Bundesamt
für Sicherheit in der
Informationstechnik

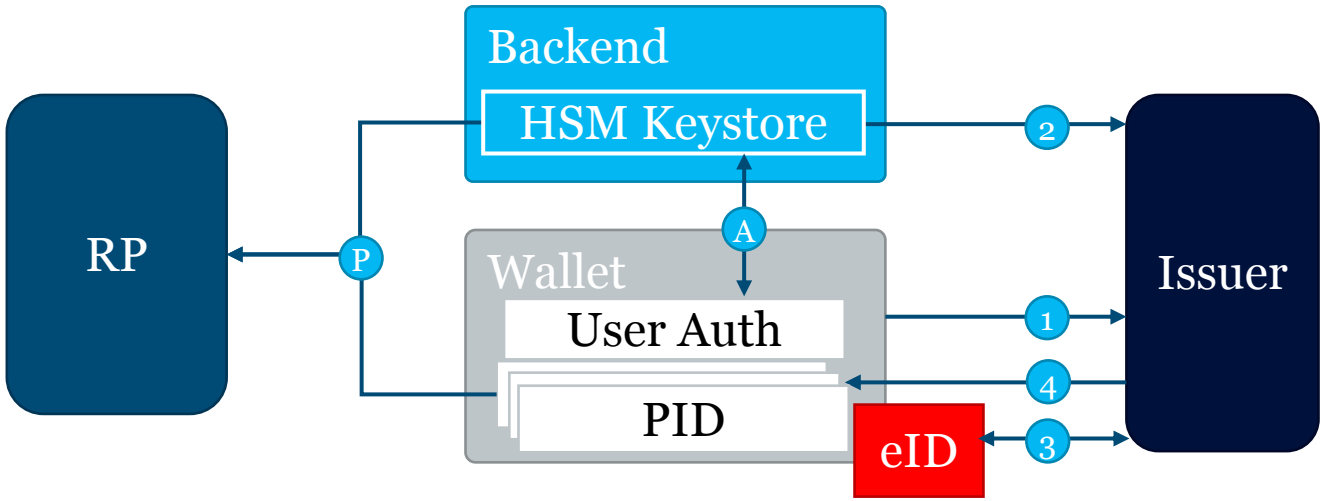
Deutschland
Digital•Sicher•BSI•

EUDI Wallet: Deutschland

Frederic Kehrein – OmniSecure 2025

Erste Iteration der Deutschen EUDI Wallet

Oversimplified!



1. Attribute Issuance Request
2. Attribute Key + Key Attestation + PoP
3. User identification + data from eID
4. Issuing of PID into Wallet

A. Two-Factor user Authentication for HSM key usage

P. Create presentation from local attributes PID with HSM key

Wallet Backend zur Absicherung:

- Sichere Schlüssel Speicherung
- Nutzer Authentisierung

Tracking Mitigation durch Wallet App:

- PID Daten liegen in Wallet App
- RP Identifizierung durch Wallet

▶ Backend kennt weder Nutzer noch Dienst

Herausforderungen

Viele offene Probleme mit Umsetzung von Wallets

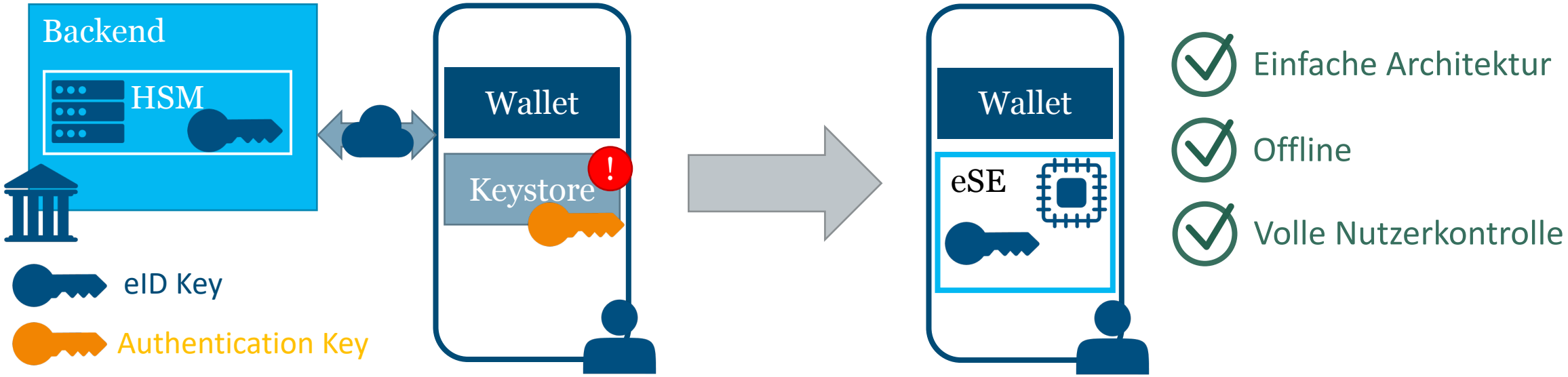
Offline Fähigkeit

Zertifizierung

Trackingschutz

Kosten

Secure Element als Sicherheitsanker



Erste Iteration:

- Sicherheitsfunktionen von Backend bereitgestellt
- Online Verbindung zu Backend benötigt
- Gerät als Authentisierungsfaktor und Interface

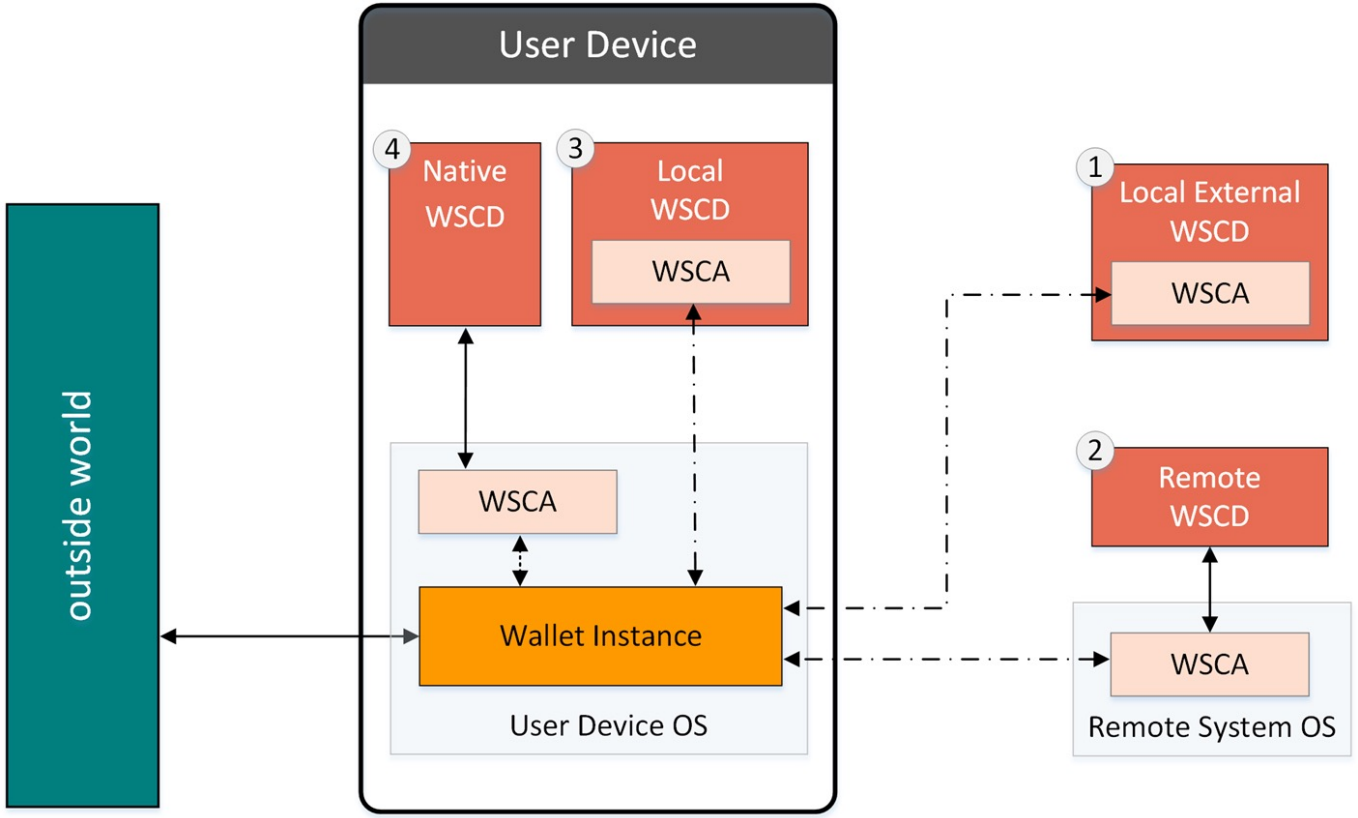
Ziellösung:

- Secure Elements als Sicherheitsanker
- Schützen Schlüssel und Authentisieren Nutzer
- Zertifizierte Hardware für Assurance

! Anforderungen und Zertifizierung für LoA High noch offen

Mobile Hardware

Wallet Secure Cryptographic Application & Device (WSCA/WSCD)



- Architektur der Wallet aus den Durchführungsrechtsakten
- „Critical Assets“ Management durch WSCA und WSCD
- Resistenz gegen hohes Angriffspotential
- Remote: HSM

Hardware in SmartPhones

System Keystores:

- TEE: Virtualisierungslösung auf ARM TrustZone basis
- Secure Enclave: Sicherheitsprozessor als Part von SoC von Apple
- Stongbox: API zu dediziertem Sicherheitschip mit Strongbox Applet

- Weitflächiger Zugang für Anwendungen
- Fehlende Zertifizierung (Zertifizierbarkeit) und fragwürdige Sicherheitseigenschaften
- Proprietäre Software durch Gerätehersteller
  - Eingeschränkte Funktionalität
  - Kontrolle durch OEMs

Secure Element und embedded SIM

- Smartphones verfügen über zusätzliche Sicherheitselemente
  - Embedded Secure Element (eSE): Dedizierter Sicherheitschip im Smartphone
  - Embedded SIM (eSIM): Dedizierter Sicherheitschip mit MNO Profilen für SIM
- EUCC Zertifizierbar gegen hohes Angriffspotential
  - CC Technical Domain „Smartcards and similar devices“
- Erlaubt eigene Applets in offener JavaCard Architektur

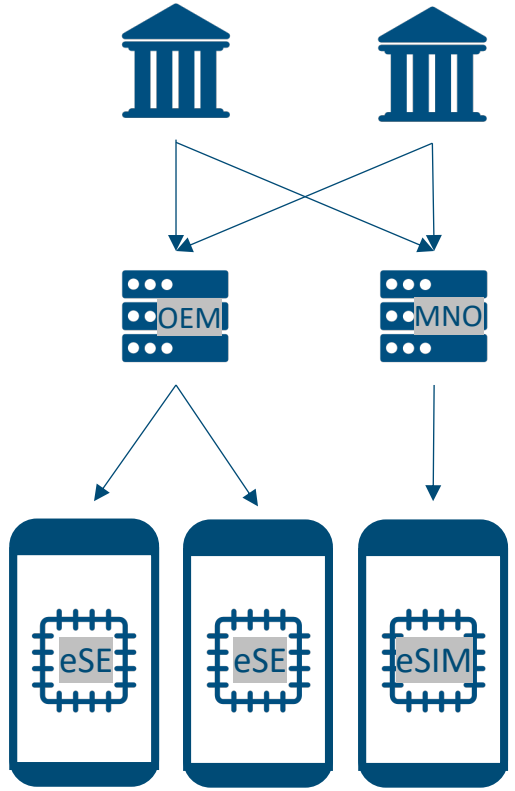
Aber:
! Zugang nur durch OEMs oder MNOs

eSE und eSIM

Technische Herausforderungen und Entwicklungen

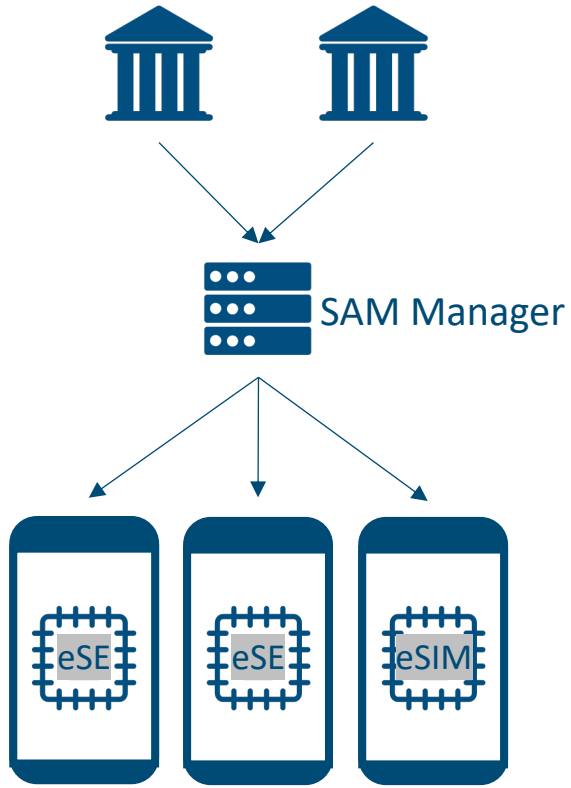
Applet Provisionierung

- Provisionierung auf eSE und eSIM nicht standardisiert
  - OEM-spezifische Infrastruktur und Schnittstellen
  - Potentiell sogar gerätespezifische Anforderungen
- MNO Profile auf eSIM
  - MNOs können Applets nur in eigenes Profil laden
  - Profilwechsel oder Deaktivierung beeinflusst eID Applet
- OEM/MNO als Gatekeeper
  - Bilaterale Verträge mit allen OEMs und MNOs benötigt
  - Kontrolle über erlaubte Applets bei OEM/MNO
    - OEMs außereuropäisch



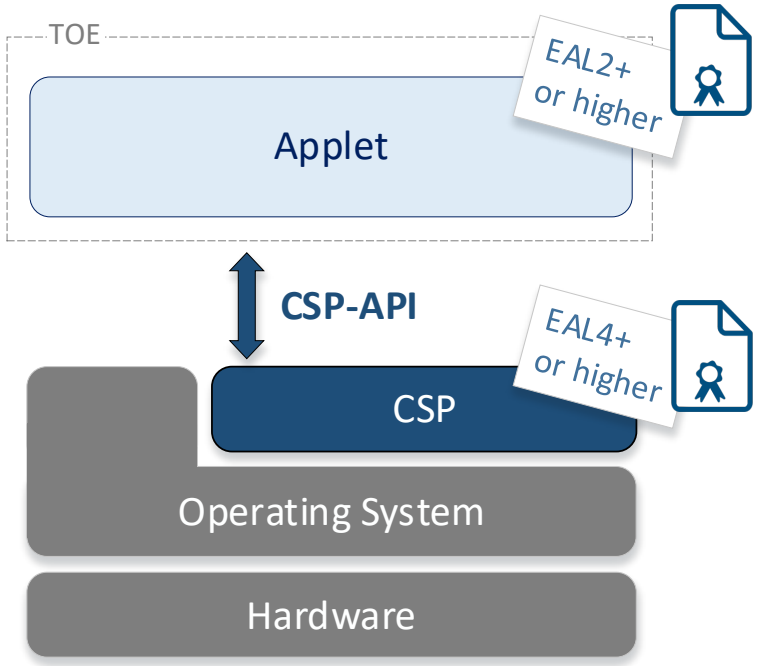
Secure Applications on Mobile (SAM)

- Standardisierte Schnittstelle zum Provisionieren von Applets
  - Standardisiert von GlobalPlatform und GSMA
  - Einheitliche Protokolle und Technologien unabhängig von MNO und OEM
- SAM PKI Schlüssel werden von Herstellern auf Chips provisioniert
  - Unabhängig von OEMs
  - Zertifizierung beim Chip Hersteller
- Provisionieren von Applets in eigene unabhängige SAM Scopes
  - Autorisiert durch unabhängige PKI
    - Vergleichbar mit RSP durch GSMA



Cryptographic Service Provider (CSP)

- Vereinfacht Applet Zertifizierung
  - Erreicht hohes Level in Kombination CSP + Applet
  - Unabhängig von unterliegender Hardware
- Plattformunabhängigkeit durch Zertifizierte API
  - Management von Assets, Schlüsseln, etc.
  - Übernimmt alle kritischen Funktionalitäten
  - Zusammen mit Hardware vom Hersteller zertifiziert (>EAL4+)
- Harmonisiert Basisfunktion
  - Kryptografische Operationen
  - Erweiterter Funktionsumfang (Schnorr ZKPs, Protokolle, etc.)



Wie Geht’s Weiter?

Wie geht’s weiter?

SAM technische Spezifikation verfügbar

- Referenziert in Annex I der Durchführungsrechtsakte zur Wallet Kernfunktionalität
- Schutzprofil für Zertifizierung in Arbeit

SAM Governance noch offen

- Provisionierungs PKI für EU eID Applets fehlt
- OEMs müssen EU PKI kompatible, SAM-enabled Chips einbauen

Enge Zusammenarbeit mit der Kommission und den Herstellern

- Arbeitsgruppe für Secure Element Access auf EU Ebene
- Ausarbeitung der Governance auf EU Level
- Kontakt mit Herstellern bezüglich Umsetzung und Zugang

Wie geht’s weiter?

CSP 1.0 als Schutzprofil verfügbar

- Von ENISA referenziert
- Bereits im Feld (Registrierkassen, Smart-eID)
- Aber: Unterspezifiziert

CSP 2.0 als Spezifikation bei GlobalPlatform

- Aktuell noch in der Standardisierung
- Höherer Funktionsumfang: Soll möglichst viele use-cases abdecken

Einbringen der Anforderungen für EUDI Wallet und andere eID Systeme

- Aktuelle Anforderungen zur Umsetzung einer Wallet nach eIDAS
- Abdecken zukunftsfähiger Technologien für zukünftige Iterationen der EUDI Wallet

Bild: ©Adobe Stock, Bee

Backup

Wallet Secure Cryptographic Application & Device (WSCA/WSCD)

Hardwareanker wird durch WSCD/WSCA bereitgestellt

(1) ‘wallet secure cryptographic application’ means an application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the wallet secure cryptographic device;

(12)‘wallet secure cryptographic device’ means a tamper-resistant device that provides an environment that is linked to and used by the wallet secure cryptographic application to protect critical assets and provide cryptographicfunctions for the secure execution of critical operations;

- Sichere Speicherung und Verarbeitung von „critical assets“
  - Authentisierungsschlüssel, Nutzerauthentisierung
  - Resistenz gegen hohes Angriffspotential
- Remote: HSM, Lokal: ???

Applet Zertifizierung

- Chip Zertifiziert von Hersteller
  - Bis zu EAL6
- Applet Zertifizierung gegen Schnittstelle von Chip
  - Composite Zertifizierung
  - Zertifiziert Kombination von Applet und Hardware
- Mobiltelefonmarkt sehr Heterogen
  - Hohe zertifizierungskosten skaliert mit jeder Geräte Kombination
  - Unwirtschaftlich mit aktuellen Zertifizierungschemata