

Transparenz und Datensparsamkeit von elektronischen Ausweisdokumenten in Deutschland

Dominik Oepen



Humboldt-Universität zu Berlin
Institut für Informatik, Lehrstuhl für Systemarchitektur
Unter den Linden 6, 10099 Berlin

30. November, 2012

Agenda

Einleitung

Elektronische Ausweisdokumente in Deutschland

Der elektronische Reisepass

Der neue Personalausweis

Der elektronische Aufenthaltstitel

Transparenz und Privatsphäre

Fazit

Elektronische Ausweisdokumente



- ▶ Standardisierung durch die International Civil Aviation Organisation (ICAO)
- ▶ Tochterorganisation der UNO
- ▶ ICAO DOC 9303: Machine Readable Travel Documents
- ▶ Mai 2003: Beschluss zur Einführung von RFID Chips und biometrischer Merkmale
 - ▶ Digitales Gesichtsbild
 - ▶ Optional zwei Fingerabdrücke, Irisscan
- ▶ Über 100 Länder, über 300 Millionen ausgegebene Ausweisdokumente

- ▶ ISO 14443
- ▶ Reichweite laut Spezifikation: 5-10 cm
- ▶ Aktives Ansprechen:
 - ▶ 40 cm in Simulation und Modellierung
 - ▶ 25 cm in Praxis
- ▶ Passives Abhören: Mehrere Meter

Elektronische Ausweisdokumente in Deutschland

- ▶ März 2005: eCard Strategie des Bundes
- ▶ Nov. 2005: ePass mit Funkchip
- ▶ Nov. 2007: Erweiterung um Fingerabdrücke
- ▶ Nov. 2010: Einführung neuer Personalausweis
- ▶ Sept. 2011: Einführung elektronischer Aufenthaltstitel

Der elektronische Reisepass



Datengruppe	Inhalt
EF.COM	Inhaltsverzeichnis
EF.SOD	Signierte Hashes der Datengruppen
DG1	MRZ
DG2	Biometrisches Gesichtsbild
DG3	Fingerabdrücke

Datengruppen eID

Datengruppe	Inhalt
DG1	Dokumenttyp
DG2	Ausgebender Staat
DG3	Ablaufdatum
DG4	Vorname(n)
DG5	Familienname
DG6	Ordensname/Künstlernamen
DG7	Doktorgrad
DG8	Geburtsdatum
DG9	Geburtsort
DG13	Geburtsname
DG17	Adresse
DG18	Wohnort ID

eID - Spezielle Funktionen

- ▶ Restricted Identification:
 - ▶ Dienstanbieterspezifisches Pseudonym
 - ▶ Soll dienstübergreifendes Tracking verhindern
- ▶ Altersverifikation:
 - ▶ Ist der Ausweisinhaber alt genug um einen Dienst zu nutzen?
- ▶ Wohnort ID:
 - ▶ Wohnt der Ausweisinhaber in einem bestimmten Gebiet?

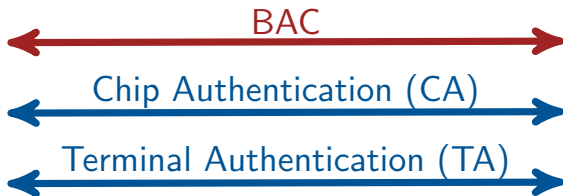
Extended Access Control (Version 1)



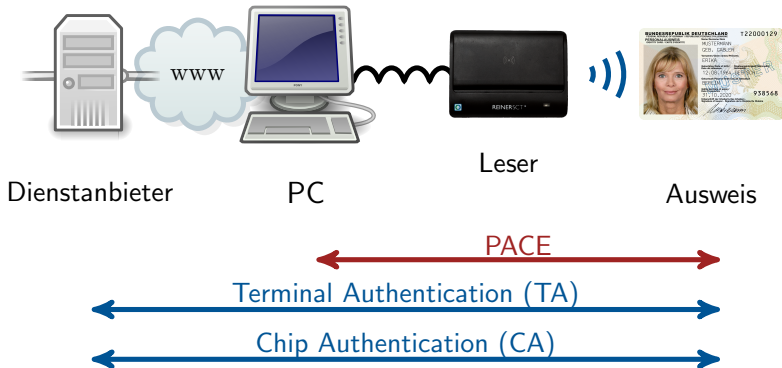
Terminal



ePass



Extended Access Control (Version 2)



Extended Access Control (Version 2)

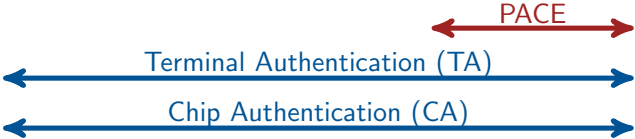


Dienstanbieter

PC

Leser

Ausweis



EAC 1 vs EAC 2

- ▶ BAC: Geringere Entropie der Sitzungsschlüssel, kein Sicherheitsbeweis

EAC 1 vs EAC 2

- ▶ BAC: Geringere Entropie der Sitzungsschlüssel, kein Sicherheitsbeweis
- ▶ CA vor TA ermöglicht Tracking ohne Zertifikat

EAC 1 vs EAC 2

- ▶ BAC: Geringere Entropie der Sitzungsschlüssel, kein Sicherheitsbeweis
- ▶ CA vor TA ermöglicht Tracking ohne Zertifikat
- ▶ Reisepass und eAT: Auslesen der ePass Daten teilweise nach BAC
- ▶ nPA: Auslesen von Daten erst nach kompletter EAC

Terminal Authentication

Identitätsnachweis – Anbieterinformationen

Anbieterinformationen

Angefragte Daten

PIN-Eingabe

Übermittlung

Angaben des Anbieters

Name des Diensteanbieters:
Innenministerium Baden-Württemberg

Internetadresse des Diensteanbieters:
<https://www.service-bw.de/cp-web-portal/>

Angaben des Diensteanbieters:
Name, Anschrift und E-Mail-Adresse des Diensteanbieters:
Innenministerium Baden-Württemberg
Postfach 10 24 43
70020 Stuttgart
poststelle@im.bwl.de

Geschäftszweck:
- Registrierung / Login "mein service-bw" -

zuständige Datenschutzbehörde:

Bildschirmtastatur

Zurück Weiter Abbrechen

- ▶ Anzeige von Diensteanbieterinformationen
- ▶ Abwahl von Berechtigungen

Terminal Authentication

The screenshot shows a window titled "Identitätsnachweis – Angefragte Daten". On the left is a sidebar with menu items: "Anbieterinformationen", "Angefragte Daten", "PIN-Eingabe", and "Übermittlung". The main area is titled "Angefragte Daten" and contains the following text: "Für den genannten Zweck bitten wir Sie, die folgenden Daten aus Ihrem Personalausweis zu übermitteln." Below this is a list of data fields with checkboxes:

<input checked="" type="checkbox"/> Vorname(n)	<input type="checkbox"/> Ordens- oder Künstlername
<input checked="" type="checkbox"/> Name	<input type="checkbox"/> Ausweistyp
<input type="checkbox"/> Doktorgrad	<input type="checkbox"/> Ausstellendes Land
<input type="checkbox"/> Anschrift	<input type="checkbox"/> Wohnortbestätigung
<input type="checkbox"/> Geburtsdatum	<input type="checkbox"/> Altersverifikation
<input type="checkbox"/> Geburtsort	<input checked="" type="checkbox"/> Pseudonym / Kartenkennung

Below the list is a note: "Wenn Sie mit der Übermittlung der ausgewählten Daten einverstanden sind, geben Sie bitte Ihre 6-stellige Personalausweis-PIN ein." and a text input field labeled "Personalausweis-PIN". At the bottom of the window are four buttons: "Bildschirmtastatur", "Zurück", "Weiter", and "Abbrechen".

- ▶ Anzeige von Dienstanbieterinformationen
- ▶ Abwahl von Berechtigungen

Chip Authentication

Verwendung von Gruppenschlüsseln:

- ▶ CA Schlüssel nicht chipindividuell
- ▶ Ein CA Schlüssel pro Charge

Chip Authentication

Verwendung von Gruppenschlüsseln:

- ▶ CA Schlüssel nicht chipindividuell
- ▶ Ein CA Schlüssel pro Charge
- ▶ Brechen eines Schlüssel ermöglicht Emulation beliebiger Ausweise
- ▶ Reaktion: EF.ChipSecurity

Open Source Implementierungen

- ▶ Mittlerweile viele Projekte
- ▶ Auch von/in Zusammenarbeit mit offiziellen Stellen

Open Source Implementierungen

- ▶ Mittlerweile viele Projekte
- ▶ Auch von/in Zusammenarbeit mit offiziellen Stellen
- ▶ Grenzen von Transparenz durch OSS
- ▶ Nur eID
- ▶ Karte und Terminals sind weiterhin Blackbox
- ▶ Ende-zu-Ende Verschlüsselung nach CA

Fazit

- ▶ Verschiedene Mechanismen um Transparenz und Datensparsamkeit zu gewährleisten
 - ▶ Vor allem für eID
 - ▶ Weniger für ePass
- ▶ Schwierigkeit Fälschungssicherheit und Datensparsamkeit zu vereinbaren
- ▶ Verbesserung der kryptografischen Protokolle
- ▶ Oft problematisch auf Grund von Rückwärtskompatibilität
- ▶ Anstrengungen zur internationalen Standardisierung