Technik des neuen elektronischen Personalausweises

Henryk Plötz
ploetz@informatik.hu-berlin.de

29. Dezember 2009

Einleitung

- Neuer elektronischer Personalausweis ab 1. November 2010
- Soll bisherige, hauptsächlich hoheitliche, Funktionen um erweiterte Funktionalitäten im privatwirschaftlichen und elektronischen Bereich ergänzen
- Plastekarte mit RFID-Chip (ISO 14443)

Kartenformat

- Zwei Optionen:
  - Altes Format ID-2: groß, großes Bild (gut für Sichtkontrolle), passt in keinen kontaktbasierten Leser → Muss mit RFID
  - „Kreditkartenformat“ ID-1: klein, kleineres Bild, passt in Standard-Smartcardleser → kann auch kontaktbasiert
- Wahl gefallen auf ID-1 mit kontaktloser Schnittstelle
  - Sieht aus wie die Kombination der Nachteile der beiden Alternativen
  - Immerhin: kontaktlose Schnittstelle ermöglicht flexible Leserformate (z.B. USB-Stick)

Begriffe

CVCA	Country Verifying CA, Root-CA beim BSI
DV	Document Verifier, bei einem Trustcenter angesiedelt
Terminal	Dienst oder lokales Lesegerät (für elektronische Signatur oder hoheitliche Identitätskontrolle)
$SK_{\dots}$	Privater Schlüssel
$PK_{\dots}$	Öffentlicher Schlüssel
$D_{\dots}$	Domain-Parameter
$\widetilde{\dots}$	Ephemerale Parameter
KA	Schlüsselaushandlungsfunktion

Funktionalitäten

- Sichtprüfung
- elektronische Identitätskontrolle im hoheitlichen Bereich (ähnlich ePass, nicht im Fokus hier)
- elektronische Identitätskontrolle im nichthoheitlichen Bereich (eID)
- Sonderfunktionen:
  - Altersverifikation
  - Restricted Identification (aka Sektoridentifikation)
- Sicherheitsmedium für die qualifizierte elektronische Signatur (QES)

Bindung an den Ausweisinhaber

- im hoheitlichen Bereich: Inhaberbindung durch Sichtkontrolle (vergleich mit dem aufgedruckten Bild)
  - Alternativ: Biometrie: Gesichtsbild und Fingerabdrücke (optional)
  - Biometrie hat keine Verbindung zum nichthoheitlichen Teil
- im nichthoheitlichen Bereich/Internet: Inhaber-PIN

Elektronischer Identitätsnachweis

- Ausweis enthält mehrere Felder (Name, Vorname, Adresse, Stadt, etc.) die einzeln freigegeben werden können
- Dienst authentifiziert sich mit Anbieterzertifikat, darin enthalten sind die Felder die dieser Dienst auslesen kann (verwaltet vom Bundesverwaltungsamt)
- Ausweis authentifiziert sich mit Chip-Authentication-Zertifikat
- Ausweisinhaber authorisiert Datenfreigabe mit PIN

eID (fortg.)

- Datenfelder im eID-Bereich sind nicht signiert
  - Reduziert Wert der Daten für Addresshandel
  - Erleichtert Änderungen (kein Zugang zu einem Document Signer nötig)
  - Authentizität implizit gesichert durch den sicheren Kanal
- Daten können in jedem Bürgeramt geändert werden
- eID-Funktion kann deaktiviert werden (deaktiviert die PIN)

eID-Datenfelder (Ausschnitt)

Datengruppe	Inhalt
1	Dokumenttyp
2	Ausstellender Staat
3	Ungültigkeitsdatum
4	Vorname
5	Nachname
6	Künstler/Ordensname
7	Titel
8	Geburtsdatum
9	Geburtsort
10	Nationalität
11	Geschlecht
12	Optionale Daten
17	Wohnort

Altersverifikation

- Wenn der Dienst berechtigt ist, kann pro PIN-Eingabe eine Altersverifikation stattfinden
- Dienst sendet an Ausweis ein Datum, kriegt binäre Antwort „Geburtsdatum liegt nach Datum“ oder nicht

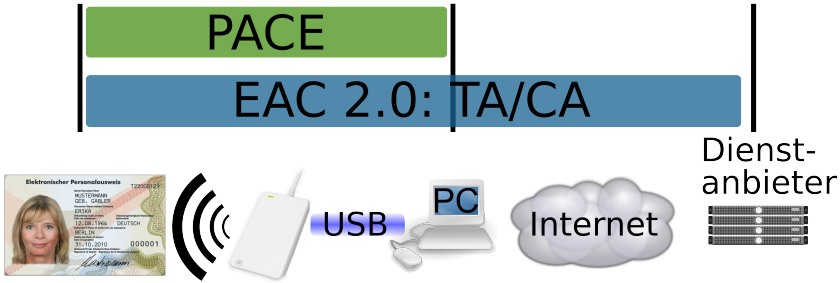
Restricted Identification

- Pseudonyme Identifikation pro Anbieter („Sektor“)
- Ausweis generiert ein Pseudonym, spezifisch für das Paar Ausweis–Anbieter
  - Verschiedene Dienstanbieter können nicht kooperativ ihre Datenbasen zusammenlegen
- Dient zur Wiedererkennung, „Login merken“ etc.

PIN-Verwaltung

- PIN kann aktiviert oder deaktiviert sein (kann im Bürgeramt umgeschaltet werden)
- PIN mit Fehlbedienungszähler
  - Vor dem letzten Versuch wird die PIN suspended
  - Unsuspend mit CAN
  - Wenn Fehlbedienungszähler=0: Zähler zurücksetzen mit PUK
- PIN kann geändert werden:
  - Mit PIN
  - Mit Berechtigungszertifikat

Protokollablauf aus der Vogelperspektive



Password Authenticated Connection Establishment (PACE)

- Setzt Schlüssel für Secure Messaging auf, zwischen Lesegerät und Karte
- Kann ein Geheimnis verifizieren ohne es zu übertragen
- Mögliche Geheimnisse:

PIN	Persönliche Identifikationsnummer für eID-Anwendung
CAN	„Karten-PIN‘, aufgedruckt, nur für hoheitliche Anwendung
MRZ	Machine Readable Zone, nur ePass-Anwendung
PUK	PIN Unblocking Key, setzt den PIN-Fehlerzähler zurück

PACE, fortg.

- Kann mit ECC und diversen symmetrischen Chiffren eingesetzt werden
- Designt, um Patent-frei zu sein
  - Alternative, ähnliche Protokolle (SPEKE, EKE, etc.) sind in der Regel patentiert
- Formaler Sicherheitsbeweis auf ISC09 vorgestellt

PACE-Protokoll

Karte		Lesegerät
	Geteiltes Geheimnis π	
Zufällige Nonce s $z := \mathrm{Enc}_\pi(s)$	$\xrightarrow{z, D_{PICC}}$	
		$s := \mathrm{Dec}_\pi(z)$
$\widetilde{D} := \mathbf{Map}(D_{PICC}, s)$		$\widetilde{D} := \mathbf{Map}(D_{PICC}, s)$
zufällige Schlüssel: $\widetilde{SK_{PICC}}, \widetilde{PK_{PICC}}, \widetilde{D}$		zufällige Schlüssel: $\widetilde{SK_{PCD}}, \widetilde{PK_{PCD}}, \widetilde{D}$
	$\xleftrightarrow{\widetilde{PK_{PICC}}, \widetilde{PK_{PCD}}}$	
$K := \mathbf{KA}(\widetilde{SK_{PICC}}, \widetilde{PK_{PCD}}, \widetilde{D})$		$K := \mathbf{KA}(\widetilde{SK_{PCD}}, \widetilde{PK_{PICC}}, \widetilde{D})$
	$\xleftarrow{T_{PCD}}$	$T_{PCD} = \mathbf{MAC}(K_{MAC}, \widetilde{PK_{PICC}})$
$T_{PICC} = \mathbf{MAC}(K_{MAC}, \widetilde{PK_{PCD}})$	$\xrightarrow{T_{PICC}}$	

TA/CA

- Gegenseitige Authentisierung von Personalausweis und „Terminal“ (Dienst)
- Dienst authentifiziert sich zuerst (Terminal Authentication, TA), mit Anbieterzertifikat und Zertifikatskette
  - Zertifikat enthält Terminaltyp und Berechtigungen
  - Für hoheitliche Terminals wird ggbf. der interne Vertrauensanker aktualisiert
  - Für hoheitliche Zertifikat wird die interne Datumsannäherung aktualisiert
- Personalsausweis authentifiziert sich mit CA (Chip Authentication)
  - CA-Zertifikat/Schlüssel wird zwischen mehreren Ausweisen geteilt (größeres Anonymity Set)
- TA/CA-Vorgang generiert neue Sitzungsschlüssel

TA-Protokoll

Karte	Terminal
	Ephemeralschlüsselpaar: $(\widetilde{SK_{PCD}}, \widetilde{PK_{PCD}}, D_{PICC})$
Wähle r_{PICC}	
	$\xrightarrow[\text{Übertrage } r_{PICC}]{}$
	$s_{PCD} := \mathbf{Sign}(SK_{PCD}, ID_{PICC} \parallel r_{PICC} \parallel \mathbf{Comp}(\widetilde{PK_{PCD}}))$
	$\xleftarrow[\text{Übertrage } s_{PCD}]{}$
$\mathbf{Verify}(\widetilde{PK_{PCD}}, s_{PCD}, ID_{PICC} \parallel r_{PICC} \parallel \mathbf{Comp}(\widetilde{PK_{PCD}}))$	

CA-Protokoll

Karte | Terminal

CA-Schlüsselpaar:
$(SK_{PICC}, PK_{PICC}, D_{PICC})$

$$\xrightarrow{\text{Übertrage } PK_{PICC}, D_{PICC}}$$

$$\xleftarrow{\text{Übertrage } \widetilde{PK_{PCD}}}$$

$K := \mathbf{KA}(SK_{PICC}, \widetilde{PK_{PCD}}, D_{PICC})$ $\quad$ $K := \mathbf{KA}(\widetilde{SK_{PCD}}, PK_{PICC}, D_{PICC})$

$T_{PICC} = \mathbf{MAC}(K_{MAC}, \widetilde{PK_{PCD}})$

$$\xrightarrow{\text{Übertrage } T_{PICC}}$$

Restricted Identification

- Diffie-Hellman-Key-Agreement, generiert sektor-spezifischen Identifikator

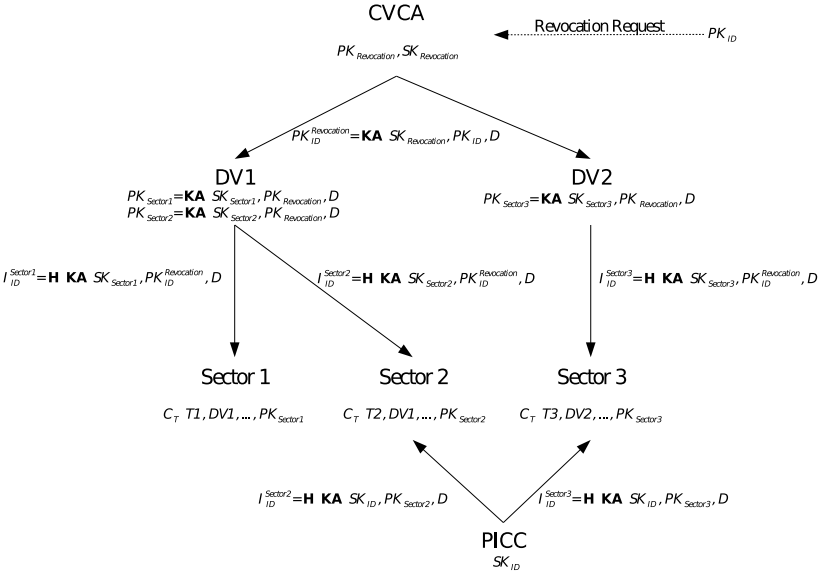
rID-Protokoll

Karte		Terminal
Chip-Identifier: PK_{ID}		Sektor-Schlüssel: (PK_{Sector}, D)
	$\xleftarrow{PK_{Sector}, D}$	
$I_{ID}^{Sector} := \mathbf{H}(\mathbf{KA}(SK_{ID}, PK_{Sector}, D))$		
	$\xrightarrow{\text{Übertrage } I_{ID}^{Sector}}$	

Revocation

- Sektor-spezifische Revocation-Identifier werden als schwarze Liste an die Terminal-Betreiber übergeben
- Ausweis kann auf Anfrage den eigenen sektor-spezifischen Identifier generieren und an das Terminal weiterleiten
- Wenn der Identifier auf der schwarzen Liste ist, ist der Ausweis gesperrt

Revocation-Protokoll



Unerwünschte Nebenwirkungen

- Keine anonyme Benutzung der eID-Funktion
- eID-PIN mächtiger als QES-PIN
- Bruch des Chip-Authentication-Schlüssels ermöglicht Emulation beliebiger Personalausweise

Keine anonyme Benutzung der eID-Funktion

- Revocation und rID sind identisch
- rID kann im Berechtigungszertifikat deaktiviert werden
- Beispiel Porno-Anbieter: Obwohl nur Altersverifikation nötig ist, muss rID erlaubt sein (sonst keine Revocation-Prüfung)

eID-PIN mächtiger als QES-PIN

- Kann mit eID-PIN die QES-Anwendung initialisieren und ein Zertifikat beantragen
- Wird evt. einige Benutzer überraschen, da sonst eID-PIN ‚nur' „Daten freigeben" ist und QES-PIN signieren ist, was ‚mehr' erscheint

Große Angriffsfläche: CA-Schlüssel

- Keine Signatur auf den Datenfeldern, keine Bindung von CA-Schlüssel an Name, Adresse, etc.
- Revocation-Protokoll ineffektiv bei vollständig emuliertem Ausweis
- Kein definiertes Revocation-Protokoll für CA-Schlüssel
  - Vollständiges Zurückziehen eines veröffentlichten CA-Schlüssels unpraktikabel, da sehr viele Ausweise betroffen
- Angriff aufwendig/teuer (ca. 100kUSD-200kUSD)[a]
  - Aber: Sehr großer Nutzen: Beliebige Ausweisdaten fälschen, QES-Zertifikate auf falschen Namen beantragen

[a] Schätzung: Karsten Nohl

Ende

?|!