. Auch mit Blick auf den angeforderten Nachweistyp in bestimmten Domänen ist der Requestinhalt entsprechend zu erweitern. Beispielsweise ist im Rahmen des Hochschulwesens ggf. eine Matrikel-Nummer im Request anzugeben, um die Angaben zum Evidence-Subject zu vervollständigen. Dafür sind für solche Anwendungsfälle ergänzende Slots zu definieren.

4.6.4. Abbildung der Kopfstellen-Infrastruktur auf das 4-Corner-Modell

C3 und C4. Das KRZN-Meldeportal deckt Leistungen des Knoten C3 (Empfängerinfrastruktur), außerdem Leistungen des Knoten C4 (Verarbeitung des Payload) ab. Als Knoten C4 operiert es immer dann, wenn Payload-Daten zugegriffen und verarbeitet werden. Deswegen ist die Entkopplung der Knoten C3 und C4 über XTA-WS ein wichtiges Thema der Erprobung.

Nur C3. Eine Kopfstelle im SDG-Sinn leistet hingegen nur Infrastruktur-Dienste im Sinne eines Access Points, entspricht also lediglich dem C3-Knoten mit Routing-Funktionalität

4.6.5. Begriffliche Abgrenzungen und Erläuterungen

Abgrenzung vom Consumer Gateway

Die Kopfstelle im Erprobungsszenario leistet auch als C3-Knoten mehr als ein Access Point, der sich auf Transportaufgaben beschränkt. Beispielsweise könnten im Sinne eines XTA-Servers Mehrwertdienste erbracht werden, wie beispielsweise die Auswahl des passenden Messaging Protokolls.

[1] Die aktuellen Fassungen des Implementing Act und der TDD berücksichtigen die deutschen Anforderungen. Insofern ist davon auszugehen, dass die von unserer Seite vorgeschlagenen Ergänzungen für das Routing im OOTS auch für das Routing im NOOTS ausreichen werden.

Im Erprobungsszenario übernimmt nicht die Kopfstelle, sondern der eingesetzte XTA-Server das Routing über DVDV. Dies geschieht auf der Basis von Angaben im XTA-Header.

Begriffe Kopfstellen und Access Points

Kopfstelle. Es ist eine Entscheidung zu treffen über Einrichtung von Kopfstellen zur Anbindung des nationalen OOTS an das SDG-OOTS, entsprechend eine Empfehlung an die betroffenden Fachministerkonferenzen (FMK) zu domänenspezifischen Kopfstellen

Access Points. Es steht die Entscheidung an über Anzahl, Zuschnitt und Zuständigkeit der deutschen Access Points, entsprechend eine Empfehlung an die FMK zur Anbindung über eine Access Point Infrastruktur.

Access Points sind hier im Sinne von Peppol-eDelivery als Knoten C2 bzw. C3 zu verstehen.

Das ist auf die Infrastruktur im Erprobungsprojekt übertragbar, in der ein XTA-Server als Access Point dient, ansprechbar für die Fachdienste über die XTA-Schnittstelle, während zwischen den Access Points das Protokoll OSCI verwenet wird.

Nicht behandelt wurde im erprobten Szenario die Konzeption der Verteilung von Nachweisabrufen bei der SDG-Umsetzung in Deutschland. Insbesondere wurde nicht untersucht, wie diese mit einer Kopfstellen-Infrastruktur zusammenpassen könnte.

4.6.6. Extended Routing

Definiert für den Routing-Request an das DSD sind von der EU ursprünglich die Parameter *Evidence Type* und *Member State*.

Ausgeliefert wird in der Response eine Liste von Providern.

Der Vorschlag Deutschlands aus 2021 zur Erweiterung dieser Struktur - besonders im Dienste der Auffindbarkeit in einer dezentralen Registerinfrastruktur - wurde dann integriert und die TDD in Januar 2022 entsprechend ergänzt.

DSD reagiert auf fehlende Parameter mit der Meldung „die folgenden Attribute werden benötigt“

Der Requester startet auf der Basis einen zweiten Request an das DSD mit ergänzten Attributen, die in Bezug auf einen Nachweistyp zu definieren sind.

Dies können Attribute sein zur Auffindbarkeit oder ergänzende Attribute zum Nachweistyp. Für die Abfrage einer Geburtsurkunde würde z.B. die Postleitzahl oder die Bezeichnung des Geburtsorts benötigt, so dass auf dieser Basis das Geburtsstandesamt identifiziert werden kann.

Die ergänzenden Angaben sind in diesem Szenario vom User beizusteuern.

4.7. Mechanismen der Validierung beim OO-Abruf

4.7.1. Technologie der Validierung

Voraussichtlich werden im Rahmender SDG-VO-Umsetzung Eigenschaften von Nachweisen syntaxneutral zu beschreiben sein (mittels der Technologie RDF). Dadurch soll die Bereitstellung in verschiedenen Formaten (beispielsweise XML oder JSON) ermöglicht werden.

Im Rahmen der Once Only Erprobung wurde im ersten Schritt die XML Repräsentation als primäres Zielformat für Nachweise festgelegt. Dies entspricht der Vorgehensweise des TOOP Projekts. Die Struktur der RegReg 4 Nachrichten wird zunächst durch deren XSD Schema festgelegt. Darüber hinaus nutzt TOOP Business Rules: *In order to facilitate interoperability for the once-only principle, TOOP defined a set of **business rules which should be applied in each transaction**. For each business rule, a corresponding **Schematron rule** is described. The business rules are sets of rules that clarify the content of instances by stating mandatory fields, fixed values*

(like code lists), dependency between fields in the same object and dependency between different objects. Abbildung 4.4 zeigt einen Ausschnitt der für TOOP und SDG festgelegten Geschäftsregeln.

Abbildung 4.4. SDG Geschäftsregeln (Auszug)

rule ID	flag	Schematron message	Checked by
br_check_country_countrycode	fatal	The country code must always be specified using the correct code list.	Business Rules Schematron
br_check_currency_code	fatal	A currency type code code must always be specified using the correct code list.	Business Rules Schematron
br_check_distribution_format	fatal	A distribution format code must always be specified using the correct code list.	Business Rules Schematron
br_check_doc_mediatype	warning	A mediaType code SHOULD always be specified using the correct code list.	Business Rules Schematron
br_check_error_code	fatal	An 'error code' code must always be specified using the correct code list.	Business Rules Schematron
br_check_error_data_element_response	fatal	An 'error code' code must always be specified using the correct code list.	Business Rules Schematron
br_check_error_origin	fatal	An error origin code must always be specified using the correct code list.	Business Rules Schematron

Das bedeutet, dass die TOOP Validierungsmechanismen ganz klassisch auf XML Instanzen ausgerichtet sind. (Schematron funktioniert nicht mit JSON). Darüber hinaus gilt;

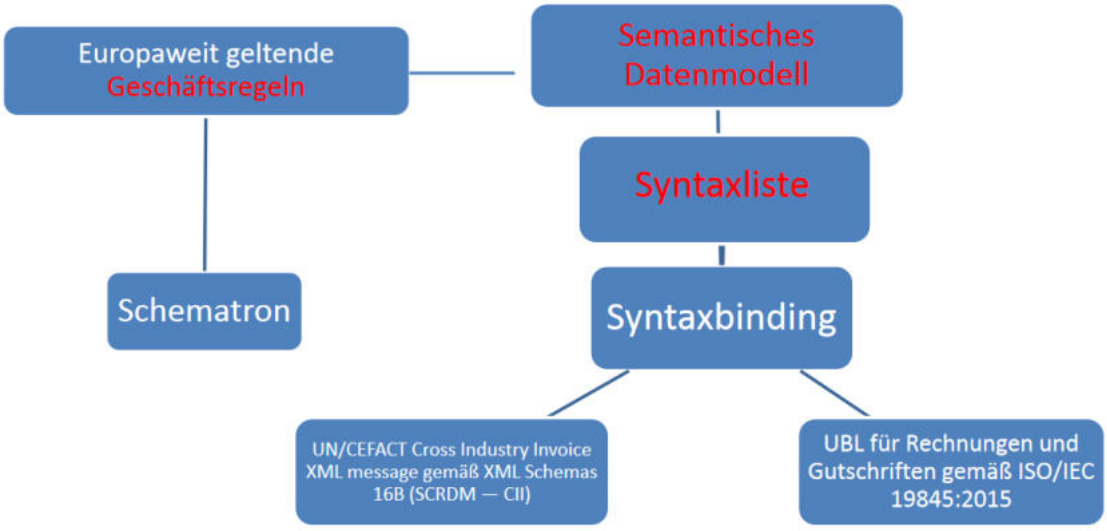
1. Die Struktur wird mit XML Schema Version 1.0 beschrieben;
2. Darüber hinaus werden Business Rules mit ISO Schematron definiert;
3. Sowohl die Struktur als auch die Business Rules sollen bei jeder Transaktion geprüft werden;
4. Dehalb müssen alle Kommunikationspartner in der Lage sein, XML Instanzdokumente sowohl gegen XSD 1.0 Schemata als auch ISO Schematron Regeln zu prüfen.

Dieses Vorgehen ist von anderen XÖV Standards wie beispielsweise XRechnung bereits bekannt.

4.7.2. Analogie zur Standardisierung XRechnung

Die EU Richtlinie 2014/55/EU verpflichtet öffentliche Auftraggeber zur Verarbeitung elektronischer Rechnungen. Deren Format wird im Normenwerk der EN 16931 Electronic Invoicing definiert. Die Umsetzung in Deutschland ist der von der KoSIT herausgegebene Standard XRechnung. Die Elemente einer Kernrechnung sind syntaxneutral beschrieben. Die EU Kommission hat zwei Syntax Mappings festgelegt (UBL und CII), die beide auf eine klassische XML Repräsentation abzielen.

Abbildung 4.5. Prüfung von Geschäftsregeln am Beispiel XRechnung



1. Die Struktur einer Rechnung wird durch XML Schema 1.0 beschrieben. Zwei verschiedene Schemata (UBL, CII) dürfen genutzt werden.

2. Darüber hinaus werden Business Rules von der EU-KOM festgelegt. Sie werden durch ISO Schematron umgesetzt. Da zwei Syntaxen zulässig sind, gibt es je ein Schematron Schema pro Syntax.

3. Sowohl die Struktur als auch die Business Rules sollen bei jeder Übermittlung einer elektronischen Rechnung geprüft werden;

4. Deshalb müssen alle Kommunikationspartner in der Lage sein, jede elektronische Rechnung gegen die jeweils erforderliche Kombination aus XSD Schema und zugehörigen Schematron Regeln zu prüfen.

Um dies bundesweit zu ermöglichen, hat die KoSIT im Auftrag des IT-Planungsrats den KoSIT Validator entwickelt und in Form einer Referenzimplementierung bereitgestellt. Das Produkt kann gegen beliebige XSD- und Schematron Schemata validieren. Für den Einsatz im Kontext elektronischer Rechnungen werden die entsprechenden Konfiguration und die Schematron Regeln ebenfalls auf GitHUB bereitgestellt. Der KoSIT Validator ist bei den Empfängern elektronischer Rechnungen beim Bund (ITZ Bund) und Ländern (u. a. Dataport) im Einsatz.

Nachfolgend ein Beispiel für Business Rules aus der Spezifikation XRechnung, welche die in XSD Schema vorliegende Strukturbeschreibung ergänzen.

Abbildung 4.6. Beispiel für Geschäftsregeln am Beispiel der Norm EN 16931-1

BR-CO-20	Wenn die Gruppe „INVOICE LINE PERIOD“ (BG-26) verwendet wird, müssen entweder das Element „Invoice line period start date“ (BT-134) oder das Element „Invoice line period end date“ (BT-135) oder beide gefüllt sein.	Invoice line period	BT- 134, BT-135
BR-CO-21	Jede Gruppe „DOCUMENT LEVEL ALLOWANCES“ (BG-20) muss entweder ein Element „Document level allowance reason“ (BT-97) oder ein Element „Document level allowance reason code“ (BT-98) oder beides enthalten.	Document level allowance	BT-97, BT-98

4.7.3. Validierung gegen nationale Vorgaben

Im Projekt wurde auch der Umgang mit zusätzlichen nationalen Anforderungen untersucht. Dafür wurde folgendes Beispiel gewählt:

- Für die Schreibweise der Namen natürlicher Personen dürfen in Melderegistern ausschließlich lateinische Buchstaben genutzt werden. Diese verbindliche Vorgabe korrespondiert mit entsprechenden Beschlüssen des IT-Planungsrats. Sie ist auch in dem Standard XMeld umgesetzt, das bedeutet, dass es technisch nicht möglich ist einen Datenabruf im Standard XMeld zu formulieren, bei dem der Name der betroffenen Person andere als lateinische Zeichen enthält.

- Der in Beispiel 4.1 dargestellte Ausschnitt der Anforderung eines Nachweises für eine Person mit dem Namen Μίκης Θεοδωράκης kann daher nicht in eine korrekte XMeld Nachricht überführt werden. Selbst wenn es möglich wäre, eine entsprechende XMeld Nachricht zu erstellen, würde die Anfrage nicht zu einem Ergebnis führen, weil in keinem Melderegister der Bundesrepublik eine Person gespeichert sein kann, deren Name mit griechischen Buchstaben geschrieben ist.

  Vielmehr ist durch Verwaltungsvorschriften sichergestellt, dass ein in griechischen Zeichen geschriebener Name durch Transliteration in die lateinische Schrift überführt wird (in diesem Fall *Mikis Theodorakis*).

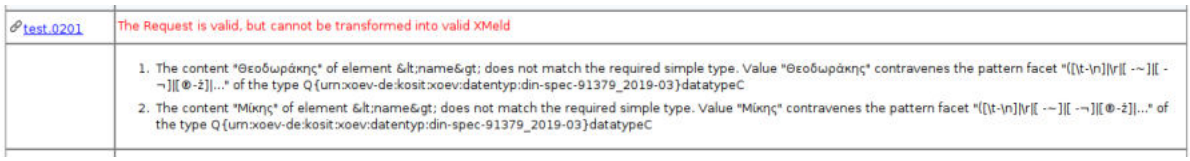
- Es scheint daher sinnvoll zu sein, nationale Vorgaben in Strukturvorgaben oder in zusätzliche Geschäftsregeln zu überführen, die ebenfalls überprüft werden. Im betrachteten Beispiel lautet die abstrakte Regel: „Die Datenfelder Vorname und Nachname einer Person dürfen ausschließlich lateinische Buchstaben enthalten“. Ein Verstoß gegen entsprechende Regeln führt zu einem technischen Fehler (siehe Abbildung 4.7).

Dies führt jedoch an anderer Stelle zu Komplikationen, denn der bisherige Entwurfsstand der Dokumente der EU-Kommission macht keine Vorgaben zu dem Zeichensatz, der für Datenübermittlungen im OOTS zulässig ist. Das bedeutet, dass eine Nachweisanforderung mit dem in Beispiel 4.1 gezeigten Fragment aus Sicht des SDG Systems fehlerfrei ist (kein Verstoß gegen die europaweit abgestimmten Regelungen des SDG OOTS), während sie aus nationaler Sicht fehlerhaft sind (Verstoß gegen Regeln, die durch nationale Vorgaben begründet sind).

Beispiel 4.1. Angaben zur Person, die nach nationalem Recht nicht gültig sind

```
<rim:Slot name="NaturalPerson">
         <rim:SlotValue xsi:type="rim:AnyValueType">
            <xoevoo:NaturalPersonQuery>
               <xoevoo:FamilyName absent="false">Θεοδωράκης</xoevoo:FamilyName>
               <xoevoo:GivenName absent="false">Μίκης</xoevoo:GivenName>
               <xoevoo:GenderCode>m</xoevoo:GenderCode>
               <xoevoo:BirthDate>1925-07-29</xoevoo:BirthDate>
               <xoevoo:Address>
                  <cvb:LocatorDesignator>7a</cvb:LocatorDesignator>
                  <cvb:Thoroughfare>Waldrand</cvb:Thoroughfare>
                  <cvb:PostName>Berlin</cvb:PostName>
                  <cvb:PostCode>32657</cvb:PostCode>
                  <xoevoo:AddressCode listName="AGS">11000000</xoevoo:AddressCode>
               </xoevoo:Address>
            </xoevoo:NaturalPersonQuery>
         </rim:SlotValue>
      </rim:Slot>
```

Abbildung 4.7. Fehlermeldung beim Verstoß gegen nationale Vorgaben (Beispiel)



Der Sachverhalt konnte im Erprobungsprojekt lediglich als problematisch identifiziert, aber nicht geklärt werden. Vermutlich werden solche Fälle in der Praxis zunächst zu unterschiedlichen Auffassungen verschiedener Mitgliedsstaaten und der zuständigen SDG Gremien führen, bevor irgendwann eine generelle Regelung zum Umgang mit nationalen Vorgaben gefunden wird.

4.7.4. Schlussfolgerungen

1. Für die formale Beschreibung von Nachweisen (Syntax, Semantik, Geschäftsregeln) ist eine syntaxneutrale Semantic Web Methodik (RDF, SHACL, ...) angestrebt. Diese Methodik hat aber noch nicht die erforderliche Reife für die Validierung der zugehörigen Instanzdokumente.

2. XML ist das primäre Datenformat der Instanzdokumente für den Abruf und die Übermittlung von Nachweisen. Deshalb werden Validierungsmechanismen für XML normativ festgelegt. XML Instanzen von *Request* und *Response* werden mittels einer Kombination von XSD 1.0 und ISO Schematron validiert.

3. Die Regeln zur Anbindung von Data Providern und Data Consumern *MÜSSEN* so gefasst werden, dass diese in der Lage sein müssen die ausgetauschten Nachrichten nicht nur gegen XSD Schema 1.0, sondern auch gegen ISO Schematron zu validieren. Sie *SOLLTEN* so gefasst, dass Data Provider oder Data Consumer *bei jeder Transaktion verpflichtet* sind gegen die offiziell herausgegebenen Schemata zu prüfen - es ist noch unklar, ob das bedeuten würde dass andere Formate als XML faktisch ausgeschlossen sind.

4. Die Spezifikationen der verfügbaren Nachweise müssen das zugehörigen XSD Schema und das zugehörige Schematron Schema beinhalten. Herausgeber der Spezifikation, und damit der beiden Schemata, ist die jeweils originär für den Nachweis zuständige Behörde bzw. ein assoziiertes Standardisierungsvorhaben (z. B. XInneres für Nachweise aus Registern der Innenverwaltung). XSD Schema und Schematron Schema sollten in einem atomatisierten Verfahren aus der syntaxneutralen Formulierung abgeleitet werden (also eine automatisierte Transformation von RDF+SHACL in XSD+Schematron). Dies *kann* Gegenstand der Erweiterung des XÖV Rahmenwerks im Rahmen des Gesamtvorhabens sein.

5. *Wie* die öffentlichen Stellen diese Validierung durchführen bleibt ihnen überlassen. Aber zur Unterstützung bei dieser Aufgabe bietet der IT-Planungsrat den KoSIT Validator als Referenzimplementierung an.

4.8. Lessons learnt - Umsetzung der XTA-Schnittstellen

Der Standard XTA besteht aus einer WSDL-Spezifikation. Er definiert also nur, was über den Draht gehen muss (Serialisierung). Das stellt in der Entwicklung vor die Herausforderung, dass client-seitig dafür zu sorgen ist, dass der XTA-Server genau die passenden Zeichensequenzen empängt.

Die KoSIT bietet für die entsprechende XTA-Version Beispielcode für einen XTA-Client an (siehe Überschrift *Nicht-normative Hilfsmittel zu XTA 2 Version 3* auf der Seite https://www.xoev.de/downloads-2316#XTA).

Für die Umsetzung der XTA-Schnittstellen erwies sich diese Unterstützung in Ansätzen als hilfreich. Auch trug Support durch erfahrene XTA-Entwickler aus dem Netzwerk zum Erfolg bei. Dies war aber mit erheblichem Koordinationsaufwand verbunden und wird sich unter gewöhnlichen Bedingungen so nicht bewähren. Hersteller von IT-Fachanwendungen bzw. von Software für registerführende Behörden würden entsprechende Wege nicht auf sich nehmen können.

Der Einsatz des XTA-Servers COM Despina erwies sich als hilfreich, es zeigte sich aber, dass er weniger Flexibilität mitbringt als für ein Erprobungsprojekt gefordert ist. So läßt sich beispielsweise nicht konfigurieren, dass über die OSCI-Strecke (von Knoten C2 an Knoten C3) unverschlüsselt übertragen werden kann. Für den produktiven Einsatz wäre dies eine sehr ungewöhnliche Anforderung, aber für die Erprobung war das von Nachteil, weil für die Unterstützung der E2E-Sicherheit eine eigene Kryptobibliothek entwickelt und eingesetzt worden war. In diesem speziellen Fall ist eine zusätzliche Verschlüsselung hinderlich, da für den Sender aufwändig und vom Empfänger doppelt und darüberhinaus mit unterschiedlichen Zertifikaten zu entschlüsseln. Dadurch wurde die Komplexität unnötig gesteigert.

Zusammenfassend werden folgende Maßnahmen für den erfolgreichen Einsatz von XTA 2 zusammen mit OSCI empfohlen:

- Die **Governance** sollte optimiert werden - die Steuerung der Anbindung von Behörden an die OSCI Infrastruktur mittel XTA 2 sollte quer zu den Fachbereichen durch den IT-Planungsrat gefordert und gefördert werden.

- Die **Mechanismen der E2E-Verschlüsselung** müssen weiter optimiert werden, die Funktionalität ist in die XTA-Server zu integrieren (Spezifikation von Containern und Mechanismen im OO-Standard, anschlussfähig an AS4, OSCI und XTA).
- Der Support für XTA 2 muss grundlegend ausgebaut werden.
- Der Beispielcode für den XTA-Client (von der KoSIT seit 2020 angeboten) ist hilfreich, aber nicht ausreichend. Dieses Angebot sollte zur **Bereitstellung einer XTA-Bibliothek** nach dem Vorbild der OSCI-Bibliothek ausgebaut werden.
- Funktionalität der Bibliothek sollte alle **Methoden der XTA-Applikationsebene** umfassen, also die für die Knoten C1 und C4 relevante Funktionalität mit dem Fokus auf: synchroner Nachweisabruf per XTA, Transport von Attachments, DVDV-Einbindung).
- Für den **Betrieb dieser Bibliothek** (Wartung und Pflege) ist zu sorgen.
- Parallel sollten die Eintrittshürden für die XTA-Umsetzung weiter gesenkt werden. Die aktuelle Basistechnologie für XTA ist SOAP bzw. WSDL. Es sollte geprüft werden, ob auch hier in Zukunft (wie von DVDV 2 bereits umgesetzt) stärker auf REST Protokolle zu setzen ist.

Kapitel 5. Weitere konzeptionelle Arbeiten

5.1. Rollen beim Once Only Abruf

5.1.1. Anwendung von Core Vocabularies in TOOP

In der Tabelle wird aufgelistet, wie bestimmte grundlegende Entitäten gemäß Once Only Technical Specification der EU (TOOP) durch Objekte aus den ISA^2 Core Vocabularies abzubilden sind (Stand Mitte 2021).

Tabelle 5.1. Nutzung von Elementen des Core Vocabulary

Actor/Entity	Description	Core Vocabularies Used
Evidence Requester (ER)	The Evidence Requester is the initiator of an OOTS transaction. It can be a public service that requires some data about the data subject.	CPOV, CPSV-AP (Agent)
Evidence Provider (EP)	The Evidence Provider is the responder of an OOTS transaction. It can be either a public or private organisation providing data on behalf of the Data Subject.	CPOV, CPSV-AP (Agent)
User	The User is the Entity on whose behalf the evidence is requested. It can be either a Natural Person or a Legal Person.	Core Person (Natural Person) Core Business (Legal Person)
Evidence Type	An Evidence Type is a Dataset that is required to prove a Requirement or Criterion.	CCCEV
Dataset	A collection of data, published or curated by a single agent (DP), and available for access in one or more representations.	CCCEV, DCAT, BREG-DCAT-AP
Criterion/Requirement	A requirement either expressed as a criterion with a legal basis or an information requirement, is a question or a request for data that must be fulfilled.	CCCEV

5.2. Abstraktes Protokoll-Binding

In diesem Abschnitt werden die unterschiedlichen Modelle von SDG-OO (basierend auf TOOP) mit seinen derzeitigen, recht konkreten Nachrichtenaustauschkonzepten (Nachrichtenformate, eDelivery-Transport) mit den generellen Konzepten von OSCI-Transport, AS4, eDelivery (inkl. SBDH) und XTA gegeneinander gehalten. Zweck ist Gemeinsamkeiten und Unterschiede zu identifizieren, um eine Abstraktion insbesondere der Protokollschicht zu entwickeln. Gerade vor dem Hintergrund der Unsicherheiten hinsichtlich Fortschreibung von SDG-OO ist aus nationaler Sicht eine stärkere Entkopplung vom Transportprotokoll und ein damit einhergehender vereinfachter Austausch der Transporttechnologie wünschenswert (→ Transportagnostik).

5.2.1. Kommunikationstopologie (4-Corner, multi-hop)

In vielen in diesem Kontext relevanten, transportbezogenen Spezifikationen (OSCI, AS4, eDelivery, SBDH, XTA) wird auf die Topolgie der Kommunikation, also den Rollen der beteiligten Kommunikationsknoten, eingegan-

gen. Und auch das RegMoG verweist explizit auf die Rolle der Vermittlungsstellen. Im Einzelnen unterscheiden sich dabei u.a.

- die Anzahl der (möglichen) Knoten
- die Verbindlichkeit bzw. Optionalität für deren Nutzung
- die Abstraktion und Ebene (physisch oder logisch)
- die Rolle und Verantwortung der Knoten
- die verwendeten Begriffe.

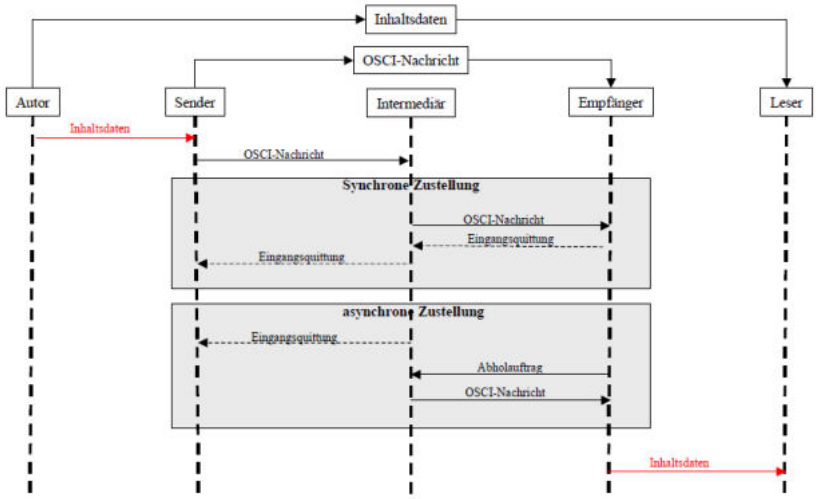
Allgemein gibt es mittlerweile so etwas wie einen Konsens darüber, dass eine Topolgie mit vier Knoten (4-Corner-Topology) und einer damit verbundenen, definierten Verantwortlichkeit eine in mehrfacher Hinsicht sinnvolle Ausprägung darstellt. Es lohnt daher, die verschiedenen Spezifikationen hinsichtlich der Aspekte zur Topologie zu analysieren und zu vergleichen.

5.2.2. OSCI-Transport

OSCI-Transport definiert einerseits logische Rollen (Autor, Leser, Sender und Empfänger) und andererseits einen physischen und verbindlichen Kommunikationsknoten, dem OSCI-Intermediär. In der Praxis hat sich für reine, direkte OSCI-Kommunikationen (ohne Nutzung von Vermittlungsstellen und XTA) eine 3-Corner-Topologie etabliert: Die logischen Rollen Autor/Sender und Empfänger/Leser werden physisch i.d.R. nicht getrennt, sondern von einem Knoten jeweils gemeinsam eingenommen. Das liegt u.a. daran, dass die OSCI-Transport-Bibliothek mit ihrem Programmiermodell eine physische Aufspaltung der Rollen nicht direkt unterstützt. Grundsätzlich lässt die OSCI-Spezifikation aber eine Auftrennung der Instanzen von Autor/Sender bzw. Empfänger/Leser zu (Zitat aus OSCI-Transport 1.2: "*Auch liegt der gegebenenfalls notwendige Datentransport von den Autoren zum Sender und vom Empfänger zu den Lesern außerhalb des Anwendungsbereichs dieser Spezifikation.*").

Jedoch ist die Rolle „Autor" nicht gleichzusetzen mit einem Knoten "Corner 1" bzw. der "Leser" mit "Corner 4". Corner sind immer reine Kommunikationsknoten. Allerdings ist die Wahrnehmung der Rolle "Autor" durch den Kommunikationsknoten "Corner 1" sicherlich eine sinnvolle und in Ende-zu-Ende-Szenarien anzunehmende Ausgestaltung (Fachverfahren als "Corner 1“ konstruiert und verschlüsselt eine Nachricht und sendet sie anschließend unmittelbar an eine (bzw. seine) Vermittlungsstelle; mit Einführung von XTA zumeist als XTA-Server ausimplementiert und im Sinne des OSCI-Rollenmodells dann als OSCI-Sender agierend).

Abbildung 5.1. OSCI Rollenmodell



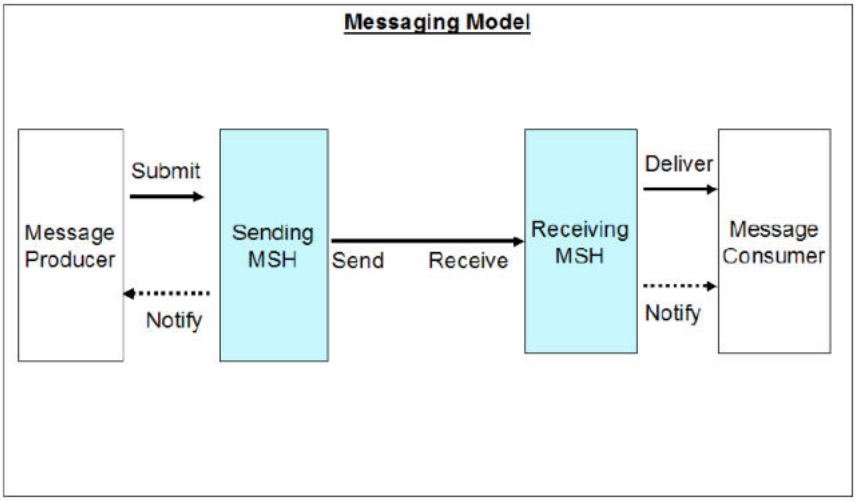
Desweiteren hat sich in der Praxis eingestellt, dass der OSCI-Intermediär in der Verantwortungsdomäne (meist „Datenverarbeitung im Auftrag") des Empfängers betrieben wird, auch wenn die OSCI-Spezifikation eher eine

neutrale, vertrauenswürdige Stelle nahelegt. Der Intermediär nimmt in der Praxis daher eine Stellung ein, wie der Corner 3 bei einer 4-Corner-Topologie, wobei diese Funktion für n Empfänger (logische Mandanten) erbracht wird. Erfolgt die Kommunikation über XTA-angebundene Vermittlungsstellen, wie es in XInneres-Szenarien sehr verbreitet ist (Kommunikation über "Clearingstellen“), so nehmen diese die Funktionalität eines Corner 3 bzw. Corner 2 wahr.

5.2.3. OASIS ebMS3 / AS4

Zwar verwendet ebMS3 (und das stark vereinfachende Profile OASIS AS4) nicht den Begriff „Corner", allerdings definiert das "Messaging Model" von ebMS3 eine Topologie mit vier Komponenten, deren Beziehungen über Ereignisse definiert sind (“ *Submit „, “ Send „, “ Receive „, “ Deliver „*). Die vier Komponenten heißen dort “ *Message Producer „, “ Sending Messaging Service Handler „, “ Receiving Messaging Service Handler „* und “ *Message Consumer*".

Abbildung 5.2. OASIS ebMS Messaging Model



Ob die aufgeführten Ereignisse zwingend mit (zwischen entfernten Knoten verlaufenden) Kommunikationen assoziiert sind, ist zumindest interpretationsfähig. Dei ebMS3-Core-Spec spricht bei allen Komponenten abstrakt von "*entity*". Die Spezifikation enthält Abschnitte, die Interpretationen in beide Richtungen nahelegen:

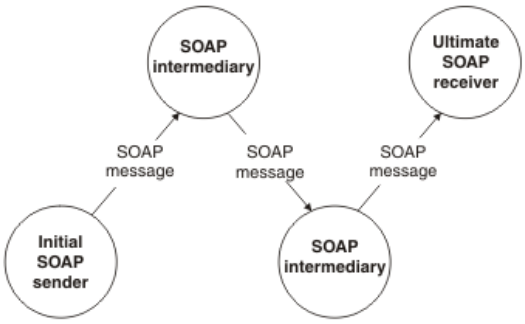
- Im Abschnitt 2.1 „Terminology and Concepts" der ebMS-Core-Spec steht “ *Producer and Consumer are always MSH endpoints*". Demnach handelt es sich bei ebMS3/AS4 nicht um eine 4-Corner-Topologie, weil Producer und Consumer selbst MSH-Knoten sind und daher keine entfernte Kommunikation stattfindet.

- Im Abschnitt 4.1 "*Messaging Service Processing Model*" der ebMS3-Core-Spec wird der *Producer* aber als „Application or SOAP Processor“ bezeichnet, der vor dem Interface des MSH platziert ist. Das legt nahe, dass in Übereinstimmung mit dem (in der Spec. wiederholt referenzierten) *SOAP Processing Model* die Applikation in der Rolle *Producer* selbst initial die SOAP-Nachricht konstruiert, die dann über entfernte Transportwege (Message Queues, http o.a.) an den MSH zur Weiterverarbeitung leitet. In dieser Auslegung entspräche das *ebMS3 Messaging Model* eher einer 4-Corner-Topologie.

Fakt ist aber, dass ebMS3 sowie AS4 lediglich den Nachrichtenaustausch zwischen den MSH spezifizieren. Die Trennung zwischen Producer und MSH bzw. Consumer und MSH bleibt unscharf und ist für die Spezifikation weitgehend irrelevant.

Ergänzend unterstützt ebMS3 und AS4 als Option ein „multi-hop-Szenario", bei dem Nachrichten durch eine beliebige Anzahl von Intermediären sukzessive druchgeleitet werden. Jeder Hop routet zu seinem "next-hop“, bis der empfangende MSH erreicht ist. Das multi-hopping-Szenario ist konform zum SOAP- Processing Model mit seinen Rollen:

Abbildung 5.3. Multi-HOP am Beispiel SOAP



Fazit: Auch wenn die ebMS3-Spezifikation Interpretationen zulässt, scheint es jedoch am wahrscheinlichsten, dass ebMS3/AS4 ein direktes *point-to-point* Kommunikationsmodell zugrunde legt - zumindest wird die Auftrennung in physische Knoten in keiner Weise vorausgesetzt. In diesem Sinne ähnelt das *Messaging Model* eher dem Rollenmodell von OSCI-Transport: Der *Message Producer* entspricht dem OSCI-Autor und der *Message Consumer* dem Leser. Die MSH (Sending und Receiving) entsprechen den Sendern und Empfängern von OSCI-Transport.

Die Trennung zwischen Producer bzw. Consumer und den MSH lässt ebMS3 - ähnlich wie OSCI-Transport (s.o.) - offen.

5.2.4. eDelivery / AS4

Der Begriff "*Four Corner Topology „* ist (zumindest für diesen Kontext) erst durch CEF eDelivery eingeführt worden. eDelivery ist eine erweiternde Profilierung des OASIS AS4-Profils. Die 4-Corner-Toplogie ist eine explizit spezifizierte, optionale Erweiterung von OASIS AS4. Hier werden die vier Corner als “ *parties „* bezeichnet, siehe Abbildung 4.2. Der Corner 1 wird als “ *original sender party „* und der Corner 4 als “ *final recipient party „* bezeichnet - sie werden also explizit als entfernte Kommunikationsknoten verstanden. CEF eDelivery definiert in diesem Zusammenhang die Intermediärsknoten "Access Point“, die stellvertretend für Corner 1 und 4 senden bzw. empfangen. Die Access Points sind als geteilt nutzbare IT-Infrastrukturen im Sinne eines Mandantenprinzips vorgesehen, die komplexe und kritische Mehrwertdienste realisieren (z.B. Routing, Reliable Messaging, Two-Way-Correlation).

Kein Multi-Hop in eDelivery

Die Spezifikation von eDelivery sieht (überraschenderweise) für die Architektur der 4-Corner-Topologie und für die „Access Points" nicht das multi-hop-Feature von ebMS3 vor (siehe CEF eDelivery AS4 1.15: Abschnitt 1.5.1.4 “ *Relation to SOAP and ebMS3 intermediary concepts*"). Es wäre sicher möglich gewesen, Corner 1 und 4 als MSH auszuprägen und die Access Points als ebMS3-Intermediaries analog dem SOAP Processing Model zu platzieren (*Anmerkung*: Die „OSCI-Gateways“ von OSCI 2.0 waren als Intermediäre gemäß SOAP Processing Model vorgesehen).

Stattdessen sind die Kommunikationsstrecken sowie die Schnittstellen C1/C2 und C3/C4 out-of-scope bei eDelivery.

Die einzige konkrete Erweiterung von eDelivery hinsichtlich 4-Corner sind die Definitionen der Property-Namen „originalSender" und "finalRecipient", die als Message-Properties verbindlich bei 4-Corner-Szenarien anzufügen sind. Als Property-Werte sind IDs ("PartyId", z.B. die "Leitweg-ID“ be eRechnung) für die Corner 1 und 4 einzutragen. Eine eDelivery-AS4-Nachricht innerhalb eines 4-Corner-Szenarios enthält also vier PartyIds:

- `env:Envelope/env:Header/eb:Messaging/eb:UserMessage/eb:PartyInfo/eb:From/eb:PartyId`

- `env:Envelope/env:Header/eb:Messaging/eb:UserMessage/eb:PartyInfo/eb:To/eb:PartyId`
- `env:Envelope/env:Header/eb:Messaging/eb:UserMessage/eb:MessageProperties/eb:Property/[@name=„originalSender“]`
- `env:Envelope/env:Header/eb:Messaging/eb:UserMessage/eb:MessageProperties/eb:Property/[@name=„finalReceiver“]`

Darüber hinaus sind Konventionen formuliert, wie der "*Standard Business Document Header*" (SBDH) bei 4-Corner-Szenarien zu befüllen ist.

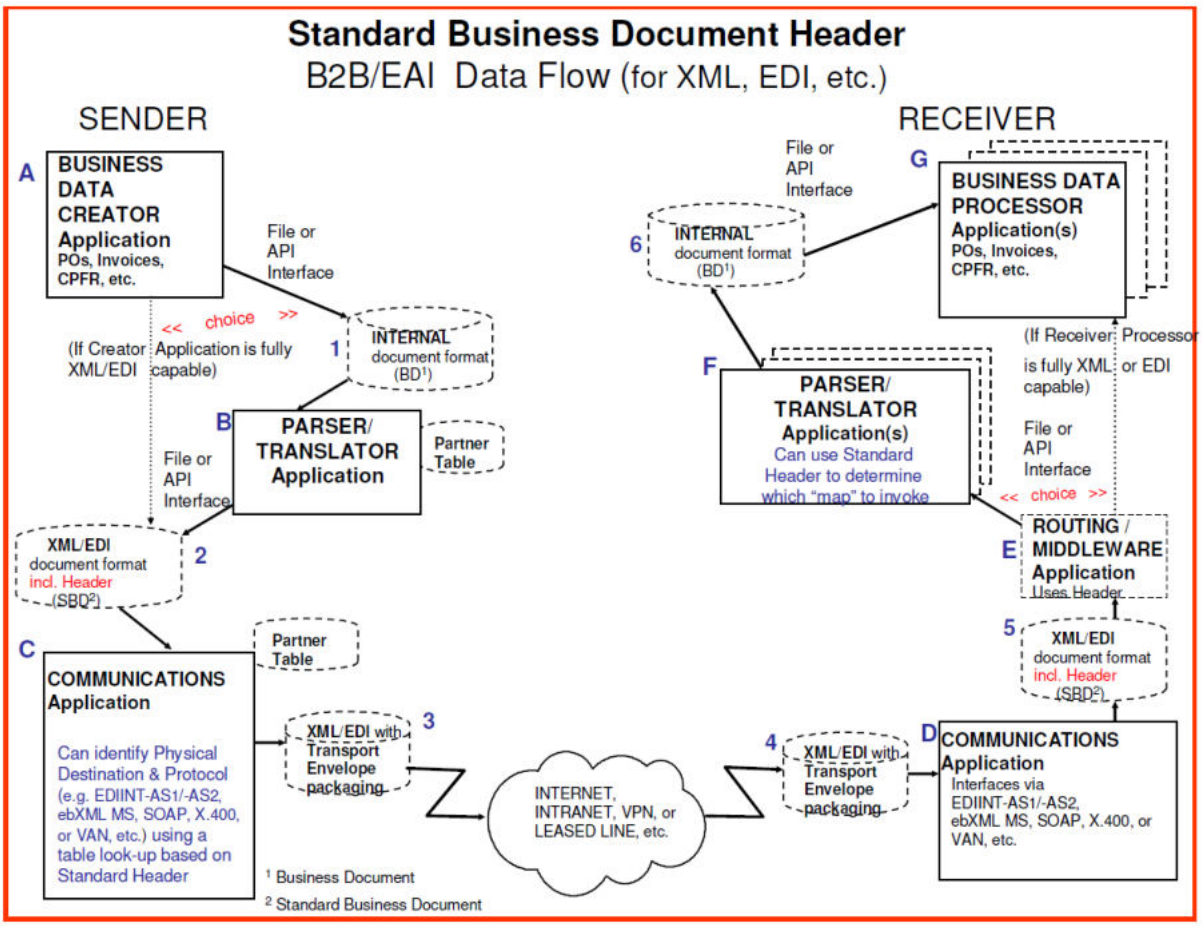
5.2.5. Standard Business Document Header

Eine der Erweiterungen des eDeilvery-Profils ist die optionale Verwendung der Metadatenstruktur UN/CEFACT *Standard Business Document Header* (SBDH). Die aktuellen Entwürfe der SDG-Gremien sehen SBDH derzeit *nicht* vor, gleichwohl ist im Erprobungsvorhaben über eine mögliche Erweiterung in diese Richtung diskutiert worden.

Der Bezug von SBDH zur 4-Corner-Topologie ensteht aus zwei Gründen:

- eDelivery profiliert die Wertebelegung der SBDH-Struktur auch explizit bei Verwendung in einem 4-Corner-Szenario (Abschnitt 1.5.2.6 "*Using the SBDH in a Four Corner Topology*").
- Die Spezifikation zu SBDH selbst beschreibt ein Prozessmodell, das einem 4-Corner-Modell entspricht (siehe Diagramm, Komponenten A, C, D und G).

Abbildung 5.4. Standard Business Document Header



Interessant in dem SBDH-Modell ist, dass es alternative Wege skizziert, wie der Header an die vermittelnde Komponente C übermittelt wird und welche Instanz ihn konstruiert und befüllt. Ein Weg ist, dass eine Komponente (B) im Zuge des Dokument-Mappings (unter Zuhilfenahme einer Partner-Tabelle für Routinginformationen) den Header konstruiert. Dieser Ansatz korrespondiert gut mit den Vermittlungsstellen aus dem RegMoG.

Die SBDH-Spec. definiert zwei alternative Formen der Paketierung:

- integrated packaging: Der XML-SBDH-Header ist direkt eingebunden in das XML-Businessdocument.
- non-integrated packaging: Der XML-SBDH-Header wird als separater Nachrichtenteil transportiert, z.B. innerhalb eines eigenen MIME-Parts.

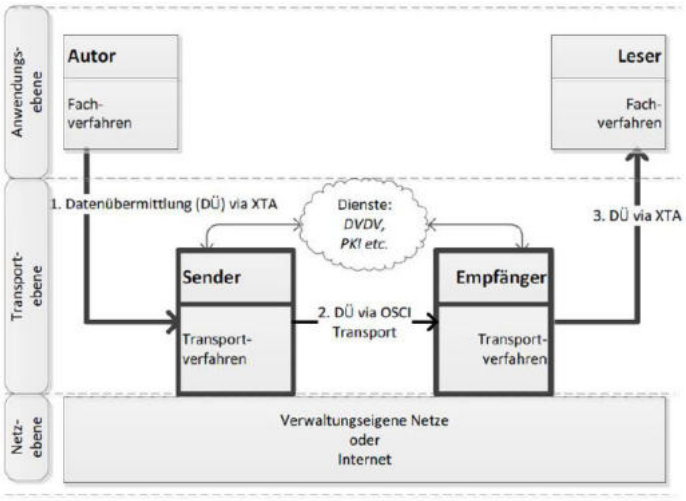
Auch eDelivery greift die beiden Paketierungen auf und gestattet sie als Alternativen. Der Transport als separaten Nachrichtenteil ermöglicht eine differenzierte Verschlüsselung, so dass eine empfangende Vermittlungsstelle zwar Zugriff auf die Header-Informationen erhält, um die Inhaltsdaten an den „finalReceiver“ zu routen, ohne aber die Inhaltsdaten einsehen zu können. Je nach Trasportprotokoll zwischen Corner2/3 wäre dies unterschiedlich umzusetzen. Bei OSCI-Transport könnte ein zweiter, (auf Inhaltsdatebnebene) unverschlüsselter ContentContainer gepackt werden, der nur von dem OSCI-Empfänger lesbar wäre.

5.2.6. XTA

Die XTA-Spezifikation greift das Rollenmodell von OSCI-Transport auf und bringt es in direkte Verbindung mit einer 4-Corner-Topologie. In dem XTA-Modell werden die Rollen Autor, Leser, Sender und Empfänger, wie sie OSCI-Transport definiert hat, abgebildet auf Kommunikationsknoten. Auch werden die Sender- und Empfängerknoten als geteilt nutzbare Transportinfrastrukturen verstanden - analog zu den Access Points von eDelivery. Im Unterschied zu eDelivery berücksichtigt das XTA-Modell aber ausdrücklich eine Ende-zu-Ende-Sicherheit (E2E), wie die Rollen Autor und Leser nahelegen. E2E hat eDelivery nicht im Blick, was sich u.a. in den Metadaten von SMP-v1.0 ausdrückt.

XTA spezifiziert konkret generische Schnittstellen zwischen den Fachverfahren und der Transportinfrastruktur. Es spezifiziert daher genau das, was ebMS3 und eDelivery ausgeklammert haben.

Abbildung 5.5. Der Standard XTA 2 des IT-Planungsrats



Optimierungspotenzial im Zusammenspiel XTA und OSCI

Auch wenn die Rollenbezeichner bei XTA und OSCI-Transport eine sehr homogene, nahtlose Integration beider Spezifikationen vermuten lassen, wurden im Erprobungsprojekt Optimierungspotenziale festgestellt. Dies galt insbesondere für den Umstand, dass XTA die möglichen Signatur- und Verschlüsselungs-Container offen lässt, während diese bei OSCI-Transport integraler Bestandteil der Spezifikation und auch der Nachrichten sind (*osci:ContentContainer*).

Das hat zur Folge, dass ein XTA-und OSCI-Transport-basiertes E2E-Szenario im Erprobungsprojekt nicht mit den inhärenten Mitteln von OSCI-Transport abgebildet werden konnte. Dies kann auch dadurch begründet sein, dass die OSCI-Bibliothek Serialisierung, Deserialisierung und (zeitlich und räumlich getrennte) Integration eines ContentContainers in eine OSCI-Transportnachricht unterstützt hat (inkl. dem Kopieren/Verschieben der Signatur-/Verschlüsselungszertifikate in den *env:Body* des Nachrichtenumschlags).

Ansatz für Fortentwicklung:

Der KoSIT wurden daher folgende Überlegungen zur Fortentwicklung der Standards vorgeschlagen:

- Das Programmiermodell und die API der OSCI-Bibliothek wird dahingehend erweitert, dass signierte und/oder verschlüsselte ContentContainer (bzw. deren EncyptedData-Repräsentanten) als XML-Dokumente serilaisiert werden können, um sie in dieser Form vom XTA-Autor zum XTA-Sender bzw. vom XTA-Empfänger zum XTA-Leser zu transferieren. Desweiteren unterstützt die OSCI-Bibliothek auch die Deserialisierung der ContentContainer, um sie anschließend in ein konstruiertes OSCI-Message-Objekt einfügen zu können.

- XTA wird so erweitert, dass es serialisierte `osci:ContentContainer` in `xta:GenericContentContainer` verpacken kann (als alternatives Container-Format zu XML-Signature und XML-Encryption). Ideal wäre eine XTA-Bibliothek, die transparent die OSCI-Bibliothek zum Zwecke der Serialisierung/Deserialisierung von osci:ContentContainern einbindet. Der Anwendungsentwickler, der mit der XTA-Bibliothek die Nachrichtenkonstruktion und Versand programmiert, müsste lediglich als Parameter das beabsichtigte Corner2/3-Transportprotokoll angeben (z.B. OSCI-1.2 oder eDelivery-AS4). Der Programmierer müsste zwar das Wissen über das Transportprotokoll besitzen, das Programmiermodell wäre aber identisch. Das Wissen über das Protokoll ist in der Praxis eh vorhanden, alternativ könnte auch ein DVDV-Verzeichnisabfrage die Information liefern. Sofern als Corner2/3-Protokoll z.B. eDelivery gewählt wird, wird statt eines `osci:ContentContainer` eine XML-Signature (attached) als Containerstruktur verwendet.

5.3. Abstrakte Berechtigungsprüfung

Es wird ein Mechanismus gesucht, um die Prüfung der Berechtigung zum Nachweisabruf entsprechend § 7 Abs. 2 IdNrG konfigurierbar und nachvollziehbar zu gestalten.

Der etablierte Mechanismus in XÖV und DVDV für die Prüfung der Berechtigung von C1 durch C3 ist seit 2007 die DVDV-Funktionalität *verifyCategory*. Die Regelungen sind hart kodiert (gemäß Festlegungen im Fachstandard) in der Fachlogik, die der C3-Knotens ausführt.

Die Planung in TOOP war ursprünglich, für diese Funktionalität einen Verzeichnisdienst einzusetzen (Repository of Authorities - RoA) zu verwenden und „verify Data Consumer“ durch C4 aufrufen zu lassen. Die SDG Gremien haben sich letztendlich aus Gründen der Komplexität dagegen entschieden.

Ein allgemeingültiger Mechanismus (Policy basiert) wird beschrieben und vorgeschlagen (siehe Seite Berechtigungsprüfung), der gleichzeit flexibler ist. Er basiert auf hinterlegten Regeln (Policy based). Die Knoten C3 und C4 könnten diese Regeln als verlässliche Entscheidungsinstanz nutzen.

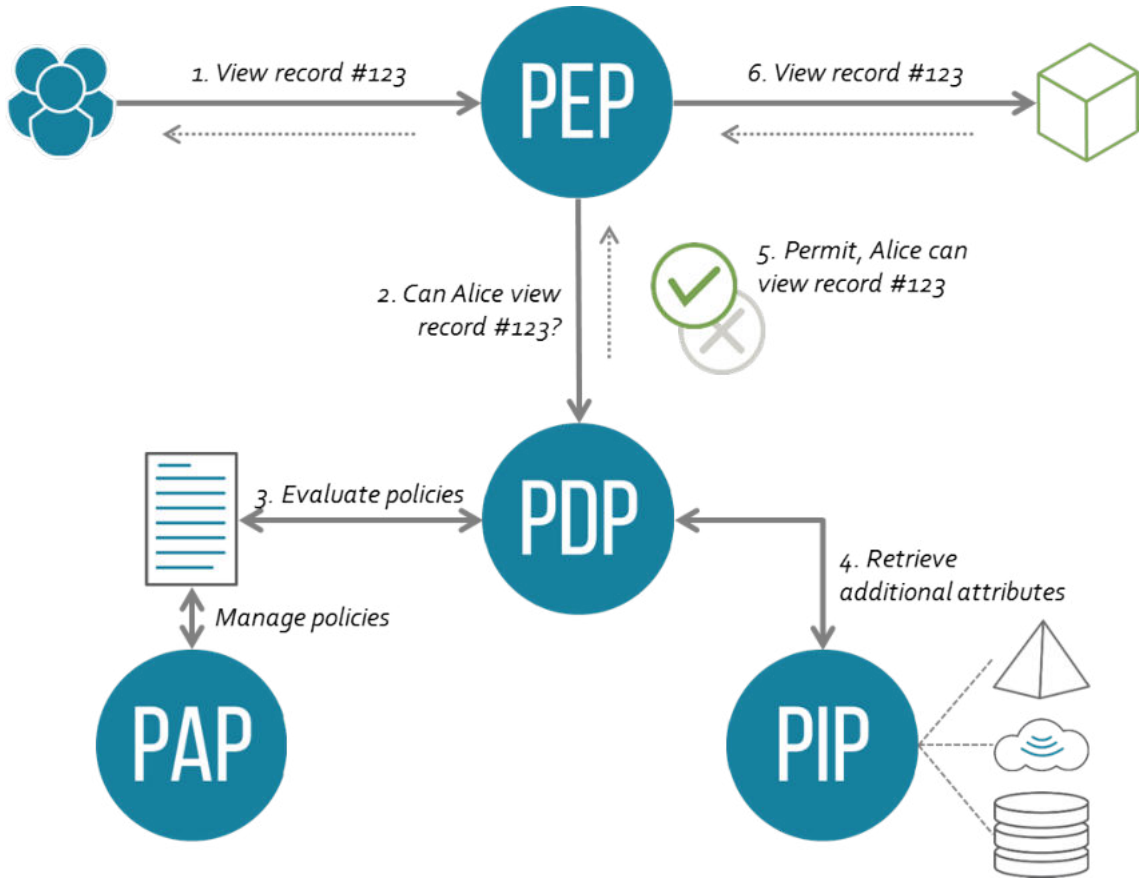
5.3.1. Abstraktes Modell für Berechtigungsprüfung

Als ein mögliches Muster für die Berechtigungssteuerungen von Nachweisabrufen sollen hier kurz die Grundzüge des "*Attrbite based Access Management*" (ABAC) und der konkreten, zugehörigen Referenzarchitektur XACML skizziert werden. Es soll zunächst nur als möglicher Ideengeber für eigene Überlegungen dienen, aber auch eine enge Orientierung bis hin zu den spezifizierten Schnittstellen wären denkbar. Eine kurze Einführung zu XACML ist z.B. hier beschrieben.

5.3.2. Grundprinzipien

Nach ABAC erfolgen Autorisierungsentscheidungen (*Policy Decision*) auf Basis von Regelsätzen (Policies). Für eine Entscheidung können mehere Policies herangezogen werden und eine Policy kann mehrere Regeln enthalten. Welche Polcies und welche Regeln für eine Entscheidung relevant sind, ist im XACML-Konzept spezifiziert (Bestimmung der *Targets*) und ist relativ komplex. Auch wird definiert, welche Vorrangregel greift, wenn z.B. mehrere Policies relevant sind, aber unterschiedliche Entscheidungsergebnisse liefern.

Abbildung 5.6. XACML-Referenzarchitektur (Quelle: Wikipedia)



Eine Policy bzw. dessen Regeln stützen sich allgemein ausschließlich auf Attribute, d.h. logische Ausdrücke werten das Vorhandesein oder Nicht-Vorhandensein von Attributen oder die Werte von Attributen aus. Bei XACML werden Attribute vier Kategorien zugeordnet:

- **Subject** Hierzu zählen Attribute, die den Zugreifenden beschreiben. Das kann z.B. eine ID, eine Rolle, eine Gruppenzugehörigkeit, das Alter oder die zugehörige Organisation sein. Beliebig viele Attribute zum Subjekt können in Policies referenziert werden. Hinweis: In XACML 3.0 kann das Subject noch weiter klassifiziert werden in *access-subject, intermediary-subject, recipient-subject* und *requesting-machine,* was im OOP-Kontext sinnvoll sein könnte.

- **Resource** Attribute zum Objekt, auf das zugegriffen werden soll, meist eine ID, aber auch andere beschreibende Attribute sind natürlich möglich.

- **Action** Attribute beschreiben die Aktion bzw. Operation des Zugriffs (z.B. „read", "write", "delete“).

- **Environment** Diese Attribute beschreiben den allgemeinen Kontext, z.B. Uhrzeit, Wochentag oder das Netzwerk, aus dem der Zugriff erfolgt.

Trennung von Durchsetzung und Entscheidung

Nach der Referenzarchitektur wird die Durchsetzung der Berechtigung und die Entscheidung durch unterschiedliche Instanzen verantwortet. Die Durchsetzung erfolgt durch den *Policy Enforcement Point* (PEP), quasi ein Türsteher unmittelbar vor der Resource, der Zugriffe bei nicht vorhandener Berechtigung verhindert.

Die Entscheidung zur Berechtigung erfragt der PEP beim meist zentralen *Policy Decision Point* (PDP), der die relevanten Policies ermittelt, die Attribute beschafft und die Auswerung aller Regeln durchführt.

Beschaffung der erforderlichen Attribute

Die Attribute samt ihrer Werte, die die Entscheidungsmaschine (*Policy Decision Point*) für die Auswertung der Regeln benötigt, können entweder bereits in der Autorisierungsanfrage (*Policy Request*) enthalten sein oder aus anderen Quellen (Datenbanken, Verzeichnisse) herangezogen werden. Ist ein notwendiges Attribut nicht zu beschaffen, ist die Entscheidung des PDP nicht bestimmbar. Für die Beschaffung der Attribute vor der Auswertung der Policy ist der *Policy Information Point* (PIP) zuständig.

Auf die Attributwerte können in den Regeln verschiedene Funktionen angewendet werden. Es gibt bei XACML eine große Anzahl von Standardfuktionen (lexikalische, arithmetische). Es kann aber um spezielle Funktionen erweitert werden, z.B. um einen Consent-Token zu validieren.

Vertrauenswürdigkeit der Attribute

Die Berechtigungsentscheidungen sind so verlässlich und vertrauenswürdig wie die zugrunde gelegten Attribute. Daher ist entscheidend, wie die Attribute bezogen worden sind - das schließt den gesamten Prozess der Attributbereitstellung mit ein (z.B. den Prozess bei der Verzeichnispflege inkl. Authentisierung und Autorisierung der Datenpfleger, die Manipulationssicherheit der Vezeichnisse uvm.).

5.3.3. Bezug zu den Kontexten RegMoG und OOP

Die Policies und deren Regeln könnten formale Repräsentanten der gesetzlichen Bestimmungen sein. Die Form der Strukturierung (verteilt auf mehrere Policies, PolicySets oder eher gebündelt zu mehrere Regeln in einer oder wenigen Policies) wäre im Einzelfall zu bestimmen. Übergreifende Bestimmungen würden vermutlich in separate Policies verlagert werden.

Ein wichtiger Teil der Policies wäre die Festlegung der Target-Bedingungen, mit denen definiert wird, unter welchen Umständen (z.B. für welche Ressourcen, welche Subjekte usw.) eine Policy oder eine Regel greifen soll.

Ansätze für Attributausprägungen im RegMoG-Kontext

Es wäre eine Modellierung und Festlegung von Attributsätzen vorzunehmen, d.h. die Menge der Attribute, auf die sich Policies stützen können, muss bekannt sein. Gleichzeitig müsste bestimmt werden, in welcher Weise die Attribute vertrauenswürdig ermittelt werden können. Stützt sich der PEP (Torwächter, der die Autorisierungsanfrage stellt) ausschließlich auf Parameter aus dem OOP- oder XÖV-Request (d.h. auf eine Selbstauskunft des Anfragers (also *Procedure Portal* oder *Ecplicit Request Service*)? Oder bezieht der PDP alle oder einige der benötigten Attribute selbst aus Verzeichnissen auf Basis von gesicherten Identitäten (Zertifikaten)?

Mögliche Attributtypen sind z.B.:

- **Subject** Für die *Subject*-Kategorie sind diverse Ausgestaltungen denkbar, um eine abstrakte Autorisierungsentscheidung fällen zu können. Relevante Informationen für eine Autorisierung könnten z.B. sein: - Signaturzertifikat der konsumierenden Behörde (insb. im XÖV-Kontext) - Consent-Token des Nutzers im explicit-OOP-Kontext - Typ/Kategorie der anfragenden Behörde - Identität des Access-Points oder der Kopfstelle (ID und/oder Zertifikat) - Typ und Identität des stellvertretend anfragenden Systems (z.B. *Explicit Request Service* oder *Procedure Portal*) - anfregender Mitgliedstaat, um cross-border und inner-border-Szenarien in Regeln unterscheiden zu können Hier wäre eine sinnvolle Modellierung der Subkategorien des Subjects (*access-subject, intermediary-subject, recipient-subject* und *requesting-machine*) vorzunehmen.

- **Resource** Im XÖV-Kontext entspricht eine Ressource einem in DVDV verzeichneten Dienst. Das kanonische XACML-Attribut *resource-id* hätte als Wert die WSDL-URI. Für OOP wäre der *resource-id*-Wert belegt mit der ID für den EvidenceType (*TOOP-DataSetIdentifier*). Bei einer *concept-based*-Query könnte ggf. die Refe-

renzierung der logischen Ressource zusätzlich zum EvidenceType noch um Attribute für die jeweiligen (einschränkeden) Konzepte ergänzt werden.

- **Action** Im OOP-Kontext könnte mit Attributen der Kategorie *Action* z.B. die *Public Procedure* referenziert werden. Im XÖV/DVDV-Kontext wären *Action*-Attribute vermutlich nicht erforderlich. Ggf. könnte für übergreifende Dienste (z.B. *return-to-sender*) noch der Scope-Dienst attributiert werden. Auch ob es sich um einen *explicit* oder *non-explicit* Request handelt, könnte hier kodiert werden.

- **Environment** Denkbar wäre, dass das Netz, aus dem der Request erfolgt (z.B. Verbindungsnetz oder Internet), in Regeln berücksichtigt werden kann.

Eine Umsetzung der einfachen XMeld-Richtlinie, dass nur Meldebehörden bestimmte XMeld-Dienste konsumieren dürfen, wäre einfach umzusetzen:

1. In den XACML-Policy-Request würde der PEP (als Bestandteil der XMeld-Dienstimplementierung) das OSCI-Inhaltssignaturzertifikat des Anfragers als Subject-Attribut legen. Weiteres Attribut im Request ist die WSDL-URI als Wert der Resource-Attributs *resource-id*.

2. Die Policy bezieht sich auf eine oder mehere WDL-URIs (ResourceTarget-Bedingung).

3. Die einzige Regel lautet, wenn die Behördenkategorie (Subject-Attribut) den Wert „Meldebehörde" hat, dann ist das Ergebnis "Permit", sonst "Deny“.

4. Der *Policy Information Point* weiß, dass das Attribut für die Behördenkategorie aus dem DVDV auf Basis des Signaturzertifikats zu beziehen ist.

5.4. OSCI-Binding

In diesem Abschnitt wird die Ausgestaltung der Once-Only-Kommunikation via OSCI-Transport im Rahmen der Erprobung beschrieben. Die beabsichtigte Ausgestaltung hinsichtlich OSCI-Profil kann durch folgende Festlegungen skizziert werden:

- **Sychrones Request/Response-Muster** Nachweisanfrage (TOOP-Request) und Nachweis (TOOP-Response) werden als synchroner OSCI-Dialog ("*Request-Response, passiver Empfänger, Protokollierung*") abgewickelt. Der TOOP-Request wird also als Inhaltsdaten einer MediateDelivery- bzw. ProcessDelivery-Nachricht zum Evidence Provider transportiert. Der Nachweis wird innerhalb eines TOOP-Responses als Inhaltsdaten einer ResponseToProcessDelivery- bzw. ResponseToMediateDelivery-Nachricht zum Evidence Provider über den http-Backchannel synchron zum Requester zurückgesendet.

- **Ende-zu-Ende-Sicherheit** In Übereinstimmung mit dem XMeld-Profil wird Signatur und Verschlüsselung auf OSCI-Transport-Inhaltsdatenebene sowohl für den Request als auch für den Response angewendet. Zusätzlich wird auch die Transportebene jeweils signiert und verschlüsselt. Dagegen wird keine TLS-Security (https) angewendet.

Für die konkrete prototypische Realisierung im Rahmen der Erprobung gilt zumindest für die erste Umsetzungsstufe:

- Die OSCI-Kommunikation wird im Requester (Testclient) und beim Provider (KRZN Meldeportal) direkt auf Basis der OSCI-Bibliothek realisiert, d.h. es findet eine 3-Corner Kommunikation ohne XTA statt.

- Als OSCI-Intermediär wird ein bei Governikus betriebener Testintermediär verwendet.

- Die Weiterleitungs-URI ist eine physische URL auf den Endpunkt im KRZN.

- Es wird kein Verzeichnis (DVDV) genutzt, sondern Zertifikate und URLs sind hart im Requestor und Provider konfiguriert.

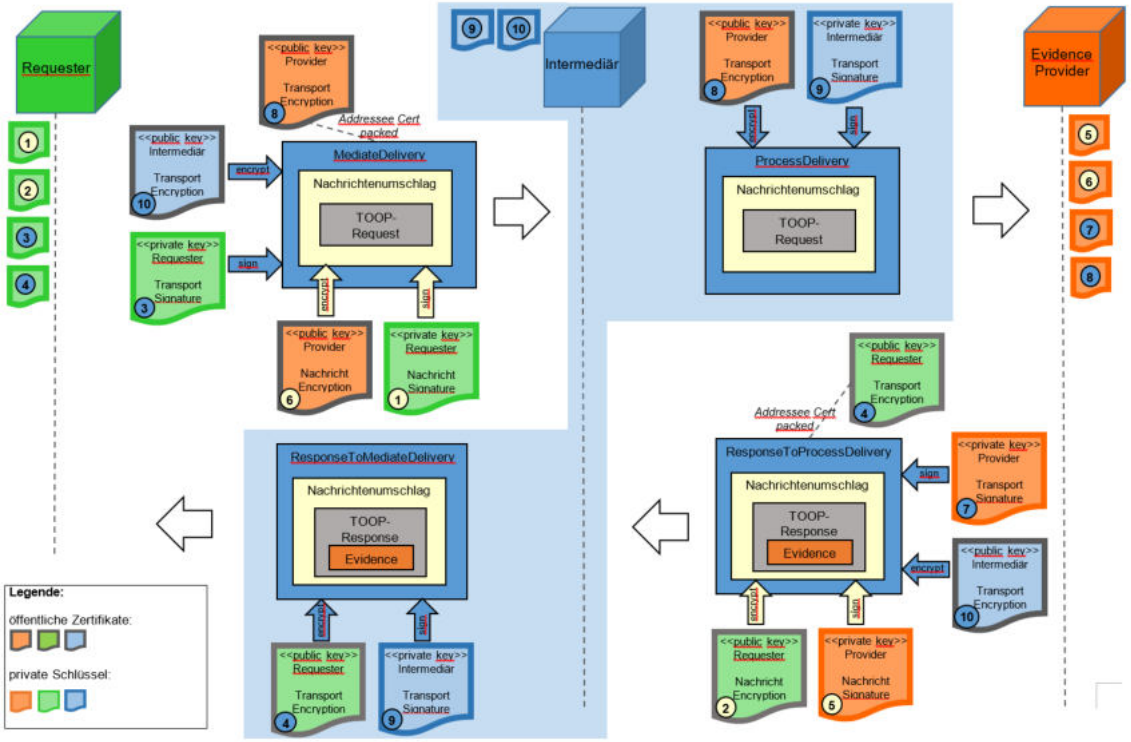
Insgesamt werden in dem Szenario 10 Zertifikate benötigt, wobei zwei Zertifikate fest dem Test-Intermediär zugeordnet sind (für Verschlüsselung zum Intermediär und Signatur der vom Intermediär konstruierten Nachrichten).

Tabelle 5.2. Zordnung von Zertifikaten

Nr.	Owner	Zweck	Angewendet auf Nachrichtentyp	Zertifikatsname (.cer und .pfx)
1	Requester	Signatur des Request-Nachrichtenumschlags	MediateDelivery	RequesterAuthorSigning
2	Requester	Entschlüsselung des Response-Nachrichtenumschlags	ResponseToMediateDelivery	RequesterReaderEncryption
3	Requester	Signatur des Request-Transportumschlags	MediateDelivery	RequesterSenderSigning
4	Requester	Entschlüsselung des Response-Transportumschlags, Adressierung des OSCI-Empfängers (Response)	ResponseToMediateDelivery	RequesterReceiverEncryption
5	Provider	Signatur des Response-Nachrichtenumschlags	ResponseToProcessDelivery	ProviderAuthorSigning
6	Provider	Entschlüsselung des Request-Nachrichtenumschlags	ProcessDelivery	ProviderReaderEncryption
7	Provider	Signatur des Response-Transportumschlags	ResponseToProcessDelivery	ProviderSenderSigning
8	Provider	Entschlüsselung des Request-Transportumschlags, Adressierung des OSCI-Empfängers (Request)	ProcessDelivery	ProviderReceiverEncryption
9	Intermediär	Signatur der Transportumschläge	ProcessDelivery, ResponseToMediateDelivery	-
10	Intermediär	Entschlüsselung der Transportumschläge	ProcessDelivery, ResponseToMediateDelivery	-

Abbildung 5.7 illustriert die Nachrichten und Nachrichtenbestandteile sowie die Verwendung der öffentlichen und privaten Schlüssel. Die an den Zertifikaten und privaten Schlüsseln dargestellten Nummern beziehem sich auf die Tabelleneinträge.

Abbildung 5.7. Zertifikate im PoC



Es werden im Diagramm nur die kryptographischen Operationen im Rahmen der Nachrichtenkonstruktion (Verschlüsselung und Signaturerstellung) dargestellt. Die inversen Operationen bei der Verabeitung der empfangenden Nachricht (insb. Entschlüsselung und Signaturvalidierung der Inhaltsdaten) sind aus Gründen der Übersichtlichkeit nicht dargestellt.

Die Verschlüsselungszertifikate der OSCI-Empfänger (Auftragsverschlüsselung für ProcessDelivery (Request) und ResponseToMediateDelivery (Response)) werden vom Requester bzw. Provider nicht kryptographisch verwendet, sondern der Nachricht beigepackt und so zum Intermediär übertragen. Das erfolgt implizit durch Instanzierung des *Addressee*-Objektes der OSCI-Transport-Bibliothek).

Projekt „Gesamtsteuerung Registermodernisierung“: Bericht zum Umsetzungsstand

März 2022

Inhaltsverzeichnis

Kernbotschaften

Das im Juni 2021 vom IT-Planungsrat (IT-PLR) beschlossene Projekt „Gesamtsteuerung Registermodernisierung“ unter Federführung des Bundes (Bundesministerium des Innern und für Heimat (BMI)) sowie der Länder Baden-Württemberg, Bayern, Hamburg und Nordrhein-Westfalen soll im Rahmen eines übergreifenden Programmmanagements die Realisierung des Zielbilds der Registermodernisierung voranbringen (Beschluss Nr. 2021/25).

2021 wurden in allen Säulen des Zielbilds bereits erste Ergebnisse erzielt sowie grundlegende Voraussetzungen für die weitere Umsetzung in 2022 geschaffen. So wurden im Bereich Architektur und der Weiterentwicklung von Registern erste grundlegende Rahmenbedingungen definiert, die auf eine Validierung des Architekturzielbilds und den Anschluss der Register abzielen. Zudem wurden im Rahmen erster Pilotvorhaben zur Erprobung der Zielarchitektur der Registermodernisierung konkrete Ergebnisse erzielt. Im Bereich Recht wurden erste Arbeitsergebnisse zur Schaffung erforderlicher rechtlicher Rahmenbedingungen für die Realisierung des Zielbilds erarbeitet sowie rechtliche Fragestellungen zur Ausgestaltung der technischen Architektur geklärt. Daneben erfolgte der Aufbau der Steuerungsstrukturen auf Grundlage des vom IT-PLR ebenfalls in der 35. Sitzung mit Beschluss Nr. 2021/25 beschlossenen Konzepts mit Blick auf die Transformationseinheit, den Lenkungskreis, das Projekteboard, die Kompetenzteams (KTs) und die Beiräte. Übergreifend wurden zudem erste Ergebnisse im Bereich Finanzierung, Kommunikation, der Schnittstelle Onlinezugangsgesetz (OZG)/Registermodernisierung sowie dem Aufbau der Registerlandkarte erzielt.

Auf Basis der 2021 erarbeiteten Ergebnisse wurde die Programmplanung bis 2025 von den Federführenden anhand konkreter Programmmeilensteine entlang der vier Säulen sowie der übergreifenden Querschnittsthemen erarbeitet und konkretisiert. Hier ergeben sich konkrete Zielstellungen für das Jahr 2022, die durch die verantwortlichen Federführenden und KTs im Rahmen einer operativen Umsetzungsplanung für 2022 detailliert wurden.

Die mit dem Aufbau und Betrieb des Projekts „Gesamtsteuerung Registermodernisierung“ verbundenen Aufwände werden für die Jahre 2021 und 2022 auf Beschluss des IT-PLR (Nr. 2021/35) aus dem Digitalisierungsbudget finanziert. Ein durch die Federführenden gestellter Antrag wurde genehmigt. Da das bestehende Digitalisierungsbudget Ende 2022 ausläuft, steht nach derzeitigem Stand für die Zeit danach kein Bund-Länder-Budget für Digitalisierungsvorhaben zur Verfügung. Als Bund-Länder-Projekt des IT-PLR werden die Federführenden gemeinsam mit der Föderalen IT-Kooperation (FITKO) im nächsten Schritt einen geeigneten Umsetzungsvorschlag zur Finanzierung für ein Budget zur Programmsteuerung ab dem Jahr 2023 ausarbeiten.

Zudem sind die Gesamtaufwände für die Umsetzung der Registermodernisierung zu evaluieren. Der im Frühjahr 2021 entwickelte Entwurf eines Aufwandsschätzmodells (ASM) zur Schätzung der Aufwände von Bund und Ländern (inklusive Kommunen) zur Erreichung des Zielbilds wurde bundseitig initial validiert. Die länderseitige Validierung dauert derzeit noch an.

1. Umsetzungsstand Projekt „Gesamtsteuerung Registermodernisierung“

Das Projekt „Gesamtsteuerung Registermodernisierung“ unter Federführung des BMI sowie der Länder Baden-Württemberg, Bayern, Hamburg und Nordrhein-Westfalen strebt an, die Realisierung des Zielbilds der Registermodernisierung ressort- und ebenenübergreifend konzertiert voranzubringen. Der aktuelle Projektstand wird nachfolgend vorgestellt.

Den Kern des Gesamtprogramms bilden die vier im Zielbild Registermodernisierung beschriebenen Säulen: eine interoperable und sichere technische Architektur, anschlussfähige Register auf Seiten der registerführenden Stellen, rechtliche Rahmenbedingungen für einen sicheren und datenschutzkonformen Datenaustausch sowie eine zukunftsweisende Governance (Kontroll- und Steuerungsstrukturen im laufenden Betrieb). Um ein zielgerichtetes Vorgehen zur Umsetzung des Zielbilds sicherzustellen, wurden die wesentlichen Ziele für 2021 und eine arbeitsteilige Aufgabenwahrnehmung unter den Federführenden bis zum Jahresende definiert.

Abbildung 1: Übergreifende Ergebnisse 2021 entlang der Säulen des Zielbilds der Registermodernisierung (siehe Anhang)

2021 wurden in allen vier Säulen des Zielbilds bereits erste Ergebnisse erzielt sowie grundlegende Voraussetzungen für die weitere Umsetzung in 2022 geschaffen. Neben der inhaltlichen Ausgestaltung der Registermodernisierung entlang der vier Säulen wurden zudem übergreifende Querschnittsthemen wie z.B. Finanzierung/Haushaltsvorsorge sowie Kommunikation und Stakeholdermanagement in den Blick genommen (siehe folgende Unterkapitel).

1.1 Technische Architektur

Die Befassung mit und inhaltliche Ausarbeitung der Säule „Technische Architektur“ findet vorrangig in einem etablierten KT Architektur in enger Zusammenarbeit mit einem

ebenfalls aufgebauten KT EU-Interoperabilität statt. Zwischen den beiden KTs gibt es zudem eine relevante Überschneidung der Mitglieder, was die Zusammenführung der Arbeiten beider KTs signifikant erleichtert.

Bisherige Arbeitsergebnisse

Das KT Architektur[1] hat zunächst typische Prozesse des Abrufs von Nachweisen sowie die Rollen der Komponenten und deren Zusammenspiel in diesen Prozessen untersucht. Zeitgleich wurden Anforderungen abgeleitet sowie kategorisiert und es wurde damit begonnen, diese den Komponenten zuzuordnen. Die Ergebnisse der Analysen sind in ein technisches Modell eingeflossen, dem nun die folgenden Informationen entnommen werden können:

- Funktionen der Komponenten
- Produkte und Lösungen, die zur Umsetzung der Komponenten zum Einsatz kommen können, z.B. Deutsche Verwaltungsdiensteverzeichnis (DVDV)
- Technische Interaktionen der Komponenten untereinander

Die Detailmodellierung wird erst 2022 abgeschlossen werden können. Gleichwohl haben sich bereits jetzt Präzisierungs- und Klarstellungsbedarfe ergeben (z.B. hinsichtlich der notwendigen Komponenten). In Fortschreibung der vereinfachten Darstellung der Zielarchitektur ergibt sich als aktueller Arbeitsstand die folgende Darstellung:

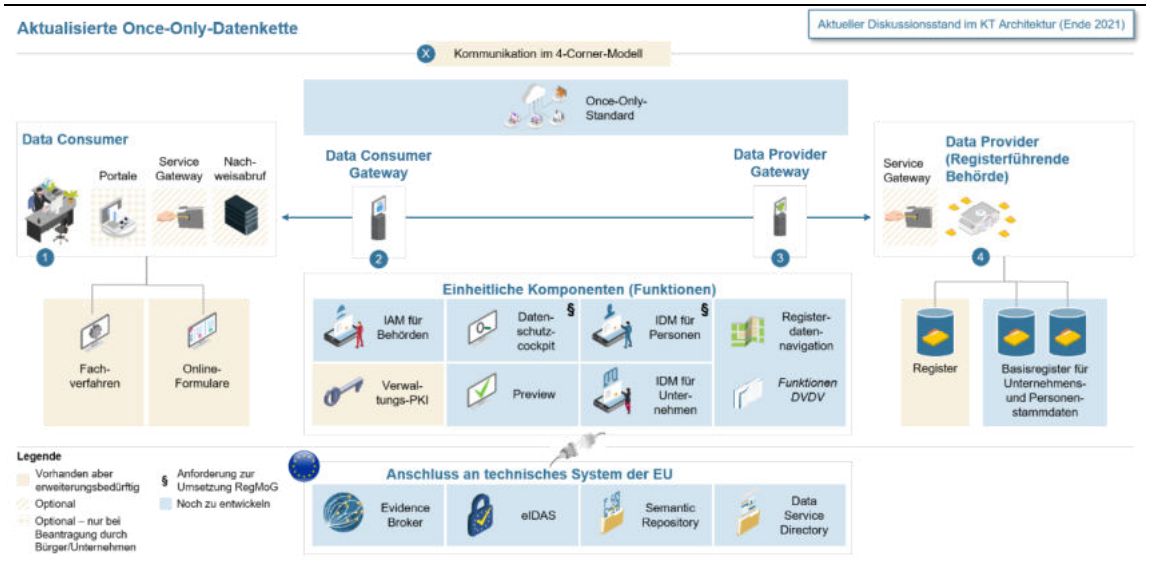


Abbildung 2: Aktualisierte Once-Only-Datenkette nach aktuellem Diskussionsstand im KT Architektur, Ende 2021 (siehe Anhang)

Das Zielbild wurde in folgenden Punkten präzisiert:

[1] Bestehend aus Vertreterinnen und Vertretern des BVA, des Landes Nordrhein-Westfalen, der KoSIT sowie der Dienstleister msg,]init[und McKinsey.

- Die Komponente „übergreifendes Identitätsmanagement“ (IDM) wurde aufgeteilt in die Komponenten „IDM für Personen“, „IDM für Unternehmen“ und „Identity Access Management (IAM) für Behörden“.
- Die Komponente „Anschluss an technisches System der EU“ wurde durch die konkreten technischen Komponenten der EU („Evidence Broker“, „eIDAS“, „Semantic Repository“ und „Data Service Directory (DSD)“) ersetzt, die an das nationale System anzubinden sind.

Hinsichtlich des Gesamtsystems und der einheitlichen Komponenten in der Once-Only-Datenkette haben sich folgende Anpassungen ergeben:

- **Nationales Once-Only-Technical-System (NOOTS):** Das sich derzeit bei der Europäischen Kommission (EU-KOM) in Entwicklung befindliche EU-OOTS nach Art. 14 SDG-Verordnung (VO (EU) 2018/1724) verzögert sich weiter. Es ist derzeit nicht absehbar, wann eine praktische Einsatzreife besteht. Daneben gibt es nationale Anforderungen, die vom EU-OOTS nicht abgedeckt werden können. Dies macht ein NOOTS erforderlich. Die Anschlussfähigkeit an das EU-OOTS erfolgt voraussichtlich über Kopfstellen, die von einem „SDG-Konnektor“ unterstützt werden. Dem IT-PLR wird im Zuge der weiteren Arbeiten ein Beschlussvorschlag zur Umsetzung eines NOOTS vorgelegt werden.
- **Komponente Nachweisabruf:** Die im ursprünglichen Zielbild geführte Komponente Nachweisabruf stellt aus Sicht des KT Architektur keine eigenständige Funktionalität im Sinne des Zielbilds bereit, sondern unterstützt Data Consumers als optionale Komponente bei ihrer Aufgabe im Kontext des Nachweisabrufs.
- **Komponente Registerdatennavigation:** Derzeit wird davon ausgegangen, dass diese Funktion im Rahmen einer Weiterentwicklung des DVDV bereitgestellt wird.
- **Komponente Consent-Modul:** Aufgabe der Komponente war es, die Initiierung des Nachweisabrufs durch die Nutzer und Nutzerinnen zu dokumentieren und für alle Teilnehmenden der Once-Only-Datenkette, insbesondere die Data-Provider, überprüfbar zu machen. Da die Verantwortung für den Nachweisabruf in der Regel allein beim Data Consumer liegt, wird auf Seiten des Data-Providers kein Bedarf mehr für ein Consent-Modul gesehen. Es wird jedoch noch geprüft, ob es Anforderungen aus dem Bereich der IT-Sicherheit gibt, welche die Implementierung einer entsprechenden technischen Lösung gleichwohl erforderlich machen.

Komponenten im Zielbild

Data Consumers sind in der Regel Onlinedienste öffentlicher Stellen, die Antragstellenden die zur Beantragung einer Verwaltungsleistung notwendigen Formulare bereitstellen, diese um Nachweise aus Basisregistern ergänzen und die Formulare zusammen mit den Nachweisen an das zuständige Fachverfahren weiterleiten. Behörden, die Nachweise bzw. Daten

aus Basisregistern abrufen, welche zur Aufgabenwahrnehmung erforderlich sind, sind ebenfalls Data Consumers.

Data-Provider sind registerführende Behörden oder Basisregister, die Nachweise über Antragstellende zur Bearbeitung einer Verwaltungsleistung in einem Fachverfahren ausstellen.

Data Consumer Gateway und **Data Provider Gateway** sind Vermittlungsstellen, die Nachrichten sicher und nachvollziehbar transportieren. Dazu gehört auch die abstrakte Berechtigungsprüfung.

Service Gateways (SGs) sind optionale Produkte, die die Anbindung von Data Consumers und Data-Providern an das NOOTS vereinfachen und beschleunigen können. Sie bündeln Authentifizierung und Autorisierung, Schemavalidierung, Protokollübersetzung oder Datentransformation. Data Consumers und Data-Provider können Anbindungen wahlweise über eigene Schnittstellen/Komponenten oder über SGs umsetzen.

Das **Datenschutzcockpit** (DSC, Art. 2 Registermodernisierungsgesetz (RegMoG)) soll es Bürgerinnen und Bürgern ermöglichen, durchgeführte behördliche Datenübermittlungen unter Nutzung der Identifikationsnummer (IDNr) nach dem Identifikationsnummerngesetz (IDNrG) nachzuvollziehen und die zur Person erfassten Registerdaten einsehen zu können.

Die **Verwaltungs-Public-Key-Infrastructure (V-PKI)** stellt eine zertifikatsbasierte Infrastruktur für elektronische Signatur und Verschlüsselung zum Schutz der Vertraulichkeit, Integrität und Authentizität in der digitalen Kommunikation zur Verfügung.

Das **IAM für Behörden** ermöglicht die technische Authentifizierung von Behörden durch die Prüfung von Zertifikaten sowie die Überprüfung der Gültigkeit durch einen bereitgestellten Onlinedienst der V-PKI.

Das **IDM für Personen** (Art. 1 RegMoG) stellt die IDNr eines Bürgers bzw. einer Bürgerin und weitere Basisdaten zur Person bereit.

Die **Preview**-Komponente ermöglicht Antragstellenden, die für die Erbringung einer Verwaltungsleistung übermittelten Nachweise einzusehen und zu entscheiden, ob der Prozess mit den Nachweisen fortgeführt oder abgebrochen werden soll.

Das **IDM für Unternehmen** stellt die Wirtschaftsidentifikationsnummer (W-IDNr) eines Unternehmens und weitere Basisdaten zum Unternehmen bereit.

Validierung des Zielbilds durch Piloten

Die Erprobung der technischen Architektur ist in 2021 bereits parallel zur Konzeption gestartet, um möglichst Erfahrungen für die weitere Umsetzung des Zielbilds zu sammeln. Durch diese Parallelität ergibt sich für die Piloten inhaltlich und planerisch die Herausforderung, dass zentrale Komponenten des Zielbilds noch nicht verfügbar sind, sondern sich erst in Ausgestaltung befinden. Die Erprobung wird zudem dadurch erschwert, dass der

Durchführungsrechtsakt nach Art. 14 Abs. 9 SDG-VO sowie die zugehörigen technischen Dokumente weit hinter dem Zeitplan liegen und seitens der EU-KOM noch nicht erlassen wurden. Dennoch liegen erste Ergebnisse aus den laufenden Pilotprojekten vor.

In einem ersten Piloten[2] wird die Einspielung der IDNr in das Nationale Waffenregister (NWR) technisch erprobt. Hierbei wurde eine herausfordernde rechtliche Anforderung identifiziert. Das Protokollierungserfordernis für Datenübermittlungen zwischen öffentlichen Stellen (Art. 9 IDNrG) könnte bei sehr enger rechtlicher Auslegung voraussetzen, dass bereits vor der Befüllung mit Echtdaten ein DSC (Art. 2 RegMoG) bereitgestellt wird, da auch dies eine Übermittlung zwischen öffentlichen Stellen darstellen würde. Diesbezüglich erfolgt aktuell eine enge Abstimmung der zeitlichen Planungen zwischen dem DSC und dem Pilotvorhaben, eine abschließende Klärung der rechtlichen Anforderungen sowie eine Evaluation möglicher Alternativoptionen (z.B. Beschränkung auf künstliche Daten). Als Ergebnis liegt ein erstes Konzept zum Abruf von IDNr und deren Einspielung in das NWR vor.

In zwei weiteren Pilotprojekten[3] wurde der Einsatz von SGs als Komponenten zur Anbindung von Registern evaluiert. Im Ergebnis konnte die grundsätzliche Nutzbarkeit für die Register des Bundesverwaltungsamts (BVA) und technisch ähnlich umgesetzte Register durch die Piloten bestätigt werden. Die Frage der Weiterentwicklung der SGs obliegt einer weiterführenden Prüfung, bei der zunächst insbesondere der Bedarf seitens der Register abgeschätzt werden soll.

In einem weiteren Pilotprojekt[4] wird derzeit ein Nachweisabruf aus dem Melderegister beispielhaft implementiert, um das Zusammenspiel europäischer Technologievorgaben mit bestehenden Lösungen bei deutschen Behörden zu erproben. Aufgrund der erwähnten Verzögerung des europäischen Durchführungsrechtsakts (Implementing Act) nach Art. 14 SDG-VO liegen hierzu noch keine abschließenden Erkenntnisse vor. Das Projekt arbeitet aktuell an der Abbildung des SDG-Verfahrens „Confirmation of current address“ auf die entsprechende Anfrage im nationalen IT-Standard XMeld, muss dazu aber vorläufig auf Entwurfsdokumente der EU zurückgreifen. Von besonderem Interesse sind konzeptionelle Unterschiede zwischen dem generischen Abrufstandard des EU-OOTS und dem für das deutsche Meldewesen spezifischen Fachstandard XMeld, sowie die Auswirkungen der unterschiedlichen Transportstandards (AS4 bei SDG, OSCI in Deutschland).

Entlang der für 2022 geplanten Konkretisierung der Architektur ist durch die Gesamtsteuerung der fortlaufende Ausbau dieser oder weiterer Pilotierungsprojekte beabsichtigt, bis hin zur vollständigen Abbildung von digitalen Verwaltungsleistungen nach dem Once-Only-Prinzip.

---

[2] Pilot 1 „Einspeicherung der ID-Nummer in das Nationale Waffenregister“ (Plan: 05.2021 – 04.2023, verantw.: BVA/DII 1).
[3] Pilot 5 „Weiterentwicklung der Service Gateways im Sinne des Zielbilds“ (abgeschlossen, verantw.: BVA/DII 1), Pilot 3 „Nutzung der SGs zur Anbindung des Bundesportals an FaStA-Register“ (Plan: 03.2021 – 05.2022, verantw.: BVA/DII 1).
[4] Pilot 7 „Erprobung Once-Only Architektur für Melderegister mit KRZN“ (Plan: 01.2021 – 03.2022, verantw.: KoSIT).

Vorgehensmodell zur Anbindung an das europäische Once-Only-Technical-System (EU-OOTS)

Beim Vorgehen zur Umsetzung der nationalen Anbindung an das EU-OOTS müssen vier Bereiche abgedeckt werden:

- Anbindung der nationalen **Komponenten** an die zentralen Komponenten des EU-OOTS
- Anbindung der nationalen **Transportinfrastruktur** an die Transportinfrastruktur des EU-OOTS
- Anbindung von nationalen **Onlineservices** an Evidence Provider des EU-OOTS
- Anbindung nationaler **Register** an Evidence Requester des EU-OOTS.

Das KT EU-Interoperabilität koordiniert und steuert die Anbindung der Komponenten und Transportinfrastruktur und unterstützt bei der fachlichen und technischen Anbindung der Onlineservices und Register. Fachliche Vorgabe für die Arbeiten des KT sind die von der EU-KOM veröffentlichen Entwürfe des Durchführungsrechtsakts und der Technical Design Documents. Das KT EU-Interoperabilität hat sich zudem in organisierten Arbeitsgruppen (Working Packages) und bilateralen Formaten mit technischen Experten und Expertinnen der EU-KOM und anderer Mitgliedstaaten ausgetauscht; die Erkenntnisse fließen ebenfalls in die Erstellung des Vorgehensmodells ein.

Die zentralen Komponenten des EU-OOTS umfassen das DSD, den Evidence Broker sowie das Semantic Repository. Wichtige Fragestellungen bleiben hier unter anderem die Nutzung der Wahlrechte im Hybridmodell (Nutzung der zentralen europäischen Dienste oder eigenständige nationale Bereitstellung), die Organisation von Pflegeprozessen und die Ausgestaltung notwendiger Schnittstellen.

Bezüglich der Transportinfrastruktur ist eine Anbindung an die AS4-Kommunikation und eine Transformation in das European Exchange Data Model über Kopfstellen angedacht. Dazu muss ein Konzept erstellt und im Rahmen eines Pilotprojekts verprobt werden.

Hinsichtlich der Anbindung von Onlineservices und Register müssen Verwaltungsverfahren ermittelt werden, die unter den Anwendungsbereich des Art. 14 Abs. 1 SDG-VO fallen. Zusätzlich werden die deutschen Nachweistypen erhoben, welche die Nachweisanforderungen der EU-KOM abdecken. Weiterhin werden die nationalen Register ermittelt, die eine Anbindung an das EU-OOTS benötigen.

Ausblick Technische Architektur 2022

Im Jahr 2022 sollen die folgenden Ziele möglichst frühzeitig erreicht werden:

- Weiterentwicklung bisheriger Arbeiten zu einem durchgängigen Architekturkonzept

- Bestätigung des Architekturkonzepts und des daraus erwachsenden Zielbilds durch den IT-PLR
- Erstellung von Entscheidungsvorschlägen für alle zentralen Once-Only-Datenkettenkomponenten
- Initiierung von Pilotvorhaben unter anderem zur Registerdatennavigation und zum Anschluss des NOOTS an das EU-OOTS
- Initiierung der Umsetzung und Weiterentwicklung von im Architekturkonzept beschriebenen Komponenten.

1.2 Weiterentwicklung von Registern

2021 lag der Fokus auf der Definition des grundsätzlichen Vorgehens zur Weiterentwicklung von Registern im Hinblick auf die Einspielung der IDNr und den Anschluss an die Once-Only-Datenkette sowie die Initiierung von Erprobungsaktivitäten für priorisierte Register. Konkret wurde seitens des BVA damit begonnen, ein Vorgehensmodell für den Rollout der IDNr und der übrigen Basisdaten in die nach dem IDNrG berechtigten registerführenden Stellen zu erstellen. Im Rahmen der in diesem Modell vorgesehenen Anbahnungsphase soll eine initial erstellte Checkliste erprobt werden, mit der eine erste Einschätzung zur Anschlussfähigkeit der Register an das beim BVA zu entwickelnde Identitätsdatenabruf(IDA)-Verfahren getroffen werden soll. Hieraus sollen Erkenntnisse gewonnen werden, um in 2022 einen ersten Rolloutplan, insbesondere für die vom IT-PLR priorisierten Register zu erstellen. Aktuell wird hier bereits die Einspielung der IDNr in das NWR durch das BVA in einem Pilotprojekt erprobt (siehe Kapitel 1.1.1).

2021 wurden zudem konkrete Gespräche mit weiteren registerführenden Stellen aufgenommen, um zusätzliche Pilotvorhaben aus dem Kreis der OZG-nutzungsträchtigen Top-18-Register des Zielbilds anzustoßen. Hierbei liegt der Fokus auf der Erprobung konkreter Once-Only-Anwendungsfälle entlang von priorisierten OZG-Verwaltungsleistungen, um Praxiserfahrungen in Bezug auf die Umsetzbarkeit und das Nutzenversprechen ableiten zu können. Die Spezifizierung dieser geplanten Pilotvorhaben erfolgt aktuell mit den jeweils beteiligten registerführenden Stellen.

Hierbei wird eine Kooperation mit den Umsetzungsprojekten zum Handelsregister und zu einem oder zwei der Top-18-Register des Zielbilds angestrebt. Gleichzeitig sollen erste notwendige Infrastrukturkomponenten im Rahmen der Registermodernisierung pilotiert werden.

1.3 Rechtliche Grundlagen

Im Jahr 2021 konnten erste Arbeitsergebnisse im Bereich rechtlicher Grundlagen gelegt werden, die im Folgenden inhaltlich vertieft werden.

Ergebnisse zur Klärung rechtlicher Fragen zum OOTS gemäß Art. 14 SDG-VO inklusive noch möglicher offener Fragen

Das KT Recht/Datenschutz[5] hat in Abstimmung mit dem KT EU-Interoperabilität die rechtlichen Fragen zum OOTS gemäß Art. 14 SDG-VO priorisiert und die wichtigsten davon beantwortet. Die Prüfergebnisse wurden mit den SDG-Koordinierenden der Länder und den jeweiligen rechtlichen Ansprechpersonen abgestimmt. Die Konsolidierung und Finalisierung der Ergebnisse sowie eine Aktualisierung im Hinblick auf die laufenden Abstimmungen zum Durchführungsrechtsakt gemäß Art. 14 Abs. 9 SDG-VO werden zeitnah erfolgen.

Das KT Recht/Datenschutz hat die Klärung von rechtlichen Fragen zum NOOTS an der Schnittstelle zum EU-OOTS gemeinsam mit dem KT EU-Interoperabilität sowie dem KT Architektur aufgenommen und hierfür einen Zusammenarbeitsmodus etabliert.

In Umsetzung der rechtlichen Prüfungsergebnisse hat das KT Recht/Datenschutz eine Änderung des Art. 27 des geplanten Durchführungsrechtsakts bei der EU-KOM angeregt. Die ursprüngliche Fassung des Durchführungsrechtsakts und die SDG-VO sahen keine spezifische Regelung zur Verteilung der datenschutzrechtlichen Verantwortlichkeit zwischen der datenübermittelnden Stelle (Evidence Provider) und der datenabrufenden Stelle (Evidence Requester) bei Nutzung des EU-OOTS vor. Angesichts der geplanten technischen Architektur wird eine solche Regelung auf Grundlage von Art. 4 Nr. 7 DSGVO für angemessen gehalten. Nach der durch die EU-KOM vorgelegten, geänderten Entwurfsfassung ist nun allein die datenabrufende Stelle für die Rechtmäßigkeit der Datenübermittlungen durch das EU-OOTS verantwortlich. Diese Regelung soll Rechtsunsicherheit vorbeugen und dadurch das Vertrauen der Bürgerinnen und Bürger in die Nutzung des OOTS stärken. Ergänzt wurde zudem eine Regelung zur Einführung von Stichprobenverfahren. Der Durchführungsrechtsakt befindet sich noch in der Abstimmung zwischen der EU-KOM und den Mitgliedstaaten, sodass noch nicht sicher ist, ob er insgesamt oder in Bezug auf Art. 27 in dieser Ausgestaltung beschlossen wird. Das KT Recht/Datenschutz begleitet den weiteren Abstimmungsprozess.

Ergebnisse aus rechtlicher Begleitung des Piloten im Melderecht

Das KT Recht/Datenschutz hat dabei unterstützt, Rechtsfragen, die sich im Zusammenhang mit dem Piloten im Melderecht gestellt haben, zu beantworten. Zudem hat das KT Recht/Datenschutz bei der AG BMG am 24. September 2021 sowie bei der UAG Recht der Melderechtsreferenten am 30. November 2021 jeweils einen Impulsvortrag zu Art. 14 SDG-

[5] Bestehend aus Vertreterinnen und Vertretern des BMI sowie der Länder Bayern, Nordrhein-Westfalen, Baden-Württemberg und Hamburg.

VO und dem geplanten EU-OOTS gehalten. Ziel war es, den Fachverantwortlichen eine Hilfestellung für die fachseitige Analyse von etwaigen Rechtsänderungsbedarfen im Melderecht im Hinblick auf Art. 14 SDG-VO an die Hand zu geben. Die sich dort ergebenden Rückfragen wurden für die weitere Arbeit im KT Recht/Datenschutz aufgenommen.

Status und Ergebnisse der Initiierung Screening Rechtsänderungsbedarfe ressort- und länderübergreifend (EU-weit)

Das KT Recht/Datenschutz hat einen Leitfaden zur Auslegung von Art. 14 SDG-VO und zur Ermittlung sich daraus ergebender Rechtsänderungsbedarfe zur grenzüberschreitenden Umsetzung des Once-Only-Prinzips entwickelt, inklusive der Prüfung einer möglichen Once-Only-Generalklausel. Der Leitfaden dient der einheitlichen Auslegung des Art. 14 SDG-VO, insbesondere des Anwendungsbereichs nach Art. 14 Abs. 2 SDG-VO, sowie der Unterstützung der Fachverantwortlichen bei der Analyse etwaiger Rechtsänderungsbedarfe und deren Umsetzung. Der Leitfaden befindet sich derzeit in der internen Qualitätssicherung im KT Recht/Datenschutz und wird vor dem Hintergrund der geplanten Änderung des Art. 27 des Durchführungsrechtsakts und der Überlegungen zu einer Once-Only-Generalklausel erneut angepasst. Zur Evaluierung der Inhalte einer solchen Once-Only-Generalklausel hat das KT Recht/Datenschutz Interviews mit Expertinnen und Experten aus Wissenschaft und Forschung, aus Österreich zwecks eines Rechtsvergleichs sowie mit Experten und Expertinnen aus den Teilprojekten der Registermodernisierung geführt.

1.4 Governance

Die Steuerungsstrukturen auf der Grundlage des vom IT-PLR in der 35. Sitzung beschlossenen Projekts „Gesamtsteuerung Registermodernisierung“ sind im Wesentlichen aufgebaut und haben ihre Arbeit aufgenommen. In der Transformationseinheit wurde zwischen den Federführenden ein kontinuierlicher Arbeitsmodus in den einzelnen Aufgabenfeldern sowie eine übergreifende Zusammenarbeit etabliert. Der Lenkungskreis hat sich am 13. Oktober 2021 konstituiert und tagt nunmehr mindestens vierteljährlich. Die Besetzung des Registerbeirats sowie des Wissenschafts- und Innovationsbeirats wurde initiiert, ein aktueller Stand wird dem Lenkungskreis in seiner nächsten Sitzung zur Kenntnis gebracht. Nach erfolgter Benennung der Mitglieder nehmen die Beiräte im nächsten Schritt ihre Arbeit auf.

Die KTs Architektur, EU-Interoperabilität und Recht/Datenschutz haben ihre inhaltliche Arbeit aufgenommen und sind in einen kontinuierlichen Arbeitsmodus übergegangen. Das KT Register wird Anfang 2022 aufgebaut und in Q1 2022 seine Arbeit aufnehmen (siehe Kapitel 2, Umsetzungsplanung 2022).

Aktuelle Teilprojekte im Hinblick auf die Umsetzung des Zielbilds der Registermodernisierung sowie assoziierte Vorhaben wurden identifiziert. Eine Abfrage in allen Bundesländern

nach entsprechenden Projekten hat ergeben, dass dort derzeit noch keine Vorhaben mit direktem Bezug zur Umsetzung des Zielbilds Registermodernisierung laufen oder in Planung sind. Der Lenkungskreis hat mit Beschluss vom 13. Oktober 2021 die im Anhang (siehe Anhang, Abbildung 7) aufgeführten Teilprojekte in das Projekt Registermodernisierung integriert sowie assoziierte Vorhaben bestätigt. Das Projekteboard, das unter anderem dem Informationsaustausch der Teilprojekte und assoziierten Vorhaben untereinander dient, fand erstmalig am 27. und 28. September 2021 statt und tritt seitdem monatlich zusammen. Die KTs informieren hier über ihre Arbeitsergebnisse, während einzelne Teilprojekte jeweils den Stand ihres Projekts vorstellen.

Für die Teilprojekte wurde mit fachlicher Unterstützung des BVA ein Controlling eingeführt. In erster Linie erfolgt das Controlling im Hinblick auf die Einhaltung der zeitlichen Vorgaben anhand projektspezifischer Meilensteine. Der erste Controllingbericht erfolgte im Februar 2022. In diesem Rahmen ist auch ein übergreifendes Programmcontrolling hinsichtlich der Ziele und Meilensteine zur Umsetzung des Zielbilds Registermodernisierung eingerichtet worden.

1.5 Querschnittsthemen

Identifizierung der von Art. 14 SDG-VO betroffenen Fachverantwortlichen mittels eines Evidence Survey

Der Evidence Survey ist eine zentrale Erhebung durch die EU-KOM, die durch innerstaatliche Vorarbeiten vorbereitet wird. Ziel des Evidence Survey ist die Identifikation von Nachweisen für den automatisierten grenzüberschreitenden Austausch zu SDG-relevanten Verfahren. Die Identifizierung der von Art. 14 SDG-VO betroffenen Fachverantwortlichen ist ohne Erkenntnisse aus diesem Evidence Survey nicht möglich. In diesen innerstaatlichen Vorarbeiten wurden 58 Leistungen (LeiKa-Leistungen) 24 Verfahren zugeordnet. Bei vier von 24 Verfahren gibt es aktuell Klärungsbedarf mit der EU-KOM, bei fünf von 24 Verfahren konnten nicht genügend LeiKa-Leistungen identifiziert werden.

Finanzierung

Grundsätzlich sind im Kontext der Registermodernisierung zwei Ressourcenbedarfe und deren Finanzierung zu unterscheiden: Zum einen sind die Aufwände auf Seiten Bund und federführender Länder zum Aufbau und Betrieb des Projekts „Gesamtsteuerung Registermodernisierung“ zur finanzieren, welche eine erfolgreiche Steuerung zur Erreichung des Zielbilds gewährleisten sollen. Zum anderen entstehen auf Bundes- und Landesebene (inklusive Kommunen) erhebliche Aufwände für die Umsetzung des Zielbilds, welche ebenfalls einer entsprechenden Finanzierung bedürfen. Bezugnehmend auf die vorangegangenen Beschlüsse des IT-PLR in der 36. Sitzung sowie die Beschlussvorlagen für

die 37. Sitzung werden beide Finanzierungsaspekte in einem dedizierten Kapitel dieser Anlage behandelt (siehe Kapitel 4, Budget zur Programmsteuerung, sowie Kapitel 5, Finanzierungsbedarf des Gesamtvorhabens Registermodernisierung).

Kommunikation, Change- und Stakeholdermanagement

Zur Koordination der projektinternen Kommunikation und der gezielten Ansprache von externen Stakeholdern der Registermodernisierung wurde 2021 eine übergreifende Kommunikationsstrategie für die Gesamtsteuerung Registermodernisierung entwickelt. Für ein übergreifendes Stakeholdermanagement wurden relevante Akteure aus Behörden, Ministerien, Verbänden und von IT-Dienstleistern systematisch identifiziert und angesprochen. Zur Information der Fachöffentlichkeit fand im Dezember 2021 mit dem Forum Registermodernisierung eine niedrigschwellige Informations- und Diskussionsveranstaltung mit über 300 Teilnehmenden statt. Zudem wurde unter www.onlinezugangsgesetz.de/registermodernisierung ein zentraler Internetauftritt geschaffen.

Registerlandkarte

Die Registerlandkarte ist eine Übersicht über bestehende Register, die den Planungs- und Priorisierungsprozess der Registermodernisierung unterstützen soll. Kurzfristig soll im ersten Quartal 2022 eine Übersicht mit Informationen zu den 51 Registern der Anlage nach IDNrG und ergänzend zu den Top-18-Registern bereitgestellt werden (Registerübersicht). Der Fokus liegt auf den technischen Informationen zur Anbindungsfähigkeit der Register und dem Umsetzungsstand der angebundenen OZG-Leistungen.

Gleichzeitig schreiten die Arbeiten an einer dauerhaften und öffentlich zugänglichen Registerlandkarte voran. Das Grobkonzept der Registerlandkarte sieht eine hohe Anknüpfungsfähigkeit an vorhandene Datenbanken vor. Die Registerlandkarte soll vorhandene Informationen, die bei einer Vielzahl von Akteuren vorliegen, bündeln. Dies beinhaltet insbesondere eine enge Kooperation mit der Verwaltungsdateninformations-Plattform des Statistischen Bundesamtes. Befragungen von registerführenden Stellen werden so auf ein notwendiges Minimum reduziert.

Die Registerlandkarte wird nach aktuellem Planungsstand 2023 frei und öffentlich zugänglich sein. Die Daten werden maschinenlesbar aufbereitet sein und können über Schnittstellen von Fremdanwendungen eingebunden werden.

Schnittstellen zwischen Registermodernisierung/Art. 14 SDG-VO und OZG-Umsetzung

Im Fokus 2021 stand die Initiierung eines Austauschs zu Schnittstellen zwischen der Registermodernisierung, der nationalen Umsetzung des Art. 14 SDG-VO und der OZG-Umsetzung, um grundlegende Schnittmengen sowie Chancen für Synergien zu identifizieren. Unter Einbezug relevanter Beteiligter wurde der Austausch aufgenommen und gemäß Beschluss auf der 36. Sitzung des IT-PLR ein erstes Vorgehensmodell für eine verzahnte

Reifegrad-4-Umsetzung im Sinne des Once-Only-Prinzips entworfen. Der aktuelle Ergebnisstand sowie nächste Schritte werden in Kapitel 3 detailliert (Schnittstelle Registermodernisierung/Art. 14 SDG-VO und OZG).

2. Umsetzungsplanung bis 2025

Das im 34. IT-PLR beschlossene Zielbild der Registermodernisierung markiert die Eckpunkte für die Umsetzungsplanung bis 2025. Auf Basis der 2021 gewonnenen ersten Erkenntnisse zur Ausgestaltung des Zielbilds ist diese Umsetzungsplanung weiter zu konkretisieren und mit konkreten Meilensteinen sowie einer Zeitleiste zu hinterlegen (siehe Beschluss der 36. Sitzung des IT-PLR).

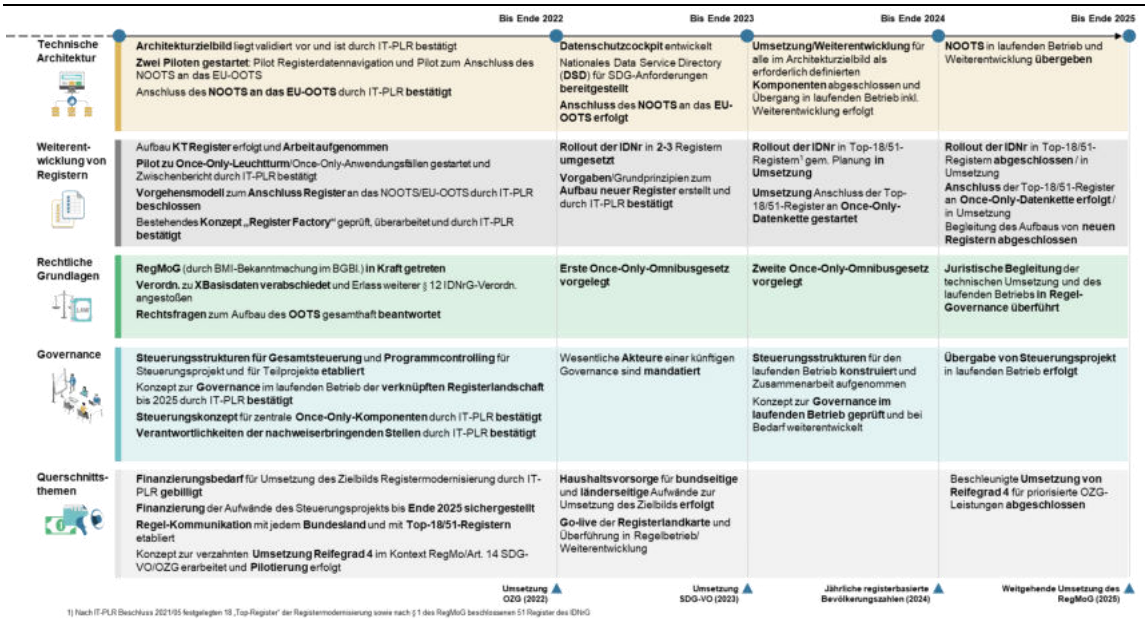


Abbildung 3: Wesentliche Meilensteine der Umsetzungsplanung bis 2025 (Auszug) mit Blick auf das Zielbild Registermodernisierung (siehe Anhang)

Die übergreifende zeitliche Umsetzungsplanung wurde von den Federführenden entlang der fünf Säulen des Zielbilds anhand konkreter Programmmeilensteine bis 2025 definiert. Die in Abbildung 2 (detailliert im Anhang) dargestellten Programmmeilensteine stellen dabei lediglich einen Auszug mit Blick auf die wesentlichen Themen dar:

- **Technische Architektur:** Bis Ende 2022 sollen das validierte Architekturzielbild bestätigt vorliegen sowie weitere Piloten zur Erprobung und zum Anschluss an das EU-OOTS gestartet sein. Zudem gilt es, zentrale Entscheidungen zur Umsetzung der Preview-Verpflichtung nach der SDG-VO zu treffen, sowie zur Entwicklung eines nationalen Once-Only-Standards und zum Anschluss des NOOTS an das EU-OOTS. Bis Ende 2023 soll das DSC entwickelt und das NOOTS an das EU-OOTS angeschlossen sein. Ein nationales DSD wird für SDG-Anforderungen bereitgestellt. 2024 soll die Umsetzung/Weiterentwicklung aller im Architekturzielbild als erforderlich definierten Komponenten abgeschlossen und 2025 der Übergang in den laufenden Betrieb inklusive Weiterentwicklung erfolgt sein.
- **Weiterentwicklung von Registern:** 2022 sollen ein Rolloutplan inklusive Priorisierungslogik, Vorgehensmodell und Anforderungen an Register zur Einführung der

IDNr in Top-18/51-Register[6] entwickelt, ein Vorgehensmodell zum Anschluss der Register an das EU-OOTS/NOOTS beschlossen sowie ein Pilotvorhaben zu Once-Only-Anwendungsfällen gestartet werden. Gleichzeitig erfolgt der Aufbau des KT Register und das bestehende Konzept der „Register Factory“ wird auf seine künftige Rolle hin überarbeitet. 2023 wird der Rollout der IDNr in zwei bis drei priorisierte Register umgesetzt sein, bis Ende 2025 dann in den definierten Top-18/51-Registern. Der Anschluss der Top-18-/51-Register an die Once-Only-Datenkette soll 2023 starten und ebenfalls bis 2025 vollzogen sein. Parallel dazu soll die Begleitung des Aufbaus von im Zielbild definierten neuen Registern bis 2025 abgeschlossen werden.

- **Rechtliche Grundlagen:** 2022 sollen die Prüfung priorisierter Rechtsfragen zum EU-OOTS gem. Art. 14 SDG-VO, die Evaluation sowie die Entscheidung für die Konzeption einer Once-Only-Generalklausel und ggf. bereits die Vorlage dieser auf Bundesebene erfolgen. Die Verordnung zu XBasisdaten soll verabschiedet und der Erlass weiterer § 12 IDNrG-Verordnungen angestoßen sein. Zudem ist die Qualitätssicherung und Abstimmung des Leitfadens zur Auslegung des Art. 14 SDG-VO und zur Ermittlung sich daraus ergebender Rechtsänderungsbedarfe zur grenzüberschreitenden Umsetzung des Once-Only-Prinzips geplant. Eine Prüfung der Möglichkeit einer Verordnungsermächtigung zur Festlegung der Anschlussbedingungen sowie der Realisierbarkeit des Konzepts von Kopfstellen für angeschlossene Register und deren Verhältnis zueinander ist ebenfalls für 2022 vorgesehen. Noch im selben Jahr ist – soweit die technischen Voraussetzungen vorliegen – das Inkrafttreten weiterer Artikel des RegMoG geplant. Bis Ende 2023 soll ein erstes Once-Only-Omnibusgesetz auf Bundesebene, inklusive ergänzender Vorschriften zum RegMoG, zur Umsetzung des Art. 14 SDG-VO, sofern erforderlich, und zur Novellierung des § 5 EGovG Bund vorgelegt werden. Weiterhin sollen die Länder insbesondere auf Grundlage des Leitfadens bei der Ermittlung möglicher Rechtsänderungsbedarfe zur Umsetzung des Art. 14 SDG-VO unterstützt sowie die Notwendigkeit einer Verordnungsermächtigung zur Festlegung einer Anschlussverpflichtung im nationalen OOTS geprüft werden. Die Vorlage eines zweiten Once-Only-Omnibusgesetzes ist bis Ende 2024 geplant. Die juristische Begleitung der technischen Zielbildumsetzung und des laufenden Betriebs soll bis 2025 in Regelstrukturen überführt werden.
- **Governance:** 2022 sind die Steuerungsstrukturen inklusive Controlling gemäß Zielbild für die Gesamtsteuerung Registermodernisierung etabliert sowie ein Konzept zur Governance im laufenden Betrieb der verknüpften Registerlandschaft entwickelt und bestätigt. Darüber hinaus gilt es, ein Steuerungskonzept für zentrale Once-

[6] Nach IT-PLR Beschluss 2021/05 festgelegten 18 „Top-Register“ der Registermodernisierung sowie nach § 1 des RegMoG beschlossenen 51 Register des IDNrG.

Only-Komponenten zu erarbeiten und die Verantwortlichkeiten der nachweiserbringenden Stellen festzulegen. Die anschließenden zentralen Meilensteine sind bis 2023 die Mandatierung maßgeblicher Akteure einer künftigen Governance und bis Ende 2024 die Konstituierung der Steuerungsstrukturen für den laufenden Betrieb und Aufnahme der Zusammenarbeit. Die Überführung des Steuerungsprojekts in den laufenden Betrieb soll bis Ende 2025 erfolgen.

- **Übergreifende Themenbereiche:** Bis Ende 2022 sind der Finanzierungsbedarf für die Umsetzung des Zielbilds zu schätzen sowie die Finanzierung der Aufwände des Steuerungsprojekts sicherzustellen. Auf dieser Basis kann die Haushaltsvorsorge für bund- und länderseitige Aufwände zur Umsetzung des Zielbilds unterstützt werden. Des Weiteren wird 2022 eine Regelkommunikation mit den Top-18/51-Registern, den Bundesländern etabliert. Gleichzeitig gilt es, ein Konzept zur verzahnten Umsetzung von Reifegrad-4-Leistungen zu erarbeiten und zu pilotieren – diese wird bis Ende 2025 für priorisierte OZG-Leistungen abgeschlossen sein. 2023 erfolgt außerdem der Go-live der Registerlandkarte und die Überführung in den Regelbetrieb.

3. Schnittstelle Registermodernisierung/Art. 14 SDG-VO und OZG

3.1 Ausgangslage

Die Registermodernisierung bildet die Basis für eine weiterführende nutzerfreundliche Digitalisierung von Verwaltungsleistungen. Insofern weist sie enge Schnittstellen zur OZG-Umsetzung auf und ist darüber hinaus im Kontext der Anforderungen auf europäischer Ebene gemäß Art. 14 SDG-VO zu betrachten. Ein wesentliches Ziel der Registermodernisierung ist die Realisierung des Once-Only-Prinzips. Das RegMoG schafft eine rechtliche Basis für das Once-Only-Prinzip und somit für eine perspektivische OZG-Reifegrad-4-Umsetzung von Verwaltungsleistungen durch die Einführung eines bereichsübergreifenden Identifiers, der den Austausch von Registerdaten zwischen Behörden ermöglicht. Durch die SDG-VO besteht zudem die Anforderung, bestimmte Leistungen und Nachweise grenzüberschreitend digital anzubieten.

Gemäß Beschluss der 36. Sitzung des IT-PLR wird im Folgenden ein erster Grobentwurf eines Vorgehensmodells zur verzahnten Umsetzung des OZG-Reifegrads 4 in priorisierten Registern dargelegt.

3.2 Vorgehensmodell zur verzahnten Umsetzung des OZG-Reifegrads 4 für priorisierte Register

Eine Verzahnung der eingangs beschriebenen Schnittstellen eröffnet die Möglichkeit zu einer beschleunigten Umsetzung des OZG-Reifegrads 4 unter Nutzung relevanter Register im Sinne des Once-Only-Prinzips. In einem ersten Entwurf wurde hierfür ein Vorgehensmodell entwickelt, das grundlegende, auch parallel anzugehende Schritte zur Identifikation der Datenbasis, zur Prüfung der rechtlichen und technischen Voraussetzungen und zur praktischen Erprobung enthält (siehe Abbildung 4).

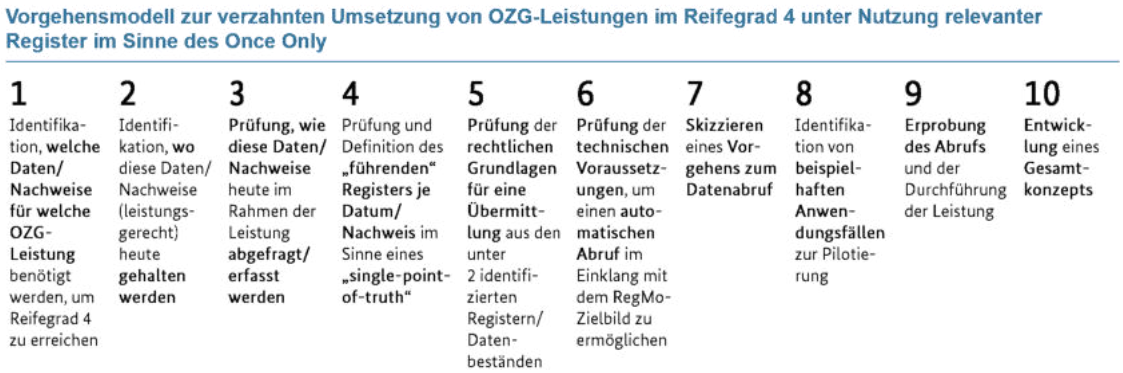


Abbildung 4: Vorgehensmodell zur verzahnten Reifegrad-4-Umsetzung unter Nutzung relevanter Register im Sinne des Once-Only-Prinzips (siehe Anhang)

- **Identifikation der Datenbasis (Schritte 1 und 2):** In den ersten beiden Schritten ist zu ermitteln, welche Daten und Nachweise für welche OZG-Leistung benötigt werden, um den Reifegrad 4 umsetzen zu können, und in welchen Registern diese Daten und Nachweise heute ggf. bereits gehalten werden. Dies bildet die Datenbasis für die weitere Umsetzung.
- **Prüfung der Datenbasis (Schritte 3 bis 6):** In den nächsten Schritten ist die Verfügbarkeit dieser Daten/Nachweise mit Blick auf den Digitalisierungsgrad und das Qualitätsniveau zu prüfen (Schritt 3) sowie das „führende“ Register im Sinne eines „Single Point of Truth“ (Schritt 4) zu bestimmen. Schritt 5 umfasst die Prüfung aus rechtlicher Sicht, inwiefern die identifizierten Daten/Nachweise (automatisiert) übermittelt werden können. Im Ergebnis sind ggf. erforderliche rechtliche Anpassungsbedarfe zu ermitteln und zu initiieren. Schritt 6 umfasst schließlich die technische Prüfung, inwiefern ein Abruf der Daten/Nachweise automatisiert erfolgen kann bzw. welche Voraussetzungen hier aus technischer Sicht zu schaffen sind.
- **Erprobung und Skalierung des Vorgehens (Schritte 7 bis 10):** Die weiteren Schritte umfassen die Skizzierung eines grundsätzlichen Vorgehens zum Datenabruf für betrachtete Leistungen (Schritt 7) sowie die Erprobung anhand konkreter Anwendungsfälle (Schritt 8 und 9). Basierend auf der Pilotierung können im letzten Schritt Erfahrungswerte abgeleitet und ein Gesamtkonzept zur Skalierung einer verzahnten Reifegrad-4-Umsetzung auf weitere Leistungen entwickelt werden (Schritt 10).

Zur Schaffung der Datenbasis (Schritt 1 und 2) fand im Rahmen der Gesamtsteuerung ein Initialaustausch zur Sichtung und Einordnung der vorhandenen Datenquellen statt. Neben der OZG-Informationsplattform und dem Föderalen Informationsmanagement (FIM) ergeben sich hier auch Anknüpfungspunkte zur QSL-Datenbank aus dem OZG-Themenfeld Querschnittsleistungen, dem aktuell laufenden Evidence Survey der EU-KOM sowie der Registerlandkarte als Teilprojekt der Registermodernisierung. Hierzu bedarf es weiterfüh-

render Aktivitäten zur Definition der konkreten Anforderungen für die benötigte Datenbasis und dem darauf basierenden Abgleich mit vorhandenen Datenquellen. Auf dieser Basis soll seitens der beteiligten Federführenden eine Empfehlung für die künftige Datenbasis im Rahmen des skizzierten Vorgehensmodells erarbeitet sowie etwaige Weiterentwicklungsbedarfe für vorhandene Datenquellen zur Umsetzung der Datenbasis abgeleitet werden. Parallel sollen auf Basis bereits vorhandener Analysen zu OZG-leistungsbezogenen Once-Only-Potenzialen von Registern erste Pilotierungen initiiert werden.

3.3 Geplante Pilotprojekte in 2022 zur verzahnten Umsetzung des OZG-Reifegrads 4 für priorisierte Register

In 2022 ist ferner geplant, durch verschiedene Pilotprojekte die beiden strategischen Ziele der OZG-/EfA-Umsetzung und der Registermodernisierung zu harmonisieren. Im Rahmen einer generischen Nutzerreise in einem Länderportal sollen medienbruchfreie Nachweisabrufe zur Erfüllung des Once-Only-Prinzips und damit zur Erreichung des OZG-Reifegrads 4 an ausgewählten Registern pilotiert werden. Die Verwaltungsschnittstelle für einen medienbruchfreien Nachweisabruf soll mittels einer technologieneutralen, fachbereichsübergreifenden Formatstandardisierung (generischer Nachweisdatenabrufstandard) gemeinsam mit der Koordinierungsstelle für IT-Standards (KoSIT) im Rahmen der Leistungsverwaltung beim Gewerbezentralregister entwickelt werden. Hierbei soll ebenfalls bereits eine Infrastrukturbasiskomponente im Rahmen der Registermodernisierung zur Umsetzung des 4-Corner-Modells im Sinne eines NOOTS pilotiert werden.

Ergänzend dazu soll in ausgewählten EfA-Umsetzungsprojekten Themenfeld übergreifend zu OZG-/SDG-Verwaltungsleistungen ein medienbruchfreier Nachweisabruf bei zentralen ausgewählten nachweisführenden Stellen pilotiert werden. Die Entwicklung soll in Ergänzung der Digitalisierung der Verwaltungsleistungen im EfA-Umsetzungsprojekt erfolgen. Auch hier soll der Nachweisabruf als Fachmodul eines generischen Nachweisabrufstandards gemeinsam mit der KoSIT entwickelt werden.

Im Hinblick auf diese Once-Only-Pilotierungen wird eine Kooperation mit den Umsetzungsprojekten zum Handelsregister und zu einem oder zwei der Top-18-Register des Zielbilds angestrebt.

Die Erkenntnisse aus den Pilotprojekten soll dazu dienen, das zu entwickelnde Vorgehensmodell anhand von Praxisbeispielen zu schärfen.

4. Budget zur Programmsteuerung

Für das Bund-Länder-Projekt „Gesamtsteuerung Registermodernisierung“ hat der IT-PLR mit Beschluss Nr. 2021/25 die Einrichtung eines Budgets zur Programmsteuerung vorgesehen. In der 36. Sitzung wurde beschlossen, dass die Finanzierungsbedarfe für den Aufbau und Betrieb der Gesamtsteuerung Registermodernisierung in den Jahren 2021 und 2022 aus Mitteln des Digitalisierungsbudgets der FITKO zu finanzieren sind (Beschluss Nr. 2021/35). Ein entsprechender Antrag wurde Mitte Oktober 2021 bei der FITKO gestellt und unter projektmanagementrelevanten Aspekten bewertet. Nach Antragsprüfung bestätigte die FITKO Anfang Dezember 2021, dass die Kriterien für festgelegte Projekte des IT-PLR durch die Antragstellenden erfüllt wurden. Die FITKO hat daraufhin gegenüber den Projektverantwortlichen eine Kostenübernahmeerklärung in Höhe von rund 7 Mio. EUR erteilt, wodurch die Aufwände der Federführenden im Projekt für die Gesamtsteuerung für die Jahre 2021 und 2022 gesichert sind.

Die Finanzierung der steuerungsrelevanten Aufgaben ab 2023 bis zur geplanten Zielbilderreichung 2025 ist noch nicht geklärt. Da das bestehende Digitalisierungsbudget Ende 2022 ausläuft, steht für die Zeit danach bislang kein Bund-Länder-Budget für Digitalisierungsvorhaben zur Verfügung. Als Bund-Länder-Projekt des IT-PLR werden die Federführenden daher gemeinsam mit der FITKO im nächsten Schritt einen geeigneten Vorschlag zur Finanzierung für ein Budget zur Programmsteuerung ab dem Jahr 2023 ausarbeiten.

5. Finanzierungsbedarf des Gesamtvorhabens Registermodernisierung

Die verfassungsfeste Registermodernisierung und ein damit verbundenes vertrauenswürdiges, allgemein anwendbares Identitätsmanagement haben nach dem unterzeichneten Koalitionsvertrag auch für die neue Bundesregierung Priorität (Rn. 408f.)[7]. Ehe es jedoch soweit ist, dass die modernisierte Registerlandschaft in Deutschland bei Bürgerinnen und Bürgern, Unternehmen und Verwaltung zu enormen Entlastungspotenzialen führen wird, bedarf es einer konsequenten Umsetzung des vom IT-PLR beschlossenen Zielbilds (Beschluss Nr. 2021/05). Dabei fallen bei Bund und Ländern (inklusive Kommunen) erhebliche Aufwände an. Um eine erste grobe Schätzung der Aufwände des Gesamtvorhabens Registermodernisierung im Sinne des Zielbilds vornehmen zu können, wurde hierzu im Februar 2021 im Rahmen des Koordinierungsprojekts Registermodernisierung ein Aufwandsschätzmodell (ASM) entwickelt, das eine erste Indikation des Gesamtaufwands bezifferte.

5.1 Validierung des ASM

Mit Beschluss Nr. 2021/35 hat der IT-PLR die Federführenden gebeten, den im Frühjahr entwickelten Entwurf eines ASM für die Umsetzung des Gesamtprojekts Registermodernisierung mit Bund und Ländern unter Einbeziehung kommunaler Expertise weiter zu validieren und auf dieser Basis den geschätzten Finanzierungsbedarf für die Umsetzung des Zielbilds bei Bund und Ländern (inklusive Kommunen) vorzulegen. Das validierte ASM sollte so als haushaltsbegründende Unterlage für Bund und Ländern dienen können, ohne die Haushaltsverhandlungen des Bundes zu präjudizieren.

In diesem Rahmen fanden von August bis Dezember 2021 eine Vielzahl an Validierungsgesprächen mit unterschiedlichen Stakeholdern der 43 identifizierten Aufwandstreiber des ASM statt, für welche Aufwände auf Seiten des Bundes geschätzt wurden. Für die Validierung der groben Schätzung des bundseitigen Finanzierungsbedarfs wurden die folgenden fünf zentralen Fragen adressiert: (1) Welche Aufwände fallen im Rahmen der Registermodernisierung an? (2) Wie hoch sind die Aufwände? (3) Bei wem fallen die Aufwände an? (4) Wann fallen die Aufwände an? (5) Welche Aufwände sind bereits finanziert? Nach Beantwortung dieser zentralen Fragen basierend auf dem aktuellen Arbeits- und Wissensstand konnte so im Dezember 2021 eine erste initial validierte Aufwandsschätzung für den Bund vorgenommen werden.

Die Validierung der länderseitigen (inklusive der kommunalen) Aufwände dauert derzeit noch an. Nach ihrem Abschluss sollen die Länder vor der Frühjahrssitzung des IT-PLR ein

[7] https://www.bundesregierung.de/resource/blob/974430/1989762/4fe5f73596ec3ca1f41ff5a190ef1337/2021-12-08-koalitionsvertrag-data.pdf?download=1

Informationspaket mit den relevanten Informationen zu den länderspezifischen Aufwänden der Registermodernisierung, unter anderem eine aktualisierte Liste der relevanten Aufwandstreiber erhalten. Weiterhin soll ihnen eine Vorgehensweise für die Ermittlung von Schätzwerten vorgelegt werden, auf deren Grundlage sie Haushaltsvorsorge betreiben können. Im Laufe des Jahres 2022 wird eine präzisere Aufwandschätzung bei Bund, Ländern und Kommunen mit zunehmender Spezifizierung der technischen Anforderungen möglich sein.

5.2 Erste Ergebnisse der initial validierten Aufwandsschätzung

Die Validierung des ASM hinsichtlich der bundseitigen Aufwände hat ergeben, dass die einmaligen Aufwände zur Realisierung des Zielbilds Registermodernisierung weiterhin auf 0,5 Mrd. EUR bis 0,6 Mrd. EUR für den Bund geschätzt werden. Dabei ist anzumerken, dass es sich dabei keineswegs um eine Fortschreibung der ursprünglichen Annahmen und Schätzungen aus dem Koordinierungsprojekt Registermodernisierung handelt, sondern die durch die Validierung vorgenommenen alternativen Annahmen im ASM in Summe die gleiche Spanne an einmaligen Aufwänden ergeben. Bei den Ländern und Kommunen wird aufgrund der hohen Dezentralität der deutschen Registerlandschaft der Großteil der einmaligen Umsetzungsaufwände anfallen. Auch die jährlichen Aufwände nach vollständiger Inbetriebnahme aller Aufwandstreiber sind in ihrer Größenordnung gleichgeblieben und werden weiterhin auf 0,1 Mrd. EUR bis 0,2 Mrd. EUR für den Bund geschätzt.

Im Rahmen der Validierung kam es insbesondere zu einer Reihe an Verschiebungen bei den geschätzten Daten der Inbetriebnahme einzelner Aufwandstreiber, die im Frühjahr 2021 noch nicht abschätzbar waren. Diese Verschiebungen haben jedoch ausdrücklich keine Auswirkung auf die geplante Zielbilderreichung bis Ende 2025. Nichtsdestotrotz resultieren die neuen Erkenntnisse zu den zeitlichen Abhängigkeiten von Aufwandstreibern in einer Verschiebung der Gesamtaufwände über den Betrachtungszeitraum 2021 bis 2025 hinaus in spätere Jahre hinein. Dies begründet sich dadurch, dass ein signifikanter Teil an Aufwandstreibern erst nach 2025 jährliche Aufwände generieren wird, da diese – wie oben dargelegt – nach erfolgter Validierung erst zu einem späteren Zeitpunkt fertiggestellt und in Betrieb genommen werden. Im Ergebnis wird daher Stand heute davon ausgegangen, dass sich die Gesamtaufwände mit Blick auf den Betrachtungszeitraum bis 2025 bei rund 2 Mrd. EUR für Bund und Länder bewegen. Im Ergebnis ist somit darauf hinzuweisen, dass sich mit Blick auf die Differenz zu den ursprünglich – vor Validierung – angenommenen rund 2,9 Mrd. EUR Gesamtaufwänden (siehe Anlage zum 36. IT-PLR) ein Teil der jährlich anfallenden laufenden Aufwände in die Zeit nach dem Betrachtungszeitraum (ab 2026) verschieben.

Grundsätzlich können die Annahmen des ASM nicht als finale Schätzung oder Berechnung der Aufwände verstanden werden. Es handelt sich hierbei lediglich um eine grobe Schätzung basierend auf dem aktuellen Arbeits- und Wissensstand im Projekt „Gesamtsteuerung Registermodernisierung“, die mit jeder neuen Erkenntnis weiter verfeinert werden muss.

Abkürzungsverzeichnis

ASM	Aufwandsschätzmodell
BMI	Bundesministerium des Innern und für Heimat
BVA	Bundesverwaltungsamt
DSC	Datenschutzcockpit
DSD	Data Service Directory
DSGVO	Datenschutz-Grundverordnung
DVDV	Deutsche Verwaltungsdiensteverzeichnis
EfA	„Einer für Alle“
eIDAS	electronic IDentification, Authentication and trust Services
ELFE	„Einfach Leistungen für Eltern“
EStA	Entscheidungen in Staatsangehörigkeitsangelegenheiten
EU-KOM	Europäische Kommission
FIM	Föderales Informationsmanagement
FITKO	Föderale IT-Kooperation
GWR	Gebäude- und Wohnungsregister
IAM	Identity Access Management
IDA	Identitätsdatenabruf
IDM	Identity Management
IDNr	Identifikationsnummer
IDNrG	Identifikationsnummerngesetz
IT-PLR	IT-Planungsrat
KoSIT	Koordinierungsstelle für IT-Standards
KRZN	Kommunale Rechenzentrum Niederrhein
KT	Kompetenzteam
LeiKa	Leistungskatalog
NKR	Nationaler Normenkontrollrat
NWR	Nationales Waffenregister
OOTS	Once-Only-Technical-System
OSCI	Online Services Computer Interface

OZG	Onlinezugangsgesetz
PMO	Project Management Office
RegMoG	Registermodernisierungsgesetz
SDG	Single Digital Gateway
SDG-VO	SDG-Verordnung
SG	Service Gateway
UBRegG	Unternehmensbasisdatenregistergesetz
VIP	Verwaltungsdaten-Informationsplattform
V-PKI	Verwaltungs-Public-Key-Infrastructure
W-IDNr	Wirtschaftsidentifikationsnummer

Abbildungsverzeichnis

Anhang

Anhang 1: Übergreifende Ergebnisse 2021 entlang der Säulen des Zielbilds der Registermodernisierung

Abbildung 5: Übergreifende Ergebnisse 2021 entlang der Säulen des Zielbilds der Registermodernisierung

Anhang 2: Aktualisierte Once-Only-Datenkette nach aktuellem Diskussionsstand im KT Architektur, Ende 2021

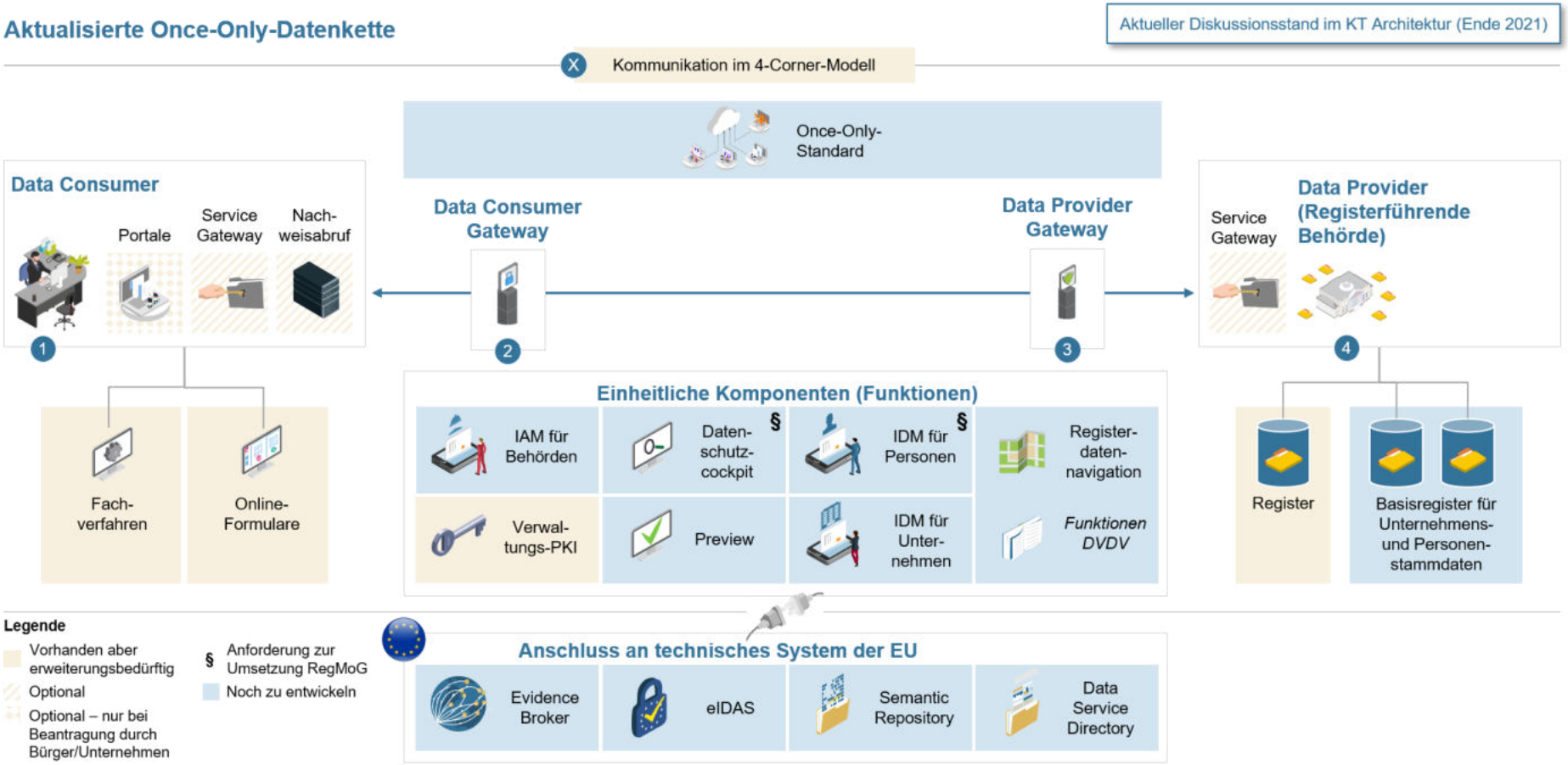


Abbildung 6: Aktualisierte Once-Only-Datenkette nach aktuellem Diskussionsstand im KT Architektur, Ende 2021

Anhang 3: Teilprojekte und assoziierte Vorhaben der Registermodernisierung (Beschluss Lenkungskreis vom 13. Oktober 2021)

Cluster		Laufende Teilprojekte und Vorhaben	Anbindung an die Gesamtsteuerung
Teilprojekte RegMo Bereits laufende Projekte und Vorhaben, die das RegMo-Zielbild umsetzen	Technische Architektur	– Weiterentwicklung Rahmenwerk xÖV-Standards – Datenschutzcockpit – V-PKI – Basiskomponente Registerabruf – IDA (Einführung IDNr mit Identifikationsabfrage)	– Obligatorische Teilnahme am Projekteboard – Integration in das Programmcontrolling – Mögliche Teil- oder Vollfinanzierung über zu schaffendes RegMo-Budget[1]
	Rechtliche Grundlagen	– Once-Only-Check NKR (BW)	
	Übergreifend	– Registerlandkarte	
	Pilotvorhaben	– Einspeicherung der IDNr in das Nationale Waffenregister – Erprobung Once-Only-Architektur für Melderegister mit KRZN – Nutzung SGs[2] zur Anbindung des Bundesportals an EStA-Register – Weiterentwicklung der SGs[2] im Sinne des Zielbilds	
Assoziierte Vorhaben Bereits laufende Projekte und Vorhaben, die eine inhaltliche Schnittstelle zur RegMo aufweisen		– Digitalisierungsprogramm OZG – Portalverbund – SDG-VO – Registerzensus – GWR (Gebäude- und Wohnungsregister) – ELFE („Einfach Leistungen für Eltern“) – VIP (Verwaltungsdateninformationsplattform) – FIM (Förderales Informationsmanagement) – DVDV (Deutsches Verwaltungsdienstverzeichnis) – Basisregister für Unternehmen (UBRegG)	– Einladung zur Teilnahme am Projekteboard – Keine Integration in das Programmcontrolling – Finanzierung über RegMo-Budget[1] als Option, individuell zu evaluieren

1. Aktuell in Prüfung; 2. SG - Service Gateway

Abbildung 7: Teilprojekte und assoziierte Vorhaben der Registermodernisierung

Anhang 4: Wesentliche Meilensteine der Umsetzungsplanung bis 2025 (Auszug) mit Blick auf das Zielbild Registermodernisierung

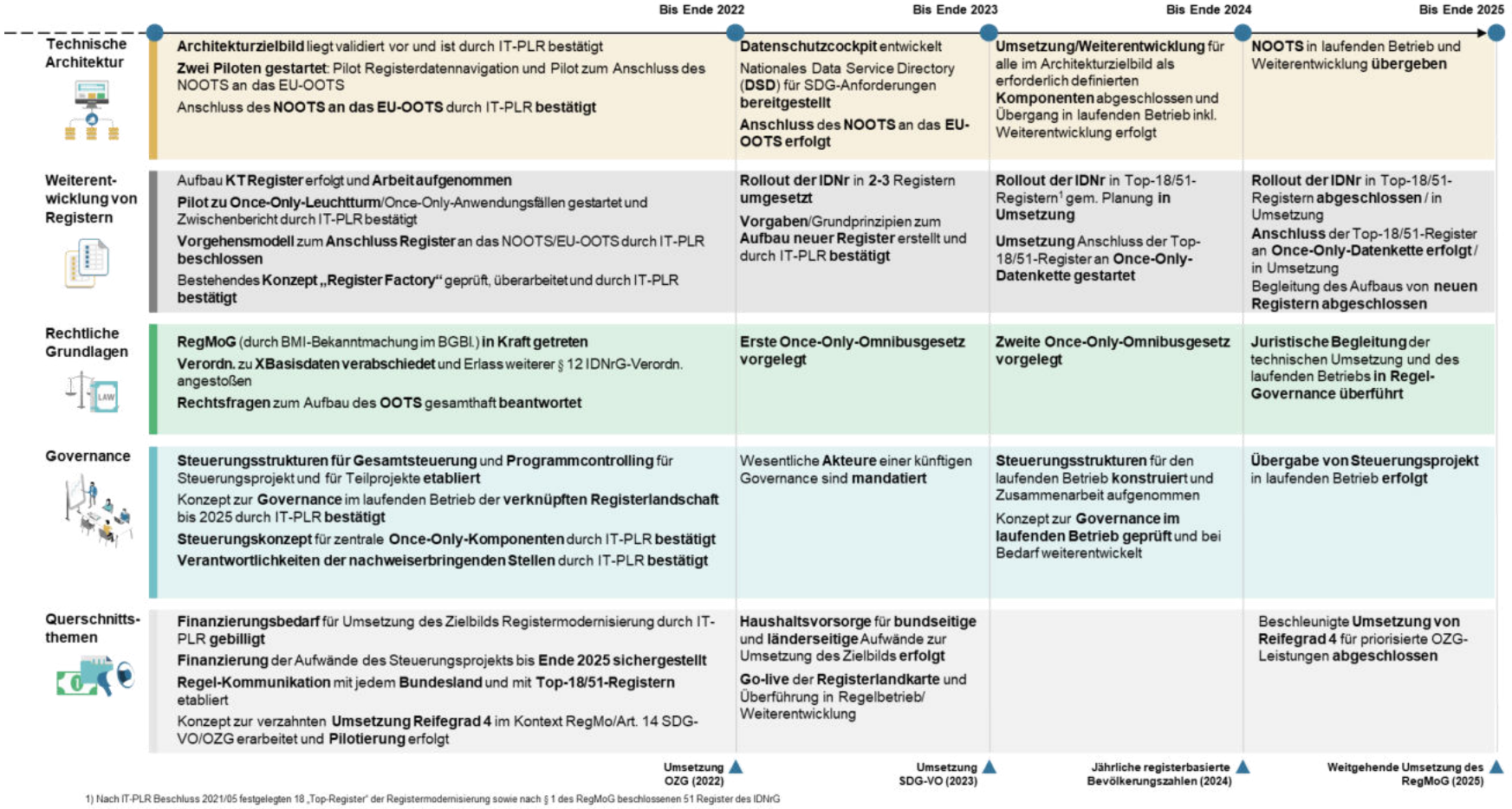


Abbildung 8: Wesentliche Meilensteine der Umsetzungsplanung bis 2025 (Auszug) mit Blick auf das Zielbild Registermodernisierung

Anhang 5: Detaillierte Programmplanung bis 2025

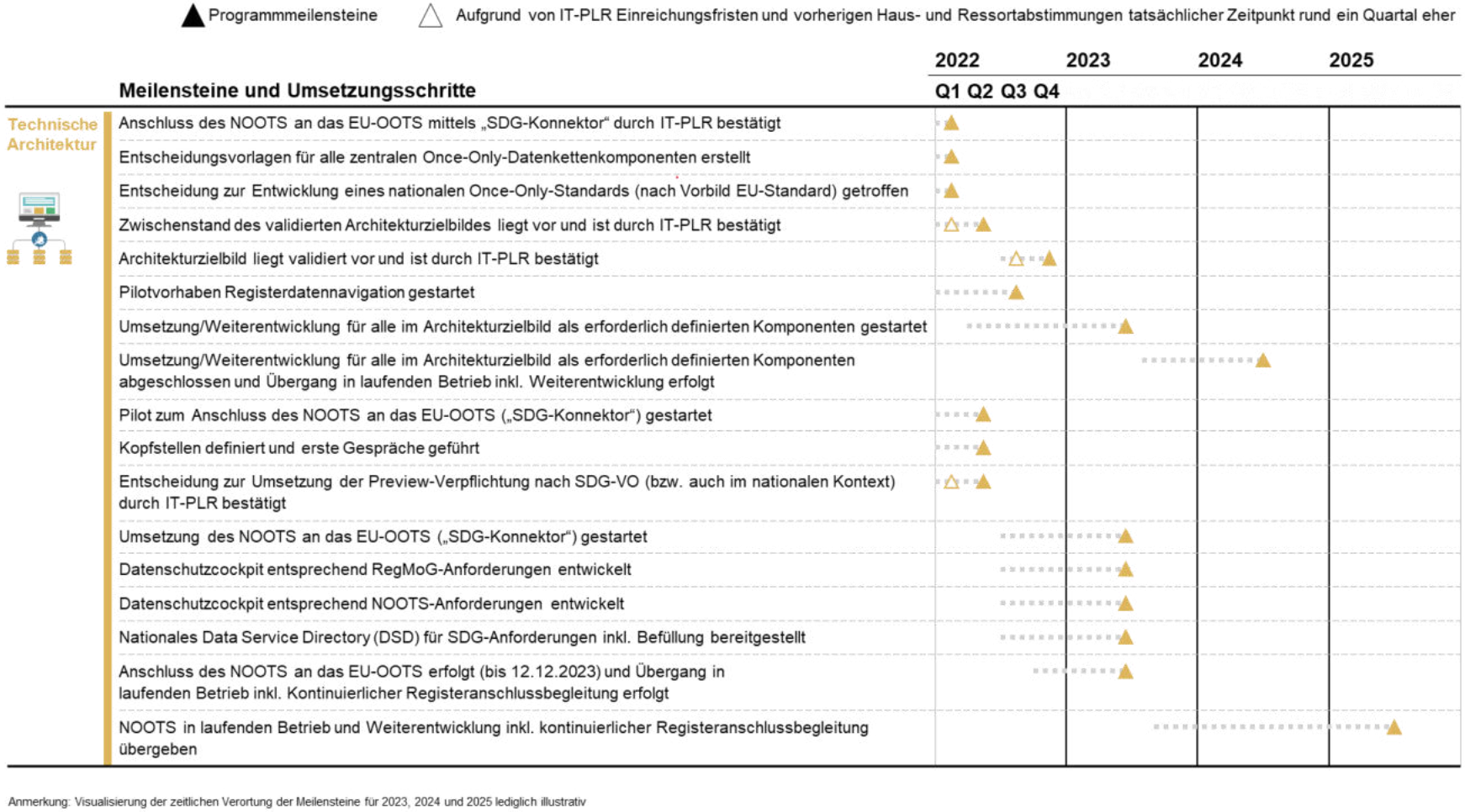


Abbildung 9: Technische Architektur – Detaillierte Programmplan bis 2025

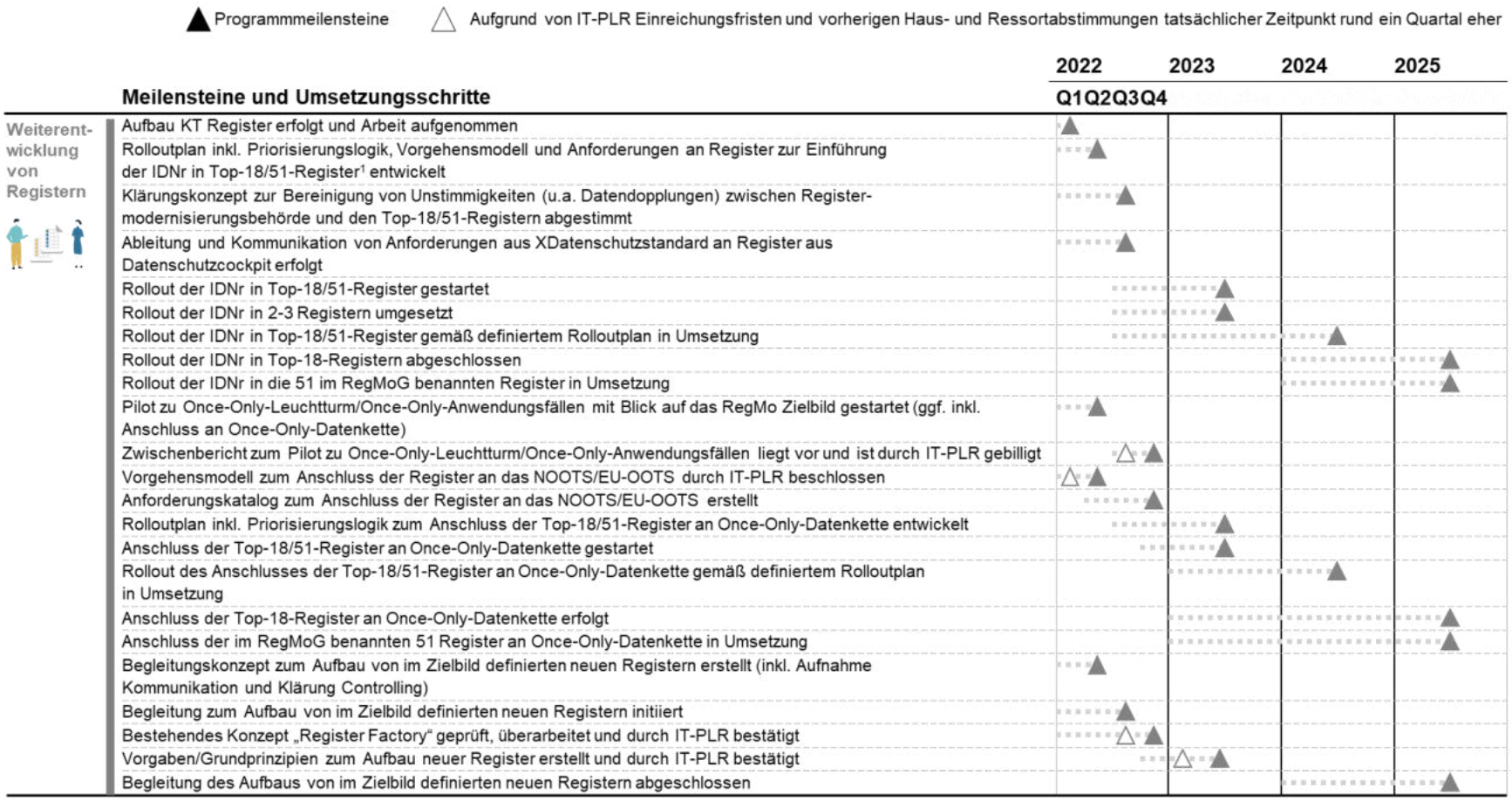


Abbildung 10: Weiterentwicklung von Registern – Detaillierte Programmplan bis 2025

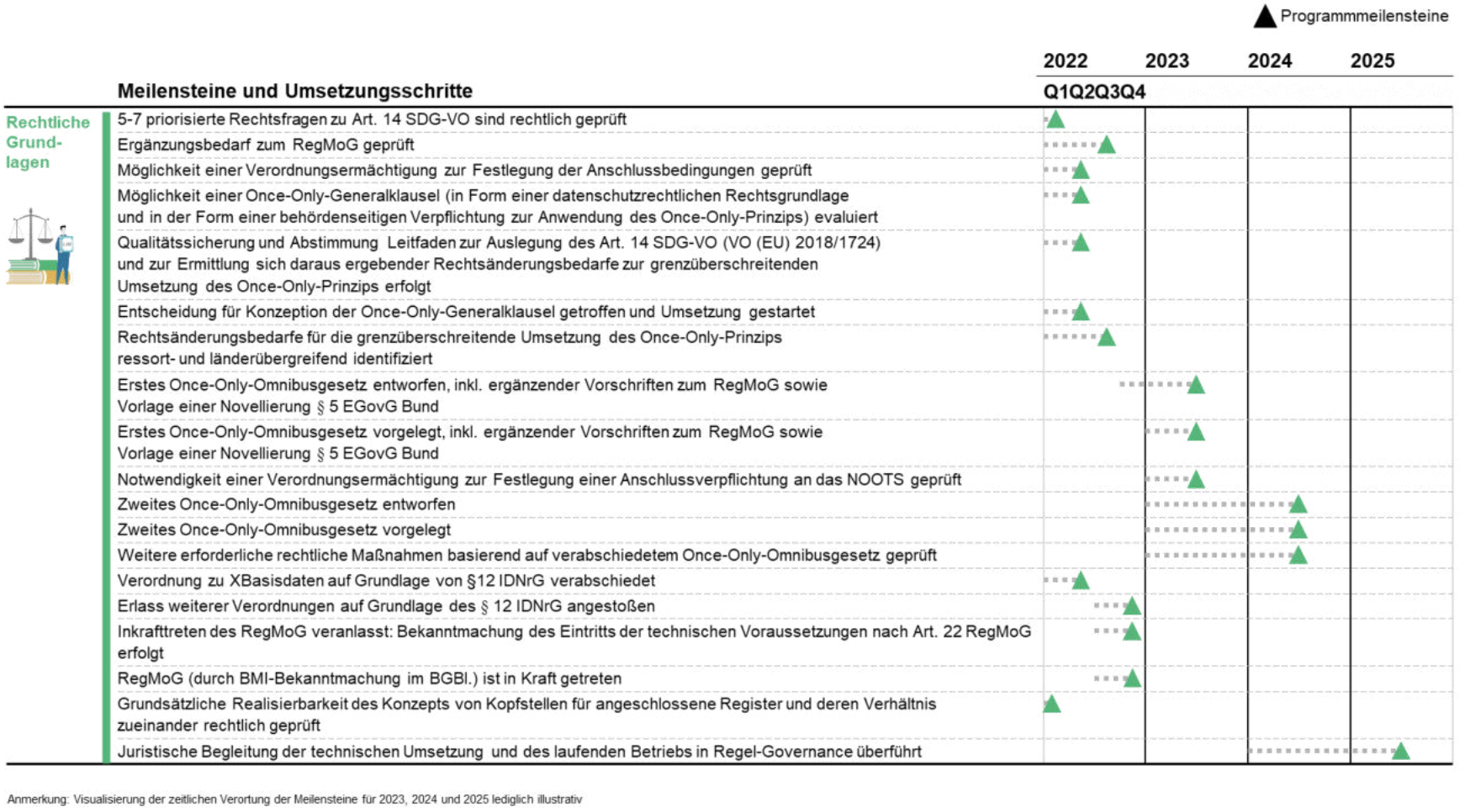


Abbildung 11: Rechtliche Grundlagen – Detaillierte Programmplan bis 2025

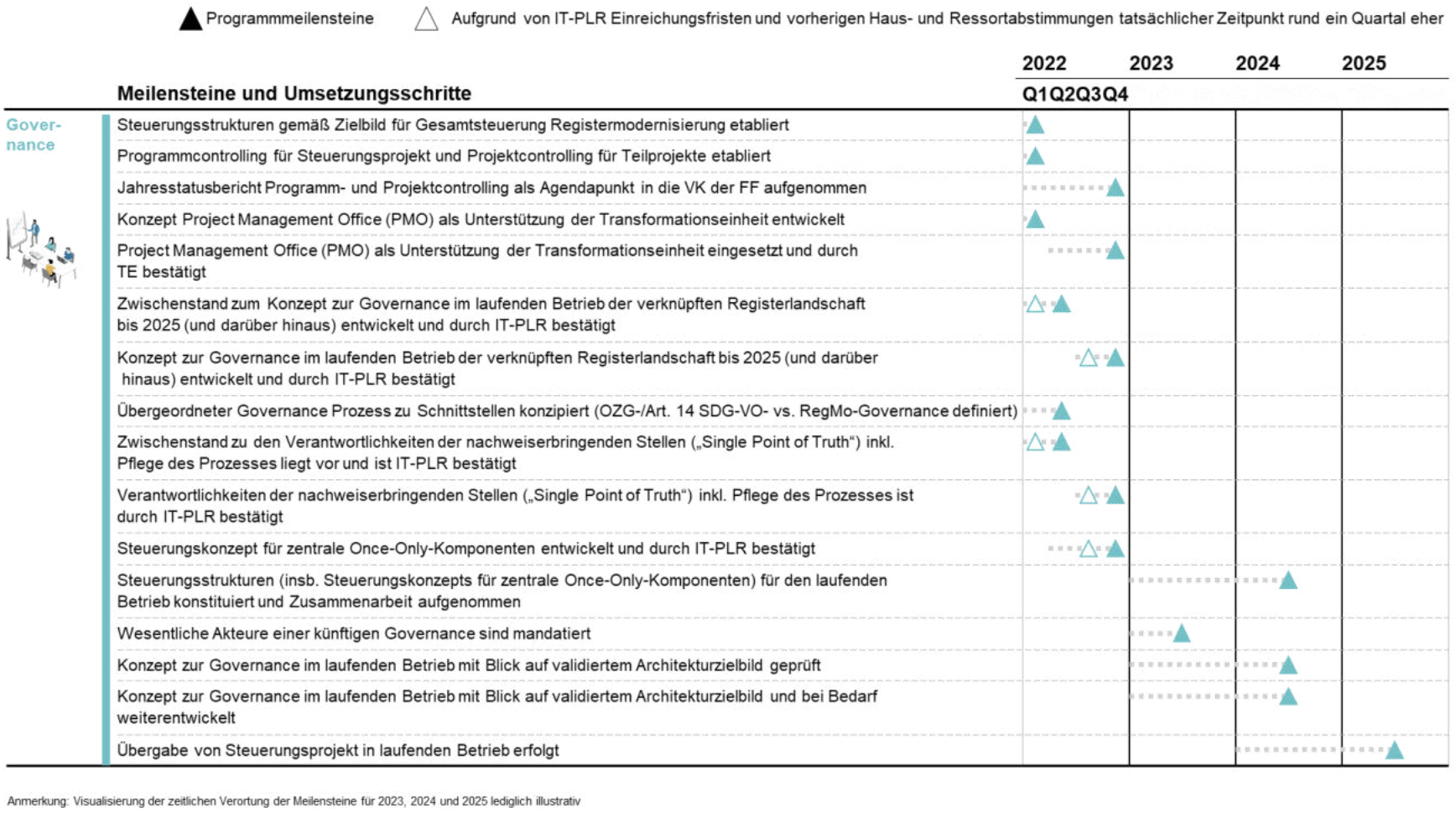


Abbildung 12: Governance – Detaillierte Programmplan bis 2025

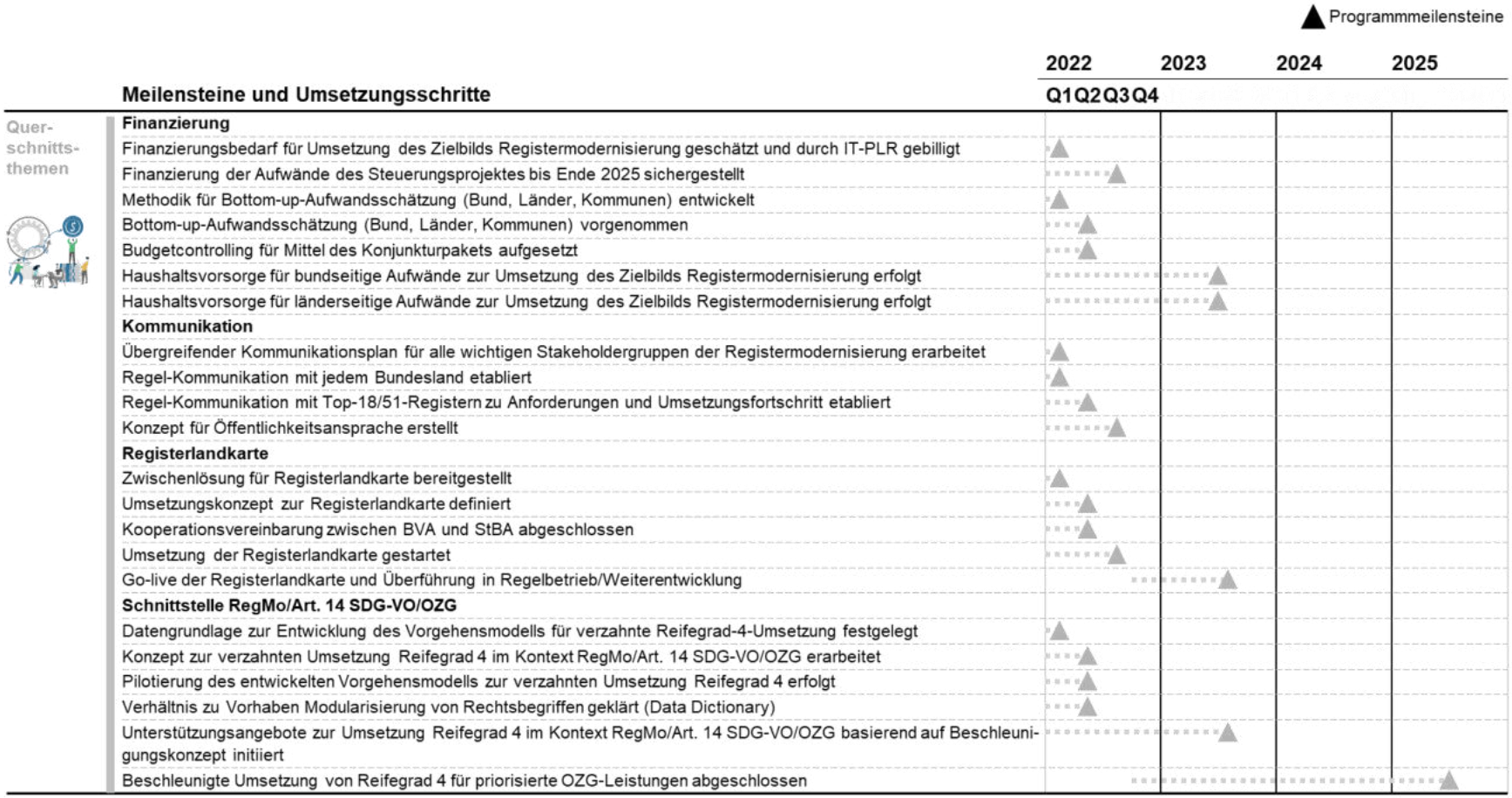


Abbildung 13: Querschnittsthemen – Detaillierte Programmplan bis 2025

Anhang 6: Vorgehensmodell zur verzahnten Reifegrad-4-Umsetzung unter Nutzung relevanter Register im Sinne des Once-Only-Prinzips

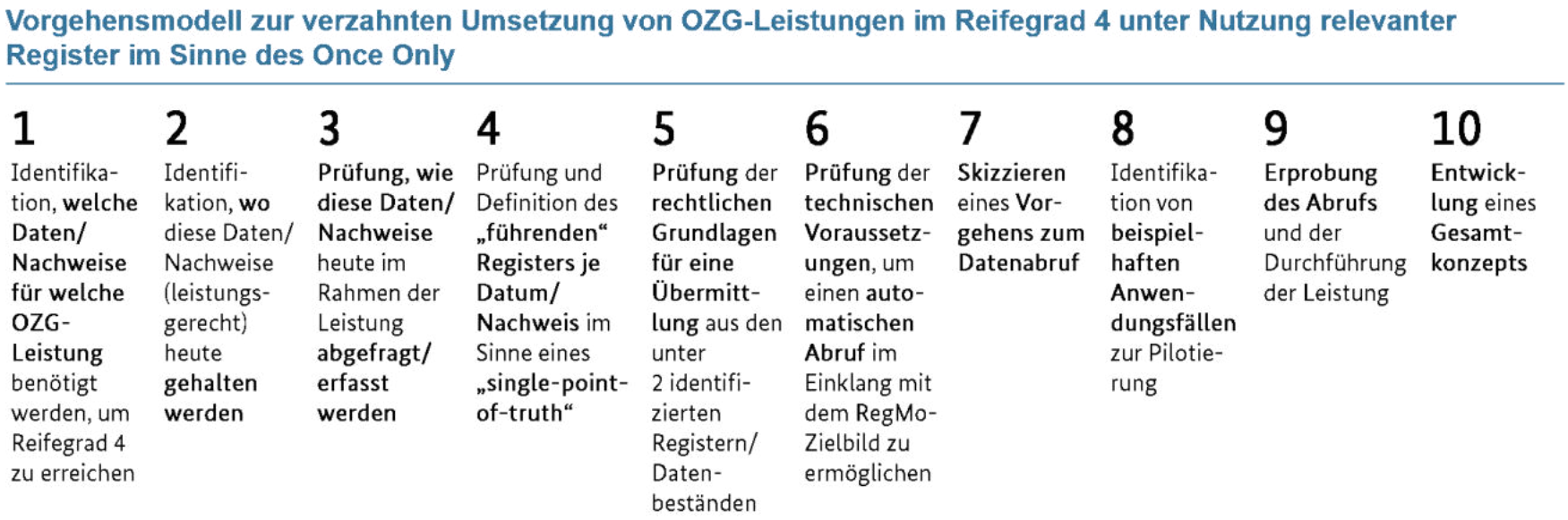


Abbildung 14: Vorgehensmodell zur verzahnten Reifegrad-4-Umsetzung unter Nutzung relevanter Register im Sinne des Once-Only-Prinzips

Projekt „Gesamtsteuerung Registermodernisierung“: Bericht zum Umsetzungsstand

Juni 2022

Inhaltsverzeichnis

Kernbotschaften

Das im Juni 2021 vom IT-Planungsrat (IT-PLR) beschlossene Projekt „Gesamtsteuerung Registermodernisierung“ unter Federführung des Bundes (Bundesministerium des Innern und für Heimat (BMI)) sowie der Länder Baden-Württemberg, Bayern, Hamburg und Nordrhein-Westfalen soll als übergreifendes Programmmanagement die Realisierung des Zielbilds der Registermodernisierung voranbringen (Beschluss Nr. 2021/25).

Es ergeben sich in diesem Kontext verschiedene Herausforderungen für die Gesamtsteuerung Registermodernisierung. Als ein wesentlicher Schlüsselfaktor sind an dieser Stelle die Personalressourcen in der Gesamtsteuerung und den mit der Umsetzung der Registermodernisierung betrauten Fachbereichen zu benennen. Für eine kohärente Beförderung des Vorhabens in der Breite bei Bund und Ländern ist die derzeitige Ressourcenausstattung nicht ausreichend, um den Steuerungsansprüchen gegenüber der komplexen Stakeholder-Landschaft gerecht zu werden. Der Nationale Normenkontrollrat hat die Registermodernisierung in ihrer Dimension mit der Umsetzung des Onlinezugangsgesetzes verglichen. Es ist daher entscheidend, eine mehrjährige Finanzierung für die Gesamtsteuerung Registermodernisierung sicherzustellen, um erfolgreich Personal für die Steuerung und Umsetzung des Vorhabens gewinnen zu können (vgl. Beschlussvorlage Nr. 1).

Damit die Registermodernisierung Erfolg hat und Modernisierungsimpulse Resonanz finden, bedarf es sowohl einer stringenten Beförderung der Umsetzung als auch einer engen Einbeziehung der Expertise und Interessen einer komplexen Stakeholderlandschaft. Auch bei der vorgenommenen Fokussierung auf die Top-18-Register müssen tausende registerführende Stellen auf allen föderalen Ebenen ihre Register modernisieren. Das macht die Steuerungsaufgabe ressourcenintensiv, derzeit kann die Gesamtsteuerung das erforderliche Veränderungsmanagement unter strikter Priorisierung nur punktuell betreiben.

Die Gesamtsteuerung Registermodernisierung begegnet diesen Herausforderungen im Rahmen ihrer Möglichkeiten proaktiv (Priorisierung, Risikomanagement). Auch unter weiterer Ausschöpfung gegensteuernder Maßnahmen zeigt sich jedoch deutlich: ohne einen personellen Ressourcenaufwuchs in der Gesamtsteuerung auf Basis einer

mehrjährigen Finanzierungsgrundlage ist die Zielerreichung der durch den IT-Planungsrat beschlossenen Umsetzungsplanung gefährdet.

Einen weiteren Schwerpunkt im Jahr 2022 stellt die umsetzungsorientierte Definition von Anforderungen an die Register dar. Die Anforderungen umfassen rechtliche, technische und organisatorische Dimensionen, die konkrete Modernisierungsschritte für die Registerlandschaft beschreiben. Die Konkretisierung der Technischen Architektur ist ein essentieller Meilenstein, damit registerführende Behörden Klarheit über Modernisierungsbedarfe und Anschlussbedingungen gewinnen können.

Im Bereich der Technischen Architektur haben die Arbeitsergebnisse aus dem ersten Quartal 2022 das grundsätzliche Zielbild bestätigt. Thematisch wurden hier die Unterstützung asynchroner Prozesse in der Architektur der Registermodernisierung vereinbart, um das Once-Only Prinzip auch für Behörden untereinander verwirklichen zu können. Ein Konzept zur Entwicklung eines allgemeinen Standards für den Nachweisabruf für die nationale Registermodernisierung wurde erarbeitet. Die Entscheidung zur Umsetzung der Komponente Registerdatennavigation wurde auf den Weg gebracht und der Aufbau eines nationalen Data Service Directory und Nutzung des europäischen Evidence Brokers angestoßen. Daneben wurde die Einführung eines Reifegradmodells für die Registermodernisierung und Ausrichtung eines Nationalen Once-Only-Technical-Systems (NOOTS) auf die Erreichung eines datensparsamen, zielgerichteten Nachweisabrufes zur Leistungserbringung vorgeschlagen. Ein weiterer Fokus des Bereichs lag auf der Unterstützung des Nationalen SDG-Koordinators zur Gesamtarchitektur des europäischen Once-Only-Technical-Systems (EU-OOTS) nach Art. 14 SDG-Verordnung. Bislang ist die Europäische Kommission zu keiner Einigung zu einer Gesamtarchitektur mit den Mitgliedstaaten gekommen. Zur Erprobung grenzüberschreitender Nachweisaustausche im Kontext der SDG-Umsetzung wurden Pilotierungsmöglichkeiten mit den Niederlanden untersucht. Die Untersuchung wird bis April 2022 abgeschlossen, ergebnisabhängig kann eine Pilotierung ab Mai / Juni 2022 erfolgen.

Im Bereich der rechtlichen Grundlagen konnten verschiedene wichtige Arbeitsergebnisse erzielt und eine rechtliche Begleitung der Verhandlungen zum Durchführungsrechtsakt gemäß Art. 14 Abs. 9 SDG-VO gewährleistet werden. In diesem Rahmen hat das Kernteam Recht priorisierte Rechtsfragen des KT EU-Interoperabilität zum EU-OOTS beantwortet und einen Leitfaden zur Auslegung des Art. 14 SDG-VO

entwickelt, der im Hinblick auf die laufenden Verhandlungen zum Durchführungsrechtsakt fortlaufend aktualisiert wird. Nicht in der Meilensteinplanung tauchen die Unterstützungsaktivitäten für das KT Architektur auf. Das Kernteam Recht hat Rechtsfragen des Kompetenzteams Architektur mit dem Themenschwerpunkt NOOTS beantwortet und an das Kompetenzteam übergeben. Aufgrund fehlender personeller Ressourcen und pandemiebedingten Abwesenheiten konnten zwei gesetzt Meilensteine für das erste Halbjahr 2022 nicht erreicht werden: Die Prüfung einer Möglichkeit einer Verordnungsermächtigung zur Festlegung der Anschlussbedingungen und der grundsätzlichen Realisierbarkeit des Konzepts von Kopfstellen für angeschlossene Register und deren Verhältnis zueinander.

Der Aufbau der Governance-Strukturen der Gesamtsteuerung ist im Wesentlichen abgeschlossen. Für Mai bzw. Juni 2022 sind die konstituierenden Sitzungen des Registerbeirats sowie Wissenschafts- und Innovationsbeirats vorgesehen.

Im Bereich Kommunikation wurden auf Grundlage der durchgeführten Stakeholderanalyse zielgruppenspezifisch die verschiedenen Stakeholdergruppen adressiert. Die Information von Kommunen war Schwerpunkt im ersten Halbjahr.

Betroffene Fachministerkonferenzen (FMK) werden verstärkt eingebunden und zukünftig Einvernehmen über die Ziele und Umsetzungsschritte des Vorhabens Registermodernisierung hergestellt. Mit den Fachministerkonferenzen sollen weitere Schritte zu einer aktiven Einbeziehung und gemeinsamen Umsetzung vereinbart werden.

1 Überblick Projektziele und Ergebnisse 1. Halbjahr 2022

Das Projekt „Gesamtsteuerung Registermodernisierung“ unter Federführung des Bundes (BMI) sowie der Länder Baden-Württemberg, Bayern, Hamburg und Nordrhein-Westfalen hat die Aufgabe, die Realisierung des Zielbilds der Registermodernisierung ressort- und ebenenübergreifend konzertiert voranzubringen. Der aktuelle Umsetzungsstand wird nachfolgend vorgestellt.

Den Kern des Gesamtprogramms bilden die vier im Zielbild Registermodernisierung beschriebenen Säulen: eine interoperable und sichere technische Architektur, anschlussfähige Register auf Seiten der registerführenden Stellen, rechtliche Rahmenbedingungen für einen sicheren und datenschutzkonformen Datenaustausch sowie eine zukunftsweisende Governance (Kontroll- und Steuerungsstrukturen im laufenden Betrieb). Um ein zielgerichtetes Vorgehen zur Umsetzung des Zielbilds sicherzustellen, wurden die wesentlichen Ziele für 2022 (s.u.) und eine arbeitsteilige Aufgabenwahrnehmung unter den Federführenden bis zum Jahresende definiert.

Im ersten und zweiten Quartal 2022 konnten die Säulen im Rahmen vorhandener Ressourcen im Wesentlichen planmäßig ihre Aktivitäten weiterführen. Es konnten erste Erfolge durch den Abschluss von Meilensteinen erzielt werden, jedoch werden mit dem Fortschreiten des Vorhabens auch zunehmende Herausforderungen deutlich.

So zeigen sich in allen Säulen erste Verzögerungen, da es bislang noch nicht gelungen ist, erforderliches Personal für eine intensive Beförderung der prioritären Meilensteine bereitzustellen. Der Sicherstellung eines mehrjährigen Budgets für die Bund-Länder-Steuerung kommt daher entscheidende Bedeutung zu. Damit die Registermodernisierung Erfolg hat und Modernisierungsimpulse Resonanz finden, bedarf es sowohl einer stringenten Beförderung der Umsetzung als auch einer engen Einbeziehung der Expertise und Interessen einer komplexen Stakeholderlandschaft. Auch bei der vorgenommenen Fokussierung auf die Top-18-Register müssen tausende registerführende Stellen auf allen föderalen Ebenen ihre Register modernisieren. Das macht die Steuerungsaufgabe ressourcenintensiv, derzeit kann die Gesamtsteuerung das erforderliche Veränderungsmanagement unter strikter Priorisierung nur punktuell betreiben.

Die derzeit vorhandenen Ressourcen reichen nicht aus, um in 2022 sämtliche prioritären Meilensteine der Gesamtsteuerung in der nach der Umsetzungsplanung erforderlichen Geschwindigkeit umzusetzen. Im Interesse einer zügigen Definition der Anforderungen im Bereich „Technische Architektur“ und der Exploration von Pilotierungen mussten

beispielsweise essentielle Aktivitäten im Bereich der „Weiterentwicklung von Registern“ (z.B. Aufbau einer Datenbasis zur Identifizierung von Once-Only-Potentialen; Schärfung der OZG-Schnittstelle) depriorisiert werden. Im Bereich Stakeholdermanagement/ Kommunikation sind niedrigschwellige und breit angelegte Partizipationsformate (u.a. Forum Registermodernisierung) etabliert und die Kommunikation mit den Kommunen sowie Fachministerkonferenzen wurde verstärkt. Die Ressourcen reichten jedoch nicht aus, um diese Formate in der erforderlichen Intensität und Kontinuität zu begleiten. Im Bereich Recht mussten essentielle Aktivitäten zur Prüfung der Möglichkeiten einer Festlegung von Anschlussbedingungen ressourcenbedingt zurückgestellt werden.

Die Gesamtsteuerung Registermodernisierung begegnet diesen Herausforderungen proaktiv: Sie betreibt u.a. die Herbeiführung erforderlicher Beschlusslagen zur Sicherstellung einer mehrjährigen Finanzierung in enger Abstimmung mit der FITKO, baut auf Basis eines im März 2022 etablierten Controllings ein Risikomanagement auf und entwickelt eine meilensteinbasierte Ressourcenplanung als Basis konsequenter Priorisierung. Auch unter weiterer Ausschöpfung gegensteuernder Maßnahmen zeigt sich aus Sicht der Federführer jedoch deutlich: ohne einen personellen Ressourcenaufwuchs in der Gesamtsteuerung auf Basis einer mehrjährigen Finanzierungsgrundlage ist die Zielerreichung der durch den IT-Planungsrat beschlossenen Umsetzungsplanung gefährdet.

1.1 Technische Architektur

Bisherige Arbeitsergebnisse

Das Kompetenzteam (KT) Architektur hat sich in enger Zusammenarbeit mit dem KT EU-Interoperabilität im Q1 2022 intensiv mit der Validierung der einheitlichen Komponenten des Zielbildes beschäftigt und dem Lenkungskreis Registermodernisierung folgende Fragestellungen zur Entscheidung vorgelegt. Auf dieser Basis hat der Lenkungskreis folgende Richtungsentscheidungen getroffen, die nun mit den Fachministerkonferenzen abgestimmt werden sollen:

- **Unterstützung asynchroner Prozesse in der Architektur der Registermodernisierung:** Im bisherigen Zielbild waren sowohl fachlich synchrone[1] als auch fachlich

[1] Die Begriffe synchron und asynchron sind nicht im engen technischen Sinne zu verstehen, sondern in ihrer Eignung für direkte Nutzerinteraktion. „Synchron“ in diesem Sinne ist der Nachweisabruf, wenn der Nachweis innerhalb weniger Sekunden zur Verfügung steht. „Asynchron“ hingegen erlaubt eine fast beliebige Dauer zwischen dem Nachweisabruf und der Bereitstellung des Nachweises – von Minuten bis zu mehreren Tagen.

asynchrone Nachweisabrufe vorgesehen. Für die Behörde-zu-Behörde-Kommunikation soll dies weiterhin bestehen bleiben. Für Zugriffe aus Onlineverfahren sollen jedoch – analog zur Umsetzung im europäischen Once-Only-Technical-System (EU-OOTS) – nur fachlich synchrone Nachweisabrufe unterstützt werden. Dadurch können Komplexitätstreiber, z.B. im Bereich Preview, vermieden werden.

- **Entwicklung eines allgemeinen Standards für den Nachweisabruf für die nationale Registermodernisierung:** Der einheitliche Standard soll sicherstellen, dass der Nachweisabruf bei den Data Providern zu grundsätzlich gleichen rechtlichen, organisatorischen und technischen Bedingungen erfolgt und die Data Consumer davon entlasten, für verschiedene Nachweise jeweils neue Fachstandards und deren Schnittstellen implementieren zu müssen. Der zu entwickelnde Standard für das nationale Once-Only-Technical-System (NOOTS) soll auf dem der EU-Kommission basieren und nur dann abweichen, wenn dies aufgrund nationaler Anforderungen erforderlich ist. Es ist beabsichtigt, die Verwendung des Standards als Teil der Anschlussbedingung an das technische System verbindlich vorzugeben.
- **Einführung eines Reifegradmodells für den Nachweisabruf und Ausrichtung des NOOTS auf Reifegrad D:** Entscheidung zur Einführung eines vierstufigen Reifegradmodells für den Nachweisabruf im NOOTS und Festlegung auf Reifegrad C als Mindestziel der Registermodernisierung im nationalen Kontext.

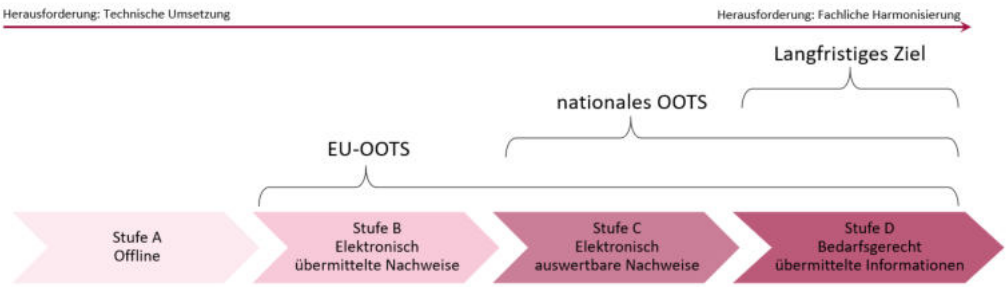


Abbildung 1: Reifegradmodell für die Registermodernisierung

Die Erreichung des Reifegrads C fördert den medienbruchfreien und automatisiert verarbeitbaren Abruf von Nachweisen und kann als kritischer Erfolgsfaktor der Umsetzung der Registermodernisierung angesehen werden. Als langfristiges Ziel ist Reifegrad D anzustreben. Dabei ist Reifegrad D überall so schnell wie (technisch) möglich (und soweit fachlich nötig) zu realisieren. Register, bei denen es kurzfristig nicht möglich ist Reifegradstufe C zu erreichen, können ausnahmsweise in einer

Übergangszeit auch im Reifegrad B angebunden werden. Diese Übergangszeit sollte jedoch – ggf. auch rechtlich – begrenzt werden.

- **Entscheidung zur Umsetzung der Komponente Registerdatennavigation:** Die Registerdatennavigation stellt Funktionen zur Ermittlung der für einen Nachweistyp zuständigen Registerinstanz und notwendiger Verbindungsparameter bereit. Sie soll als zentraler Routing-Dienst (Routing as a Service) auf Grundlage des Deutschen Verwaltungsdiensteverzeichnis (DVDV) unter Wiederverwendung von geeigneten Bausteinen der Lösung FIT-Connect umgesetzt werden. Das KT Architektur wird Zielsetzung und Rahmenbedingungen ausarbeiten, die zur Formulierung eines Projektauftrags notwendig sind. Mit der Umsetzung soll die FITKO beauftragt werden.

Eine Entscheidungsvorlage für die Preview-Komponente konnte entgegen der ursprünglichen Planung noch nicht erstellt werden. Hierzu haben sich im Bereich der Planungen des EU-OOTS neue Entwicklungen ergeben, die zunächst abzuwarten und zu bewerten sind.

Entscheidungen im KT EU-Interoperabilität in Abstimmung mit dem KT Architektur:

- **Aufbau eines nationalen Data Service Directory und Nutzung des europäischen Evidence Brokers**: Entscheidung über eine nationale Implementierung des Data Service Directory (DSD) und die Nutzung der zentral bereitgestellten europäischen Lösung eines Evidence Brokers. Das Data Service Directory (DSD) stellt ein Verzeichnis aller Register zur Verfügung, die an das OOTS angebunden sind, und ermöglicht es, für einen konkreten Nachweisabruf das richtige Register zu identifizieren. Es muss dafür die Zuständigkeitslogiken der jeweiligen Domäne abbilden können. Das KT EU-Interoperabilität empfiehlt, die im Rahmen des NOOTS zu entwickelnde Komponente Registerdatennavigation, um DSD-Funktionalitäten zu erweitern.

Daneben hat das KT EU-Interoperabilität den nationalen SDG-Koordinator weiterhin bei den Verhandlungen zu den noch offenen Punkten der Gesamtarchitektur des EU-OOTS unterstützt. Hierbei konnten im Austausch mit der Europäischen Kommission wesentliche Verhandlungserfolge erzielt werden, u.a. bzgl. der Flexibilität zur Abbildung mitgliedsstaatsspezifischer Zuständigkeitslogiken und bei den expliziten Regelungen verschiedener Sonderfälle des Datenabrufs, mit denen Missbrauchsrisiken verhindert werden sollen. Es gelang der Europäischen Kommission im Berichtszeitraum allerdings weiterhin nicht, die notwendige Einigkeit über die Gesamtarchitektur unter den

Mitgliedstaaten zu erreichen. Das KT EU-Interoperabilität unterstützt den nationalen SDG-Koordinator daher auch laufend bei der Bewertung möglicher politischer Kompromissvorschläge für die Verhandlungen.

Darüber hinaus unterstützt das KT EU-Interoperabilität die Ressorts weiterhin bei der Identifikation der Online-Services und Register, die an das EU-OOTS angeschlossen werden müssen, und trägt damit auch zu einer besseren Datenbasis für die Verknüpfung von Leistungsdigitalisierung und Registermodernisierung bei.

Änderung im Zielbild

Die Arbeitsergebnisse aus dem Q1/2022 haben das Zielbild bisher bestätigt. Daher bleibt die grafische Darstellung im Zielbild unverändert.

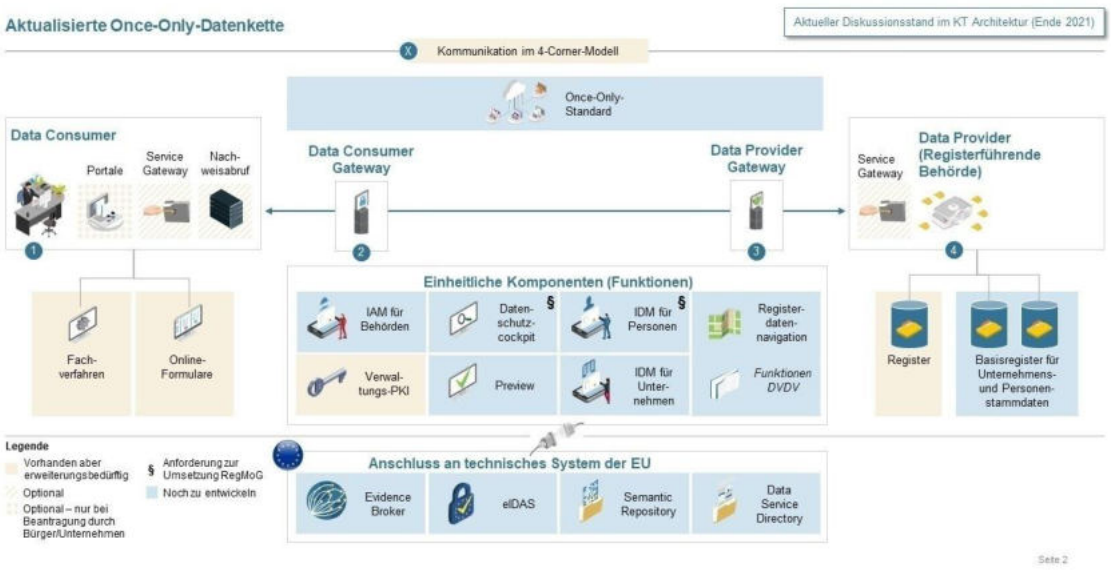


Abbildung 2: Zielbild Registermodernisierung

Ausblick auf die technische Architektur Q2 / 2022

Im zweiten Quartal 2022 sollen die folgenden Themen bearbeitet werden:

- Fortführung der Validierung des Zielbilds mit Schwerpunkt auf die folgenden Komponenten:
    - Vermittlungsstellen
    - Identity Access Management (IAM) für Behörden
    - Identity Management (IDM) für Unternehmen

- Konkretisierung der Aufgaben von Kopfstellen im europäischen Once-Only-Technical-System (EU-OOTS).
- Umsetzung einer Preview-Komponente für das nationale Once-Only-Technical-System (NOOTS).
- Ausarbeitung des Projektauftrags für die Registerdatennavigation.
- Erarbeitung einer abgestimmten Basis für die Entwicklung des Once-Only-Standards.
- Prüfung, ob der Ansatz von Kopfstellen auch auf das nationale Once-Only-Technical-System (NOOTS) übertragen werden kann, um dort die Anbindung bestehender Informationsverbünde zu vereinfachen.
- Weitere konzeptionelle Ausarbeitung des Zusammenspiels des nationalen Once-Only-Technical-Systems (NOOTS) mit Portalen und Fachverfahren.
- Klärung der nicht-funktionalen Anforderungen im Bereich der IT-Sicherheit an das nationale Once-Only-Technical-System (NOOTS) und seine Komponenten.

1.2 Weiterentwicklung von Registern

Die Arbeiten an den anstehenden Meilensteinen wurden im Rahmen vorhandener Ressourcen aufgenommen. Hierzu wurden entsprechende Arbeitspakete definiert, Verantwortlichkeiten festgelegt und erste Schritte zur Umsetzung begonnen. Die Entwicklung eines Vorgehensmodells zur Weiterentwicklung von Registern und die Durchführung von Pilotierungen weisen hohe Abhängigkeiten zur Konkretisierung der Architektur auf. Ohne konkretisierte technische Anforderungen kann die Weiterentwicklung von Registern nicht zielgerichtet betrieben werden. Aufgrund begrenzter Ressourcen mussten Aktivitäten in der Säule „Weiterentwicklung Register“ daher zugunsten der Erzielung von Validierungsergebnissen in der Säule „Technische Architektur“ teilweise zurückgestellt werden.

Die Kommunikation mit den Top-18/51 Registern wurde intensiv fortgesetzt, um auf dieser Basis einen Rolloutplan für die Einspeicherung der Identifikationsnummer (IDNr) nach IDNrG zu entwickeln. Neben der Frage der durch die Register zu erfüllenden Anforderungen für die Einführung der IDNr sind dazu insbesondere ein Vorgehensmodell und Priorisierungskriterien zu entwickeln.

Zudem wurden vorbereitende Aktivitäten für das Kompetenzteam Register bearbeitet, das ab Anfang des 2. Quartals seine Arbeit aufnehmen wird. Zu seinen Aufgaben gehören unter anderem Analysen im Registerbereich, die Unterstützung registerführender Stellen beim Anschluss an das NOOTS und seiner Komponenten, die Entwicklung von Vorgaben für den Aufbau neuer Register, die Begleitung der Umsetzung der im Zielbild definierten neuen Register sowie die Prüfung der „Register Factory“ des BVA hinsichtlich der Nutzbarkeit als Grundlage einer einheitlicheren und wirtschaftlicheren Umsetzung von Registern.

Exploration einer grenzüberschreitenden Once-Only-Pilotierung

Im Rahmen der „Gesamtsteuerung Registermodernisierung“ werden derzeit Möglichkeiten und konkrete Umsetzungsrahmen für grenzüberschreitende Once-Only-Pilotierungsvorhaben im Kontext der SDG-Umsetzung ausgelotet. Ziel ist es grenzüberschreitende Once-Only-Verfahren mit Nutzen für Bürgerinnen und Bürger sowie die Wirtschaft zu pilotieren und dabei skalierbare Erkenntnisse für die nationale Umsetzung des Art. 14 der SDG-Verordnung in Deutschland zu gewinnen. Konkret findet derzeit eine Exploration mit den Niederlanden zur Erprobung der Erfüllung des Once-Only-Prinzips in ausgesuchten Use Cases unter Nutzung des Wirtschafts-Service-Portals NRW (WSP.NRW) statt. Der Schwerpunkt liegt auf der Anschlussfähigkeit des nationalen Systems (NOOTS) an das OOTS der EU-Kommission und der Pilotierung eines grenzüberschreitenden Datenaustauschformats, das sich weitestgehend an den Vorgaben im OOTS orientiert.

In den verabredeten Use Cases soll die Entwicklung eines sog. „SDG-Connectors“ als technische Lösung für den Anschluss des NOOTS an das OOTS der EU untersucht werden. Dieser ist erforderlich, um grenzüberschreitend zwischen den verschiedenen technischen Systemen der EU-Mitgliedstaaten einen Datenaustausch zu ermöglichen. Es handelt sich um eine zentral bereitzustellende Software, welche technische Grundfunktionalitäten, die für den Anschluss an das europäische bzw. nationale technische System kapselt und zwischen unterschiedlichen Formaten vermittelt. Hierbei sollen neben einer Bewertung einer Entwicklung aus Österreich auch die seitens der Niederlande gewonnen Erfahrungen aus dem bis Ende 2022 laufenden EU-Large-Scale-Pilotvorhaben „Digital Europe 4 all“ (DE4A) einfließen. Deutschland wird durch eine beobachtende Teilnahme (observer-role) an den Ergebnissen von DE4A partizipieren und diese im Rahmen der Pilotierung nutzen, soweit damit eine SDG-konforme Umsetzung befördert werden kann.

In Zusammenarbeit mit den Niederlanden werden derzeit Möglichkeiten der Pilotierung grenzüberschreitenden Gewerbeanzeige nach dem Once-Only-Prinzip mit Nachweisen aus

den Handelsregistern des jeweils anderen Landes geprüft. Es handelt sich hierbei um ein SDG-relevantes Verfahren nach Anhang 2 der Verordnung (EU) 2018/1724) mit konkretem Entlastungspotential für die Wirtschaft im Binnenmarkt. Im ersten Teilprojekt könnte die Umsetzung des Once-Only-Prinzips (d.h. aus Nutzersicht „nachweisfreie“ Verwaltungsleistung) beim Anwendungsfall „ein niederländischer Einzelunternehmer stellt eine Gewerbeanzeige im WSP.NRW“ pilotiert werden. Im zweiten Teilprojekt soll reziprok der Use-Case der „nachweisfreien“ Gründung eines deutschen Unternehmens in den Niederlanden pilotiert werden.

Derzeit werden in einer Explorationsphase die Rahmenbedingungen für die grenzüberschreitende Zusammenarbeit mit den Niederlanden erarbeitet. Diese Phase wird bis April 2022 abgeschlossen. Sollten die beteiligten Akteure im Ergebnis eine Pilotierung befürworten, könnte diese im Mai / Juni 2022 initiiert werden.

Standardisierte Ausgangsschnittstelle des Basisregisters für Unternehmen im Kontext von XUnternehmen

Das Basisregister für Unternehmen sieht eine Schnittstelle zu den sog. angebundenen Registern vor, über die Abrufe und Mitteilungen aus dem Basisregister an die angebundenen Register erfolgen können. Diese Ausgangsschnittstelle des Basisregisters soll standardisiert werden. Eine entsprechende Bedarfsmeldung an die Koordinierungsstelle für IT-Standards (KoSIT) sieht die Erstellung eines entsprechenden Fachmoduls im Standard XUnternehmen vor.

1.3 Rechtliche Grundlagen

Die Arbeiten im KT Recht/ Datenschutz konnten fortgesetzt werden. Dabei sind die Aufgaben vorwiegend im Kernteam Recht bearbeitet worden. Bei Fragen mit datenschutzrechtlichem Schwerpunkt hat sich das Kernteam Recht mit Datenschutzvertretern der Federführer sowie mit Vertretern der Kontaktgruppe der Datenschutzkonferenz (DSK) ausgetauscht und in dieser Zusammensetzung als KT Recht/Datenschutz zusammengearbeitet. Thematischer Schwerpunkt war hier die Befassung mit der Once-Only-Generalklausel, hinsichtlich derer jedoch noch grundlegende verfahrensrechtliche und kompetenzrechtliche Fragen der Klärung bedürfen. Aufgrund knapper Ressourcen im Kernteam Recht sowie aufgrund pandemiebedingter Abwesenheiten konnten nicht alle gesteckten Meilensteine für das erste und zweite Quartal 2022 vollumfänglich erreicht werden. Der seitens der Kommission erst Ende März an die

Mitgliedstaaten erfolgte Versand der aktualisierten Dokumente zu Art. 14 der SDG-VO (Implementing Act und Technical Design Documents) hat die inhaltliche Finalisierung der Arbeiten weiter verzögert.

Ergebnisse zur Klärung rechtlicher Fragen zum OOTS gemäß Art. 14 SDG-VO inklusive noch möglicher offener Fragen

Das Kernteam Recht hat die Antworten auf die gemeinsam mit dem KT EU-Interoperabilität am höchsten priorisierten Rechtsfragen zum OOTS im Hinblick auf die laufenden Abstimmungen zum Durchführungsrechtsakt gemäß Art. 14 Abs. 9 SDG-VO aktualisiert. Die aktualisierten Antworten hat das Kernteam den Datenschutzexpertinnen und –experten der Federführer, den SDG-Koordinatoren der Länder sowie den jeweiligen rechtlichen Ansprechpartnern vorgelegt und die konsolidierten Ergebnisse dem KT EU-Interoperabilität zur Verfügung gestellt. Ein neuerlicher Aktualisierungsbedarf kann sich aus den andauernden Verhandlungen zum Durchführungsrechtsakt ergeben. Die Kommission hat den Mitgliedstaaten zuletzt am 25.03.2022 eine aktualisierte Fassung übermittelt, auf deren Grundlage die Verhandlungen mit den Mitgliedstaaten fortgesetzt werden.

Das Kernteam Recht hat in Abstimmung mit dem KT EU-Interoperabilität neue Fragen zum OOTS in den Prüffragenkatalog[2] aufgenommen und die wichtigsten offenen Fragen entsprechend ihrer Priorität bearbeitet. Die Prüfergebnisse werden – soweit sie einen datenschutzrechtlichen Schwerpunkt haben – den Datenschutzexpertinnen und –experten der Federführer, bei grundsätzlicher Bedeutung den Vertretern der Kontaktgruppe der DSK und im Anschluss den SDG-Koordinatoren sowie den jeweiligen rechtlichen Ansprechpartnern der Länder zur Stellungnahme übersandt. Nach der Finalisierung werden sie dem KT EU-Interoperabilität übergeben.

Leitfaden zur Auslegung Art. 14 SDG-VO

Das Kernteam Recht hat einen Leitfaden zur Auslegung des Art. 14 SDG-VO und zur Ermittlung sich daraus ergebender Rechtsänderungsbedarfe zur grenzüberschreitenden Umsetzung des Once-Only-Prinzips als Arbeitshilfe entwickelt. Der Leitfaden wurde im SDG-Netzwerk geteilt (Version 2.8, Stand: 29.03.2022), das aus Fachreferentinnen und –referenten des Bundes und der Länder mit SDG-Bezug besteht. Der Leitfaden dient der einheitlichen Auslegung des Art. 14 SDG-VO, insbesondere des Anwendungsbereichs nach

[2] Der Prüffragenkatalog listet alle Projekt-Rechtsfragen auf und dient dem Kernteam Recht zur internen Organisation.

Art. 14 Abs. 2 SDG-VO, sowie der Unterstützung der Fachverantwortlichen bei der Analyse etwaiger Rechtsänderungsbedarfe und deren Umsetzung. Dieser Stand wird vor dem Hintergrund der geänderten Bestimmungen zu den Verantwortlichkeiten des Evidence Requesters und Evidence Providers des Durchführungsrechtsakts nach Art. 14 Abs. 9 SDG-VO, diesbezüglicher laufender Verhandlungen der Kommission mit den Mitgliedstaaten und mit Blick auf den Abstimmungsstand zur Once-Only-Generalklausel aktualisiert werden.

Ergebnisse zur Klärung rechtlicher Fragen zum NOOTS

Die Gesamtsteuerung Registermodernisierung hat im letzten IT-Planungsratsbericht zum Umsetzungsstand der Registermodernisierung[3] die Notwendigkeit eines Nationalen Once-Only-Technical-System (NOOTS) erläutert und das Vorhaben, im Zuge der weiteren Arbeiten einen Beschlussvorschlag zur Umsetzung eines NOOTS vorzulegen, dargestellt. Im Zusammenhang mit einem NOOTS ergeben sich Rechtsfragen, die das KT Architektur an das KT Recht/ Datenschutz übergeben hat. Diese wurden in den Prüffragenkatalog aufgenommen und durch das KT Architektur priorisiert. Die wichtigsten Fragen prüft das Kernteam Recht parallel zu den Rechtsfragen des KT EU-Interoperabilität. Neben den spezifischen Rechtsfragen stellen sich vor allem folgende rechtliche Grundsatzfragen.

Möglichkeit einer Verordnungsermächtigung zur Festlegung der Anschlussbedingungen

Dieser Meilenstein war für Q2 2022 geplant. Er konnte aufgrund fehlender Kapazitäten im Kernteam Recht nicht erreicht werden. Hier wäre insbesondere eine enge Abstimmung mit den KT EU-Interoperabilität und Architektur erforderlich gewesen, weil die Frage der inhaltlichen Gestaltung einer Verordnungsermächtigung und möglicher auf dieser Grundlage festzulegender Anschlussbedingungen Voraussetzung und Kernbestandteil der rechtlichen Prüfung gewesen wäre.

Grundsätzliche Realisierbarkeit des Konzepts von Kopfstellen für angeschlossene Register und deren Verhältnis zueinander

Die rechtliche Prüfung der grundsätzlichen Realisierbarkeit des Konzepts von Kopfstellen für angeschlossene Register und deren Verhältnis zueinander wird zeitnah in einem Workshop mit dem KT EU-Interoperabilität und dem KT Architektur gemeinsam diskutiert

[3] Anlage zum Beschluss 2022/06, beschlossen auf der 37. Sitzung des IT-Planungsrats am 09.03.2022, abrufbar unter https://www.it-planungsrat.de/beschluss/beschluss-2022-06, zuletzt abgerufen am 29.03.2022.

und erarbeitet. Dieser Meilenstein war bereits für Q1 2022 geplant. Eine frühere Bearbeitung war aufgrund fehlender Kapazitäten im Kernteam Recht zu einem früheren Zeitpunkt nicht möglich.

Möglichkeit einer Once-Only-Generalklausel

Das Kernteam Recht hat die Möglichkeit einer Generalklausel für Once-Only-Datenabrufe über das EU-OOTS und NOOTS im Sinne einer gesetzlichen Verarbeitungsbefugnis, um die Notwendigkeit fachgesetzlicher Änderungen zu reduzieren, geprüft. Der erste Entwurf einer solchen Generalklausel wurde in Interviews mit Expertinnen und Experten aus Wissenschaft und Forschung, aus Österreich zwecks eines Rechtsvergleichs sowie mit Expertinnen und Experten aus den Teilprojekten der Registermodernisierung evaluiert. Die Ergebnisse dienten als Ausgangspunkt für die gemeinsamen Abstimmungstermine mit den Datenschutzvertretern der Federführer sowie den Vertretern der Kontaktgruppe der DSK. Nächster thematischer Schwerpunkt wird sein, den verfahrensrechtlichen und kompetenzrechtlichen Rahmen einer Once-Only-Generalklausel zu erheben.

Verordnung zu XBasisdaten auf Grundlage von § 12 IDNrG

Nachdem der IT-Planungsrat in seiner 37. Sitzung am 09.03.2022 gem. § 12 Abs. 3 Nr. 3 IDNrG sein Benehmen zur Verordnung zur Einführung eines Datenübermittlungsstandards XBasisdaten (XBasisdaten-Verordnung – XBasisdatenV) erklärt hat, wurde diese am 01.04.2022 im Bundesgesetzblatt[4] verkündet. Die Verordnung ist die rechtliche Grundlage für den Standard XBasisdaten, der für den elektronischen Datenaustausch der registerführenden Stellen und weiteren öffentlichen Stellen mit der Registermodernisierungsbehörde (BVA) im Rahmen des Identitätsdatenabrufs nach dem Identifikationsnummerngesetz (IDNrG) genutzt werden soll. Der Standard wurde in der Version 1.0 vom BVA veröffentlicht, ist öffentlich zugänglich und wird somit den registerführenden Stellen nach dem IDNrG zur Umsetzung entsprechender Schnittstellen frühzeitig bereitgestellt.

1.4 Governance

[4] Bundesgesetzblatt I Nr. 12 vom 1. April 2022, abrufbar unter https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=%2F%2F%2A%5B%40attr_id=%27bgbl122s0601.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl122s0601.pdf%27%5D__1649070712927, zuletzt abgerufen am 04.04.2022.

Die Projektstrukturen des Projekts „Gesamtsteuerung Registermodernisierung“ sind weitgehend aufgebaut.

Die konstituierende Sitzung des Registerbeirats ist für den19.5.2022 vorgesehen. Der Wissenschafts- und Innovationsbeirat wird seine konstituierende Sitzung voraussichtlich im Juni/ Juli 2022 abhalten.

Das Controlling im Hinblick auf die Teilprojekte der Registermodernisierung und die geplanten Meilensteine der Gesamtsteuerung Registermodernisierung ist etabliert. Der Lenkungskreis wird vierteljährlich über den Stand des Projekts informiert. In der Transformationseinheit werden der Stand des Gesamtvorhabens dargelegt und notwendige Entscheidungsbedarfe diskutiert. Daneben wird ein Risikomanagement unter Berücksichtigung der wechselseitigen Abhängigkeiten von Meilensteinen aufgebaut.

Zur Entwicklung einer Ziel-Governance für den laufenden Betrieb einer modernisierten Registerlandschaft („Betriebsgovernance“) ist ein Vorgehen – insbesondere unter Einbeziehung des KT Architektur – abgestimmt, das nun umgesetzt werden soll.

1.5 Querschnittsthemen

Once-Only-Schnittstelle

Im letzten Bericht zum Umsetzungsstand des Projekts „Gesamtsteuerung Registermodernisierung“ wurde bereits dessen Bedeutung für die Realisierung des OZG-Reifegrades 4 erläutert. Darüber hinaus konnte ein zehnstufiges Vorgehensmodell zur Planung einer verzahnten Umsetzung des Once-Only-Prinzips im Rahmen der Registermodernisierung entwickelt und vorgestellt werden (vgl. Abbildung 2).

Entsprechend dem Beschluss in der 37. Sitzung des IT-PLRs wird im Folgenden eine Empfehlung zur Entwicklung einer zusammengeführten Datenbasis zur Identifizierung von Once-Only-Potentialen abgeben. Damit bewegen wir uns in den Stufen 1 und 2 des Verfahrenskonzepts.

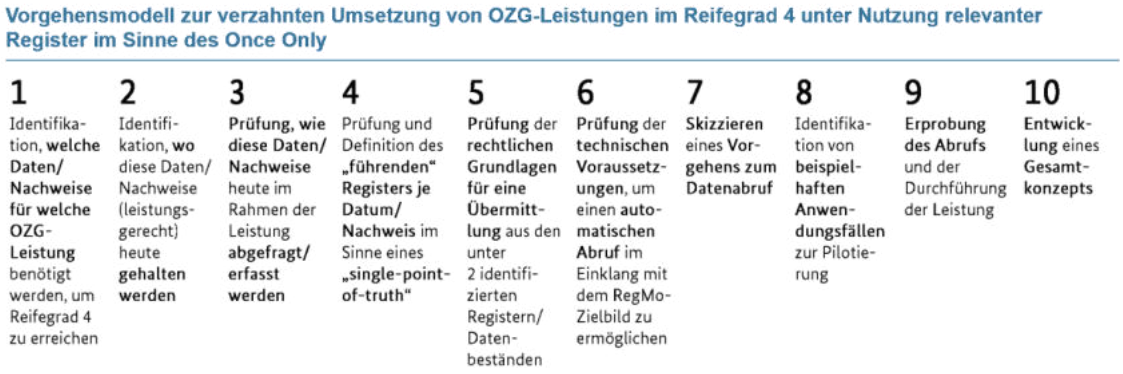


Abbildung 3: Vorgehensmodell zur verzahnten Reifegrad 4-Umsetzung unter Nutzung relevanter Register im Sinne des Once-Only-Prinzips

Sachlage zu aktuellen Datenbeständen

Die Datenbasis soll die Beantwortung zwei verschiedener Fragen leisten:

1. Welche Daten und Nachweise werden für welche OZG-Leistung benötigt, um den Reifegrad 4 zu erreichen?
2. In welchen Registern werden diese Daten und Nachweise gehalten bzw. welche Daten verfügen derzeit über kein Register?

Die Recherche zur Identifikation einer geeigneten Datenquelle zur Beantwortung der Fragen zeigte, dass bisher kein umfassender Datensatz, aus dem sich alle erforderlichen Erkenntnisse ableiten lassen, vorliegt. Die erste Frage kann derzeit nur unspezifisch beantwortet werden. Dienlich zeigt sich dazu der Datenbestand des „Portalverbund Online Gateway“ (PVOG). Zu einer Leistung können unterschiedliche landes- oder kommunalspezifische Nachweisanforderungen vorliegen. Um diese Problematik zu lösen, lohnt sich ein Blick auf die europäische Ebene. Im Rahmen der Umsetzung der SDG-VO wird aufgrund notwendiger nationaler Vorarbeiten für den sog. „Evidence Survey“ (Übersicht über alle Nachweistypen, die zur Erfüllung der aus der SDG-Verordnung resultierenden Verpflichtungen erforderlich sind) geprüft, welche Nachweistypen beim grenzüberschreitenden Verfahrensablauf benötigt werden und in welchen Registern diese abgerufen werden können. Der Evidence Survey bildet dabei die Datenbasis für die Übersetzung und Zuordnung zwischen verfahrensbezogenen Nachweisanforderungen des Online Services in einem Mitgliedstaat zu den Nachweistypen anderer Mitgliedstaaten. Folgende Ergebnisse werden im Rahmen der deutschen Vorarbeiten für die Evidence Survey in der nächsten Arbeitsphase (Q2-Q4 2022) erzielt:

1. Liste der SDG-2-relevanten LeiKa-Leistungen: Erhebung und fachliche Freigabe aller deutscher Verfahren (LeiKa-Leistungen), die den in Art. 14 SDG-VO genannten SDG-Verfahren zuzuordnen sind.
2. Liste der SDG-2-relevanten verfahrensbezogenen Nachweisanforderungen: Erhebung der verfahrensbezogenen Nachweisanforderungen (die zu beweisenden Tatsachen) für jede SDG-2-relevante LeiKa-Leistung.
3. Liste SDG-2-relevanter Nachweistypen: Jene Nachweistypen, mit denen die verfahrensbezogenen Nachweisanforderungen bewiesen werden können. Ergänzend werden Informationen zum Digitalisierungsstand der benötigten Nachweistypen erhoben.
4. Liste der Register und registerführenden Stellen, die die benötigten Nachweistypen führen.

Aufgrund der Überschneidung im Vorgehen wird empfohlen, das Vorgehen im Rahmen des Once-Only-Datenaustausches im NOOTS und im OOTS aufeinander abzustimmen, um eine Doppelbearbeitung und unterschiedliche Ergebnisdokumentation zu vermeiden. Zudem wird nahegelegt, die Unterscheidung von Nachweisanforderungen und Nachweistypen auch im Kontext der Registermodernisierung zu verwenden.

Die Frage nach dem Ort der Datenaufbewahrung lässt sich mit der Hinzunahme der vom BVA bereitgestellten Registerübersicht ermitteln. Die Datenbank dient als Zwischenlösung auf dem Weg zur Registerlandkarte, welche nach §3 Abs. 1 IDNrG von der Registermodernisierungsbehörde bereitzustellen ist. Sie enthält derzeit Informationen zu den 51 im Anhang des IDNrG genannten Registern und wird monatlich aktualisiert den Federführenden der Gesamtsteuerung Registermodernisierung zur Verfügung gestellt.
Die Metadaten zu den Registern konnten der vom Statischen Bundesamt betriebenen Verwaltungsdateninformationsplattform (VIP) entnommen werden. Zusätzlich wurden bereits Informationen aus der OZG-Informationsplattform ergänzt. Dadurch ist eine noch nicht bestätigte Zugehörigkeit von LeiKa-Leistung zu den einzelnen Registern erfolgt. Die Registerübersicht schafft damit nicht nur den vordergründig erwünschten Überblick über die Anschlussfähigkeit von Registern, sondern kann auch zur Anbindungsplanung von Verwaltungsleistung genutzt werden. Das Projekt wird in Kooperation mit dem Statistischen Bundesamt stetig weiterentwickelt und auf weitere Register ausgeweitet. Im dritten Quartal 2023 sollen die Daten dann frei zugänglich veröffentlicht werden. Zudem wird in Erwägung gezogen durch Befragung der registerführenden Stellen die bisherigen Erkenntnisse zu validieren und zu spezifizieren.

Mit einem „Matching“ aus bei den Registern vorliegenden und den benötigten Nachweisen aus der Leistungsperspektive, lässt sich ermitteln, welche Leistungen derzeit noch nicht in einem Register gehalten werden und an welcher Stelle es ggf. den Aufbau neuer bzw. der Erweiterung bestehender Registerdaten bedarf. Daher wird empfohlen die Registerübersicht als zentrales Planungstool zu verwenden und durch die Datenintegration aus dem „Portalverbund Online Gateway“ (PVOG) und der OZG-Informationsplattform eine umfangreiche Datenbasis zu schaffen.

Finanzierung

Die Finanzierung der Aufwände der federführenden Länder für das Projekt „Gesamtsteuerung Registermodernisierung“ erfolgte für die Jahre 2021 und 2022 aus dem Digitalisierungsbudget, welches Ende des Jahres 2022 ausläuft. Ob es in den Folgejahren ein weiteres Digitalisierungsbudget geben wird, ist offen.

Der IT-Planungsrat hat daher in der 37. Sitzung die Federführer der Gesamtsteuerung Registermodernisierung beauftragt, einen mit der FITKO abgestimmten Vorschlag zur Finanzierung eines Budgets für die weitere Programmsteuerung ab dem Jahr 2023 auszuarbeiten.

Um die Fortführung der Gesamtsteuerung Registermodernisierung über das Jahr 2022 sicherzustellen, wurde mit der FITKO abgesprochen, dass die Mittel im Stammbudget der FITKO aufgenommen werden. Aufgrund einer groben Schätzung durch die federführenden Länder wurde im Wirtschaftsplan 2023 ein Betrag in Höhe von 7,44 Mio. € eingeplant. Für die mittelfristige Finanzplanung der Jahre 2024-2026 wurde dieser Betrag mit einer Steigerung von 3% fortgeschrieben.

Dies ist aus Sicht der Gesamtsteuerung Registermodernisierung derzeit eine schnelle und akzeptable, aber nicht die optimale Lösung.

Nach Beschluss des IT-Planungsrats über den Wirtschaftsplan der FITKO wird dieser zur Genehmigung der Finanzministerkonferenz der Länder sowie dem BMI und BMF vorgelegt. Dies wird voraussichtlich erst in der 2. Jahreshälfte 2022. Erst danach können die Federführer davon ausgehen, dass die Mittel 2023 zur Verfügung stehen.

Hinsichtlich der Planungen ab 2024 stehen die Mittel unter Haushaltsvorbehalt und sind somit nicht gesichert.

Das ist für die weitere Programmplanung ein großes Hindernis, da die federführenden Länder infolge der Jährlichkeit des FITKO-Wirtschaftsplans keine kontinuierlich verfügbaren Personalressourcen bis zum Programmende aufbauen können, sondern immer nur befristete Stellen zur Verfügung haben. Angesichts der sehr guten Lage auf dem Arbeitsmarkt ist es fast unmöglich, fachlich kompetentes Personal auf befristete Stellen einzustellen. Auch die Dienstleister haben nur begrenzte Kapazitäten und benötigen langfristige Planungen, um das Personal vorzuhalten.

Daher erachten es die Federführenden als essentiell, die kontinuierliche Finanzierung bis zum Ende des Projekts zeitnah zu sichern. Dies könnte z.B. über ein weiteres auf mehrere Jahre angelegtes Budget „Gesamtsteuerung Registermodernisierung“ im Rahmen eines neuen Digitalisierungsbudgets erfolgen.

Weiteres Ziel ist, Bund und Ländern (auch mit Blick auf deren Kommunen) kontinuierlich ergänzende Informationen als Grundlage für die zukünftige Haushaltsvorsorge zur Finanzierung der Gesamtkosten Registermodernisierung zur Verfügung zu stellen. Dies soll auf Basis von Entscheidungen zur IT-Architektur, von Rückmeldungen der Länder zu dem bereits entwickelten Aufwandschätzmodell (ASM) und der Prüfung der bisher im ASM genannten 54 Aufwandstreiber Aufwandsschätzmodell im Rahmen eines Workshops durch die Federführenden erfolgen.

Kommunikation, Change- und Stakeholdermanagement

Das Kommunikations- und Stakeholdermanagement für die Gesamtsteuerung Registermodernisierung verantworten der Bund und Hamburg. Unterstützt werden sie dabei durch das BVA und Baden-Württemberg.

<u>Kommunikationsplan der Gesamtsteuerung Registermodernisierung</u>

Dem Kommunikationsplan ging eine Stakeholderanalyse voraus. Es wurden drei verschiedene Stakeholdergruppen identifiziert:

- Konzeptionsbeteiligte:
  Stakeholder, die in das Steuerungsprogramm Registermodernisierung bzw. die Bund-Länder-Transformationseinheit eingebunden sind.
- Umsetzungsbeteiligte:
  Registerführende Behörden, Ressorts und föderale Akteure der 51 im Identifikationsnummerngesetz genannten Register.

- Weitere Stakeholder
  Stakeholder, die direkt oder indirekt durch die Registermodernisierung betroffen sind und ggf. Einfluss auf die inhaltliche und rechtliche Ausgestaltung des Vorhabens Registermodernisierung haben.

Konzeptions- und Umsetzungsbeteiligte werden primär über Push-Kommunikation angesprochen. Das heißt, sie werden durch die Gesamtsteuerung Registermodernisierung oder das BVA direkt angesprochen. Dazu gehören Informationsschreiben, Gespräche mit einzelnen Stakeholdern und Veranstaltungen für einzelne Stakeholdergruppen, sogenannte „Austausche Registermodernisierung“. So hat das BVA am 27.4.2022 gemeinsam mit der Gesamtsteuerung Registermodernisierung einen Austausch Registermodernisierung für Kommunen als registerführende Behörden durchgeführt. Die Gesamtsteuerung Registermodernisierung informiert die Kommunen zusätzlich über Schreiben, welche über die kommunalen Spitzenverbände verteilt werden. Auch weitere Stakeholdergruppen werden zukünftig vermehrt schriftlich informiert.

Die weiteren Stakeholder Einfluss auf Entscheidungen werden ebenso durch Push-Kommunikation angesprochen, u. a. über das Forum Registermodernisierung. Dieses Veranstaltungsformat wurde bereits 2021 etabliert und wird als umfassend angelegte Informationsveranstaltung auch in den nächsten Jahren regelmäßig fortgeführt. Die Gesamtsteuerung Registermodernisierung und das BVA werden zudem zunehmend auf Fachkongressen präsent sein. Damit soll ein breites Fachpublikum erreicht werden. Einige Stakeholdergruppen werden auch über die Gremienarbeit kontinuierlich angesprochen, z.B. über ihre Mitgliedschaft im Lenkungskreis oder den Beiräten der Gesamtsteuerung Registermodernisierung.

Mindestens ebenso relevant für eine erfolgreiche Stakeholder-Ansprache ist die Pull-Kommunikation: Die Gesamtsteuerung Registermodernisierung stellt Informationen transparent für alle Interessierten bereit. Dabei zentral: Eine Webpräsenz. Informationen zur Registermodernisierung stehen der (Fach-)Öffentlichkeit deshalb auf https://ozg-umsetzung.de/registermodernisierung zur Verfügung und werden kontinuierlich erweitert.

Als zentralen Kontaktpunkt hat das BVA die E-Mail-Adresse Registermodernisierung@bva.bund.de eingerichtet. Zudem ist das BVA für registerführende Behörden immer der erste Ansprechpartner.

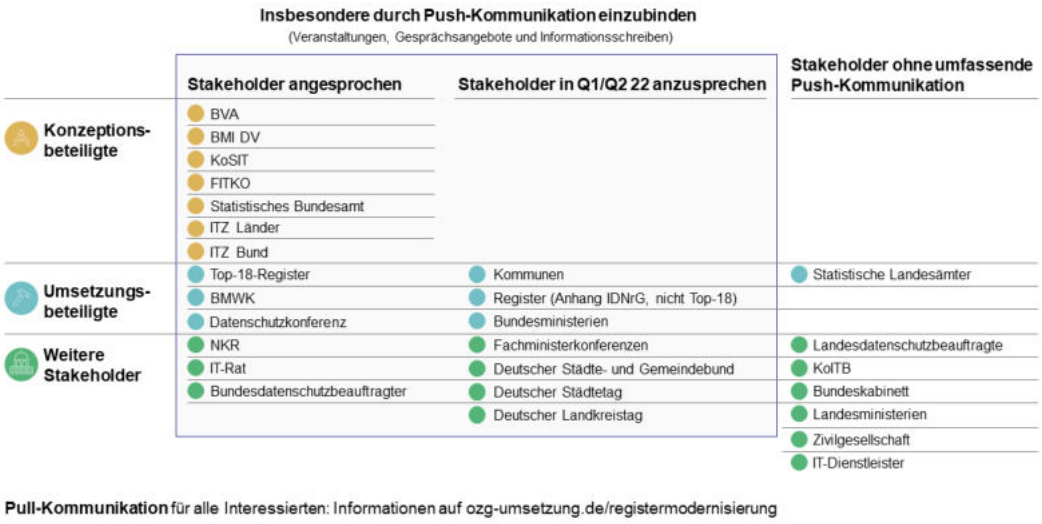


Abbildung 4: Stakeholdergruppen der Registermodernisierung

Einbindung der Fachministerkonferenzen

In Bezug auf den Beschluss in der 37. Sitzung des IT-PLRs hat die Gesamtsteuerung Registermodernisierung den Dialog mit den Fachministerkonferenzen (FMKen), die schwerpunktmäßig betroffen sind, eröffnet.

Dabei verfolgt die Gesamtsteuerung Registermodernisierung drei Ziele:

- Die FMKen und ihre Arbeitsgruppen können selbst für das Vorhaben Registermodernisierung sensibilisiert werden, indem sie (1) einen Überblick erhalten, welche Register in ihrem Bereich für die Registermodernisierung relevant sind und (2) Informationen über die nächsten Umsetzungsschritte und den Zeitplan der Gesamtsteuerung Registermodernisierung erhalten.
- Fachministerien und die Arbeitskreise der FMKen können aktiv die Einbindung der dezentralen Register unterstützen, indem sie (1) Informationen weiterleiten, (2) als zentrale Ansprechpartner für dezentrale Register fungieren und (3) auf Herausforderungen aufmerksam werden, vor denen speziell dezentrale Register bei der Modernisierung stehen – und diese in Richtung Gesamtsteuerung weitergeben.
- Betroffene Arbeitskreise werden aktiv in einzelnen Umsetzungsthemen mitarbeiten, indem die Gesamtsteuerung Registermodernisierung diese konsultiert und sie bei der Problemlösung integriert werden.

- Es erfolgt nach der Beratung im IT-Planungsrat eine Abstimmung mit den FMK, insbesondere, wenn in den jeweiligen Bereichen mit größeren fachlichen, finanziellen und personalintensiven Auswirkungen gerechnet werden muss.
- Auch bei der Vorbereitung von Beschlussfassungen des Lenkungskreises Registermodernisierung wird künftig die Herstellung von Einvernehmen mit betroffenen Fachministerkonferenzen angestrebt, um die Planungssicherheit für alle Beteiligten zu erhöhen.

Damit sollen die Fachministerkonferenzen zukünftig verstärkt in die Registermodernisierung integriert und eine Partizipation der bestehenden Informationsverbünde zügig ermöglicht werden.

2 Ausblick: Umsetzungsplanung bis Ende 2022

Die in der 37. Sitzung des IT-Planungsrates beschlossene Meilenstein- und Programmplanung bilden die Grundlage der Umsetzungsplanung bis Ende 2022.

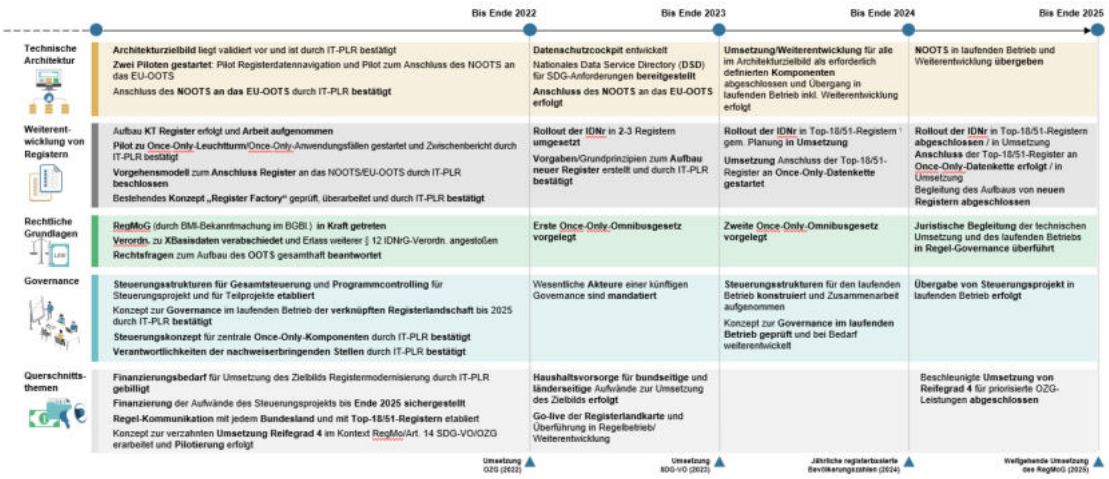


Abbildung 5: Meilenstein- und Programmplanung der Gesamtsteuerung Registermodernisierung

Technischen Architektur

- Im Fokus der Säule **Technische Architektur** stehen im weiteren Verlauf des dritten Quartals die Abstimmung eines validierten Architekturbildes, welches zum vierten Quartal finalisiert vorliegen und dem IT-PLR zur Beschlussfassung vorgelegt wird.
- Der Start des Pilotvorhaben Registerdatennavigation ist für das dritte Quartal eingeplant.

Weiterentwicklung von Registern

- Im Rahmen der Säule **Weiterentwicklung von Registern** sollen im dritten Quartal die Abstimmung zum Klärungsbedarf zur Bereinigung von Unstimmigkeiten (u.a. Datendoppelungen) zwischen Registermodernisierungsbehörde und den TOP-18/51 Register abgestimmt werden.
- Zentral zu klärende Frage wäre zum Ende des dritten Quartals wie die Übermittlungsanpassung von den Registern zum Datenschutzcockpit vollzogen wird.
- Die Piloten zu den Once-Only- Anwendungsfällen werden dem IT-PLR einen Zwischenbericht im vierten Quartal vorlegen.
- Es soll ein Vorgehensmodell zum Anschluss der Register an das Nationale OOTS sowie des EU-OOTS durch den IT-PLR beschlossen werden.
- Die im Zielbild genannten neu zu schaffenden Register sollen durch das KT Registern ab dem dritten Quartal begleitet werden.
- Das bestehende Konzept zur „Register Factory“ wird geprüft, überarbeitet und durch IT-PLR Ende Q3 bestätigt.
- Es werden die Vorgaben/Grundprinzipien zum Aufbau neuer Register erstellt und im Q4 durch IT-PLR bestätigt.

Rechtliche Grundlagen

- Der verfahrensrechtliche und kompetenzrechtliche Rahmen des Projekts ist zu klären.
- Bis zum Ende Q3 2022 wird der Ergänzungsbedarf zum RegMoG geprüft.
- Des Weiteren wird die Entscheidung für die Konzeption der Once-Only-Generalklausel getroffen.
- Im Q3 2022 sollen die Rechtsänderungsbedarfe für die grenzüberschreitende Umsetzung des Once-Only-Prinzips ressort- und länderübergreifend identifiziert sein.

- Die Notwendigkeit einer Verordnungsermächtigung zur Festlegung einer Anschlussverpflichtung an das NOOTS wird bis zum Ende des vierten Quartals 2022 geprüft.
- Der Erlass weiterer Verordnungen auf Grundlage des § 12 IDNrG wird bis Ende Q4 2022 angestoßen.
- Das Inkrafttreten des RegMoG soll bis Ende Q4 2022 veranlasst werden, sodass die Bekanntmachung des Eintritts der technischen Voraussetzungen nach Art. 22 RegMoG erfolgen kann.
- Zum Ende Q4 2022 wird das RegMoG (durch BMI-Bekanntmachung im BGBl.) in Kraft treten.

Governance

- Der Jahresstatusbericht Programm- und Projektcontrolling als Agendapunkt wird im vierten Quartal in die Videokonferenz der Federführer (VK der FF) aufgenommen.
- Mit Ende des vierten Quartals wird ein Project Management Office (PMO) als Unterstützung der Transformationseinheit eingesetzt und durch die TE bestätigt.
- Das Konzept zur Governance wird im laufenden Betrieb der verknüpften Registerlandschaft bis 2025 (und darüber hinaus) entwickelt und durch den IT-PLR im vierten Quartal bestätigt.
- Die Verantwortlichkeiten der nachweiserbringenden Stellen („Single Point of Truth“) inkl. Pflege des Prozesses sind durch IT-PLR im vierten Quartal bestätigt.
- Das Steuerungskonzept für zentrale Once-Only-Komponenten wird entwickelt und ist durch den IT-PLR im vierten Quartal bestätigt.

Querschnittsthemen

Finanzierung

- Finanzierung der Aufwände der Gesamtsteuerung werden zum Quartal 3 bis Ende 2025 sichergestellt.

Kommunikation

- Regel-Kommunikation mit Top-18/51-Registern zu Anforderungen und Umsetzungsfortschritt wird zu Ende Q2 2022 Quartale etabliert.

Registerlandkarte

- Die Kooperationsvereinbarung zwischen BVA und StBA soll zum Ende Q4 2022 abgeschlossen sein.

Abkürzungsverzeichnis

ASM	Aufwandsschätzmodell
BVA	Bundesverwaltungsamt
DE4A	„Digital Europe 4 all“
DSD	Data Service Directory
DSK	Datenschutzkonferenz
DVDV	Deutsches Verwaltungsdiensteverzeichnis
EU	Europäische Union
EU-OOTS	Europäisches Once-Only-Technical-System
EUR	Euro
FITKO	Föderale IT-Kooperation
FMK	Fachministerkonferenz
IAM	Identity Access Management
IDM	Identity Management
IDNr	Identifikationsnummer
IDNrG	Identifikationsnummerngesetz
IT-PLR	IT-Planungsrat
KOM	Europäische Kommission
KoSIT	Koordinierungsstelle für IT-Standards
KT	Kompetenzteam
Mio.	Millionen
NOOTS	Nationales Once-Only-Technical-System
NRW	Nordrhein-Westfalen
OOTS	Once-Only-Technical-System
OZG	Onlinezugangsgesetz
RegMoG	Registermodernisierungsgesetz
SDG	Single Digital Gateway
SDG-VO	SDG-Verordnung

Abbildungsverzeichnis

4. Sitzung des Lenkungskreises der Registermodernisierung

09.05.2022

TOP 2: Entscheidung zur Einführung eines Reifegradmodells für Nachweisabrufe und Ausrichtung des NOOTS auf Reifegrad D

1. **Der Lenkungskreis Registermodernisierung beschließt, das im Folgenden skizzierte Reifegradmodell für Nachweisabrufe einzuführen. Dabei sollte mindestens der Nachweisabruf-Reifegrad C erreicht werden. Das Ziel ist die Erreichung von Nachweisabruf-Reifegrad D.**
2. **Der Lenkungskreis Registermodernisierung beauftragt das Kompetenzteam Architektur, das nationale Once-Only-Technical-System (NOOTS) auf die Erreichung des Reifegrad D auszulegen und konkrete Vorschläge zu erarbeiten, wie der Reifegrad erreicht werden kann. Dazu sollen das Reifegradmodell weiter ausgearbeitet und die Konsequenzen der Reifegrade C und D detailliert werden.**
3. **Die Beschlüsse bedürfen der Zustimmung des IT-Planungsrates und einer hieran anschließenden Abstimmung mit den Fachministerkonferenzen.**

Sachverhalt: *(kurze Darstellung des Problems)*

Für die erfolgreiche Umsetzung des Once-Only-Prinzips in der öffentlichen Verwaltung müssen Data Consumer (Antrags- bzw. Fachverfahren) und Data Provider (registerführende öffentliche Stellen) umfassend digitalisiert werden, um einen medienbruchfreien und automatisierten Abruf von Nachweisen zu ermöglichen. Die Umsetzung der zugrundeliegenden fachlichen Anforderungen, die sowohl im nationalen als auch im europäischen Once-Only-Technical-System (OOTS) definiert ist, stellt einen kritischen Erfolgsfaktor bei der Umsetzung der Registermodernisierung dar.

Im Rahmen der Entwicklung des Architekturzielbilds für die Registermodernisierung hat das Kompetenzteam Architektur den Abruf von Nachweisen untersucht und ist dabei zu dem Ergebnis gekommen, dass vier unterschiedliche Reifegrade eines Nachweises vorliegen können. In den frühen Stufen des im Folgenden beschriebenen Reifegradmodells müssen zunächst technische Grundlagen für den digitalen Abruf von Nachweisen geschaffen werden. Mit zunehmendem Nachweisabruf-Reifegrad, insbesondere in der letzten Stufe, muss zudem eine fachliche Harmonisierung innerhalb der Verwaltung erfolgen.

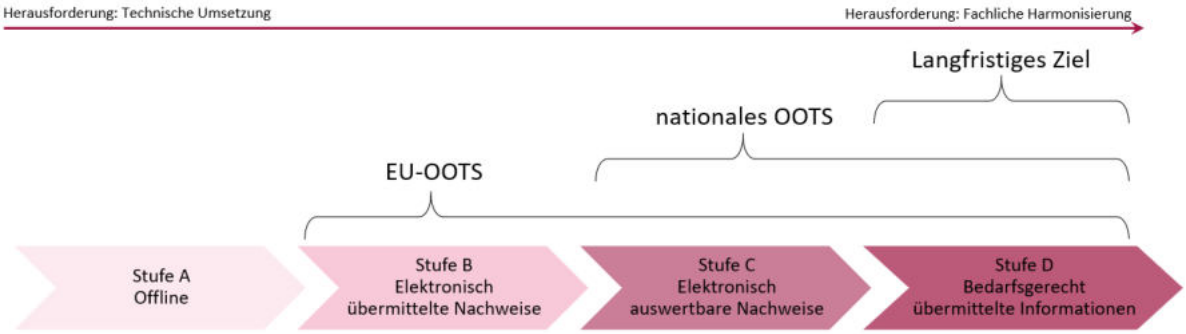


Abbildung 1: Reifegradmodell Nachweisabruf

Stufe A – Offline: Die zur Leistungserbringung notwendigen Nachweise werden ausschließlich in papiergebundener Form bereitgestellt oder lediglich auf Anfrage manuell digitalisiert. Ein sofortiger elektronischer Abruf ist nicht möglich. Der Austausch eines Nachweises erfolgt entweder durch Bezug und Einreichung durch den Bürger oder durch den direkten Austausch zwischen Data Consumer (Fachverfahren) und Data Provider (registerführenden Behörde). Die Übermittlung erfolgt auf postalischem Weg oder über Fax. Eine Übermittlung per Mail ist ebenfalls denkbar, wenn der notwendige Nachweis auf Anfrage manuell digitalisiert wird. Eine automatisierte Verarbeitung im Online- oder Fachverfahren ist nicht zeitgerecht möglich. Entspricht noch weitgehend dem Status quo in der Leistungsverwaltung.

Stufe B – Elektronisch übermittelte Nachweise: Die zur Leistungserbringung notwendigen Nachweise liegen in einem Format vor, das eine elektronische Datenübermittlung ermöglicht, beispielsweise im PDF- bzw. JPEG-Format. Eine maschinelle Auswertung zum Zweck der Datenübernahme in das Antragsformular im Online- oder Fachverfahren ist nicht (oder nur mit erheblichem zusätzlichem Aufwand) möglich. Das entspricht dem durch die Europäische Kommission festgelegten Mindest-zustand für die Anbindung an das europäische Once-Only-Technical-System (EU-OOTS).

Stufe C – Elektronisch auswertbare Nachweise: Die zur Leistungserbringung notwendigen Nachweise können elektronisch in strukturierter Form abgerufen werden. Oft entsprechen diese dabei den heutigen papiergebundenen Nachweisen, bspw. Geburtsurkunden oder Meldebescheinigungen. Die elektronische Repräsentation orientiert sich an bestehenden Fachstandards, wie sie heute in Registerauskünften genutzt werden, bspw. XMeld oder XPersonenstand. Nachweise werden mindestens in maschinenlesbarer Form übermittelt, was eine automatisierte Datenübernahme im Online- oder Fachverfahren ermöglicht. Das Kompetenzteam Architektur spricht sich dafür aus, diesen Reifegrad als Mindestvoraussetzung für die Registermodernisierung im nationalen Kontext anzustreben.

Stufe D – Bedarfsgerecht übermittelte Informationen: Die zur Leistungserbringung notwendigen Informationen können zielgerichtet elektronisch abgerufen werden. Statt einem Nachweis, der heute auch immer nicht benötigte personenbezogene Daten enthält, werden lediglich die auf den konkreten Bedarf zugeschnittenen Informationen ausgetauscht. Besteht zum Beispiel die Notwendigkeit, den Wohnort einer Person zu validieren, würde zukünftig keine vollständige Meldebescheinigung ausgetauscht werden, sondern lediglich ein maschinenlesbarer Datensatz, der ausschließlich Informationen zur Meldeadresse einer Person beinhaltet. Möglich wäre damit auch, eine konkrete Frage zur Prüfung eines Sachverhalts zu verschicken, die dann durch die registerführende Behörde beantwortet wird. Beispielsweise könnte eine Prüfung auf Volljährigkeit im Antragsprozess notwendig sein, was eine registerführende Behörde dann mit einem "Ja" oder "Nein" beantwortet.

Das Kompetenzteam Architektur spricht sich dafür aus, so schnell wie möglich den Nachweisabruf-Reifegrad D zu erreichen. Solange dies technisch noch nicht möglich ist, soll zumindest der Reifegrad C als Mindestziel der Registermodernisierung festgelegt werden. Register, bei denen es kurzfristig nicht möglich ist Reifegradstufe C zu erreichen, können in einer Übergangszeit auch im Reifegrad B angebunden werden. Diese Übergangszeit sollte jedoch – ggf. auch rechtlich – begrenzt werden.

Das Kompetenzteam Architektur spricht sich zudem dafür aus, den Nachweisabruf und die Nachweisverarbeitung auf Seiten der Online-Services im Sinne des hier

vorgeschlagenen Nachweis-Reifegrades C zu einer Voraussetzung für die Erreichung der OZG-Reifegradstufe 4 zu erklären. Die vorläufige Erreichung der OZG-Reifegradstufe 4 soll im Sinne einer Übergangslösung bereits im Nachweis-Reifegrad B möglich sein, sofern Online-Dienste daraufhin arbeiten, Nachweise der Reifegradstufe C zukünftig abrufen und verarbeiten zu können.

Vorteile:

- Förderung von Datensparsamkeit und Datenschutz durch den deutlich reduzierten Austausch nicht benötigter personenbezogener Daten zwischen Fachverfahren und registerführenden Behörden.
- Bei einer Implementierung entsprechend abgesicherter Übertragungswege zwischen Fachverfahren und registerführenden Behörden erhöht sich die Informationssicherheit gegenüber einer Übermittlung via Fax oder E-Mail.
- Setzung ambitionierter Modernisierungsziele. Eine Modernisierung, die den papierbasierten Austausch von Dokumenten durch den Austausch von nicht automatisiert auslesbaren PDF-Dokumenten o.ä. ersetzt, kann nicht nachhaltig erfolgreich sein.
- Vereinfachte Aufnahme von Nachweisdaten im Prozess der Antragsstellung. Nachweise der Stufe D enthalten keine zusätzlichen Informationen, die aufwändig gefiltert werden müssen, sondern lediglich die korrekt benötigten Daten.
- Insgesamt deutlich bessere Digitalisierbarkeit von Antrags- und Bearbeitungsprozessen (ermöglicht auch eine weitgehende Automatisierung, soweit diese rechtlich zulässig und fachlich möglich ist).

Nachteile:

- Hoher Umsetzungsaufwand durch die notwendige, fachliche Harmonisierung von Online- und Fachverfahren und registerführenden Stellen ab Stufe C.
- Für Stufe D sind zusätzlich Anpassungen an fachlichen Prozessen bis in die Gesetzgebung hinein erforderlich.

Alternativen:

- Der IT-Planungsrat entscheidet, lediglich Reifegrad Stufe C als langfristiges Ziel der Registermodernisierung festzulegen.
- Der IT-Planungsrat entscheidet, dass die OZG-Reifegradstufe 4 bereits ab Nachweis-Reifegradstufe B dauerhaft erreicht wird.

4. Sitzung des Lenkungskreises der Registermodernisierung

09.05.2022

TOP 3: Entscheidung zur Unterstützung asynchroner Prozesse in der Architektur der Registermodernisierung

1. **Der Lenkungskreis Registermodernisierung beschließt, das Zielbild der Registermodernisierung dahingehend zu schärfen, dass die Architektur der Registermodernisierung**
    a. **durch einen Online-Dienst nur für fachlich synchrone Nachweisabrufe genutzt werden kann und**
    b. **im Rahmen der Behörde-zu-Behörde-Kommunikation zusätzlich auch fachlich asynchronen Nachweisabruf ermöglicht.**
2. **Der Beschluss bedarf der Zustimmung des IT-Planungsrates und einer hieran anschließenden Abstimmung mit den Fachministerkonferenzen.**

Sachverhalt: *(kurze Darstellung des Problems)*

Das vom IT-Planungsrat beschlossene Zielbild vom Januar 2021 beschreibt zwei Arten des Nachweisabrufs: (fachlich) synchron und (fachlich) asynchron. Die Begriffe synchron und asynchron sind nicht im engen technischen Sinne zu verstehen, sondern in ihrer Eignung für eine direkte Nutzerinteraktion. „Synchron“ ist der Nachweisabruf, wenn der Nachweis innerhalb weniger Sekunden zur Verfügung steht. „Asynchron“ hingegen erlaubt eine fast beliebige Dauer zwischen dem Nachweisabruf und der Bereitstellung des Nachweises – von Minuten bis zu mehreren Tagen.

Wenn der Data Consumer ein Online-Dienst ist (z. B. ein Portal oder ein Formularmanagementsystem), sollen **nur fachlich synchrone Nachweisabrufe** möglich sein.

Dies entspricht den Anforderungen des EU-OOTS, das ausschließlich synchrone, "automatisiert austauschbare" Nachweisabrufe unterstützt. Auch das Zielbild der Registermodernisierung sieht den synchronen Nachweisabruf ausdrücklich vor (zum Beispiel zur automatischen Vorbefüllung von Online-Anträgen bzw. zur Ergänzung von Nachweisen während des Antragsprozesses).

Die Beschränkung auf rein synchrone Abrufe in diesem Anwendungsfall begründet sich dadurch, dass sich die Komplexität und der Umsetzungsaufwand deutlich erhöhen würden, wenn auch eine asynchrone Antwort möglich wäre:
Es müssten zusätzliche Mechanismen für die Möglichkeit der Preview durch die betroffene Person bzw. das jeweilige Unternehmen geschaffen werden. Eine Nachnutzung von Lösungen des Europäischen Systems käme nicht in Betracht, weil asynchrone Prozesse dort nicht betrachtet werden, so dass mit einer vollständigen Neuentwicklung zu rechnen wäre. Zudem müssten vermutlich neue Rechtsgrundlagen für die Datenverarbeitung im Rahmen dieser Interaktion mit den Nutzern geschaffen werden. Letztendlich ist auch unklar, ob eine entsprechende Lösung Akzeptanz bei betroffenen Personen und Unternehmen finden würde.

Nach Erkenntnissen des Kompetenzteams Architektur haben von den 18 TOP Registern acht Register für synchrone Nachweisabrufe geeignete technische Voraussetzungen.

- Melderegister
- Ausländerzentralregister
- Stammsatzdatei der DSRV (Datenstelle der Rentenversicherung, gemäß § 150 SGB VI)
- Versichertenkonten der Rentenversicherungsträger
- Zentrales Fahrzeugregister
- Verzeichnis der gem. § 14 der Gewerbeordnung angezeigten Gewerbebetriebe
- Identifikationsnummernregister
- Versichertenkonten der Rentenversicherungsträger gemäß § 149 SGB VI

Diese Einschätzung basiert auf der beim BVA geführten Registerübersicht in Verbindung mit der Verwaltungsdateninformationsplattform und einer Recherche der verwendeten Standards. Die Auswirkungen auf andere Registerbestände wurden durch das Kompetenzteams Architektur noch nicht untersucht.

Sollte ein Register gegenüber einem Online-Dienst nicht in der Lage sein, einen Nachweis synchron zu liefern, so besteht weiterhin die Möglichkeit, dass der Nachweis nach erfolgter Online-Antragstellung im Wege der Behörde-zu-Behörde Kommunikation über den asynchronen Kanal eingeholt wird, sofern hierfür eine rechtliche Grundlage gegeben ist (vgl. auch Zielbild Registermodernisierung S. 10 f.)[1].

Für die **Behörde-zu-Behörde-Kommunikation** sollen auch **fachlich asynchrone Nachweisabrufe** möglich sein. Dies ermöglicht die Anbindung von Registern, die noch nicht in der Lage sind, synchron zu antworten. Insbesondere im Bereich der Leistungsverwaltung sind asynchrone fachliche Prozesse verbreitet, eine synchrone Antwort wird derzeit nicht erwartet.

Neben technischen Gründen, Nachweisdaten nicht synchron zu übermitteln, ist es auch möglich, dass der Data Provider einen Nachweis zunächst digitalisieren oder ihn freigeben muss (weil zum Beispiel eine qualifizierte elektronische Signatur eines Sachbearbeiters benötigt wird).

Eine Architektur, die sowohl asynchrone als auch synchrone Nachweisabrufe unterstützt, ist komplexer als eine, die ausschließlich synchrone Nachweisabrufe unterstützt. Dies hat folgende Gründe:

- Zum einen müssen Data Consumer und Data Provider sich dauerhaft gegenseitig erreichen können und den Status zu laufenden Anfragen speichern. Diese zusätzlichen Aufgaben könnten zum Teil von Service Gateways oder der Transportinfrastruktur übernommen werden. Hierbei kommt zum Beispiel die auf Lösungen des IT-Planungsrats basierende Infrastruktur der Innenverwaltung in Frage. Wenn das NOOTS mit dieser Infrastruktur startet, verfügt es bereits über alle für die asynchrone Datenübermittlung erforderlichen Bestandteile.
- Zum anderen führt eine Architektur die sowohl asynchrone als auch synchrone Nachweisabrufe unterstützt, dazu, dass sich der von der EU vorgesehene generische Standard für den Nachweisabruf und der des deutschen Nachweisabrufstandards noch stärker unterscheiden werden, da der deutsche Standard um asynchrone Nachweisabrufe erweitert werden muss.

[1] IT-PLR Beschluss 2021/05

Abschließend kann festgestellt werden, dass der beschriebene Entwicklungsaufwand für die zusätzliche Unterstützung asynchroner Abrufe überschaubar wäre, wenn die Nutzung auf die Behörde-zu-Behörde-Kommunikation beschränkt wird.

Vorteile:

- Es können kurzfristig mehr Register für die Behörde-zu-Behörde-Kommunikation angeschlossen werden.
- Das System kann im Rahmen bestehender, asynchroner Datenabrufe genutzt werden, wie sie insbesondere in der Eingriffsverwaltung üblich sind.
- Es werden Anwendungsfälle abgedeckt, die im Sinne der SDG-Verordnung als „nicht automatisiert abrufbar“ gelten (Beispiel: Personenstandswesen wegen der Nacherfassung).

Nachteile:

- Etwas komplexere Architektur als bei einer rein synchronen Kommunikation.
- Größerer Erweiterungsbedarf des deutschen Nachweisabrufstandards.
- Größere Abweichungen vom europäischen OOTS.

Alternativen:

- Rein synchrone Kommunikation in allen Anwendungsfällen: Man wäre dem europäischen OOTS näher und würde eine klare Vision der Registermodernisierung transportieren. Der Modernisierungsdruck auf die Register würde wachsen. Allerdings wären mittelfristig viele Register ausgeschlossen und viele Anwendungsfälle nicht umsetzbar. Die eingesparte Komplexität wäre gering.
- Asynchrone Kommunikation in allen Anwendungsfällen (nicht nur in der Behörde-zu-Behörde-Kommunikation): Dieses Variante würde bei der Anbindung der Architektur eine maximale Flexibilität erlauben. Allerdings wäre die Architektur wesentlich komplexer und die Umsetzung deutlich aufwändiger.

4. Sitzung des Lenkungskreises der Registermodernisierung

09.05.2022

TOP 4: Entwicklung eines allgemeinen Standards für den Nachweisabruf für die nationale Registermodernisierung

1. **Der Lenkungskreis Registermodernisierung beauftragt die Registermodernisierungsbehörde einen allgemeinen Standard für den Nachweisabruf zu entwickeln, der die Kommunikation zwischen Data Consumer und Data Provider fachübergreifend regelt. Der Standard soll zunächst technologieneutral entwickelt werden (also keine Festlegung bezüglich des Transportbindings treffen). Der Fokus liegt entsprechend auf technischen Vorgaben, dabei werden auch Anforderungen an die Sicherheit der Datenübertragung berücksichtigt.**

2. **Der Lenkungskreis Registermodernisierung beauftragt das Kompetenzteam Recht/Datenschutz zu prüfen, inwieweit die Nutzung des allgemeinen Standards für den Nachweisabruf als Teil der Anschlussbedingungen an das nationale technische System der Registermodernisierung verbindlich vorgegeben werden kann.**

3. **Der Beschluss bedarf der Zustimmung des IT-Planungsrates und einer Abstimmung mit den Fachministerkonferenzen.**

Sachverhalt: *(kurze Darstellung des Problems)*

Bereits das Zielbild Registermodernisierung aus dem Januar 2021[1] sieht die Entwicklung eines einheitlichen Datenstandards für den Nachweisabruf als zentralen Bestandteil der Once-Only-Architektur vor.

Der Austausch von Nachweisen zwischen öffentlichen Stellen erfolgt derzeit in diversen Informationsverbünden, die hinsichtlich der rechtlichen, organisatorischen und technischen Gegebenheiten historisch gewachsen und für die jeweilige Fachlichkeit optimiert sind. Folglich stellt der Abruf von Nachweisen innerhalb eines Informationsverbundes in der Regel kein Problem dar, wohingegen der Nachweisabruf über die Grenze des Informationsverbundes hinweg mit Schwierigkeiten verbunden ist. Dies verlangsamt die Umsetzung des Once-Only-Prinzips: Eine möglichst weitgehende Entlastung von Nachweispflichten setzt voraus, dass die für ein Verfahren verantwortliche Behörde möglichst alle relevanten Nachweise direkt bei anderen öffentlichen Stellen abruft – auch wenn diese Nachweise aus unterschiedlichen Fachlichkeiten stammen und daher aktuell über unterschiedliche Informationsverbünde und deren jeweilige Fachstandards bereitgestellt werden. So werden z.B. viele OZG-/Einer-für-Alle-Services Nachweise aus ganz unterschiedlichen Verwaltungsbereichen benötigen.

Für eine flächendeckende Umsetzung des Once-Only-Prinzips sollte daher ein Zwang zur Anbindung an diverse fachspezifische Informationsverbünde vermieden werden. Ein wichtiger Baustein hierfür ist ein allgemeiner Nachweisabrufstandard für alle

[1] IT-PLR Beschluss 2021/05

anzuschließenden Behörden. Diese verbindliche Schnittstellenvorgabe soll sicherstellen, dass der Nachweisabruf bei den Data Providern zu grundsätzlich gleichen rechtlichen, organisatorischen und technischen Bedingungen erfolgt und die Data Consumer davon entlasten, für verschiedene Nachweise jeweils neue Fachstandards und deren Schnittstellen implementieren zu müssen. Der Standard soll zudem über den Anschluss des nationalen Once-Only-Technical-Systems (NOOTS) an das europäische Once-Only-Technical-System (EU-OOTS) deutschen Behörden den einheitlichen Nachweisabruf von Behörden im Ausland und umgekehrt ermöglichen.

Der allgemeine Standard stellt fachübergreifende Mechanismen für die Anforderung von Nachweisen, die Übermittlung von Nachweisen und für die Behandlung von Fehlerfällen bereit und vereinheitlicht damit die Übermittlung der Nachweise. Er legt nicht fest, in welchem Format die Nachweise selbst bereitgestellt werden und macht daher weitergehende Standardisierungsbemühungen nicht überflüssig. Der Standard selbst, ist möglichst einfach zu halten, was durch die Entkopplung von der Struktur der Nachweise unterstützt wird. Bereits dieser erste Schritt einer Vereinheitlichung des Übertragungsmechanismus bewirkt in vielen Fällen eine deutliche Entlastung von Stellen, die unterschiedliche Nachweise abrufen und zusammenführen müssen. Das Kompetenzteam Architektur wird zudem prüfen, inwieweit eine vorgeschaltete Kopfstelle ggf. die Umwandlung zwischen dem allgemeinen Standard und bereits etablierten Fachstandards übernehmen kann, ohne dass der Data Consumer sich hierfür mit Besonderheiten des jeweiligen Fachstandards beschäftigen muss. Dadurch könnten insbesondere kommunale Register von der Implementierung einer weiteren Schnittstelle entlastet werden. Die prinzipielle Möglichkeit dieses Ansatzes konnte in 2021 bereits in einem Pilotprojekt der Registermodernisierung für das Meldewesen demonstriert werden.

Im EU-OOTS wird ebenfalls ein generischer Standard für den Nachweisabruf zum Einsatz kommen. Der zu entwickelnde Standard für das NOOTS soll auf dem der EU-Kommission basieren und nur dann abweichen, wenn dies aufgrund nationaler Anforderungen erforderlich ist. Bei der Entwicklung des Standards für das NOOTS soll das vom Kompetenzteam EU-Interoperabilität vorgelegte Dokument "Nachweisabruf im nationalen OOTS / Konzept eines generischen Standards für den Nachweisabruf" (Fassung vom 02.03.2022) zu einem mit dem Kompetenzteam Architektur abgestimmten Dokument fortgeschrieben und den weiteren Arbeiten zugrunde gelegt werden.

Vorteile:

- Der generische Standard definiert einheitliche, vom jeweiligen Verwaltungsbereich unabhängige Mechanismen des Abrufs von Nachweisen von allen an das NOOTS angeschlossenen Registern und erleichtert damit in der Breite die Umsetzung des Once-Only-Prinzips.
- Da der generische Standard neu geschaffen wird, kann er von Beginn an mit Blick auf die besonderen Anforderungen bei Datenübermittlungen unter Nutzung der Identifikationsnummer gestaltet werden.
- Durch eine möglichst weitgehende Konvergenz mit dem von der EU vorgesehenen allgemeinen Standard für grenzüberschreitende Nachweisabrufe wird die Anbindung des NOOTS an das EU-OOTS erleichtert.
- Für den Kern des Standards kann eine hohe Stabilität erreicht werden, die unnötige Kosten durch häufige Schnittstellenanpassungen verhindert.

- Ein generischer Standard ermöglicht ein einheitlich hohes Level an Informationssicherheit und somit ein konsolidiertes Vorgehen bei der Einhaltung und Überwachung von Sicherheitsmaßnahmen bei der Datenübermittlung.
- Der Standard ist eine präzise Anforderung an IT-Verfahren im Sinne einer Schnittstellenvorgabe, die bei Bedarf in Verordnungen des Bundes referenziert werden kann.

Nachteile:

- Für Register, die aktuell bereits einen Nachweisabruf über einen fachspezifischen Standard ermöglichen, muss der allgemeine Standard als zusätzliche weitere Schnittstelle implementiert werden.
- Da das Fachrecht zum Teil spezifische Zusatzangaben beim Nachweisabruf fordert, muss auch ein allgemeiner Standard die Möglichkeit bieten, derartige fachspezifische Zusatzangaben zu übermitteln und kann daher nicht vollständig fachunabhängig gestaltet werden. Zudem muss ein Pflegeprozess für die Regelung derartiger fachspezifischer Zusatzangaben vorgesehen werden.

Alternativen:

- Keine Vereinheitlichung: Es werden lediglich bessere Informationen zur Anbindung an die jeweils fachspezifischen Informationsverbünde bereitgestellt (z.B. durch einen Leitfaden), jedoch findet keine Vereinheitlichung der Mechanismen zum Nachweisdatenabruf statt. Die gewünschte Entlastung bei der Umsetzung des Once-Only-Prinzips wird damit nicht erreicht.
- Dezentrale Umsetzung einheitlicher Vorgaben in den jeweiligen Fachstandards: Es werden übergreifende Vorgaben für Nachrichten zum Nachweisabruf entwickelt, die dann in jedem einzelnen, relevanten Fachstandard analog implementiert werden. Eine Entlastung der Data Consumer wird nur teilweise erreicht, weil die Beschäftigung mit jedem einzelnen Fachstandard notwendig bleibt. Änderungen der übergreifenden Vorgaben werden zudem zu unterschiedlichen Zeitpunkten, je nach Release-Zyklen der jeweiligen Fachstandards, umgesetzt und wirksam, was Anpassungsprozesse erschwert.

9. Sitzung des Lenkungskreises der Registermodernisierung

09.05.2022

TOP 5: Aufbau eines nationalen Data Service Directory und Nutzung des europäischen Evidence Brokers

1. **Der Lenkungskreis Registermodernisierung beschließt, bei der Bereitstellung des Data Service Directory (DSD) für das technische System der EU zum Nachweisabruf nach Art. 14 SDG-VO zur Bereitstellung der Routing-Informationen zu deutschen Evidence Providern (registerführenden Stellen) auf eine nationale Implementierung des DSD zu setzen.**
2. **Der Lenkungskreis Registermodernisierung bittet das Kompetenzteam Architektur, bei der weiteren Konzeption der Registerdatennavigation vorzusehen, dass diese zugleich als nationale Implementierung des DSD die Aufgaben nach den Vorgaben des technischen Systems der EU zum Nachweisabruf nach Art. 14 SDG-VO übernimmt.**
3. **Der Lenkungskreis Registermodernisierung beschließt, bei der Bereitstellung des Evidence Brokers (EB) für das technische System der EU zum Nachweisabruf nach Art. 14 SDG-VO die von der Europäischen Kommission zentral bereitgestellte Lösung zu nutzen und auf eine separate nationale Implementierung zu verzichten.**
4. **Der Beschluss bedarf der Zustimmung des IT-Planungsrates und einer hieran anschließenden Abstimmung mit den Fachministerkonferenzen.**

Sachverhalt: *(kurze Darstellung des Problems)*

Für die Umsetzung des Once-Only-Prinzips in der EU bedarf es eines von allen Mitgliedstaaten genutzten technischen Systems (europäisches Once-Only-Technical-System – EU-OOTS), das von der Europäischen Kommission in Zusammenarbeit mit den Mitgliedstaaten entwickelt wird. Für dieses System sind zentrale Verzeichnisse der Nachweistypen (Evidence Broker) und der an das System angeschlossenen Register (Data Service Directory) notwendig.

Für beide Verzeichnisse ist ein hybrides Bereitstellungsmodell vorgesehen. Die Mitgliedstaaten können jeweils ihre Daten zu einem zentralen Verzeichnis der Europäischen Kommission zuliefern oder ein eigenes nationales Verzeichnis für diese Aufgaben bereitstellen.

Aufgabe des Evidence Broker ist es, zu einer abstrakten, nachzuweisenden Tatsache den richtigen Nachweistyp in einem bestimmten Mitgliedstaat zu ermitteln. Damit wird das Problem adressiert, dass die meisten Nachweistypen in der EU nicht harmonisiert sind und daher verschiedene Mitgliedstaaten unterschiedliche Nachweise vorsehen können, um den gleichen Sachverhalt zu belegen.

Das Data Service Directory stellt ein Verzeichnis aller Register zur Verfügung, die an das EU-OOTS angebunden sind, und ermöglicht es, für einen konkreten Nachweisabruf das richtige Register zu identifizieren. Es muss dafür die Zuständigkeitslogiken der jeweiligen Domäne abbilden können.

Nach Einschätzung der Kompetenzteams EU-Interoperabilität und Architektur kann im nationalen Kontext in aller Regel davon ausgegangen werden, dass ein Data Consumer beurteilen kann, welche deutschen Nachweise sie für ihren Fachprozess benötigt/akzeptieren kann. Zudem sind diese häufig einheitlich durch Bundesrecht vorgegeben. Die Funktionalität des Evidence Broker wird daher im nationalen Rahmen nicht zwingend benötigt. Zudem ändert sich die Menge der über das nationale OOTS (NOOTS) verfügbaren Nachweistypen und deren Geltungsbereich nur selten, was eine Pflege in einem zentralen Verzeichnis der EU möglich macht. Perspektivisch könnte ein Evidence Broker auch in Deutschland interessant sein, um z.B. Änderungen an den rechtlichen Nachweisanforderungen für einzelne Verfahren dynamisch ohne Anpassung an den jeweiligen Online-Service oder das Fachverfahren ausspielen zu können. Im Sinne einer Priorisierung der Umsetzungsaufwände soll dennoch zunächst die zentrale europäische Lösung genutzt werden. Dies schließt einen späteren Übergang zu einer nationalen Implementierung nicht aus.

Im Gegensatz dazu wird die Ermittlung des konkreten Registers, aus dem im Einzelfall der gesuchte Nachweis abgerufen werden kann, auch im nationalen Kontext benötigt und ist dort als Komponente „Registerdatennavigation“ im Zielbild des IT-Planungsrats[1] vorgesehen. Für viele existierende Informationsverbünde – insbesondere in der Eingriffsverwaltung – gibt es hierfür bereits Lösungen, in der Regel durch die Abbildung der Zuständigkeitslogik auf ein DVDV-Schlüsselkonzept. Die Registerdatennavigation soll hierfür zukünftig jedoch eine allgemeinere und dadurch zugleich für die Anbindung neuer Kommunikationspartner niedrigschwelligere Lösung bereitstellen. Die Ermittlung der zuständigen Stelle benötigt – aus der Perspektive der Registerdatennavigation wie aus der des DSD – fachspezifische Routinglogiken, die sich für jeden Nachweistyp unterscheiden und im Zeitablauf verändern können. Daher ist es vorteilhaft, wenn diese Logiken direkt national implementiert und nicht erst an die Europäische Kommission vermittelt werden müssen. Zudem benötigen das DSD und die Registerdatennavigation sehr stark überschneidende Datenbestände zu Registern und deren Zuständigkeiten. Es ist sinnvoller, diese Informationen zentral an einer Stelle vorzuhalten, statt sie redundant in einem deutschen und einem europäischen System zu pflegen.

<u>Vorteile</u>

- Reduktion der Umsetzungsaufwände durch Fokussierung der nationalen Implementierung ausschließlich auf die für Deutschland spezifische und auch im nationalen Kontext benötigte Funktionalität
- Schnelle und weniger fehleranfällige Umsetzung von nationalen Zuständigkeitslogiken
- Reduktion der Pflegeaufwände durch Vermeidung einer Doppelpflege von Registerinformationen in einem deutschen und einem europäischen Verzeichnis
- Arbeiten zur Umsetzung des DSD können mit denen zur Registerdatennavigation gebündelt werden und dadurch in wichtigen Bereichen bereits voranschreiten, bevor die europäischen Vorgaben final beschlossen sind

[1] IT-PLR Beschluss 2021/05

Risiken

- Alle Planungen bauen auf dem aktuellen Verhandlungsstand des Durchführungsrechtsakts zu Art. 14 SDG-VO und der begleitenden technischen Dokumente auf, die bisher nicht in einer finalen Fassung vorliegen. Die für diese Entscheidung relevanten Aspekte sind aktuell zwischen Kommission und Mitgliedstaaten nicht mehr kontrovers und daher voraussichtlich stabil. Dennoch kann nicht ausgeschlossen werden, dass sich noch Änderungen in diesen Rahmenbedingungen ergeben. Mit Blick auf die enge Umsetzungsfrist bis 12.12.2023 kann die Planung der deutschen Anbindung des OOTS aber nicht erst auf einen finalen europäischen Beschluss warten.
- Die genauen Pflegeprozesse und -mechanismen für den zentralen europäischen Evidence Broker sind noch nicht abschließend definiert.
- Die zentrale europäische Instanz der Evidence Broker könnte durch die Kommission ggf. verspätet bereitgestellt werden.

Alternativen

- Nationale Umsetzung des Evidence Brokers: schafft eine zum europäischen Evidence Broker redundante Infrastruktur, für die derzeit kein Bedarf erkennbar ist.
- Nutzung des zentralen europäischen Data Service Directory statt einer nationalen Implementierung: spart den Umsetzungsaufwand für eine nationale Lösung zum DSD (aber nicht für die nationale Registerdatennavigation), führt aber zu einem dauerhaften doppelten Pflegeprozess von Registerinformationen auf nationaler und europäischer Ebene.
- Getrennte Umsetzung von nationalem Data Service Directory und nationaler Registerdatennavigation: führt zu zwei getrennten Systemen, die einen stark überschneidenden Datenbestand zu Registern und Zuständigkeiten benötigen, und damit voraussichtlich zu dauerhaft redundanter Datenpflege.

4. Sitzung des Lenkungskreises der Registermodernisierung

09.05.2022

TOP 6: Entscheidung zur Umsetzung der Komponente Registerdatennavigation als zentralen Routing-Dienst (Routing As a Service) auf Grundlage des Deutschen Verwaltungsdiensteverzeichnis (DVDV) unter Wiederverwendung von Lösungsansätzen aus FIT-Connect

1. **Der Lenkungskreis Registermodernisierung schlägt dem IT-Planungsrat folgenden Beschluss vor:**

   „Der IT-Planungsrat beauftragt die FITKO mit der Umsetzung der Komponente „Registerdatennavigation“ als zentralen Routing-Dienst (Routing as a Service) auf Grundlage des Deutschen Verwaltungsdiensteverzeichnis (DVDV) unter Wiederverwendung von Lösungsansätzen aus FIT-Connect. Der Projektauftrag ist entsprechend des Beschlusses des Lenkungskreises Registermodernisierung vom 9. Mai 2022 durch das Kompetenzteam Architektur der Gesamtsteuerung Registermodernisierung zu konkretisieren.“

2. **Der Lenkungskreis Registermodernisierung beauftragt das Kompetenzteam Architektur mit der Formulierung eines Projektauftrags, aus dem Zielsetzung und Rahmenbedingungen zur Umsetzung der Komponente Registerdatennavigation hervorgehen.**
3. **Nach einer Beschlussfassung durch den IT-Planungsrat ist im Zuge der Umsetzung eine Abstimmung mit den Fachministerkonferenzen vorzunehmen.**

Sachverhalt: *(kurze Darstellung des Problems)*

Ziel dieser Beschlussvorlage ist es, eine Entscheidung zum Funktionsumfang und der technischen Realisierung der zentralen Komponente „Registerdatennavigation“ aus dem Zielbild des IT-Planungsrats herbeizuführen.

Mit Hilfe der Registerdatennavigation ermitteln abrufende Stellen, von welcher konkreten Behörde sie einen Nachweis abrufen können und welche technischen Verbindungsparameter sie dazu benötigen. Diese Aufgabe beinhaltet zwei Schritte:

1. Ermittlung der originär für den Nachweis zuständigen Behördeninstanz anhand fachlicher, regionaler und weiterer **Zuständigkeiten**
2. Ermittlung des von dieser Behördeninstanz bereitgestellten **technischen Dienstes**, über den der Nachweis abgerufen werden kann, sowie der zu dessen Nutzung erforderlichen technischen Parameter.

Das Kompetenzteam Architektur hat in der Verwaltung etablierte Lösungen für diese Aufgabenstellung untersucht und auf ihre Eignung für die Registermodernisierung geprüft:

Das DVDV ist durch den IT-PLR bereits als zentrales Diensteverzeichnis der Verwaltung positioniert und in Teilen der Verwaltung etabliert. Für die Aufgabe als

Diensteverzeichnis wird es als geeignet erachtet. Derzeit sind dort bereits über 40.000 Stellen erfasst. Eine explizite Abbildung von Zuständigkeiten ist im DVDV nicht vorgesehen. Die in Teilen der Innenverwaltung eingesetzte Abbildung von Zuständigkeiten über Schlüssellogiken wird als nicht ausreichend flexibel für die Registermodernisierung angesehen.

In FIT-Connect wird ein Routing-Dienst bereitgestellt, der eine ähnliche Aufgabe wie die Registerdatennavigation hat. Der Routing-Dienst verwendet das DVDV als Verzeichnis der technischen Dienste, nutzt jedoch bestehende Datenbestände von Verwaltungszuständigkeiten, die bereits im „Portalverbund Online-Gateway“ (PVOG) abgebildet sind. Diese werden zunächst über die Redaktionssysteme des föderalen Informationsmanagements (FIM) gepflegt und über XZuFi in PVOG eingespielt. Der Ansatz ist tragfähig, jedoch in mehrerlei Hinsicht auf den Kontext des OZG zugeschnitten. Eine Verwendung in der Registermodernisierung würde umfangreiche Neuausrichtungen mit sich bringen, bspw.:

- Erweiterung der Zuständigkeitslogik um eine mehrstufige Ableitung
- Aufnahme von potenziell sehr vielen Registerabrufleistungen in den Leistungskatalog (LeiKa), die dort bisher noch nicht existieren
- Erweiterung der bestehenden Systematik des Leistungskatalogs (LeiKa) zur Abbildung feingranularer Nachweisabrufe
- Erweiterung der Prozessmodelle des föderalen Informationsmanagements um große Teile der Eingriffsverwaltung
- Eingeschränkte Nutzung des DVDV, da Metadaten zu Diensten und Behörden nicht mehr im DVDV gespeichert werden würden.

Das Kompetenzteam Architektur empfiehlt daher, die Komponente Registerdatennavigation als neue Komponente nach dem Vorbild des FIT-Connect Routingdienstes aufzubauen. Die technischen Dienste werden, wie bisher im DVDV, zentral verwaltet. Für die Zuständigkeiten wird ein neues Zuständigkeitsverzeichnis aufgebaut, das jedoch Zuständigkeiten in einer verallgemeinerten Form speichert, so dass es gleichermaßen für Leistungen aus dem LeiKa, für Nachweise aus der Registermodernisierung und für Zuständigkeiten für beliebige Rechtsgrundlagen geeignet ist. Die Pflege der Daten soll analog zum PVOG über XZuFi erfolgen. Darüber sind bspw. automatisierte Abgleiche mit dem PVOG möglich. Perspektivisch kann dieses Zuständigkeitsverzeichnis zu einem zentralen Zuständigkeitsverzeichnis der Deutschen Verwaltung (DVZV) entwickelt werden.

Der Zugriff auf die Registerdatennavigation soll über einen Routingdienst erfolgen, der die Kapselung der Datenhaltung übernimmt und eine einfach zu nutzende Schnittstelle nach außen bereitstellt. Als Vorlage des Routingdienstes wird der FIT-Connect-Ansatz mit dessen Routing-API empfohlen, eine Wiederverwendung bestehender Bausteine sollte durch die FITKO und möglichst unter Beteiligung betroffener Stellen geprüft werden.

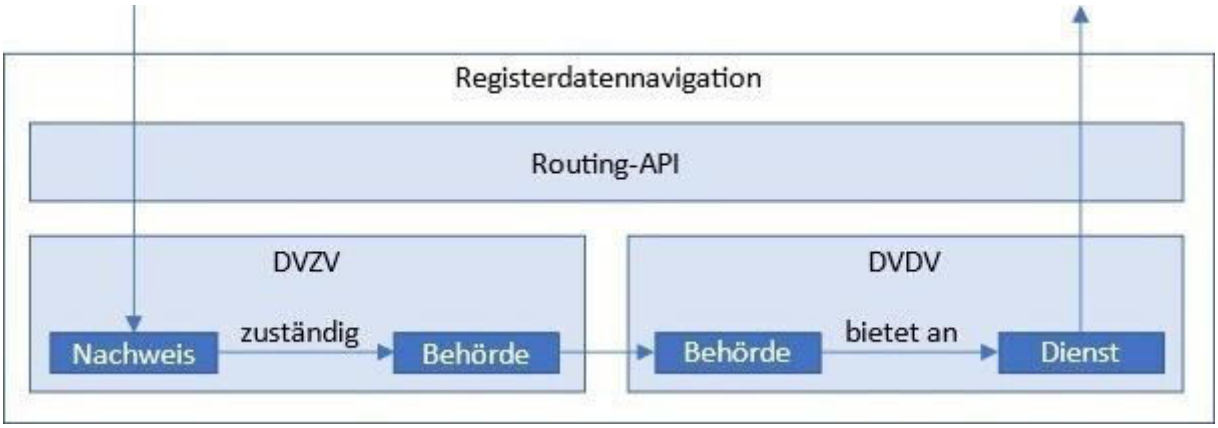


Abbildung 1: Darstellung Registerdatennavigation

Mit der Umsetzung der neuen Komponente soll die FITKO beauftragt werden. Als Produktverantwortliche des DVDV, des PVOG und FIM sowie dem Projekt FIT-Connect kann sie weitreichendes Know-how zu beiden Lösungen einbringen und dafür Sorge tragen, dass die Verzeichnisse DVDV und DVZV konform zu den strategischen Zielsetzungen des IT-Planungsrats in geeigneter Weise gekoppelt und die zugehörigen Pflegeprozesse entsprechend aufeinander abgestimmt werden. Zudem können Lösungsansätze und bestehende Softwarekomponenten aus FIT-Connect wiederverwendet und auf die neue Komponente übertragen werden.

Die folgenden, bisher nicht abschließend geklärten Aspekte, müssen durch die Formulierung des Projektauftrags durch das Kompetenzteam Architektur und nachfolgend im Rahmen der Umsetzung durch die FITKO weiterführend ausgearbeitet werden:

- Verantwortung der Erstellung, Pflege, Speicherung und Bereitstellung der Nachweistypen mit eindeutigen IDs. (Denkbar ist die Nutzung von FIM-Datenfelder zur Abbildung der Nachweistypen, indem Dokumentensteckbriefe vom Typ "Registerantwort" angelegt werden. Dies würde auch eine Definition der Datenstruktur und Datenaustauschformate der Nachweistypen in FIM ermöglichen.)
- Darstellung von Pflege- und Austauschprozessen zwischen Dienste- und Zuständigkeitsverzeichnis
- Realisierung des Anschlusses der Registerdatennavigation an die Systeme des europäischen Once-Only-Technical-Systems (EU-OOTS) und notwendiger Pflegeprozesse.
- Prüfung des Konzepts unter den Gesichtspunkten des Datenschutzes und der IT-Sicherheit.[1]
- Prüfung, ob bestehende Zuständigkeitsinformationen in DVDV und PVOG, die bereits heute redundant vorliegen und mehrfach gepflegt werden müssen, perspektivisch im Zuständigkeitsverzeichnis konsolidiert werden sollten. Damit könnte ein zentrales Zuständigkeitsverzeichnis (DVZV) nach dem Vorbild des DVDV geschaffen werden.

[1] Mit der Komponente Registerdatennavigation als zentralen Routing-Dienst im Sinne des Beschlusses 2015/03 des IT-Planungsrates für den Datenaustausch zwischen Fachverfahren und öffentlichen Stellen durch Verwendung geeigneter Routingverfahren (ohne Anpassungen von Fachverfahren) wird sichergestellt, dass auch föderal übergreifend für den fachverfahrensbezogenen Datenaustausch zwischen öffentlichen Stellen vorrangig die sicheren Verwaltungsnetze von Bund und Ländern genutzt werden.

- Prüfung von automatisierten Datenübernahmen/Datensynchronisationen ins DVDV, die bisher noch nicht technisch und konzeptionell umgesetzt sind, aber notwendig werden könnten.
- Zur Anbindung an das europäische Once-Only-Technical-System (EU-OOTS) wird die Registerdatennavigation um zusätzliche Funktionalitäten erweitert werden müssen. Da die Entwicklung der europäischen Komponenten Data Service Directory (DSD) und Evidence Broker, die in engem Zusammenhang mit der Registerdatennavigation stehen, weiter andauert, kann eine Detaillierung dieser Funktionen erst zu einem späteren Zeitpunkt erfolgen.

Vorteile:

- Wiederverwendung der bestehenden technischen Lösung und bereits etablierter Pflegeprozesse des Deutschen Verwaltungsdiensteverzeichnis (DVDV).
- Schaffung einer wiederverwendbaren und skalierbaren Lösung zur Abbildung und Ermittlung von Zuständigkeiten innerhalb der öffentlichen Verwaltung (DVZV).
- Wiederverwendung existierender Lösungsansätze aus dem Portalverbund Online Gateway (PVOG) und dem Zuständigkeitsfinder (XZuFi).

Nachteile:

- Aufbau einer weiteren Zuständigkeitsdatenbank, die teilweise redundant zu PVOG & DVDV ist. Die Zuständigkeitsinformationen sollten perspektivisch im DVZV konsolidiert werden.

Alternativen:

- Umbau der XZuFi basierten Redaktionssysteme um einen nachweisorientierten Ansatz. Die oben genannten Anpassungserfordernisse sind detailliert zu untersuchen.
- Umsetzung der Registernavigation auf Basis eines leistungsorientierten Ansatzes mit Registerabrufleistungen, der eine 1:1 des bisherigen XZuFi Standards ermöglicht, aber eine zusätzliche Abstraktionsschicht schafft.