Federal Office
for Information Security

Hardware-Based Trust Anchors for European eID Technologies

Market Reach and Interoperability via Standardisation: Cryptographic Service Provider and Secured Applications for Mobile

Heinfried Cznottka, achelos GmbH

Dr. Ullrich Martini, G+D ePayments GmbH

Dr. Tobias Damm, BSI Division TK11

Dr. Tobias Fiedlschuster, BSI Division SZ34

Omnisecure 2024

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

Motivation

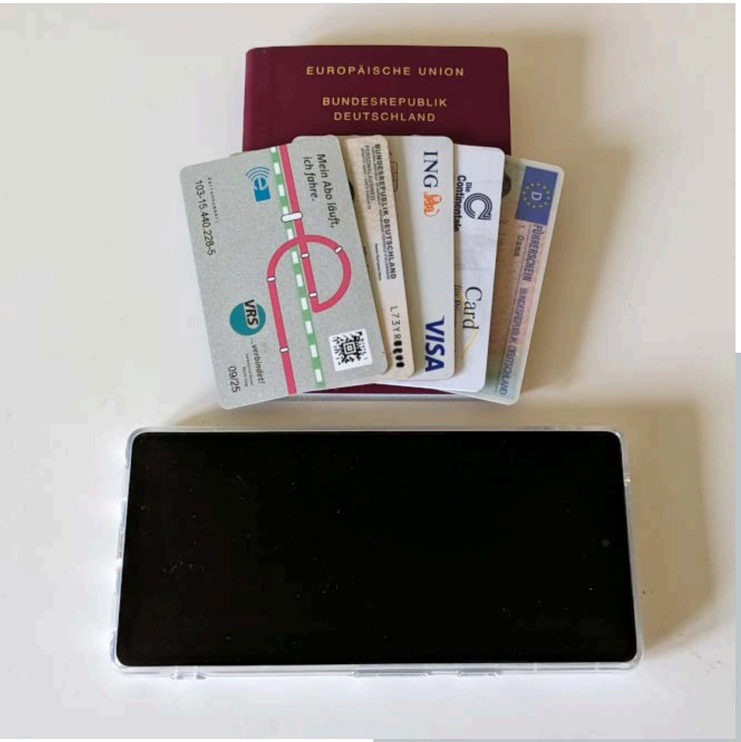
Digital Identities on mobile platforms …

Goals:

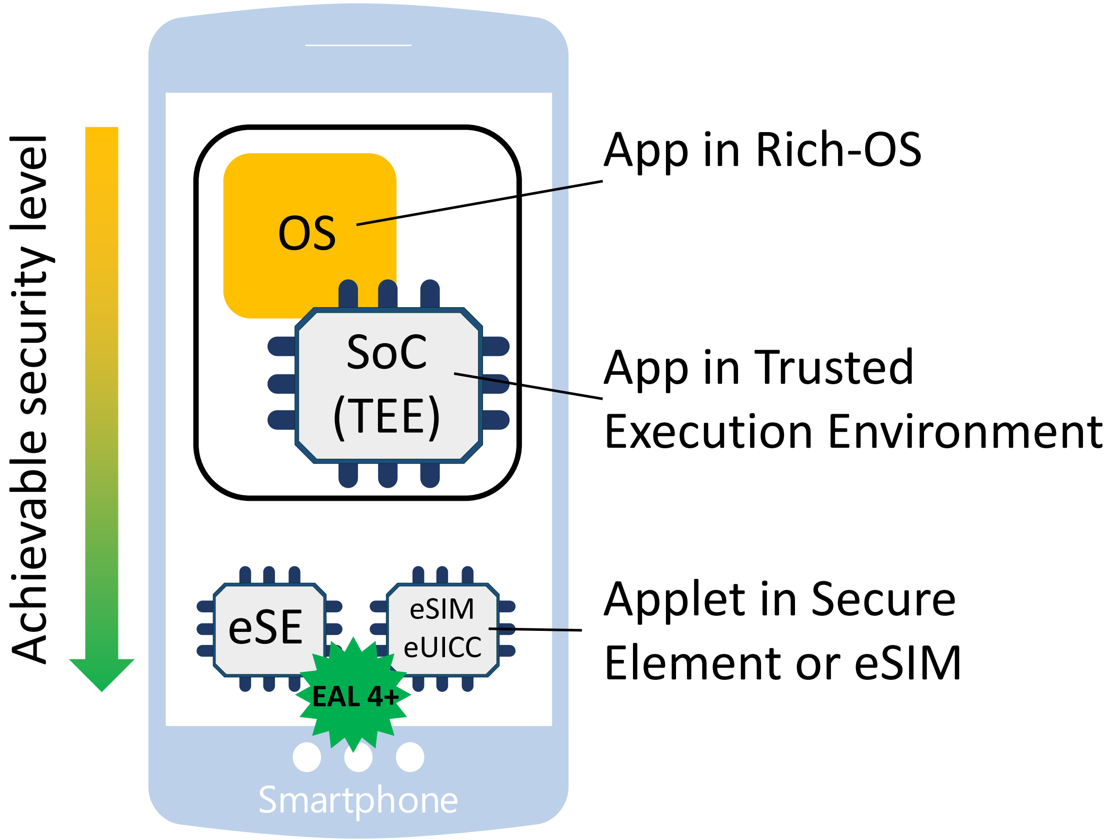
- Ease of use
- High functionality
- Broad availability
- New use cases
- Much more …

Common questions:

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



… designed secure !



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

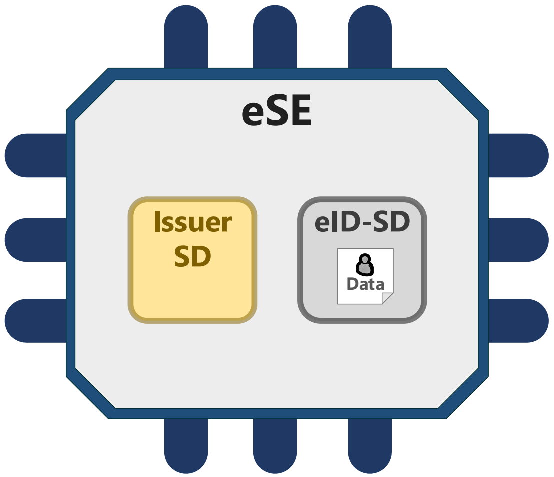
> *The Secured Applications for Mobile specification defines a capability allowing cellular connected Devices to use a wide range of secured applets within an eUICC. Such applets can be managed by a service provider, and may be paired with applications running in the Device itself.*
>
> *- GSMA SAM v1.1*

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

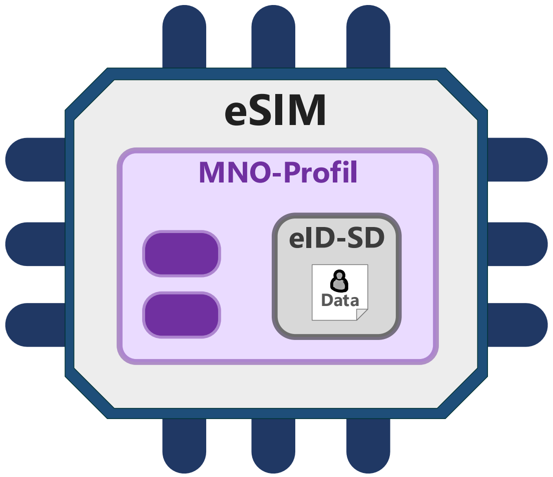
eID in eSE



Dependencies on OEM

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

eID in MNO-Profile on eSIM



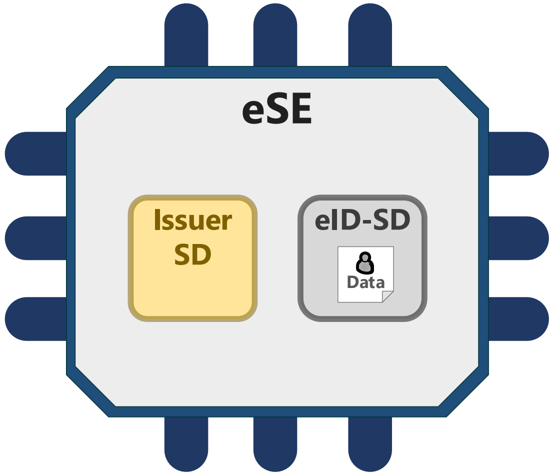
Dependencies on MNO

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.

SAM as foundation for third party applications on eSE / eSIM

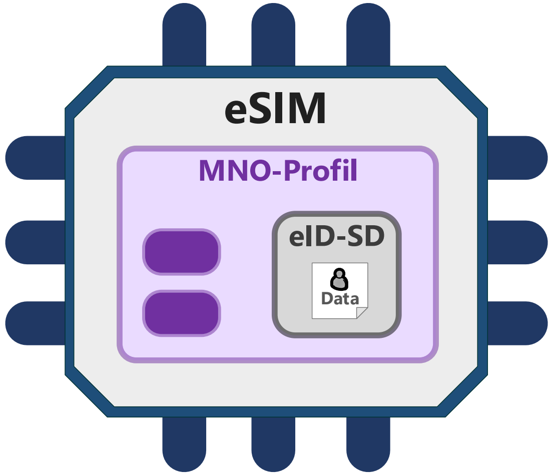
eID in eSE



Dependencies on OEM

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

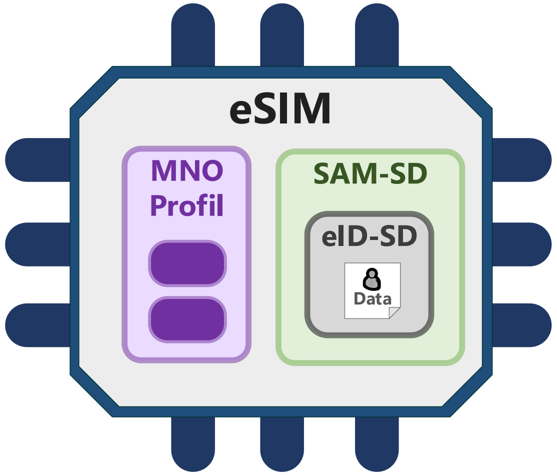
eID in MNO-Profile on eSIM



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

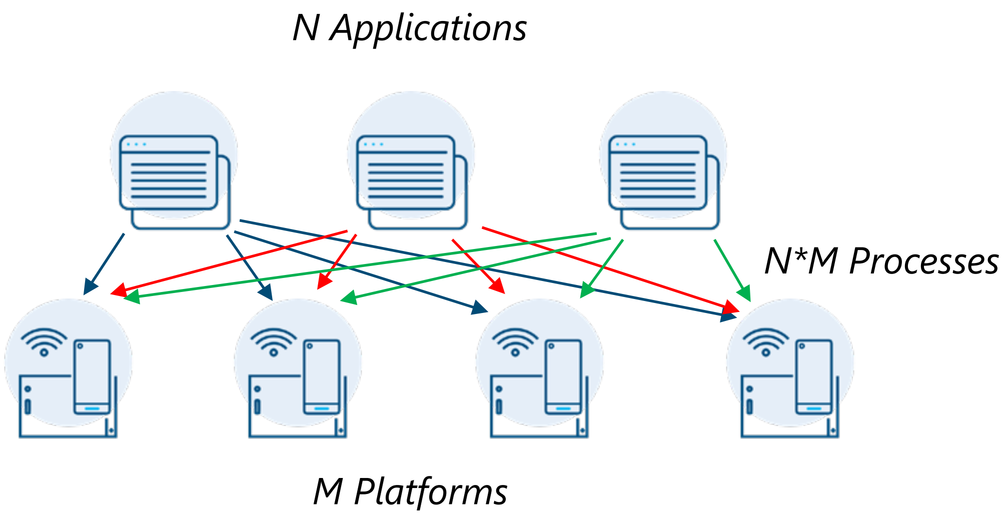
② **Cryptographic Service Provider (CSP)**

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

Scalability of security certifications

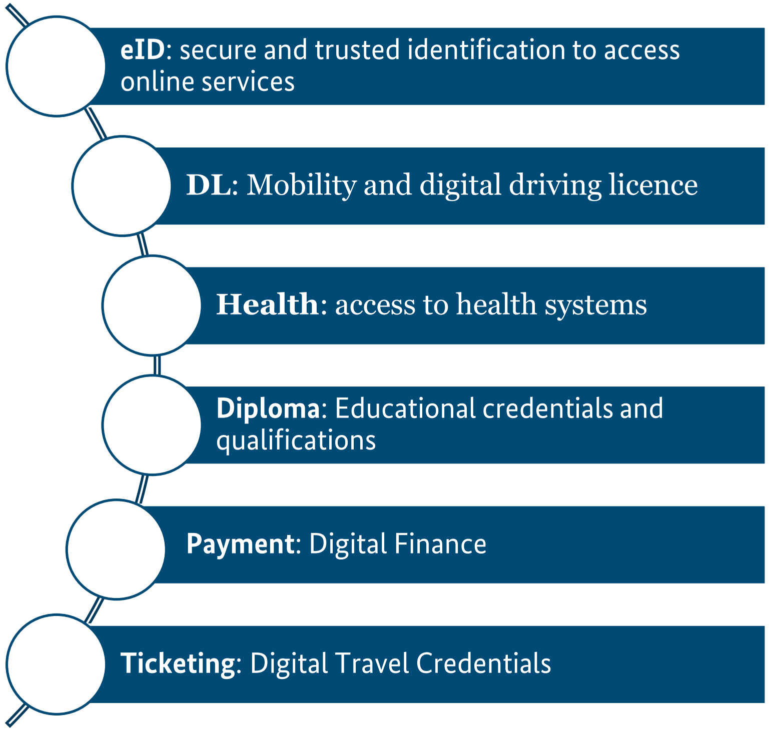
‘Composite evaluation’ for high assurance classes

- 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

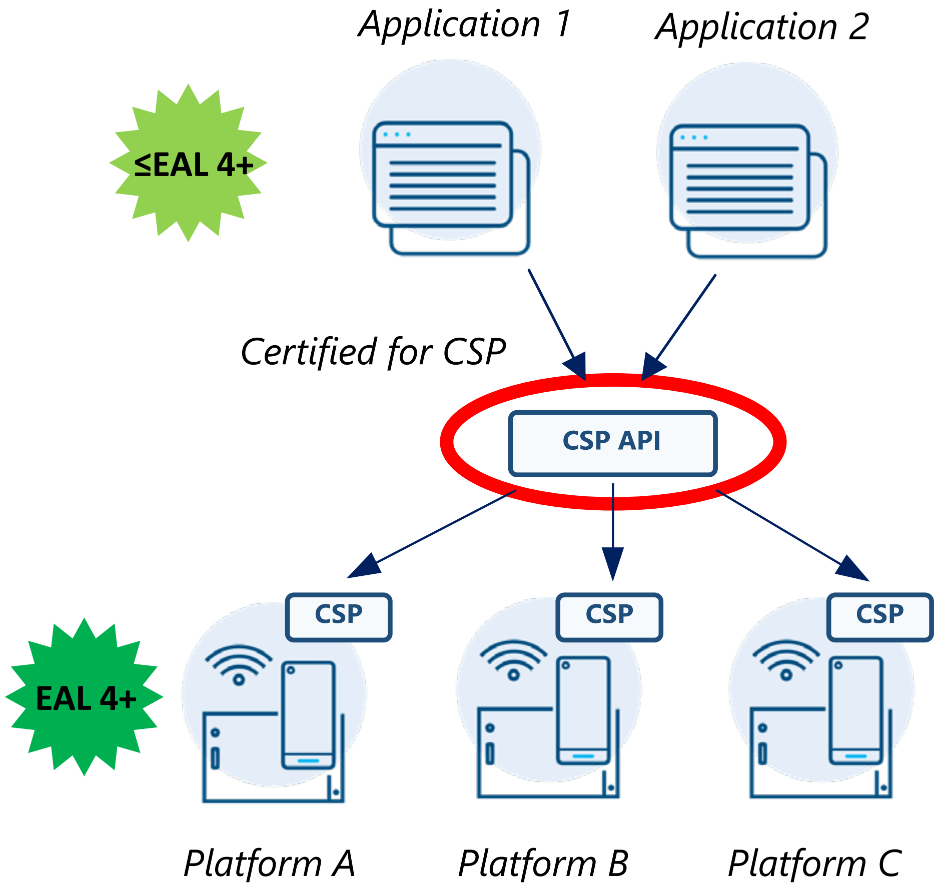
Payment: Digital Finance

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):

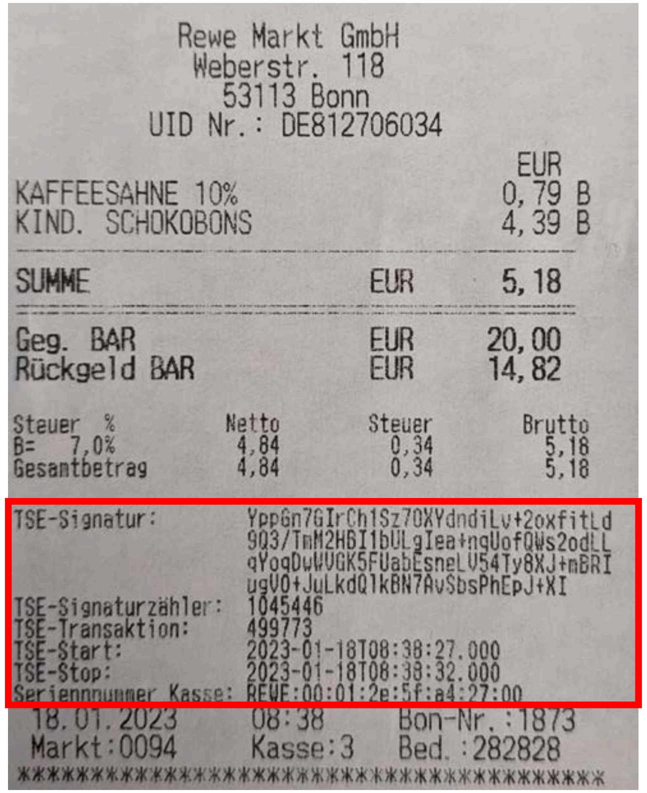
(derived from BSI-CC-PP-0104 & BSI TR-03181 CSP2)

- 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!

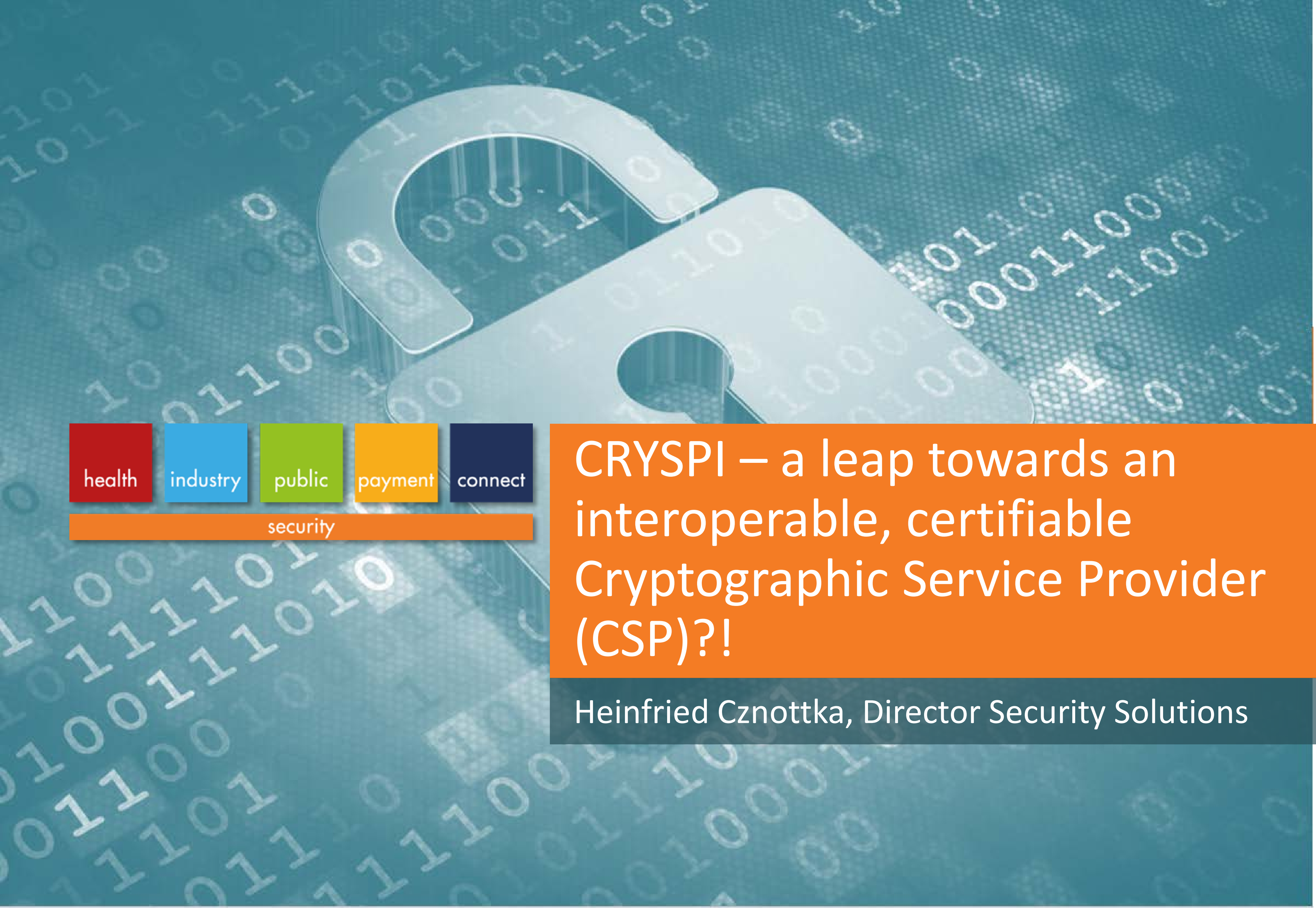
Contact

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.



achelos

health industry public payment connect

security

CRYSPI – a leap towards an interoperable, certifiable Cryptographic Service Provider (CSP)?!

Heinfried Cznottka, Director Security Solutions

Integriertes Managementsystem DQS ISO 9001 ISO/IEC 27001

Allianz für Cyber-Sicherheit Partner

SecurITy made in Germany

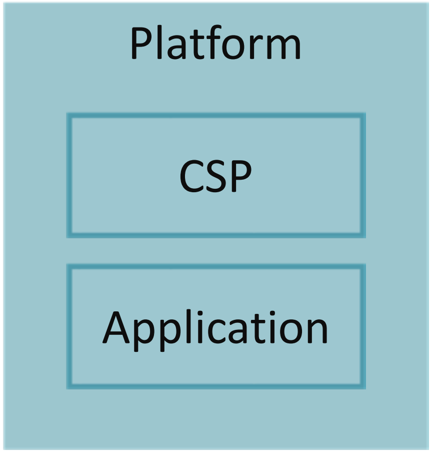
Trust Seal www.teletrust.de/itsmig

CRYSPI – What is CRYSPI?

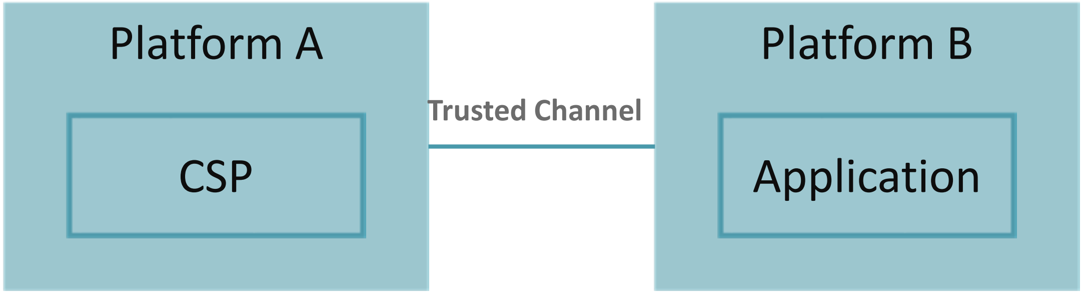
- BSI project
  - Prototypical implementation of a Cryptographic Service Provider (CSP)
  - CRYSPI is based on the draft of TR-CSP2 and
  - the existing security specifications (BSI-CC-PP-CSP)
- Main goal and motivation
  - Creation of a generic API interface description, test specification and executable tests on API level
  - Support implementation, certification and interoperability for secure applications

What has been achieved so far (1/3) ?

- CSP uses a generic approach, platform mode, client-server mode
- Focus on platform mode



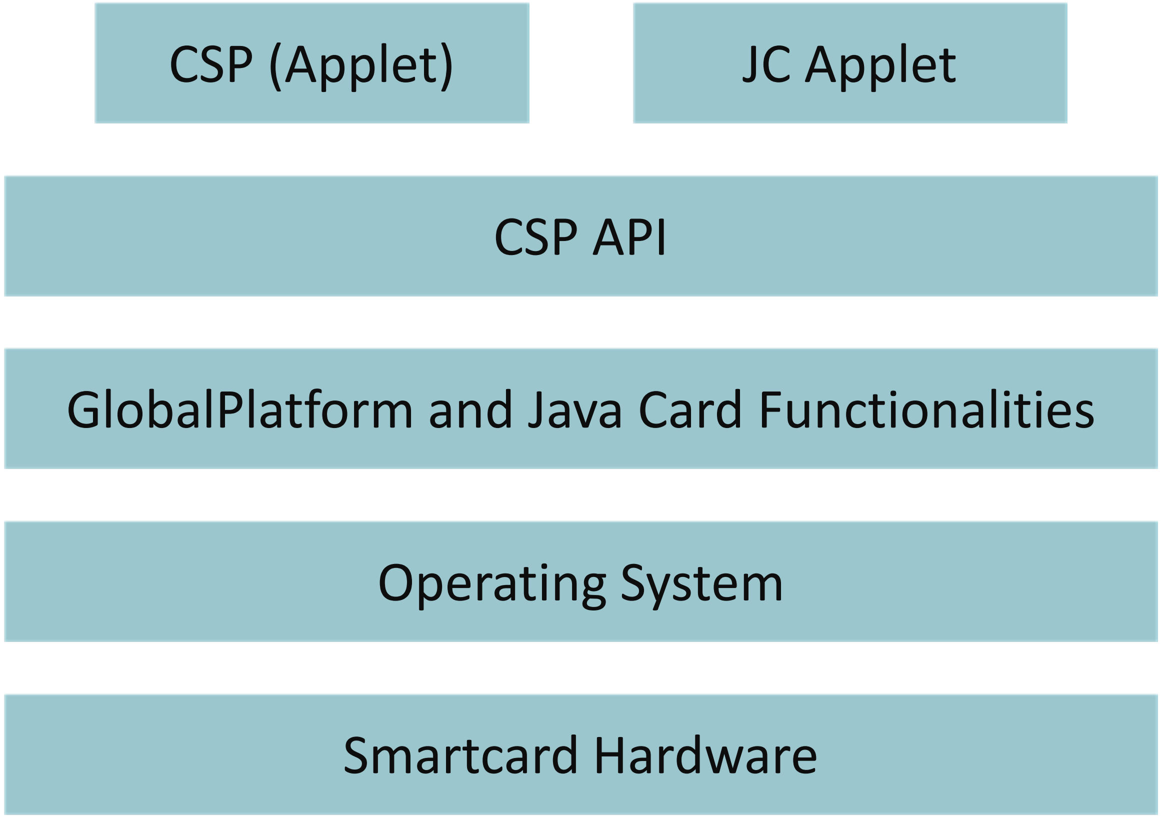
Platform mode



Client-Server mode

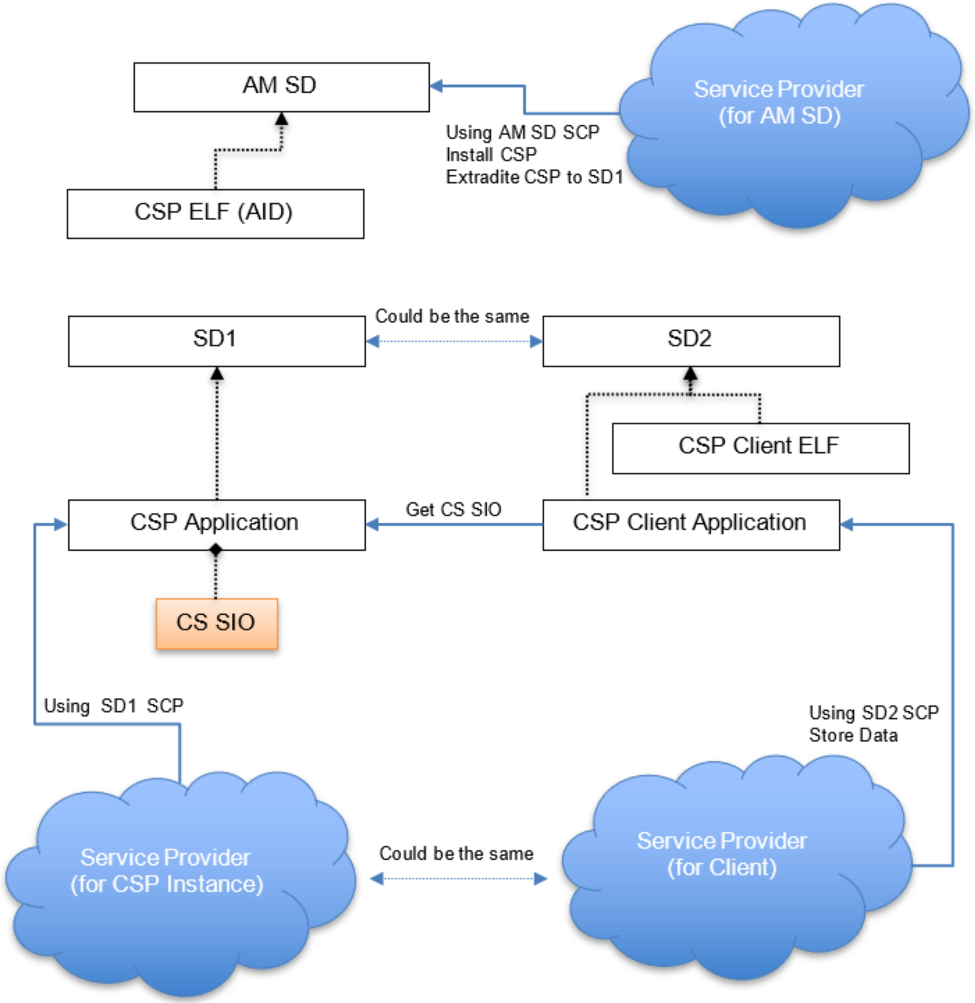
What has been achieved so far (2/3) ?

- CSP uses a secure element as basis
- Use/Reuse of technological standards from Java Card and GlobalPlatform
- CSP client applet as Java Card applet



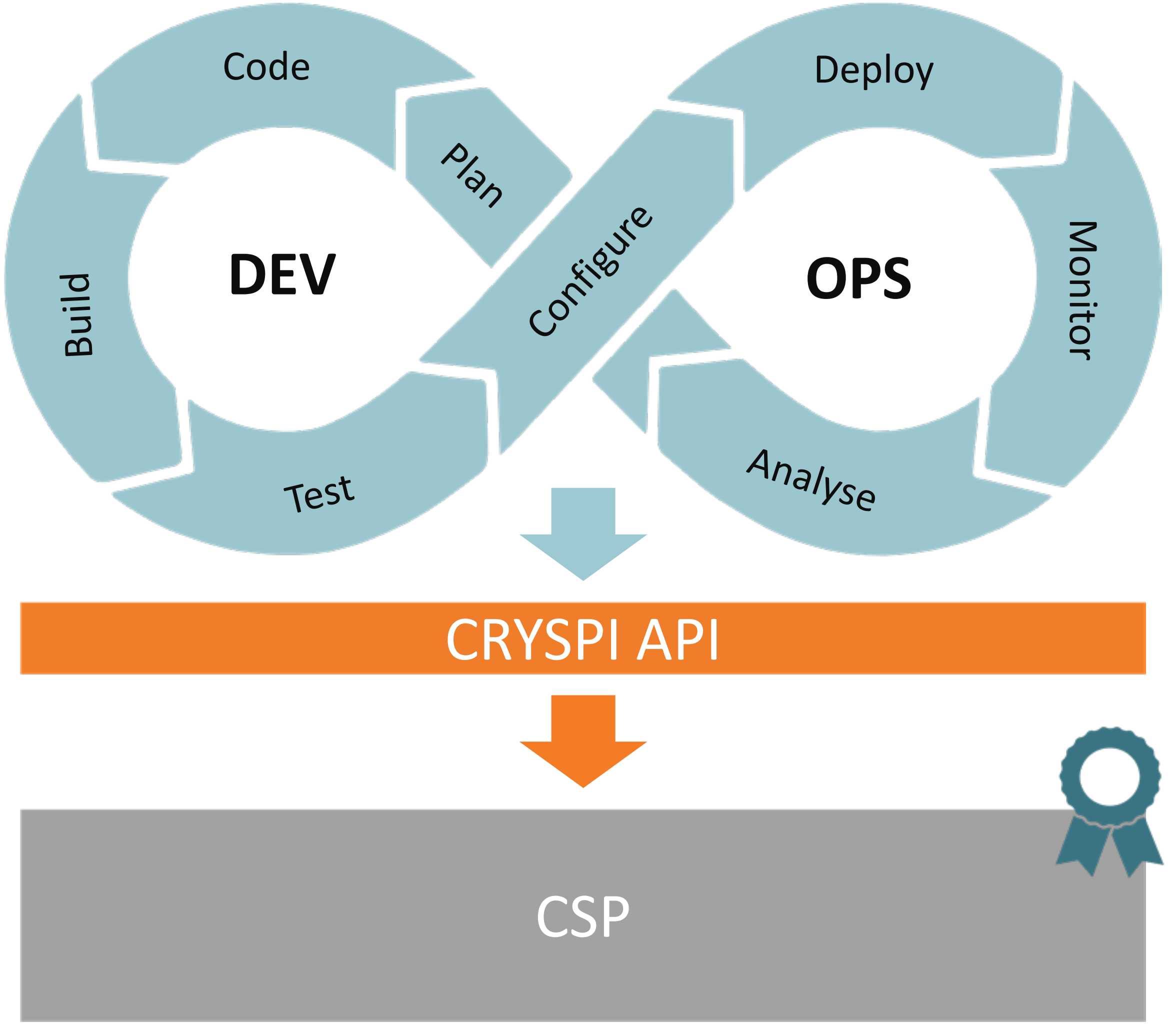
What has been achieved so far (3/3) ?

- System management architecture
  - Hardware and vendor neutral approach
  - Security domains act as the on-card representatives of off-card authorities
  - Security domains ensure separation between card issuer and service providers



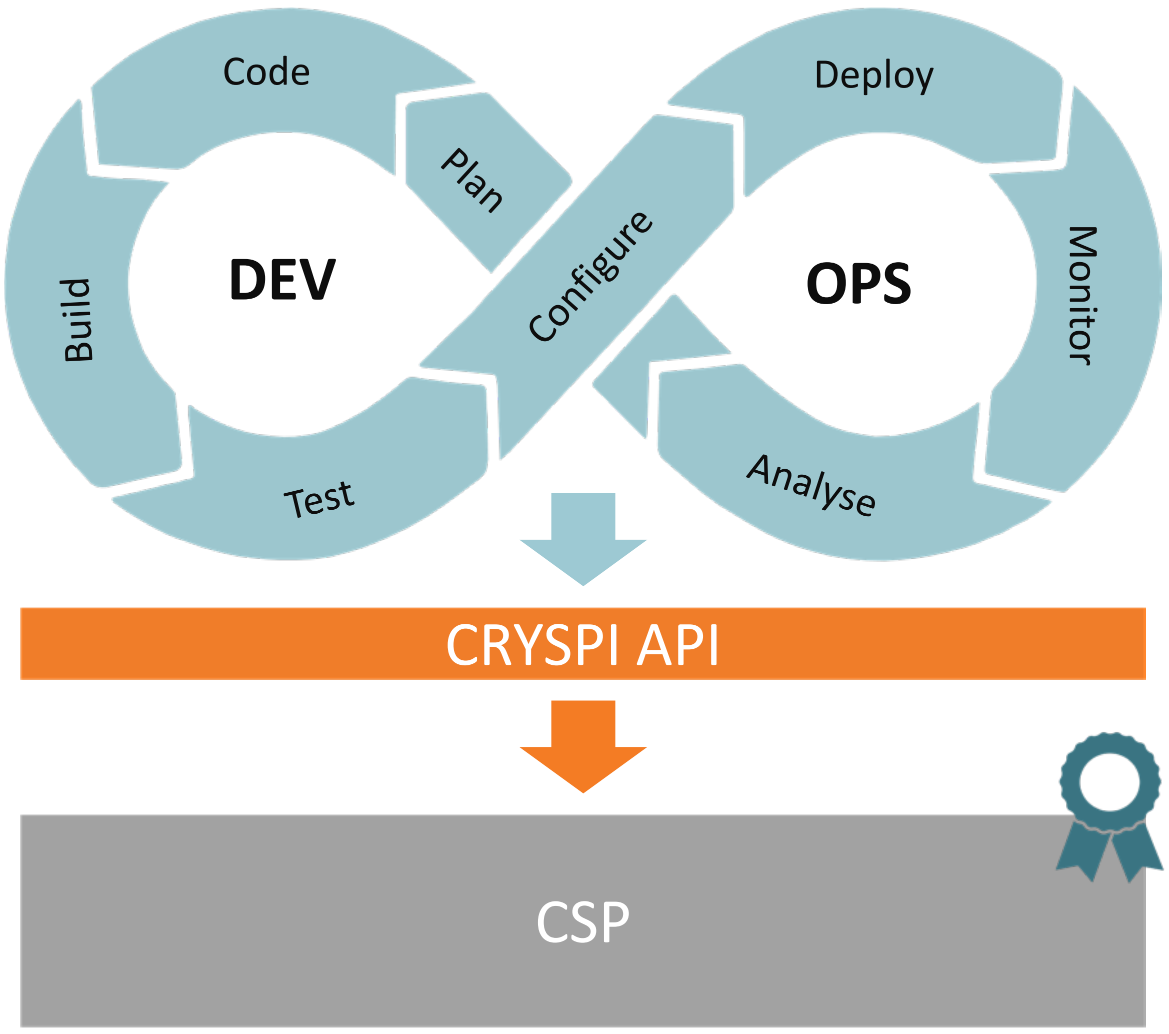
Requirements for developing secure applications

- Issues
  - Fast development cycles vs. need for certification
  - Lacking know how about crypto functionality and usage
  - High efforts for implementation of crypto functionality
  - Need to follow protection profiles (PP) and technical guidelines (e.g. TRs)
  - Time consuming certification process
- Solution
  - Secure foundation for Crypto functionality



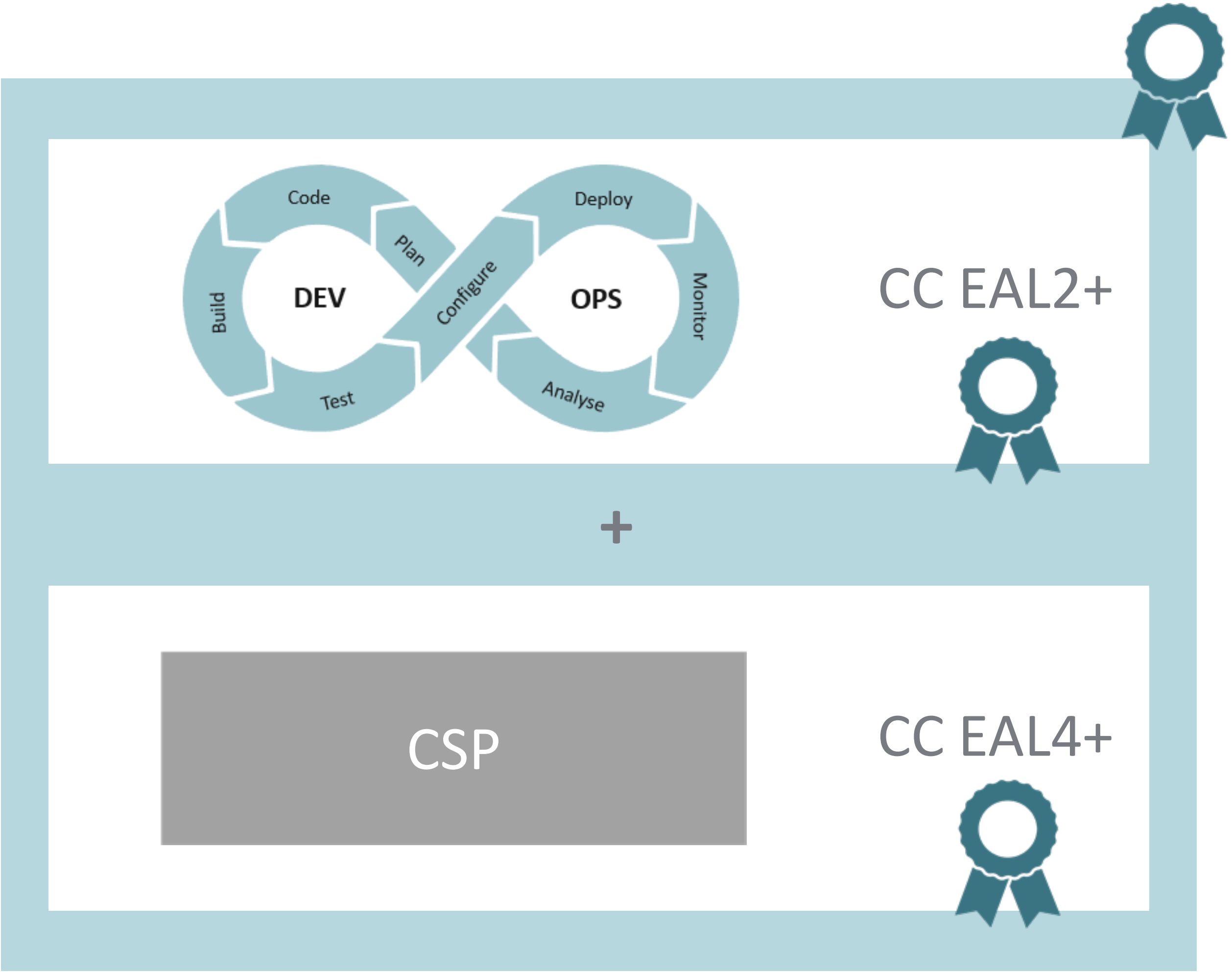
How does CRYSPI help with implementation?

- Faster implementation
- "Easier" usage of an API rather than developing crypto functionality
- No detailed crypto know how necessary
- Domain knowledge powers the application logic



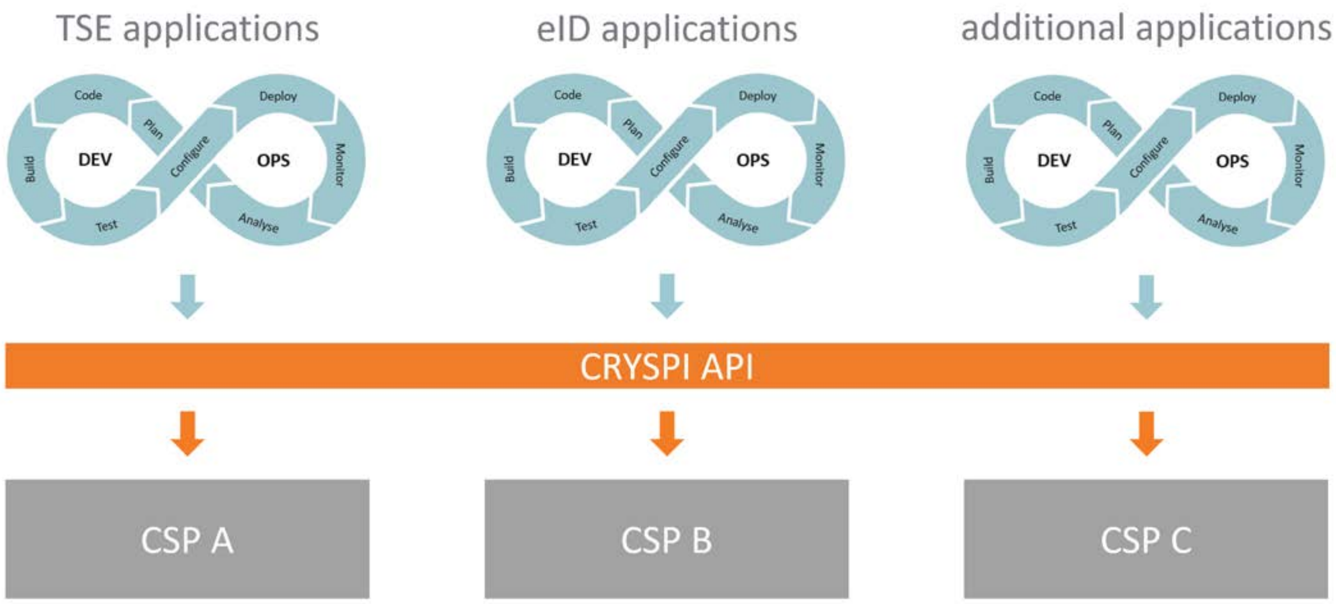
How does CRYSPI help with certification?

- Coordinated certification
- Application logic can be certified (e.g. EAL 2) independently from the CSP (EAL 4+)
- Time and money for the certification can be reduced significantly



How does CRYSPI help with interoperability?

- The application logic can be based on different implementations of the CSP
- Implementation can support different platforms and architectures



TSE applications

eID applications

additional applications

CRYSPI API

CSP A

CSP B

CSP C

Conclusion

- CRYSPI helps to simplify and accelerate the implementation and independent security certification of applications based on a CSP while ensuring interoperability of applets for different CSPs!

- The API is published as open source
- The project can only succeed if the API is used!

Head office	achelos GmbH | Vattmannstraße 1 | 33100 Paderborn | Germany
Management board	Kathrin Asmuth, Thomas Freitag
Company	Manufacturer-independent system house for cyber security and digital identity management in Paderborn, founded in May 2008
Competences	Comprehensive IT security expertise with a specialist knowledge in cryptography, embedded development, PKI, telematics infrastructure (TI), eSIM management
Target markets	Security, health, industry, public, payment, connect
Offer	System integration, consulting, development, testing, security engineering, certification support, managed services, test suites & simulations, e-SIM management
Focus	Comprehensive IT security topics and industrial solutions for the national and international market
Customers | Partner	Private companies, government institutions and organizations with a need for cyber security solutions in security critical application fields

Vielen Dank! | Thank you!

Heinfried Cznottka – heinfried.cznottka@achelos.de
achelos GmbH
Vattmannstraße 1 | 33100 Paderborn | GERMANY
T +49 5251 14212-0 | info@achelos.de

Mobile Payment Applications

- Session: Hardwarebasierte Vertrauensanker für die europäische eID Technologie
- Dr. Ullrich Martini, G+D ePayments GmbH
- Omnisecure Berlin, 22.01.2024

Mobile Payment Applications

- Branded
  - Good, UI owned by service provider
- Secure
  - Good, lab-tested and certified
- Personalized
  - Challenge, because not delivered physically
- Convenient

➢ Ready for payment applications

Vision

- Standardized
- Secure personalization
- Full branding on iOS
- Unified solution for iOS and Android

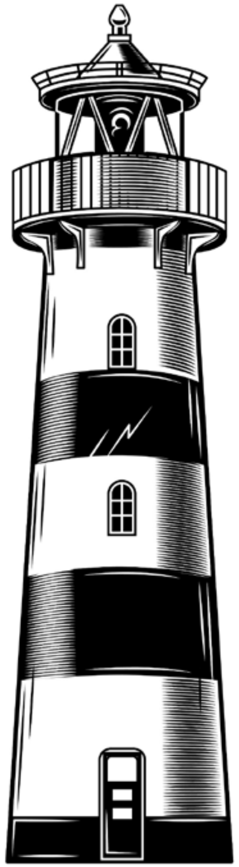


Bild von pch.vector auf Freepik

Way Forward

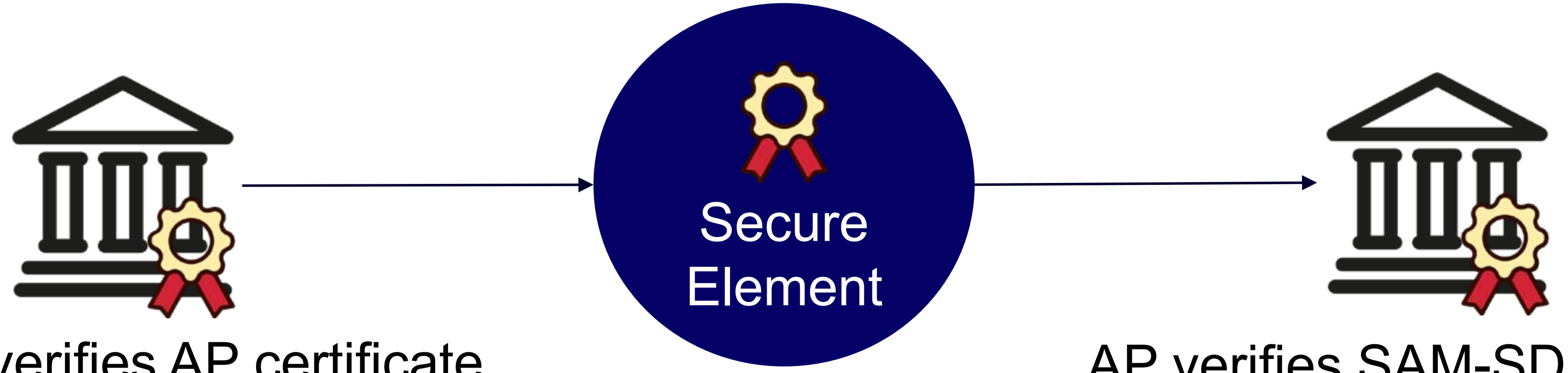
- Rely on specification: ISO, GlobalPlatform, JavaCard Forum, GSMA
- Secured Application for Mobile "SAM-SD" (GSMA specification)
  - Reliable vendor-independent end-to-end specification
  - Secure installation of applet and key material
  - Tested independently of vendors
- Will be ready for online rollout
- Requires dedicated security hardware in the device
  - Embedded SIM (eSIM)
  - Dedicated chip

Technical Basis

- JavaCard hardware and OS
  - EAL4+ or better
  - Embedded SIM
  - Other Embedded Secure Element
- Pre-personalized by silicon vendor, root of certificate chain
- GlobalPlatform SAM configuration
  - Amd A: Certificate verification; Key Generation inside Security Hardware
  - Amd F: Certificate verification; Secure Channel to Application Provider
  - Amd N: CSP; Improved internal cryptographic API inside Security Element
- Specified by GSMA

Lifecycle of a SAM-SD

- Silicon vendor pre-personalizes the SAM-SD with keys and certificates
- Application Provider performs Mutual Authentication with SAM-SD
  - Secure Channel between SAM-SD and Application Provider
- Application Provider (AP) installs and personalizes its own Security Domain (APSD)
  - Secure Channel between APSD and Application Provider

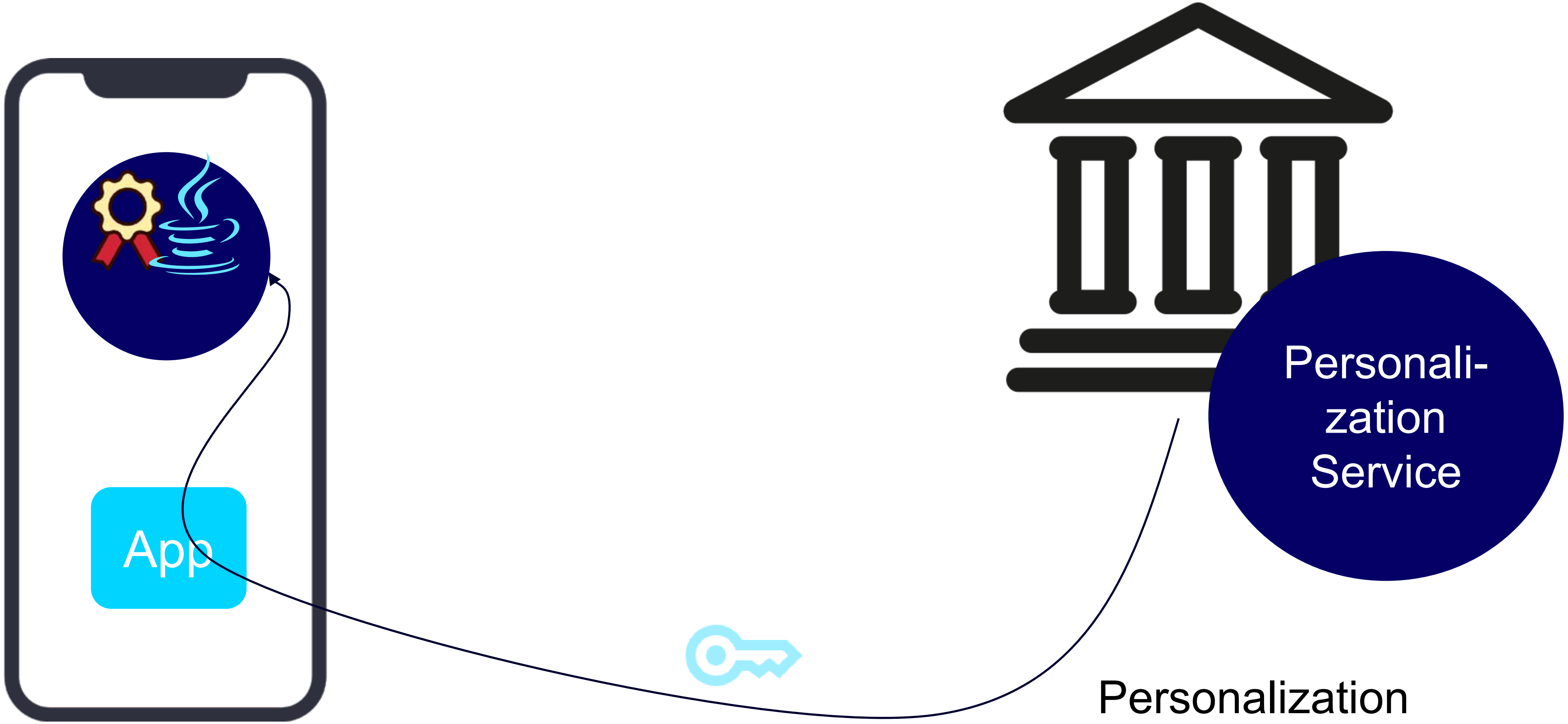


Secure Element

SAM-SD verifies AP certificate

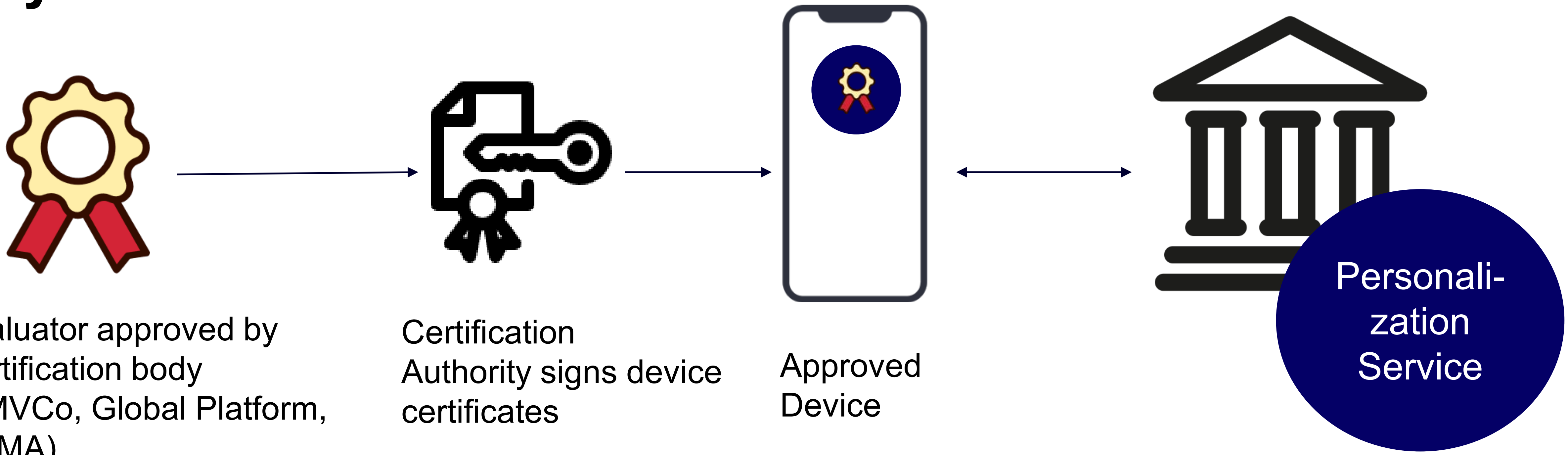
AP verifies SAM-SD certificates

Personalization



Personalization
Requires Mutual Trust
between Service and Device

Why Is It Secure?



Evaluator approved by Certification body (EMVCo, Global Platform, GSMA)

Certification Authority signs device certificates

Approved Device

Personali-zation Service

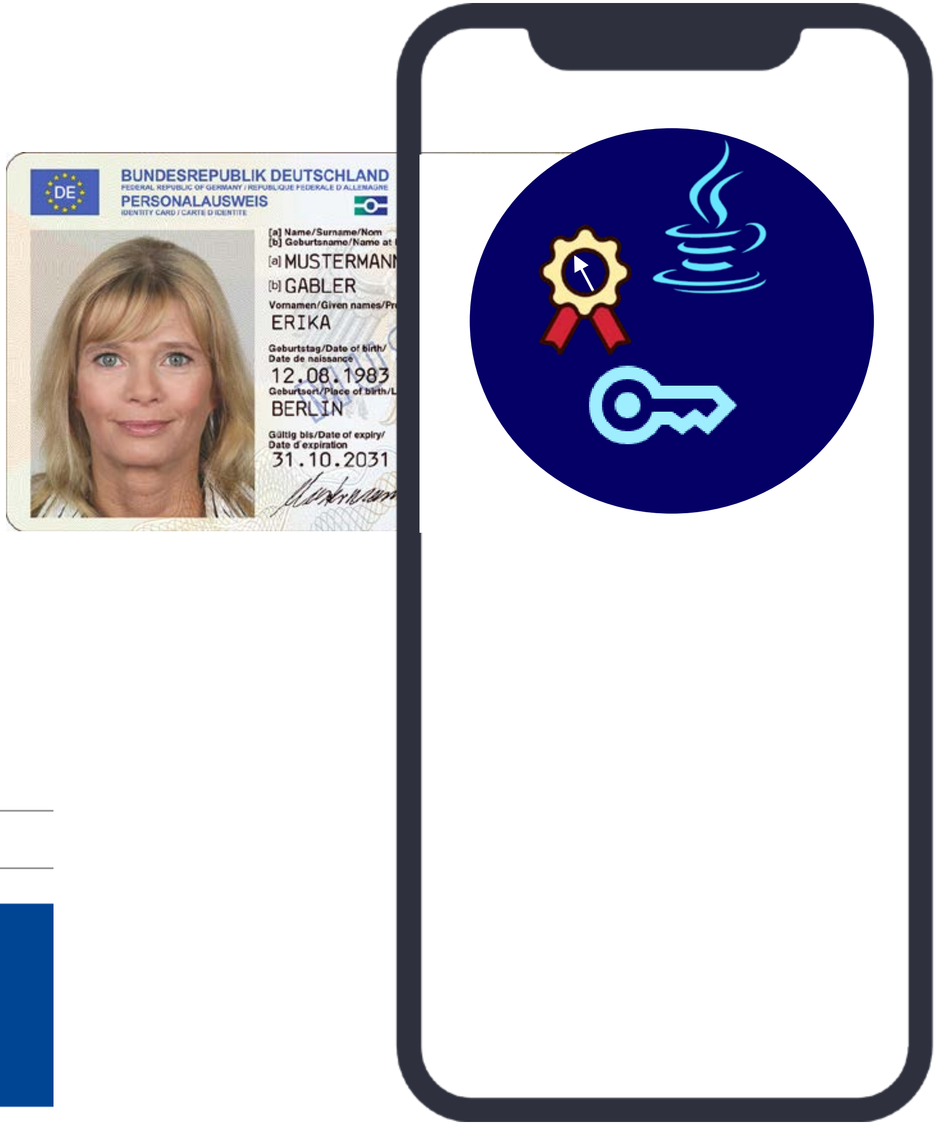
Bank issues digital payment card if certificates are correct

Identification Challenge

- Need to connect the pseudonymous internet user to a banking customer
- Customers cannot be asked to visit a branch office
- Need internet-native solution

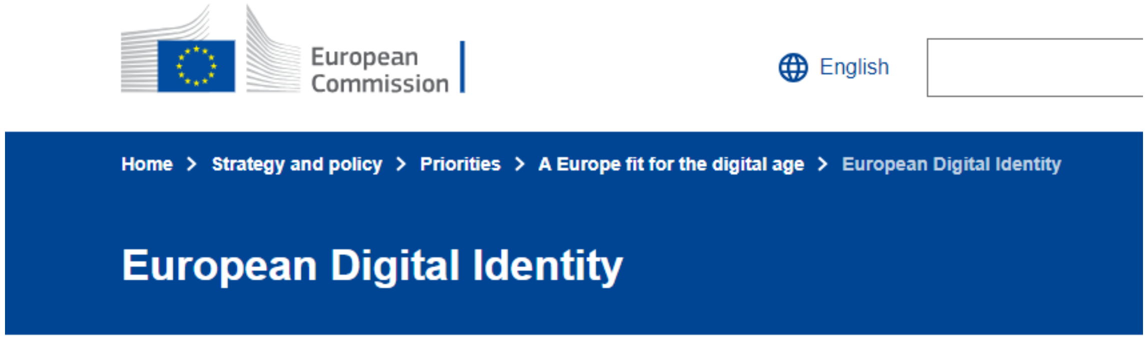
European Digital Identity

- Identity established by the local government
- Requires interaction between application backend and eID provider



BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D ALLEMAGNE
PERSONALAUSWEIS
IDENTITY CARD / CARTE D IDENTITE

[a] Name/Surname/Nom
[b] Geburtsname/Name at
[a] MUSTERMANN
[b] GABLER
Vornamen/Given names/Pr
ERIKA
Geburtstag/Date of birth/
Date de naissance
12.08.1983
Geburtsort/Place of birth/L
BERLIN
Gültig bis/Date of expiry/
Date d'expiration
31.10.2031



Home > Strategy and policy > Priorities > A Europe fit for the digital age > European Digital Identity

European Digital Identity

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Dr. Ullrich Martini

ullrich.martini@gi-de.com

Giesecke+Devrient ePayments GmbH

Prinzregentenstraße 161
81677 München, Germany

Current State, Literature, and Further Readings

Federal Office
for Information Security

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

Contact (session moderator)

Tobias Fiedlschuster
Division SZ34

tobias.fiedlschuster@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.