Zusammenspiel von Datenschutz und Informationssicherheit

Oliver Klein / Florian Bierhoff
Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn

Kiel, 25.08.2014

Agenda

1. Das BSI im Überblick

2. Begrifflichkeiten, Schnittmengen und gemeinsame Schutzziele

3. Informationstechnische Lösungen für Anforderungen des Datenschutzes

4. Aktuelle Beispiele für das Zusammenspiel von Datenschutz und Informationssicherheit und aktuelle politische Entwicklungen

Bundesamt
für Sicherheit in der
Informationstechnik

Das BSI im Überblick: Aufgaben und Zielgruppen

Regierung und Verwaltung

- IT-Sicherheitsberatung
- Entwicklung von Kryptosystemen
- Sicherheit der Regierungsnetze
- CERT-BUND
- Cyber-Abwehrzentrum

Wissenschaft

- Mitwirkung beim IT-Sicherheitsforschungs-programm des BMBF
- Kooperation mit Universitäten

Bürger

- Sensibilisierungskampagnen
- Internetangebote für Bürger
- Informationsmaterialien
- Service-Center für Privatanwender

Wirtschaft

- Zertifizierung von Produkten
- BSI IT-Grundschutz
- Kooperation mit ISPs
- UP KRITIS
- Allianz für Cyber-Sicherheit

Begrifflichkeiten, Schnittmengen und gemeinsame Schutzziele

- Datenschutz = Schutz personenbezogener Daten vor Missbrauch

- Informationssicherheit = Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität

Begrifflichkeiten, Schnittmengen und gemeinsame Schutzziele

- § 9 BDSG und Anlage: Technische und organisatorische Maßnahmen
- Art. 16 (Vertraulichkeit der Verarbeitung) und Art. 17 (Sicherheit der Verarbeitung) der europäischen Datenschutzrichtlinie (95/46/EG)
- Art. 23 (Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen), Art. 30 (Sicherheit der Verarbeitung) und Art. 39 (Zertifizierung) im Entwurf EU-DSGVO
- Spezialgesetzliche Regelungen, bspw. im PAuswG oder De-Mail-G

Informationstechnische Lösungen für Anforderungen des Datenschutzes

- Privacy / Security by Design
- Kryptographie
- Public-Key-Infrastrukturen
- Mehrfaktoren-Authentisierung
- IT-basierte Rollen- bzw. Zugangskonzepte
- ...

Aktuelle Beispiele und Entwicklungen

- Millionenfache Online-Identitätsdiebstähle im Jahr 2014
- Datenschutz- und informationssicherheitsrelevante Vorfälle bei großen IT-Unternehmen (z.B. “ebay-Hack” im Mai 2014)

- “Digitale Sicherheit und Datenschutz” als Ziele im Koalitionsvertrag für die 18. Legislaturperiode
- Handlungsfeld “Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft” in der Digitalen Agenda 2014 - 2017 der Bundesregierung

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Oliver Klein
Godesberger Allee 185-189
D-53175 Bonn

Telefon: **022899-9582-5847**
Fax: **022899-9582-5847**

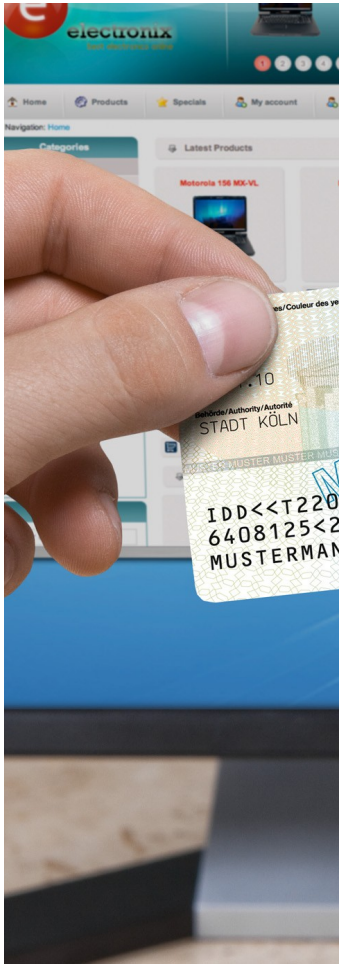
oliver.klein@bsi.bund.de

www.bsi.bund.de
www.bsi-fuer-buerger.de
www.buerger-cert.de

Agenda

1. Personalausweis und De-Mail
2. Elektronische Bildübermittlung
   - Übersicht
   - Status und Datenschutz
3. Sichere elektronische Identitäten
   - Vertrauensniveaus und -dienste
   - Elektronischer Schriftformersatz
   - Bürgerkonten

Personalausweis Kurz & Knapp

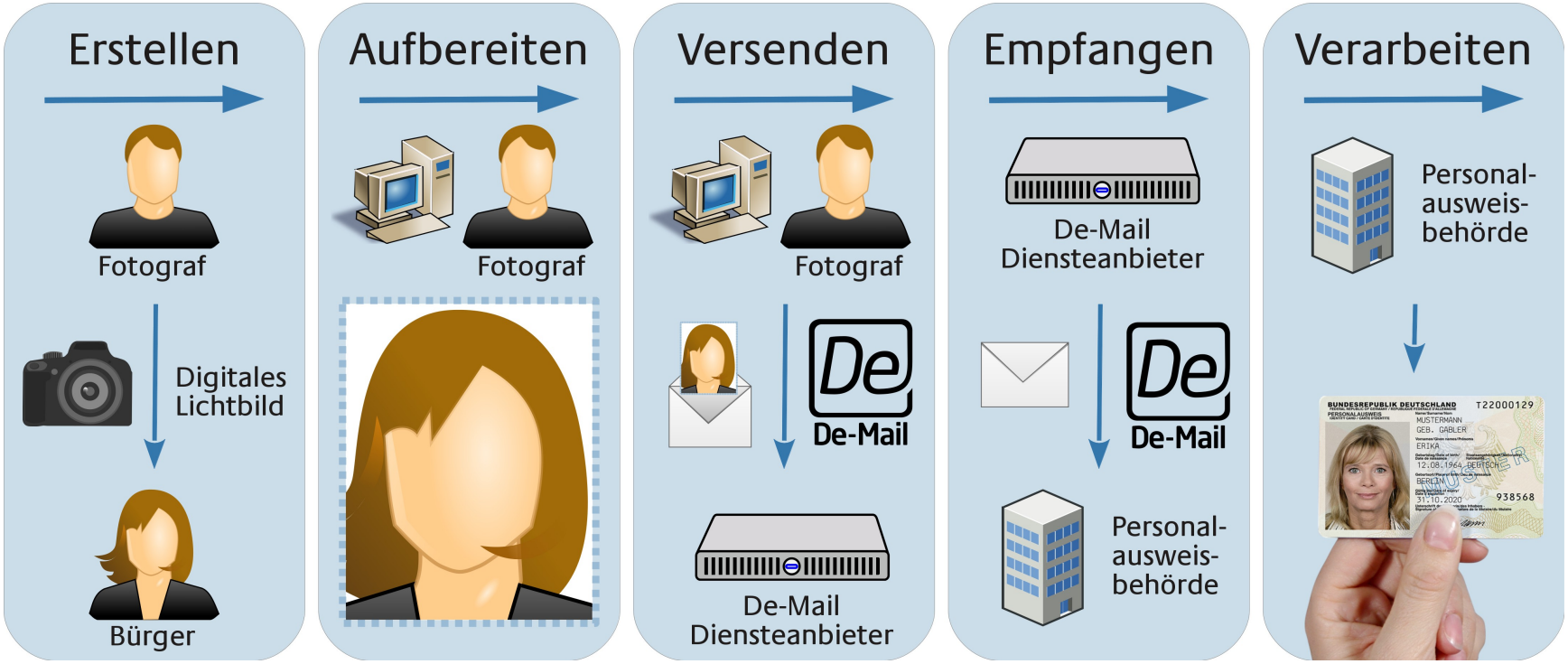


- Es sind drei Anwendungen implementiert
  - **ePass:** Identitätsfeststellung für berechtigte Behörden.
  - **eID:** Online-Ausweisfunktion für E-Government und E-Business.
  - **eSign (Optional):** Qualifizierte elektronische Signatur.
- Beidseitige Authentisierung
  - Diensteanbieter benötigt Berechtigungszertifikat
- 2-Faktor Authentisierung des Inhabers durch
  - **Besitz** (Zertifikat im nPA) und
  - **Wissen** (PIN)

De-Mail Kurz & Knapp

- Verbund von Providern ermöglicht NutzerInnen den verbindlichen und vertraulichen Versand von Nachrichten und Dokumenten
- Staat und Wirtschaft haben gemeinsame Vorgaben definiert, welche die Provider nun umsetzen
- 3 Kernanwendungen
  - **Postfach-& Versanddienst**
  - Identitätsbestätigungsdienst
  - Dokumentenablage

Elektronische Bildübermittlung unter Nutzung von De-Mail



Elektronische Bildübermittlung: Status und Datenschutz

- Pilotprojekt in Göttingen und Köln
  - Mittlerweile mehr als 500 übermittelte Bilder
- Umfangreiche Abstimmungen mit BfDI
  - Information der LfDI durch BfDI
  - Formulierung von Einwilligungserklärung
  - Festlegung von Speicher- und Löschfristen
  - Gestaltung der Bildkennung
    - Primäres Merkmal
      - Hashwert (8 Alphanumerische Zeichen)
    - Optionale sekundäre Merkmale
      - Initialen (2 Buchstaben)
      - Geburtstag (2 Ziffern)
      - Geburtsmonat (2 Ziffern)

Sichere elektronische Identitäten

- Strategie für eID und andere Vertrauensdienste im E-Government (eID-Strategie)
  - Beschluss und Projekt des IT-Planungsrat
  - 10 Maßnahmen (z.B. Akzeptanzsteigerung, Bürgerkonto, ...)
- Einrichtung der PG „eID-Strategie für E-Government“
  - Vertreter aller Bundesländer
  - BMI, BVA, BfDI und BSI
- M10: Technische Richtlinie für Vertrauensdienste
  - Technische Richtlinie (BSI TR-03107) „Elektronische Identitäten und Vertrauensdienste im E-Government“
    - Teil 1: Vertrauensniveaus und Mechanismen
    - Teil 2: Elektronischer Schriftformersatz mit elektronischem Identitätsnachweis

Vertrauensniveaus gemäß BSI TR-03107

- **normal**

  Die Schadensauswirkungen bei einer Kompromittierung sind begrenzt und überschaubar. Dieses Vertrauensniveau entspricht in etwa dem Sicherheitsniveau *normal* gemäß IT-Grundschutz.

- **hoch**

  Die Schadenauswirkungen bei einer Kompromittierung können beträchtlich sein. Dieses Vertrauensniveau entspricht in etwa dem Sicherheitsniveau *hoch* gemäß IT-Grundschutz.

- **hoch+**

  Zusätzlich zum Vertrauensniveau hoch ist eine besondere rechtliche Absicherung des Verfahrens auf Basis einer gesetzlichen Regelung notwendig, die Missachtung von rechtlichen Vorgaben hätte schwerwiegende Auswirkungen. Die Auswirkungen einer unrichtigen Identifizierung oder unrichtigen Zuordnung eines Vorgangs zu einer Identität sind als schwerwiegend anzusehen.

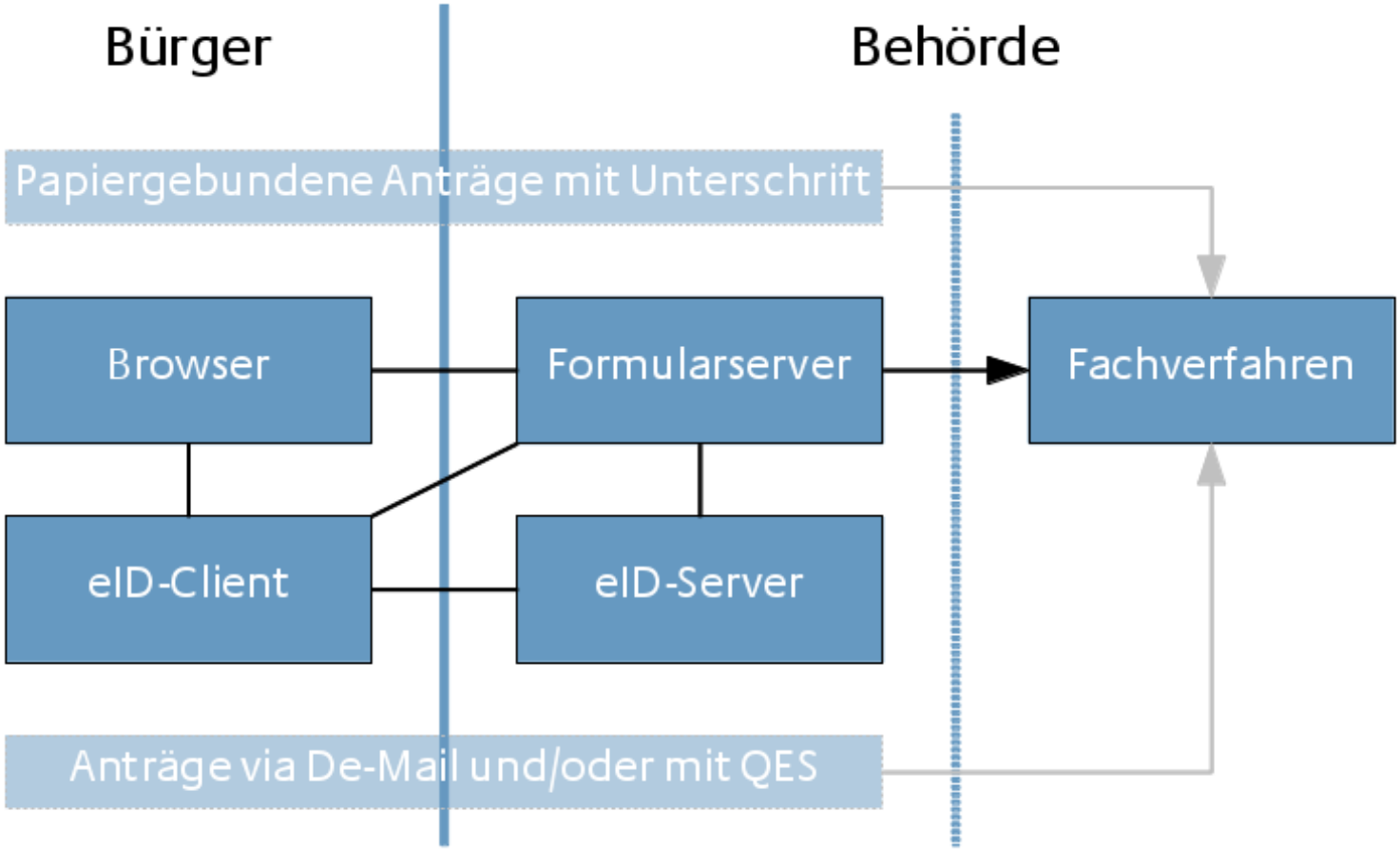
Vereinfachte Übersicht über Vertrauensdienste und -niveaus

		Vertrauensniveaus normal	hoch	hoch+
Identifizierung	Personen: Registrierung/Erstidentifizierung	eID PA		
	Personen: Anmeldung / Login	UserID/Password Krypt. SW-Token Krypt. HW-Token eID PA		
	Dienste	SSL-Zertifikat Berechtigungs-Zertifikat		
Willenserklärung	Elektronische Signaturen	FES (SW-Token) FES (HW-Token) QES		
	Nicht signaturbasiert	Nutzerinteraktion TAN-Verfahren Formular + eID PA Absenderbestätigte De-Mail		
Dokumenten-übermittlung	Versand	De-Mail E-Mail + S/MIME OSCI (Transport-verschl. + Signat.) OSCI (E2E-Verschlüsselung +Signatur) Absenderbestätigte De-Mail		
	Web-Upload	SSL-Zertifikat eID PA		

Elektronischer Schriftformersatz mit elektronischem Identitätsnachweis

- Verwaltungsverfahrensgesetz § 3a
  - Die Schriftform kann ersetzt werden durch unmittelbare Abgabe der Erklärung in einem elektronischen Formulars, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird.
  - In den Fällen [des Satzes 4 Nummer 1] muss bei einer Eingabe über öffentlich zugängliche Netze ein sicherer Identitätsnachweis nach § 18 Personalausweisgesetz oder nach § 78 Absatz 5 des Aufenthaltsgesetzes erfolgen.
- Technische Richtlinie regelt
  - Erfüllung der verschiedenen Funktionen der Schriftform
  - Technische Anforderungen zur Umsetzung

Elektronischer Schriftformersatz mit elektronischem Identitätsnachweis



Bürgerkonten und interoperables Identitätsmanagment

- Es gibt schon jetzt in vielen Bundesländern und dort in Abstimmung mit den LfDIs eigene Bürgerkonten
  - Erfahrungsaustausch in UAG Bürgerkonto
  - Datenschutzgerechter Ausbau von Bürgerkonten (M7)
- Studie zu interoperablem Identitätsmanagement (M8)
- Schaffung einheitlicher Standards für Bürgerkonten

Bürgerkonten und interoperables Identitätsmanagment

- Inhaltliche Abgrenzung „Bürgerkonto“
  - Ein Zugang zu E-Government Diensten des Bundes, der Länder und Kommunen (Interoperabler Identitätsdienst)
  - Dokumentenpostfach und -speicher
- Rahmenbedingungen
  - Nutzung immer freiwillig
  - Kein zentrales Konto
    - eher Weiterleitung an interoperable Dienste
  - Bürger kann mehrere Konten haben
  - Ein Bürgerkonto kann verschiedene Rollen erfüllen
    - Unterscheidung: natürliche / juristische Personen
    - Unterscheidung von Vertrauensniveaus

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Florian Bierhoff
Godesberger Allee 185-189
D-53175 Bonn

Telefon: 022899-9582-5169
Fax: 022899-9582-5169

florian.bierhoff@bsi.bund.de

www.bsi.bund.de
www.bsi-fuer-buerger.de
www.buerger-cert.de