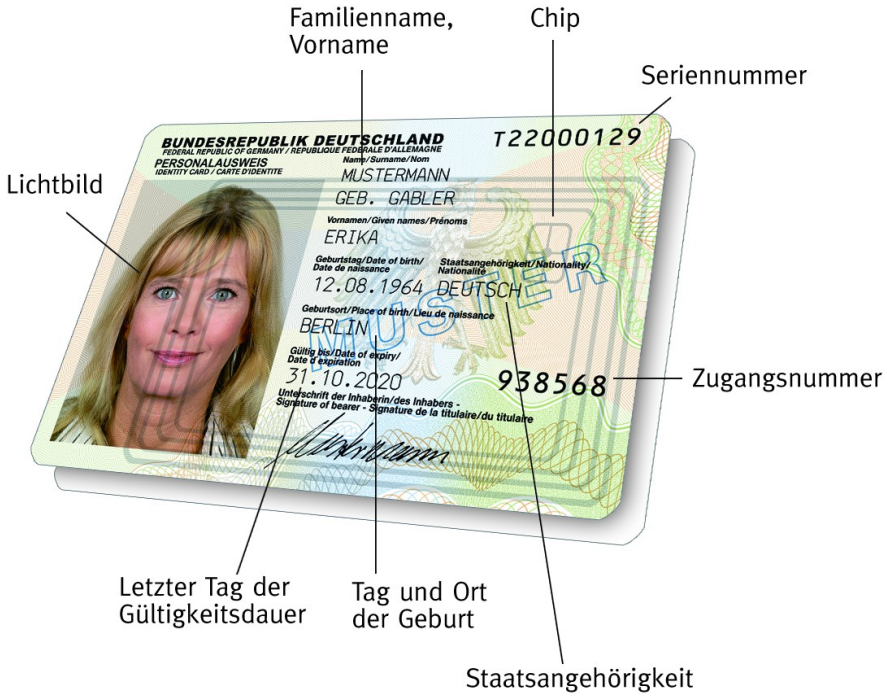
Die Sicherheit des neuen Personalausweises

Jens Bender

Bundesamt für Sicherheit in der Informationstechnik

IuK-Forum Niedersachsen / 25.08.2011

Der Personalausweis



Motivation

- Stärkere Bindung von Dokument und Inhaber durch Biometrie auch beim Personalausweis
- Kryptographie als neues Sicherheitsmerkmal
- Neue Technologien erfordern eine sichere elektronische Identifizierung, z.B. für
  - Online-Geschäfte
  - Finanztransaktionen
  - eGovernment

→ **Integration eines (kontaktlosen) Chips**

Funktionen

Sichtausweis

Der neue Personalausweis vereint den herkömmlichen Ausweis und die drei neuen elektronischen Funktionen im Scheckkartenformat.

Elektronische Funktionen

Biometriefunktion (ähnlich ePass)

- MRZ-Daten
- Lichtbild und (auf Wunsch) zwei elektronische Fingerabdrücke
- ausschließlich für zur Identitätsfeststellung berechtigte Behörden, z.B. Polizei und Grenzkontrolle

Elektronische Identität

- Abschaltbar
- „Ausweisen im Netz“
- PIN und Berechtigungszertifikat erforderlich

Qualifizierte elektronische Signatur

- Zertifikat nachladbar

Physikalische Sicherheitsmerkmale

Guillochen: komplexe Linienmuster als mehrfarbiger Sicherheitsdruck (1)

Mikroschriften (2)

Taktile Merkmale (13)

Kinematische Bewegungsstrukturen (7)

Holografische Portrait (5)

3D-Bundesadler (6)

Guillochen: komplexe Linienmuster als mehrfarbiger Sicherheitsdruck (14)

Mikroschriften (15)

Taktile Merkmale (13)

Oberflächenprägungen (19)

Laser-Kippbild (21)

Integrierter Sicherheitsfaden (23)

Elektronische Identität (eID) und qualifizierte Signatur (QES)

	Traditionell	Elektronisch (1-Faktor)	Elektronisch (Wissen & Besitz)
Identifizierung	Vorlage des Personalausweises	Username/ Passwort	**Neu: eID**
Transaktion	Unterschrift	TAN	QES

Beispiel Bankgeschäft

→ Personalausweis zur Identifizierung, Angebotserstellung, ...

→ Unterschrift zur Durchführung der Transaktion (z.B. Kontoeröffnung)

Identifizierung ist abstreitbar – Signatur ist nicht abstreitbar
unterschdl. Schadenspotential → unterschdl. Sicherheitsanforderungen

Elektronische Identität

Gegenseitiger Identitätsnachweis

Bürgerinnen und Bürger:

Kann das Unternehmen seine elektronische Identität beweisen?

Dienstanbieter weist sich mit *Berechtigungszertifikat* aus

Sowohl Bürger als auch Dienstanbieter können sich auf die Identität des Gegenüber verlassen!

Bürger weist sich mit *Ausweis* aus

Dienstanbieter:

Kann die Person ihre elektronische Identität beweisen?

Datenschutz by Design

Datensparsamkeit – Volle Nutzerkontrolle

Gegenseitige Authentisierung → Vorteile für beide Seiten

Mögliche Einsatzfelder

Registrierung

Web-Pseudonyme

Ausfüllen von Formularen

Anmeldung

Altersverifikation

Qualifizierte elektronische Signatur

Teilnehmer des zentral koordinierten Anwendungstests

E-Government

- Deutsche Rentenversicherung
- ELSTER
- Rathaus21 DIE E-GOVERNMENT LÖSUNG
- HSH
- dz Datenzentrale Baden-Württemberg
- service-bw
- AKDB
- T-Systems
- FRITZ&MACZIOL Software, Systeme und Dienstleistungen
- Umwelt Bundes Amt DEHSt
-]init[
- Fraunhofer FOKUS
- ITDZ BERLIN
- Kroschke

E-Finanzservice

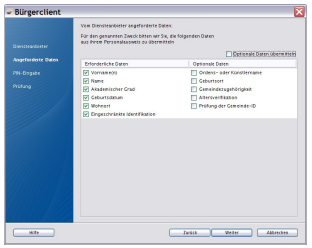
- Allianz
- DKB Deutsche Kreditbank AG
- CosmosDirekt.
- Gothaer
- HUK24 DIE ONLINE-VERSICHERUNG
- InterCard
- LVM Versicherungen
- SIZ INFORMATIKZENTRUM DER SPARKASSEN-ORGANISATION GMBH
- PROVINZIAL

E-Business

- FUJITSU
- airberlin
- WINCOR NIXDORF
- bird.i
- LOTTO Hessen
- VRR
- WEBER
- Institut für Inklusion
- schufa

Mehr als nur eine Karte

- **Der Ausweis**: Der Chip als Träger der personenbezogenen Daten muss diese schützen → der Chip ist Sicherheitsanker
- **Beantragung**: Erfassung „schlechter“ Daten bei der Beantragung führt zu „schlechten“ Daten auf dem Ausweis
- **Bürgerservices** (z.B. Adressänderung)
- **Kartenleser**: Verschiedene Typen
- **eID-Client**: Lokale Software für den Bürger
- **eID-Server**: Gegenstück zum Bürgerclient beim Dienstanbieter
- **PKI**s, **Sperrdienst**
- **Hotline**



Kommunen

- Aufgaben
  - Ausweisbeantragung
  - Datenübermittlung zum Hersteller
  - Ausweisausgabe
    - Bürgerinformation über neue Funktionen
    - Auskunftsbegehren, d.h. Anzeige der Daten
  - Änderungsdienst
  - Ausweis-/Melderegister
  - Entwertung
- Komplexe Systeme mit großer Variabilität
  - Konkrete Einzelvorgaben nicht möglich
  - Empfehlungen des BSI für Sicherheitskonzept

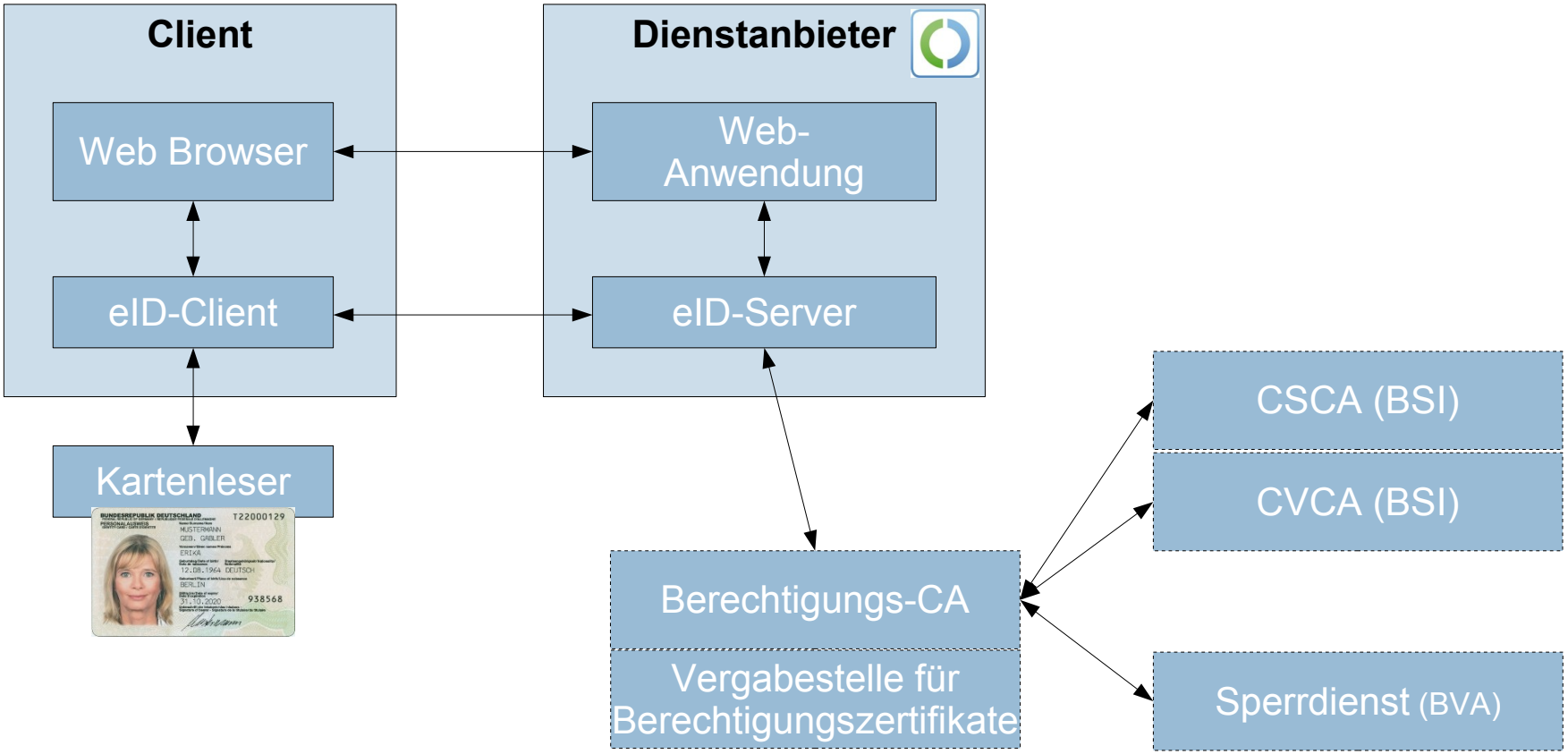
Änderungsdienst

- Aufgaben
  - Adressänderung → Anbindung an Meldewesen
  - Ein-/Ausschalten der eID-Funktion → Anbindung an Ausweisregister
  - PIN-Änderung
  - Anzeige der Chipdaten für QS und Auskunftsbegehren
- Verfügbarkeit: keine permanente Online-Anbindung, daher lokaler Schlüssel → hohe Sicherheitsanforderungen
- Technische Umsetzung durch „Änderungsterminal“ + zugehörige Software auf APC der Behörde

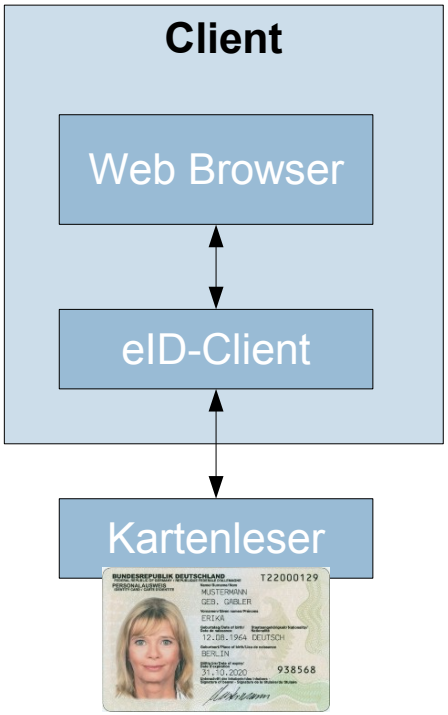
Potentielle Angriffe Kommunen

- Vortäuschung falscher Identitäten bei Beantragung
  - Wie bisher auch
- Angriff auf IT-Systeme der Behörde, z.B.
    - Verfälschung von Antragsdaten im Erfassungsprozess
    - Kompromittierung von Datenbanken
  - Wie bisher auch
  - Empfehlungen des BSI zur Sicherheit (IT-Grundschutz)
- Freischalten der eID-Funktion/PIN-Änderung „gefundener“ Ausweise
  - Behördenmitarbeiter muss vor diesen Aktionen den Inhaber identifizieren (z.B. Lichtbild)

Authentisierungsfunktion



Nutzerumgebung



- Besteht aus Nutzer-PC/Client-Software und Kartenleser
- Aufgaben
  - Zertifikatsanzeige
  - PIN-Eingabe
  - Kommunikation mit Karte, Dienstanbieter
- Je nach Lesertyp werden diese Funktion verschieden auf Leser und Nutzer-PC/Client-Software verteilt
- Empfehlung:
  - Verwendung zertifizierter Komponenten
  - Unabhängig von Ausweis: Absicherung des Rechners

Kartenleser

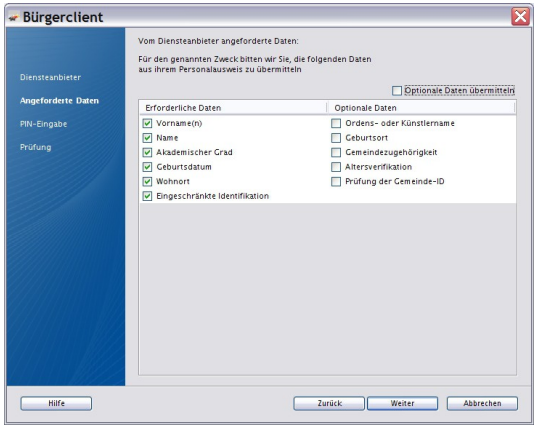
Verschiedene Kategorien:

- Basisleser
  - Eignung für mobilen Betrieb
  - Freie Wahl des Formfaktors – Integrationsfähigkeit
- Standardleser
  - PIN-Pad für PIN-Eingabe bei Anwendungen mit höherem Schutzbedarf
- Komfortleser
  - Bestätigung nach SigG für QES
  - Nutzung eines Komfortlesers wird bei PA-QES technisch erzwungen
- Liste der zertifizierten Produkte beim BSI

eID-Client

Offene Spezifikation –
Jeder kann Software schreiben und zertifizieren lassen

Der Bund stellt kostenfrei *AusweisApp* zur Verfügung



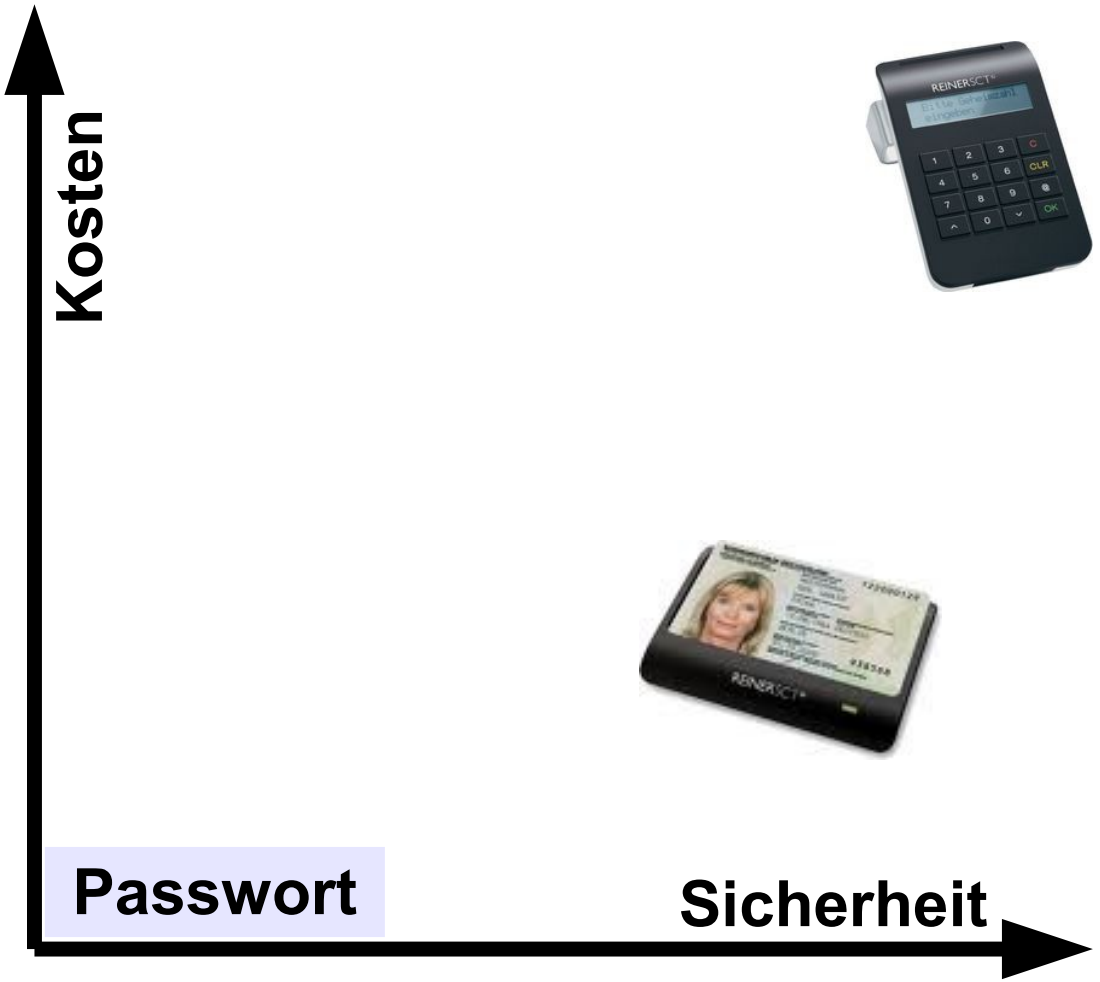
- Aufgaben
  - Anzeige der Informationen über den Dienstanbieter (Berechtigungszertifikat)
  - Abwahl von Datenfeldern durch den Nutzer
  - PIN-Eingabe, falls Basisleser genutzt wird
  - Bindeglied zwischen Karte, Bürger und Dienstanbieter
  - Keine Verschlüsselung – macht die Karte

„Sicherheitslücke“ Kartenleser

Basisleser (ohne PIN-Pad)

- PIN kann mitgeschnitten werden, falls Rechner verseucht (→ nichts neues)
- Zwei-Faktor-Authentisierung (→ PIN alleine nützt dem Angreifer nichts)
- Verschlüsselung der Daten (→ Auch Angreifer mit PIN und Karte kann keine Daten mitlesen)

Besser viele Anwender mit hoher Sicherheit als wenige mit sehr hoher Sicherheit

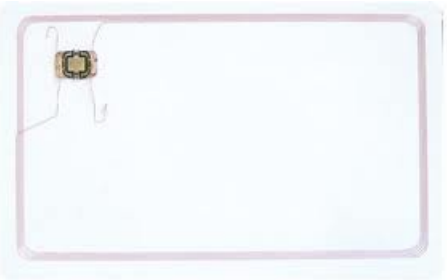


„Sicherheitslücke“ Drittanbieterplugins

- „Neuer“ „Angriff“ – Voraussetzungen:
  - Nutzer gibt PIN in fake-Client ein oder PIN wird abgephisht
  - und Plugin mit ungesichertem Zugriff auf Kartenleser installiert
  - und XSS-Lücke auf Webseite eines bestimmten Dritten
    - oder Inhaber ignoriert Warnung „Webseite will auf Kartenleser zugreifen“
  - und Karte liegt im Moment des „Angriffs“ auf Kartenleser
- Auswirkungen:
  - „Angreifer“ stößt Authentisierung gegenüber berechtigtem DA an
  - „Angreifer“ erhält keine Ausweisdaten
  - Analog zum „Trojaner-Angriff“ (Plugin + XSS statt Trojaner)
- Funktioniert (ähnlich) auch mit Standardleser, QES-Karten, …
  - → weder Problem der Lesegeräte noch des Ausweises

„Sicherheitslücken“ … und sonst

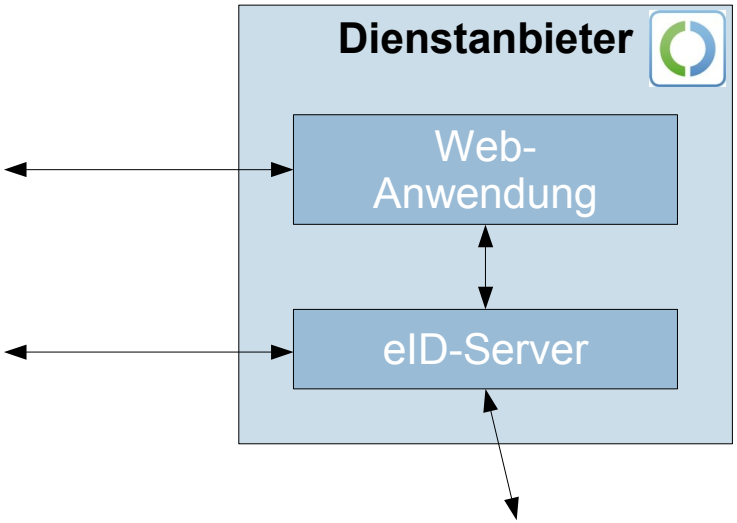
- AusweisApp
  - Fehlerhafte Überprüfung des Verbindungsaufbaus beim Update
    → Umlenken auf anderen Server möglich
    - Zugriff auf DNS-Server des Nutzers notwendig
    - Signaturprüfung des Updates vor Installation
- Zerstörung des Chips
  - Immer möglich (Schere, Knicken, …)
    - Also nichts neues oder unerwartetes
  - Auswirkungen
    - Keine Nutzung der neuen Funktionen
    - Hoheitliche Kontrolle: Nutzung anderer Merkmale



In keinem Fall Gefährdung personenbezogener Daten

„Der Personalausweis wurde gehackt“ ist falsch

Dienstanbieter



eID-Server

Kommunikation mit Anwendung des Dienstanbieters, Client-Software des Bürgers und Hintergrundsystemen

Speicherung Berechtigungszertifikat & -schlüssel, Sperrliste, ...

TR-03130: Einheitliche interoperable offene Schnittstelle

Potentielle Angriff Dienstanbieter

- Kompromittierung privater Schlüssel des Dienstanbieter
  - Nur zwei Tage gültig, nach Kompromittierung keine Ausstellung eines neuen Zertifikates
- Angriffe auf Kundendatenbanken etc.
  - Wie bisher, das „System Personalausweis“ endet nach Beendigung der Online-Authentisierung
  - Durch Datenschutzfunktionen des Ausweises (z.B. Pseudonym) weniger Daten beim Dienstanbieter
  - Keine Signatur der eID-Daten
    - kein Echtheitsnachweis gegenüber Dritten
    - eID-Daten sind nicht von Daten aus anderen Quellen unterscheidbar

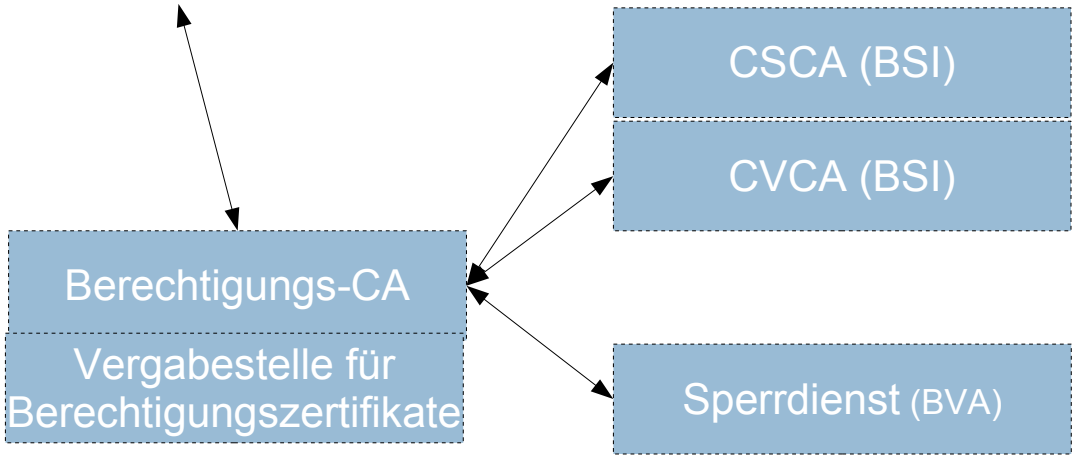
Hintergrundsysteme

Vergabestelle für Berechtigungszertifikate (VfB) beim BVA

- Verwaltungsverfahren
- Vergibt Berechtigungen für maximal 3 Jahre
- Festlegung der max. Zugriffsrechte

Berechtigungs-CA

- Trustcenter gemäß Signaturgesetz
- Stellt Berechtigungs-zertifikate entspr. Berechtigung bereit
- Stellt Zertifikate für Echtheitsprüfung und Sperrlisten bereit



Was bedeutet „Der Personalausweis ist sicher“?

Sichere kryptographische Protokolle

Kein Schutz gegen Malware

Volle Nutzerkontrolle durch Karte und PIN – solange Nutzer Karte und PIN nicht aus der Hand gibt

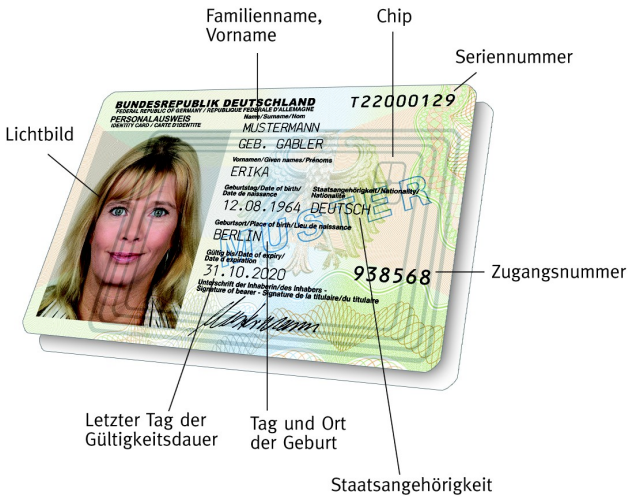
Elektronische Identität ist Infrastrukturmaßnahme zur Erhöhung der Sicherheit im Netz, kann aber nicht alle Probleme des Netzes lösen

Datenschutzfreundliche Ausgestaltung – solange der Nutzer nicht freiwillig mehr Daten preisgibt

Sichere gegenseitige Authentisierung

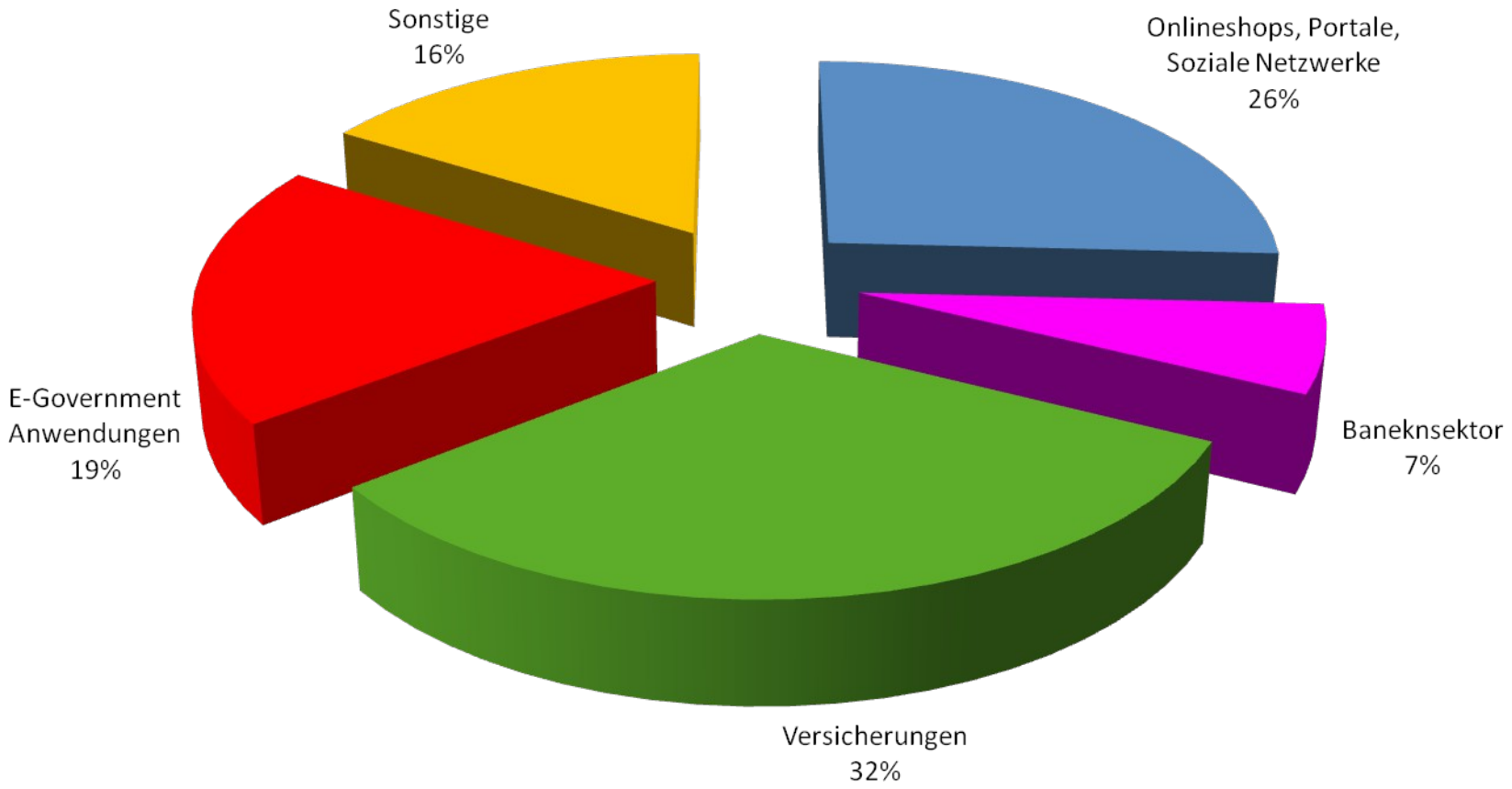
Kein absoluter Schutz gegen Social-Engineering – aber macht Phishing schwieriger

Personalausweis -- Eckdaten aus dem Livebetrieb



- Gut 7 Mio. produzierte Ausweise seit 01.11.2011
- Durchschnittliche Bearbeitungszeit 1 - 2 Wochen
- Über 30 Live-Anwendungen, über 50 weitere in Vorbereitung
- Fast die Hälfte der Bürger hinterlegt ihre Fingerabdrücke
- Knapp die Hälfte schaltet eID-Funktion frei

Anwendungsbereiche aktuelle Dienstanbieter

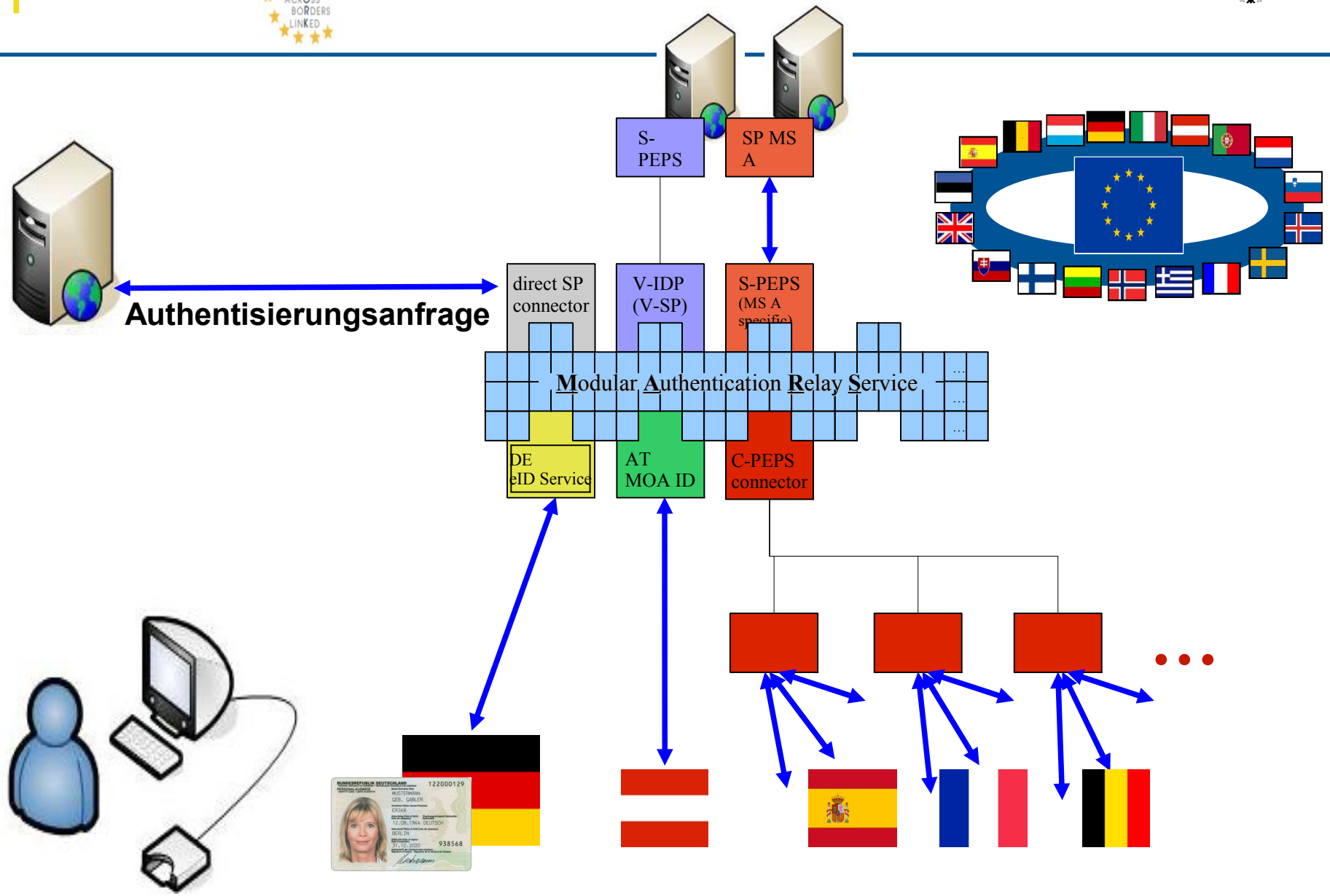


eID – Beispiele in Europa

- Finnland: FINEID seit 2000
- Estland: eCard seit 2002
- Belgien: eID seit 2003
- Österreich: eCard seit 2004
- Schweden: National eID seit 2005
- Italien: CIE & CNS seit 2006
- Portugal: Cartão de Cidadão seit 2007
- … und mehr

- Demnächst: PL und FR

STORK im Überblick



Quo vadis?

- (Fast) 1 Jahr Personalausweis
  - Das System funktioniert
  - Mehrere Anbieter eID-Client/eID-Server/eID-Service/BerCA
  - Mehr Dienstanbieter wären schön
- Weitere eID-Karten
  - 01.09.2011: elektronischer Aufenthaltstitel
  - Offen: EU-Bürger? (Zur Zeit: STORK et. al.)
- Mobile Nutzung (Smartphones als Lesegeräte)
- In Planung: eGovernment-Gesetz

Der Personalausweis ist ein lebendes, kein abgeschlossenes Projekt


BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE
T22000129
PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE
Name/Surname/Nom
MUSTERMANN
GEB. GABLER
Vornamen/Given names/Prénoms
ERIKA
Geburtstag/Date of birth/
Date de naissance
12.08.1964
Staatsangehörigkeit/Nationality/
Nationalité
DEUTSCH
Geburtsort/Place of birth/Lieu de naissance
BERLIN
Gültig bis/Date of expiry/
Date d'expiration
31.10.2020
938568
Unterschrift der Inhaberin/des Inhabers -
Signature of bearer - Signature de la titulaire/du titulaire
6408125<2010315D<<<<<<<<<<<<<<4
MUSTERMANN<<ERIKA<<<<<<<<<<<<<<

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Jens Bender
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-5051
Fax: +49 (0)22899-109582-5051

jens.bender@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de