

# Der neue Personalausweis im Kontext sicherer Identitäten

Dennis Kügler

Bundesamt für Sicherheit in der  
Informationstechnik

Vis!t, 07.-08. September 2010, Bern, CH

# Der neue Personalausweis

- ❑ Einführung am 01.11.2010
- ❑ Scheckkartenformat
- ❑ Rein kontaktlos
- ❑ Anwendungen
  - ❑ ePass
  - ❑ eID
  - ❑ eSign (optional)
- ❑ Passworte
  - ❑ PIN
  - ❑ PUK
  - ❑ CAN
  - ❑ (Separate Signatur-PIN)



# Rechtliche und Technische Vorgaben

- ❑ **Gesetz über Personalausweise und den elektronischen Identitätsnachweis**
  - ❑ Allgemeiner Rechtsrahmen
- ❑ **Verordnung über Personalausweise und den elektronischen Identitätsnachweis**
  - ❑ u.a. Vorgaben für die Sicherheit und Datenschutz der eID-Infrastruktur
- ❑ **Signaturgesetz & -verordnung**
- ❑ **Technische Richtlinien und Schutzprofile des BSI**
  - ❑ Spezifikationen
  - ❑ Zertifizierungsgrundlagen
    - ❑ CommonCriteria / Konformität nach TR

# Sichere Identitäten

- ❑ **Hoheitliches Ausweisdokument**
- ❑ **eID-Anwendung für eBusiness und eGovernment**
  - ❑ Schutz vor Identitätsdiebstahl, Phishing
- ❑ **Sicherheit und Datenschutz**
  - ❑ Informationelle Selbstbestimmung
  - ❑ Gegenseitige Authentisierung
  - ❑ Starke Verschlüsselung und Integritätssicherung
    - ❑ 256 Bit Elliptische Kurven und AES-128
- ❑ **Biometrie nur für hoheitliche Anwendung**
  - ❑ Gesichtsbild und optional Fingerabdrücke in der ePass-Anwendung

# Trennung eID und eSign Anwendung

- ❑ **eSign: Qualifizierte elektronische Signatur (optional)**
  - ❑ Elektronisches Äquivalent zur eigenhändige Unterschrift
  - ❑ Identifizierung statt Authentisierung
    - ❑ Beweiskraft gegenüber Dritten / Nichtabstreitbarkeit
    - ❑ Qualifiziertes Zertifikat ist immer personengebunden
  - ❑ Hohe Anforderung an Kartenlesegerät (SigG-Bestätigung)
- ❑ **eID: Elektronischer Identitätsnachweis**
  - ❑ Elektronisches Äquivalent zum Vorzeigen des Personalausweises
  - ❑ Keine Beweiskraft für Dritte
  - ❑ Selektive Freigabe von personenbezogenen Daten
    - ❑ Altersverifikation (z.B. über 18 Jahre,...)
    - ❑ Wohnort in einer bestimmten Region (z.B. Bonn oder NRW)

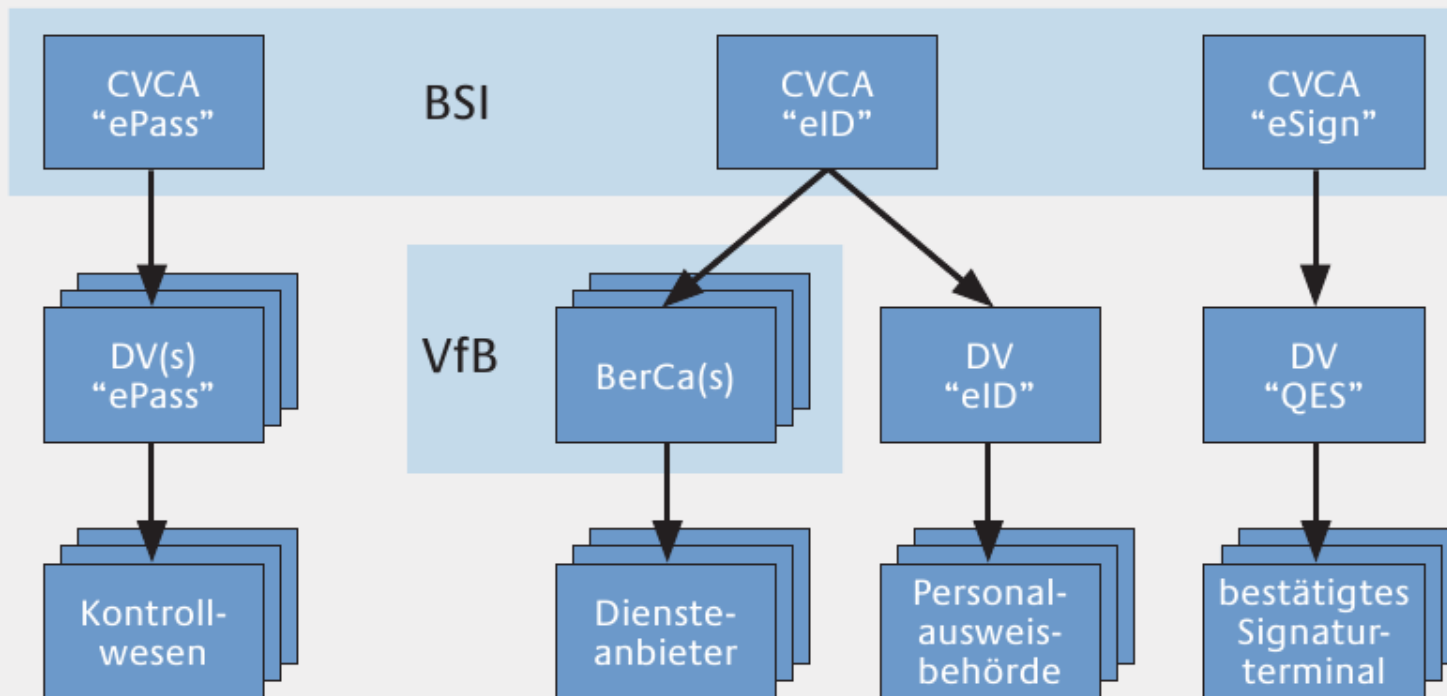
# Privacy by Design

- ❑ **Jede elektronische Nutzung des Personalausweises erfordert Berechtigungszertifikate**
- ❑ **Vergabestelle für (eID) Berechtigungszertifikate**
  - ❑ Staatliche Prüfung des Dienstanbieters
    - ❑ Welche Daten er benötigt
    - ❑ Ob er vertrauenswürdig ist
- ❑ **Berechtigungszertifikate**
  - ❑ Prüfung durch Personalausweis
  - ❑ Enthält Berechtigungen des Dienstanbieters
  - ❑ Nutzer kann Berechtigungen weiter einschränken
  - ❑ Freigabe durch 6-stellige persönliche Geheimnummer (PIN)
- ❑ **Ende-zu-Ende Verschlüsselung/Integritätssicherung**
  - ❑ Personalausweis ↔ Dienstanbieter

# Public Key Infrastrukturen

## CVCA Public Key Infrastructure

für Bürgeranwendungen des neuen Personalausweises



CVCA - Country Verifying Certification Authority  
DV - Document Verifier  
BerCA - Berechtigungs Certification Authority

VfB - Vergabestelle für Berechtigungszertifikate  
QES - Qualifizierte elektronische Signatur

# Karten- und dienstspezifische Merkmale

- ❑ **Personalausweis erzeugt Pseudonyme**
  - ❑ Eindeutiges Pseudonym pro Karte und Dienstanbieter
  - ❑ Dienstanbieter können Pseudonyme nicht verketteten
- ❑ **Nutzung der Pseudonyme beim Dienstanbieter**
  - ❑ Wiedererkennen „bekannter“ Personalausweise...
  - ❑ ...ohne personenbezogene Daten zu verwenden
- ❑ **Zwei unterschiedliche Merkmale pro Karte**
  - ❑ **Pseudonym:** Dienstanbieter benötigt Berechtigung, Pseudonym darf gespeichert werden.
  - ❑ **Sperrkennung:** Zur Sperrung gestohlener Ausweise, darf nicht gespeichert werden!

# Sperrmanagement

□ **Auslösung der Sperrung idR. durch Sperrkennwort**

□ **Sperrsumme als Hash indiziert Sperrschlüssel**

□ Name

□ Vorname

□ Geburtsdatum

□ Sperrkennwort

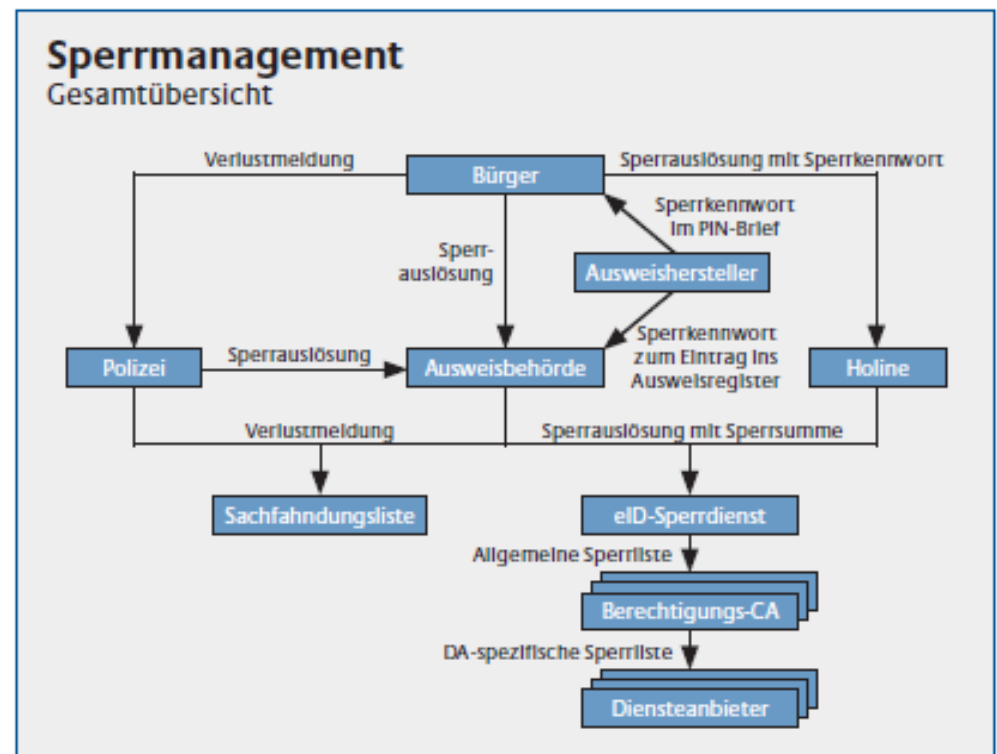
□ **Sperrdienst**

□ Aktiviert Sperrschlüssel

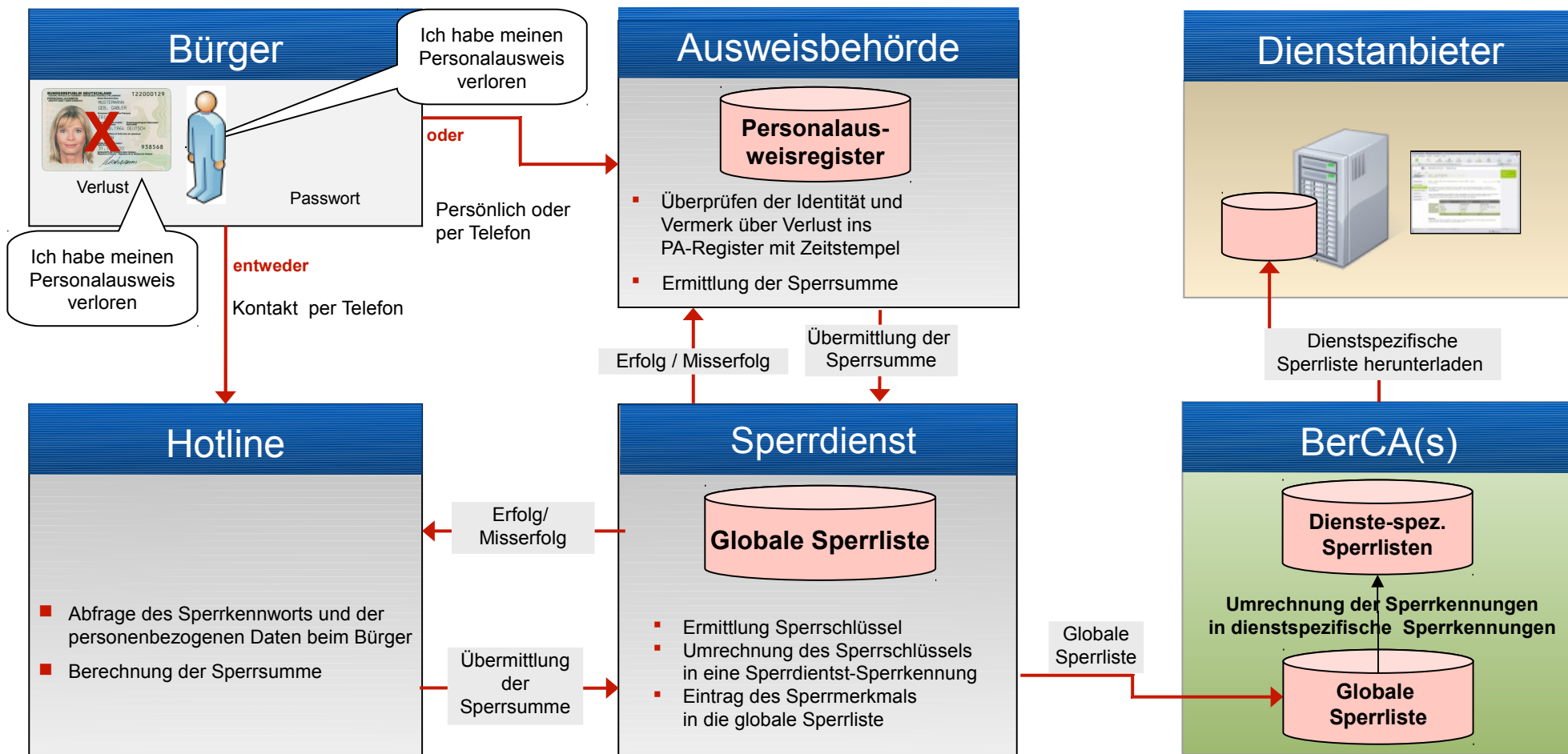
□ Erstellt globale Sperrliste

□ **BerCAs**

□ Erstellen dienstspezifische Sperrlisten mit Sperrkennungen



# Auslösen der Sperrung



# Lesegeräte mit Personalausweisunterstützung

## ❑ Basisleser

- ❑ kontaktlose Schnittstelle

## ❑ Standardleser

- ❑ PIN-Pad
- ❑ PACE Protokoll
- ❑ Optional weitere Komponenten

## ❑ Komfortleser

- ❑ Kontaktlos und kontaktbehaftet
- ❑ PIN-Pad und Display
- ❑ Berechtigungszertifikate für QES („Bauartzulassung“)
- ❑ PACE + EAC Protokoll



# Angriffe auf Lesegeräte

## ❑ Missbrauch der eID Funktion

- ❑ **Basisleser:** Mitlesen der geheimen PIN

- ❑ Keylogger / Schadsoftware am PC

- ❑ **Standardleser:** Täuschung über Dienstanbieter

- ❑ Schadsoftware, Falsche Anzeige am PC

- ❑ **Komfortleser:** Sicherste Variante, aber...

- ❑ ...idR. zweizeiliges Display, vollständige Prüfung schwierig

## ❑ Auswirkungen

- ❑ Übertragene Daten immer Ende-zu-Ende verschlüsselt

- ❑ Mitlesen durch Schadsoftware nicht möglich

- ❑ Authentisierung ist keine Willenserklärung...

- ❑ ...und nicht gegenüber Dritten nachweisbar

# Zusammenfassung

- ❑ **Sichere Identitäten durch den neuen Personalausweis**
  - ❑ Gegenseitige Authentisierung / Berechtigungszertifikate
  - ❑ Dienstanbieter staatlich durch VfB geprüft
  - ❑ Datensparsam, nur notwendige Daten werden übertragen
  - ❑ Keine Beweiskraft gegenüber Dritten
  - ❑ Erzeugung dienstspezifischer Pseudonyme
  - ❑ Ende-zu-Ende Verschlüsselung zur Absicherung gegen Schadsoftware am PC
  - ❑ Geringe Anforderungen an Kartenleser
- ❑ **Optional qualifizierte elektronische Signatur**
  - ❑ Rechtsverbindliche Unterschrift (ECDSA!)
  - ❑ Hohe Anforderungen an Kartenleser
- ❑ **Hoheitliche Nutzung erfordert ebenfalls Zertifikate**

# Kontakt

## Bundesamt für Sicherheit in der Informationstechnik (BSI)

**Dr. Dennis Kügler**  
**Referat 312**  
**Godesberger Allee 185 -189**  
**53175 Bonn**

**Tel: +49 (0)22899-9582-5183**  
**Fax: +49 (0)22899-10-9582-5183**

**[dennis.kuegler@bsi.bund.de](mailto:dennis.kuegler@bsi.bund.de)**  
**[www.bsi.bund.de](http://www.bsi.bund.de)**  
**[www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)**

