

Der neue Personalausweis

Technik, Fakten, Hintergründe

Referent: Christian Kahlo,
AGETO Service GmbH

AGETO Service GmbH

eCommerce

ERP

eGovernment

IT-Security / R&D



AGETO Service GmbH

- Im Jahr 2003 gegründet
- Derzeit 60 Mitarbeiter – Tendenz steigend
- Erfahrung aus über 150 Internetprojekten
- Integrator für eCommerce- und eGovernment-Systeme
- Individuelle Lösungen durch Eigenentwicklungen
- nPA-Anwendungsberatung und technische Integration
- Sicherheitsberatung und Machbarkeitsanalysen
- Erstellung von Technologiekonzepten für den neuen Personalausweis
- Initiierung von Ausweis-Portal.de





Alles aus einer Hand Wir bringen den Neuen Ausweis in die Anwendung

Alles aus einer Hand heißt, dass alle Partner von Ausweis-Portal.de miteinander kooperieren. Hier finden Sie den richtigen Ansprechpartner aus jedem Bereich rund um den Neuen Personalausweis. Sie können die Leistungen einzeln oder im Paket anfragen. Jedes Unternehmen steht Ihnen mit einem Ansprechpartner zur Verfügung.

Wir bringen den Neuen Personalausweis in die Anwendung.

Ausweis-Portal.de - Ist eine privatwirtschaftliche Initiative und ein Rundum-Service, der Ihnen bei allen Wünschen im Hinblick auf die Nutzung des Neuen Personalausweises qualifiziert zur Seite steht, für öffentliche und für private Onlineanwendungen.



Zur Person

Christian Kahlo

Research Manager IT-Security

Experte für

- IT-Sicherheit [> 10 Jahre Berufserfahrung]
- Kryptographie
- e-Identity, Single-Sign-On Themen seit ~ 2000
- System-Architekturen
- J2EE-Entwicklung
- Softwareentwicklung und Entwicklungsprozesse
- Aus Jena, deshalb heute hier in Jena



Zum Thema

- Neuer Personalausweis
- Am 01.11.2010 eingeführt durch Inkrafttreten des Gesetzes und der zugehörigen Verordnung
- Beleuchtung der technischen Abläufe und Hintergründe
- Fragen und Antworten im Anschluss

Aktuelle Berichterstattung

- „PIN-Hack“ mit Basisleser
- 9t-Klässler frittieren den Chip mit Blitzlicht-Elko
- Lücke im Update-Client der AusweisApp

Was ist drin im neuen Ausweis?

- Karte im ID-1 Format („Scheckkartenformat“)
- RFID-Chip mit ISO-14443 Interface
- Card-OS von T-Systems (TCOS-Basis)
- Leistungsstarke Crypto-Unit
- hoheitliche Identifikation, e-ID, Signaturkarte

Was ist dran am neuen Ausweis?

- RFID-Leser (Basis, Standard, Komfort)
- AusweisApp
- E-ID Server
- Berechtigungszertifikate
- Berechtigungs-CA (BerCA)

Zuständige Richtlinien

- BSI TR-03110 (v2.05 2010-10-14, EAC)
- BSI TR-03112 (v1.1 2009-07-15, e-Card API)
- BSI TR-03127 (v1.12 2010-09-17, nPA)
- BSI TR-03130 (v1.4.1 2010-10-08, e-ID Server)
- BSI TR-03128 (v1.02 2010-07-13, EAC-PKI)
- CEN 15480 (ECC – European Citizen Card)
- ISO 7816 (Kommandostrukturen)
- ISO 14443 (RFID-Kommunikation)
- ISO 24727 (ref. e-Card API)

Anwendungsszenario

- Kunde clickt auf Webseite „Login“ oder „Registrieren“
- Dienstanbieter (Webseite) öffnet Session am e-ID Server
- HTML object wird ausgeliefert, AusweisApp wird getriggert
- AusweisApp baut über TLS-RSA-PSK einen PAOS-Kanal zum e-ID Server auf
- Berechtigungszertifikat und angefragte Daten (Certificate Holder Authorization Template, CHAT) werden übertragen
- Terminal- und Chip-Authentication werden durchgeführt
- Verschlüsselter Kanal zwischen nPA Chip und e-ID Server wird aufgebaut
- Daten werden vom nPA an den e-ID Server übertragen
- e-ID Server überträgt Daten an den Dienstanbieter



Protokolle

- SAML
- ISO SM
- PACE
- TLS-RSA-PSK
- PAOS
- EAC-Authentication (Terminal, Chip)

Anwendungsrisiken (1)

- Trojaner jeglicher Art, → Modulabsicherung
- „halb“-gefälschte Clients, → Umgehung der SSL-Verschränkung
- freie Clients, unter unsachgemässer Verwendung (keine SSL-Verschränkung, keine Sicherung gegen Modifikationen, keine strikte Beachtung von Card-Holder-Authorization-Templates)
- Datenlecks bei Diensteanbietern
- „gefälschter“ e-ID Server kein Problem, da durch SSL-Verschränkung gesichert

Übersicht Kartenlesegeräte

- Basis-Lesegerät
Reiner SCT, SCM, Gemalto, u.a.
- Standard-Lesegerät
Reiner SCT, weitere geplant
- Komfort-Lesegerät
Reiner SCT

PACE Funktion

- Anwendung teilt nPA Authentisierungsmerkmal mit
- nPA kennt Referenzwert, leitet Schlüssel ab, bildet eine Nonce, verschlüsselt die Nonce und sendet das Ergebnis
- Anwendung fragt CAN oder PIN ab bzw. wertet MRZ aus, bildet Schlüssel und entschlüsselt Nonce „s“
- Temporäre Schlüssel werden gebildet, ECDH-KA ausgeführt, Einigung aus Punkt H
- neuer Basispunkt (Map-Funktion) : $G' = s * G + H$
- erneut ECDH-KA, gemeinsamer Punkt S, x-Achse ist shared secret
- Übermittlung von Authentication Token in SM-Kanal zur Bestätigung

Kryptografische Basis

- Elliptic Curves
- Im Anwendungstest proprietäre Definition auf dem nPA, brainpool 256t1
- In den finalen Karten implizite Definition (TR-03110) brainpool 256r1
- Definition proprietärer Kurven weiterhin möglich
- BerCAs verwenden eigene Kurven / Basispunkte
- Häufigster Mechanismus: ECDH-KA
Elliptic Curve Diffie Hellman Key Agreement
- $Pp, Qq \rightarrow pQ = qP$

Berechnung RID

- RID = Restricted Identifier = Pseudonym = Sektorspezifische Kennung = Dienste-und-Karten-spezifisches-Mermal (BVA-Sprech)
- Errechnung aus Sektorschlüssel des Berechtigungszertifikates und privatem RID-Schlüssel auf nPA
- ECDH-KA + SHA-256
- Wird ausschliesslich vom nPA berechnet und im SM-Kanal an e-ID Server geliefert

Gespeicherte Informationen

- Datengruppen aus EAC-Spec
Vornamen, Nachnamen, PlaceOfResidence,
Geburtsdatum, Geburtsort, etc.
- CAN, PIN und MRZ als Referenzwerte
- Schlüsselpaare für RID und Sperrmerkmal
- Trust-Anchor für DVCA

Fragen & Antworten

Christian Kahlo

AGETO Service GmbH

<http://www.agero.net>

c.kahlo@agero.net