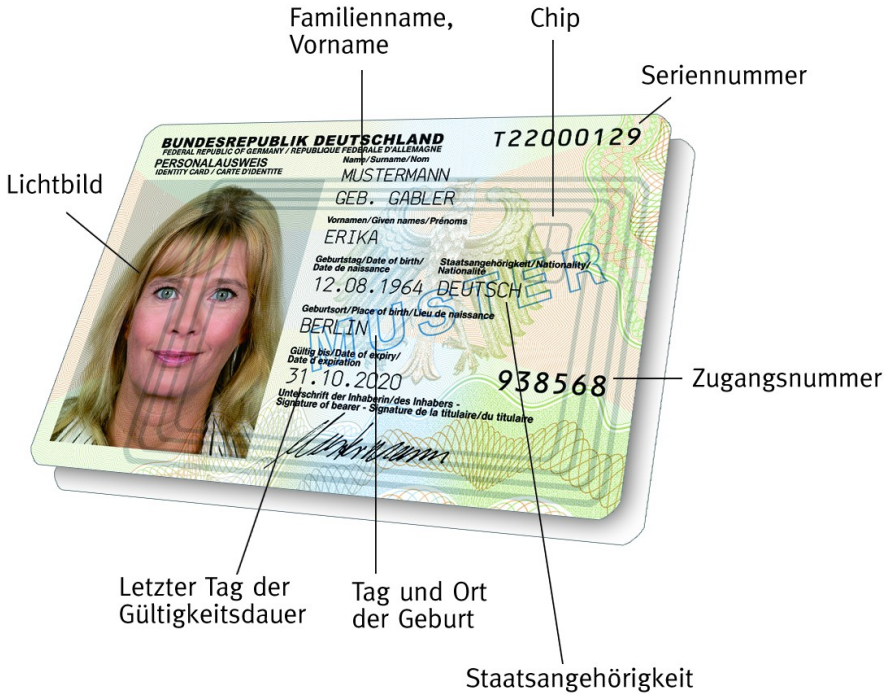
Der neue Personalausweis
Warum er so ist wie er ist.

Dr. Jens Bender

Bundesamt für Sicherheit in der Informationstechnik

CeBIT / 03.03.2011

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

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

Designprinzipien

Sichere elektronische Prozesse

Datenschutz

Sicherheit als Grundlage,
nicht als add-on

Volle Kontrolle durch
den Ausweisinhaber

Einfache Anwendbarkeit

Überschaubarer Aufwand
für alle Beteiligten

Freiwilligkeit der Nutzung

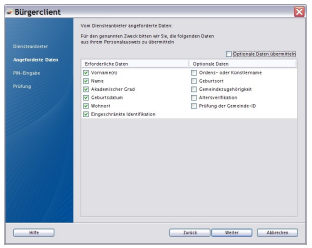
Offene Spezifikationen

Vorteile für alle Beteiligte

Keine Karte für alles
(Geldkarte, Versicherungskarte, Club-Karte, …)
→ „nur“ Identifikation und Unterschrift, das dafür richtig

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
- **AusweisApp**: Lokale Software für den Bürger
- **eID-Server**: Gegenstück zum Bürgerclient beim Dienstanbieter
- **PKI**s, **Sperrdienst**
- Hotline



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!

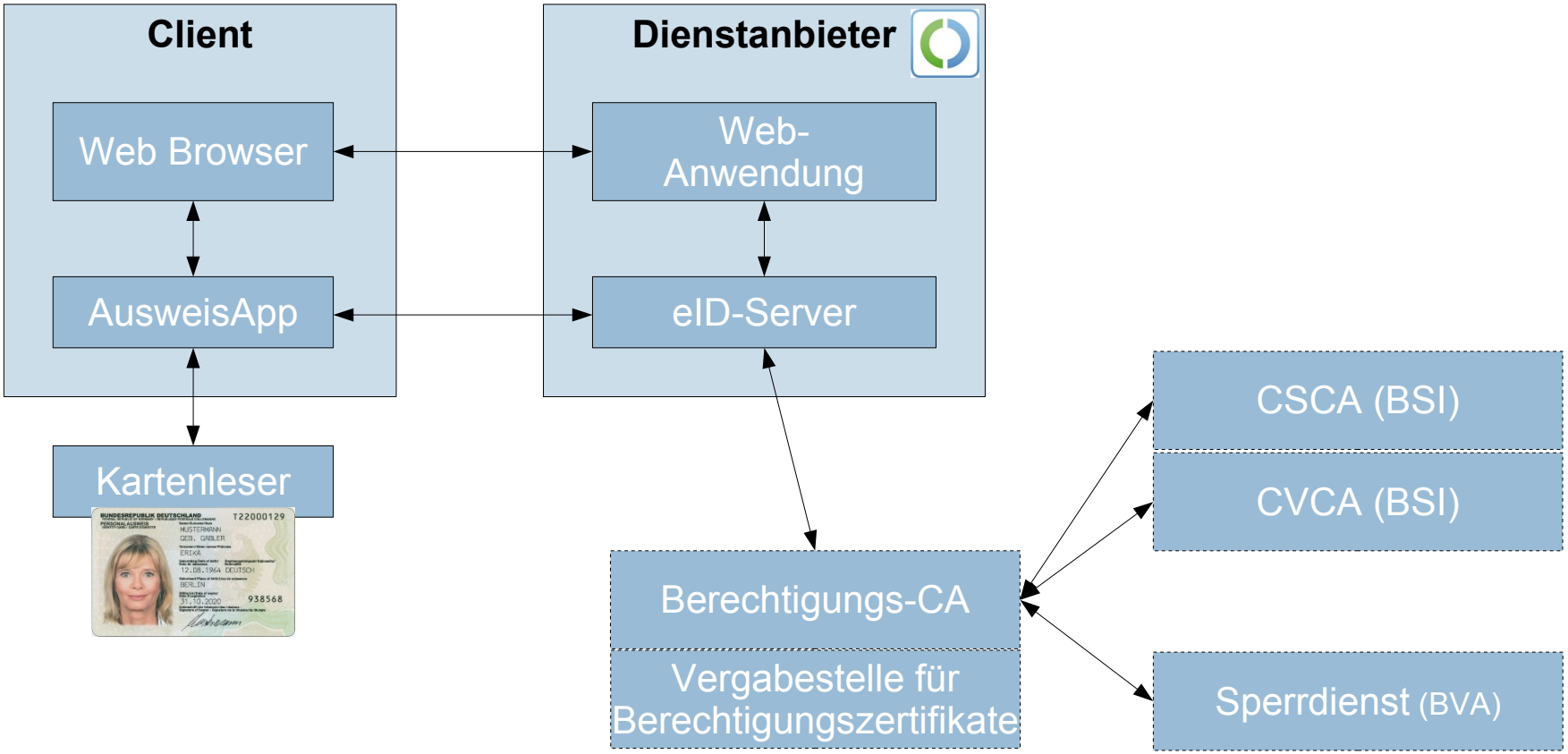
Bürger weist sich mit *Ausweis* aus

Dienstanbieter:

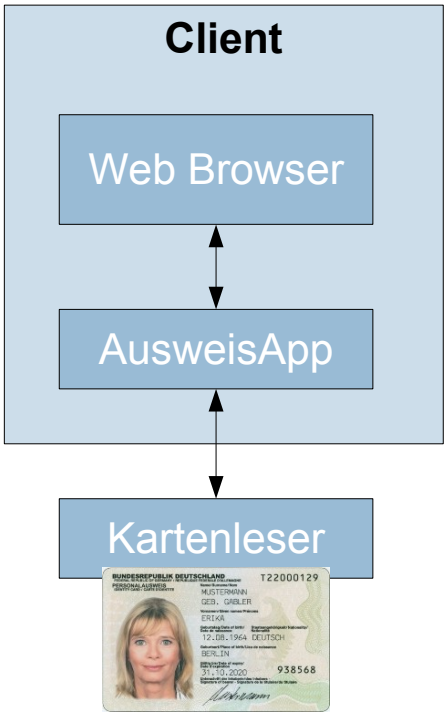
Kann die Person ihre elektronische Identität beweisen?

Datenschutz by Design
Datensparsamkeit – Volle Nutzerkontrolle

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:

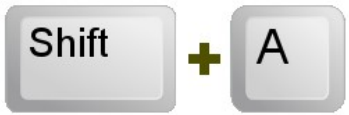
- Basisleser
  - Eignung für mobilen Betrieb
  - Freie Wahl des Formfaktors – Integrationsfähigkeit
- Standardleser
  - PIN-Pad für PIN-Eingabe bei Anwendungen mit höherem Schutzbedarf
- Komfortleser
  - Bestätigung nach SigG für QES
  - Nutzung eines Komfortlesers wird bei PA-QES technisch erzwungen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

„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



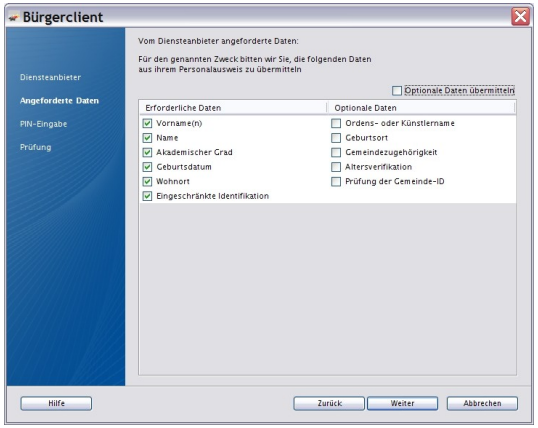
Kosten

Sicherheit

AusweisApp

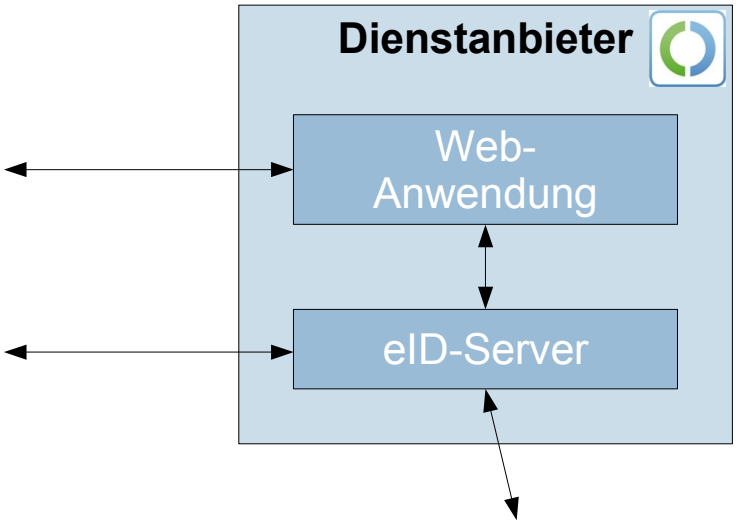
Offene Spezifikation –
Jeder kann Software schreiben und zertifizieren lassen

Der Bund stellt kostenfrei AusweisApp als zertifizierte Software 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

Dienstanbieter



eID-Server

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

Speicherung Berechtigungszertifikat & -schlüssel, Sperrliste, ...

TR-03130: Einheitliche interoperable offene Schnittstelle

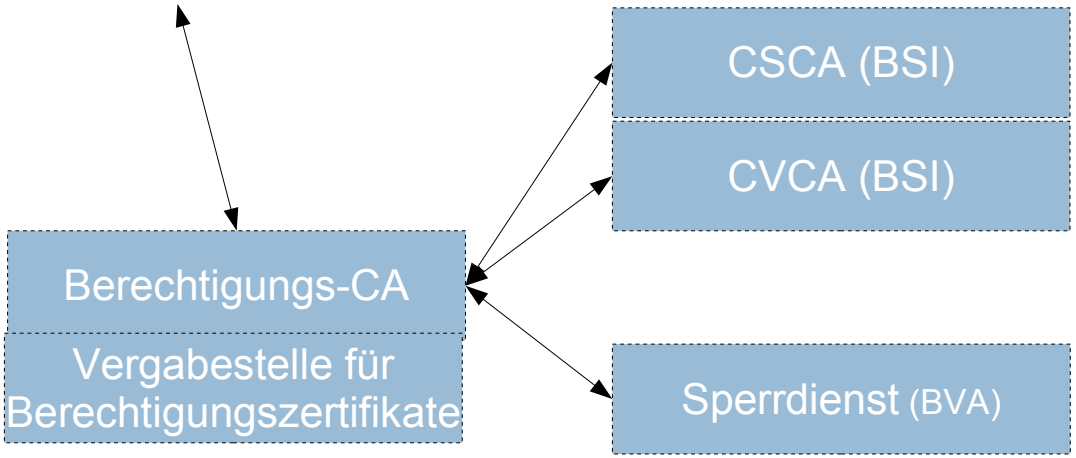
Hintergrundsysteme

Vergabestelle für Berechtigungszertifikate (VfB) beim BVA

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

Berechtigungs-CA

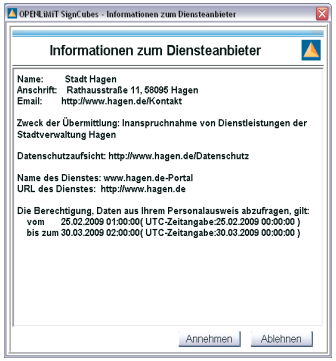
- Trustcenter gemäß Signaturgesetz
- Stellt Berechtigungs-zertifikate entspr. Berechtigung bereit
- Stellt Zertifikate für Echtheitsprüfung und Sperrlisten bereit

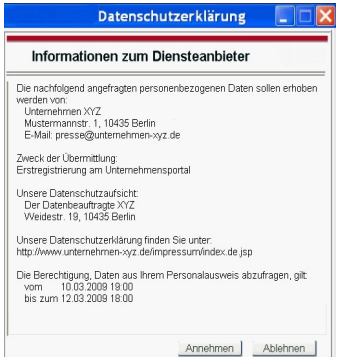


Berechtigung und Berechtigungszertifikat

Inhalt (§ 18 Abs. 4 PAuswG)

- Name, Anschrift, E-Mail des Diensteanbieters
- Kategorien der angefragten Daten (Zugriffsrechte)
- Zweck der Übermittlung
- Verweis auf Datenschutzerklärung, Datenschutzbehörde
- Gültigkeitsdauer des Berechtigungszertifikats

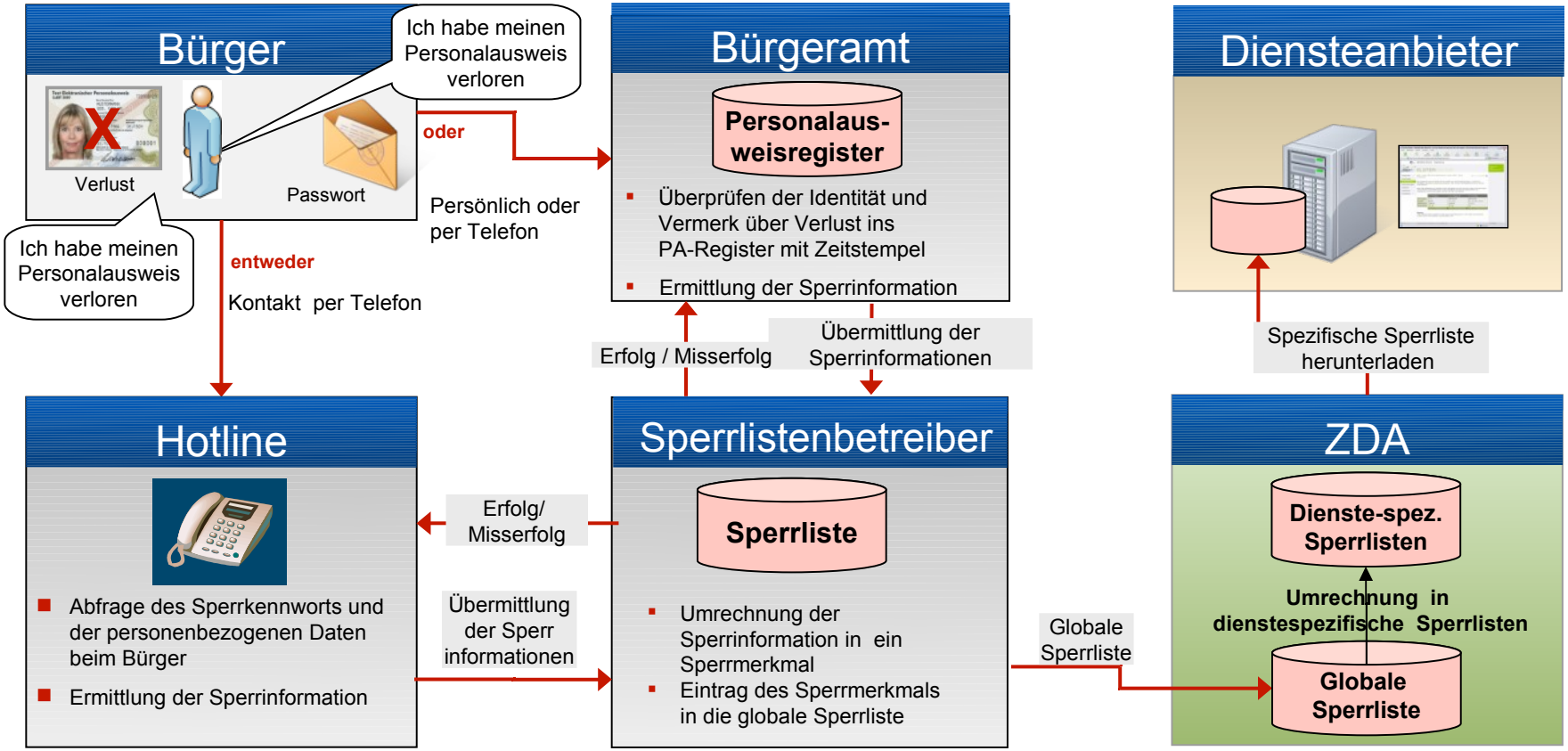




Antrags- und Erteilungsvoraussetzungen

- kein rechtswidriger Zweck
- keine geschäftsmäßige Übermittlung von Daten
- **Erforderlichkeit der Datenkategorien für den Geschäftszweck**
- Maßnahmen zu Datenschutz und -sicherheit
- keine Anhaltspunkte für missbräuchliche Verwendung

Sperrdienst



Zertifizierungen
der sicherheitsrelevanten Komponenten

- Ausweischip
  - enthält personenbezogene Daten → Sicherheitsanker
- Software für Biometrieerfassung und -qualitätssicherung
- Kommunikationsmodule Ausweishersteller
- Änderungsterminal
  - Sicherheit und Interoperabilität
- Kartenleser
  - Prüfumfang abhängig vom Lesertyp
    - Physikalische und elektronische Interoperabilität
    - Sicherheit bei Standard- und Komfortleser
- Client-Software
  - Interoperabilität mit Karte und eID-Server
  - Sicherheit der Anzeige, PIN-Eingabe, … (soweit möglich)

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

Technische Richtlinien (TR) und Schutzprofile (PP)

Technische Richtlinien (TR)	Schutzprofile (PP)
■ Kartenspezifikation (EAC, PACE, usw.) ■ QES auf eCards mit kontaktl. Schnittstelle ■ Produktionsdatenerfassung, qualitäts-prüfung und –übermittlung ■ Biometrie ■ Kartenleser mit ePA-Unterstützung ■ eCard-API-Framework – Middleware für Client und eID-Server ■ Hintergrundsysteme (PKI) ■ Elliptische-Kurven-Kryptographie ■ Kryptographische Verfahren: Empfehlungen und Schlüssellängen ■ …	■ Elektronischer Personalausweis ■ Inspektionssysteme für elektronische Ausweisdokumente (u.a. Änderungsterm.) ■ AusweisApp: QES-Funktion ■ AusweisApp: eID-Funktion 

www.bsi.bund.de/ElektronischeAusweise

Sicherheitsbeweise für Kryptographie
Zeitschriftenartikel und weiterführende Informationen


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