Herbsttagung CSI, cnlab

Der neue Personalausweis «nPA» (Bundesrepublik Deutschland)

Stephan Verbücheln

Zürich, 5. September 2018

cnlab

Verbreitung elektronische Funktion

- Seit 2010 in allen neuen Personalausweisen
- Seit 2011 in allen Aufenthaltstiteln für Ausländer
- Enthält elektronisch dieselben Daten, die auch aufgedruckt sind
- Kommunikation via NFC (Smartphone-Unterstützung ohne Lesegerät)

optional:

- Schlüsselspeicher für Qualifizierte Elektronische Signaturen (kostet extra)
- Speicher für zwei Fingerabdrücke (freiwillig)

Funktionen

Online-Funktion

- Ausweisen von Name, Adresse, Alter usw.
- Ende-zu-Ende-Krypto zwischen Ausweis und Backend beim Händler
- Händler brauchen Zertifikate, diese definieren Berechtigungen
- Benutzer muss Datensätze mit PIN bestätigen

Hoheitliche Funktion

- Mit Polizei-Zertifikat können Daten ohne Zustimmung ausgelesen werden

Besonderheiten des Protokolls

Feine Definition der Berechtigungen ist möglich

- Händlerzertifikat definiert genau, welche Daten der Händler fragen darf

Interaktives Protokoll

- Die Korrektheit der Daten ist ohne Signatur kryptographisch sichergestellt

Datensparsamkeit

- Beispiel: Altersprüfung, ohne das Geburtsdatum zu verraten

Demos heute

Dienst zum Auslesen der gespeicherten Daten

- Name
- Geburtsdatum
- Adresse

Dienst zum Beglaubigen eines PGP-Schlüssels

- Anbieter signiert PGP-Schlüssel, nachdem man sich authentisiert

Kraftfahrbundesamt

- Auskunftsbrief verlangen (über eigene Daten)

Vielen Dank für Ihre Aufmerksamkeit_

Stephan Verbücheln
sv@cnlab.ch
+41 55 214 33 36

info@cnlab-security.ch
+41 55 214 33 33

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland

cnlab