



**Freie
Hansestadt
Bremen**

Anbindungsleitfaden

Informationen für registerführende Stellen
zur Anbindung an das Datenschutzcockpit (DSC)



**Finanziert von der
Europäischen Union**
NextGenerationEU

Version

1.1

Datum

04.12.2024

Dokumententitel

Informationen für registerführende Stellen zur Anbindung
an das Datenschutzcockpit (DSC)

Autoren

Dr. Christian Janssen, Karolina Kozikowska, Markus Portz

Kontakt

Kerstin Sprock, Projektleiterin des Projektes DSC



datenschutzcockpit@finanzen.bremen.de

Abteilung Zentrales IT-Management, Digitalisierung öffentlicher Dienste

4-1 Gesamtsteuerung Datenschutzcockpit

Dienstsitz: Rudolf-Hilferding-Platz 1, 28195 Bremen

Dienststätte: Am Tabakquartier 56, 28197 Bremen

Disclaimer

Finanziert durch die Europäische Union – NextGenerationEU. Die geäußerten Ansichten und Meinungen sind ausschließlich die des Autors/der Autoren und spiegeln nicht unbedingt die Ansichten der Europäischen Union oder der Europäischen Kommission wider. Weder die Europäische Union noch die Europäische Kommission können für sie verantwortlich gemacht werden.

Inhaltsverzeichnis

Änderungsverzeichnis	5
1 Vorwort	6
2 Grundlegende Informationen	8
2.1 Rechtliche Grundlagen.....	8
2.2 Quellenmodell	11
2.3 Anmeldung und Nutzendenverwaltung	11
2.4 Ende-zu-Ende-Verschlüsselung	12
2.5 Sicherheitsarchitektur.....	13
2.6 Standard XDSC.....	14
2.7 Gesamtsystem DSC	16
2.8 Schnittstellen zur DSC-Anbindung	17
2.9 DSC User Journey	17
3 Registeranbindung Schritt für Schritt.....	19
3.1 Exkurs: Registerarten	20
3.2 Ablauf des DSC-Anbindungsprojektes	22
3.3 Anbahnung	22
3.3.1 Checkliste: Anbahnung.....	23
3.3.2 Unterstützung des DSC-Teams - Anbahnung.....	24
3.4 Initialisierung	25
3.4.1 Checkliste: Initialisierung.....	25
3.4.2 Unterstützung des DSC-Teams - Initialisierung.....	26
3.5 Konzeption, Umsetzung & Tests	26
3.5.1 Checkliste: Konzeption, Umsetzung & Tests.....	26
3.5.2 Unterstützung des DSC-Teams - Umsetzung.....	29
3.6 Produktivsetzung.....	31
3.6.1 Checkliste: Produktivsetzung.....	31
3.6.2 Unterstützung des DSC-Teams: Produktivsetzung.....	32
4 DSC-Team	Error! Bookmark not defined.
3.7 Weiterführende Informationen	33

Abbildungsverzeichnis

Abbildung 1: Startseite des DSC	8
Abbildung 2: Kommunikation des DSC mit den Registern	12
Abbildung 3: Übersicht des Gesamtsystems	16
Abbildung 4: Grober Ablauf der User-Journey	18
Abbildung 5: Vorgehensmodell zur IDA-Anbindung.....	20
Abbildung 6: Fallunterscheidungen bei der Anbindung von Registern	21
Abbildung 7: Screenshot DSC Simulator Auswahl Request Typ	30
Abbildung 8: Screenshot XDSC-Viewer – Übersicht Protokolldaten	31
Abbildung 9: Umsetzungsschritte und Rollen DSC-Team.....	33

Änderungsverzeichnis

Version	Datum	Autor	Änderung
1.0	22.11.2024	Dr. Christian Janssen (extern für die FHB)	Einfügung Änderungs- und Abbildungsverzeichnis, Übernahme der Änderungsvorschläge des BVA
1.1	04.12.2024	Dito	Überarbeitung entspr. der Änderungsvorschläge des BVA

1 Vorwort

Im Zuge der fortschreitenden Digitalisierung und der Modernisierung der Registerlandschaft in Deutschland spielt das Datenschutzcockpit (DSC) eine wichtige Rolle. Gemäß dem Registermodernisierungsgesetz (RegMoG) soll das DSC zusammen mit der Einführung der Identifikationsnummer (IDNr) in die Register, die in §1 der Anlage 1 zum Identifikationsnummerngesetz (IDNrG) genannt sind, realisiert werden. Mit Hilfe des DSC kann jede Bürgerin und jeder Bürger selbstständig überprüfen, welche Daten wann und aus welchem Grund zwischen öffentlichen Stellen, unter Verwendung der persönlichen IDNr innerhalb der letzten zwei Jahre ausgetauscht wurden. Dies ist bequem von zu Hause aus möglich, mit jedem gängigen Internetbrowser. Künftig sollen im DSC auch die Bestandsdaten angezeigt werden – also Daten, die unter der Verwendung der IDNr über die Bürgerinnen und Bürger in den Registern gespeichert sind. Dies erweitert die Transparenz und ermöglicht es den Bürgerinnen und Bürgern, einen umfassenden Überblick über ihre in den Registern gespeicherten Daten zu erhalten.

Die 50 Register, welche das IDNrG identifiziert hat, dürfen die IDNr in ihren Datenübermittlungen nur verwenden, wenn sie an das DSC angeschlossen sind. Da die Nutzung einer Nummer zur Zuordnung von personenbezogenen Daten ein besonderes Schutzniveau erfordert, enthält das IDNrG unter anderem mit dem DSC-Sicherungsmechanismen, die der verfassungsrechtlichen Rechtsprechung zur informationellen Selbstbestimmung Rechnung tragen. Der höheren Datendichte steht damit ein Transparenztool entgegen. Diese Transparenz stärkt das Vertrauen in die digitale Verwaltung und fördert die Akzeptanz der flächendeckenden Einführung des Once-Only-Prinzips.

Technisch gesehen ist das DSC eine IT-Komponente des Portalverbundes, die eine Verknüpfung von Verwaltungsportalen aus Bund, Ländern und Kommunen darstellt. Das RegMoG bildet die rechtliche Grundlage des Projektes.

Der vorliegende Anbindungsleitfaden richtet sich an alle Interessierte, Verantwortliche der registerführenden Stellen für den Anschluss an das DSC oder ihre Fachverfahrenshersteller.

Ziel ist es, den registerführenden Stellen eine erste strukturierte Vorgehensweise zu bieten, um die Integration in das DSC effizient zu gestalten.

Der Leitfaden bietet eine einführende Anleitung zur technischen Anbindung an das DSC. Er führt in das DSC, seine Grundlagen in Recht, Technik und Funktionsweise ein. Er greift auch die Spezifikationen des XDatenschutzcockpit-Standards auf. Zudem werden Verweise zur weiteren Vertiefung von Einzelthemen angeboten.

In Analogie zur IDA-Anbindung erfolgt auch die Anbindung an das DSC in vier Schritten, welche ebenfalls in diesem Dokument vorgestellt werden. Dieser Leitfaden beschreibt die notwendigen technischen Komponenten, die funktionalen und nicht-funktionalen Anforderungen sowie die rechtlichen Rahmenbedingungen, die für eine erfolgreiche Anbindung erforderlich sind. In jedem Schritt helfen Checklisten alle wesentlichen Punkte zu erfassen und zu bearbeiten.

Dieser Leitfaden liegt nun in einer ersten Version vor. Nur durch das regelmäßige und intensive Feedback seiner Lesenden kann er verbessert werden. Daher freut sich das DSC-Team (datenschutzcockpit@finanzen.bremen.de) über Anmerkungen und Verbesserungswünsche, um den Leitfaden weiter zu optimieren und den Bedürfnissen seiner Adressaten immer gerechter zu werden.

2 Grundlegende Informationen

In diesem Abschnitt werden die rechtlichen und technischen Grundlagen des Datenschutzcockpits (DSC), die User Journey ebenso wie der zugrundeliegenden Standards XDatenschutzcockpit (XDSC) beschrieben.

Das DSC ist eine Webanwendung (www.datenschutzcockpit.bund.de), die es Nutzenden ermöglicht, den Austausch ihrer persönlichen Daten zwischen öffentlichen Stellen transparent nachzuvollziehen. Darüber hinaus soll das DSC in der nächsten Ausbaustufe auch die Anzeige von Bestandsdaten bei registerführenden Behörden ermöglichen.

Das DSC wurde von der Freien Hansestadt Bremen (FHB) im Auftrag des Bundesministeriums des Innern und für Heimat (BMI) und Bundesverwaltungsamt (BVA) seit 2023 entwickelt.

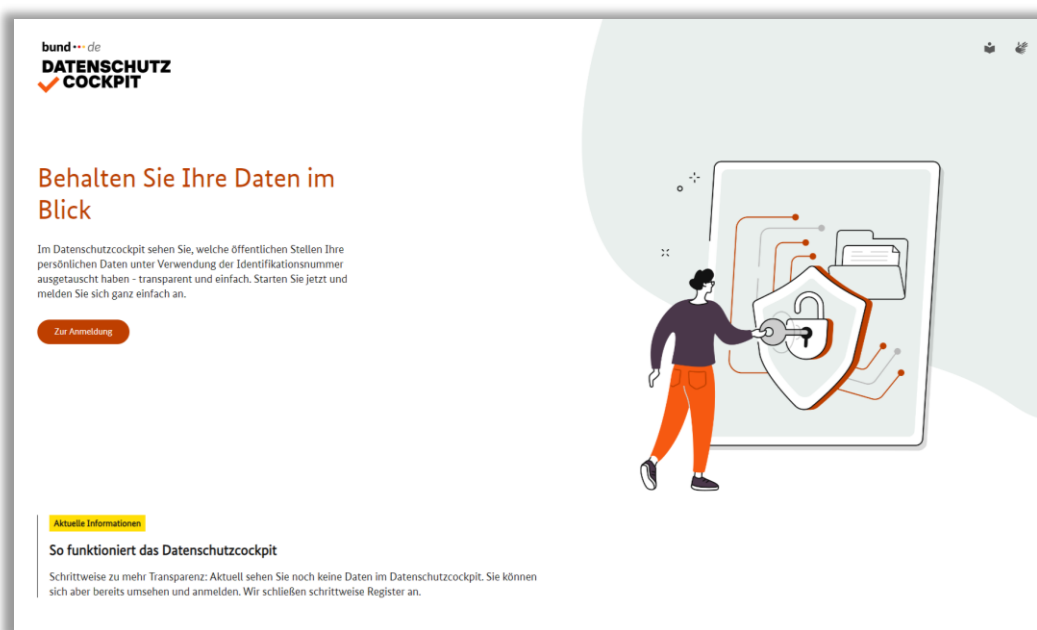


Abbildung 1: Startseite des DSC

Mit dem Datenschutzcockpit können Nutzende selbstständig überprüfen, welche Daten wann und aus welchem Grund zwischen öffentlichen Stellen unter Verwendung ihrer IDNr in den letzten zwei Jahren ausgetauscht wurden. Dies ist bequem von zu Hause aus mit einem gängigen Internetbrowser möglich.

2.1 Rechtliche Grundlagen

Die wesentliche Rechtsgrundlage für das DSC ist das Registermodernisierungsgesetz (RegMoG), das in diesem Zuge geänderte Onlinezugangsgesetz (OZG) und das in der Datenschutz-Grundverordnung (DSGVO) festgehaltene Auskunftsrecht der betroffenen Person über personenbezogene Daten, sowie weitere unten aufgelistete zu berücksichtigende Vorgaben, Gesetze und Beschlüsse.

Das DSC basiert darüber hinaus im Detail auf folgenden Grundlagen:

- Registermodernisierungsgesetz (RegMoG) insbesondere §10 Art. 2 RegMoG und Art. 21 in Verb. mit §11 Art. 2 RegMoG, mit letzter Änderung durch BeamtEReg/DienstRÄndG - BGBl I 2021, 2250
- Onlinezugangsgesetz (OZG)
- Identifikationsnummerngesetz (IDNrG)
- Datenschutz-Grundverordnung (DSGVO)
- EU-Verordnung 2018/1724 zum Single Digital Gateway (SDG)
- Berücksichtigung von Vorgaben zu „Produkten und Standards“ des IT-Planungsrates (IT-PLR) gemäß Beschluss „Jahresbericht 2020 IT-PLR/FITKO“
- IT-Sicherheitsrichtlinie des IT-Planungsrates

Als besonderer rechtlicher Bezugsrahmen für das DSC wird in § 10 OZG Folgendes zum DSC festgelegt (s. https://www.gesetze-im-internet.de/ozg/_10.html):

„(1) Ein „Datenschutzcockpit“ ist eine IT-Komponente, mit der sich natürliche Personen Auskünfte zu Datenübermittlungen zwischen öffentlichen Stellen anzeigen lassen können. Erfasst werden bis zum Vorliegen der technischen und rechtlichen Voraussetzungen für eine Erfassung weiterer Datenübermittlungen zunächst diejenigen Datenübermittlungen, bei denen eine Identifikationsnummer nach § 5 des Identifikationsnummerngesetzes zum Einsatz kommt.

(2) Im Datenschutzcockpit werden nach Maßgabe von Absatz 4 Satz 3 ausschließlich Protokolldaten nach § 9 des Identifikationsnummerngesetzes einschließlich der dazu durch die Registermodernisierungsbehörde und die Register übermittelten Inhaltsdaten sowie die Bestandsdaten der Register angezeigt. Diese Daten werden im Datenschutzcockpit nur für die Dauer des jeweiligen Nutzungsvorgangs gespeichert; nach Beendigung des Nutzungsvorgangs sind sie unverzüglich zu löschen. Der Auskunftsanspruch nach Artikel 15 der 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) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35) bleibt unberührt. Das Datenschutzcockpit ist aus Sicht des Nutzers einfach und zweckmäßig auszugestalten. Es sind technische und organisatorische Maßnahmen vorzusehen, damit staatliche Eingriffe zum Nachteil des Nutzers nicht möglich sind.

(3) Jede natürliche Person kann sich bei der öffentlichen Stelle, die das Datenschutzcockpit betreibt, für ein Datenschutzcockpit registrieren. Sie hat sich bei der Registrierung und Nutzung des Datenschutzcockpits mit einem Identifizierungsmittel auf dem Vertrauensniveau „hoch“ zu identifizieren. Zur Feststellung der Identität darf bei Registrierung und Nutzung das dienste- und kartenspezifische Kennzeichen verarbeitet

werden. Im Übrigen kann sich der Nutzer auch mit einem Nutzerkonto des Portalverbundes beim Datenschutzcockpit registrieren. In diesem Fall darf die für das Nutzerkonto zuständige Stelle das dienste- und kartenspezifische Kennzeichen an die für das Datenschutzcockpit zuständige Stelle übermitteln.

(4) Das Datenschutzcockpit darf die Identifikationsnummer nach § 139b der Abgabenordnung als Identifikator für die Anfrage zur Erhebung und Anzeige der Daten nach Absatz 2 verarbeiten. Zur Anfrage nach § 6 des Identifikationsnummerngesetzes erhebt das Datenschutzcockpit bei der Registrierung des Nutzers folgende Daten:

1. Namen, 2. Vornamen, 3. Anschrift, 4. Geburtsname und 5. Tag der Geburt.

Der Nutzer legt fest, in welchem Umfang das Datenschutzcockpit Protokolldaten einschließlich der übermittelten Inhaltsdaten sowie die Bestandsdaten der Register nach Absatz 2 erheben und anzeigen darf. Auf diese Daten hat nur der Nutzer Zugriff. Der Nutzer muss sein Konto im Datenschutzcockpit jederzeit selbst löschen können. Das Konto im Datenschutzcockpit wird automatisiert gelöscht, wenn es drei Jahre nicht verwendet wurde.

(5) Das Datenschutzcockpit wird von einer öffentlichen Stelle errichtet und betrieben, die durch Rechtsverordnung des Bundesministeriums des Innern und für Heimat im Benehmen mit dem IT-Planungsrat mit Zustimmung des Bundesrates bestimmt wird. Das Nähere zu den technischen Verfahren, den technischen Formaten der Datensätze und den Übertragungswegen legt das Bundesministerium des Innern und für Heimat im Benehmen mit dem IT-Planungsrat mit Zustimmung des Bundesrates durch Rechtsverordnung fest.“

Aus §10 OZG lassen sich die folgenden Anforderungen an das DSC ableiten, welche für die technische Umsetzung des DSC maßgeblich sind:

- In Absatz 2 Satz 2 sowie in Absatz 4 Satz 3 wird beschrieben, dass das DSC, außer den u.a. Nutzerdaten, keine Daten persistent speichert und alle Daten nach der Session gelöscht werden. Im Detail wird in Abschnitt 2.2. das dem DSC zugrundeliegende **Quellenmodell** beschrieben.
- In Absatz 3 Satz 2f. ist gefordert, dass die Registrierung und Nutzung des DSC mit einem Identifizierungsmittel Vertrauensniveau „hoch“ zu erfolgen hat, sowie das dienste- und kartenspezifische Kennzeichen verarbeitet werden kann. In Absatz 4 Satz 5 wird beschrieben, dass der Nutzende sein Konto jederzeit löschen kann. Die **Anmeldung und Nutzendenverwaltung** wird in Abschnitt 2.3. beschrieben
- Um den Anforderungen von Absatz 3 Satz 5 sowie des Absatz 4 Satz 4 Folge zu leisten, erfolgt die Kommunikation zwischen Browser, dem DSC und den angeschlossenen Registern über eine abgesicherte Kommunikation einer **Ende-zu-Ende-Verschlüsselung**, welche in Abschnitt 2.4. beschrieben wird.

- Ein hohes Vertrauensniveau, die in einem Browser zur Anzeige zu bringenden Daten, welche in sicher betriebenen Registern in der Verwaltung gespeichert werden, sowie der Schutzbedarf der personenbezogenen Daten selbst sorgen dafür, dass Datenschutz und Informationssicherheit im DSC ein wesentlicher Faktor sind. Wesentliche Elemente der **Sicherheitsarchitektur** werden in Abschnitt 2.5. beschrieben.
- Zur **Öffentlichen Stelle** für Errichtung und Betrieb des DSC wurde im Jahr 2024 das Bundesverwaltungsamt ernannt. Die FHB als dessen Realisierungspartner arbeitet mit dem BVA eng zusammen. Für den Standard X-DSC ist das BVA ebenfalls als öffentliche Stelle vorgesehen, eine entsprechende Rechtsverordnung ist aktuell in Erarbeitung. Die FHB (hier die Koordinierungsstelle für IT-Standards (KOSIT)) ist auch hier als Realisierungspartner tätig.

Die Umsetzung dieser gesetzlichen Anforderungen wird in den folgenden Abschnitten erläutert.

2.2 Quellenmodell

Eine dauerhafte Speicherung von Daten, welche das DSC abfragt und zur Anzeige bringt, ist im DSC nicht vorgesehen. Da das DSC keine eigenen Daten zur Anzeige bringt, sondern nur die von der Datenquelle erzeugten, bezeichnet man dieses als Quellenmodell (das DSC ist mit anderen Worten zustandslos).

Alle den Nutzenden zur Anzeige gebrachten Daten verbleiben im jeweiligen Register, aus dem sie abgerufen worden sind. Lediglich während einer laufenden Sitzung befinden sich abgerufene Daten auf dem Client der nutzenden Person im Speicher und können von dort aus auch auf deren Endgerät heruntergeladen werden. Nach Beendigung der Sitzung werden sämtliche abgerufene Daten aus dem Speicher gelöscht.

Die implementierte Ende-zu-Ende Verschlüsselung mit Endpunkten im Browser des Clients von am DSC angemeldeten Nutzenden und im jeweiligen Zielregister (bzw. einem für das Zielregister benannten Endpunkt) stützt das Quellenmodell. Alle Backend-Komponenten des DSC dienen lediglich der Orchestrierung der Kommunikation und haben zu keinem Zeitpunkt Zugriff auf die verschlüsselten Inhaltsdaten.

Zudem bedeutet dieses Grundprinzip, dass die Verantwortung, welche Daten wie angezeigt werden bei den jeweiligen Registern liegen. Das DSC verantwortet lediglich die Anzeige der zugelieferten Daten im Browser der Nutzenden.

2.3 Anmeldung und Nutzendenverwaltung

Die gesetzliche Anforderung, bei der Anmeldung und Nutzung des DSCs ein Identifizierungsmittel auf dem Vertrauensniveau „hoch“ zu verwenden, wird über die Identifizierung mittels Personalausweises oder Aufenthaltstitel mit

freigeschalteter Online-Ausweis-Funktion sowie einer dazugehörigen PIN realisiert. Dies entspricht einer 2-Faktor Authentifizierung mittels Wissens (PIN) und Besitz (Personalausweis).

Das DSC verwendet hierzu die AusweisApp2 (AusweisApp2: Software zur Nutzung der Online-Ausweisfunktion) und nutzt zusätzlich einen eID-Service (siehe hierzu: Personalausweisportal - eID-Service). Wie das OZG §10 fordert, ist auch eine Anmeldung über die BundID in der Umsetzung des DSC-Teams (OZG §10 Absatz 3 Satz 4).

Die Nutzenden können wählen, ob das dienste- und kartenspezifische Merkmal ihres Personalausweises gemeinsam mit ihrer Identifikationsnummer im DSC gespeichert werden. Bei den nächsten Anmeldungen erkennt das DSC das Merkmal wieder und ‚spart‘ die wiederholte Abfrage der IDNr beim Identitätsdatenabrufverfahren (IDA-Verfahren). Das IDA-Verfahren ermöglicht den registerführenden Stellen den Abruf der IDNr.

Eine nutzende Person kann ihr Konto jederzeit löschen. Spätestens drei Jahre nach der letzten Anmeldung wird das Konto automatisch gelöscht.

Sollte ein Nutzer während einer Sitzung länger als 10 Minuten inaktiv sein, wird die Session automatisch beendet, um unbefugten Zugriff zu verhindern. Die Nutzenden werden während der Sitzung rechtzeitig über das anstehende Beenden informiert. Sie können ihre Sitzung verlängern oder sich abmelden.

2.4 Ende-zu-Ende-Verschlüsselung

Das Verschlüsselungskonzept des DSCs basiert auf einer durchgehenden Ende-zu-Ende Verschlüsselung mit definierten Endpunkten. Ein fester Endpunkt ist dabei immer der Browser der angemeldeten Person. Der zweite Endpunkt ist vom Zielregister zu bestimmen, mit dem eine Kommunikation aufgebaut werden soll.

Zwischen beiden Endpunkten sorgt eine Verschlüsselung für den sicheren Informationsaustausch.

Diese E2E-Verschlüsselung verhindert Man-in-the-Middle-Angriffe (MITM-Angriffe) auf dem Weg vom Browser zum jeweiligen Register, sowohl in zentralen DSC-Komponenten als auch in sonstigen Zwischenstationen zu den Registern (Intermediäre, Proxies etc.). Keine Komponente zwischen dem Browser einer das DSC nutzenden Person und dem Register kann den symmetrischen Schlüssel entschlüsseln und damit XDSC-Requests einsehen oder valide XDSC-Responses erzeugen. Mehr Informationen zu E2E-Verschlüsselung, Token-Authentifizierung und Verarbeitung des XDSC-Fachnachrichten sind im Dokument „Integrationskonzept-Datenschutzcockpit“ zu finden (Das Dokument kann beider für das DSC verantwortlichen Stelle angefragt werden).

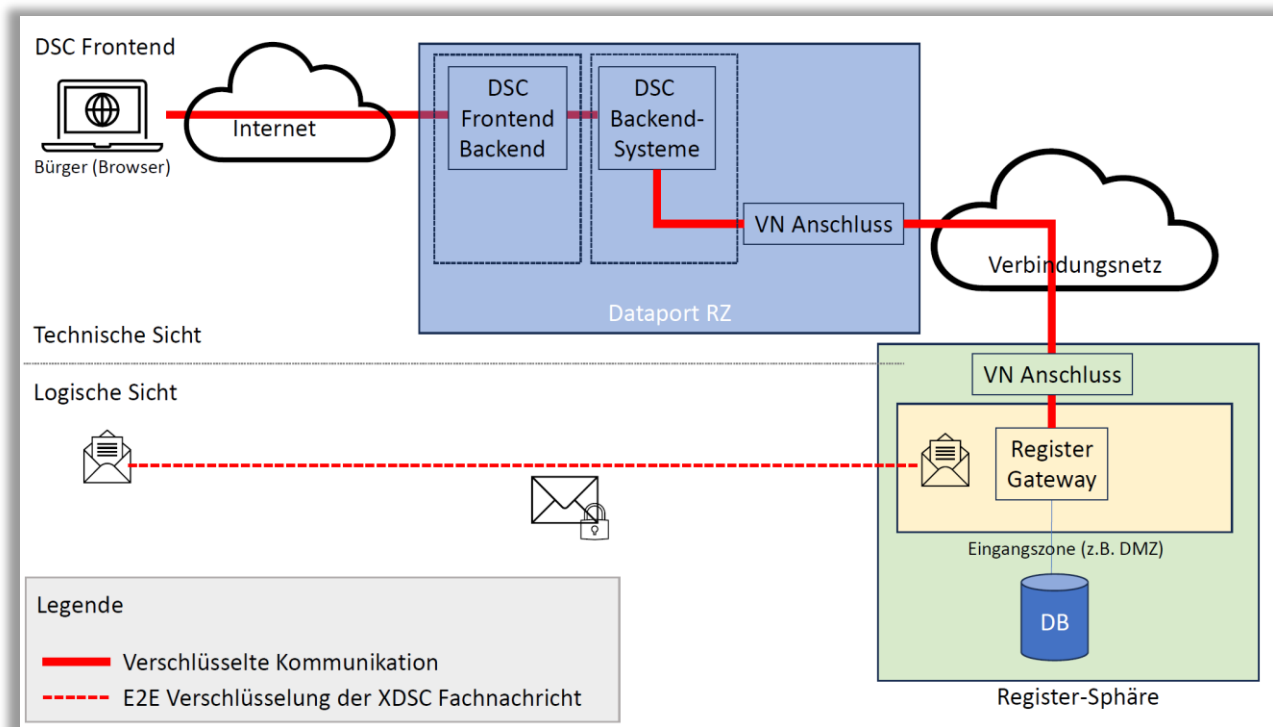


Abbildung 2: Kommunikation des DSC mit den Registern

2.5 Sicherheitsarchitektur

Datenschutz und IT-Sicherheit haben im DSC einen sehr hohen Stellenwert. Die Sicherheitsarchitektur des DSC ist ein wesentlicher Bestandteil der Gesamtarchitektur und besteht aus verschiedenen Kernelementen, die ineinandergreifen und zusammen ein ganzheitliches Konzept zur Gewährleistung der drei wesentlichen Schutzziele der IT-Sicherheit „Vertraulichkeit“, „Verfügbarkeit“ und „Integrität“ bilden.

Neben den bereits in den vorhergehenden Abschnitten beschriebenen Sicherheitsarchitekturen zu Quellenmodell, Anmeldung und Ende-zu-Ende-Verschlüsselung, erfolgt der Betrieb des für das DSC erforderlichen Informationsverbundes in einem Rechenzentrum der öffentlichen Hand, welches nach Bundesamt für Sicherheit in der Informationstechnik (BSI)-Grundschutz zertifiziert ist. Der Informationsverbund schließt Softwarekomponenten sowie die Betriebsinfrastruktur, aber auch alle notwendigen Begleitprozesse, wie beispielsweise sichere Entwicklung, Betriebs-, Patch- und Serviceprozesse ein. In einem mehrstufigen, standardisierten Prozess wird eine umfangreiche Sicherheitsdokumentation erstellt, die alle relevanten Anforderungen der BSI IT-Grundschutzbausteine prüft, auf Anwendbarkeit hin bewertet und den Grad der Erfüllung dokumentiert.

Der Nachweis der IT-Sicherheit wird im DSC neben der BSI-GS Zertifizierung des Informationsverbundes noch auf einer weiteren Ebene erbracht. Neben den fachlichen und technischen internen Tests der Umsetzung der

getroffenen IT-Sicherheitsmaßnahmen durch den technischen Betreiber, erfolgen regelmäßige Penetration-Tests externer Dritter, wie z.B. initial durch das BSI.

2.6 Standard XDSC

Im DSC werden gemäß § 10 Abs.2 Satz 2 OZG keine Protokoll- oder Inhaltsdaten gespeichert, sondern für die Dauer einer Nutzer-Session von den öffentlichen Stellen über eine Schnittstelle abgerufen. Das Format der über die Schnittstelle zu übermittelnden Nachrichten wird im Standard XDSC spezifiziert. Der Standard XDSC ist ein Standard, der den Austausch zwischen dem DSC und den angebundenen Registern definiert. Er stellt sicher, dass alle beteiligten Systeme konsistent und sicher miteinander kommunizieren können. Entwickelt und betrieben wird dieser Standard aktuell von der KoSiT aus Bremen. Der XDSC-Standard umfasst eine Spezifikation, die die Datenstrukturen, Nachrichtenformate und Sequenzen beschreibt, die für den sicheren und transparenten Datenaustausch notwendig sind, sowie ein Fachmodell in XML. Die Transportprofile für die drei möglichen Anbindungen (OSCI, XTA2, XML über HTTP) sind in den Anlagen der Spezifikation aufgeführt.

Gut zu wissen

Im XRepository unter <https://www.xrepository.de/details/urn:xoev-de:kosit:standard:xdatenschutzcockpit> befindet sich die aktuelle Version des Standards XDSC sowie begleitende Dokumentation. Insbesondere empfehlen wir das Dokument zur Spezifikation des XDatenschutzcockpits, welches die technischen Rahmenbedingungen für den Datenaustausch zwischen dem Datenschutzcockpit und den beteiligten Registern beschreibt.

Der Standard XDSC umfasst mehrere technische Aspekte, die für die Implementierung und den Betrieb eines DSCs entscheidend sind. Hier sind einige der wichtigsten technischen Details:

Datenstrukturen

Der Standard definiert spezifische Datenformate und -typen, die für den Austausch zwischen dem DSC und anderen Systemen erforderlich sind. Dies umfasst:

- XML-Schemata: Diese werden verwendet, um die Struktur der Daten zu definieren.

Nachrichtenformate

Für die Kommunikation zwischen dem DSC und anderen Systemen werden standardisierte Nachrichtenformate festgelegt. Diese Formate stellen sicher, dass alle beteiligten Systeme die ausgetauschten Informationen korrekt interpretieren können. Beispiele hierfür sind:

- Anfragen und Antworten: Strukturierte Nachrichten, die spezifische Anfragen und die entsprechenden Antworten enthalten.

Sicherheitsanforderungen

Ein zentraler Aspekt des XDSC-Standards sind die Maßnahmen zur Sicherstellung der Datensicherheit. Dazu gehören:

- Verschlüsselung: Alle Datenübertragungen müssen verschlüsselt erfolgen, um die Vertraulichkeit zu gewährleisten.
- Authentifizierung und Autorisierung: Strenge Mechanismen zur Überprüfung der Identität und der Zugriffsrechte der Benutzer.

Die aktuelle Version des Standards kann im XRepository (<https://www.xrepository.de/details/urn:xoev-de:kosit:standard:xdatenschutzcockpit>) bezogen werden.

2.7 Gesamtsystem DSC

Das DSC besteht aus verschiedenen Komponenten. Zum besseren Verständnis stellt die folgende Abbildung ein Übersichtsdiagramm des Gesamtsystems dar. Die originäre DSC-Sphäre und die mit dem DSC kommunizierenden Peripheralsysteme sind farblich unterschieden:

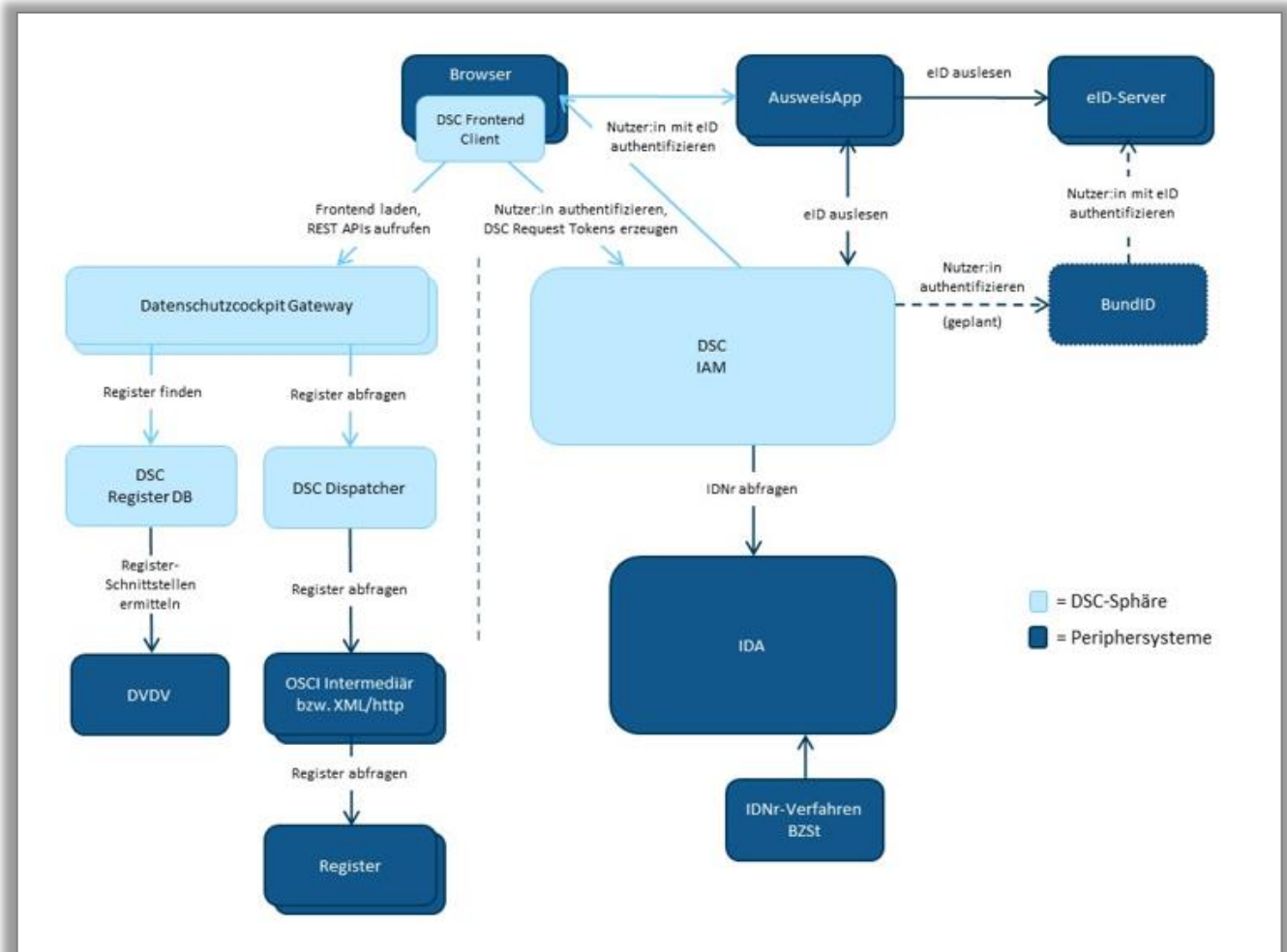


Abbildung 3: Übersicht des Gesamtsystems

Komponente	Zweck
DSC Frontend	Diese Komponente stellt das webbasierte Frontend im Browser der Nutzenden dar.
DSC Gateway	Diese Komponente stellt die notwendigen REST-basierten Schnittstellen für die SPA bereit.
DSC Dispatcher	Diese Komponente stellt eine Schnittstelle bereit, über die Anfragen an die angeschlossenen Register zugestellt werden können. Die Schnittstelle liefert eine synchrone Antwort.

DSC Register DB	Diese Komponente stellt eine DSC-interne Datenbank bereit, aus der Metadaten (Verbindungsparameter, Standard- und Versionsinformationen) zu den Registern abgerufen werden, die vom DSC angesprochen werden können.
DSC IAM	Diese Komponente stellt Funktionen zur Authentifizierung und Autorisierung bereit, sowohl für die Web-Anwendung DSC selbst als auch für die vom DSC angesprochenen Register-Schnittstellen gemäß XDSC. Diese Komponente erzeugt signierte Token für die Kommunikation mit den Registern.

2.8 Schnittstellen zur DSC-Anbindung

Um die von den Registern benötigten Daten abrufen zu können, unterstützt das DSC zwei Formen der logischen Registeranbindung:

1. OSCI-Schnittstelle: Diese Schnittstelle basiert auf dem OSCI-Standard (Online Services Computer Interface) und ermöglicht eine sichere und standardisierte Kommunikation zwischen verschiedenen Verwaltungssystemen.
2. XML-über-HTTP-Schnittstelle („REST“): Diese Schnittstelle nutzt das HTTP-Protokoll zur Übertragung von XML-Daten. Dieses stellt eine flexible und weit verbreitete Methode zur Integration und Kommunikation zwischen Systemen dar.

Im Fall des OSCI-Transportverfahrens werden die spezifischen OSCI-Verbindungsdaten des Register-Endpunkts (WSDL mit OSCI-Zertifikatsinformationen und Intermediär-Endpunkt) von einem DVDV-Server abgerufen. Anschließend wird mit diesen Verbindungsdaten über den jeweiligen OSCI Intermediär des Registers das synchrone OSCI-Backend des Registers angesprochen.

Im Fall vom Transportverfahren XML über http („REST“) werden die spezifischen Verbindungsparameter des Register-Endpunkts von einem DVDV-Server abgerufen. Anschließend wird der Register-Endpunkt mithilfe dieser Parameter und ggfs. zusätzlicher Absicherungslogiken direkt vom DSC angesprochen.

Für die physische Anbindung an das DSC benötigt das Register einen Zugang zum Verbindungsnetz des Bundes und der Länder (NdB-VN).

2.9 DSC User Journey

Um die vorgenannten Grundlagen mit Leben zu füllen, wird nachfolgend die User Journey des DSC beschrieben und in der nachfolgenden Abbildung dargestellt:

- Die Nutzenden melden sich mit Ihrer eID am DSC an. Das DSC liest das dienste- und kartenspezifische Kennzeichen (DKM) sowie den für XBasicdaten notwendigen Datenkranz aus der eID aus.
- Das DSC erfragt beim IDA-Verfahren die zum Datenkranz zugehörige IDNr ab. Diese Nummer ist notwendig, um die Datenübermittlungen zur Person eindeutig zu identifizieren, die in den letzten zwei Jahren über den Nutzenden in den angeschlossenen Registern anzeigepflichtig stattgefunden haben.
- Das DSC speichert nach Zustimmung der Nutzenden die abgefragte IDNr sowie das DKM.
- In einem dreistufigen Abfrageprozess können Anfragen an verschiedene Register gestellt werden, um Informationen über ihre Datenübermittlungen zu erhalten:
 - Eine Statusabfrage fragt ein Register, ob es Datenübermittlungen vorliegen hat. Die entsprechenden Antworten der Register werden an das DSC übermittelt und im Browser angezeigt.
 - Ein Protokolldatenabruf erfolgt, um Art und Umfang von Datenübermittlungen des Registers zu erfahren, d.h. welche Nachrichten zur IDNr vom Register mit welchen Kategorien an Daten wann an wen übermittelt wurden?
 - Der Inhaltsdatenabruf findet statt, um den konkreten Inhalt einer bestimmten Datenübermittlung des Registers abzurufen, welche Nachrichten zur IDNr vom Register mit welchen Inhalten wann an wen übermittelt wurden?
- Auch die abgefragten Protokoll- und Inhaltsdaten werden im Browser dem Nutzenden zur Anzeige gebracht.
- Nach Abmeldung des Nutzenden werden alle angezeigten Daten gelöscht, das DSC ist wieder zustandslos.

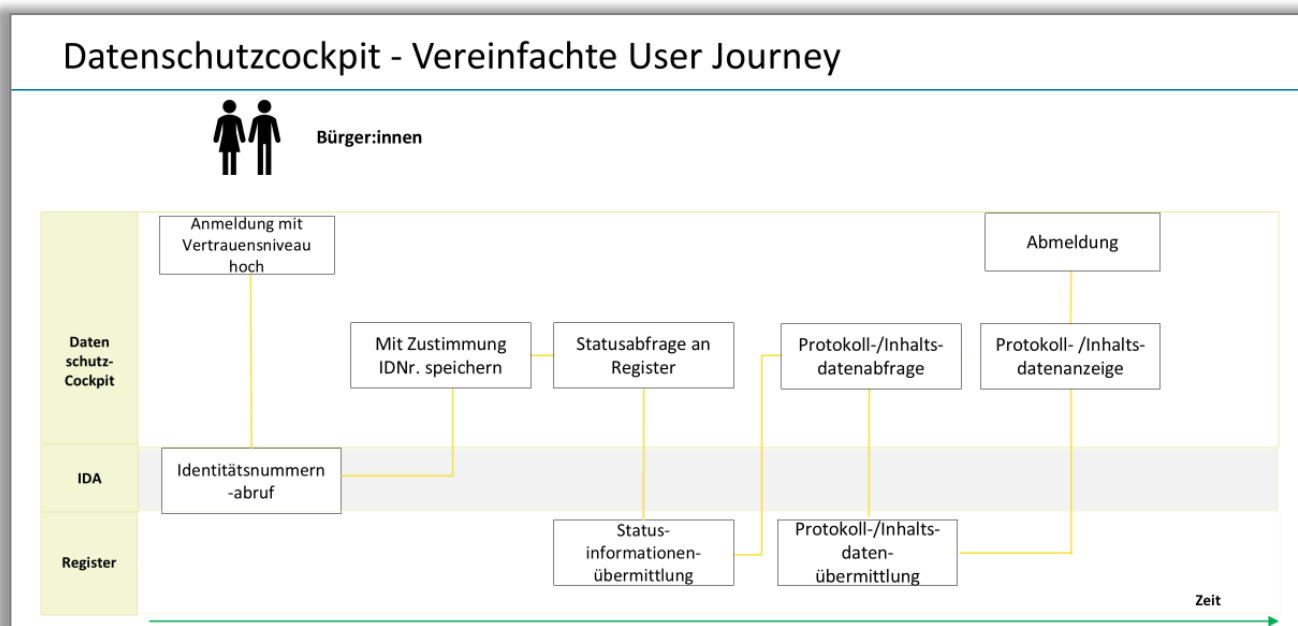


Abbildung 4: Grober Ablauf der User-Journey

3 Registeranbindung Schritt für Schritt

Nach der Einführung in die rechtlichen und technischen Grundlagen des DSC und des Standards XDSC wird in diesem Kapitel der Ablauf eines Register-Anbindungsprojekt in vier Schritten dargestellt. Es werden die einzelnen Schritte erläutert, voneinander abgegrenzt und die Unterstützungsleistungen des DSC-Teams der FHB sowie unterstützende Hilfsmittel wie Checklisten und Werkzeuge vorgestellt.

Das Ziel des Register-Anbindungsprojekt ist die erfolgreiche Produktivsetzung der XDSC-konformen-Schnittstelle des Registers. Über diese Schnittstelle empfängt das Register XDSC-konforme Nachrichten und liefert XDSC-konform Statusinformationen, Protokoll- und Inhalts- sowie zukünftig Bestandsdaten an das DSC, so dass sie dort bürgerfreundlich angezeigt werden können. Fortan besteht für die Bürgerinnen und Bürger die Möglichkeit, sich diese IDNr-basierte Datenübermittlungen des Registers anzeigen zu lassen. Das Register erfüllt damit zugleich die Voraussetzungen für eine erfolgreiche IDA-Nutzung.

Dieser Leitfaden richtet sich an alle Registerverantwortlichen oder ihre Fachverfahrenshersteller mit dem Ziel, die Vorbereitung und Durchführung effizient zu gestalten. In den Leitfaden fließen die aus vorherigen Projekten oder der RegMo-Kommunikation gewonnenen Erkenntnisse und Informationsbedarfe der Register ein. Dieser Anbindungsleitfaden soll ein lebendiges sich weiterentwickelndes Dokument werden, welches durch die Interaktion mit den Beteiligten eines Anbindungsprojektes ständig besser werden soll.

In den nächsten Versionen des Anbindungsleitfadens werden durch das DSC-Team sukzessive weitere Bereiche mit detaillierteren Informationen ergänzt.

Das DSC und der Identitätsdatenabruf (IDA) sind eng miteinander verbunden und spielen gemeinsam eine zentrale Rolle in der Registermodernisierung. Eine geplante oder bereits erfolgte produktive Anbindung an das IDA-Verfahren ist Voraussetzung für eine Anbindung an das DSC. Aufgrund der zeitlichen Koinzidenz der Anbindungen von IDA und DSC orientiert sich dieser Anbindungsleitfaden in seinen Schritten an dem Anbindungsleitfaden für register-

führende Stellen zur Anbindung an IDA (siehe unter https://www.bva.bund.de/SharedDocs/Downloads/DE/Behörden/Verwaltungsdienstleistungen/Registermodernisierung/Anbindungsleitfaden_IDA.pdf), welcher in der folgenden Abbildung dargestellt ist.

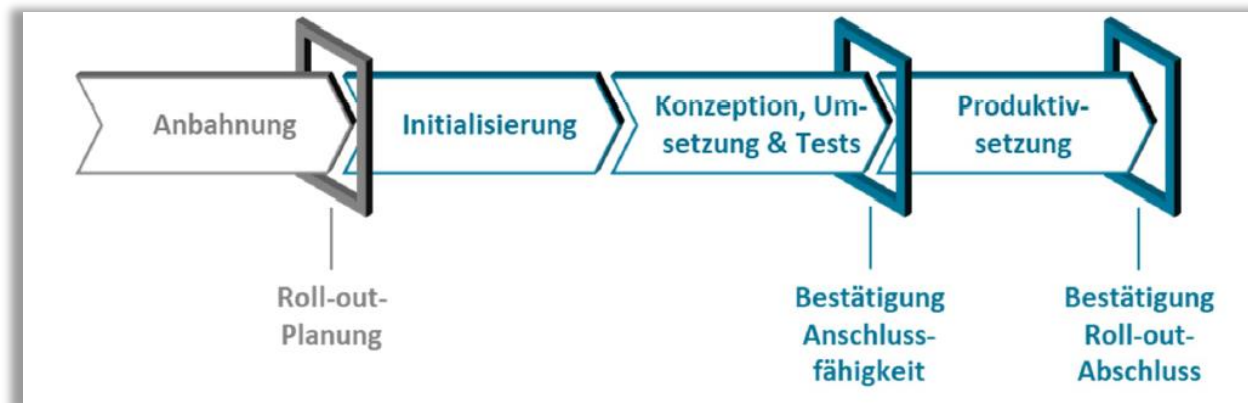


Abbildung 5: Vorgehensmodell zur IDA-Anbindung

Mit der Anbindung an IDA und der anschließenden Nutzung des IDA-Verfahrens entsteht die Notwendigkeit, dass sich das Register auch an das DSC produktiv anschließt. Dabei ist zu beachten, dass der initiale Abruf der IDNr keine Datenübermittlung im Sinne des § 9 Abs. 1 IDNrG darstellt und daher nicht im DSC angezeigt werden muss. Die Anzeigepflicht gilt jedoch für Abrufe zur Datenaktualisierung, die unter Verwendung der IDNr durchgeführt werden.

Die registerführenden Stellen, die ein Register gemäß der Anlage zu § 1 IDNrG führen, sind verpflichtet, die IDNr als zusätzliches Ordnungsmerkmal bis Ende 2028 in ihr Register zu speichern und ihre (Basis-)Daten durch die (Basis-)Daten des Bundeszentralamts für Steuern (BZSt) zu ersetzen. Zu diesem Zweck stellt das BVA den betroffenen Stellen das IDA-Verfahren zur Verfügung. Ein Pilotprojekt wurde bereits mit dem Nationalen Waffenregister (NWR) durchgeführt, um die technischen Voraussetzungen und die praktische Umsetzung zu testen. Die Ergebnisse dieser Erprobung sollen als Grundlage für die weitere Anbindung anderer Register dienen.

3.1 Exkurs: Registerarten

Im Rahmen des Registermodernisierungsgesetzes bezeichnet der Begriff „Register“ die elektronisch geführten Datensammlungen innerhalb einer Behörde. Das IDNrG hat insgesamt 50 Register identifiziert (*siehe Anlage (zu § 1) in <https://www.gesetze-im-internet.de/idnrg/BJNR059110021.html>*), in die eine bereichsübergreifende IDNr als allgemeines Ordnungsmerkmal für natürliche Personen integriert werden soll. Diese Register dürfen die IDNr in ihren Datenübermittlungen nur verwenden, wenn sie an das DSC angeschlossen sind.

Bei der Anbindung von Registern lassen sich zwei verschiedene Anbindungsfälle unterscheiden –zentrale und dezentrale Register.

Fallunterscheidung (nach Registerarten)

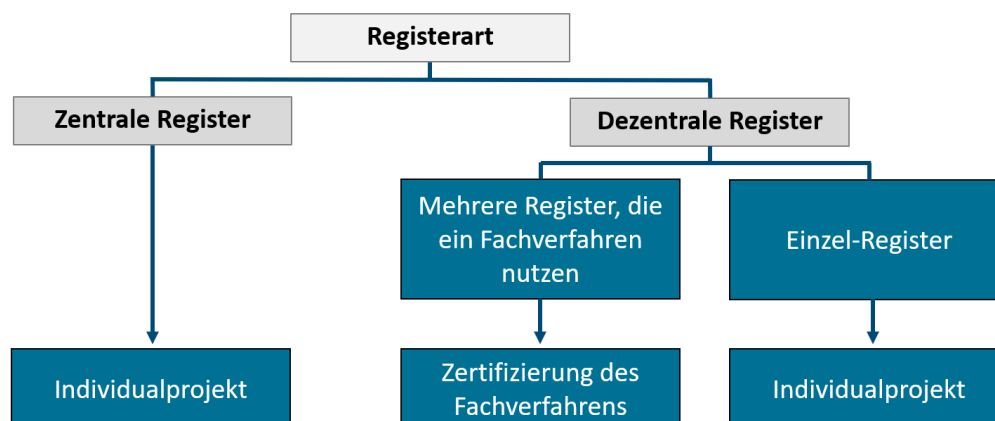


Abbildung 6: Fallunterscheidungen bei der Anbindung von Registern

Diese beiden Anbindungsfälle werden nachfolgend genauer beschrieben.

1. Anbindung von zentralen Registern

Zentrale Register sind Register, welche einmalig in Deutschland sind und deshalb individuell an das DSC angebunden werden. Beispiele für zentrale Register auf Bundesebene sind das Nationale Waffenregister, Zentrales Fahrzeugregister, etc. Zentral geführte Register nutzen in der Regel Individualsoftwarelösungen und verfügen meistens über eine zentrale Organisation. Die Anbindung dieser Register erfolgt über individuell aufgesetzte Projekte, um maßgeschneiderte Lösungen zu realisieren. Die registerführende Stelle ist sowohl für die fachliche und technische Ertüchtigung des Registers als auch für die Anbindung an das DSC verantwortlich.

2. Anbindung von dezentralen Registern

Dezentrale Register sind i.d.R. nicht einmalig, sondern in einer Mehrzahl in der Verwaltung auf verschiedenen Ebenen (Bund, Länder, Kommunen) im Einsatz. Dezentrale Register werden in der Regel in Verbindung mit einem Fachverfahren betrieben. Ein Beispiel für dezentrale Register sind die über 5.000 Melderegister, die Einwohnerdaten auf kommunaler Ebene in einem Fachverfahren bearbeiten und speichern.

Aufgrund der Vielfalt der eingesetzten Fachverfahrensprodukte und deren Versionen strebt das DSC-Projekt an, eine konformitätsgeprüfte DSC-Anbindung mittels einer Zertifizierung von Fachverfahrensherstellern und deren DSC-Schnittstelle (mit dem Datenaustauschformat XDatenschutzcockpit) zu erreichen. Von diesem standardisierten Vorgehen erhofft sich das DSC-Team eine reduzierte Komplexität der Anbindung, einen beschleunigten Rollout sowie einen fehler-minimalen und kostengünstigeren Rollout und Betrieb.

Dezentrale Register, die kein Fachverfahren nutzen, werden wie Einzelregister und damit wie Zentrale Register behandelt.

Dezentrale Register, die ein nicht zertifiziertes Fachverfahren nutzen, wenden sich entweder an ihren Fachverfahrenshersteller mit der Bitte um Zertifizierung oder wählen den Weg der o.a. Einzelregisteranbindung.

Der aktuelle Leitfaden betrachtet zurzeit die Anbindung von zentralen oder Einzel-Registern an das DSC. Eine Fortschreibung für die dezentrale Register i.S. einer Fachverfahrenszertifizierung erfolgt in einer der nächsten Versionen des DSC-Anbindungsleitfadens. Im Folgenden wird der Ablauf der einzelnen Anbindungsschritte eines zentralen/Einzel- Registers beschrieben.

3.2 Ablauf des DSC-Anbindungsprojektes

Das IDA-Vorgehensmodell besteht im Wesentlichen aus den vier nachfolgend aufgeführten Phasen. In allen vier Phasen werden die Aufgaben des Anbindungsteams, bestehend aus Vertretern der registerführenden Stellen, und dem DSC-Team, beschrieben. Die Verantwortung für die Planung und Umsetzung der DSC-Anbindung liegt bei der registerführenden Stelle. Das DSC-Team begleitet auf Anforderung beratend und unterstützend die Vorbereitung und Umsetzung der DSC-Anbindung des Registers. Die Integrationstest vor der Produktivsetzung der Schnittstelle werden dann gemeinsam durchgeführt.

Die dargestellten Quality Gates müssen erfolgreich erreicht worden sein, um in die nächste Phase überzugehen.

Ein grober Zeitrahmen der Anbindung orientiert sich hierbei am Anschluss an das IDA-Verfahren, da die Anbindung von IDA und DSC Hand in Hand erfolgen müssen.

3.3 Anbahnung

In der Anbahnungsphase des DSC-Anschlussprojektes werden die grundlegenden Voraussetzungen für die Anbindung eines Registers geschaffen. Diese Phase umfasst folgende Aufgaben:

- **Kontaktaufnahme und Planung:** Die registerführende Stelle nimmt Kontakt mit dem DSC-Team auf, um die Anbindung zu planen und erste notwendige technische und organisatorische Voraussetzungen zu klären.
- **Technische Vorbereitung:** Es werden technische Anforderungen definiert und die IT-Infrastruktur vorbereitet, um den Anschluss an das DSC zu ermöglichen.

Anbahnungsworkshop: Das DSC-Team empfiehlt in dieser Phase die Organisation eines Anbahnungsworkshops, in dem grundlegende Fragen der Anbindung an das DSC geklärt werden. In diesem Workshop können technische

Anforderungen und Voraussetzungen geklärt, erste technische Festlegungen für die Schnittstellen getroffen, die Datenquellen und -strukturen identifiziert sowie die Verantwortlichkeiten und Art der Zusammenarbeit bestimmt werden.

Quality Gate: Auf der Grundlage der ersten Festlegungen des Registers stimmen das Register und das DSC-Team den zeitlichen Beginn und die Gesamtdauerzeit des Anbindungsprojektes gemeinsam ab.

3.3.1 Checkliste: Anbahnung

Nachfolgende Fragenstellungen müssen bei den Registern bedacht werden, um einen möglichst reibungslosen Ablauf des Anbahnungsschrittes zu gewährleisten:

Nr.	Frage
1	Wurde bereits eine IDA-Rollout-Planung abgestimmt? Ist der Anschluss an das IDA-Verfahren bereits terminiert?
1.1	Ist die Vereinbarung zur Umsetzung des Identifikationsnummerngesetzes / Projektsteckbrief bereits in Erstellung?
2	Ist der Standard XDSC in der aktuellen Version bekannt und zur Kenntnis genommen? https://www.xrepository.de/details/urn:xoev-de:kosit:standard:XDSC
2.1	Hat die registerinterne Definition der anzeigepflichtigen Daten (wichtig u. a. der Fachdaten) begonnen, die unter Verwendung der Identifikationsnummer an oder von anderen öffentlichen Stellen übertragen oder dauerhaft gespeichert werden? <u>Anmerkung:</u> Hierbei sind die geltenden Vorgaben z.B. aus der Spezifikation XDSC, der eigenen Fachdomäne, den fachgesetzlichen Vorgaben und den Gesetzen/Verordnungen (insbesondere RegMoG und IDNrG) zu berücksichtigen.
2.2	Gibt es eine Entscheidung/ Aussage aus der fachlichen Entscheidungsebene (wie bespw. Fachministerkonferenz), die Vorgaben dazu macht, wie die Anbindung der Register an das Datenschutzcockpit aussehen soll?
2.3	Welche Protokoll- und Inhaltsdaten sollen zur Anzeige gebracht werden? a) Anlass (Welcher Antrag?) b) Kategorie(n) der übertragenen Daten? c) Zeitpunkt der IDNr- Nutzung? d) von welcher Behörde (Kommune bzw. Wohnortgemeinde)?

	e) an welche Behörde? f) Inhalt der übertragenen Daten?
2.4	Welche Bestandsdaten zu der jeweiligen IDNr befinden sich im Register? Anmerkung: Die Bestandsdatenanzeige ist noch nicht im DSC umgesetzt
3	Sind die technischen Rahmenbedingungen für die physische und logische Anbindung an das DSC ermittelt worden?
3.1	Welche Form der Anbindung soll genutzt werden? • Physisch: Zugang zum NdB oder VN • Logisch: Über die Schnittstellen REST oder OSCI?
3.2	Kann die Datenübertragung von Protokoll-, Inhalts- und Bestandsdaten synchron erfolgen? <u>Anmerkung:</u> Erwartete Response-Zeit liegt bei < 500ms
4	Gibt es bereits eine Projektorganisation?
4.1	Wie ist das Projektteam aufgebaut?
4.2	Wer ist der Ansprechpartner für das DSC-Team und wie erfolgt der Austausch?

3.3.2 Unterstützung des DSC-Teams - Anbahnung

Nachfolgende Leistungen werden Registern durch das DSC-Team unterstützend bereitgestellt, um einen möglichst reibungslosen Ablauf des Anbindungsprojektes in der Anbahnungsphase zu gewährleisten:

- ✓ Beteiligung an den Abstimmungsprozessen zur Erstellung der Vereinbarung mit dem BVA , welche die Meilensteinplanung für den Anschluss an das IDA-Verfahren und an das DSC beinhaltet
- ✓ Mitwirkung bei der Durchführung von Workshops
- ✓ Einladung zur Teilnahme an den Sprechstunden/Informationsveranstaltungen (z.B. Sprechstunde XDSC)
- ✓ Beantwortung von Fragen und Bereitstellung von Informationen s. 7.2.:

3.4 Initialisierung

In dieser Phase erfolgt die konkrete zeitliche und organisatorische Planung der Umsetzungsschritte zum Anschluss an das DSC.

Quality Gate: Die Vereinbarung mit dem BVA ist geschlossen. Die Ziele, Anforderungen und Vorgehen des Anbindungsprojekts, einschließlich der technischen und rechtlichen Rahmenbedingungen sind festgelegt.

3.4.1 Checkliste: Initialisierung

✓/X	Frage
1	Sind die technischen und rechtlichen Anforderungen für die Konzeption der Anbindung geklärt und beschrieben?
1.1	Die Rechtsgrundlage ist geklärt
1.2	Die logische und physische Anbindung ist beschrieben
1.3	Werden die Daten über IDNr-basierte anzeigepflichtige Datenübermittlungen der letzten zwei Jahre im eigenen Datenbestand für die DSC-Abrufe vorhanden und auf die Datenstruktur gemäß XDSC angepasst sein?
1.4	Ist der mehrstufige Abruf der Datenübermittlungen gem. XDSC gewährleistet, d.h. Empfang der XDSC-Nachrichten und Bereitstellung der Antworten zu Status-, Protokoll und Inhaltsdaten?
1.5	Ist die hohe Verfügbarkeit des Registers für eine 7x24 synchrone Kommunikation mit dem DSC sichergestellt? <u>Anmerkung:</u> Register, die an das Datenschutzcockpit angeschlossen sind, müssen prinzipiell eine hohe Verfügbarkeit haben (Das DSC selbst kalkuliert mit einer Systemverfügbarkeit von 98,5%) und sollten innerhalb von 500 Millisekunden angefragte Daten liefern. Es ist vorgesehen, dass Nutzende die Daten bei allen angebundenen Registern jederzeit abrufen können. Sollte ein Register beispielsweise aus technischen Gründen temporär nicht verfügbar sein, so wird den Nutzenden mitgeteilt, dass die Behörde aus technischen Gründen nicht erreicht wurde.

2	Sind die für das Anbindungsprojekt notwendigen Ressourcen, wie Personal, Budget und technische Infrastruktur identifiziert und bereitgestellt?
3	Ist ein gemeinsamer Zeitplan und die vom DSC-Team erwarteten Mitwirkungsleistungen beschrieben?
4	Ist die Vereinbarung mit dem BVA inhaltlich unterschriftsreif abgestimmt?

3.4.2 Unterstützung des DSC-Teams - Initialisierung

Neben den bereits in dem Schritt Anbahnung beschriebenen Unterstützungsleistungen bietet das DSC-Team den Registern die folgenden Leistungen an:

- ✓ Beratende Unterstützung bei der Planung der DSC-Meilensteine bezogen auf die Meilensteinplanung der Vereinbarung mit dem BVA
- ✓ Klärung von technischen Fragen zur Anbindung
- ✓ Definition und Planung des individuellen Unterstützungsbedarfs des Registers für die Konzeption, Umsetzung & Test

3.5 Konzeption, Umsetzung & Tests

In diesem Schritt erfolgt die eigentliche Umsetzung der Anbindung des Registers an das Datenschutzcockpit. Aufgehend von den zuvor definierten Anforderungen konzipiert und entwickelt das Register eine XDSC-konforme Schnittstelle. Anschließend wird die Schnittstelle gemeinsam mit dem DSC-Team getestet. Das Register sorgt zudem dafür, dass die erforderlichen datenschutzrechtlichen Maßnahmen umgesetzt sind.

Quality Gate: Das Register bestätigt gegenüber dem BVA und dem DSC-Team, dass die Voraussetzungen für den Anschluss an das DSC vorliegen.

3.5.1 Checkliste: Konzeption, Umsetzung & Tests

✓/X	Frage
	<u>Konzeption und Umsetzung</u>

1	Fließt der Standard XDSC in der aktuellen Version in die Konzeption ein?
1.1	Stimmt die Datenstruktur der an das DSC zu übermittelnden Daten mit der Struktur gemäß XDSC überein?
1.2	Wird die „Bürgerlesbarkeit“ der übermittelnden Daten gewährleistet? <u>Anmerkung:</u> Gemäß §10 des OZG sollen Datenübermittlungen "aus Sicht des Nutzers einfach und zweckmäßig" gestaltet sein. Das DSC kann nur auf einer sehr allgemeinen Ebene Vorgaben zur Bürgerlesbarkeit machen, die sich aus den Pflichtfeldern des Standards XDSC ergeben. Die Prüfung liegt daher bei der registerführenden Stelle. Es ist möglich, dass im Zuge der fortschreitenden Anbindung und Nutzung des DSC durch Nutzenden Best-Practice-Ansätze für diese Thematik entstehen, die vom Projekt DSC gesammelt und zukünftig registerführenden Stellen im Rahmen der Anbindungsprojekte zur Verfügung gestellt werden.
2	Ist die logische und physische Anbindung an das DSC (REST/OSCI, Zertifikate, IP-Adressen etc.) konzipiert und umgesetzt?
2.1	Wurden alle IT-Sicherheitsrelevanten Aspekte der Anbindung berücksichtigt? <u>Anmerkung:</u> Erforderlich sein können Datenschutzkonzepte für Anbindung und Datenbereitstellung, IT-Sicherheitskonzepte, Sicherheitsbeurteilung (abhängig von registerinterner Vorgabe und technischer Lösung).
2.2	Wurde das Verschlüsselungskonzept berücksichtigt? <u>Anmerkung:</u> Bei OSCI ist die Verschlüsselung bereits im Transportprotokoll enthalten. Da dieses bei XML über HTTP derzeit noch nicht standardisiert ist, ist ein Verschlüsselungskonzept zu erstellen.
2.3	Ist ein Eintrag im DVDV mit der Hinterlegung des Zertifikats gemäß DVDV-Eintragungskonzept für XDSC erfolgt?
2.4	Wurden die konkreten Freischaltungen und (Client-)Zertifikate für die Anbindung an das DSC beantragt, implementiert und auf ihre grundsätzliche Erreichbarkeit getestet?

	<u>Anmerkung:</u> Die über NdB oder VN erreichbaren Endpunkte müssen zwischen dem DSC-Team und dem anzubindenden Register vorab ausgetauscht werden und jeweils gegenseitig entsprechende Freischaltungen beantragt werden. <u>Anmerkung:</u> Es gibt unterschiedliche Endpunkte z.B. für Produktions- und Testumgebungen. <u>Anmerkung:</u> Es Zertifikaten der PKI-1 zu verwenden, welche über DOI/telesec beantragt und anschließend im DVDV hinterlegt werden.
3	Sind die Tools XDSC-Viewer und dem DSC-Simulator bekannt und werden sie in der Umsetzung eingesetzt? <u>Anmerkung:</u> Die Beschreibung der Tools befindet sich im nächsten Unterkapitel. Ein erfolgreicher Test mit dem DSC-Simulator ist Voraussetzung für die weiteren Testphasen.
4	Sind die begleitenden Informationen z. B. Register-Kontaktdaten, zuständiger Datenschutz für das DSC definiert und an das DSC-Team übergeben?
5	Sind alle notwendigen Freigaben definiert und die dafür relevanten Stakeholdern identifiziert und informiert?
	<u>Test</u>
1	Liegen gemeinsam zwischen Register und dem DSC-Team definierte Testdaten für die verschiedenen Use-Cases z.B. für den Statusabruf, die Übermittlung von Protokoll- und Inhaltsdaten, sowie von Fehlermeldungen vor? <u>Anmerkung:</u> Eine Bibliothek an Testcases mit erwarteten Ergebnissen, Fehlermeldungen und einem Basis-Testdatensatz ist gerade beim DSC-Team in Erarbeitung.
2	Können erfolgreich Testdatenabrufe mit den Testdaten in der Testumgebung durchgeführt werden und es liegen keine Fehler vor? Die Schnittstelle liefert auf beiden Seiten, dem Register und dem DSC, fehlerfreie Ergebnisse.
3	Sind die notwendigen Dokumentationen und Prozessbeschreibungen erstellt/aktualisiert worden?
4	Wird die IDNr als neues Ordnungsmerkmal im Register aktiv/produktiv gespeichert (§ 2 Nr. 1 IDNrG)?
4.1	Wird die IDNr und weitere Basisdaten initial abgerufen (§ 2 Nr. 2 IDNrG)?

4.2	Werden alle technischen und organisatorischen Maßnahmen zur Protokollierung nach § 9 Abs. 1 IDNrG umgesetzt?
5	Sind die organisatorischen Prozesse und Supportstrukturen definiert, um bei Störungen oder Rückfragen der Nutzer angemessen reagieren zu können? <u>Anmerkung:</u> Sind diese mit dem DSC-Team besprochen.
6	Ist das Datum der Produktivsetzung festgelegt und den relevanten Stakeholdern kommuniziert?
7	Liegen alle notwendigen Freigaben vor?

3.5.2 Unterstützung des DSC-Teams – Umsetzung

Neben den bereits in den vorherigen Schritten beschriebenen Unterstützungsleistungen bietet das DSC-Team dem Register die folgenden Leistungen an:

- ✓ Beratende Unterstützung bei Rückfragen zur Konzeption der Schnittstelle.
- ✓ Bereitstellung eines Werkzeugs zur Visualisierung der an das DSC übermittelten Daten (XDSC-Viewer)
- ✓ Bereitstellung eines Werkzeugs zur Simulation des Datenaustauschs inkl. Verschlüsselung (DSC-Simulator)
- ✓ Gemeinsame Definition eines Testplanes für Testdaten und Testcases auf der Basis bereits erfolgter Integrationstests und deren Datenpool und UseCases
- ✓ Unterstützung bei der technischen Anbindung an das DSC-Team (IP-Freischaltung und Überprüfung der Erreichbarkeit)
- ✓ Gemeinsame Durchführung der Integrationstests gem. Testplan
- ✓ Unterstützung bei Bestätigung der Anschlussfähigkeit

▪ DSC-Simulator

Der DSC-Simulator ist ein Tool, um die Funktionsweise der XDSC-Kommunikation mit dem DSC zu simulieren. Mit diesem Tool können die registerführenden Stellen den Empfang von XDSC-Anfragen und deren Beantwortung sowie die Verschlüsselung von Anfragen und Antworten simulieren. Die Anwendung wird dabei lokal bei den registerführenden Stellen gestartet. Anschließend kann für Statusdaten, Protokolldaten und Inhaltsdaten die Kommunikation (Anfragen und Antworten) mit dem DSC simuliert werden.

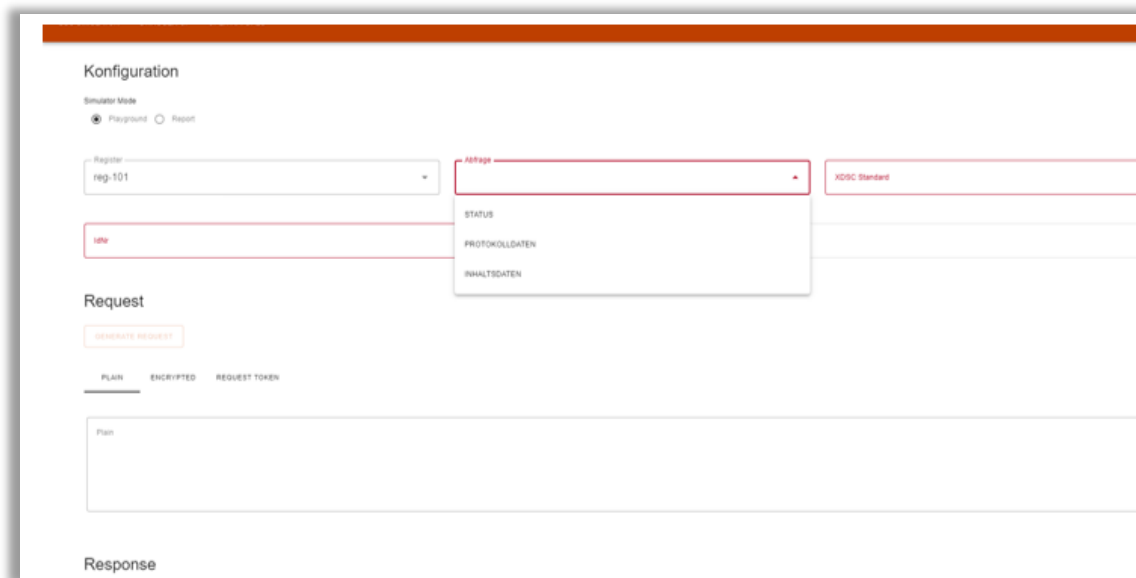


Abbildung 7: Screenshot DSC Simulator Auswahl Request Typ

Der Simulator wird als Docker-Container bereitgestellt. Der XDSC-Simulator wird immer für die aktuelle Version des XDSC-Standards bereitgestellt. Das Register sollte dieses prüfen.

■ XDSC-Viewer

Der XDSC-Viewer ist ein Tool, das die XSC-spezifischen XML-Nachrichten in eine grafische Darstellung umwandelt. Mit diesem Tool können die registerführenden Stellen sich visualisieren lassen, wie das DSC ihre XML-basierten Nachrichten aus dem Register anzeigt. Das Tool wird die Status-, Protokoll- und Inhaltsdaten des Registers so darstellen, wie sie im DSC zur Anzeige gebracht werden. Die Daten können zuvor mit dem DSC-Simulator erzeugt und anschließend im XDSC-Viewer getestet werden.

Die Benutzeroberfläche ermöglicht die Auswahl von Registern und das Starten von Anfragen. Abfragedaten werden als XML-Dateien in spezifischen Ordnern abgelegt. Die Oberfläche zeigt zunächst die Statusdaten an. Durch Klicken auf Einträge werden Protokolldaten und anschließend Inhaltsdaten angezeigt.

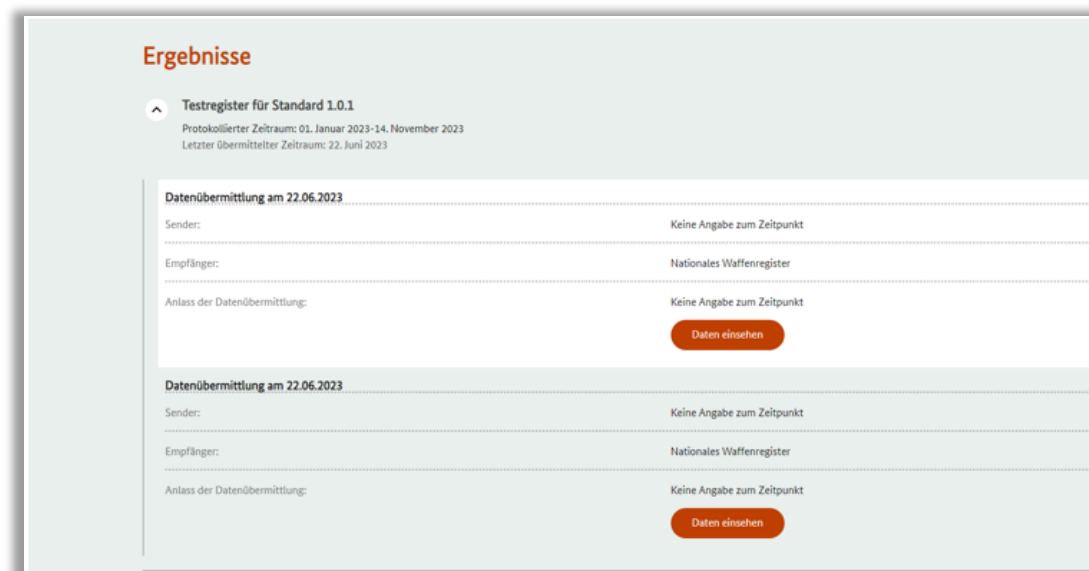


Abbildung 8: Screenshot XDSC-Viewer – Übersicht Protokolldaten

Der XDSC- Viewer steht zum Download bereit und ist anschließend lokal zu installieren. Der XDSC-Viewer wird immer für die aktuelle Version des XDSC-Standards bereitgestellt. Die registerführende Stelle sollte dieses prüfen.

Es werden vom DSC-Team zwei Werkzeuge für anzubindende Register bereitgestellt, welche bei der Umsetzung der Schnittstelle hilfreich sind. Die beiden Tools werden auf Anfrage an dsc-service@governikus.de bereitgestellt:

3.6 Produktivsetzung

In dieser Phase erfolgt die Inbetriebnahme und die Überführung in den Regelbetrieb. Die auf der Integrationsumgebung erfolgreich getestete Schnittstelle wird vom DSC und dem Register auf dem jeweiligen Produktivsystem(-en) bereitgestellt. Die Nutzenden können das Register im DSC erkennen und auswählen und sich Informationen zu den Datenübermittlungen anzeigen lassen. Damit endet das Anbindungsprojekt. Die Registeranbindung wird ab jetzt im Regelbetrieb verantwortet.

3.6.1 Checkliste: Produktivsetzung

✓/X	Frage
	Ist die Schnittstelle auf dem Produktivsystem(-en) eingespielt?

3.6.2 Unterstützung des DSC-Teams: Produktivsetzung

Neben den bereits in den vorherigen Schritten beschriebenen Unterstützungsleistungen bietet das DSCTeam dem Register die folgende Leistung an:

- ✓ Mitwirkung bei den Schritten der Produktivsetzung

4 DSC-Team und weitere Informationen

Das Anbindungsteam DSC unterstützt die registerführenden Stellen in allen Phasen des Anbindungsprojekts zum einen durch das Engagement seiner Teammitglieder (s. Abschnitt 7.1.). Zum anderen stellt es allen Interessierten weiterführende Informationen zur Verfügung (s. Abschnitt 7.2.).

4.1 DSC Team

Die nachfolgende Grafik zeigt, welche Mitglieder des DSC-Teams in welcher Phase das jeweilige Anbindungsprojekt begleiten:

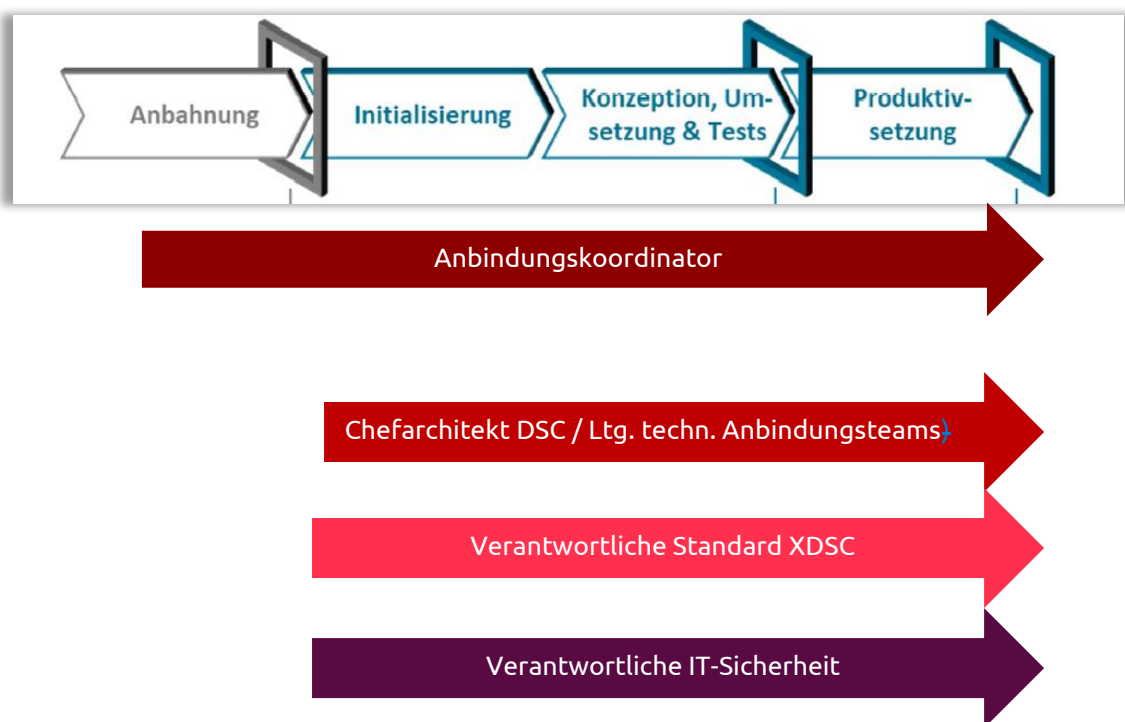


Abbildung 7: Umsetzungsschritte und Rollen DSC-Team

4.2 Weiterführende Informationen

Das DSC-Team stellt die folgenden Informationen und Werkzeuge zur Vorbereitung und Vertiefung der DSC-Anbindung zur Verfügung:

- **OZG § 10 Datenschutzcockpit:**
https://www.gesetze-im-internet.de/ozg/_10.html

- **Spezifikation des Standards XDatenschutzcockpit:**
<https://www.xrepository.de/details/urn:xoev-de:kosit:standard:xdatenschutzcockpit>
- **Integrationskonzept Datenschutzcockpit:**
Auf Anfrage beim Anbindungsteam DSC: datenschutzcockpit@finanzen.bremen.de
- **DVDV-Eintragungskonzept XDSC:**
<https://docs.fitko.de/dv dv/pflegende-stellen/Eintragungskonzepte/>
[DVDV-Eintragungskonzept XDatenschutzcockpit 1.0.1](#)
- **FAQ: Häufig gestellte Fragen zum Datenschutzcockpit:**
<https://www.finanzen.bremen.de/digitalisierung/digitalisierungsbuero/datenschutzcockpit/faq-haeufig-gestellte-fragen-zum-datenschutzcockpit-123768>
- **XDSC Viewer und -Simulator:**
Auf Anfrage bei: dsc-service@governikus.de
- **IDA-Anbindungsleitfaden:**
https://www.bva.bund.de/SharedDocs/Downloads/DE/Behoerden/Verwaltungsdienstleistungen/Registriermodernisierung/Anbindungsleitfaden_IDA.pdf

Dieser Leitfaden kann nur durch Ihr Feedback verbessert werden. Daher freut sich das DSC-Team (datenschutzcockpit@finanzen.bremen.de) über Anmerkungen und Verbesserungswünsche, um den Leitfaden weiter zu optimieren und den Bedürfnissen seiner Adressaten immer gerechter zu werden.