Der neue Personalausweis

Vortrag am 29.09.2015

Reinhard Mutz

EIDAS - NPA

Der neue Personalausweis

Technik

Chancen

Risiken

NPA – die Technik

Allgemeines

- Der neue Personalausweis enthält einen intelligenten Chip
- Der Chip kann per RFID ausgelesen werden
- Der Chip beherrscht Kryptografie
- Der Chip ist gegen unbefugtes Auslesen gesichert
- Die Seriennummer wird zufällig erzeugt und ändert sich mit jeder Abfrage

NPA – die Technik

- Der Chip ist durch eine User Pin gesichert
- Die User Pin ist nur dem User bekannt
- Der User kann einen Lesevorgang jederzeit abbrechen
- Technische Spezifikation aller elektronischen Ausweise unter https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/elektronischeausweise_node.html

NPA – die Technik

Lesegeräte

- Lesegeräte mit RFID / ISO-14443 sind inzwischen breit verfügbar
- Lesegeräte müssen vom BSI für das Auslesen des NPA zertifiziert werden

Autsch! Der Basisleser bietet nicht die versprochene Sicherheit, da der Hostrechner an der Eingabe der Userpin beteiligt ist!

NPA – das Marktmodell

- 3 Parteien, alle voneinander unabhängig, sind nötig, um die Daten auf dem Chip auslesen zu können
- Der Ausweisinhaber
- Ein Serviceprovider
- Ein Mandant

NPA – das Marktmodell

Ablauf eines Lesevorgangs

- Der Ausweisinhaber besucht eine Webseite
- Er stimmt zu, sich mit dem NPA zu identifizieren
- Er sieht die Datengruppe, die ausgelesen werden soll
- JETZT muss er zustimmen oder abbrechen
- Bei Abbruch erfolgt keine neue Abfrage – die Session wird beendet

NPA – das Marktmodell

Die Rolle als Ausweisinhaber

- Beantragt die Ausstellung des Ausweises
- Liefert alle Daten, die auf den Ausweis aufgebracht werden, siehe https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/Personalausweis/personalausweis_node.html
- Die Bundesdruckerei fertigt den Ausweis
- Die Behörde liefert den Ausweis
- Die Behörde liefert das initiale User Passwort

NPA – das Marktmodell

Die Rolle als Mandant

- Ein Mandant liest die Daten vom Ausweis aus
- Der Mandant benötigt ein Berechtigungszertifikat
- Die Behörde – Vergabestelle für Berechtigungszertifikate – prüft Antrag und Interesse für Datengruppen
- Der Mandant schliesst einen Vertrag mit einem Serviceprovider

NPA – das Marktmodell

Die Rolle als Serviceprovider

- Der SP betreibt ein Servicecenter
- Die Hardware wird vom BSI zertifiziert
- Der SP schliesst einen Vertrag mit einem Mandanten
- Das Berechtigungszertifikat definiert die Rechte zum Auslesen von Gruppendaten
- Der eID-Server ist wie eine Blackbox
- Der SP sieht die ausgelesenen Daten nicht

NPA – das Marktmodell

- BSI – Bundesamt für Sicherheit in der Informationstechnik – zeichnet verantwortlich für
  - Design, Spezifikation und Zertifizierung der Hardware
- Die Behörde – unterschiedliche Ämter – sind verantwortlich für
  - Ausstellung des Ausweises
  - Ausstellung der Berechtigungszertifikate

EID-Client Applikationen

Es gibt mittlerweile mehrere Versuche, den neuen Personalausweis in der Praxis auch einsetzen zu können.

Zunächst wurde ein Browserinterface entwickelt.

Die Entwickler hatten nicht bedacht, dass die Zeit der 32bit PC soeben abläuft.

Mittlerweile gibt es eine Applikation, die als Library konzipiert wurde und zur Entwicklung eigener eID-Clients zur Verfügung steht.

NPA - Datenschutz

- Anbieter mit gültigem Berechtigungszertifikat
- Daten werden nur nach Zustimmung verschlüsselt übertragen
- Zertifiziertes Kartenlesegerät erforderlich
- Auslesen „aus der Ferne“ nicht möglich

NPA - Chancen

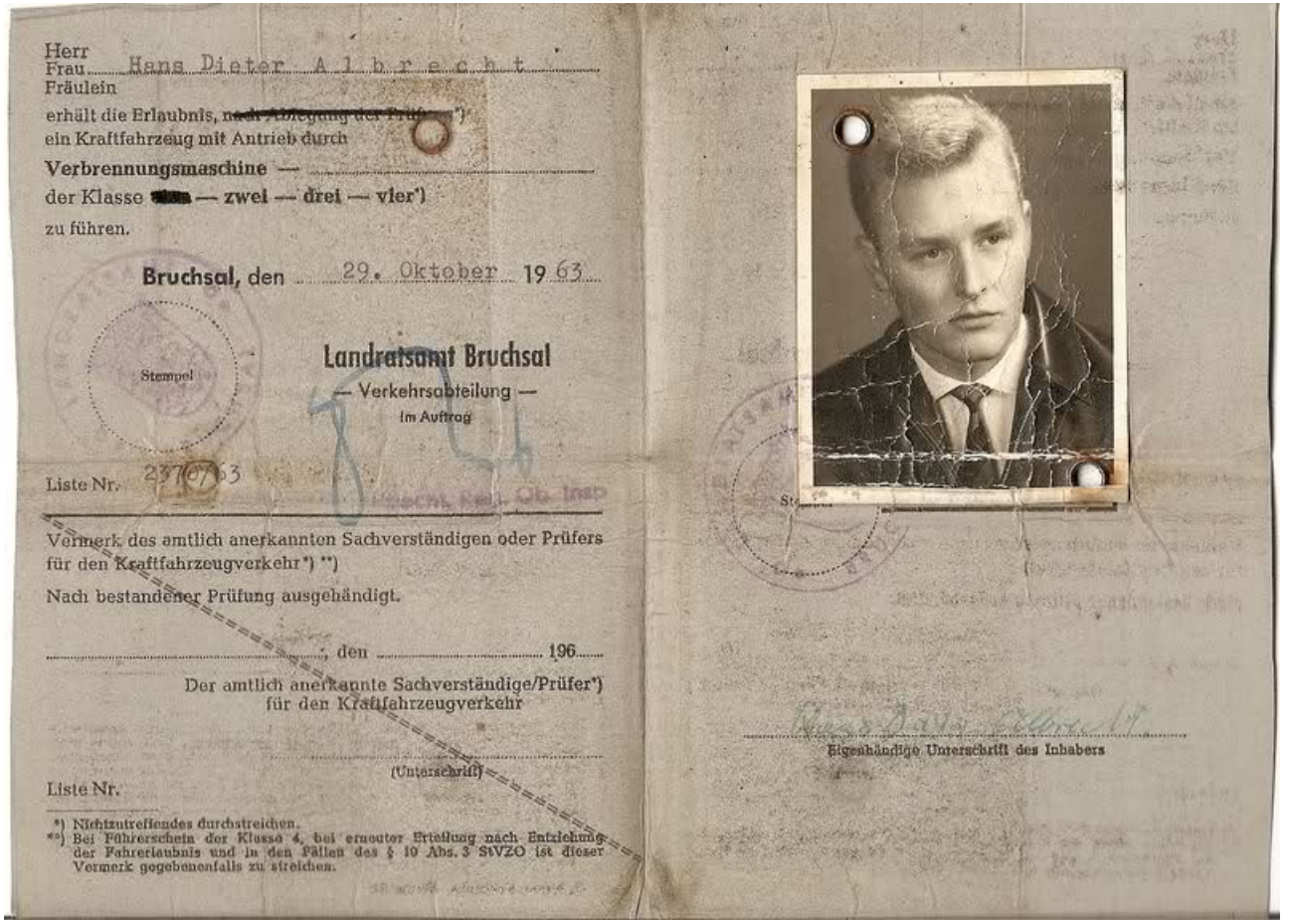
- Sichere Architektur
- Keine Signaturkarte wie in Österreich und den baltischen Staaten
- Sichere Identifizierung im Internet
- Ab 2020 europaweit verfügbar?
- EIDAS – everything here http://ec.europa.eu/digital-agenda/en/trust-services-and-eid

NPA – Risiken?

Auf dem Chip ist reichlich Platz! Wofür?

- Genocide Marker?
  Riccardo Genghini verweist auf seiner Homepage in diesem Zusammenhang auf den Judenstern!
- Säuferbalken?

Ein Säuferbalken



Herr
Frau Hans Dieter Albrecht
Fräulein

erhält die Erlaubnis, ~~nach Ablegung der Prüfung~~ *)
ein Kraftfahrzeug mit Antrieb durch
Verbrennungsmaschine —
der Klasse ~~eins~~ — **zwei** — **drei** — **vier***)
zu führen.

Bruchsal, den 29. Oktober 1963

Stempel

Landratsamt Bruchsal
— Verkehrsabteilung —
Im Auftrag

Liste Nr. 2370/63

Vermerk des amtlich anerkannten Sachverständigen oder Prüfers für den Kraftfahrzeugverkehr*) **)

Nach bestandener Prüfung ausgehändigt.

....., den ..... 196.....

Der amtlich anerkannte Sachverständige/Prüfer*)
für den Kraftfahrzeugverkehr

.....
(Unterschrift)

Liste Nr.

*) Nichtzutreffendes durchstreichen.
**) Bei Führerschein der Klasse 4, bei erneuter Erteilung nach Entziehung der Fahrerlaubnis und in den Fällen des § 10 Abs. 3 StVZO ist dieser Vermerk gegebenenfalls zu streichen.

Hans Dieter Albrecht
Eigenhändige Unterschrift des Inhabers

Noch ein Säuferbalken

NPA – versteckte Markierungen?

- Pseudonyme Signaturen?
  Anonyme Identifikation über Pseudonym
- MERA, modular Enhanced Role Authentication
  Authorization Extensions für feinere Rollen von Terminals
- Attribut Provider
  Aufbringen von zusätzlichen Merkmalen,
  z.B. Versichertennummer

NPA – ein Produkt aus dem Innenmisterium

- Erste Ausgabe 2010
- Geheimniskrämerei um die Funktionen auf dem Chip
- Einzelne Technologien gelten als gebrochen z.B RFID, - Fingerabdrücke, wozu?
- Zu viele Fragen – keine guten Antworten
- Bis heute fast keine überzeugenden Anwendungen

Hilft ein NPA Beschleunigungsgesetz?

eIDAS

The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted by the co-legislators on 23 July 2014 is a milestone to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities.

CA DAY Berlin 9.06.2015

- https://www.tuvit.de/en/company/1898.htm

  besonders empfehlenswert:
- Andrea Servida, European Commission

  eIDAS Regulation: State of play
- Riccardo Genghini, Chairman of ETSI ESI
- Implementation of eIDAS through the member s tates Supervisory Bodies

Danke

für die Aufmerksamkeit

Zur Homepage von Riccardo Genghini

http://riccardogenghini.eu

Lesenswert
http://riccardogenghini.eu/digital-agreement/digital-identity-freedom.php