Bundesamt
für Sicherheit in der
Informationstechnik

BSI and the FIDO Alliance

Joachim Weber

Federal Office for Information Security

RSA Conference, 2016

Federal Office for Information Security

- BSI: Bundesamt für Sicherheit in der Informationstechnik
- Germany's national IT Security Agency
- Founded in 1991
- Staff: ~ 630 employees
- Annual Budget: 62 million Euro

Federal Office for Information Security

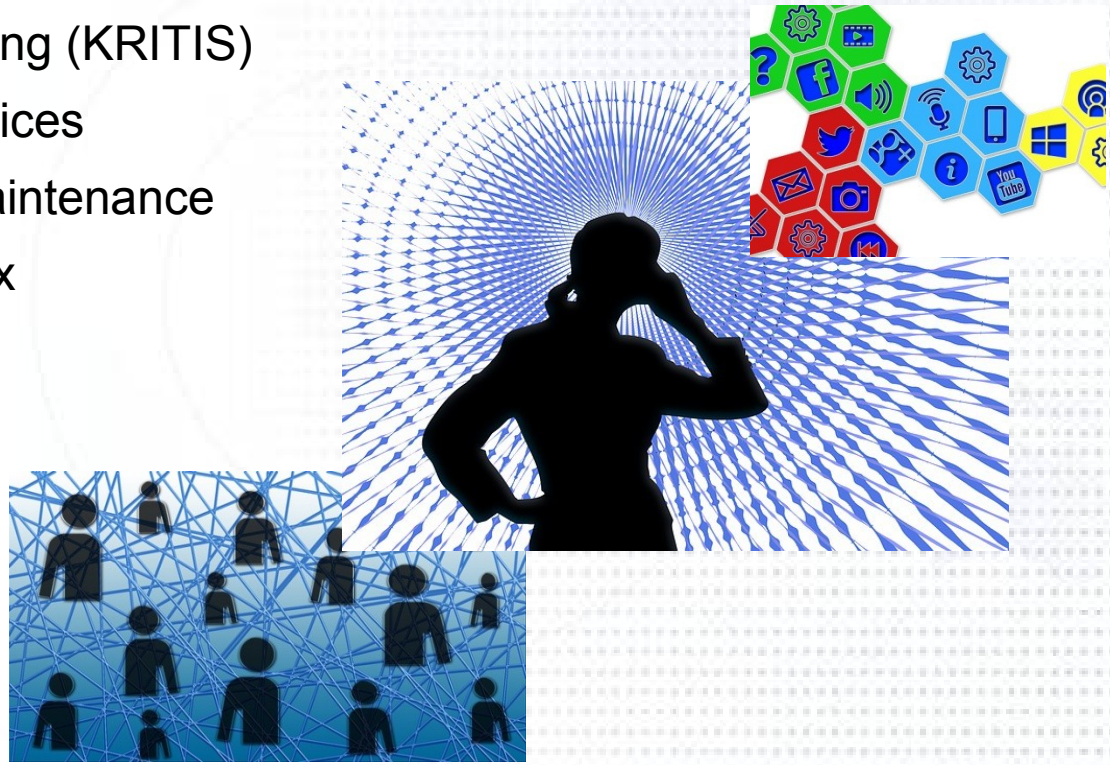
BSI services:

- **Analysis and evaluation of IT security risks, information and awareness-building**
- Technical standards, Test- and Certification Services for the security of **IT components and systems**
- **Security solutions** for government networks and applications

Challenges
Digital Agenda

Digitization, automation, interconnection required in all sectors:

- **Smart Grid**, Smart Metering (KRITIS)
- **Smart Home**, Smart Services
- **Industry 4.0** / Remote Maintenance
- **eMobility** / car2car / car2x
- **eHealth/eGovernment**
- **Cloud** Computing
- **eID / ePayment**
- eCommerce
- Big Data



Need for Secure ID & Trust Services

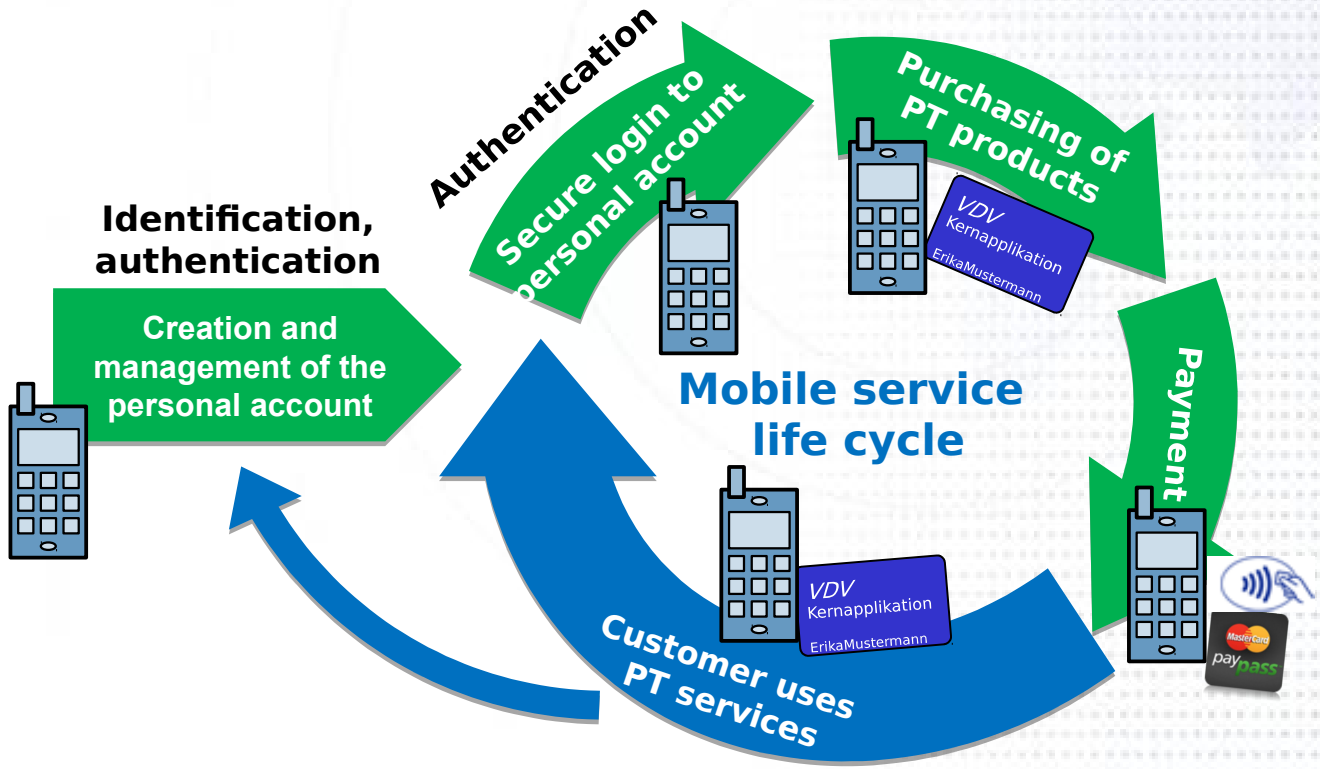
General View on Identification and Authentication to Online Services

- **Secure identification and authentication is a fundamental requirement for reliable, fraud-proof online services**
- **Classical "username - password" authentication proved to be error-prone and insufficient**
  - Recent incidents show that theft of login information occurs on a large scale
    → can't be avoided and constitutes a major threat
  - Current concept does not reflect the limited competences and skills of the average user: Guidelines for secure passwords and diversification of passwords are not user-friendly and consequently widely ignored
    („dke475§V/(ezq9kfeyr#!")
- **Identification and authentication have to support privacy features:**
  - Protection against tracking / creation of profiles
  - Support of pseudonyms
- **Trend for mobile services has to be met**

Business Requirements for Mobile Services

Seamless mobile service approach:

- Customer should be able to **handle all steps of the service life cycle by using his mobile device**
- Purchasing of products should be supported **from any location, at any time and without waiting times** for e.g. activation of a personal account or payment scheme



Example: Mobile service life cycle in Public Transport.

Market potential: > 5 Mio eTicketing customers in Germany, > 1Billion worldwide

Use case related requirements

Requirements to identification and authentication vary by use case:

- **Use case „ Creation and management of the personal account“**
  - Only used for setting up and in case of changes to personal data → moderate requirements to user-friendliness and process execution time
  - Use case requires reliable personal data for user account and creation of derived ID → trusted electronic primary ID as data source
  - Legally binding authorization of payment
- **Use case „ Secure login to personal account“**
  - Frequently used for purchasing, managing products → demanding requirements to user-friendliness and process execution time
  - Shall support personal accounts using pseudonyms and protect against tracking and profiling → distinction from identification
  - Shall support several user devices (Smart phone, tablet, PC)

➲ It makes sense to use electronic **primary ID** for **identification-centric** use cases and specific solutions for **authentication-centric** use cases **and to find ways to connect these.**

Secure ID & Mobility
Primary and Derived IDs and FIDO 2-Factor Authentication

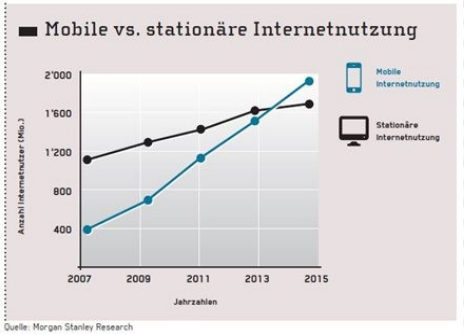
- **German eID card** for **identification-centric** use cases
  - Serves as electronic primary ID and trusted token for authorization
  - Authentication (i.e. as fallback solution for FIDO, and resetting of FIDO authentication for the dedicated user account)
- **FIDO two-factor authentication** for **authentication-centric** use cases
  - FIDO-relation to a personal account will be established after creating the account and its derived ID, be it personalized or psydonymized
  - Established either on or off token, using a derived ID stored on the token or connected with the personal account in the backend
  - Usage of external cards / tokens or secure space in mobile devices
  - Support of several tokens or user devices to the same account
- **NFC as preferred interface** between mobile device and external cards and tokens
  - Supports passive secure eID, transportation and payment cards / infrastructures
  - Supports implementation of FIDO

Security of mobile devices, cards and tokens

- **Topics related to security of mobile devices**
  - Implementation and management of secure storage for credentials and software, interfaces
  - Security of user interfaces (keyboard, display)
- **Professional solutions require**
  - Security analysis of the entire system incl. mobile devices and integrated secure element, SIM
  - Definition of practical, scalable security measures
- **Comparability of security levels**
  - Security demand depends on applications, offered products and services
  - Business partners have to be sure that the partner's equipment supports the required security level
  - ➲ Introduction of security classes (e.g. normal, high and very high protection) **and / or trust levels (i. e. different levels of verified ID data)**
  - ➲ Definition of requirements per class → protection profiles, security targets
  - ➲ Introduction of certification for the demanding security classes

Secure ID & Mobility
Requirements of Strong ID for Mobile Usage

- **Market needs**
  - **Mobile internet usage** is increasing rapidly
  - **E-Government usage** in GER > 45% in 2014
  - **Passwords** alone not **adequate** for strong ID



- **Security element with complex communication interface required**
  - Compatibility between **NFC** mobile devices and **ISO** smart cards
  - Sufficient **field strength** required
  - Transfer **big size of data**
  - **Integration** of strong ID token in **mobile platforms**
    - either: external token, SIM, SD-Card, or embedded SE

Solution approach

Introduction of the **mobile ID management** as synergetic combination of primary ID, derived IDs and two-factor authentication:

- German eID card for identification-centric use cases
  - Serves as electronic primary ID and trusted token for authorization
  - Authentication (i.e. as fallback solution for FIDO, and resetting of FIDO authentication for the dedicated user account)
- **FIDO two-factor authentication** for authentication-centric use cases
  - FIDO-relation to a personal account will be established after creating the account and its derived ID. **Derived ID could be created by the Service provider or taken from a token from an ID-provider.** Works for personalized and pseudonym accounts.
  - Could be established either on or off token, i.e. using a derived ID stored on the token or connected with the personal account in the back end system
  - Can be implemented in external cards / tokens or in the secure space of mobile devices
  - Supports authentication with several tokens or user devices to the same account
- **NFC as preferred interface** between mobile device and external cards and tokens
  - Only common interface of mobile devices that supports passive secure eID, transportation and payment cards / infrastructures
  - Supports implementation of FIDO on deployed basis of transportation cards, etc.

The German National ID-Card
Derived Identities

Primary Identity

1. Transfer Datagroups

Authentic Data + **Identifier (secret)** = **Derived Identity**

2. Register Authentication Device (build secret)

Technologies for Derived Identities

Authentication Systems

SSL

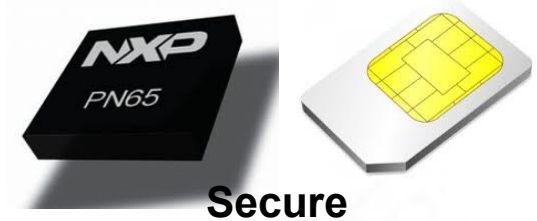
SSL

fido alliance

OpenID®

OAUTH 2

Authentication Devices



Secure Elements

Mobile Connect

Yubikey

VDV core app

German National Project “NFC-Initiative”
Strong ID for Public Transport

BVG

+

1. Creating and Managing of a Customer Account

BVG

+

2. Creating and secure storage of a derived identity

BVG

+

+

3. Contactless purchasing and paying of a ticket by using a derived identity

4. Contactless ticketing by using a smartphone

Secure and safe identification

Comfortable use

German National Project “NFC-Initiative” Project Partners

- The NFC initiative is ...
  - a joint activity of the BMI, BMWi and the BMVI in the context of the “Digital Agenda”
  - with the participation of German industry, represented by the following companies:

  - supported by the Federal Office for Information Security in Germany.
- Challenges for the NFC initiative:
  - Harmonization of standardization in various committees focusing on NFC Forum

  - Target: Functionality is important, therefore interoperability before strict conformity
  - Field implementation as a "proof-of-concept" for technical specifications and acceptance of public transport companies and their customers

➡ comfortable and safe ticketing for the citizens!

Implementation of the FIDO authentication function

- In principle, the **FIDO authentication** function could be implemented in
  - the **mobile device** (preferably in a secure space)
  - **external tokens with "vicinity"-interface** → connects automatically as soon as in reach (e.g. Bluetooth Low Energy / max. 10 m)
  - **external tokens with "proximity"- interface** → very short reading distance, requires user-action to connect (e.g. NFC / max. 0,05 m)
- Considerations
  - Having all mobile devices equipped with integrated FIDO function incl. credentials would probably be the **most convenient solution** for the user
  - Today's mobile devices usually don't provide secure user interfaces. The password or the bio-data could be eavesdropped by a malware when entered
  - An **external token** can be used with several mobile devices, also those of friends, etc.
  - **Certified contactless chipcards** available (Signature cards, partly in Banking, Ticketing)
- **External proximity tokens seem to be the best choice**
  - Proximity connection principle makes attacks by eavesdropped password difficult
  - Certified security solutions available, existing cards can be used → reduces invest

Achievements

The German solution approach is still on its way. However, there are already achievements and experiences that we are willing to share:

- **German ID-card (Primary eID) and related infrastructure established**
  - > 35 Million cards in the field
  - Based on open implementation and test standards → CC certified solution
  - Maintenance and continuous improvement covered by federal activities
- **Infrastructures of service providers match the eID-concept**
  - Example: German Public Transport Service Providers, Financial industry
  - Extensive application testing
- **Leading position in international standardization**
  - eID-infrastructures require long-term support by the industry → open technology basis and documentation in standards
  - Experts contributing to the relevant standardization bodies
- **Strong industry in identity management, security management, secure semiconductors and chipcards**
- **Leading testing houses**

Perspectives

Corner stones of the German approach:

1) **German eID-card as primary ID** and foundation of the **mobile ID-management approach**, generation and use of **derived eID** complementing the primary ID
2) **Structured system approach** with clear differentiation and **defined interfaces** between **identification** and **authentication-centered** use cases and solutions.
3) **External tokens with NFC interface** as preferred solution for identification and authentication
4) **Introduction of FIDO** as open authentication solution with significant market reach
5) **Scalable security classes and trust levels** for hardware and ID data
6) **Focus on privacy and user-centricity**
7) **Open specifications and test concepts** -> available to any supplier and operator, platform independent

Summary

- Growing risks through **misuse of conventional IDs** (passwords)
- Digital society requires **strong IDs** with **Secure Elements** and **2-Factor Authentication**
- **Regulatory Framework** required for sufficient **Technical ID-Standards** in critical areas
- **European Market has a sufficient size** to set future eID-Standards

Contact

Federal Office
for Information Security (BSI)

Joachim Weber
Godesberger Allee 185-189
53175 Bonn
Germany

joachim.weber@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de