IBA Conference 2021

Digital identity and facial recognition: industry trends and legal challenges.

Christian Stengel
Lead Architect
Deutsche Telekom Security GmbH

October, 11th 2021

LIFE IS FOR SHARING.

Agenda

01 Expectations of citizens and business service providers

02 „Greetings“ from the eIDAS regulation

03 Design-criteria for a mobile trust ecosystem

04 Trusted Service Management System (TSMS) as a good basis

05 Definition and benefits of a certificate-based eIDs

06 Certificate-based eID in mobile trust ecosystems

07 „Demo“ – Generating and storing the eID as a Mobile ID

08 Conclusion and outlook

Expectations of Citizens

01

Major factor: Usability

- **Easy installation**
- **Intuitive way of usage**
- **Interoperability**
- **One ID** for different purposes, (e.g. single sign on)

02

Privacy / Security

- **Secure smartphone applications**
- Guarantee of **privacy** of the stored data.
- **Protection** of data against different attacks like unwanted copying or identity thefts.

03

Sustainability

- **Small footprint** due to climate change
- **Long-term usability** for the own ID

04

Digital Sovereignty

- **Self-determined** use of the ID under full control and exchange of data.
- **Erasability** and **portability** of the ID **to other ID-Providers** (against Lock-In effects)

Key Fact I

Security and privacy have to be guaranteed by design!

I.e. the users expect security and legal compliance but do not want to think about it!

Expectations of Business Service Providers

01

Major factor: Easy integration

- **Easy integration** in established or new services
- **Interoperability**

02

Conformity and Liability

- **Conformity** to national and international **standards**
- **Responsibility/ Liability** of the ID-Provider for the quality of the issued ID.

03

„Security“

- **IT-Security by design**
- Sufficient Security measures
- **Crypto agility**
- **Ecological and financial sustainability**
- **Future proof** of investment

04

Cost Reduction and more business

- **Reduction of costs** for different services
- Enabling of more business

Key Fact II

Like citizens also service providers expect secure IDs with a high (guaranteed) quality and legal compliance but also do not want to think about them.

„Greetings“ from the eIDAS-regulations

The following requirements taken from the new eIDAS draft regulation:

- Increase of user convenience
- Need for secure service access
- Satisfaction of different policy areas
- Reusage of existing solutions
- EU-ID Toolbox for Identity Wallet integration

Leed to the following proposal:

- **A building block** to derive and virtualize notified eID-solutions on smartphones.
- **The provisioning of eID functionalities into hardware based Secure Elements** on smartphones.
- A **secure platform for EU Digital Identity Wallets** (EU-ID Wallet).
- The provision of **interoperability**, **security** and **privacy** through appropriate standards.

(Some) Design-Criteria for a Mobile Trust Ecosystem

- **Easy-to-use eID-infrastructure** for various **Service Providers**

Open Infrastructure

- Support of international requirements as **eIDAS**
- Participation in committees and standardi-zation activities

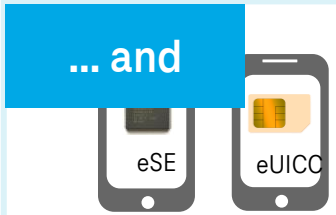
Uniform Standards

- **Efficiency**
- Strict demand for a **low energy consumpting** solution.

High Sustainability

- System with **clear responsibilities** for the issued IDs.
- **Legal Compliance**

Clear Responsibilities



- **Secure storage** of the (critical) data of eIDs
- Use of the mobile devices' secure elements like **eSE** or **eUICC**

Hardware Security

TSMS as a Basis for the Mobile Trust Ecosystem

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)

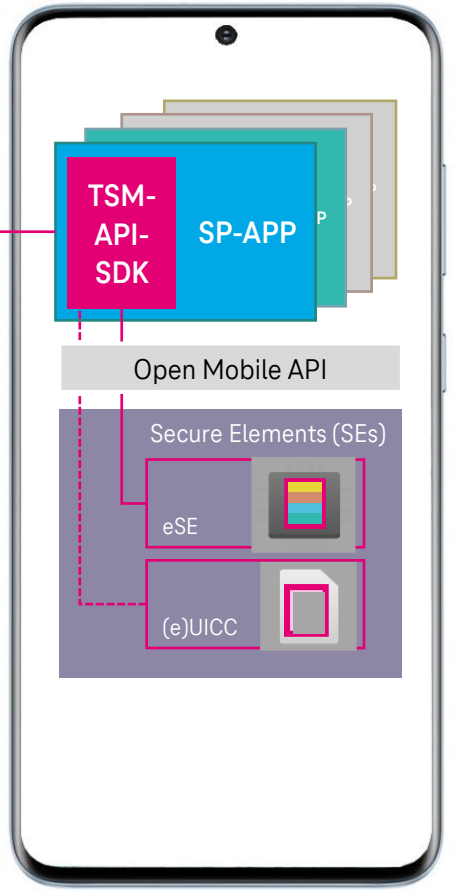
Application Manager for Service-Provider

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

Trusted-Service-Manager for Secure Elements

TSMS Lifecycle Management for eID- or other Applets (Provisioning, Update, Deletion)

MAGENTA SECURITY INSIDE



Services

First established service

Smart-eID

The german ID-card on the Smartphone to be notified.

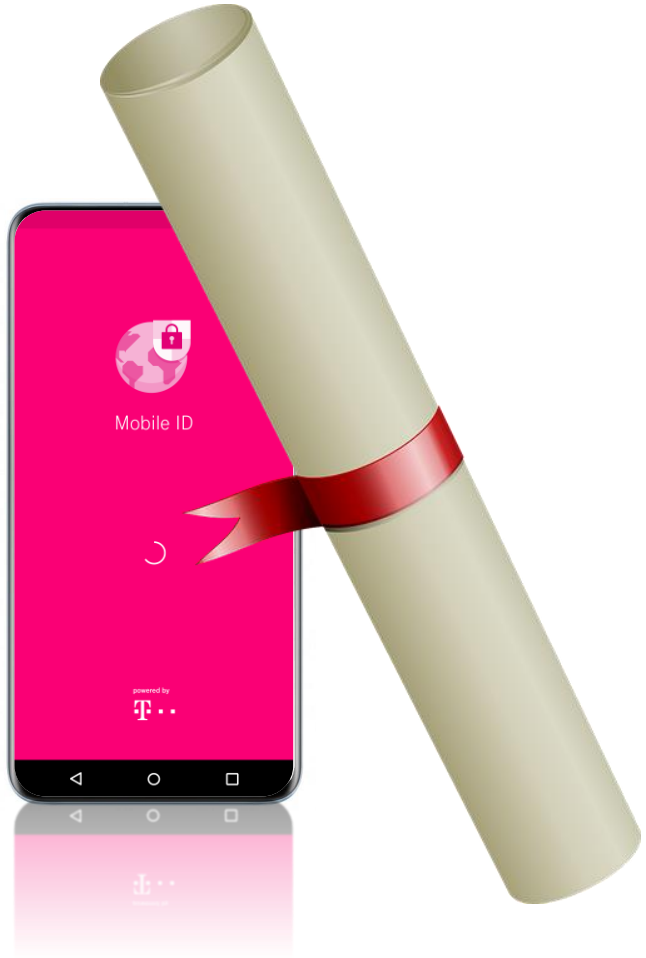
Due to german „eID-law“ from 1st September 2021 up to **eIDAS „high“**

Usage of open standards (GP, GSMA, ISO, ...)

Definition and Benefits of a Certificate-Based eID

The certificate based Mobile eID defines a digitale identity based e.g. on X.509-certificates:

- **It reduces the complexity of know applications like the** governmental ID and allows the enrichment of the eIDs with additional ID data of attributes,
- it is conform to the **Verifiable Credential Standard (SSI),**
- its **X.509-Certificates** can be used in standard protocols,
- it is based on the **TSMS** to transport the eID into Secure Elements on Smartphones,
- It is an **energy saving** system im comparison to other SSI-based IDs
- it supports the **informational self-determination** of the holder and
- it defines a **clear responsibility** for the eID.



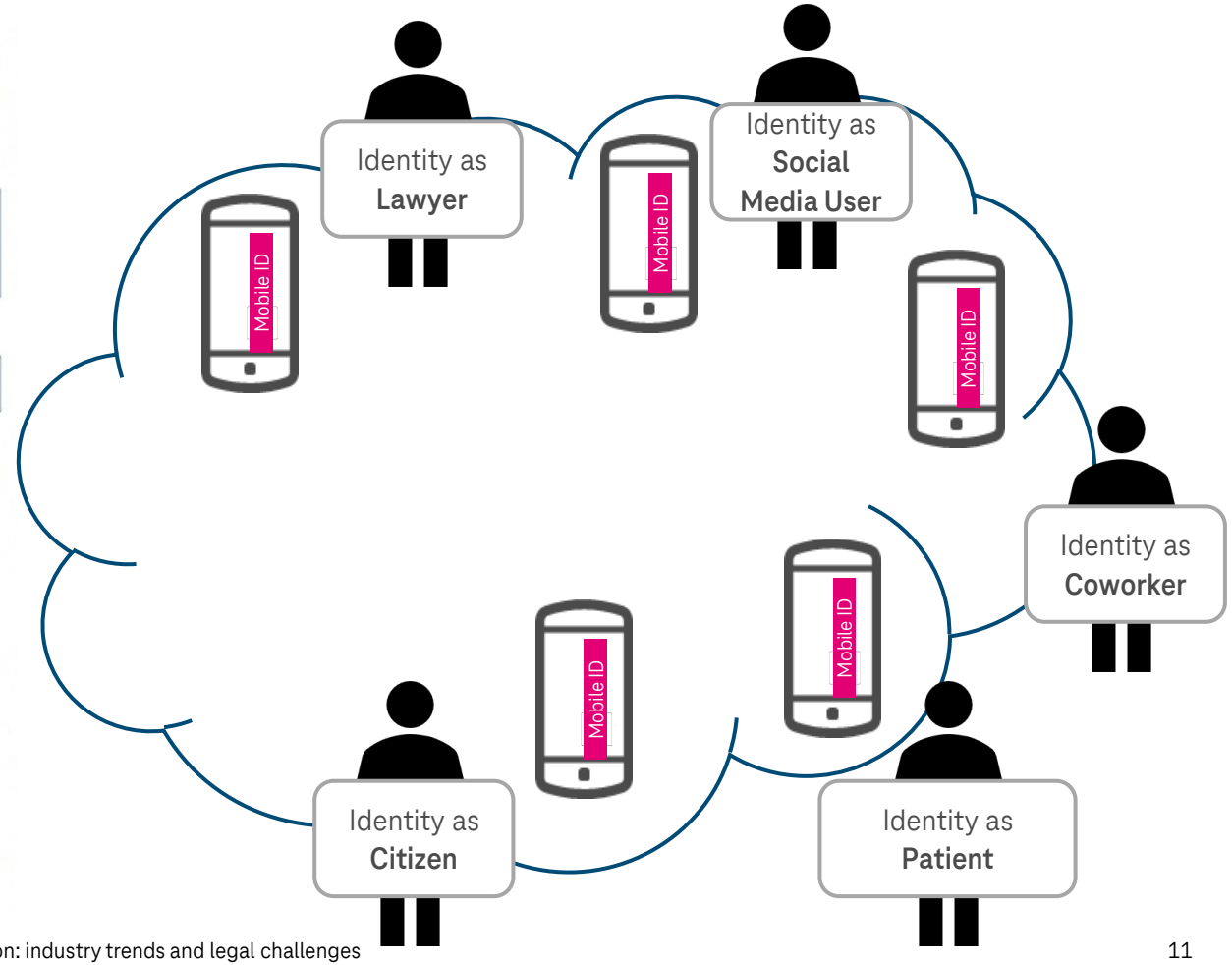
Certificate-Based eID in Mobile Trust Ecosystems

Physical eID or existing ID-systems

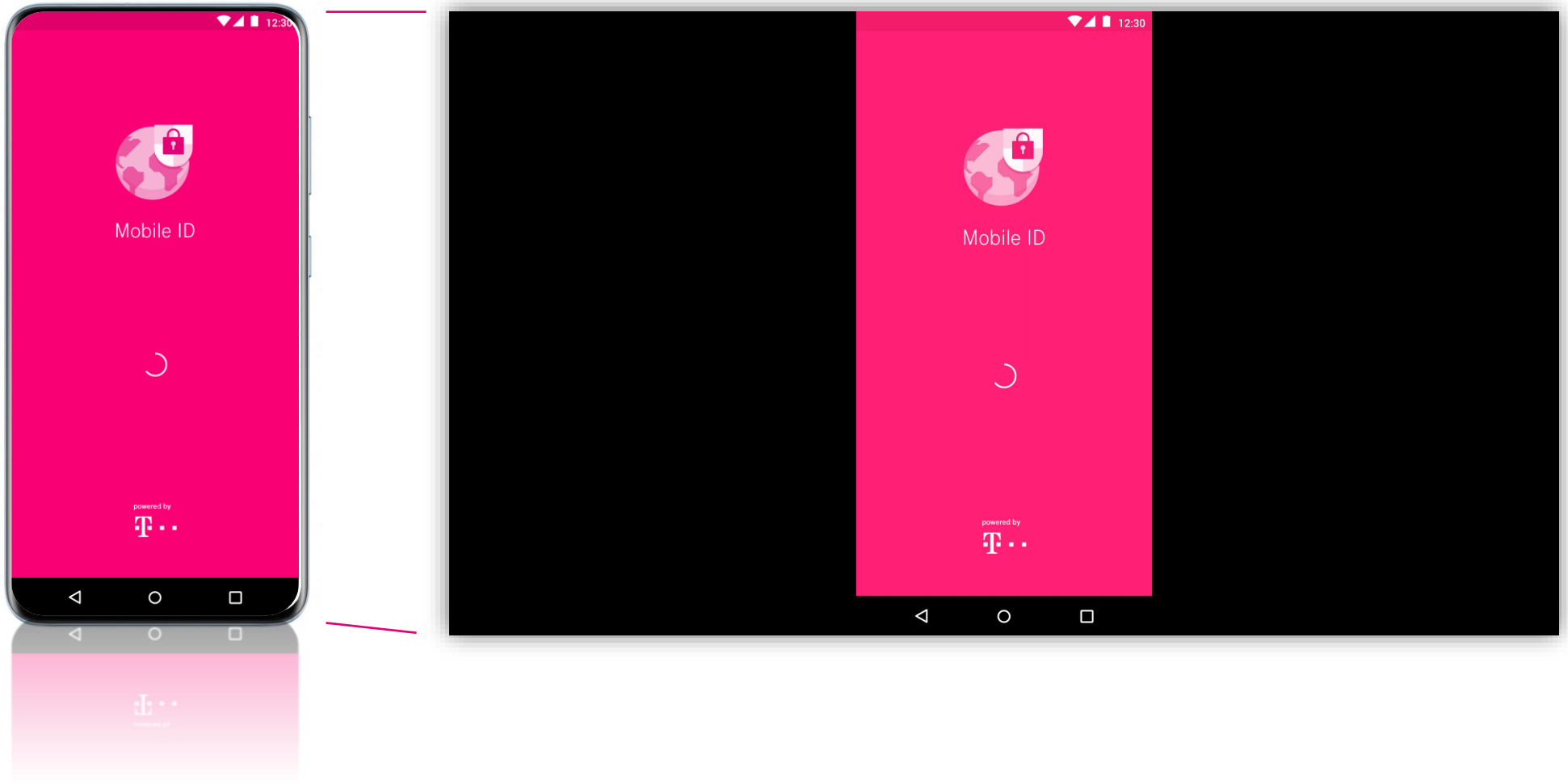
Derivation of the eID into a Mobile ID on the Smartphone

Mobile ID (usage)

Identification an **derivation** of the eIDs into user smartphones



„Demo“ – Generating and Storing eID as Mobile ID



Conclusion and Outlook

In the future we need and have …

- a push of digitalization worldwide,
- reduction of bureaucratic overhead and technical complexity,
- sufficient security and privacy

and

- more and easier business and less costs (“keep it simple and stupid”).

From an ID point of view this leads to …

- **a new integrated and easy to use (mobile) eID-ecosystem** with standardized security and privacy measures, e.g. based on eIDAS,
- the integration of **high-level security in smartphones,** e.g. based on **certified smartcard security** and certificate based eIDs and
- a high-quality **ID-basis for high secured mobile services for end customers.**

Thank you for your attention!

Dipl.-Math. Christian Stengel
Lead Architect
Deutsche Telekom Security GmbH
christian.stengel@t-systems.com

LIFE IS FOR SHARING.