Microtraining e-Security AGETO

25.03.2014

Neuer Personalausweis (Technik)

- Überblick Protokolle für die Online-Funktion

1. PACE: Nutzer-Legitimierung via PIN
2. EAC: Server-Legitimierung via CVC
3. TA/CA: Ausweis-Legitimierung via DS
4. RID: Berechnung eines Pseudonyms

Neuer Personalausweis - PACE 1/3

Password **A**uthenticated (PIN-Prüfung)
Connection **E**stablishment
(Verschlüsselung)
(BSI TR-03110 & ISO 7816)

- PIN-Übertragung findet nicht statt
- Indirekter Nachweis mit Authentication Token
- Erzeugung von Secure Messaging Schlüsseln
- Gegensatz zu z.B. SIM-Karten (plaintext PIN)

Neuer Personalausweis - PACE 2/3

Ablauf via GENERAL AUTHENTICATE (0x86)

- nPA erzeugt und verschlüsselt 128-Bit Nonce
- eID-Client entschlüsselt Nonce mit

  s = AES128(SHA1(pw)[0..15], nonce)
- ECDHE auf G von brainpoolP256r1 => H
- ECDHE auf G’ = s * G + H => S

Neuer Personalausweis - PACE 3/3

- KEY_n = KDF(S[x], CTR)
- Für AES128: KDF = SHA1(S[x], CTR)[0..15]
- Secure Messaging mittels AES128-CBC und CMAC mit Send Sequence Counter
- beidseitige Berechnung des Authentication Token (CMAC über letzten ECDHE-Schlüssel der Gegenseite) und Vergleich

Neuer Personalausweis - EAC 1/2

Extended **A**ccess **C**ontrol

(Terminal Authentication)

- Erweiterung ggü. Basic Access Control (BAC) in ICAO MRTDs (Reisepässe)
- Übertragung einer Kette von Card Verifiable Certificates vom eID-Server zum nPA
- CVCA -> DVCA -> Terminal

Neuer Personalausweis - EAC 2/2

- Verifikation der Zertifikatskette gegen die im Ausweis hinterlegte Root
- Ggf. Update des Root-Ankers durch Link-Zertifikate in der Kette
- Bestätigung des Terminals durch ECDSA-Signatur über Challenge vom Ausweis und ECDHE-Schlüssel vom eID-Server

Neuer Personalausweis - TA / CA 1/2

Terminal **A**uthentication / **C**hip **A**uthentication

1. Während TA wird ECDHE-Schlüssel vom eID-Server zum nPA übergeben
2. Nach TA wird Zugriff auf EF.CardSecurity freigegeben, enthält Batch-Key und Signatur
3. ECDHE auf G von brainpoolP256r1 => S
4. KEY_n = KDF(S[x], CTR)

Neuer Personalausweis - TA / CA 2/2

- Secure Messaging Kanal zwischen eID-Server und Ausweis-Chip
- AuthenticationToken beweist Kenntnis des Batch-Key im Chip
- Signatur von EF.CardSecurity identifiziert DocumentSigner
- Prüfung gegen Whitelist der DSCA

Neuer Personalausweis - RID 1/3

Restricted **ID**entifier - Pseudonym

Dienste- und Kartenspezifisches Merkmal

- eindeutig je Ausweis und Sektor Beziehung (Sektorschlüssel = Diensteanbieter)
- Diensteübergreifend nicht verfolgbar, da immer verschieden,d.h. keine Datenspuren
- gut geeignet für Login (Wiedererkennung)

Neuer Personalausweis - RID 2/3

- technisch zwei Pseudonyme vorhanden, da Sperrlistenabgleich mit Sperrmerkmal erfolgt
- Sektorschlüssel wird durch DVCA vergeben, kein “Durchprobieren” durch Diensteanbieter möglich - z.B. berechnen eines fremden RID
- Neuer Ausweis = neues Pseudonym, da Schlüssel geheim “on-chip” erzeugt wird

Neuer Personalausweis - RID 3/3

- Berechnung durch ECDHE mit öffentlichem Sektorschlüssel aus Berechtigungszertifikat
- RID = SHA256(S[x]), S = ECDHE(pRID, Q)
- Sperrliste wird von DVCA berechnet unter Kenntnis des privaten Sektorschlüssels und des öffentlichen Sperrschlüssels des Ausweis zum Produktionszeitpunkt

Neuer Personalausweis - Sperrliste

- ~6 Mio. gesperrte Dokumente in 10 Jahren
- ~1600 Sperrungen täglich
- Sperrung muss binnen 24h propagiert werden
- bei 1000 Diensteanbietern 1,6 Mio Sperr- merkmale pro Tag = ~50MB DB-Inserts / Tag
- Sperrprüfung muss in kürzester Zeit erfolgen (-> in-memory DB, ~200MB / Sektor)

Vielen Dank.

Fragen und Antworten

Christian Kahlo
Research Manager IT-Security
AGETO Innovation GmbH

Glossar

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CMAC	Cipher MAC
CVC	Card Verifiable Certificate
DS (CA)	Document Signer (Certification Authority)
DV (CA)	Document Verifier (Certification Authority)
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
KDF	Key Derivation Function
MAC	Message Authentication Code
SHA	Secure Hash Algorithm