



Bundesministerium  
des Innern

# Meldewesen, Personalausweis, Bürgerportale - Bausteine einer elektronischen Identitätsmanagement- Infrastruktur des Bundes



**Jan Möller**

**Projektleiter „Elektronischer Personalausweis“  
IT-Stab im Bundesministerium des Innern**

**E-Government in medias res**

**Bremen, 12.07.2007**



## Auftrag



- „Unser moderner Staat braucht eine innovative, leistungsfähige und effiziente Verwaltung. Deshalb werden wir den mit „Deutschland online“ begonnenen Weg fortsetzen und staatliche Zusammenarbeit auf der Basis der Informationstechnologie (IT) neu ordnen, um damit gezielt Bürokratiekosten zu reduzieren. Durch die Einführung zentraler und IT-gestützter Verfahren bei den wichtigsten Dienstleistungen des Staates für Unternehmen und Bürger (eGovernment) wollen wir eine führende Rolle für eine innovative und Kosten sparende Verwaltung übernehmen. IT-Strategie und IT-Sicherheit werden durch das Bundesministerium des Innern als Sicherheits- und Organisationsministerium weiterentwickelt.“
- „Eine moderne Sicherheitsarchitektur muss moderne Informationstechnik unter Wahrung des Datenschutzes konsequent einbeziehen. Daher wollen wir biometrische Verfahren verstärkt einsetzen (Pässe, Personalausweise, Visa, Aufenthaltstitel) und dazu das Pass- und Personalausweisgesetz novellieren.“...

Koalitionsvertrag vom 11.11.2005



## Auftrag



- „Der Personalausweis erfüllt als staatlich bereitgestelltes Hochsicherheitsdokument die Anforderungen für eine sichere und einfache Identifizierung. Eine vergleichbare, einfache und sichere Identifizierung ist auch für das elektronische Handeln zu vertretbaren Kosten für die Nutzerinnen und Nutzer bereitzustellen. Ab 2008 wird der elektronische Personalausweis dies sicherstellen.“

Programm eGovernment 2.0

- „Die Einführung eines elektronischen Personalausweises für das Internet, die die Bundesregierung angekündigt hat, schafft eine notwendige Infrastruktur zur Bekämpfung von Online-Identitätsmissbrauch. Damit werden Online-Anwendungen sicherer und komfortabler nutzbar und neue Anwendungen in Wirtschaft und Verwaltung möglich.“

Nationaler IT-Gipfel vom 18.12.200



# Deutschland – Strategie zum Thema Identifizierung

## Projekte:

- ePass
- elektronischer Personalausweis
- Visa
- elektronische Aufenthaltstitel
- elektronischer Dienstausweis
- Melderegister
- .....

Die Biometrie-Strategie bezieht sich auf unmittelbar verfügbare Daten.

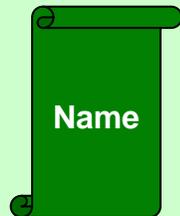


Gesichtsbild

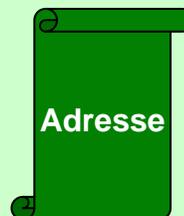


Fingerabdrücke

Die eldentity-Strategie bezieht sich auf den Umgang mit elektronisch verfügbaren Repräsentationen von Daten.



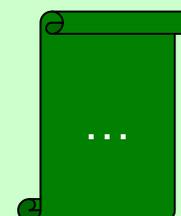
Name



Adresse



Geb.-  
datum



...



# Strategien und Kartenprojekte

*Hoheitliche  
Einsatzfelder*



ePass

**Biometriestrategie**



VISA

**Elektronischer  
Personalausweis,  
elektronische  
Aufenthaltstitel**

**Strategie  
Elektronisches  
Identitätsmanagement  
(z.B. Meldewesen)**

**IT-Sicherheit  
(z.B. Zugangs- und  
Zutrittskontrolle)**

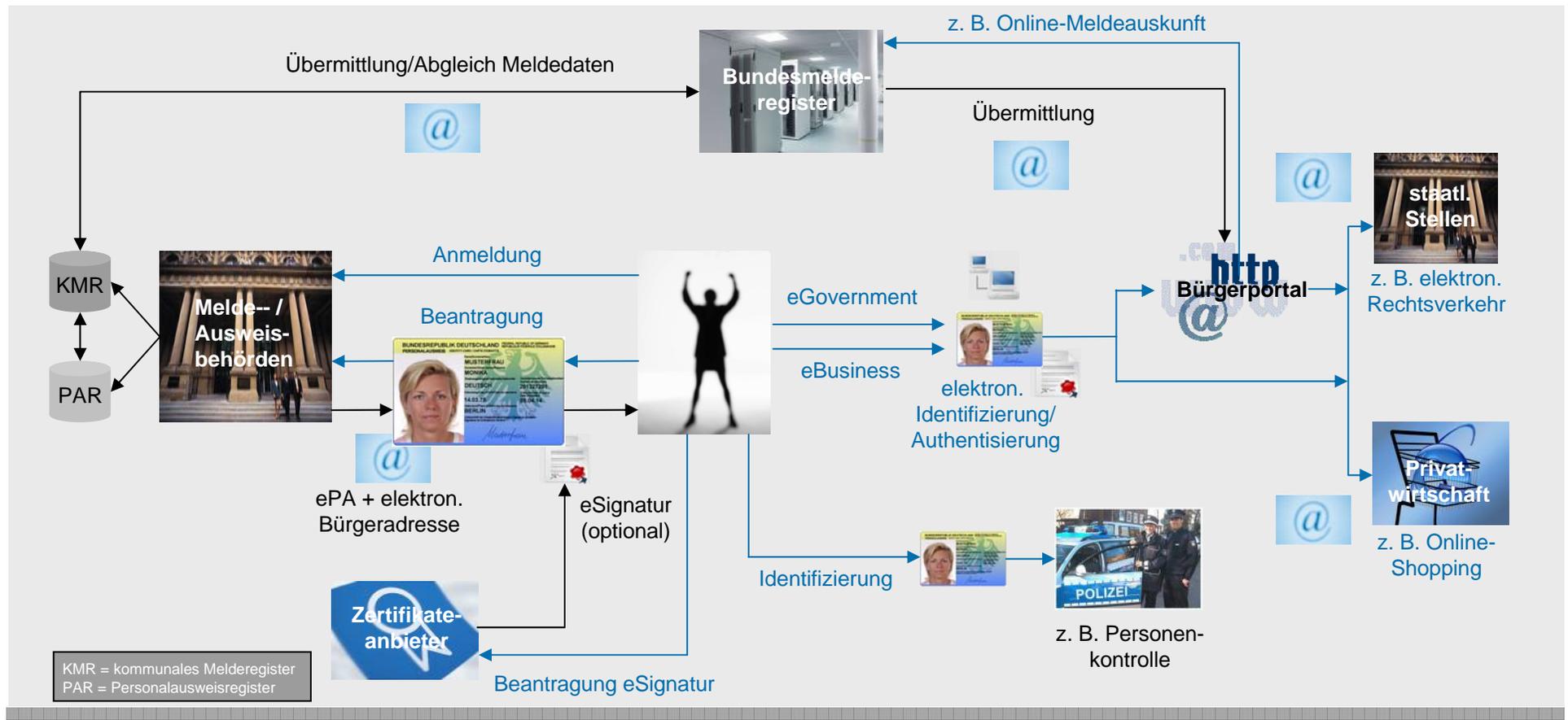


**Elektronischer  
Dienstausweis**

*E-Business  
E-Government*



## Zusammenspiel elektronischer Personalausweis, Bürgerportale und Bundesmelderegister





# Elektronischer Personalausweis

## Herausforderungen:

- **Identitätsdiebstahl und Phishing-Attacken** führen zu wirtschaftlichen Schäden bei Bürgern und Unternehmen
- **Missbrauch von Personaldokumenten** u.a. im Reiseverkehr

## Ziele:

- **Höhere Sicherheit bei E-Government und E-Business** durch Authentisierungs- und Signaturfunktion
- **Höhere Fälschungssicherheit** der Dokumente und höherer Schutz vor Dokumentenmissbrauch **durch Biometrie**



## Ziele des elektronischen Personalausweises



- Erhalt des bestehenden hohen Sicherheitsstandards des Dokumentes
- Erhöhte Sicherheit der Identifizierung und des Personalausweises als Reisedokument im Schengenraum und weiteren Staaten durch zusätzliche elektronische Funktionen
- Garantie für ein hohes Sicherheitsniveau in der elektronischen Welt
- Wirtschaft und Verwaltung durch Identitätsstruktur des elektronischen Personalausweises modernisieren
- Den elektronischen Personalausweis als Komponente der EU-weit harmonisierten Online-Authentisierung etablieren



## Die zwei neuen Eigenschaften des Personalausweises

### Biometrie

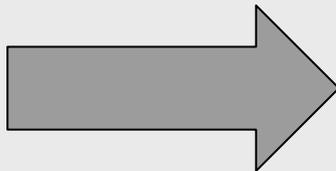
elektronisch gespeichert  
- Zugriff nur für Behörden! -

gespeichert werden:

- Fingerabdruck
- Gesichtsbild

Die Identifizierung wird dadurch  
verbessert (Grenzkontrolle/Fahndung).

Sicherheitsniveau wie ePass

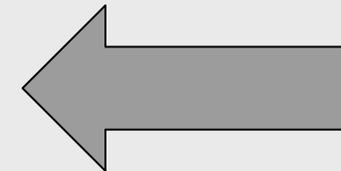


### elektronischer Identitätsnachweis

personenbezogene Daten (Name,  
Vorname, Anschrift ...) sind  
elektronisch gespeichert

Mit Zustimmung des Inhabers können  
die Daten abgerufen werden.

Anwendungsfelder: eBusiness (eBay,  
Amazon), eBanking, eGovernment,  
Automaten, Jugendschutz





## Authentisierungs- und Signaturfunktion



### Optische Authentisierung – klassische Funktion

- im staatlichen Bereich (Grenz- und polizeiliche Kontrollen)
- im wirtschaftlichen Bereich (Kontoeröffnung, Hotelaufenthalt, ...)



### Elektronische Authentisierung – neue Funktion

- in elektronischen Netzwerken (Internet, Intranet, ...)
- im eGovernment (Steuer, Antragsverfahren, Auskünfte, ...)
- im eBusiness (eBay, Online-Banking, Bestellungen, ...)



### Qualifizierte Signatur – optionale Funktion

- als elektronisches Äquivalent zur eigenhändigen Unterschrift
- für zahlreiche Anwendungen (Verträge, Urkunden, ...)



# Anwendung der elektronischen Authentisierung

## Online- Authentisierung



### Potentielle Beispiele:

- Authentisierung von E-Mails
- alle elektronischen Anträge, die nicht die Schriftform erfordern
- Elektronische Steuererklärung (ELSTER)
- Online-Banking
- Internetauktionen, Internetversandhandel
- Anmeldung bei Internetservice Providern
- Jugendschutz



## Offline- Authentisierung

### Potentielle Einzelbeispiele:

- automatische Paketausgabe (Identitätsnachweis)
- Zigaretten- und Alkoholautomaten (Altersnachweis)
- Videothekenautomaten (Altersnachweis)

**Allgemein: Zugangskontrollen**  
(Identitätsnachweis)

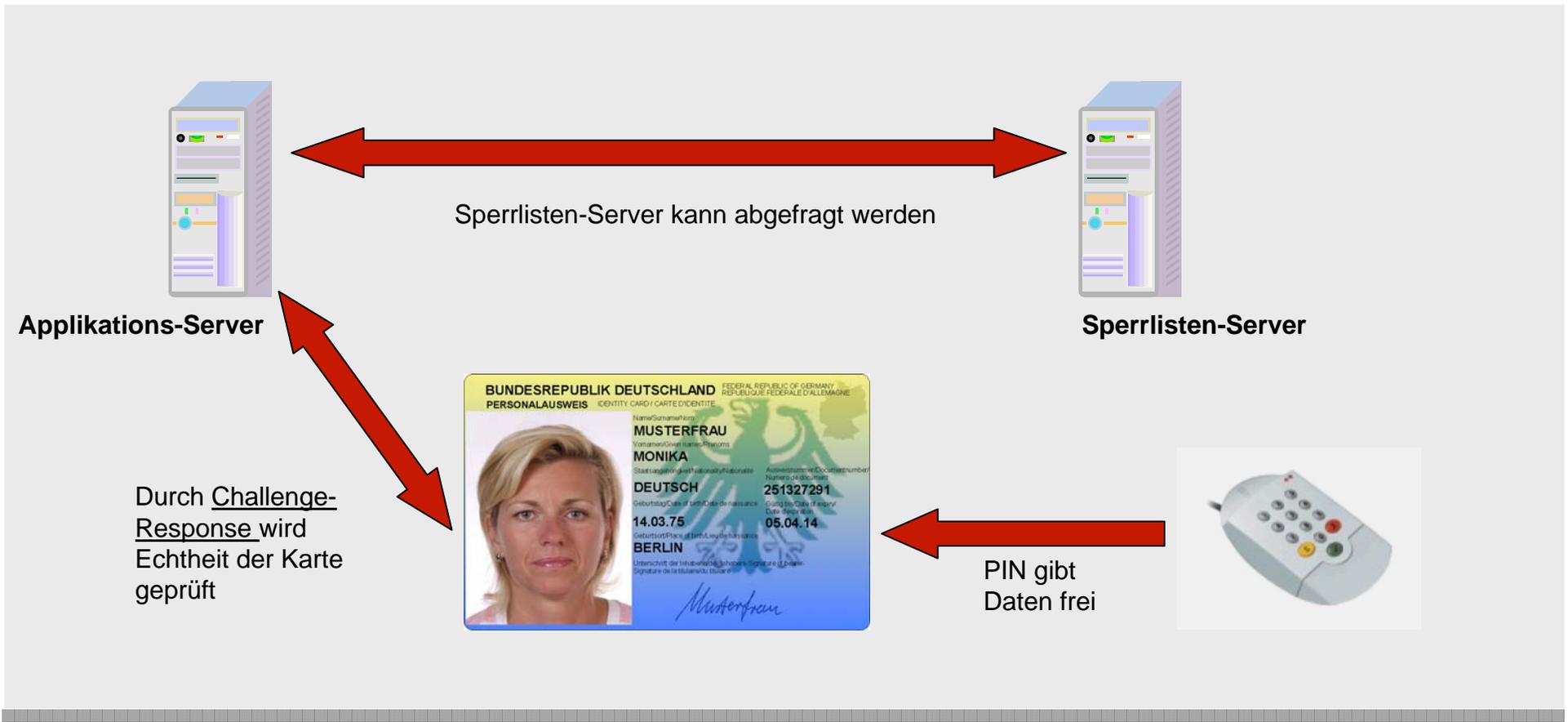


## Anforderungen an die elektronische Authentisierung

- Authentisierung soll auf **Zertifikaten** basieren welche die Daten des Inhabers enthalten
- Zugriff auf die Daten soll durch „**Berechtigungszertifikate**“ geregelt werden. Zweckgebundene Vergabe unter Berücksichtigung datenschutzrechtlicher Erforderlichkeit.
- Datenfreigabe muss in jedem Fall durch den PA-Inhaber erfolgen (z.B. per **PIN**)
- Datenzertifikate müssen **nachgeladen** werden können z.B. zur Aktualisierung der Adresse
- Beschränkung der **biometrischen Daten** auf den **hoheitlichen Bereich** (Reisefunktion), keine Verwendung für die Authentisierungsfunktion
- Gestohlene oder verlorene PA müssen **gesperrt** werden können



## Sicherheitsfunktionen bei der Authentisierung (Planung)





## Die elektronische Identität - Schutz der Bürgerinnen und Bürger vor Internetbetrug

"Sowohl öffentliche Stellen als auch Unternehmen müssen dafür sorgen, dass die Nutzer die Echtheit ihres Online-Angebots überprüfen können,,

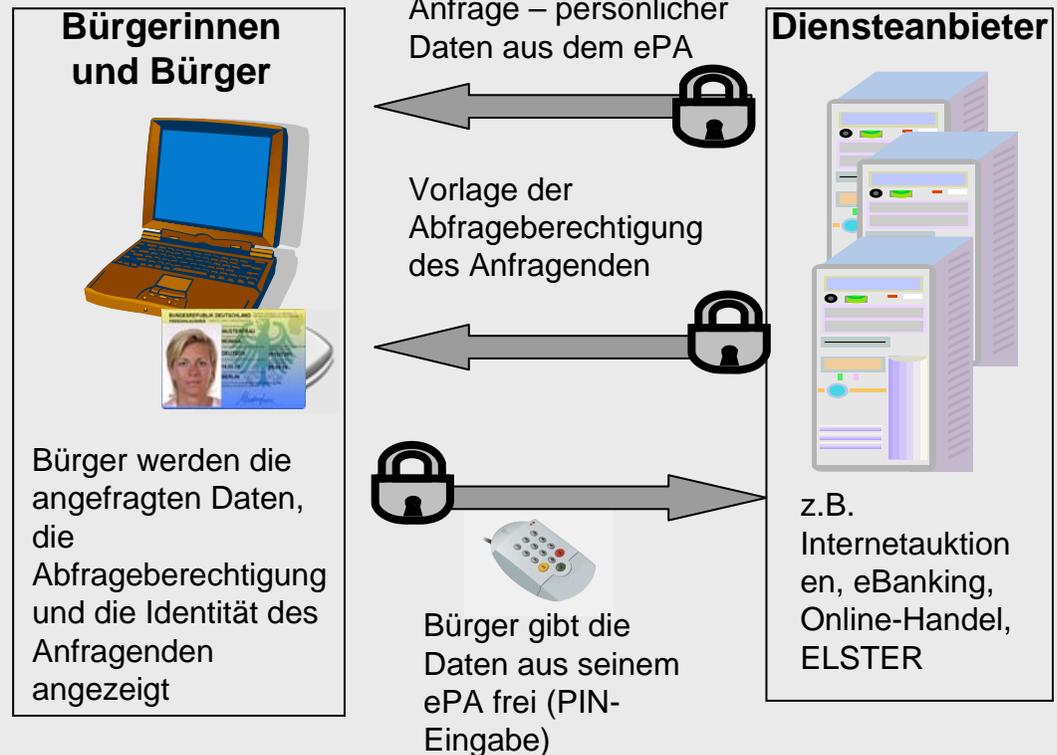
Peter Schaar, BfDI, Bericht 2005/2006

In der Polizeilichen Kriminalstatistik für das Jahr 2006 wird ein **Anstieg des Warenkreditbetruges um 8,8 %** ggü. dem Vorjahr festgestellt. Der nochmalige Anstieg dürfte auf die Zunahme des Warenverkehrs im Internet zurückzuführen sein.

### Bürgerinnen und Bürger und Dienstanbieter

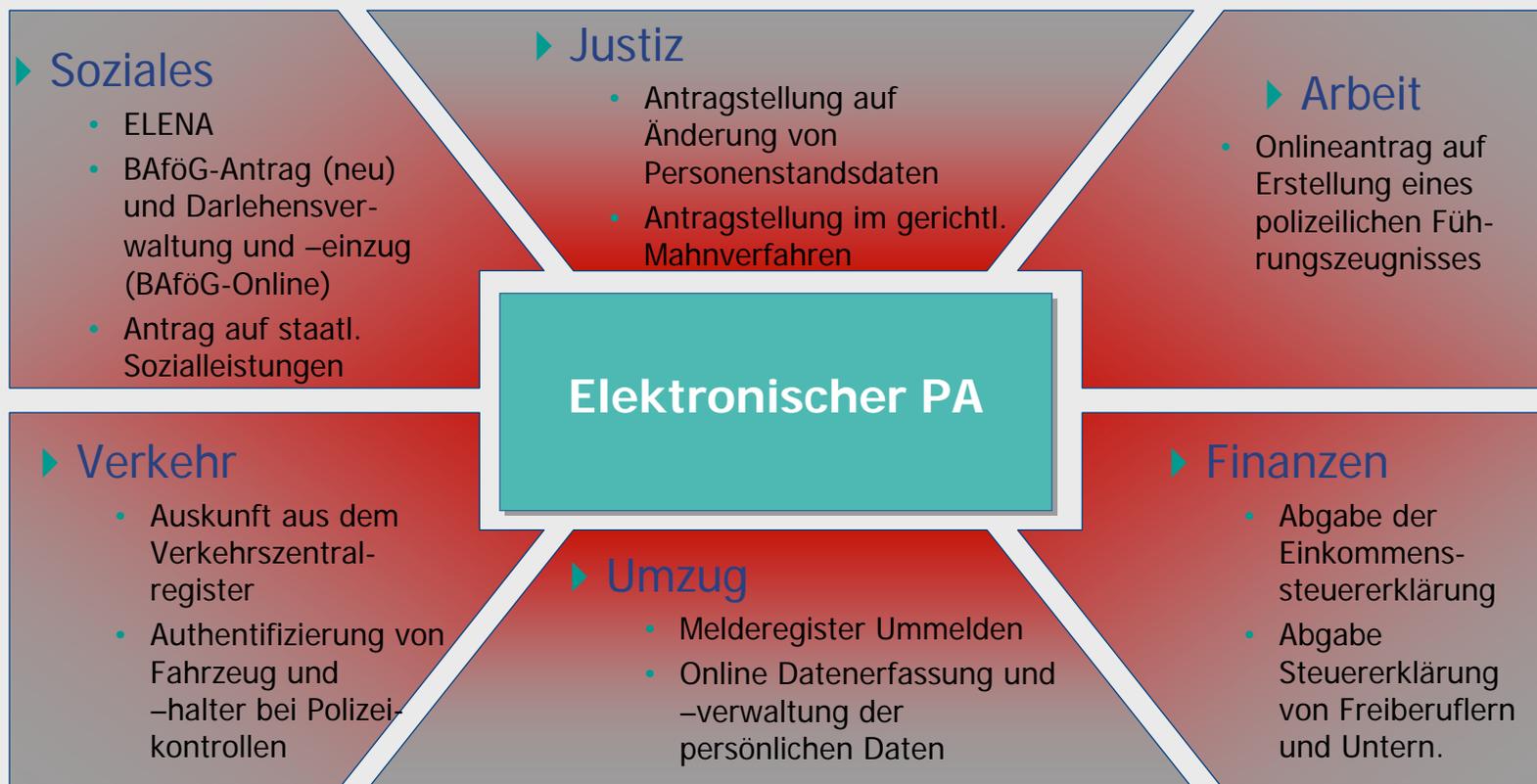
können sich bei der Nutzung des ePA auf die Identität des Gegenüber verlassen!

### Kundenkontoeröffnung mit dem ePA





## Definition von Top-Dienstleistungen für den neuen Personalausweis: Beispiele Verwaltung





## Elektronischer Personalausweis und Aufenthaltskarte: Ein Konzept für beide!

| E-Cards                            | <br>elektronischer<br>PA                                     | <br>elektronische<br>Aufenthalts-<br>karte                  |
|------------------------------------|--|--|
| Geplante elektronische Funktionen: | <ul style="list-style-type: none"><li>■ Biometrie analog ePass</li><li>■ Authentisierung</li><li>■ qualifizierte Signatur (optional)</li></ul> | <ul style="list-style-type: none"><li>■ Biometrie analog ePass</li><li>■ Authentisierung</li><li>■ qualifizierte Signatur (optional)</li></ul> |
| Rechtliche Grundlagen              | Nationale Gesetzgebung (PersAuswG)   | Verordnung (EG) 1030/2002  |
| Zielgruppe                         | Deutsche   | Drittstaatsangehörige  |



## Bürgerportale und elektronischer Personalausweis

### Bürgerportale als ein Einsatzfeld des ePA

- ePA zur starken Authentisierung/Anmeldung am Bürgerportal
- ePa zur Erstregistrierung am Bürgerportal zur Einrichtung eines Bürgerportal-Accounts

### Authentisierung mittels Bürgerportalen

- Bürgerportale bieten auch Authentisierungsverfahren geringeren Sicherheitsniveaus als der ePA
- Bürgerportale können in der Übergangszeit genutzt werden (ePA noch nicht verbreitet)
- Der Authentisierungsdienst der Bürgerportale kann flexibel und mit Zustimmung des Inhabers weitere Identitätsattribute (z.B. Bankverbindung, Lieferanschrift) zur Verfügung stellen
- Auch juristische Personen können sich Bürgerportal-Accounts einrichten und den Authentisierungsdienst nutzen

**→ Authentisierung mittels ePA und Bürgerportalen schließen sich nicht aus, sondern ergänzen sich hervorragend**



Bundesministerium  
des Innern

***Herzlichen Dank  
für Ihre Aufmerksamkeit!***

***Jan Möller  
jan.moeller@bmi.bund.de***