Die smart eID kommt
Provisionierung über TSMS

Volker Reible
Deutsche Telekom Security GmbH

Webinar, 06. Juli 2022

LIFE IS FOR SHARING.

TSMS und Smart-eID

Das Trusted-Service-Management-System (TSMS)

Service Provider Application

- Service Provider „Smart-eID“
- Service Provider „SSI“
- Service Provider „Public Transport“
- Service Provider „Automotive“
- Service Provider „XY“

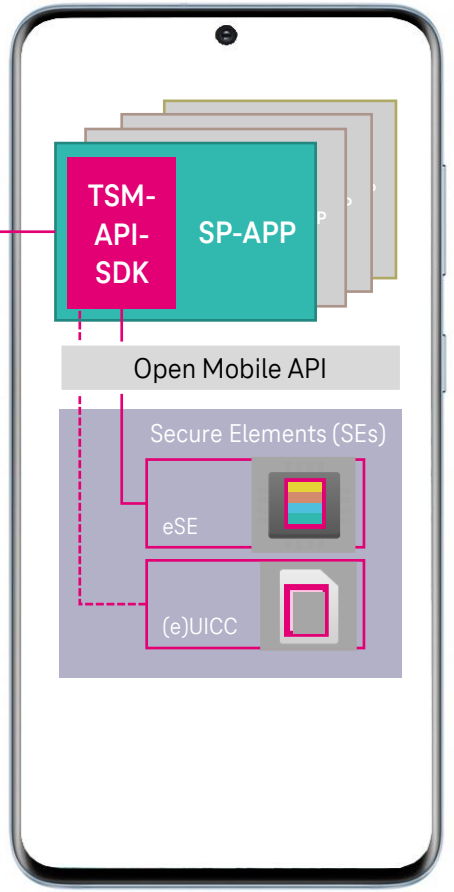
Trusted Service Management System (TSMS)

Application Manager für Service Provider

- Applet Smart-eID
- Applet SSI
- Applet PT
- Applet Car
- Applet XY

Trusted-Service-Manager für Secure Elements

TSMS Lifecycle Management für eID- oder andere Applets (Provisionierung, Update, Löschen)



- Um Secure Elements (SEs) im Smartphone nutzen zu können, sind entsprechende Programme - sog. Applets – auf dem SE erforderlich.
- Diese werden mittels des TSMS auf das Smartphone aufgebracht (Provisionierung).

Services

Erster Service

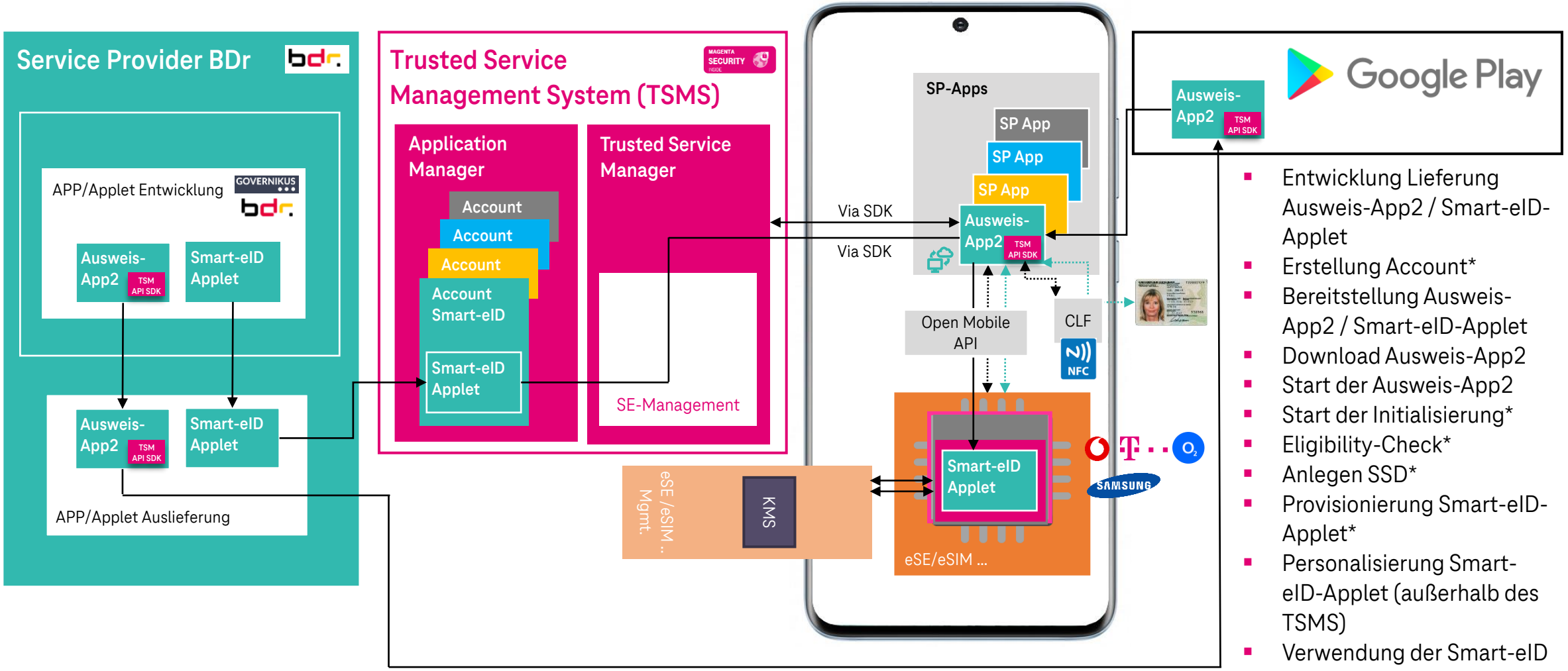
Smart-eID

Der deutsche Personalausweis auf dem Smartphone

Nach deutschem ID-Gesetz vom 01.09.2021 bis zu **eIDAS „high“**

Provisionierung der Smart-eID

Aus Sicht des TSMS – Vereinfachte Darstellung



- Entwicklung Lieferung Ausweis-App2 / Smart-eID-Applet
- Erstellung Account*
- Bereitstellung Ausweis-App2 / Smart-eID-Applet
- Download Ausweis-App2
- Start der Ausweis-App2
- Start der Initialisierung*
- Eligibility-Check*
- Anlegen SSD*
- Provisionierung Smart-eID-Applet*
- Personalisierung Smart-eID-Applet (außerhalb des TSMS)
- Verwendung der Smart-eID

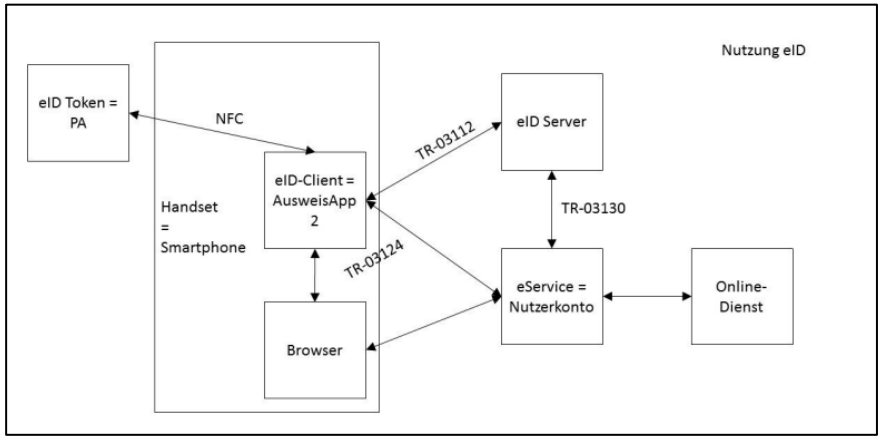
* TSMS-Einbindung

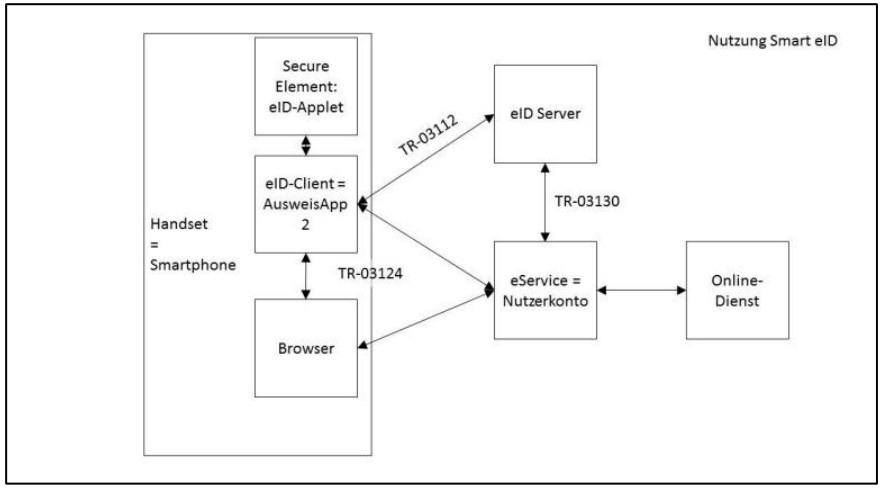
Trusted-Service-Management-System (TSMS)

Smart-eID – Aktueller Status

- Ableiten von mobilen bzw. smarten Identitäten vom Personalausweis und Speicherung im Secure Element eines Mobilgeräts.
- **Seit 28.03.2022 Pilot mit ersten Dienstanbietern** (u.a. Nutzerkonto Bund), weitere folgen.
- Integration des Identifizierungs- und Authentifizierungsverfahrens Smart-eID analog dem aktuellen Online-Ausweisen mit Personalausweis.

Quelle: Bundesministerium des Innern, für Bau und Heimat; Bundesdruckerei GmbH





Quelle: Handlungsleitfaden zur Integration der Smart-eID in ein Nutzerkonto v0.7, S.14

Warum Hardwaresicherheit?

Warum Hardwaresicherheit (z.B. Secure Elements)?

Hardwaresicherheit

Welche **Vorteile** hat **Hardwaresicherheit** z.B. gegenüber Softwarelösungen?

- Physische Kontrolle über die eigene Digitale Identität – Kombination der Sicherheit aus Wissen (z.B. PIN) und Besitz (Sicherheitshardware)!
- Schutzmechanismen der evaluierten Sicherheitshardware – u.a. Schutz gegen Seitenkanalangriffe!
- Geschütztes Schlüsselmaterial – Schlüssel bleiben immer in der sicheren Umgebung der Chipkarte!
- Umfangreicher Kopierschutz – Identitätsdiebstahl elektronisch nicht möglich!
- Geringere Zugangshemmnisse zu höherwertiger Sicherheit – z.B. kein komplexes Fraudmanagement im Backend erforderlich.

Und wie sieht es mit der Reichweite aus?

Nutzung von SIMs zur Erhöhung der Reichweite

AusweisApp2

eSE

SAMSUNG

+...

Embedded SE

Smart-eID

AusweisApp2

eSIM

Telefónica

CryptoSIM/ NFC-SIM

Smart-eID

OEM-Lösung (aktuell)

- Speicher: embedded SE
- Sicherheitslevel: high
- Applikationen: AusweisApp2 und ID Wallet

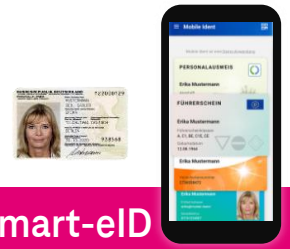
MNO-Lösung (in Arbeit)

- Speicher: eSIM und / oder neue Crypto SIM / NFC-SIM
- Sicherheitslevel: high (angestrebt)
- Applikationen: AusweisApp2 & ID Wallet
- Reichweite: Bis zu 40% (zusätzlich)

Beide Lösungen sind technisch sehr ähnlich.

Gegenüberstellung der Lösungen





Kriterium	ID card (physisch)	eID (since 2010)	Smart-eID SE in eSE (Gerät)	Smart-eID SE in eSIM	Smart-eID Softwarelösung
Datenspeicher	Chip in ID-Karte	/	Hardware: **in device**	Hardware: **in device**	TEE / Software
Applikation	-	AusweisApp 2	AusweisApp 2 + ID Wallets	AusweisApp 2 + ID Wallets	AusweisApp 2 + ID Wallets
Speicherung	Permanent	One-time only ☹	Permanent ☺	Permanent ☺	Permanent ☺
Projekt	/	/	Optimos2/Smart-eID	ONCE/Smart-eID	Smart-eID
Anzahl Use Cases	Low ☹	Low ☹	Medium 😐	Medium 😐	Medium 😐
Security level	High ☺	High ☺	High ☺ (angestrebt)	High ☺ (angestrebt)	Substantial 😐 (angestrebt)
Life Cycle	Langfristig ☺	Mittelfristig 😐 (Kanibalisierung durch Smart eID)	Langfristig ☺	Langfristig ☺	Mittel- bis langfristig 😐
Erwartung	Physische Basis	😐	☺	☺	😐

Vielen Dank für die Aufmerksamkeit!

volker.reible@telekom.de
06151-581 5656

LIFE IS FOR SHARING.