Der neue elektronische Personalausweis

JuSo Kreisverband Heilbronn

Kurt Jaeger, pi@opsec.eu

http://opsec.eu/

Heilbronn, 28. Januar 2011

Übersicht

- CCCS
- Der neue elektronische Personalausweis
- Funktionen
- Wie funktioniert er ?
- Wofür ?
- Was kostet er ?
- Was ging schon schief ?
- Was wird noch schiefgehen ?
- Hinweise
- Diskussion

Vorstellung

- CCCS, Chaos Computer Club Stuttgart e.V.
- Webseite: www.cccs.de
- Dieses Jahr: 10 Jahre alt!
- Bundesweit: Chaos Computer Club
- Geschäftsführer eines regionalen Internet Service Providers

Wie sieht der elektronische Personalausweis aus ?

- Ausweis (ePA)
- eingebauter Funk-Chip
  radio-frequency identification, RFID
- Ausweislesegerät, Reader
- AusweisApp

Funktionen des ePA

- eAusweis: Identitätsnachweis gegenüber Behörden
- Freiwillig: Fingerabdruck-Daten
- Ähnlich wie ePass (seit 11/2005, bzw. seit 11/2007 mit Fingerabdruck)
- eID: Digitaler Identitätsnachweis gegenüber Dritten
- eSign: Digitale Unterschrift gegenüber Dritten
- rechtsverbindliche elektronische Unterschrift (QES)
- Vergleich mit QES mit Kontaktfeld

Wie funktionieren das ?

- Mathematik: Verschlüsselungsverfahren
- Ein Minicomputer mit Speicher im Ausweis
- Kryptografie mit asymmetrischen Schlüsseln: Zertifikate
- Zertifikate-Hierarchien:
  One Ring to rule them all, One Ring to find them,
  One Ring to bring them all and in the darkness bind them
- Für Sicherheit: Beidseitig!
- Zertifizierung (unabhängige Prüfung durch Experten)

Wofür verwendet man das ?

- Sichere Onlinebehördengänge
- Sicheres Online-Shopping

Was kostet es ?

... für NutzerInnen

- eAusweis: 22.80 oder 28.80 EUR
- eID: 6 EUR (falls nachträglich)
- eSign: ???, ca. 70-80 EUR ?

... für Anbieter

- eSign: Ca. 2.5-60 KEUR pro Jahr

Stand der Technik! Haftungsübergang!

Was ging schon schief ?

- Basic Reader: Billig, aber unsicher
- eID freischaltbar ohne PIN
- Rufname und Reihenfolge der Vornamen: Klaus de Maiziere
- Umlaute
- AusweisApp, Update-Mechanismus war unsicher
- Standard/Komfort-Reader: Teuer, 60-160 EUR
- Keine günstige Test-Infrastruktur
- Keine einheitliche Digitale Signatur wg. RFID vrs. Kontaktchip
- Aus-der-Hand-geben verboten (PAuswG)
- EU: eIDs sind nicht portabel -¿ Internet Markt ?
- Leichte Microsoft-Lastigkeit
- Skizzierte Angriffe mit Men-in-the-Middle

Was wird noch schief gehen ?

- Kompromittierung der Schlüssel ?
  Und dann ?
- Trojaner ?

Hinweise

- RFID Schutzhüllen
- Fingerabdruck-Pflicht ?
- Personalausweisgesetz lesen,
  z.B. Störungen und Gültigkeit
- ePA im europäischen Vergleich: Kubicek-Studie
- UK: Löscht derzeit ihre biometric ID database
- Bruce Schneier Blog lesen

Fragen ?

Fragen ? Diskussion!