

ENISA Trust Service Forum

The future of Digital Identity and Trust Ecosystems

Christian Stengel
Lead Architect
Deutsche Telekom Security GmbH

September, 21st 2021





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 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.

Key Fact I

Security and privacy have to be guaranteed by design!

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



Expectations of Service Providers

01

Major factor: **Easy integration**

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

02

Conformity

- **Conformity** to national and international **standards**

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 and 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



Lead 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 standardization activities

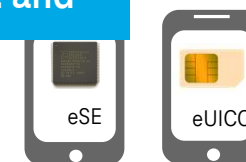
Uniform Standards



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

High Sustainability

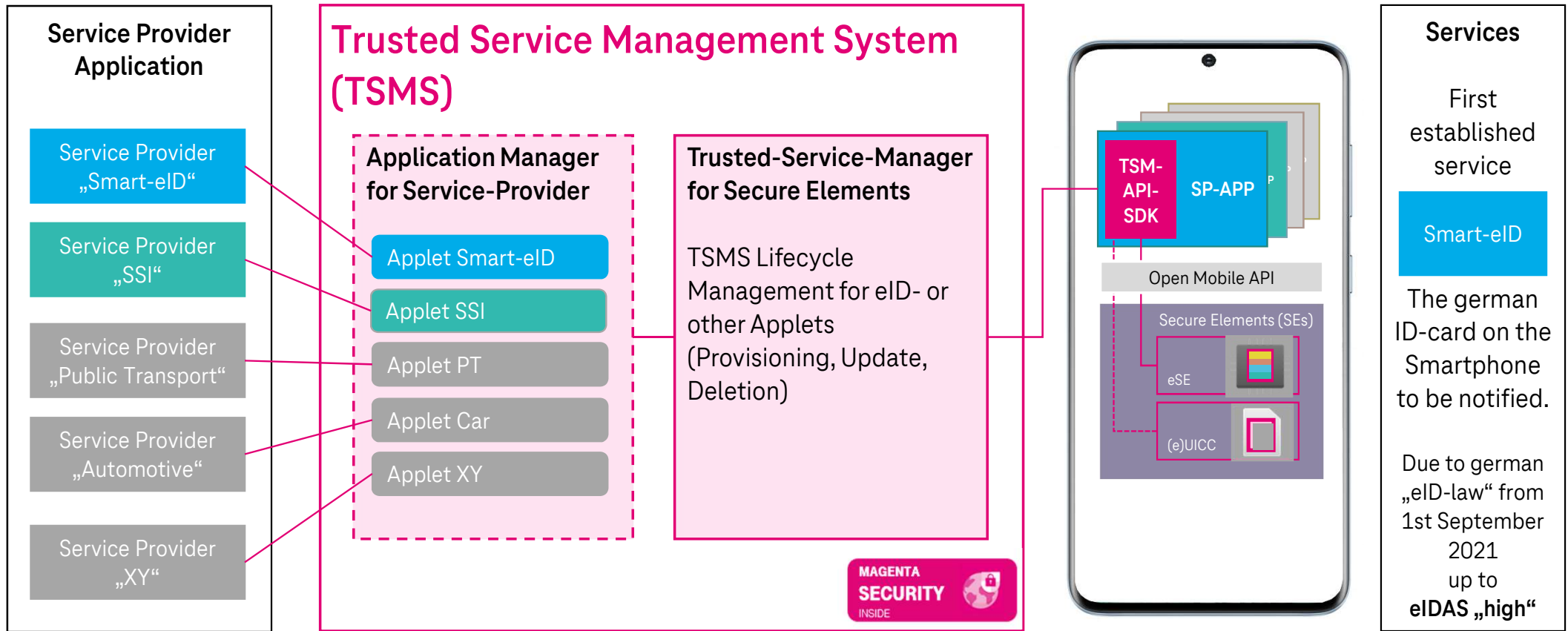
... and



- **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



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



Conclusion and Outlook

In the future we need and have ...

- a push of digitalization in Europe,
- 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 ID-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
- an ID-basis for high secured mobile services for end customers.



**Thank you for your
attention!**



LIFE IS FOR SHARING.



Dipl.-Math. Christian Stengel
Lead Architect



Deutsche Telekom Security GmbH
christian.stengel@t-systems.com