MOBILE-ID BASED ON SECURE ELEMENTS

Dr. Matthias Schwan | Tim Ohlendorf

Abstract

This paper proposes a technical realization of an eID-Scheme including mobile devices, which is based on the existing German eID-Scheme by deriving identity data from the German eID-Card into a secure element embedded in a smartphone. The paper introduces and discusses the system architecture and provides user stories. This work is done within the BMWi funded project OPTIMOS2.0.

1 Background

The German eID-Scheme including the »Online-Ausweisfunktion« [BSI17b] has been notified by the German Federal Ministry of the Interior in accordance to the eIDAS Regulation [BSI17c] [EU99] to the European Commission with a Level of Assurance »high« [BSI17a]. The notification gives German citizens and holders of a German Residence Permit the opportunity to use eGovernment services offered by other Member States of the EU requiring an assurance level up to »high«.

Cities and communities in the EU as well as in Germany are about to offer more and more electronic eGovernment service to their citizens and companies. These services go beyond the traditional service of official ID management (e.g. issuance of passports, driver›s licenses, birth certificates, living address). The majority of these eGovernment services does not require an assurance level »high« but require a cost-efficient integration of an eID-scheme for the online service providers and comfortable use of the identification means for the citizen.

Mobile devices, in particular smartphones, are today the perfect carrier of identification data as they have become personal devices of citizen and provide a high level of user convenience together with a certain level of security. A number of examples of eID-Schemes based on mobile devices can be found, such as Estonia, Moldova, Finland, UAE, Austria, Iceland, Turkey and in the US (driver›s license). International standards exist (e.g. by Global Platform and GSMA) or are under development (e.g. ISO/IEC 18013-5 on mobile driver›s license, digital travel credentials for passports and ISO/IEC 23220 on generic mobile ID functions and protocols).

The German BMWi launched an R&D project »OPTIMOS 2.0« [OPTI18] in 2018 that aims at creating an open, usable and secure identity eco-system for mobile services. The project partners including German BSI develop a proof-of-concept eID-Scheme based on mobile devices that enhances the existing German eID-Scheme of assurance level »high« and that is suitable to be additionally notified in accordance to the eIDAS Regulation with a Level of Assurance »substantial« and a high level of user convenience.

First proposals of a German mobile eID-Scheme that influenced this proposal can be found in [DiKr12] [Kahl18] [Otte16] and [Schr13].

2 Introduction into »Mobile-ID« ecosystem

A »Mobile-ID« cannot just be considered as an »app on a phone« but as a mobile eID-System consisting of:

- an application installed and running on the mobile device, i.e. an »App«,
- an application installed and running on the secure element embedded in the mobile device, i.e. an »Applet«,
- a verification component running on a mobile device or on a remote server,
- a number of interacting infrastructures managing the
  - app-provisioning for mobile devices
  - applet-provisioning for secure elements controlled by a mobile device
  - personalization of user attributes and credentials
  - revocation and renewal of user attributes and credentials.

Further a mobile eID-System describes two basic use cases. One use case adapts the identification process known from physical identity cards. That is, a citizen presents or hands over its identity card to an official or another citizen for identification purposes. This is also called a peer-to-peer use case. In the electronic scenario, the electronic identity data is transmitted from the citizen›s mobile device to the mobile device of the verifying person that in turn can electronically proof the integrity and authenticity of the identity data that include the face image (as usually printed on physical identity cards). The verifying person must compare the electronic and visualized image with the presenting citizen (see Figure 1). The transmission of the data from one mobile device to the verifying mobile devices can be realized in different ways, dependent on the capabilities of the mobile devices. Options are an optical transmission by using the display and camera, a Bluetooth, WiFi (direct) or NFC connection.

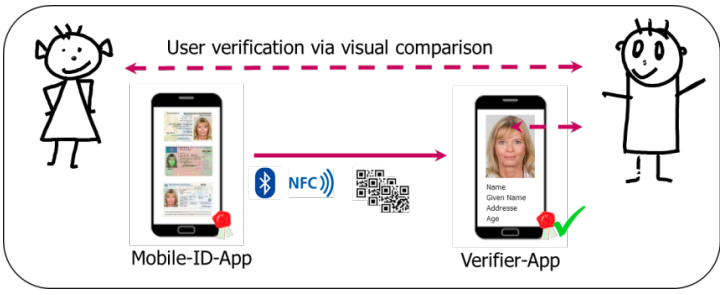

Figure 1 peer-to-peer use case

The second basic use case describes the identification and authentication of a citizen towards a remote service offering online services over the internet (see Figure 2). In contrast to the pee-to-peer use case the remote service cannot proof the binding between the user and the electronic identity data via comparison of e.g. the face image. User authentication mechanism provided locally by the mobile device may be chosen, e.g. PIN verification, fingerprint, face or iris recognition. Trust in the chosen authentication mechanism must be established between the Mobile-ID App and the verifying party.

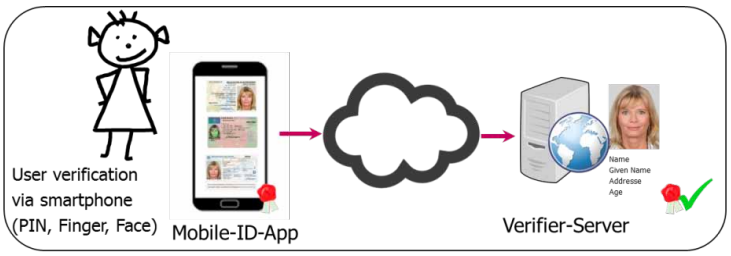

Figure 2 use case of identification towards online service

3 Requirements of »Mobile-ID« system

Functional as well as non-functional requirements describe features and/or functions that are to be implemented in order to enable users of the Mobile-ID Application to accomplish their tasks. Here:

- personalization of the App and
- identification towards online services.

The functional (FR) and non-functional (NR) requirements include:

FR1 A user can identify and authenticate with its mobile device without any further hardware and by using password or fingerprint or face recognition.

FR2 The Mobile-ID App must run on mobile devices providing an embedded secure element (eSE).

FR3 The Mobile-ID App must enable remote identification.

FR4 The user attributes are locally stored on the mobile device.

FR5 Only the authorized owner of the mobile ID can use the Mobile-ID App.

FR6 The Mobile-ID App and system must fulfill the requirements of eIDAS

FR7 assurance level substantial in particular:

- 2-factor authentication (FR6)
- dynamic authentication (FR7)

NR1 The Mobile-ID App and system must integrate into the existing German eID-System infrastructure.

NR2 The Mobile-ID App and system must meet the same data privacy principles as the existing German eID-System.

NR3 The Mobile-ID App and system must fulfill the requirements of eIDAS assurance level substantial in particular: the dynamic authentication mechanism must be resistant against »moderate attack potential«.

4 System architecture of »Mobile-ID« system

4.1 General approach

The proposed system architecture enhances the existing eID Server and eID Client component of the German eID-System [BSI17b] including the PKI for authorization certificates. A web service may either apply for its own authorization certificate and may use an eID Service that operates the eID Server on his behalf or may use an identification service provider that operates the eID Server. The interface to the eID Server, i.e. today a SAML or OIDC interface, is enhanced by the possibility to request further attributes and to set a minimal required assurance level, i.e. »substantial« or »high«, as well as by receiving the requested attributes (see NR1 and FR3).

The user attributes are stored on the mobile device within the Mobile-ID App and/or eID Applet residing on a secure element (see FR4). The enhanced eID Server and Mobile-ID App together with the eID Client and eID Applet do perform a Terminal Authentication using authorization certificates together with a Chip Authentication according to BSI TR-03110 [BSI16a]. The Chip Authentication protocol provides session keys fulfilling the requirement of »dynamic authentication« (see FR7). Access authorization to the private Chip Authentication key requires user authentication by fingerprint recognition or PIN verification performed by the operating system of the mobile device. A successful Chip Authentication is required to get access to the user attributes (see FR5). The 2-factor authentication

is achieved by possession of the private key, i.e. possession of the mobile device, and knowledge or biometrics (see FR6).

The management of the sensitive key material, i.e. private key for Chip Authentication, is done within an applet installed on a secure element. This design decision potentially allows for resistance of attack potential moderate (see NR3). This requires a correct implementation of the cryptographic primitives and protocols within the applet and Java OS. Trust in such implementation is usually achieved by a third-party evaluation and certification under the Common Criteria scheme. One possible approach to achieve such certification in a mobile device can be found in [Kueg18].

In the following, the provisioning and personalization system, as well as the online-identification process are explained in detail. Further phases of the identity lifecycle (e.g. deprovisioning, revocation, …) are not in the scope of this paper and are therefore not presented in detail.

4.2 Provisioning and personalization system

The deployment of the Mobile-ID can be divided into two general phases. In the first phase, the user who wants to register for the Mobile-ID on a mobile device gets identified and authenticated via its German eID ("Online-Ausweisfunktion"). In the second phase, the user's attributes gathered from the German eID process are used to generate a derived identity which is then deployed into the Mobile-ID App on the user's mobile device.

Figure 3 shows the two phases in detail: In a first step, the user downloads the Mobile-ID App from the mobile device's application store and installs it. After first launch, the Mobile-ID App connects to the personalization service, called PersoService and triggers a personalization request (see step 1). An eID process is performed between the embedded eID Client, e.g. AusweisApp2, the eID Server and the PersoService, acting as service provider (see steps 2, 3, 4). With the acquired user attributes from the eID process, the PersoService then generates a personalized eID Applet and deploys it via a third-party, called Trusted Service Manager (TSM) into the mobile device's secure element (see steps 5, 6 & FR2). The Mobile-ID App can now communicate with the eID Applet (see step 7).

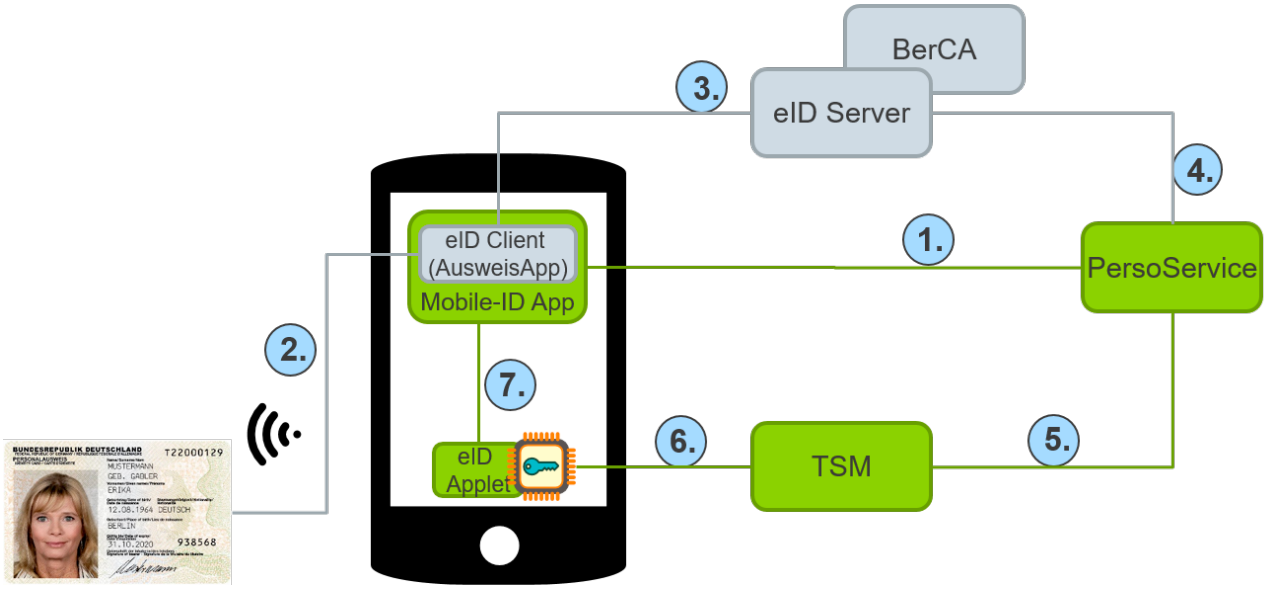

Figure 3 system architecture of personalization

Optionally, instead of deploying an already personalized eID Applet onto the user's mobile device (see steps 6, 7), deploying an unpersonalized eID Applet first and personalizing it later would also be possible.

4.3 Online-Identification system

Figure 4 shows the components and parties involved in an exemplary online-identification process. First, the user browses a web service with its mobile browser. Then, the web service requests a registration and the user chooses to register with the Mobile-ID App that is called by the mobile browser (see step 1). In step 2, the Mobile-ID App connects to the eID Server and performs a Terminal Authentication (TA). The TA determines the access permissions of the eID Server (on behalf of the web service) to the user attributes stored within the Mobile-ID App and/or eID Applet. In detail, the permissions are defined in the web service's authorization certificate, issued by the BerCA. In step 3, the eID Applet is authenticated and proven to be genuine by the eID Server via a chip-specific key pair, stored inside the eID Applet (Chip Authentication). Based on steps 2 and 3, a secure channel between eID Server and Mobile-ID App, respectively eID Applet is established. The user attributes, required for the registration, are then transmitted from the user's mobile device through the secure channel to the eID Server. Further, the user's attributes are passed on to the web service (see step 4). If the registration was successful, the user's mobile browser is forwarded to an authenticated session (see step 5 & FR1).

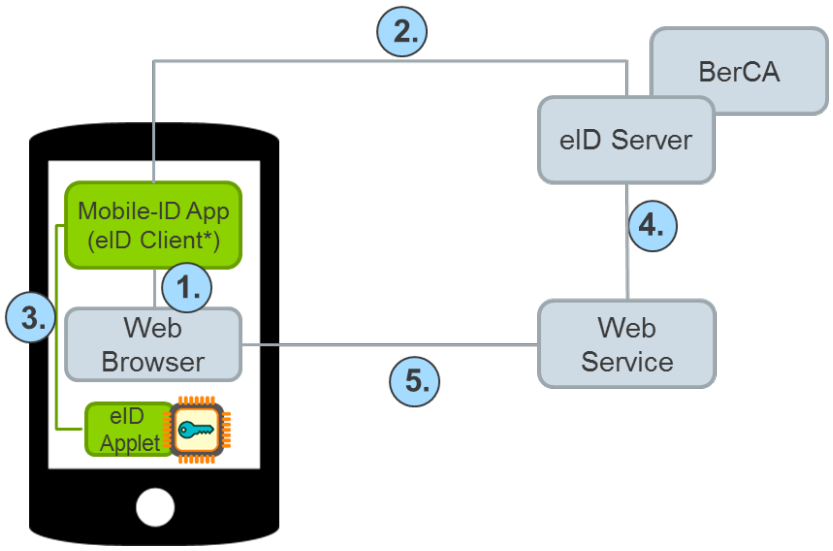

Figure 4 system architecture of online-identification

5 Prototype – »Mobile Ident«

In the following, a first prototype of the above described system is presented. The so-called Mobile Ident App, developed in the context of the OPTIMOS2 project, allows to perform functional, as well as usability tests.

5.1 Provisioning and personalization of the Mobile-ID

During the provisioning and personalization phase, a user register for a Mobile-ID with its German eID. Therefore, the Mobile Ident App must be downloaded from the mobile device's application store (e.g. Google Play). Further, it must be checked whether the mobile device's hardware fulfills the requirements needed to use the Mobile Ident App. Figure 5 provides a sequence of screenshots corresponding to the download process and requirements check:

Step 1: Download the Mobile Ident App
Step 2: Start the Mobile Ident App
Step 3: Tutorial and system requirements check starts
Step 4: Set new PIN and optionally allow fingerprint, face or iris recognition to protect ID data
Step 5: Mobile Ident App is ready to personalize one of the pre-selected virtual cards, e.g. German eID, mobile driver›s license or virtual health card

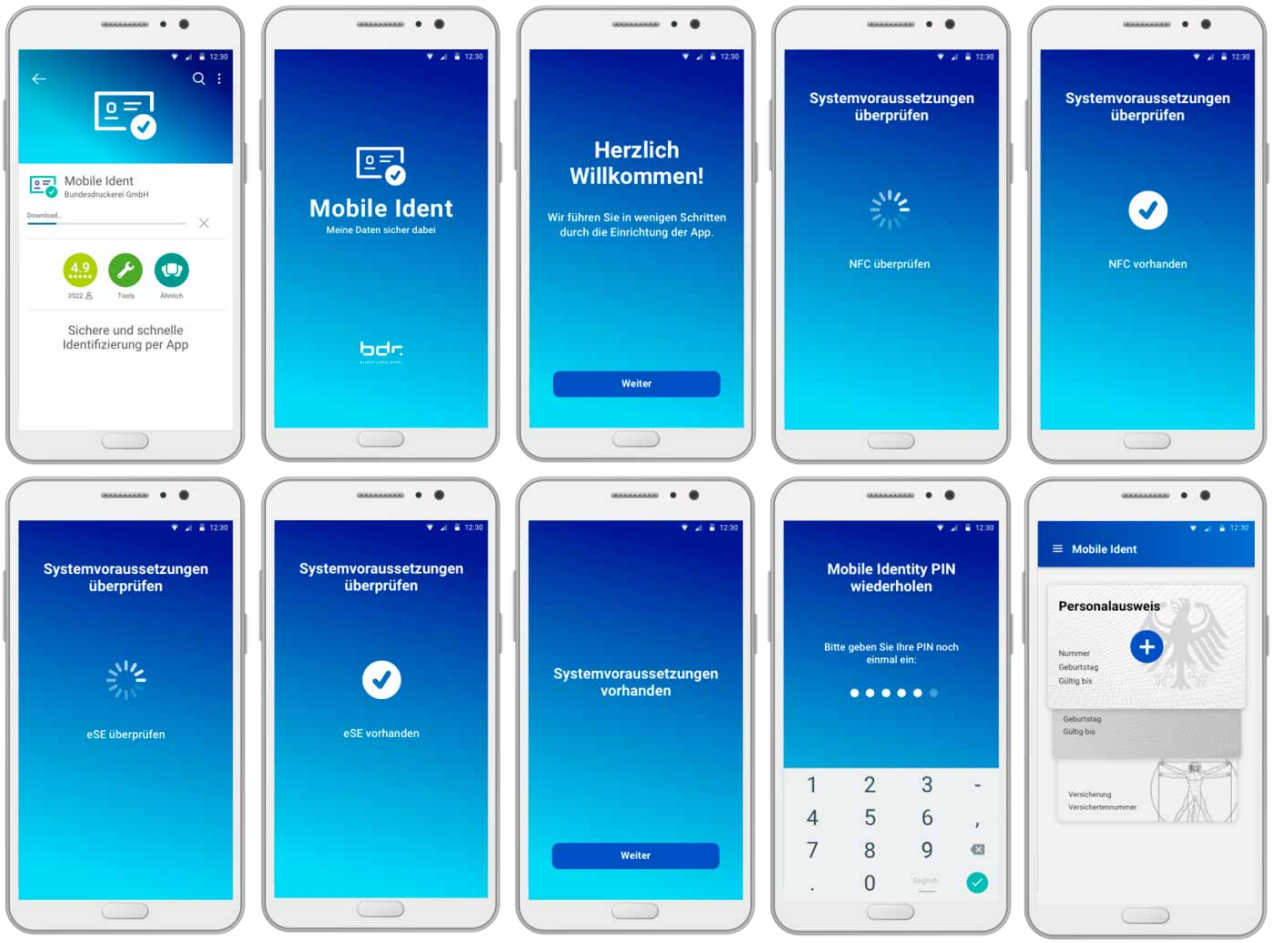

Figure 5 sequence of screens of app and applet provisioning

The sequence of steps and screens given in Figure 5 is continued by pressing the »plus« button by the user to start the issuing process with German eID card, which can be executed every time the user has started the app and authorized with the app PIN or fingerprint, face or iris recognition. The issuing process is shown in the sequence of screens in Figure 6 and explained in the corresponding enumeration below:

Step 1: User is requested for consent to read data from German eID Card
Step 2: User holds his German eID card near the NFC interface of the smartphone
Step 3: User enters his PIN of the German eID card
Step 4: Data is transferred from German eID card to personalization service and written into app and secure element
Step 5: Mobile German eID within Mobile Ident App is ready to use

5.2 Online-Identification

Figure 7 shows a sequence of screens corresponding to the online-identification process used to register or login at a web service. The following steps describe the process in detail:

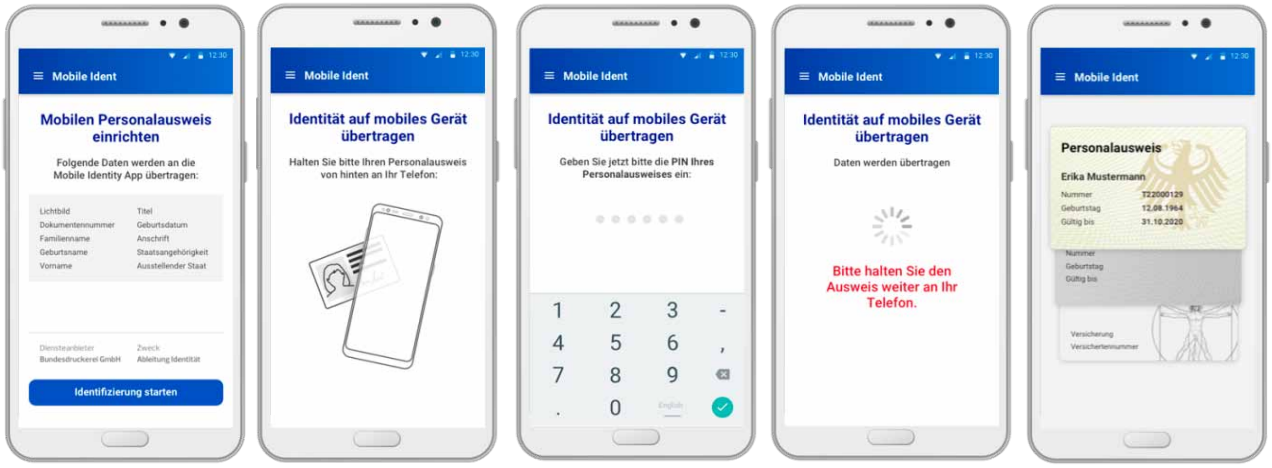

Figure 6 sequence of screens of issuing mobile German eID

Step 1: User browses webpage of demo service provider »infinishare« in order to register and rent a car. He chooses to identify with Mobile Ident

Step 2: Mobile Ident App starts and gives the information which web service requests what data for what purpose.

Step 3: Mobile Ident App requests user for consent and authentication with PIN, fingerprint, face or iris

Step 4: Data are transferred from mobile German eID to the demo service and service can finalize registration

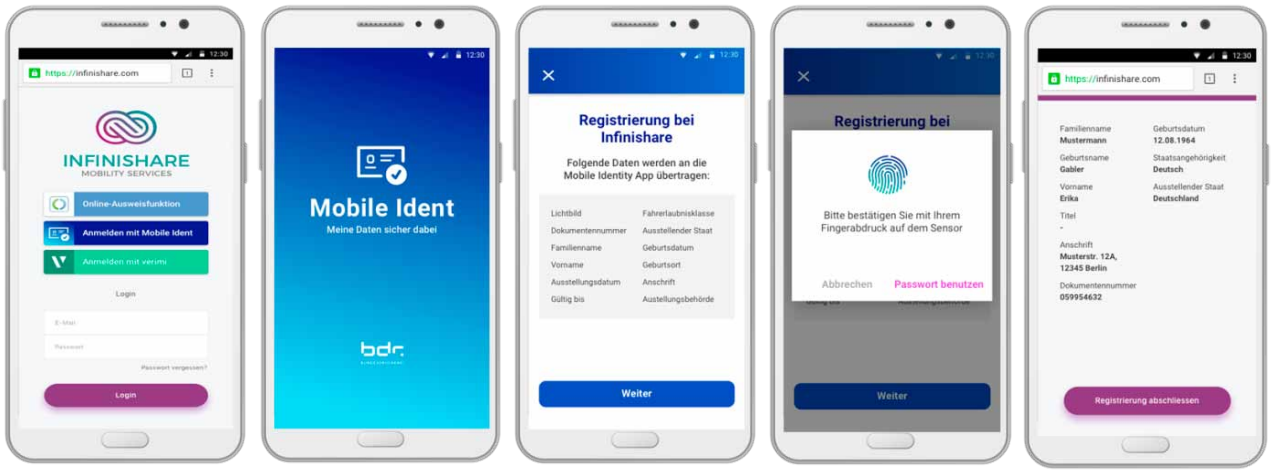

Figure 7 sequence of screens of online identification with mobile German eID

6 Outlook

Within the project OPTIMOS 2.0 the partners will elaborate the proposed system architecture and implement a proof-of-concept system. Primarily, the extent of adaption of the well-proven protocols PACE, Terminal Authentication (TA) and Chip Authentication (CA) to the environment of a mobile device as well as the work-share between the Mobile-ID App and eID Applet on a secure element is to be specified and analyzed in detail. Moreover, the deployment of the applet provisioning infrastructure, i.e. the Trusted Service Management System (TSMS), and the specification and use of the interfaces to the TSMS are the most challenging tasks in the project OPTIMOS 2.0.

References

[BSI17a] Bundesamt für Sicherheit in der Informationstechnik: German eID based on Extended Access Control v2 – LoA mapping: Mapping of the characteristics of the German eID scheme to the eIDAS Level of Assurance, Version 1.0, 20. February 2017.

[BSI17b] Bundesamt für Sicherheit in der Informationstechnik: German eID based on Extended Access Control v2 – Overview of the German eID system, Version 1.0, 20. February 2017.

[BSI17c] Bundesamt für Sicherheit in der Informationstechnik: German eID based on Extended Access Control v2 – Supporting Documentation, Version 1.0, 20. February 2017.

[BSI16a] Bundesamt für Sicherheit in der Informationstechnik: Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2, Version 2.21, 21. December 2016.

[DiKr12] Frank Dietrich, Micha Kraus: Mobile Nutzung des neuen Personalausweises, 22. Smartcard Workshop, Tagungsband, U. Waldmann (Hrsg.), Fraunhofer Verlag, 2012.

[EU99] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[Kahl18] Christian Kahlo: FIDELIO App, VX4.NET, 2018.

[Kueg18] Dennis Kügler: Digitalisierung? Mit Sicherheit!, 28. Smartcard Workshop, Tagungsband, U. Waldmann (Hrsg.), Fraunhofer Verlag, 2018.

[Otte16] Otterbein: Mobile Authentication with German eID, 2016.

[Schr13] Martin Schröder: Sichere Bereitstellung von Identitätstoken auf mobilen Endgeräten, 2013.

Dr. Matthias Schwan

Bundesdruckerei GmbH, Technology, Product and System Definition

CV

From 2007 Matthias Schwan is employed at Bundesdruckerei GmbH. In his role as product architect in the smart card group he was involved in the deployment of the second generation of the German electronic passport and German ID card. He represented Bundesdruckerei in several third-fund projects in the area of interoperable cross-border identification as STORK and TREATS as well as in the area of identification systems with mobile devices as StudIES+ and OPTIMOS. He is an active member in standardization groups of CEN and ISO in particular in ISO/IEC JTC1 SC17 WG4 leading the project 23220 »Building blocks for identity management via mobile devices« and in ISO/IEC JTC1 SC17 WG10 participating in the project 18013-5 »mobile driver›s license«.

Contact

Dr. Matthias Schwan
Technology
Bundesdruckerei GmbH
Kommandantenstraße 18
10969 Berlin
Germany
Phone: + 49 (0) 30 2598 3417
Mobile: + 49 (0) 175 2642 952
Fax: + 49 (0) 30 2598 6046
matthias.schwan@bdr.de
www.bundesdruckerei.de

Tim Ohlendorf

Freie Universität Berlin, Institut für Informatik, ID-Management Group

CV

Tim Ohlendorf is a security researcher and PhD candidate at the Identity Management Group at Freie Universität Berlin. He got his master's degree in Computer Science with a focus on IT-Security from Technische Universität Darmstadt in 2018. Currently, he is involved in the design of a secure mobile student card for Erasmus students, as well as in the implementation of a mobile version of the German ID card.

Contact

Tim Ohlendorf, M.Sc.
ID-Management Group
Institute of Computer Science
Freie Universität Berlin
Takustr. 9
14195 Berlin
Phone: +49 30 838 59541
Mobile: +49 174 261 4190
Fax: +49 30 838 475212
tim.ohlendorf@fu-berlin.de
https://www.mi.fu-berlin.de/inf/groups/ag-idm/