



Technische Richtlinien und Prüfvorgaben BSI

**FORUM 14-A Teil 3:
Die Rolle von eSIM und SE für die Sicherheit der Digitalen Identität**

Referat SZ34, Omniseure Berlin, 23.05.2023

Gliederung

1. Motivation SE
2. Regulierung SE
3. Standardisierung SE




Sicherheitszertifizierung von IT-Produkten

Eine der Kernaufgaben des BSI ist die **Sicherheitszertifizierung**, dazu gehört

- die Erstellung Technischer Richtlinien (BSI TRs)
- die Entwicklung von Prüfvorgaben zur Zertifizierung von IT-Produkten (PP: Protection Profiles)

Herausforderung der Sicherheitszertifizierung mobiler Lösungen für eine Digitale Identität:

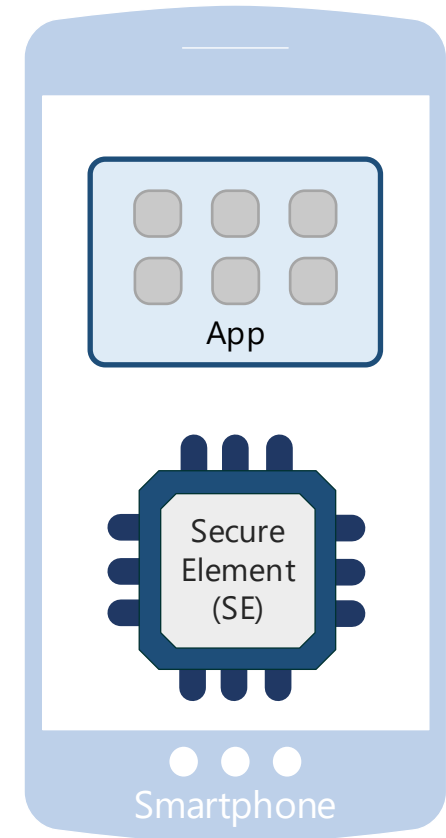
- 
- Hohe Komplexität in Software und Hardware
 - Hohe Anzahl verschiedener Hersteller und Modelle
 - Regelmäßig neue Hardware-Modelle und Software-Updates



Die Rolle von eSIM und SE für die Sicherheit der Digitalen Identität - Motivation

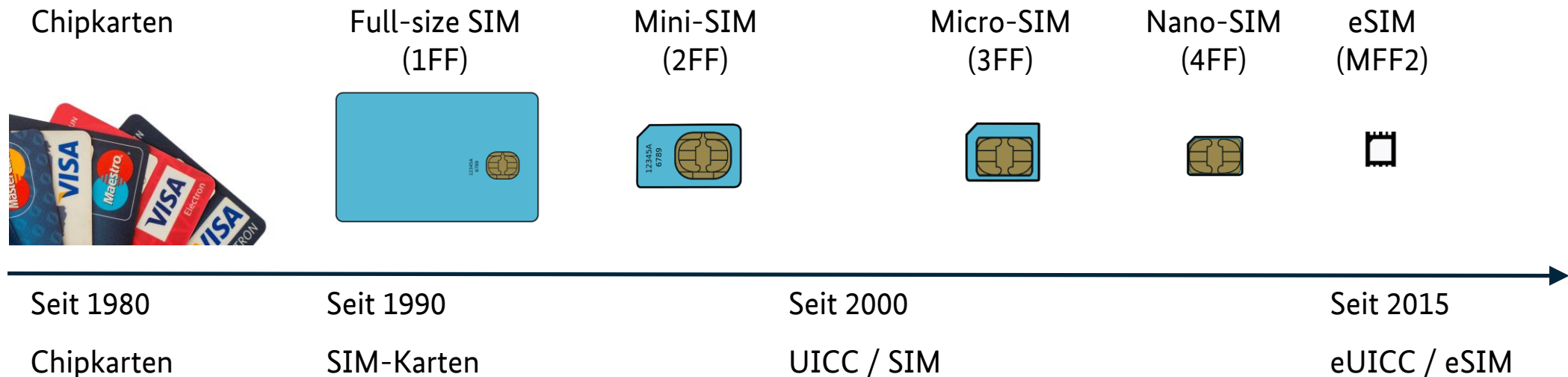
Secure Element (SE) als Hardware-Vertrauensanker mobiler Endgeräten

- **SEs sind Hardware-Sicherheitschips**
SEs können in mobile Endgeräten wie Smartphones, Smart-Watches, IoT-Geräte, etc. integriert werden.
- **SE: isoliert und manipulationssicher (tamper-resistant)**
SEs sind ideal zur Verwaltung und Nutzung von Schlüsselmaterial oder anderer sensibler Daten.
- **SEs sind geeignet für Anwendungen mit hohem Schutzbedarf**
z.B. Mobilfunk, eID, Banking, Zugangskontrollen
- **Sicherheitszertifizierung möglich**
Hardware und Software der SEs können nach Common Criteria zertifiziert werden



Übersicht Secure Elements: eine Smartcard Technologie

- SEs (UICC, SIM, eSE, eUICC, eSIM) basieren auf bewährter Smartcard-Technologie.
- eSIM bereits EAL4+ zertifiziert (für Mobilfunkzulassung).
- Es gibt viele europäische Hersteller für SEs.



SE-Regulierungsaktivitäten des BSI

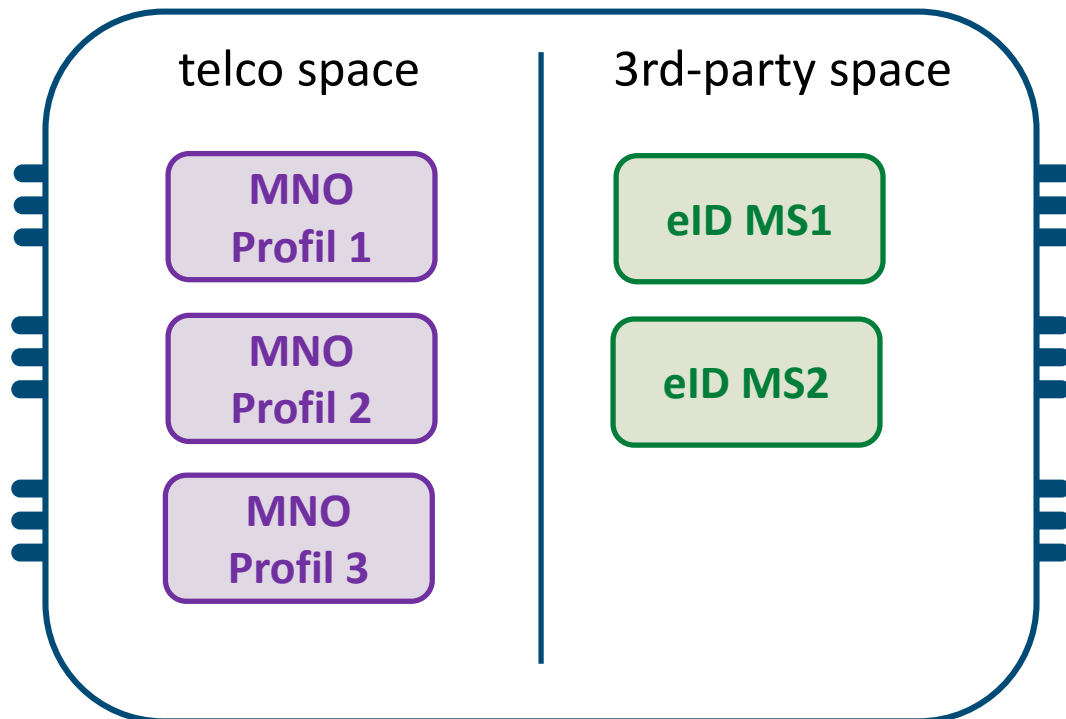
ENISA erstellt derzeit verschiedene Zertifizierungsschemas kompatibel zum Cyber Security Act (CSA). Das BSI ist aktiv in den Arbeitsgruppen und vertritt folgende Positionen zum SE:

- Platzieren von Anforderungen zur eUICC/eSIM im EU5G Zertifizierungsschema für 5G Netzkomponenten
- Zertifizierung der eUICC/eSIM basierend auf dem horizontalen EUCC Zertifizierungsschema nach Common Criteria
- Nutzung der eUICC/eSIM als Plattform für sichere Anwendungen
- Austausch mit der eIDAS Expert Group bzgl. Zertifizierung von EUDI Wallet-Lösungen



SE-Standardisierungsaktivitäten des BSI

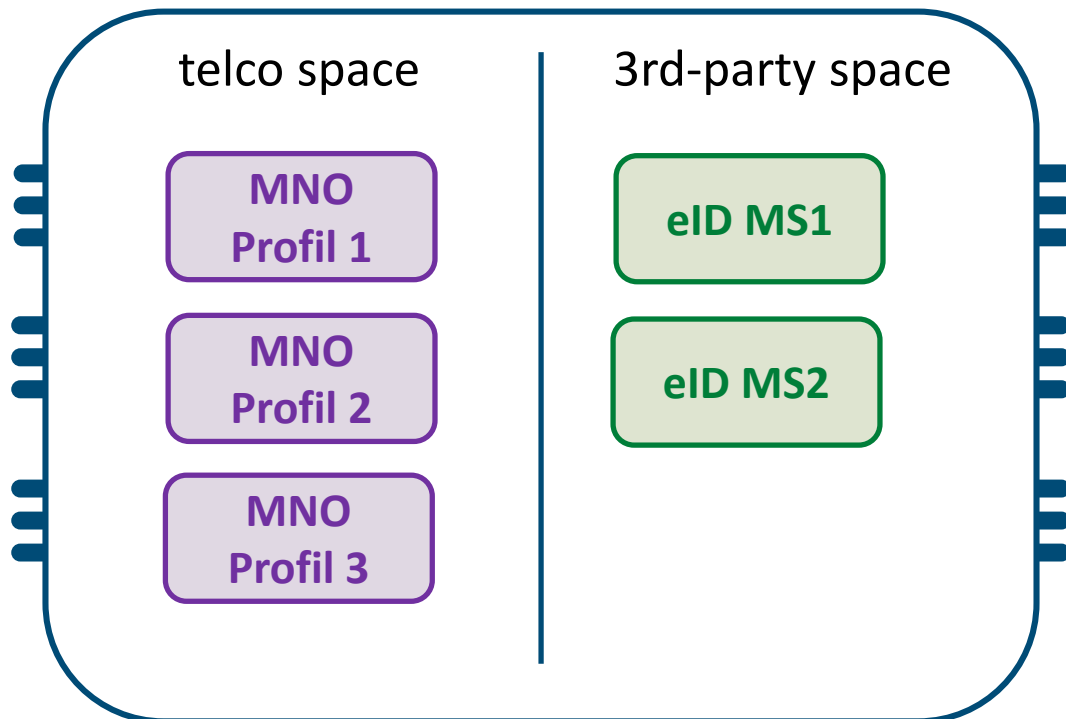
GlobalPlatform und GSMA sind zwei Standardisierungsorganisationen relevant für Secure Elements. Das BSI beobachtet, begleitet und fördert folgende aktuelle SE-Standardisierungsaktivitäten:



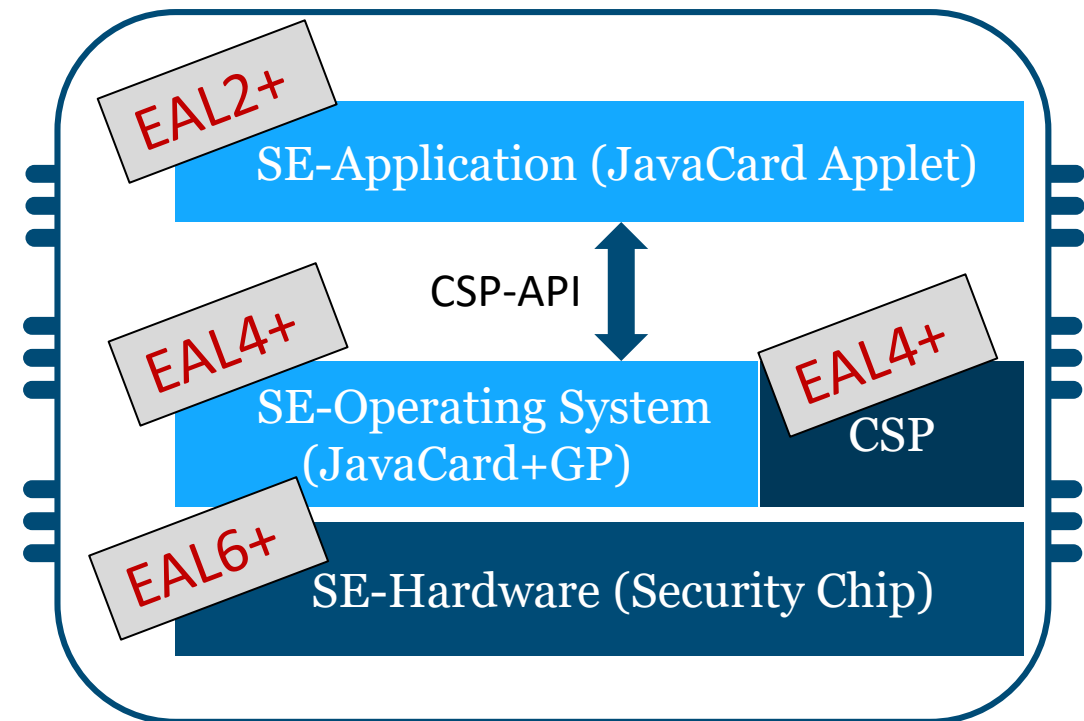
1. SE mit Secure Applications on Mobile (SAM)

SE-Standardisierungsaktivitäten des BSI

GlobalPlatform und GSMA sind zwei Standardisierungsorganisationen relevant für Secure Elements. Das BSI beobachtet, begleitet und fördert folgende aktuelle SE-Standardisierungsaktivitäten:



1. SE mit Secure Applications on Mobile (SAM)



2. SE mit Cryptographic Service Provider (CSP)

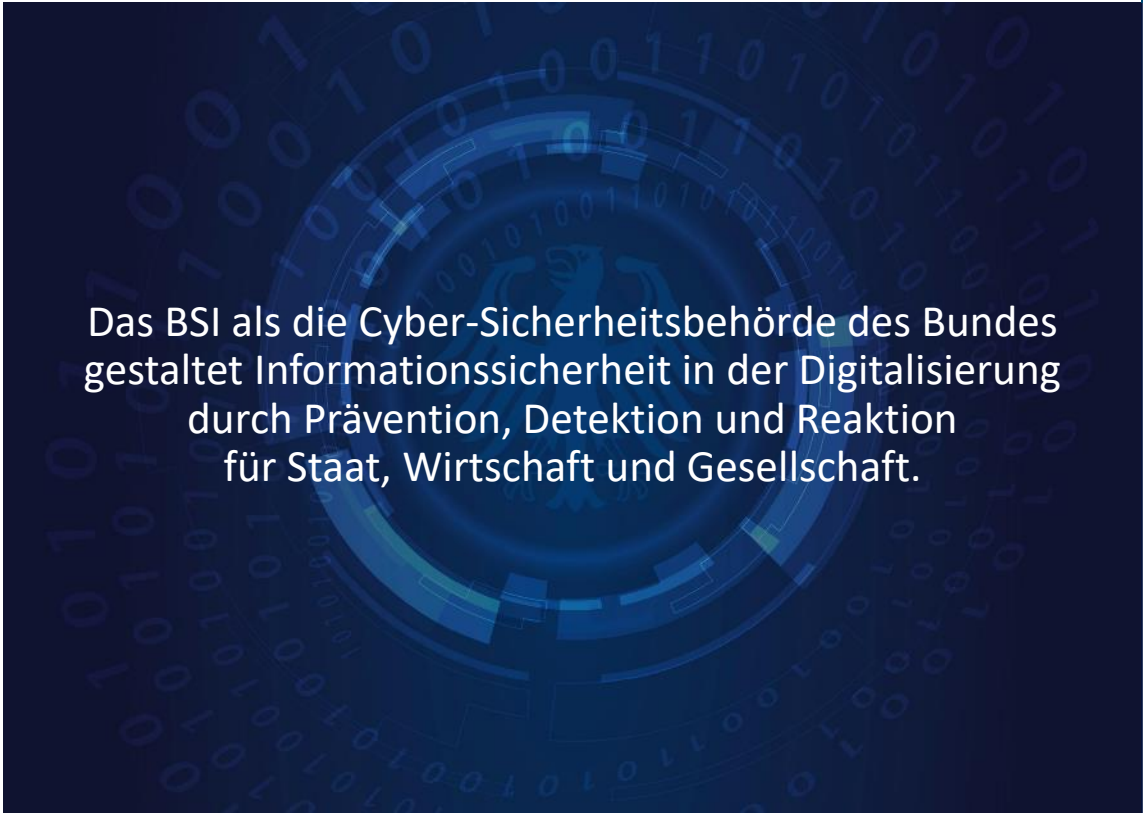
Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Referat SZ34

referat-sz34@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de



Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.