Federal Office
for Information Security

Outlook of the future German EUDI deployment

26.04.2023

Outline

eID Advantages

Status Quo

Architecture

Deployment

Hardware Security

The eID Advantages at a Glance

Citizens, companies and public entities benefit from the deployment of an secure eID

- ✓ **User-friendly:** Enables easy and secure online business and public transactions - anytime, anywhere.
- ✓ **Authentic:** Correct data transmission! Typing or recognition errors are impossible.
- ✓ **Secure:** The eID function protects personal identification data on the internet! Even if the eID is lost, access is impossible without knowledge of the PIN.
- ✓ **Fast**: Instant ID check
- ✓ **Cost-efficient**: No transport costs, no waiting times!

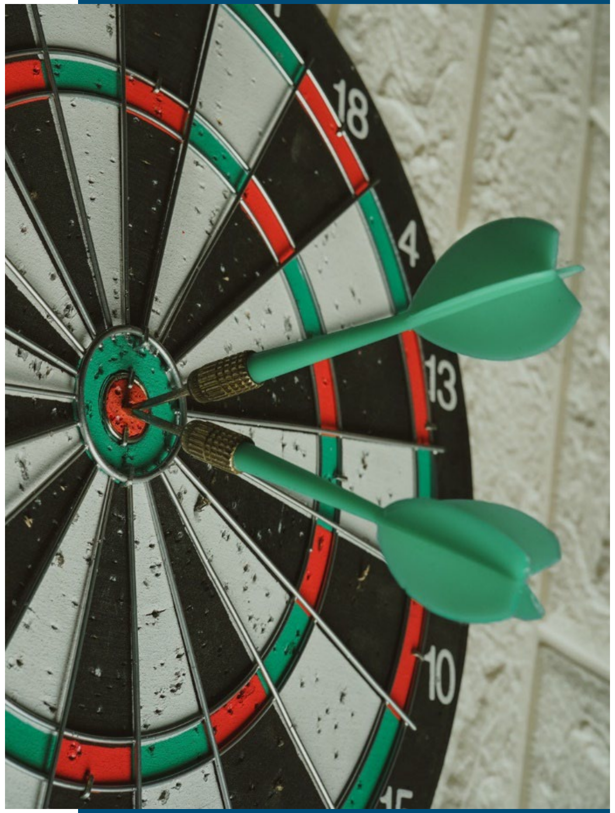
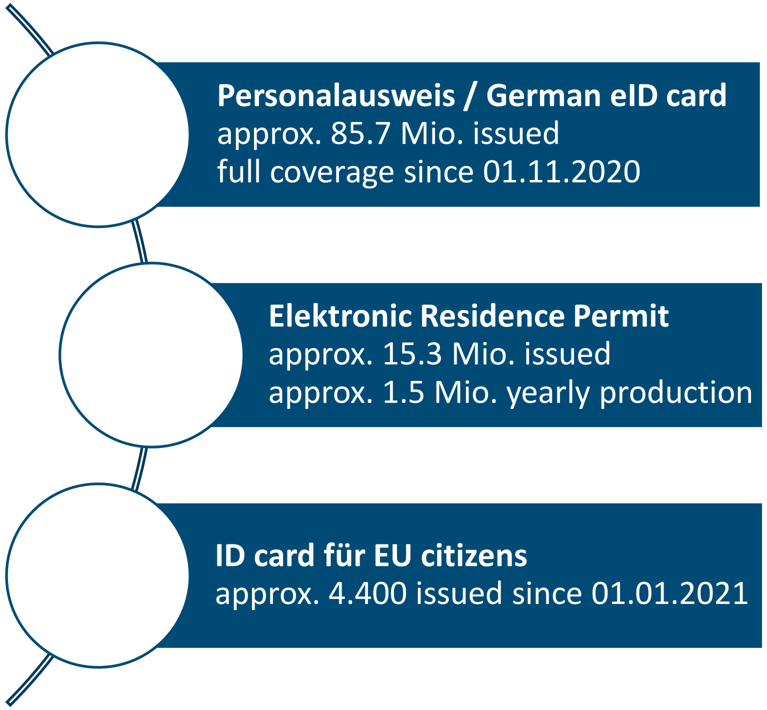


Bild: Alif Kusuma; unsplash

Status Quo - some historical data

German eID card – Facts & Figure



Personalausweis / German eID card
approx. 85.7 Mio. issued
full coverage since 01.11.2020

Elektronic Residence Permit
approx. 15.3 Mio. issued
approx. 1.5 Mio. yearly production

ID card für EU citizens
approx. 4.400 issued since 01.01.2021

BUNDESREPUBLIK DEUTSCHLAND
PERSONALAUSWEIS
L01
MUSTERMANN
GABLER
ERIKA
12.08.1964 DEUTSC
BERLIN
31.10.2029

BUNDESREPUBLIK DEUTSCHLAND
PERSONALAUSWEIS
L01X00T47
MUSTERMANN
GABLER
ERIKA
12.08.1983 DEUTSCH
BERLIN
01.08.2031
938568

*

AUFENTHALTSTITEL Y70101V03
MUSTERMANN
Erika
F AUS 12 08 1964
30 04 2030
NIEDERLASSUNGS-
ERLAUBNIS
9
PASS(ERSATZ) 874593074 BIS 30 04 2030
248848
RESIDENCE PERMIT

BUNDESREPUBLIK DEUTSCHLAND N701001V1
eID-KARTE
MUSTERMANN
Erika
12 08 1964 31 10 2029
eID-KARTE FÜR UNIONSBÜRGERINNEN/
UNIONSBÜRGER UND ANGEHÖRIGE DES
EUROPÄISCHEN WIRTSCHAFTSRAUMS
925732
eID card for Union citizens and EEA nationals
carte eID pour citoyens de l´UE et ressortissants de l´EEE
987654321

Bild: Arthimedes / shutterstock.com

*Design since 02.08.2021

Figures as of 01.2022

Status Quo – historical timeline

Online-Identification goes mobile - Timeline

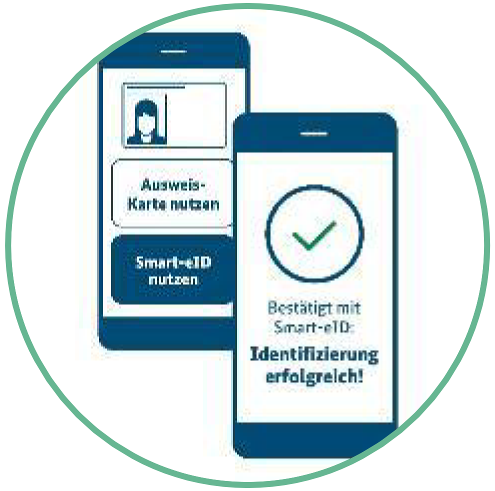
2010

Launch of the electronic German ID card on 01.11.2010. With the chip in the ID card, secure electronic identification on the Internet was possible for the first time.

2017

Since March 2017, citizens have the possibility to perform online identification via the smartphone's NFC interface without additional reader hardware.

2023

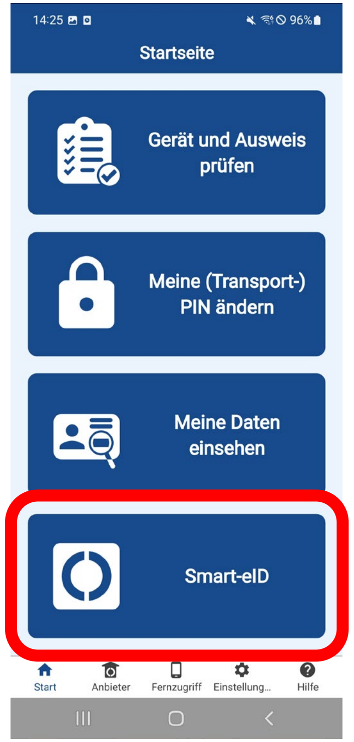


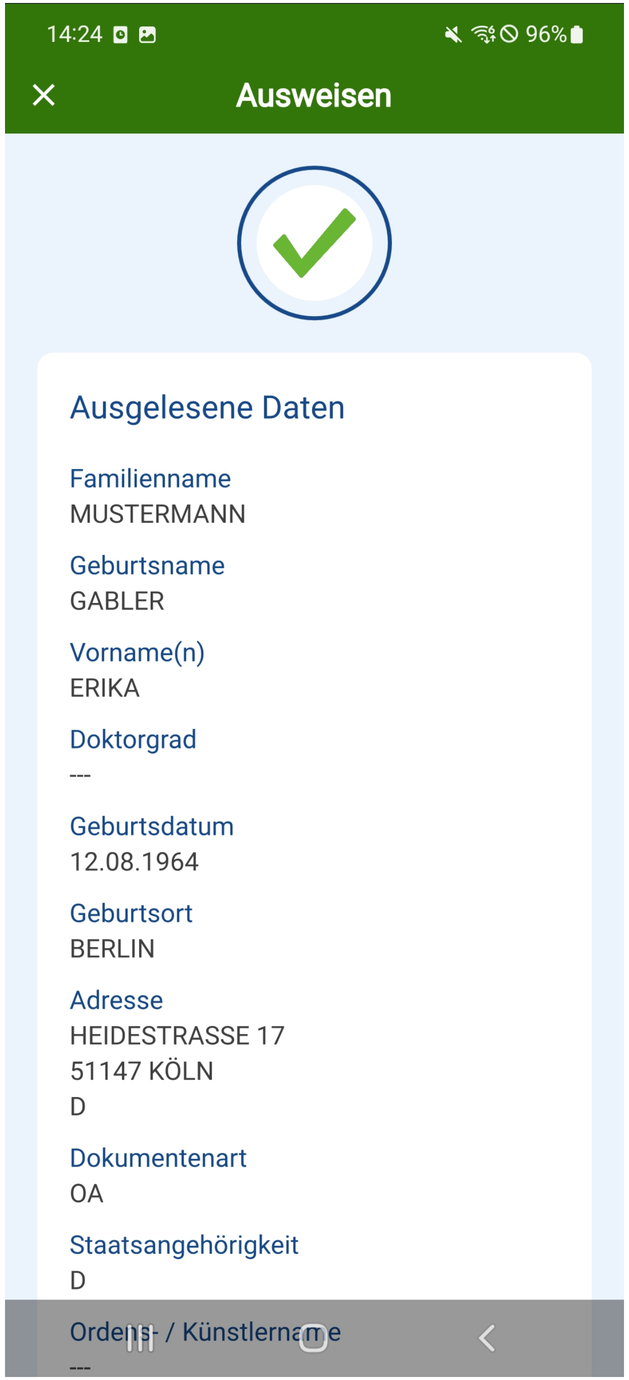
With the upcoming Smart eID, citizens in Germany will be able to use their smartphone for online identification.

Architecture – key benefits

Smart eID – Secure eID on mobile devices

- Enables online identification using only the smartphone.
- Serves as proof of identity according to §18 PAuswG (German law).
- Uses modern technology and extends the existing eID infrastructure.
- Integration with German eID-client - works "out-of-the-box" with all German eID service providers





Ausgelesene Daten

Familienname
MUSTERMANN

Geburtsname
GABLER

Vorname(n)
ERIKA

Doktorgrad

Geburtsdatum
12.08.1964

Geburtsort
BERLIN

Adresse
HEIDESTRASSE 17
51147 KÖLN
D

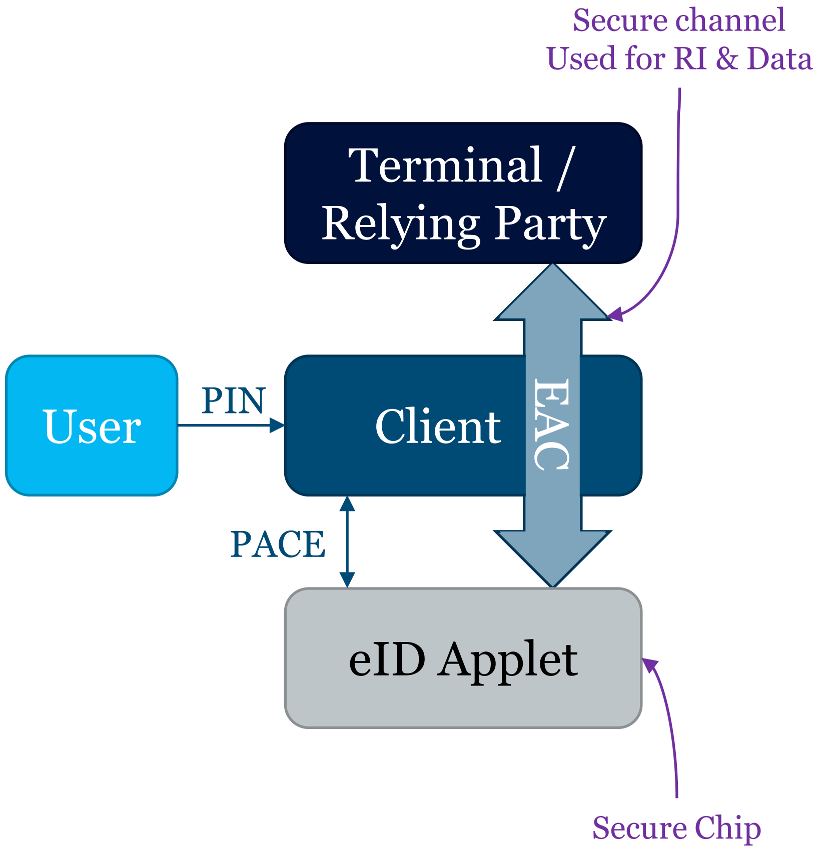
Dokumentenart
OA

Staatsangehörigkeit
D

Ordens- / Künstlername

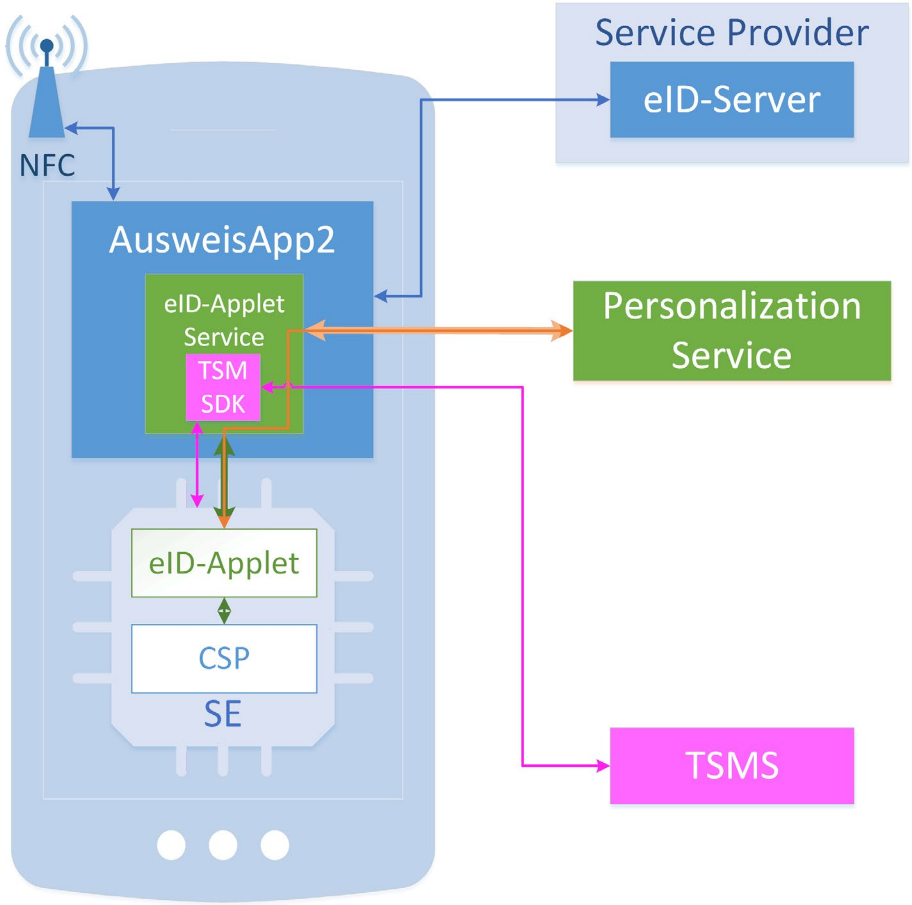
Trustworthy Protocols

- Smart-eID is based on protocols of the German identity card
  - PACE and EACv2
  - Formally proven security
  - Mutual authentication
- Privacy and security by Design
  - **Decentralized architecture**
  - **Pseudonymous identification**
  - Selective disclosure
  - Plausible deniability to third parties
  - **Hardware-based security**



Key Elements of the Smart-eID

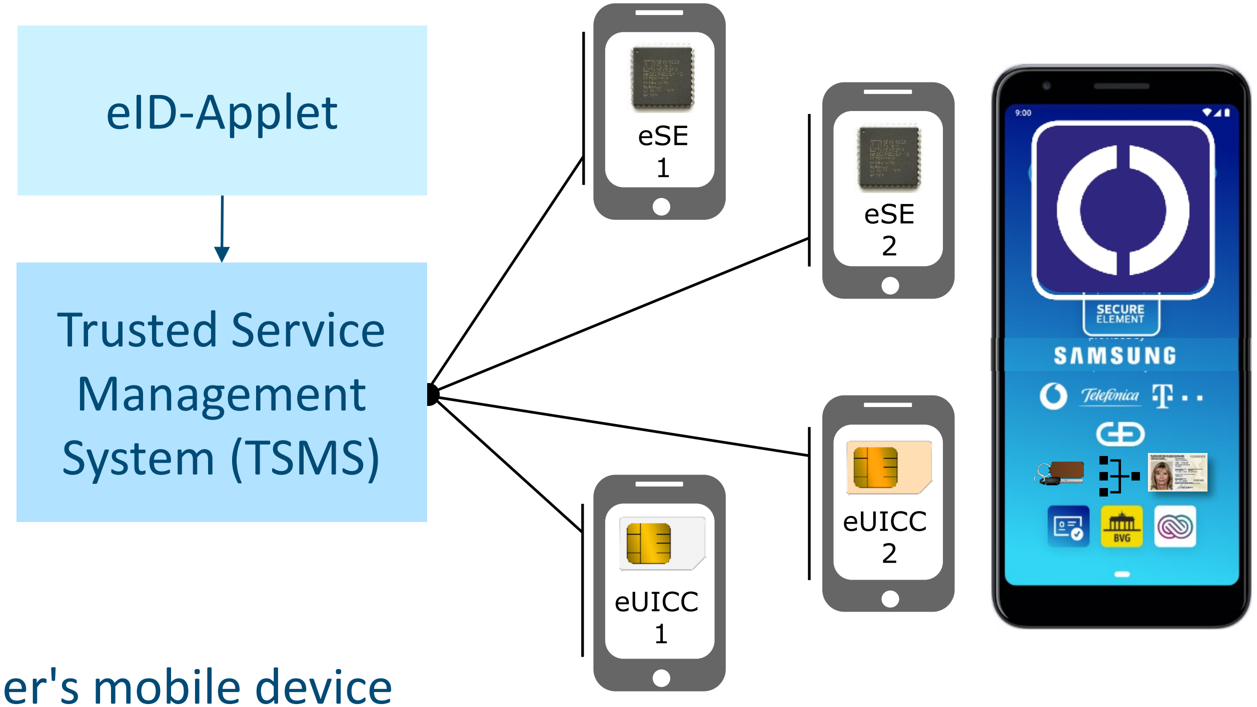
- **SE - secure element** (as dedicated eSE or eUICC/eSIM) to store and operate sensitive data like credentials and keys
- **eID-applet** issued by the national ID card manufacturer to permit the usage of citizens‘ IDs on smartphones
- **Smart-eID Personalization Service** provides eID-applet and personalization of smart-eID
- **TSMS – Trusted Service Management System** for the provisioning of eID-applets issued by the eID-Applet provider into SEs with the permission of the platform owner (OEM or MNO)



Smart eID Deployment

- eID applet is provided by ID card manufacturer
  - Security **certification and conformity** tests according to BSI specifications

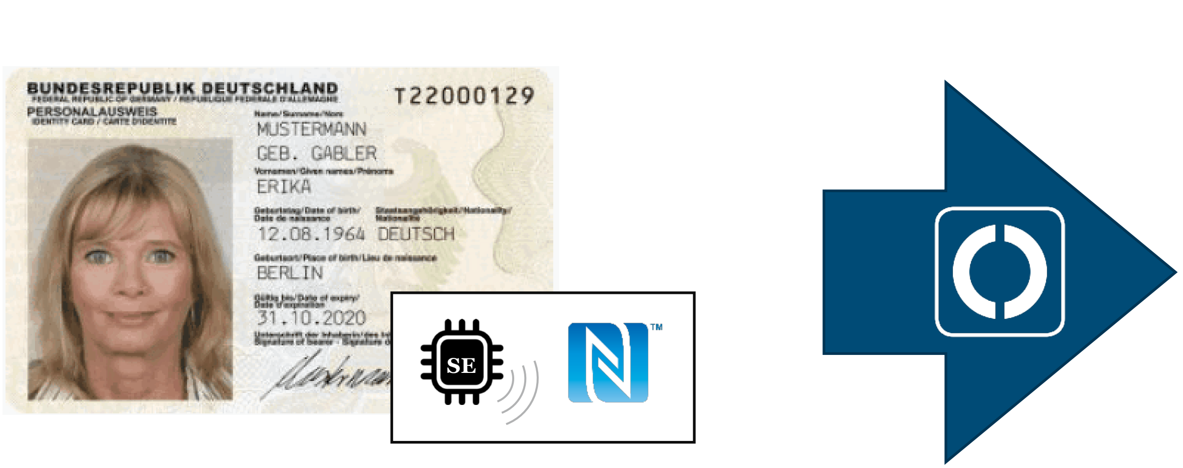
- TSMS enforces life cycle of the applet
  - Installs, updates and deletes applet on user's mobile device
  - Checks eligibility of target platform
    - ➢ Applet is only installed on trusted secure hardware
  - Deploys trust anchor for personalization service
  - Provides unified interface to underlying security hardware

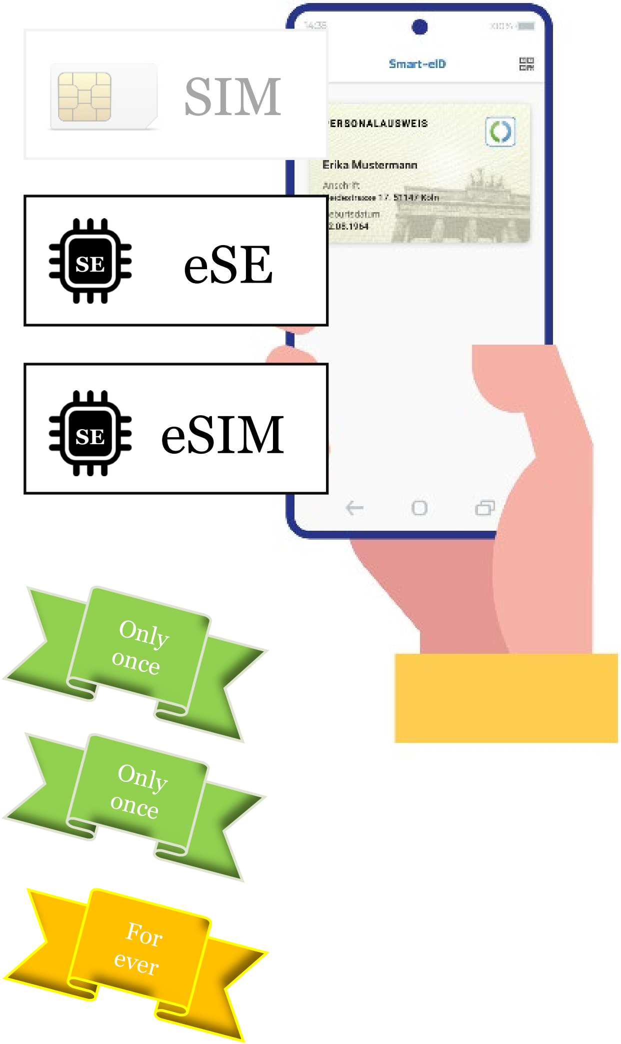


eID-Applet

Trusted Service Management System (TSMS)

Life-Cycle of the Smart-eID





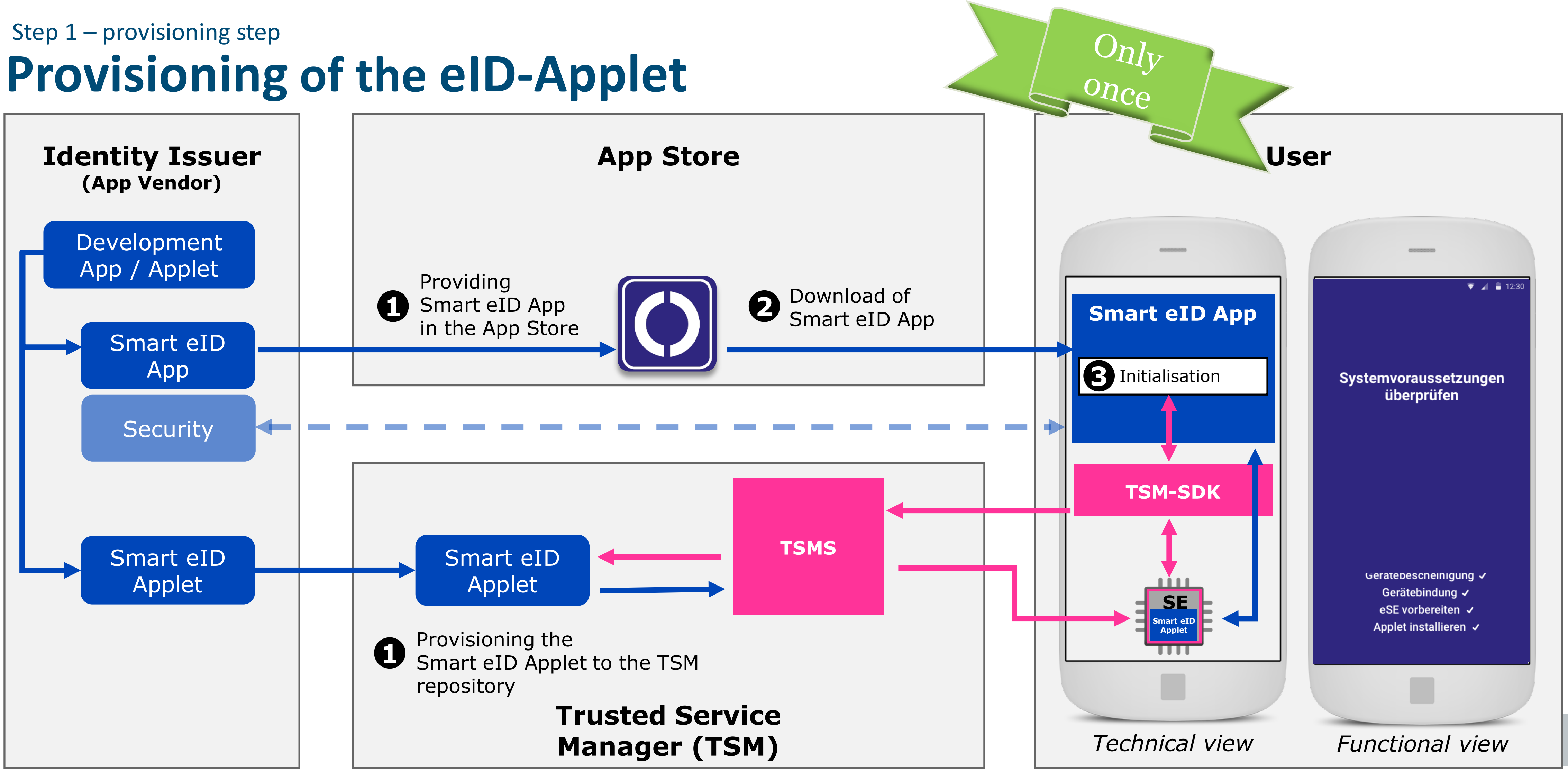
1 **Provisioning:**
App & applet installation, system initialisation

2 **Personalisation:**
Identity data derivation and storage in Smart-eID

3 **Usage:**
Identification at a relying party

Step 1 – provisioning step

Provisioning of the eID-Applet

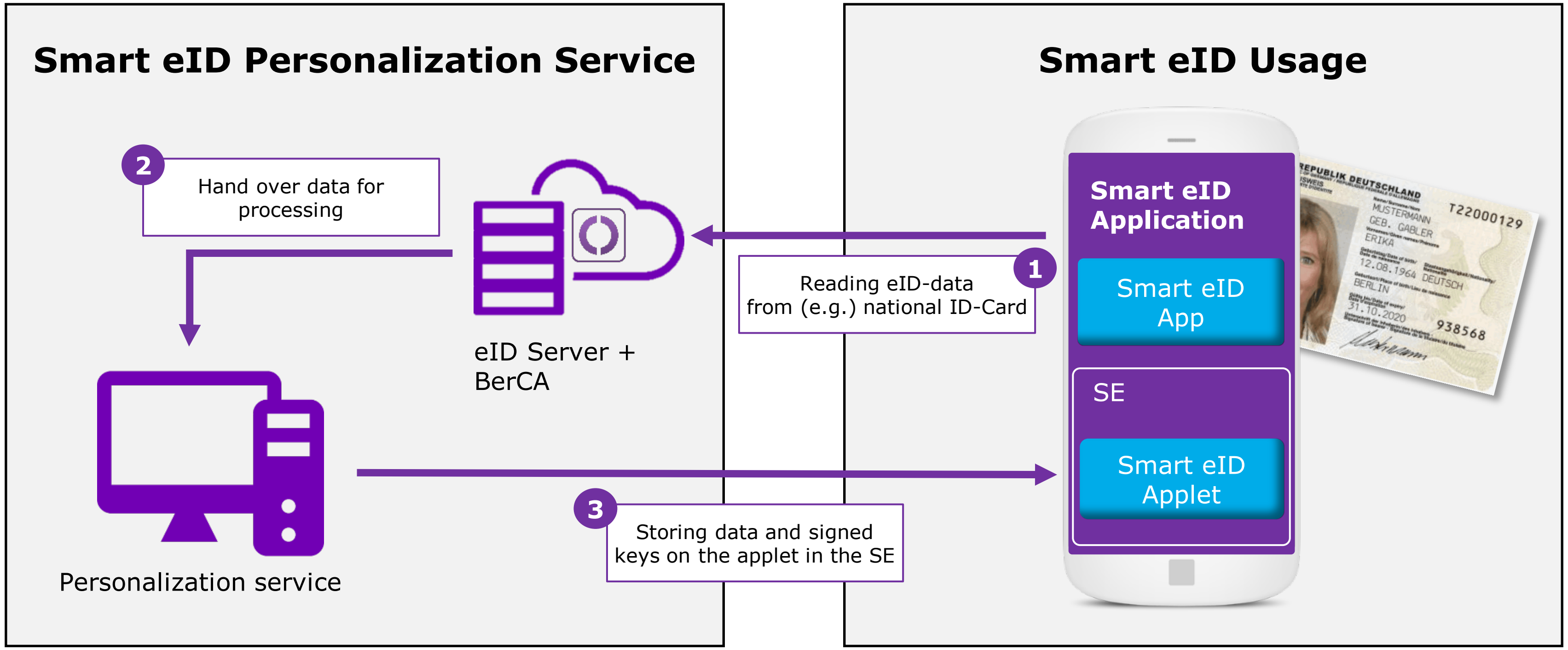


Federal Office
for Information Security

Step 2 – personalization step

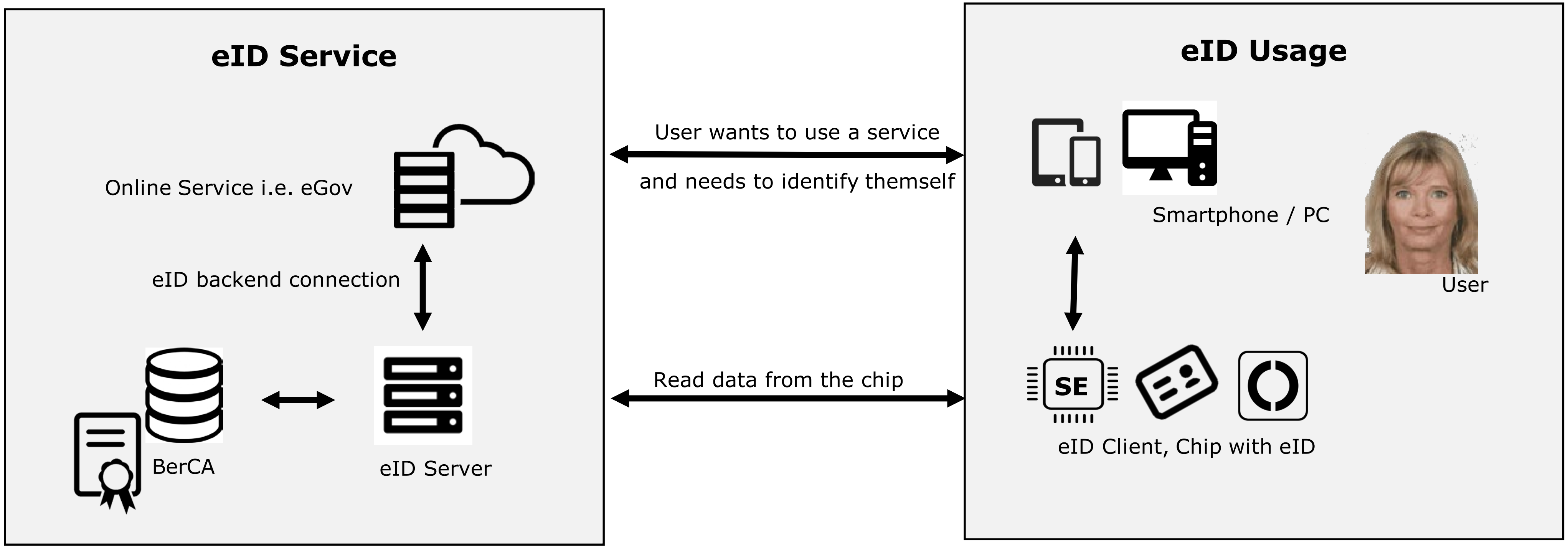
Personalisation of user‘s identity data

Only once


Smart eID Personalization Service
2
Hand over data for processing
eID Server + BerCA
1
Reading eID-data from (e.g.) national ID-Card
Personalization service
3
Storing data and signed keys on the applet in the SE
Smart eID Usage
Smart eID Application
Smart eID App
SE
Smart eID Applet

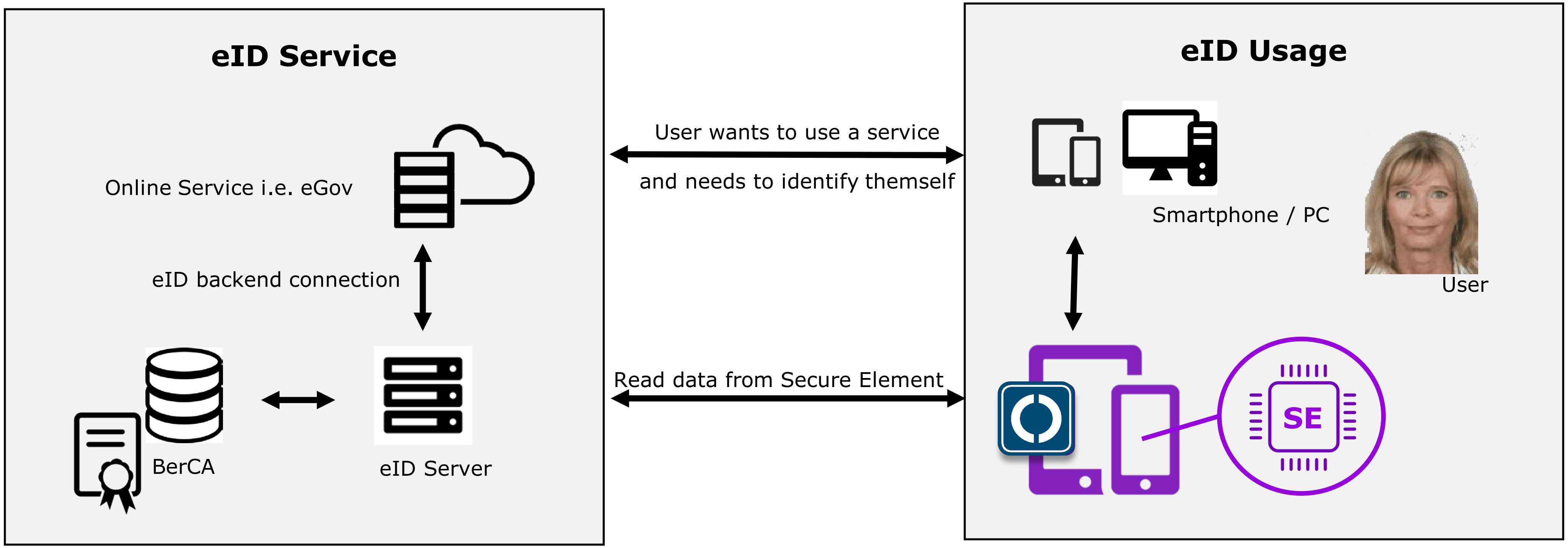
Step 3 – usage of the eID

Usage with ID card via NFC



Step 3 – usage of the eID

Direct usage of an Smart-eID on a mobile device

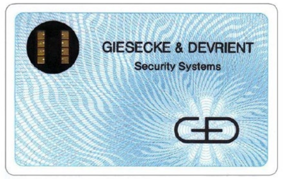


- Service Providers that already have integrated authentication via the German eID card only need minor adjustments.
- Usability for the citizen is highly improved
- All services that have already integrated the German eID can directly use the smartphone based ID
- eIDAS Interoperability stays the same

Evolution of (e)UICC

Since 1980

Chip cards



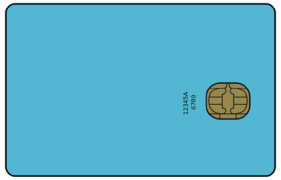
Application fields:

- Credit cards & debit cards & bank cards
- ID cards
- Access control

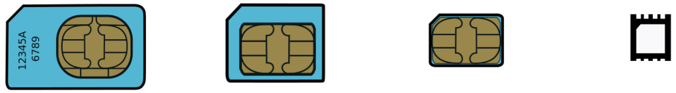
Since 1990

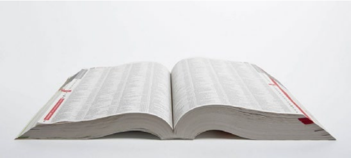
SIM cards

Full-size SIM (1FF)



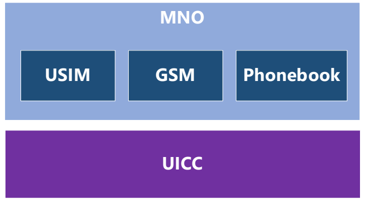
Mini-SIM (2FF) | Micro-SIM (3FF) | Nano-SIM (4FF) | eSIM (MFF2)





Since 2000

UICC / SIM



MNO

USIM | GSM | Phonebook

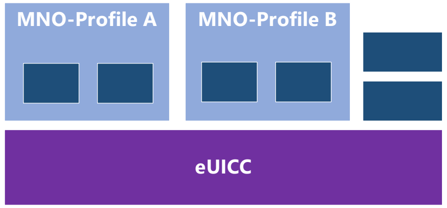
UICC

UICC Multi-Application Platform:

- Improved Software-Architecture
- Separation platform (UICC) and application (SIM)
- Further applications at SIM possible (e.g. phone book)
- Available in all form factors (2FF, 3FF, 4FF, MFF2)

Since 2015

eUICC / eSIM



MNO-Profile A | MNO-Profile B

eUICC

eUICC Multi-MNO-Profile Platform:

- Further improved software-Architecture
- Separation of different MNO-Profiles
- Further applications possible

Certification of Secure Elements and eSIMs

CC PP-0084 IC or CC PP-0117 3S

Certification of the hardware chip

CC PP-0099 JavaCard

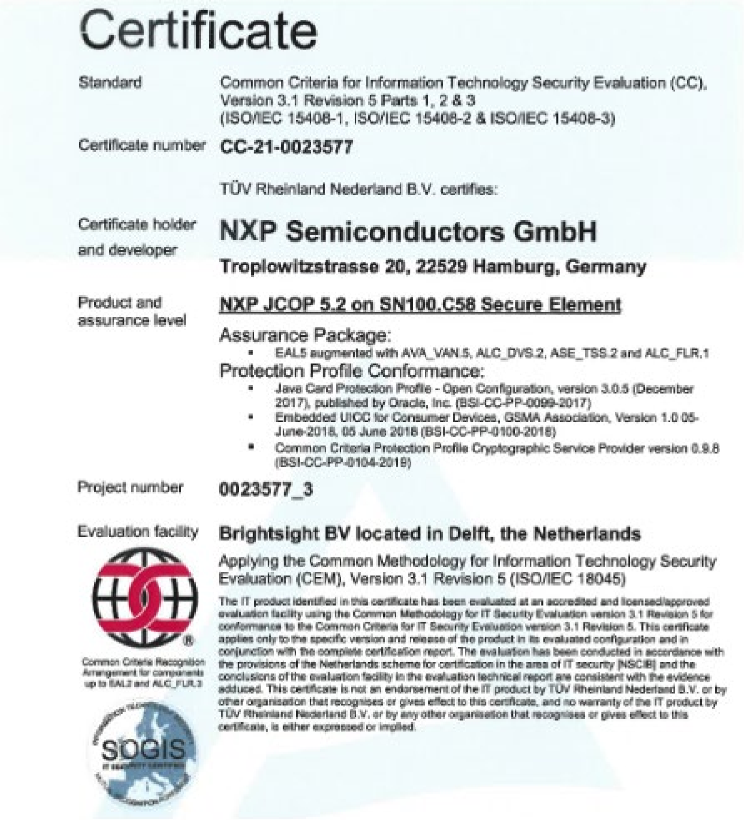
JavaCard certification of the operating system

CC PP-0100 eUICC

eSIM/eUICC functionality

CC PP-0104 CSP

Certification of hardware, operating system, and crypto library according to the requirements of the „Cryptographic Service Provider“



Certificate

Standard: Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 Parts 1, 2 & 3 (ISO/IEC 15408-1, ISO/IEC 15408-2 & ISO/IEC 15408-3)

Certificate number: **CC-21-0023577**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer: **NXP Semiconductors GmbH**
Troplowitzstrasse 20, 22529 Hamburg, Germany

Product and assurance level: **NXP JCOP 5.2 on SN100.C58 Secure Element**

Assurance Package:

- EAL5 augmented with AVA_VAN.5, ALC_DVS.2, ASE_TSS.2 and ALC_FLR.1

Protection Profile Conformance:

- Java Card Protection Profile - Open Configuration, version 3.0.5 (December 2017), published by Oracle, Inc. (BSI-CC-PP-0099-2017)
- Embedded UICC for Consumer Devices, GSMA Association, Version 1.0 05-June-2018, 05 June 2018 (BSI-CC-PP-0100-2018)
- Common Criteria Protection Profile Cryptographic Service Provider version 0.9.8 (BSI-CC-PP-0104-2019)

Project number: **0023577_3**

Evaluation facility: **Brightsight BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

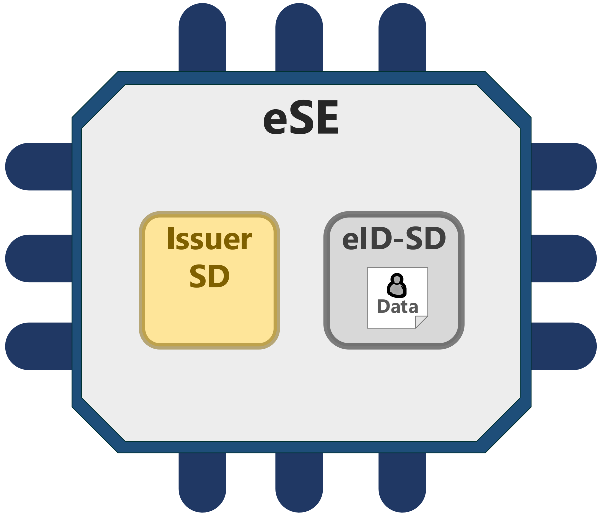
Common Criteria Recognition Arrangement for components up to EAL2 and ALC_FLR.3

Broad existing certification coverage for eSIM & eSE.

Current development and outlook

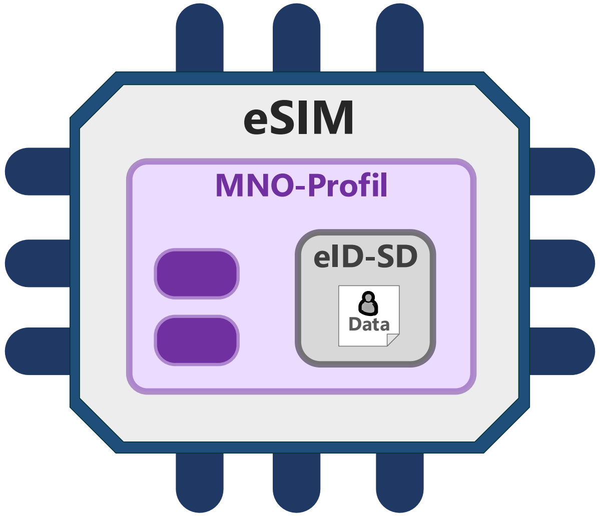
eSE

(eID-SD on eSE)



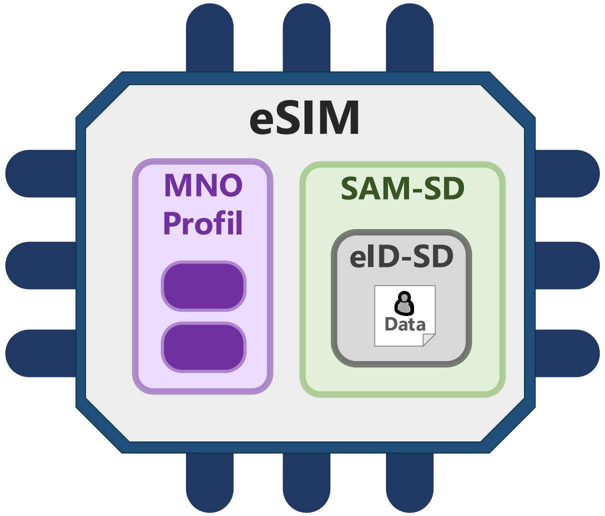
MNO-Profile

(eID-SD in MNO-Profile on eSIM)



SAM-SD

(eID-SD in SAM-SD on eSIM)



Thank you for your attention!

Contact

Dr. Mike Bergmann
Head of section SZ34
“Chip Technologies and eID Technologies for Mobile Platforms“

Mike.Bergmann@bsi.bund.de

Federal Office for Information Security (BSI)
Godesberger Allee 185-189
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.