Standards & Zertifizierungsstrategien für Wallet WSCD, Applets und SAM

Federal Office
for Information Security

Januar 2026

Anforderungen an die EUDI Wallet

Diese Anforderungen implizieren bestimmten Standardisierungsbedarf

Offline Fähigkeit

Benötigt standardisierte, plattformübergreifende Schnittstellen zu hardware-gebundenen Vertrauensankern (z.B. SE) zur sichere Speicherung der Identitätsnachweise lokal auf dem Gerät.

Zertifizierung

Erfordert neuen Evaluierungsansatz um hohe Sicherheitsniveaus wie VAN.5 auch für heterogene, sich schnell ändernde Endgeräte-Ökosysteme bewerten zu können.

Trackingschutz

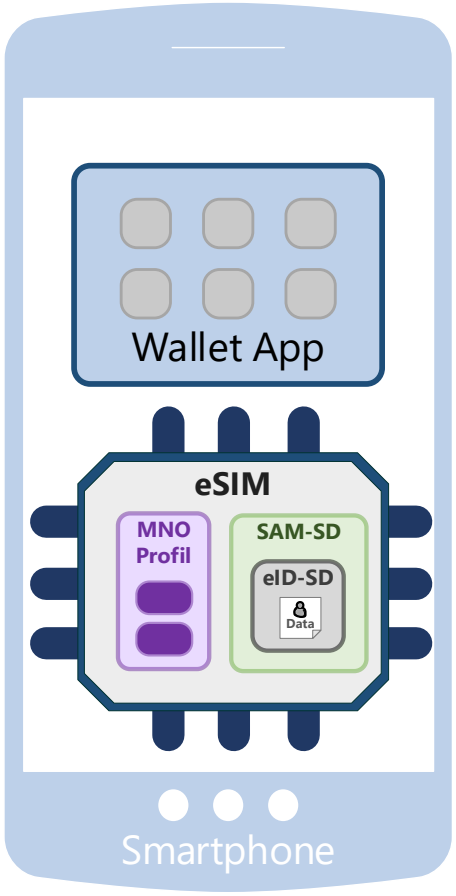
Erfordert international standardisierte kryptographische Verfahren, die interoperablen Datenaustausch ermöglichen, ohne korrelierbare Identifikatoren zu erzeugen.

Kostenfrei

Erfordert eine Verlagerung der Kosten in die Infrastruktur- und Geräteebene sowie eine Reduzierung der Integrations- und Betriebskosten durch offene, wiederverwendbare internationale Standards.

Offlinefähigkeit

Credentials sollen lokal, manipulationssicher und prüfbar gespeichert werden
– ohne Online- oder Cloud-Abhängigkeit



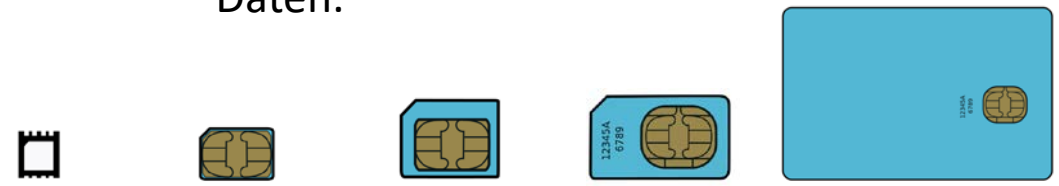
Standard: Secured Applications for Mobile (SAM)

→ Ermöglicht Zugang zu eSE und eSIM für Wallet-Anbieter zur sicheren Speicherung von Ausweisdaten

Warum Secure Element / eSIM?

- eSIM basiert auf bewährter Smartcard-Technologie
- Seit Jahrzehnten im Einsatz die bereits seit Jahrzehnten im Einsatz ist zur sicheren, manipulationssicheren Speicherung von sensiblen Daten.

Historie der eSIM:



Secured Applications for Mobile (SAM)

Standards (verfügbar):

- GSMA SAM Definition of Requirements — SAM.01 v1.2
- GlobalPlatform SAM Configuration — GPC_GUI_217 v1.0
- ETSI SET Logical Secure Element Interfaces — LSI

Regulierung & Gesetze:

- GSMA SAM.01 referenziert in ANNEX I der EU-Verordnung 2024/2979
- EU-Subgroup für Secure Elements im Gesetzestext verankert

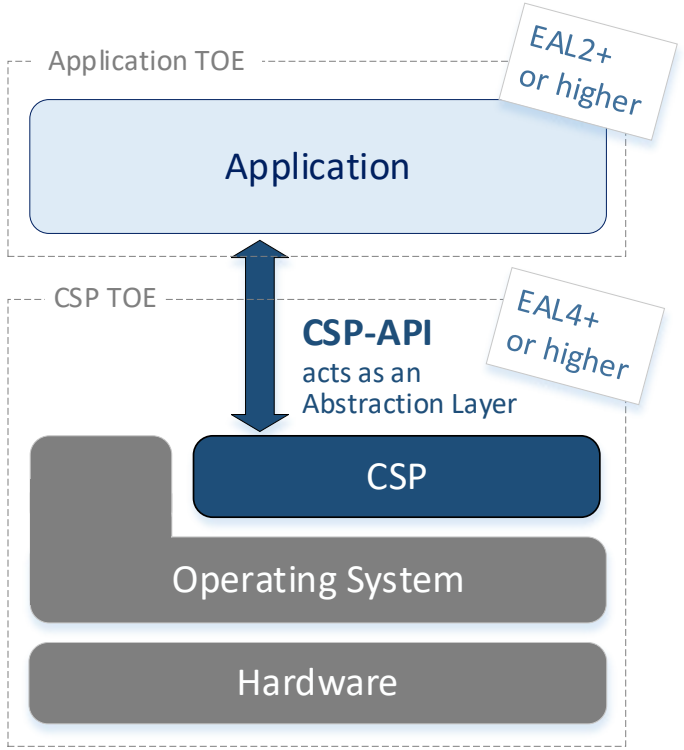
IMPLEMENTING REGULATION (EU) 2024/2981

Official Journal
of the European Union

(8) Fully mobile, secure and user-friendly wallets are supported by the availability of standardised and certified tamper-resistant solutions, such as embedded secure elements, external devices such as smartcards, or embedded SIM platforms in mobile devices. It is important to ensure the timely access to embedded secure elements for national eID means and wallets and to coordinate efforts by Member States in this area. The European Digital Identity Cooperation Group established pursuant to Article 46e(1) of Regulation (EU) No 910/2014 ('Cooperation Group'), should therefore establish a dedicated subgroup for this purpose. Consulting relevant stakeholders, this subgroup should agree on a joint roadmap for access to embedded secure elements to be considered by the Commission for the review report on the Regulation (EU) No 910/2014. In order to facilitate the uptake of the wallet at national level, the Commission should furthermore, in cooperation with Member States, develop and continuously update a manual for use cases as part of the Architecture and Reference Framework.

Zertifizierung

EUDI Wallets benötigen Zertifizierung mit hohem Vertrauensniveaus (z. B. VAN.5) – auch auf mobilen Endgeräten mit wechselnder Hardware und Software.



Standard: Cryptographic Service Provider (CSP)

→ Eine alternative Zertifizierungsmethode als Kompromiss zwischen klassischer Software Evaluierung und der Composite Product Evaluation for Smart Cards and Similar Devices

Warum CSP-API als Abstraktionsschicht?

- Mobile Applets / Apps können heute nicht generisch für VAN.5 zertifiziert werden
- Common Criteria verlangt: konkretes Hardware-Modell + Chip-Version + OS-Version
- Zertifizierung nur pro Gerätemodell → nicht skalierbar

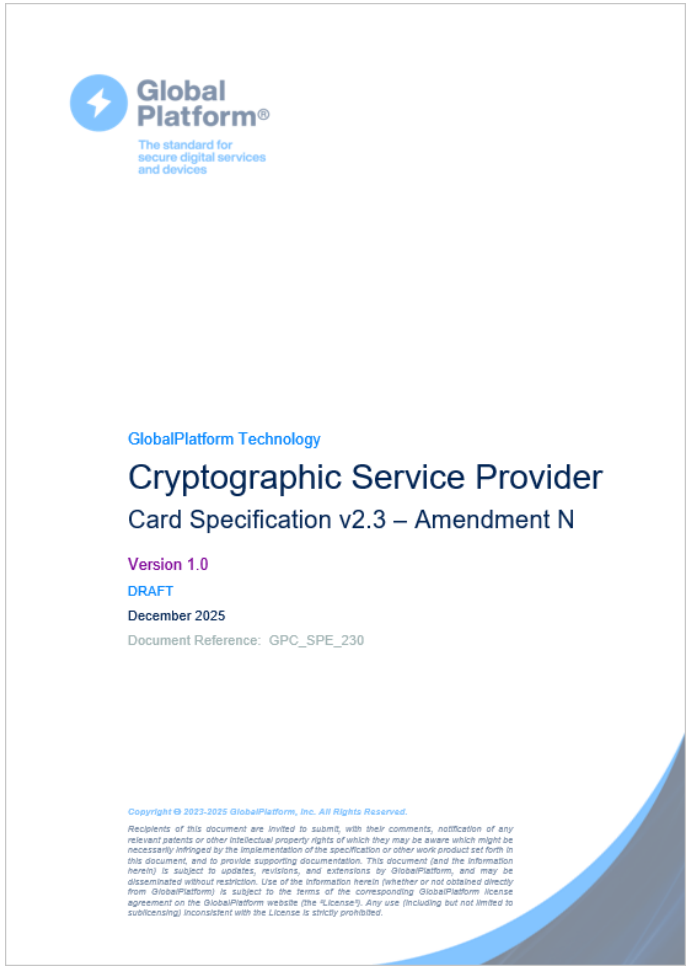
Was kann der CSP?

- CSP kapselt **anwendungs-spezifische** sicherheitskritische Funktionen
- Zertifizierungsaufwand wird auf Chip-Hersteller verlagert

Cryptographic Service Provider (CSP)

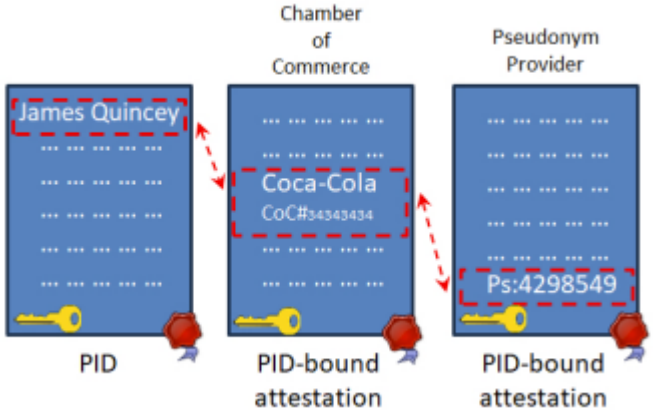
Standards :

- GlobalPlatform Ammendment N CSP - *Publikation geplant Q1 2026*
- GlobalPlatform CSP API - *Publikation geplant Q1 2026*
- GlobalPlatform CSP Configuration - *Publikation geplant Q2 2026*
- GlobalPlatform CSP Generic Guidance - *Publikation geplant Q2 2026*
- GlobalPlatform SE PP mit CSP Modul - *in Erarbeitung*



Trackingschutz

Identitäts-Nachweise der Wallet müssen authentisch und überprüfbar sein, ohne korrelierbare Signaturen oder stabile Identifier zu erzeugen.



Kryptographisch gebundene Attribute ohne stabile Identität

Standard: Unlinkable / Zero-Knowledge-Signaturen

→ BBS+ und Schnorr-basierte Verfahren als kryptographische Bausteine ermöglichen Signaturen mit Trackingschutz

Wie funktionieren die Verfahren?

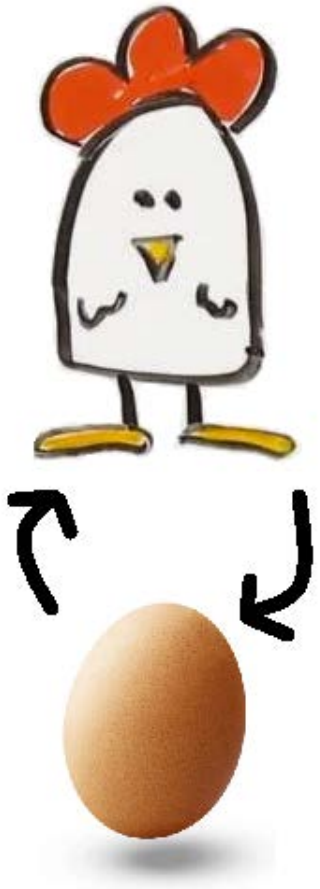
- Ableitung kontextgebundener, einmaliger Signaturen
- aus im Gerät sicher gespeicherten Schlüsseln
- ohne Offenlegung der zugrunde liegenden Schlüssel

Ergebnis?

- Verifier kann prüfen: Gültigkeit & Zusammengehörigkeit der Attribute
- Ohne: wiedererkennbare Signaturen bzw. ohne Rückschluss auf Identität oder frühere Transaktionen

Kostenfrei

Die Nutzung der Wallet muss kostenfrei für den Endnutzer sein – keine laufenden Gebühren für Identitätsnachweise oder deren Verwendung.



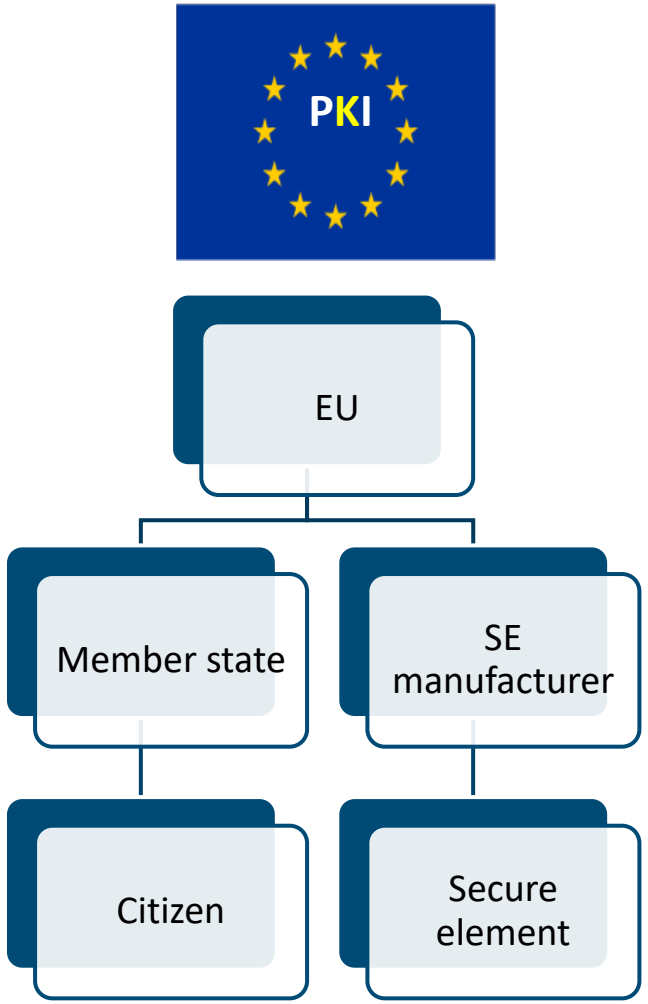
Internationale Standards reduzieren Kosten durch

→ Einheitliche APIs und wiederverwendbare Bausteine
→ Kostenverschiebung weg vom Endnutzer zu Herstellern & Plattformen

- **Erhöhter Aufwand** bei Chip-Herstellern für Implementierung & Zertifizierung der Standards und kryptografischen Protokolle
- Wallet- und Applet-Provider können zertifizierte Sicherheitsfunktionen nutzen
  → reduzierter eigener Zertifizierungsaufwand

Zugang zu Secure Elements

- Es entstehen **erhebliche Kosten**, wenn jeder Wallet-Anbieter jeden OEM bzw. Secure-Element-Hersteller einzeln kontaktieren und individuelle Verträge für den Zugang zu Secure Elements abschließen muss.
- **Essentiell** ist die Etablierung eines **Key-Managements über eine EU-SAM-PKI**, die den Zugang zu **eSIM / eSE** für alle **27 EU-Mitgliedstaaten** regelt.
- Die **EU-SAM-PKI** sollte idealerweise in der **EU-Subgroup für Secure Elements** diskutiert werden; ggf. auch im Kontext künftiger **Regelungen zum digitalen Euro**.



Federal Office
for Information Security

Danke für ihre Aufmerksamkeit!

Annegret Schöffel

Referat-D13@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 87

53175 Bonn

www.bsi.bund.de

Follow us: