Vertrauenswürdige Identitäts-Infrastrukturen

Dr. Sven Polenz
ULD4@datenschutzzentrum.de

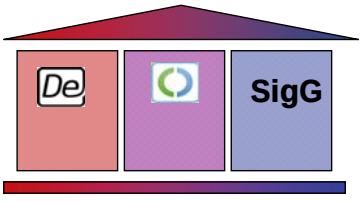
Harald Zwingelberg
ULD65@datenschutzzentrum.de

PrimeLife

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Übersicht

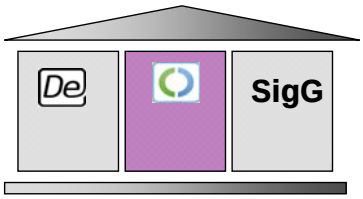
1. Der neue elektronische Personalausweis (nPA)
2. Das neue De-Mail-Gesetz
3. Signatur nach Signaturgesetz
4. Gesamtsystem der deutschen eID-Infrastruktur
5. Lebenslanger Datenschutz
6. Fazit



1. Der neue Personalausweis

1. **Der neue elektronische Personalausweis**
   - **a) Funktionen**
     - Abruf biometrischer Daten
     - Qualifizierte elektronische Signatur
     - Elektronischer Identitätsnachweis
   - **b) Fragen zur Datensicherheit**
     - Sperrmerkmale
     - Verwendung einer Zugangsnummer
     - Verarbeitungszwecke
     - PIN-Eingabe – Verfahren der Neusetzung
     - Datenübermittlungen zwischen Behörden
     - Datenübermittlung an Diensteanbieter und Berechtigungsvergabe
     - Erforderlichkeitsprüfung bei Berechtigungsvergabe

2. **Das neue De-Mail-Gesetz**
3. **PKI-Infrastruktur und SigG**
4. **Gesamtsystem der staatlichen eID-Infrastruktur**
5. **Lebenslanger Datenschutz**
6. **Fazit**



1. Der neue elektronische Personalausweis - Funktionen -

aa) Abruf biometrischer Merkmale

1. Der neue elektronische Personalausweis - Funktionen -

aa) Abruf biometrischer Merkmale durch berechtigte Behörden

- Die Unterschrift ist im Speichermedium nicht enthalten, da dies ein zu hohes Sicherheitsrisiko darstellen würde.

- Der künftige Ausweisinhaber entscheidet bei der Beantragung des Personalausweises über die Aufnahme seiner Fingerabdrücke.

- Das Lichtbild und die gegebenenfalls gespeicherten Fingerabdrücke können nur durch zur Identitätsfeststellung berechtigte Behörden abgerufen werden.

1. Der neue elektronische Personalausweis - Funktionen -

bb) Qualifizierte elektronische Signatur

Zur Nutzung (qualifizierter) elektronischer Signaturen werden benötigt:

(1) Signaturkarte (Funktion des elektronischen Personal-ausweises, der darüber hinaus als sichere Signatur-erstellungseinheit gilt)
(2) Kartenlesegerät (derzeit ab ca. 60,00 €)
(3) Zertifikat für qualifizierte elektronische Signatur (ca. 40,00 € p.a.)

1. Der neue elektronische Personalausweis - Funktionen -

bb) Qualifizierte elektronische Signatur

Beachte: Mit der elektronischen Signatur und der erfolgreichen Verifizierung werden nur die Identität des Absenders sowie die Herkunft und Integrität des Textes bestätigt.

Der Text kann bei einer fehlenden Verschlüsselung (Übertragungskanal Absender-Empfänger) von Unbefugten (zwar nicht abgeändert,) jedoch mitgelesen werden.

1. Der neue elektronische Personalausweis - Funktionen -

cc) Elektronischer Identitätsnachweis

Der Personalausweisinhaber, der **mindestens 16 Jahre alt** ist, kann seinen Personalausweis dazu verwenden, seine Identität gegenüber öffentlichen und nichtöffentlichen Stellen elektronisch nachzuweisen.

Bei der **Nutzung allgemein zugänglicher Netze** (Internet) sind Verschlüsselungsverfahren anzuwenden (vgl. auch § 9 BDSG i.V.m. Satz 3 in Anlage). Eine Nutzung des elektronischen Identitätsnachweises durch eine andere Person als den Personalausweisinhaber ist unzulässig und bußgeldbewehrt, § 32 Abs. 1 Nr. 5 PAuswG.

1. Der neue elektronische Personalausweis - Funktionen -

cc) Elektronischer Identitätsnachweis

Folgende Daten können übermittelt werden (§ 18 Abs. 3 Satz 2 PAuswG):

1. Sperrmerkmal
2. Angabe zur Gültigkeit des Personalausweises
3. Familienname
4. Vornamen
5. Doktorgrad
6. Tag der Geburt
7. Ort der Geburt
8. Anschrift
9. Dokumentenart
10. dienste- und kartenspezifisches Kennzeichen
11. Abkürzung „D“ für „BRD“
12. Angabe, ob ein bestimmtes Alter über- oder unterschritten wird
13. Angabe, ob ein Wohnort dem abgefragten Wohnort entspricht
14. Ordensname/Künstlername

1. Der neue elektronische Personalausweis - Fragen zur Datensicherheit -

aa) Sperrmerkmale

- Allgemeine Sperrmerkmale
  (Bundesverwaltungsamt führt Liste mit allg. Sperrmerkmalen)

- Diensteanbieterspezifische Sperrmerkmale
  (Zertifizierungsdiensteanbieter führt Liste mit spezifischen Sperrmerkmalen)

1. Der neue elektronische Personalausweis - Fragen zur Datensicherheit -

bb) Verwendung der Zugangsnummer

- Sechsstellige, aufgedruckte Ziffernfolge
- Bitte keine Verwendung als Geheimnummer!
- Abruf von Daten aus dem Speichermedium
- Bedienung eines Rücksetzzählers

1. Der neue elektronische Personalausweis - Fragen zur Datensicherheit -

cc) Verarbeitungszwecke für berechtigte Behörden

Ferner dürfen auch die Daten aus dem elektronischen Speicher- und Verarbeitungsmedium nur für zwei Erhebungszwecke ausgelesen werden:

(1) Überprüfung der Echtheit des Dokuments
(2) Überprüfung der Identität des Ausweisinhabers

Zu diesen Zwecken sind Polizeivollzugsbehörden, die Zollverwaltung, die Steuerfahndungsstellen der Länder sowie die Personalausweis-, Pass- und Meldebehörden befugt zum

(1) Auslesen der biometrischen Daten aus dem Speicher- und Verarbeitungsmedium
(2) Erheben der erforderlichen biometrischen Daten beim Ausweisinhaber
(3) Vergleichen dieser biometrischen Daten miteinander

1. Der neue elektronische Personalausweis - Fragen zur Datensicherheit -

dd) PIN-Eingabe – Verfahren der Neusetzung

- Datensicherheit noch nicht abschließend geklärt
- Änderung der PIN über den Bürgerclient
- Pflicht zur Dokumentation/Protokollierung nach §§ 5 Abs. 1 Nr. 3, 6 Abs. 4 LDSG:

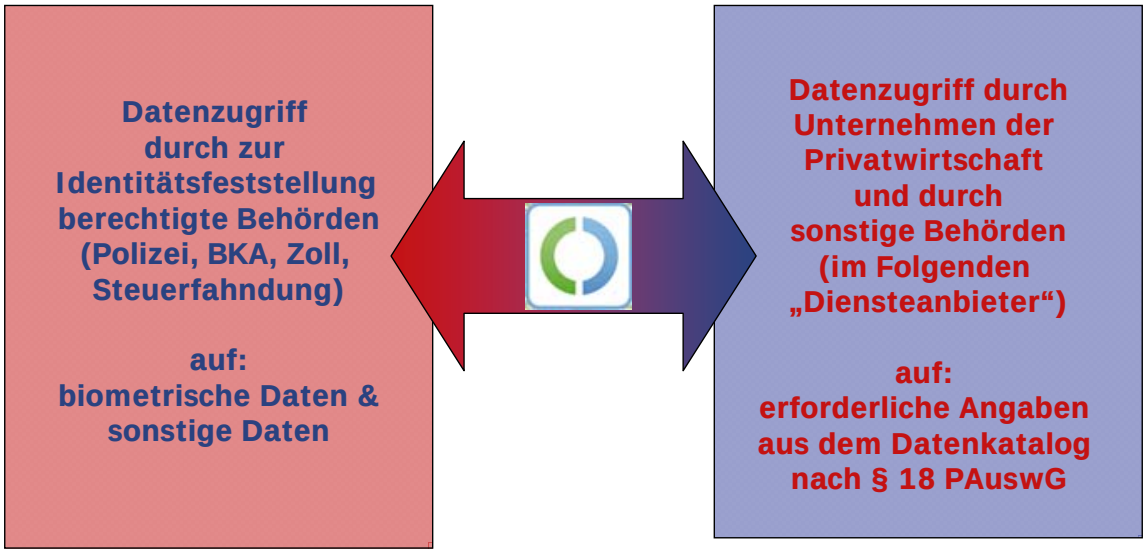
  Es ist zu gewährleisten, dass die Daten verarbeitende Person, der Zeitpunkt und Umfang der Datenverarbeitung festgestellt werden kann. Es ist zu protokollieren, wann, durch wen und in welcher Weise die Daten gespeichert wurden.

1. Der neue elektronische Personalausweis - Fragen zur Datensicherheit -

ee) Datenübermittlung zwischen Behörden und durch den Bürger

- Sperrantrag unter Nennung des Sperrkennwortes am Telefon
- Übermittlung von personenbezogenen Daten zwischen Personalausweisbehörden im Falle einer Sperrung
- Übermittlung personenbezogener Daten bei Eingang eines Sperrantrages bei Sperrnotruf
- Übermittlung personenbezogener Daten von örtlich zuständiger an ausstellende Behörde

Berechtigung zum Auslesen personenbezogener Daten aus dem nPA



Grundsätze für Datenabruf durch Diensteanbieter

- Gegenseitige Identifizierung: Unternehmen bzw. Behörde sendet vor Zugriff ein Zertifikat mit den eigenen Daten
- Nutzerzentrierung: Nutzer entscheidet via Bürgerclient / Ausweis-App pro Einzelfall bezüglich jeden Datums
- Der Abruf ist auf **erforderliche Daten** zu beschränken
- Feststellung der Erforderlichkeit zweistufiges Verfahren: Bundesverwaltungsamt prüft Erforderlichkeit und erteilt eine Berechtigung (Verwaltungsakt). Damit kann ein Berechtigungszertifikat beantragt werden.

Antragsvoraussetzungen für Berechtigungsvergabe an Diensteanbieter

- Rechtmäßiger Einsatzzweck (insbesondere kein bloßes Auslesen oder Bereitstellen der Daten an Dritte)
- Zweck besteht nicht in geschäftsmäßiger Datenübermittlung und es bestehen keine Anhaltspunkte für unberechtigte oder geschäftsmäßige Datenübermittlung (vgl. § 29 BDSG)
- Erforderlichkeit für Einsatzzweck ist nachgewiesen (dazu später)
- Anforderungen an Datenschutz und Datensicherheit gemäß der Rechtsverordnung sind erfüllt
- Keine Anhaltspunkte für missbräuchliche Verwendung der Berechtigung

Erforderlichkeit von Daten: Zwecke

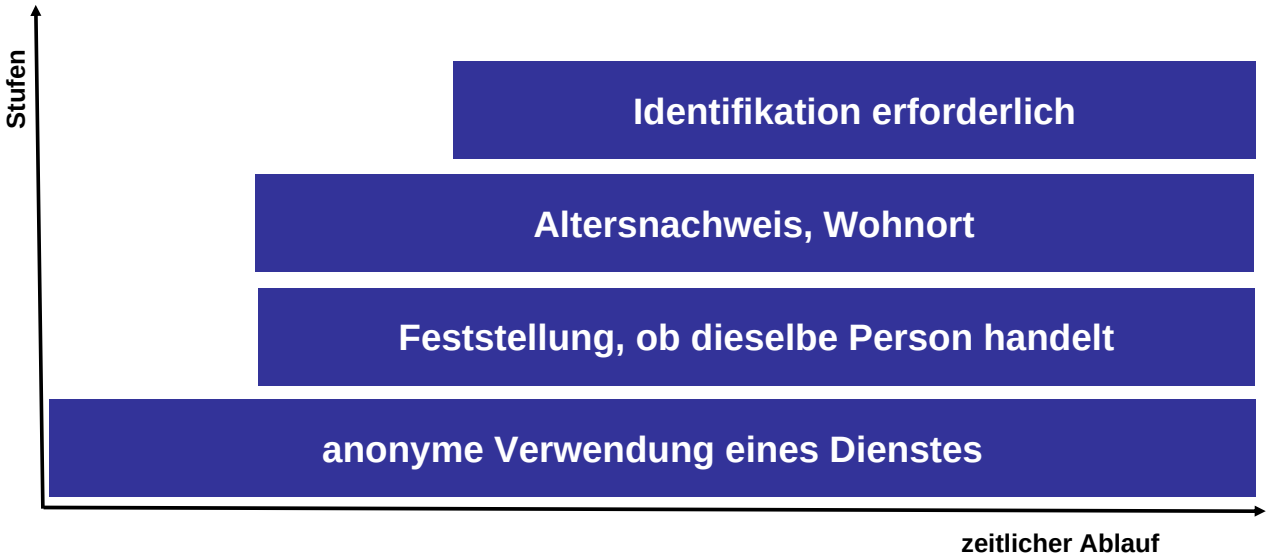
- Diensteanbieter erhalten die für die Wahrnehmung ihrer Aufgaben oder Geschäftszwecke **erforderlichen Daten**
- Problem: Abhängigkeit von der Definition des Zwecks
  - Weite Zweckbeschreibung: viele Daten
  - Enge Zweckbeschreibung: genauere Prüfung möglich, nur die wirklich erforderlichen Daten, ggf. zu kleine Untergliederung => viele Berechtigungen & Zertifikate erforderlich, hohe Kosten für Prüfung, Zertifikate,...
- Zwecke müssen hinreichend genau ein Verfahren bezeichnen und dürfen nicht zu allgemein gehalten sein

Erforderlichkeit: kein Ersatz durch Einwilligung der Betroffenen

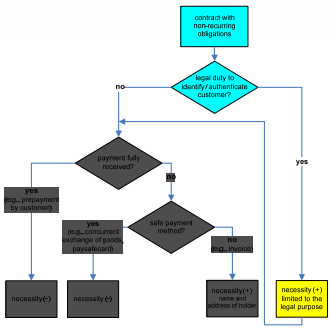
- Eine informierte Einwilligung allein genügt nicht – diese wird bereits durch den Bürgerclient + PIN vorausgesetzt.
- Erforderlichkeit wird vom BVA am Zweck gemessen.
- Auslegung: Es genügt, wenn die Daten zu einem späteren Zeitpunkt für einen rechtlich anerkennenswerten Zweck benötigt werden können (insbes. Rechtsverfolgung).

Folge: Unzulässig ist, Daten allein für die Einrichtung eines Kundenkontos abzurufen. Möglich ist aber die Nutzung von Pseudonymen zur Wiedererkennung desselben Kunden.

Erforderlichkeit von Daten: Modell zur Prüfung im Berechtigungsverfahren



Mehr zum Thema: Zwingelberg, "Necessary processing of personal data", IFIP/PrimeLife Summer School 2010, Helsingborg, Folien unter: http://www.cs.kau.se/IFIP-summerschool/program.html



einmaliges Austausch-verhältnis

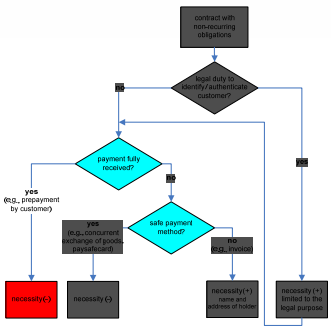
gesetzliche Pflicht zur Erhebung?

nein

ja
(Jugendschutz, TK-Recht)

Gegenleistung vollständig erhalten?

Erforderlichkeit (+) nur für diesen gesetzlichen Zweck



keine gesetzliche Pflicht zur Erhebung oder bereits erfüllt

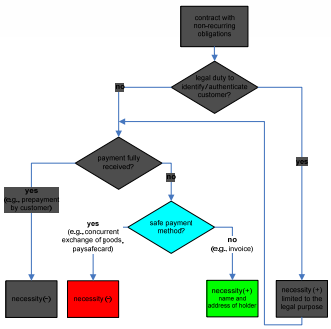
Gegenleistung vollständig erhalten?

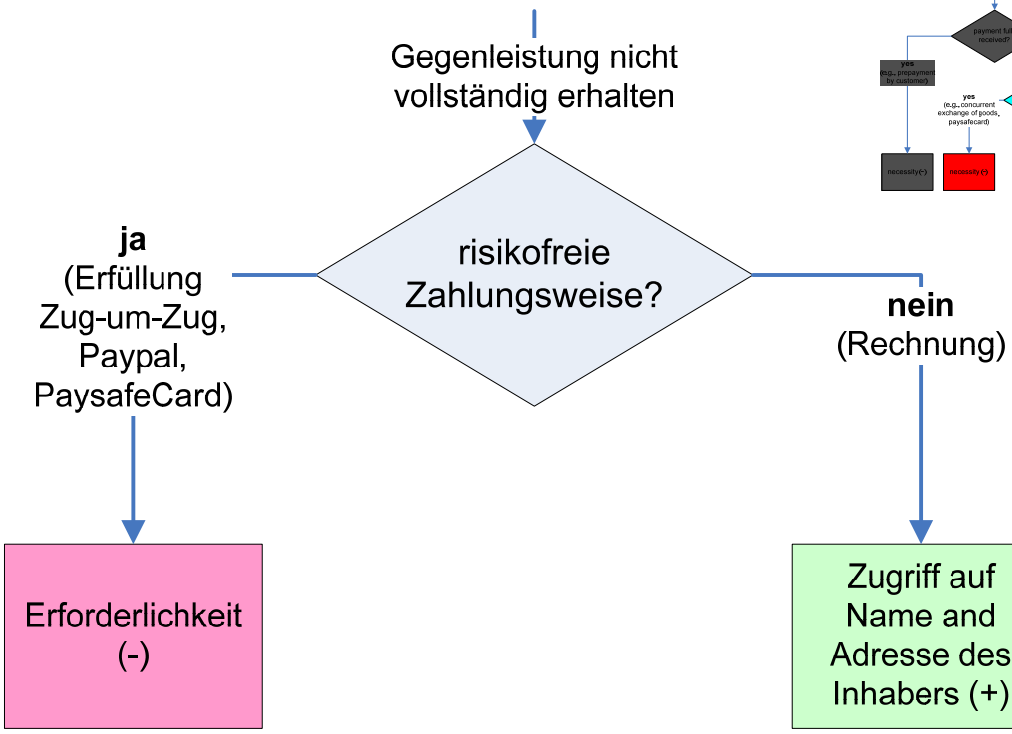
ja
(Vorkasse, Prepaid-Service)

nein

Erforderlichkeit (-)

risikofreie Zahlungsweise?





Weitere analysierte Szenarien

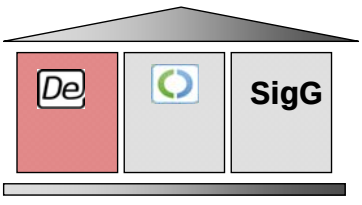
- Bloße Informationsbeschaffung: surfen
- Altersverifikation: Kauf von Tabakwaren, Jugendschutz
- Wohnortverifikation: Lizenzkontrolle für digitale Inhalte der kommunalen Bücherei, Kureinrichtungen
- Wiedererkennung: Pseudonymfunktion; Pseudonyme sind zwischen Anbietern nicht verkettbar. Bei großen Anbietern noch unklar, wie Trennung zwischen Diensten erfolgt.
- Kreditorisches Risiko bei Austauschverträgen (siehe oben) und bei Dauerschuldverhältnissen: Onlinespiele, Pay-per-view-Angebote, Fitness-Studio, Mietwagen
- Selbstauskunft nach § 34 BDSG
- Erhebung durch öffentliche Verwaltung und Behörden

Erforderlichkeit: Zusammenfassung

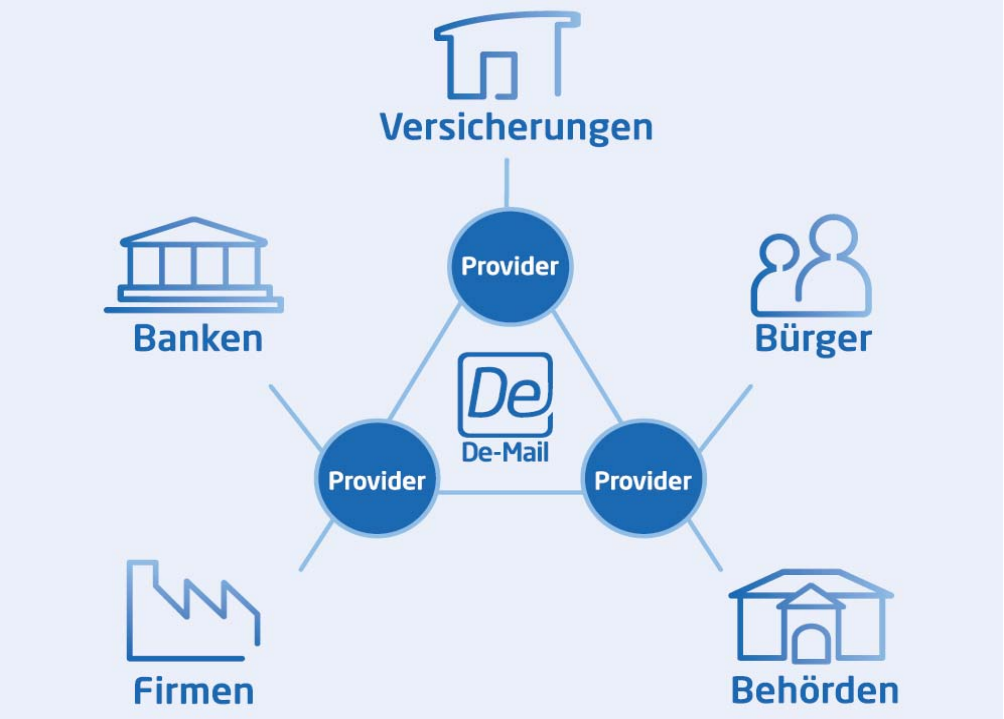
- Kernproblem: Definition des Verarbeitungszwecks und Anforderung an die Bestimmtheit des Zwecks
- Kreditorisches Risiko / Rechtsverfolgung: Es ist zu prüfen, ob im Einzelfall ein anzuerkennendes Risiko (z.B. ein kreditorisches Risiko) gegeben ist
- Behörden dürfen dort erheben, wo sie es bisher auch durften. Klarere Umgrenzung durch gesetzliche Aufgabenzuweisungen
- Begrenzung auf die notwendigen Datenkategorien

2. Das De-Mail Gesetz

1. **Der neue elektronische Personalausweis**
2. **Das neue De-Mail-Gesetz**
   - **a) Ausgangslage**
   - **b) Ziele des De-Mail-Dienstes**
   - **c) Sicherheit / Akkreditierung**
   - **d) Angebotsumfang von De-Mail**
   - **e) Risiken / Kritik**
3. **Signatur nach Signaturgesetz**
4. **Gesamtsystem der deutschen eID-Infrastruktur**
5. **Lebenslanger Datenschutz**



2. Das neue De-Mail-Gesetz



Quelle: http://www.cio.bund.de/DE/IT-Projekte/De-Mail/demail_node.html

a) Ausgangslage

- Elektronische Signaturen sind ohne zusätzliche Interaktion nicht geeignet, den Nachweis über die Absendung und den Empfang einer Nachricht zu führen.
- Selbst Zeitstempel einer dritten Instanz erbringt noch keinen Nachweis des Zugangs beim Empfänger.
- Bei Bürgerportalen muss der digitale Zugangsnachweis gesetzlich geregelt werden!
- E-Mail ist weit verbreitet, Signaturen nach SigG konnten sich bisher in der Breite nicht durchsetzen.

⇒ **Ziel:** Erreichbarkeit des Bürgers über ein sicheres elektronisches Postfach mit Zugangsbestätigung, aber nutzerseitig keine neuen Anforderungen

b) Ziele des De-Mail-Dienstes

- **Identität** des Absenders kann sicher erkannt werden (Abwehr von Spam- und Phishing-Mails)
- Digitaler **Zugangsnachweis** -> ZPO, VwVfG
- **Vertraulichkeit** – De-Mails werden auf dem Transport verschlüsselt und können nicht von Dritten abgefangen werden
- Sichere **Authentisierung** beim Zugriff auf ein Bürger-portal: Je nach Anforderungen zwingend mit Token (nPA, mobile-TAN). Passwort z.B. ungenügend für Einschreiben
- Ziel: Erreichbarkeit des Bürgers über ein **elektronisches Postfach**, vergleichbar mit der Erreichbarkeit unter der Wohnanschrift

c) Sicherheit / Akkreditierung

- Diensteanbieter können sich freiwillig akkreditieren lassen
- Voraussetzungen:
  - IT-Grundschutz / ISO 27001, spezifische Anforderungen
  - Datenschutzanforderungen
  - Zuverlässigkeit und Fachkunde
  - Funktionalität
- Verfahren: 2-stufig, vom BSI zertifizierte Prüfstelle erstellt Gutachten, das der zuständigen Behörde (Technik = BSI, Datenschutz = BfDI) zur Prüfung vorgelegt wird.

näher: Schumacher, Akkreditierung und Zertifizierung von De-Mail-Diensteanbietern, DuD 2010, 302-307

c) Sicherheit / Akkreditierung

- E-Mails werden während des Transports verschlüsselt
  - Einlieferung durch Absender über sichere Verbindung
  - Umverschlüsselung beim Provider des Absenders
  - Verschlüsselter Versand im Netz von De-Mail
  - Umverschlüsselung beim Provider des Empfängers
  - Abruf durch Empfänger über sichere Verbindung
- Umverschlüsselung unterliegt strengen Anforderungen an technische und organisatorische Maßnahmen
- Ende-zu-Ende-Verschlüsselung und Signatur sind zusätzlich möglich, aber bei De-Mail nicht Projektziel

d) Angebotsumfang von De-Mail

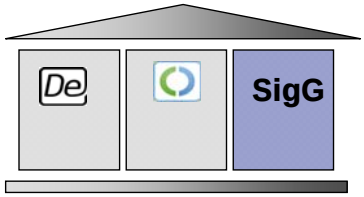
- Postfachdienst
- Versanddienst, elektronisches Einschreiben
- Dokumentensafe, elektronisches Archiv
- Authentisierungsdienst
- ... Zusatzdienste der Wettbewerber möglich

e) Risiken / Kritik

- Ende-zu-Ende-Verschlüsselung ist nicht vorgesehen
- Freie Beweiswürdigung der Gerichte bei nicht signierter Mitteilung könnte zu einer Beweiserschwernis führen
- Voraussetzungen des Auskunftsanspruchs zur Aufdeckung von Pseudonymen nicht eindeutig beschrieben
- Erhebung der Staatsangehörigkeit bei Kontoeröffnung
- Strenge Zweckbindung ist nicht im Gesetz verankert, z.B. für Angaben aus dem Verzeichnisdienst
- Löschpflicht für Verkehrsdaten und Kontrolle derselben (u.a. für Versand- und Eingangsbestätigung)
- Keine klare Zuständigkeit des BfDI für Datenschutzaufsicht

3. Signatur nach Signaturgesetz

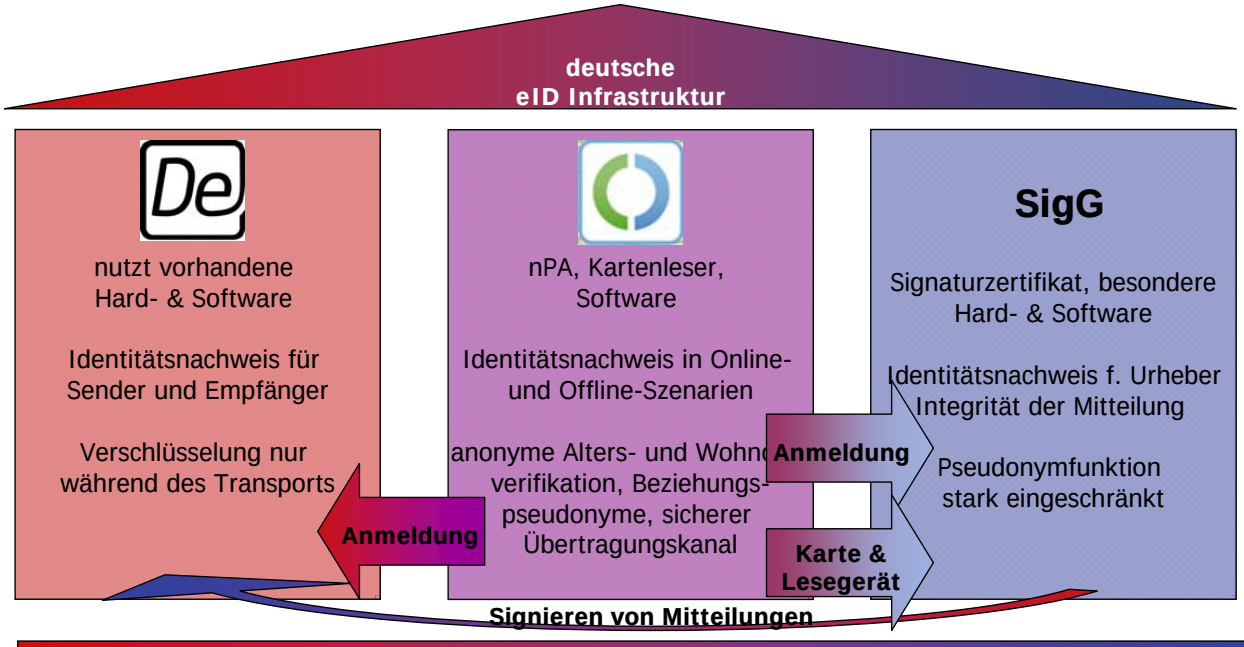
1. **Der neue elektronische Personalausweis**
2. **Das neue De-Mail-Gesetz**
3. **Signatur nach Signaturgesetz**
4. **Gesamtsystem der deutschen eID-Infrastruktur**
5. **Lebenslanger Datenschutz**



3. Signatur nach Signaturgesetz

- SigG: Gesetz von 1997, Reform 2001
- Zweck: Ersatz der Schriftform (händische Unterschrift) im Rechtsverkehr, § 126a BGB
- 3 Arten der elektronischen Signatur
  - Einfache elektronische Signatur
  - Fortgeschrittene elektronische Signatur (ermöglicht eindeutige Identifizierung des Schlüssel-Inhabers)
  - Qualifizierte elektronische Signatur (ist fortgeschrittene Signatur, die auf qualifiziertem Zertifikat beruht und mit Signaturerstellungseinheit erzeugt wurde)
- Qualifizierte Signatur ersetzt Unterschrift, § 126a BGB

4. Gesamtsystem der deutschen eID-Infrastruktur



5. Lebenslanger Datenschutz

- Prüfbarkeit für vergangene Transaktionen muss lange erhalten bleiben (Umsignierung nach SigG)
- Verkettung von Datenbeständen wird leichter möglich
- Einsatz kryptographischer Verfahren, die Anonymität bei gleichzeitiger Möglichkeit zur Aufhebung der Anonymität bei Vorliegen definierter Voraussetzungen erlauben
- Pflicht, anonyme oder pseudonyme Nutzung zu ermöglichen (z.B. durch Vorkasse, PaysafeCard, e-Cash,...)
- langfristige Planung / Risiken absehen und bewerten
- Delegationsmöglichkeit für Lebensphasen persönlichen Unvermögens (z.B. Kindheit, Unfall, Krankheit) bei zwingender Unterscheidbarkeit der Handelnden

Mehr zum Thema: PrimeLife-Projekt, www.primelife.eu
Hansen/Thomsen, Lebenslanger Datenschutz: DuD 2010, 283-288

Fazit

- Wurde die in der neuen eID-Infrastruktur (De-Mail, nPA und SigG) vorgesehene Schnittstelle zur Privatwirtschaft datenschutzgerecht umgesetzt?
- eID - eine Stärkung von Transparenz und Betroffenenrechten im Datenschutz?
- Selbstdatenschutz: Bessere Kontrolle über eigene Daten? Welche Verantwortung trifft den Staat?

Vielen Dank für Ihre Aufmerksamkeit! Fragen? Anmerkungen?

Dr. Sven Polenz
ULD4@datenschutzzentrum.de
0431 988-1215

Harald Zwingelberg
ULD65@datenschutzzentrum.de
0431/988-1228

www.datenschutzzentrum.de

PrimeLife

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein