



# Der neue Personalausweis

Marian Margraf

Bundesministerium des Innern

12.11.2010





# Übersicht



## Identifizierung

für hoheitl. Anwendungen

Gesichtsbild

Fingerabdruck

Name, Vorname

Geburtsdatum

usw.

## Authentisierung

für E-Business/E-Govern.

Name, Vorname

Adresse

Alter/Altersverifikation

Pseudonym

usw.

## Signatur

für E-Business/E-Govern.

qualifizierte

elektronische

Signatur

nach deutschem

Signaturgesetz

# Hoheitliche Funktion

*Optisches Lesen der Zugangsnummer*



**PACE**

*Optischer Zugang zum nPA sichergestellt*

*Verschlüsselte Kommunikation*



**Chip Authentication**

*Chip des nPA ist original*

*Verschlüsselte Kommunikation*



**Terminal Authentication**

*Lesegerät hat entsprechende Leserechte*

Lesen der Daten des Chips (Name, Vorname, Gesichtsbild, Fingerabdruck usw.)





# Authentisierungsfunktion

Bürger

Diensteanbieter



Terminal Authentisierung

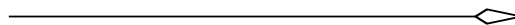


Gegenseitige Authentisierung



PACE

Chip Authentisierung





# Identitätsnachweis

**Identitätsnachweis- Anbieterinformationen**

Anbieterinformationen  
Datenauswahl  
PIN-Eingabe  
Übermittlung

**Angaben des Anbieters**

**Name und Anschrift**  
OpenLimit SgnQubes, Saarbrücker Straße 38a, 10405 Berlin  
[anwendungszentrum@openlimit.com](mailto:anwendungszentrum@openlimit.com)  
[Datenschutzerklärung](#)

**Zweck der Datenanfrage**  
Online-Kauf von Büchern (ggf. mit Altersbeschränkung)

**Betrieblicher Datenschutzbeauftragter**  
Armin Lunkeit, [armin.lunkeit@openlimit.com](mailto:armin.lunkeit@openlimit.com)

**Zuständige Datenschutzaufsicht**  
Berliner Beauftragter für Datenschutz und Informationsfreiheit  
Dr. Alexander Dix, An der Urania 4 – 10, 10787 Berlin  
[mailbox@datenschutz-berlin.de](mailto:mailbox@datenschutz-berlin.de)

**Die Berechtigung zur Abfrage von Daten ist gültig**  
vom 18. Februar 2010 1:00 Uhr (MEZ)  
bis 5. April 2010 2:00 Uhr (MEZ)

Hilfe Zurück Weiter Abbrechen



# Identitätsnachweis

**Identitätsnachweis- Datenauswahl**

Anbieterinformationen  
**Datenauswahl**  
PIN-Eingabe  
Übermittlung

### Angefragte Datenfelder

Für den genannten Zweck bitten wir Sie, die folgenden Daten aus Ihrem Personalausweis zu übermitteln: [Datenschutzerklärung](#)

<input type="checkbox"/> Vorname(n)	<input type="checkbox"/> Ordens- oder Künstlername
<input type="checkbox"/> Familienname	<input type="checkbox"/> Ausweistyp
<input type="checkbox"/> Doktorgrad	<input type="checkbox"/> Ausstellendes Land
<input type="checkbox"/> Anschrift	<input type="checkbox"/> Wohnortbestätigung
<input type="checkbox"/> Geburtstag	<input type="checkbox"/> Altersbestätigung
<input type="checkbox"/> Geburtsort	<input type="checkbox"/> Pseudonym / Kartenkennung

Wenn Sie mit der Übermittlung der ausgewählten Daten einverstanden sind, geben Sie bitte Ihre 6-stellige Personalausweis-PIN ein.

Personalausweis-PIN

Hilfe Zurück **Weiter** Abbrechen



# Identitätsnachweis

### Identitätsnachweis- PIN-Eingabe

Anbieterinformationen  
Datenauswahl  
**PIN-Eingabe**  
Übermittlung

7	3	4
2	9	0
5	8	1
6		

**PIN-Pad aus**

Angefragte Daten

Für den genannten Zweck bitten wir Sie, die folgenden Daten aus Ihrem Personalausweis zu übermitteln:

<input type="checkbox"/> Vorname(n)	<input type="checkbox"/> Ordens- oder Künstlername
<input type="checkbox"/> Familienname	<input type="checkbox"/> Ausweistyp
<input type="checkbox"/> Doktorgrad	<input type="checkbox"/> Ausstellendes Land
<input type="checkbox"/> Anschrift	<input type="checkbox"/> Wohnortbestätigung
<input type="checkbox"/> Geburtstag	<input type="checkbox"/> Altersbestätigung
<input type="checkbox"/> Geburtsort	<input type="checkbox"/> Pseudonym / Kartenkennung

Wenn Sie mit der Übermittlung der ausgewählten Daten einverstanden sind, geben Sie bitte Ihre 6-stellige Personalausweis-PIN ein:

Personalausweis-PIN

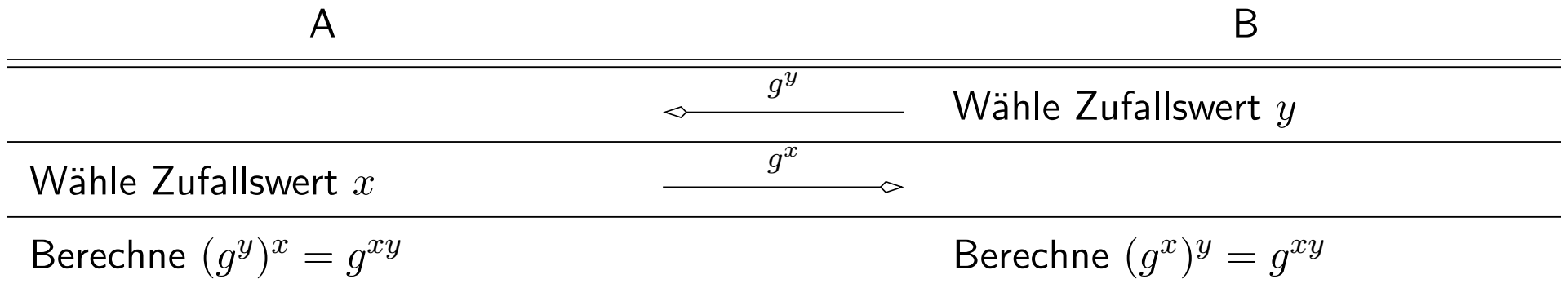
Hilfe Zurück **Absenden** Abbrechen

# Diffie-Hellman-Schlüsselaustausch

**Ziel:** Schlüsselaustausch über unsichere Kanäle.

**Diskretes Logarithmusproblem:** Es ist einfacher  $g^x$  zu berechnen, als  $x = \log_g g^x$ .

**Diffie-Hellman Problem:** Aus  $g^x$  und  $g^y$  lässt sich nicht  $g^{xy}$  berechnen.



Aus  $g^{xy}$  werden dann symmetrische Schlüssel (Authentisierung und Verschlüsselung) abgeleitet.

# PACE

- Ziele:**
- PIN-Eingabe
  - Aufbau einer verschlüsselten Verbindung zwischen Chip und Lesegerät



---

PIN-Eingabe

---

Verschlüsselter Diffie-Hellman-Schlüsselaustausch

---

# PACE

- Ziele:**
- PIN-Eingabe
  - Aufbau einer verschlüsselten Verbindung zwischen Chip und Lesegerät



PIN-Eingabe

Wähle Zufallswert  $r$

$\xrightarrow{\text{ENC}_{\text{PIN}}(r)}$

Entschlüssel  $r$

Beide berechnen aus  $r$  einen Diffie-Hellman Basispunkt  $g$

$\xleftarrow{g^y}$

Wähle Zufallswert  $y$

Wähle Zufallswert  $x$

$\xrightarrow{g^x}$

Berechne  $(g^y)^x = g^{xy}$

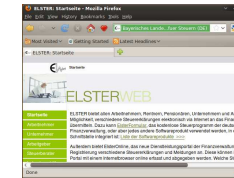
Berechne  $(g^x)^y = g^{xy}$

# Terminal- und Chipauthentisierung

- Ziele:**
- Gegenseitige Authentisierung
  - Aufbau einer verschlüsselten Verbindung zwischen Chip und Diensteanbieter



$x, g^x, C_{g^x}$



$sk_T, pk_T, C_{pk_T}$

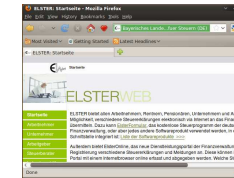
---

Authentisierter Diffie-Hellman-Schlüsselaustausch

---

# Terminal- und Chipauthentisierung

- Ziele:**
- Gegenseitige Authentisierung
  - Aufbau einer verschlüsselten Verbindung zwischen Chip und Diensteanbieter



$x, g^x, C_{g^x}$

$sk_T, pk_T, C_{pk_T}$

Prüfe  $C_{pk_T}$  und  $s_1$

$\leftarrow g^y, C_{pk_T}, s_1$

Wähle Zufall  $y$ , berechne  $g^y$  und  $s_1 = \text{Sign}(g^y, sk_T)$

Wähle Zufallswert  $r$

$\xrightarrow{r, g^x, C_{pk_T}}$

Prüfe  $g^x$

Prüfe  $s_2$

$\leftarrow s_2$

Berechne  $s_2 = \text{Sign}(r, sk_T)$

Berechne  $(g^y)^x = g^{xy}$

Berechne  $(g^x)^y = g^{xy}$

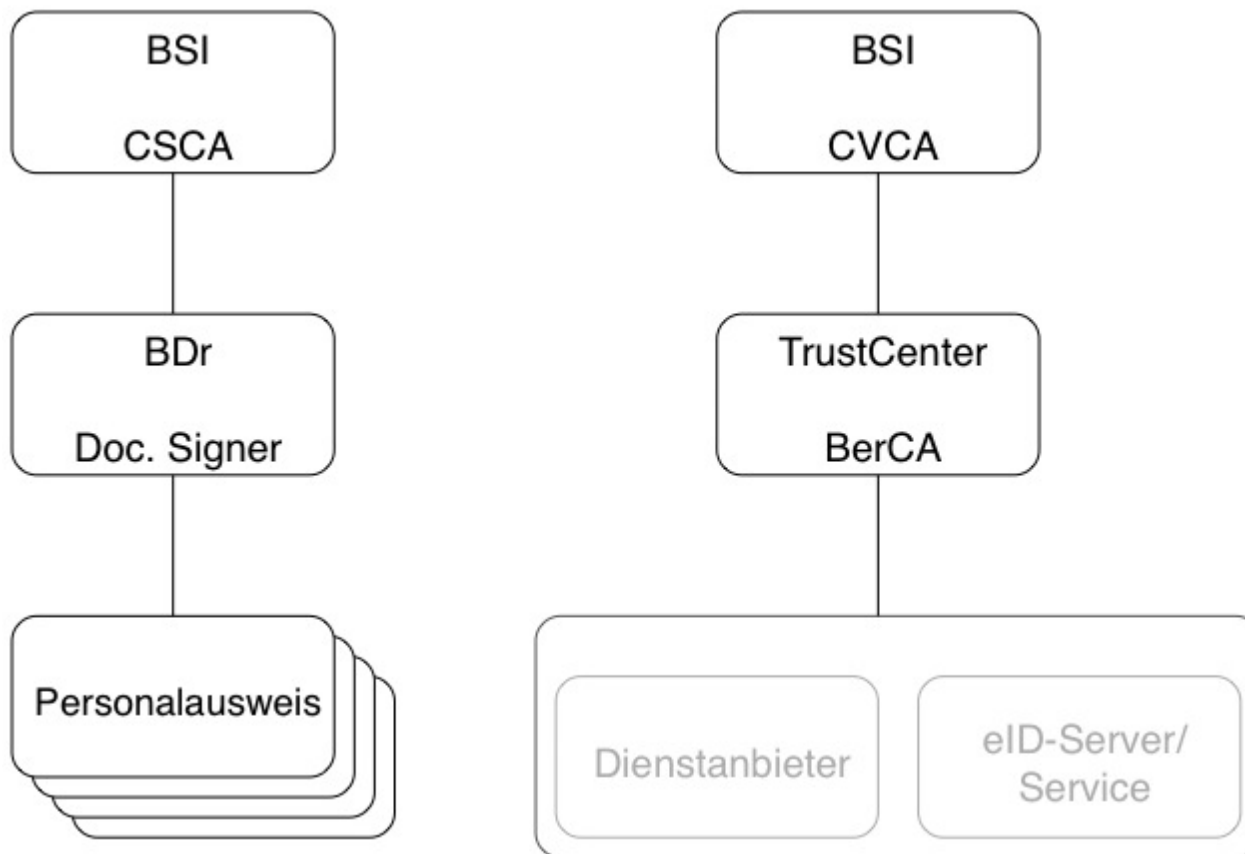


# eID-Server/Service

- eID-Server übernehmen
  - die Kommunikation mit dem Chip des Ausweises
  - die Kommunikation mit Hintergrundsystemen (Berechtigungszertifikate, Sperrlisten)
- Anbindung zwischen eID-Server und Webdienst über Standardprotokolle (SAML, TSL)
- Spezifiziert in Technischen Richtlinien des BSI

Ein eID-Service ist der Betreiber eines mandantenfähigen eID-Servers

# Infrastruktur





# AusweisApp

- **Funktionen:**

- eID-Funktion des ePA
- Signaturfunktion des ePA
- Signatur, Authentisierung und Verschlüsselung weiterer Karten

- **Unterstützte Betriebssysteme:**

- Windows 2000, XP, Vista, 7
- MacOS 10.5 (Intel) und höher
- Linux: Debian 5.0, Ubuntu 9.04, OpenSuse 11.1 und höher

- **Unterstützte Anwendungen:**

- Browser: IE V6, Mozilla Firefox V3, Safari V4 und höher
- E-Mail: MS Outlook V11, MS Outlook Express V6, Mozilla Thunderbird V2, Apple Mail V10.5, kontakt kmail V1.8 und höher



# Diensteanbieter

E-Government	E-Finanzservice	E-Business