Federal Office
for Information Security

Scalable Security using SAM and CSP

Session: Hardwarebasierte Vertrauensanker für die europäische eID Technologie

Tobias Damm, BSI - Referat TK11 – Chip Security

Omnisecure Berlin, 22.01.2024

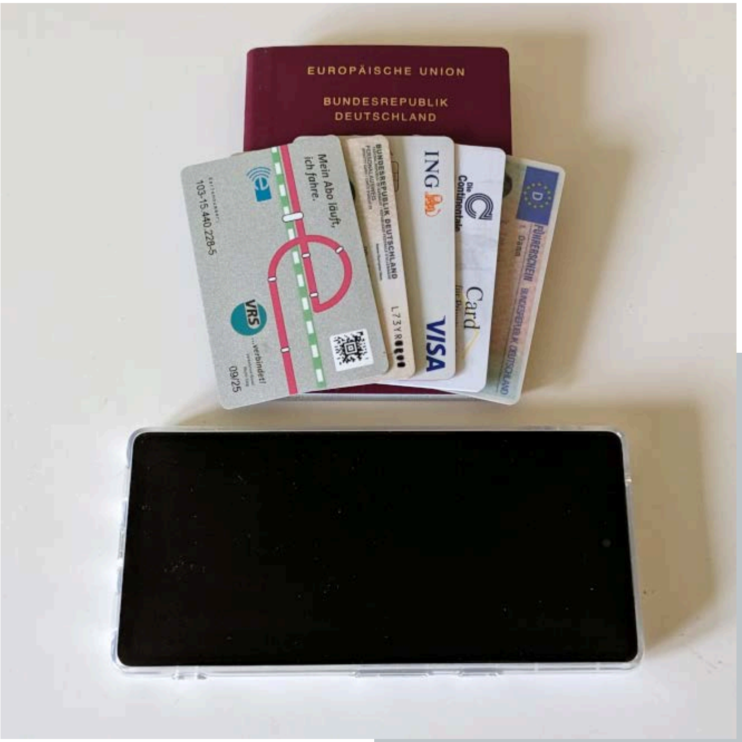
Digital Identities on mobile platforms …

Goals:

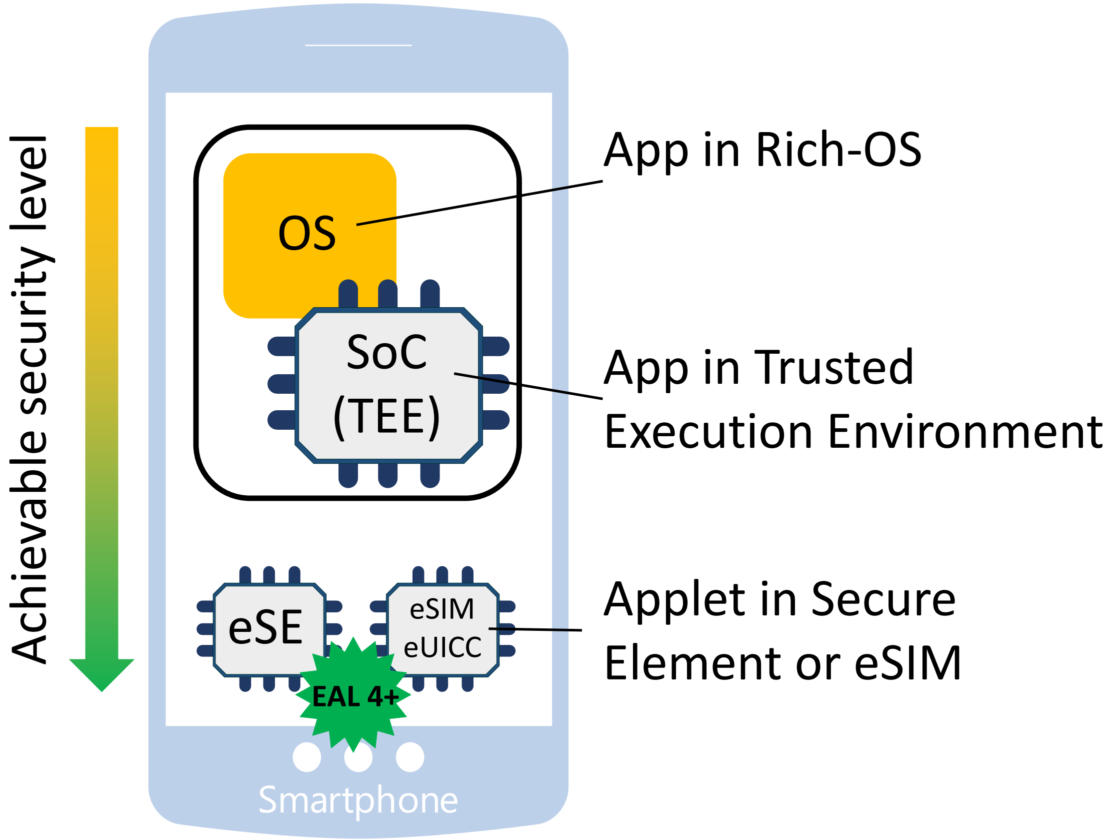
- Ease of use
- High functionality
- Broad availability
- New use cases
- Much more …

Common questions:

- Use case (What?)
- Regulation (Who?)
- Acceptance (Why?)
- **Implementation (How?!)**



… designed secure !


Achievable security level
OS
SoC
(TEE)
eSE
eSIM
eUICC
EAL 4+
Smartphone
App in Rich-OS
App in Trusted Execution Environment
Applet in Secure Element or eSIM

Security by certification

- Verifiability
- Documented security assertion
- Highest security guarantees by using dedicated hardware (EAL 4+, VAN.5 highly avail.) eIDAS 'high'

Challenging constraints:

- Mobile devices are complex
- Heterogeneous market (many OEMs & devices)
- High number of involved parties (OEMs, MNOs, Service Providers, …)

Implementation: Secure, Scalable, Available, Economical ?

Two contributions

1 **Secured Applications for Mobile (SAM)**

organizational & technical approach for the reduction of dependencies regarding the life cycle

2 **Cryptographic Service Provider (CSP)**

organizational & technical approach for secure implementation and reduction of certification requirements

Secured Applications for Mobile – Use Case

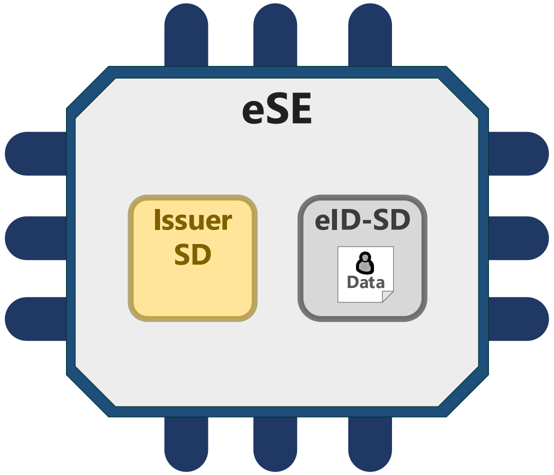
> *The Secured Applications for Mobile specification defines a capability allowing cellular connected Devices to use a wide range of secured applets within an eUICC. Such applets can be managed by a service provider, and may be paired with applications running in the Device itself.*
>
> *- GSMA SAM v1.1*

Use case / process (here: eID):

1. Download und install an app of the Application Service Providers (ASP) into Rich-OS.
2. Evaluation (by the app) if platform and eUICC are eligible (availability, version, storage space, etc.).
3. If positive: Register at ASP and in the SAM-SD of the eUICC.
4. Install the appropriate eID-applet into the SAM-SD. Transfer rights to ASP.
5. Personalize the eID-applet with user data (utilizing e.g. the physical eID-card).
6. Secure use of the eID functionality.

Challenge: Accessing the eSE / eSIM

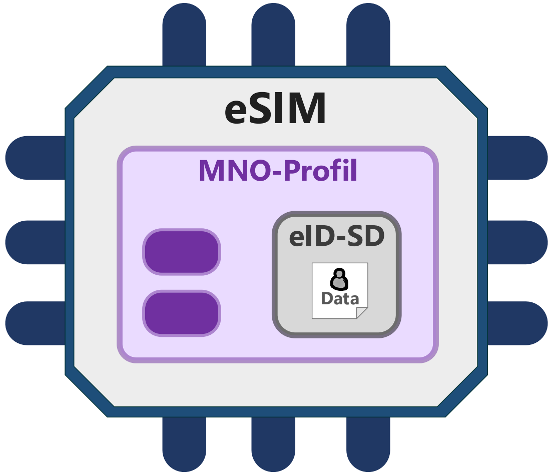
eID in eSE



Dependencies on OEM

Access to embedded Secure Elements (eSE) only possible via interfaces of the device manufacturer.

eID in MNO-Profile on eSIM



Dependencies on MNO

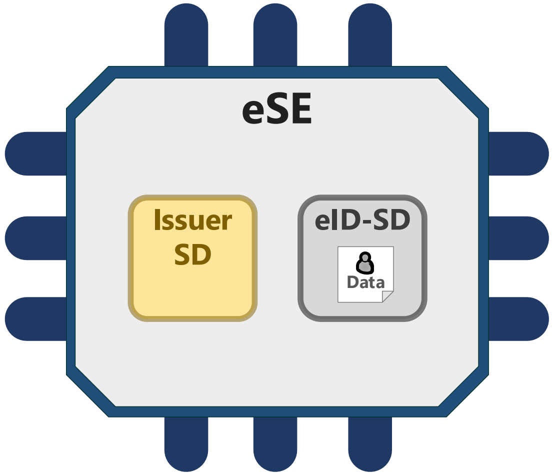
Access to eUICC/eSIM only possible via interfaces of the mobile network operator (MNO).

- Accessing the dedicated hardware to use secured applications is typically very restrictive and limited.
- Need to use OEM- and MNO- specific interfaces and background systems.

Federal Office
for Information Security

SAM as foundation for third party applications on eSE / eSIM

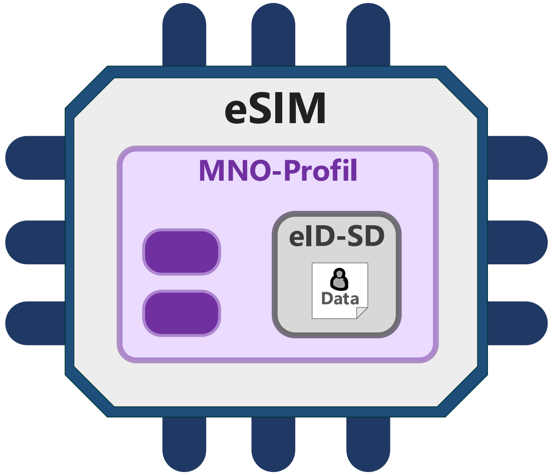
eID in eSE



Dependencies on OEM

Access to embedded Secure Elements (eSE) only possible via interfaces of the device manufacturer.

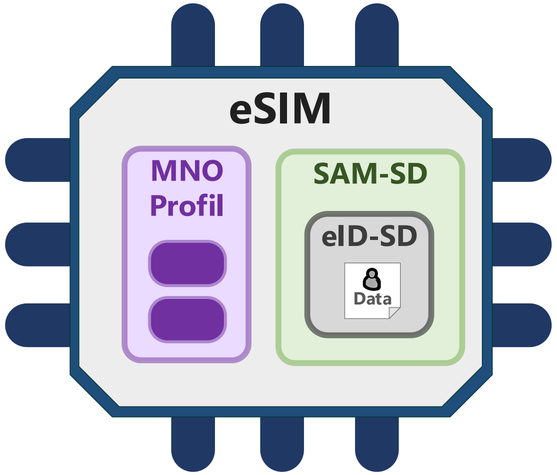
eID in MNO-Profile on eSIM



Dependencies on MNO

Access to eUICC/eSIM only possible via interfaces of the mobile network operator (MNO).

eID in SAM-SD besides MNO-Profile (eSIM) or Issuer SD (eSE)



Reduced dependencies

Access to SAM-SD on eSE / eUICC via SAM management systems and SAM-PKI.

Two contributions

① **Secured Applications for Mobile (SAM)**

organizational & technical approach for the reduction of dependencies regarding the life cycle

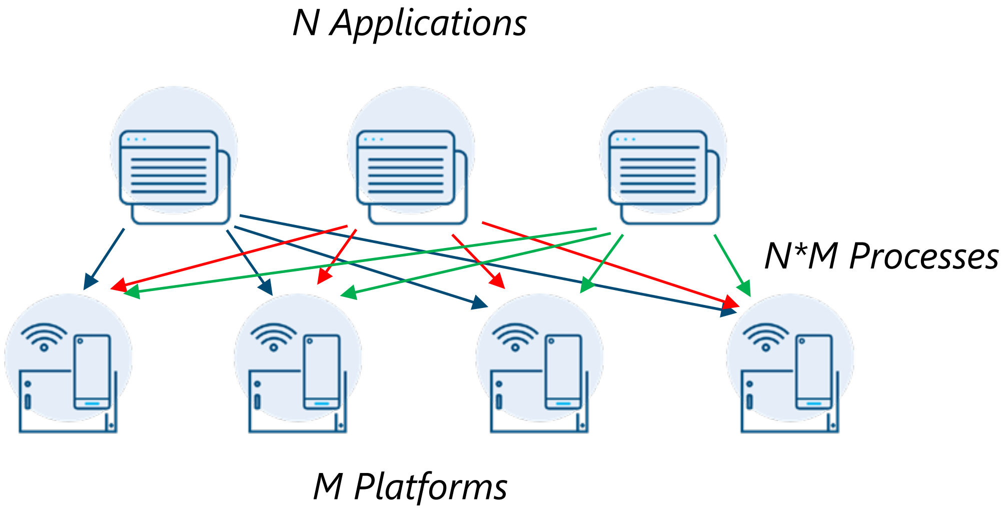
② **Cryptographic Service Provider (CSP)**

organizational & technical approach for secure implementation and reduction of certification requirements

Scalability of security certifications

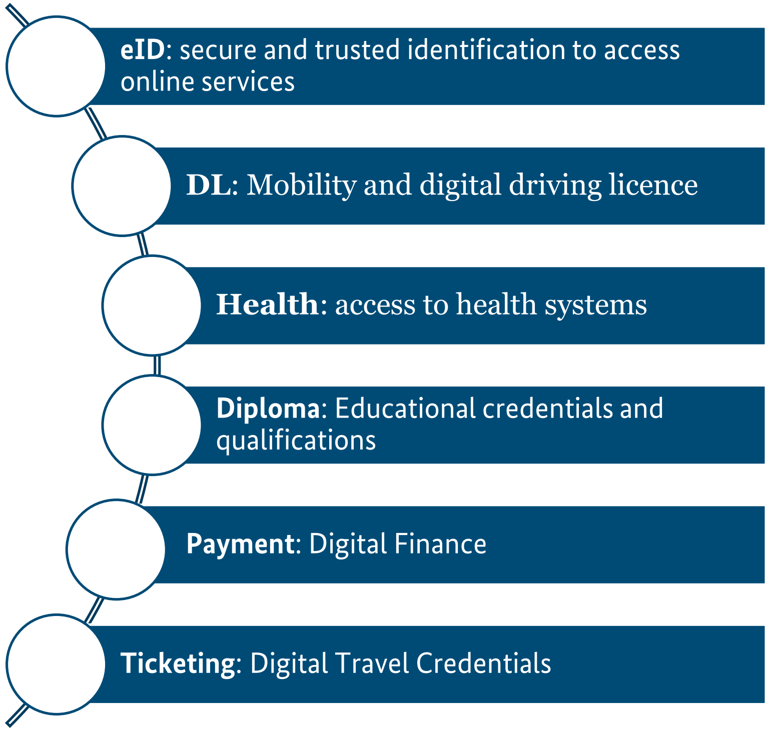
‘Composite evaluation’ for high assurance classes

- High effort (financial & time-wise)
- Requires deep understanding of the platform (requirements & restrictions)
- Limited usability of the platform certificate (18 months)
- Static assurance class, low modularity
- Low scalability



No ideal fit for products in heterogeneous markets with short product cycles

Applications



eID: secure and trusted identification to access online services

DL: Mobility and digital driving licence

Health: access to health systems

Diploma: Educational credentials and qualifications

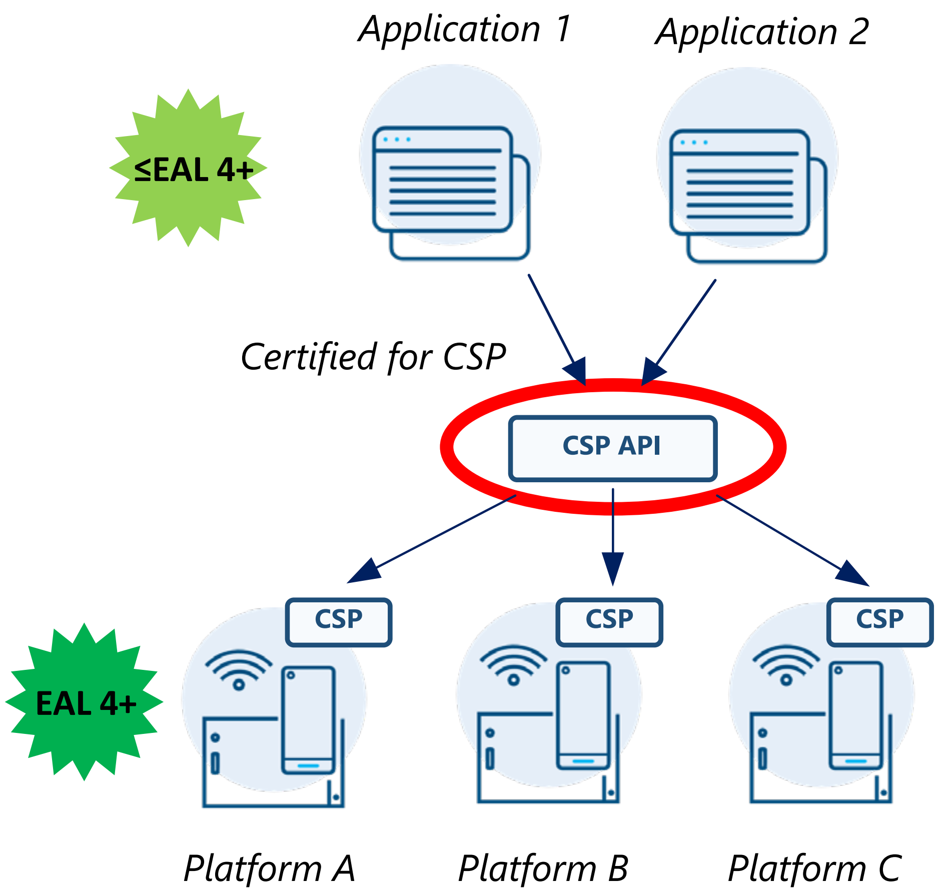
Payment: Digital Finance

Ticketing: Digital Travel Credentials

Applications require secure implementations of identical cryptographic building blocks:

- Secure key management for ID and Auth
- Secure storage for user data
- Authentication protocols
- Secure and Trusted channels, e.g. to back-end
- Signatures
- Secure Personalization
- Secure Erase and Termination

CSP Concept: More than a Crypto-Lib !



CSP goals:

- Separation of business logic and crypto
- Ease scalable certification efforts (eliminate composite certification!)
- Provide complete building blocks and protocols for the full life cycle
- Prevent misuse of cryptography

CSP Functional Requirements (excerpt):

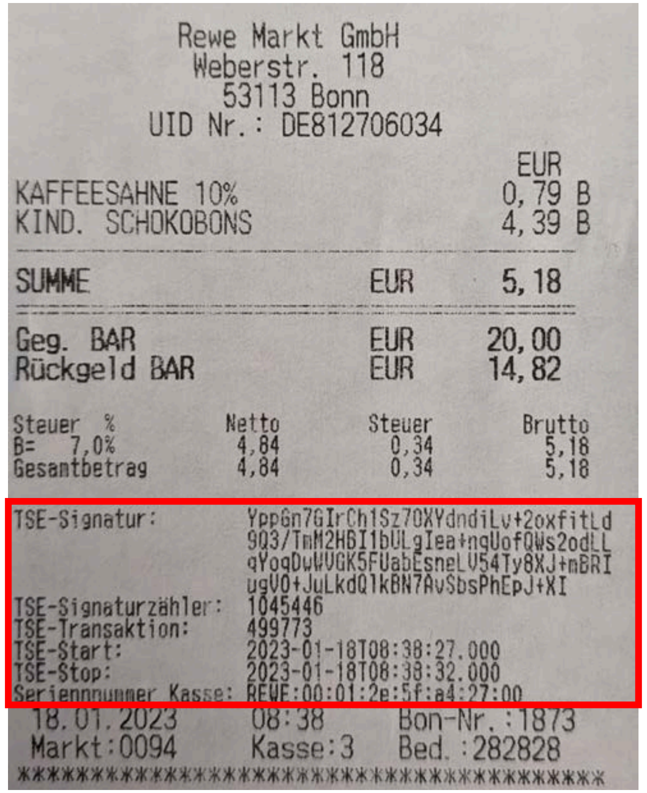
(derived from BSI-CC-PP-0104 & BSI TR-03181 CSP2)

- key management
- identification and authentication
- session handling
- signing
- secure storage (wrapped import/export)
- encryption
- attestation

CSP utilization since 2020

Security modules (TSS / TSE) for cash registers in Germany:

- > 2 M cash registers
- > 2.000 cash register manufacturers
- 6 certified TSS (+ variants)
- 4 certified CSP, incl. 2 SE (1 JavaCard)



```
                  Rewe Markt GmbH
                   Weberstr. 118
                    53113 Bonn
                UID Nr.: DE812706034
                                        EUR
KAFFEESAHNE 10%                      0,79 B
KIND. SCHOKOBONS                     4,39 B
-------------------------------------------
SUMME                       EUR       5,18
-------------------------------------------
Geg.  BAR                   EUR      20,00
Rückgeld BAR                EUR      14,82

Steuer  %         Netto      Steuer      Brutto
B=   7,0%          4,84        0,34        5,18
Gesamtbetrag       4,84        0,34        5,18

TSE-Signatur:           YppGn7GIrCh1Sz70XYdndiLv+2oxfitLd
                        9Q3/TmM2HBI1bULgIea+ngUofQWs2odLL
                        qYoqDwWVGK5FUabEsneLV54Ty8XJ+mBRI
                        ugV0+JuLkdQ1kBN7AvSbsPhEpJ+XI
TSE-Signaturzähler:     1045446
TSE-Transaktion:        499773
TSE-Start:              2023-01-18T08:38:27.000
TSE-Stop:               2023-01-18T08:38:32.000
Seriennnummer Kasse:    REWE:00:01:2e:5f:a4:27:00
  18.01.2023          08:38       Bon-Nr.:1873
  Markt:0094          Kasse:3     Bed.:282828
******************************************
```

Thank you for your attention!

Contact

Tobias Damm
Division TK11 – Chip Security

Tobias.damm@bsi.bund.de

Federal Office for Information Security (BSI)
Godesberger Allee 87
53175 Bonn
www.bsi.bund.de

BSI as the Federal Cyber Security Authority shapes information security in digitalization through prevention, detection and response for government, business and society.

Current State, Literature, and Further Readings

SAM & CSP: From Concepts to Standards

Current state on SAM:

- SAM Requirements document published by GSMA in June 2021
- SAM Configuration (technical specification document) in final phase at GlobalPlatform
- SAM PKI and PKI policy in discussion with multiple actors

Current state on CSP:

- BSI Technical Guideline TR-03181 – CSP2 published in June 2023
- technical specification currently under work at GlobalPlatform, to be published as amendment to the GP Card Specification, „Amendment N – CSP“

SAM & CSP: Literature

- BSI overview page with links to BSI SAM Position Paper, CSP Whitepaper, BSI TR-03181
  https://www.bsi.bund.de/dok/secureelements
- SAM Requirements document by GSMA
  https://www.gsma.com/newsroom/gsma_resources/sam-01-secured-applications-for-mobile-requirements/
- SAM Position Paper by Eurosmart
  https://www.eurosmart.com/european-mobile-identity-recommendations-on-sam-technology/
- SAM Position Paper by TCA
  https://trustedconnectivityalliance.org/wp-content/uploads/2023/02/TCA_SAM_PositionPaper_FINAL.pdf
- Digital Wallet
  https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en