Mobile and User-friendly Two-Factor Authentication for Electronic Government Services Using German Electronic Identity Card and a NFC-enabled Smartphone

Michael Massoth
Department of Computer Science
Hochschule Darmstadt – University of Applied Sciences
Darmstadt, Germany
E-mail: michael.massoth@h-da.de

***Abstract*— A mobile, secure and user-friendly two-factor authentication using the German electronic identity (eID) card will be presented. The new approach shall be used for the mobile online-authentication of citizens in order to get access onto high trust level electronic government services. One part of the innovation is the use of a Near Field Communication (NFC) enabled Android smartphone as ubiquitous NFC card reader. The new approach implements a mobile, as well as a stationary authentication solution for citizens. The high trust level of the mobile online-authentication will be reached by a strong two-factor authentication with the German eID card and the corresponding 6-digit Personal Identification Number (PIN).**

Keywords-mobile authentication; identity management; strong two-factor authentication; high trust level.

I. INTRODUCTION

Due to the rapid increase of digitalization within our industry and society, more and more businesses and government agencies are offering online services where a citizen can access anywhere, anytime, using the online function of the German National electronic Identity (eID) Card. Citizens shall be able to communicate with the administration simply and securely around the clock online in order to perform necessary administrative tasks. This saves costs, the way to administration, waiting times, paper and postage. Citizens and users can identify themselves not only on the Internet, but also at vending machines and the self-service terminals in public authorities. Therefore a mobile and strong two-factor authentication using the German electronic identity (eID) card will be presented in this paper. The new approach shall be used for a quick mobile online-authentication of citizens in order to get access onto all high trust level electronic government services.

The paper is structured as follows. In Section II, the online authentication process with the German eID card and the problems of previous solutions are discussed. Section III presents some related work. Section IV introduces the new mobile AusweissApp2 for Android in Germany. The new mobile authentication approach with the citizen service app is shown in Section V. In Section VI, the new stationary authentication approach with a Quick Response (QR) code is presented in detail. Section VII gives a security evaluation of the REST-interface. Section VIII presents a security evaluation of the HTTS-interface. Section IX ends this paper with a conclusion and outlook on future work.

II. ONLINE AUTHENTICATION WITH GERMAN ID CARD

The new German National Identity Card was introduced in 2010, Dec 1st, in smart card format and with a contactless chip, see Figure 1. With this activated chip, the citizen and eID card holder can use the eID function (online function). With the eID function, the citizen can prove her or his identity in a simple, secure and quick manner on the Internet or at vending machines. The eID card chip transmits the personal data using secure connections once the user authorizes such a transmission by entering the corresponding 6-digit PIN. So a strong two-factor authentication (property and knowledge) will take place. For realization of the electronic authentication, a trusted and secure channel between the chip and the service provider will be established, using an authenticated Diffie-Hellmann key agreement protocol. Both communication parties know with whom they interact (reciprocal authentication).

The German National Identity Card offers maximum security for the personal data on the chip. This applies to both the physical security features of the document and the security technologies protecting the personal data on the chip. The eID function significantly improves data security and reduces the amount of personal data collected (data minimization). The German eID system fulfills certain strong requirements described in the technical guidelines and security advices, published by the German Federal Office for Information Security (BSI), see [1] and [2]. The security and privacy details of the German eID system were addressed in various papers and articles, see, e.g., [3] and [4].

Figure 1. German National eID Card

In order to use the activated eID function, the citizen need a NFC [10] card reader (available from various retailers) and a client software, such as AusweisApp2, which ensures a secure connection between the eID chip and the Internet service provider so that data can be exchanged in encrypted form [13]. The online authentication process with the eID card (using the example of a web service) will be explained step-by-step below:

(1) The card holder opens the provider's web service requiring online authentication.

(2) The service transmits the authentication request to the eID server.

(3) A secure channel is established between the eID server, the client software (e.g., AusweisApp2), the card reader and the ID card's chip, and the authenticity of the service provider and the authenticity and integrity of the eID card (protection against forgery) are checked.

(4) The client software shows the card holder the service provider's authorization certificate and the requested personal data categories. The eID card holder decides which personal data he/she wishes to transmit.

(5) By entering the 6-digit PIN the eID card holder confirms the transmission of his/her data.

(6) The eID card data are sent to the eID server.

(7) The eID server sends an authentication response and the eID card data to the service.

(8) The authentication response and the ID card data are retrieved. The service checks the authentication results and decides whether the authentication was successful. A response is then sent to the user and/or the service is provided.

The consumer research study of GfK, determined in May 2015, stated, that only 5% of all Germans used their eID card for online authentication services within the past 12 months [6]. Also, the "AusweisApp2" (for stationary Windows and Mac OS) was only downloaded about 180,000 times from Dec 2014 to May 2015. There are probably two main reasons for that disappointing result: First, there are only few services (55 commercial and 109 from administrations, in May 2015) with eID support available on the market. Thus, the citizen and users may not see a significant benefit in using eID. Second, for the online authentication there is a special NFC card reader needed which can cost between 30 (basic) to 160 (comfort) Euros. As interim conclusion: The necessity to purchase such an expensive NFC card reader was and is a high blocking factor for the citizens and users to make use of the online authentication function of the German eID card.

III. RELATED WORK

Other countries in Europe also provide mobile authentication solutions for their citizens and users. In Austria for example a new system called “Identity Austria” (IDA) will be introduced. With the new IDA system it will be possible for an Austrian citizen to recall and display official documents and ID cards such as a driving license, passport, e-card or approval form, on the mobile phone without having to carry the different ID cards. The cards and documents are just displayed but not stored on the smartphone. The requested data can be accessed via a centralized high-security server in the Ministry of the Interior and with the consent of the person concerned via an encrypted Internet connection. First field tests has taken place in summer 2017.

The predecessor project was “My Identity App” (MIA) [6] and was developed by the Österreichische Staatsdruckerei GmbH. MIA combines electronic formats of traditional printed ID documents and electronic identities (eID) into a platform-independent smartphone app embedded in an ID ecosystem. Authentication of MIA against the backend is performed by means of a client certificate, which is stored on the users’ smartphone. All data transfers are secured using Transport Layer Security (TLS). There are no data stored on the smartphone. Personal data and digital formats of documents and ID cards are always retrieved from a trusted high-security server of a cloud backend infrastructure. A strong two-factor authentication, e.g., with a generated one-time transaction number and a biometric fingerprint, could be performed if required for authentication and proof of identity within an online service.

In Switzerland, there is so far no national eID card available, but Swisscom provides a Mobile ID solution for secure mobile authentication via the smartphone [7]. The Swisscom Mobile ID is a public key infrastructure (PKI)-based secure authentication service that enables users of business applications to access secure accounts, platforms, applications and cloud services. Mobile ID is an application that is not installed on the smartphone, but on the subscriber identity module (SIM) card over-the-air. This makes the application work on any popular smartphone. First, the mobile phone number must be entered for registration. The Swisscom's database is then checked to ascertain whether this mobile phone number is under contract with Swisscom. Then the users home address is displayed. This has to be confirmed by the user. A Mobile ID is already preinstalled on all Swisscom SIM cards as a SIM toolkit (STK) applet, which can only be accessed by the mobile provider “over the air” (OTA) via the correct identification key. Additionally an RSA key is generated, which binds the SIM card to the specific device and thus makes it a safety token. Furthermore, a user-specific Mobile ID PIN is defined, which the user must enter each time when the RSA key, which is stored on the SIM card, is to be accessed. If the user wants to log on to a website, a four-digit number is displayed on the website. At the same time, a message is sent via the SMS channel, which contains the login location and the four-digit number. If both are matching, then the user is prompted to enter his personal Mobile ID PIN. After the correct Mobile ID PIN has been entered, a message is sent back to the sender and the login is successful.

Otterbein et al. [8] presented a new approach with “derived” identities on mobile phones. They analyzed and evaluated different kinds of hardware-based security solutions in order to protect sensitive data at the smartphone.

IV. NEW MOBILE AUSWEISAPP2 FOR ANDROID IN GERMANY

The new mobile AusweisApp2 for Android was released officially on 27th April 2017 at Google Playstore. With that client software the online identification can be used with an android smartphone or tablet (version 4.3 and higher) without an additional NFC card reader. To do so, the smartphone or tablet must have an NFC interface in the first place. The second requirement for the NFC-enabled smartphone is the support of the communication function "Extended Length". This function must be supported by both the NFC chip inside the smartphone and the firmware of the respective device manufacturer. In the third place, the NFC chip must have a sufficient field strength, which ensures that the contactless eID card is supplied with sufficient power to read the stored data. Since 3rd July 2017 the open source code of the AusweisApp2 Android release (1.12.2) is available on Github under the European Union Public License (EUPL). With the new BSI-certificated mobile AusweisApp2 it is now possible to implement a mobile two-factor authentication for online services using the German eID card and a NFC-enabled Android smartphone, as demonstrated in the following sections.

V. MOBILE AUTHENTICATION WITH CITIZEN SERVICE ACCOUNT APP

The mobile two-factor authentication using the German eID card and a NFC-enabled Android smartphone as ubiquitous NFC card reader will be presented as prove of concept, demo and practical development experience, shown in Figure 2. The new approach shall be realized for a typical electronic government service with trust level “high”.

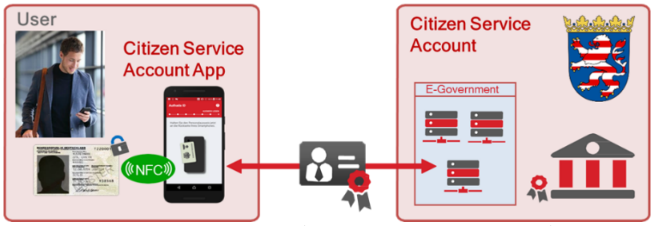
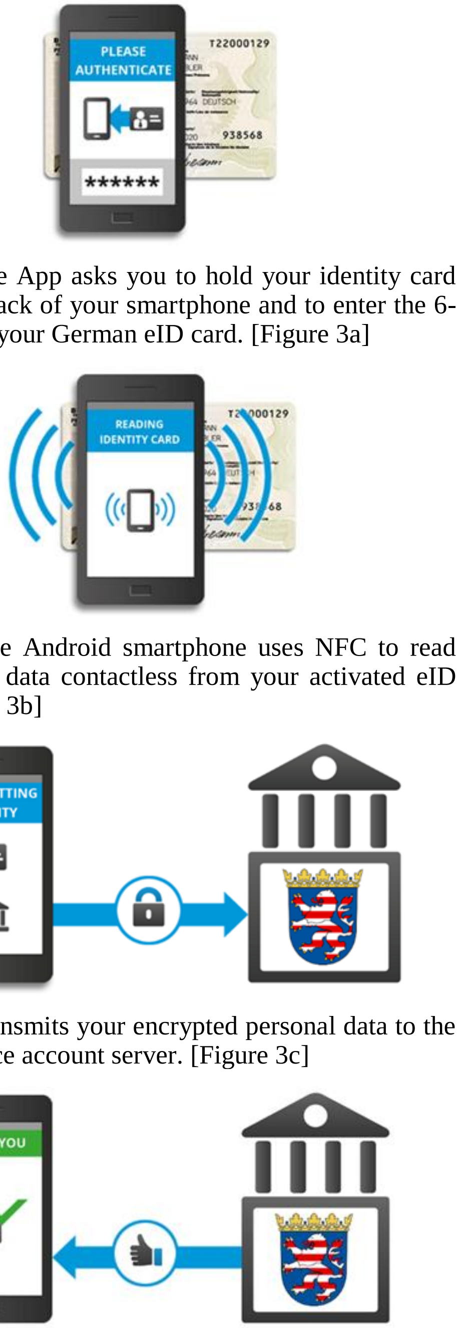


Figure 2. High level overview of the mobile authentication of a citizen

Hereby a Linux-based virtual machine from Hochschule Darmstadt (- University of Applied Sciences) is used as server platform in the backend. A Tomcat web server was installed on this site, which serves as a container for all developed web applications. A MariaDB SQL [15] database is used to store the authentication procedures, as well as the additional data of the particular e-government service. The PKI-infrastructure and the eID-Server of the Bundesdruckerei GmbH (Berlin), or as alternative the media transfer AG (Darmstadt), could be used for live testing. To enable platform-independent communication with various terminals, a Representational State Transfer (REST) [12] server based on the Jersey framework was developed as a server application. The task of the REST interface basically consists of two parts. On the one hand, it is used to authenticate a customer, using the new German eID card. It can also be used to process and terminate the particular electronic government services with trust level “high”. Further applications are possible and could be integrated into the backend architecture. The approach of a successful authentication is shown in Figure 3 below, see step (1)-(4):



Step (1): The App asks you to hold your identity card behind the back of your smartphone and to enter the 6-digit PIN of your German eID card. [Figure 3a]

Step (2): The Android smartphone uses NFC to read your private data contactless from your activated eID chip. [Figure 3b]

Step (3): Transmits your encrypted personal data to the citizen service account server. [Figure 3c]

Step (4): After successful transmission you have completed the proof of your identity. [Figure 3d]

Figure 3. Step-for-step approach for mobile authentication

The Citizen Service Account App interacts with the server via the following five essential steps:

- Request of an Authentication and Session Token
- Transmission of the Transaction Number (TAN) after successful authentication using the ID card
- Request of the user's read-out ID card data
- Transfer of the input form data
- Confirmation of the vehicle decommissioning

For this purpose, a REST client has been implemented as prototype and proof of concept, which is able to address the specified REST API of our server. The required data between the app and the server are exchanged in JSON format [17].

VI. STATIONARY AUTHENTICATION OF A CITIZEN WITH QUICK RESPONSE (QR) CODE

The complete process of online authentication of the citizen can also be done with a stationary QR code solution. The high level overview is shown in Figure 4 below:

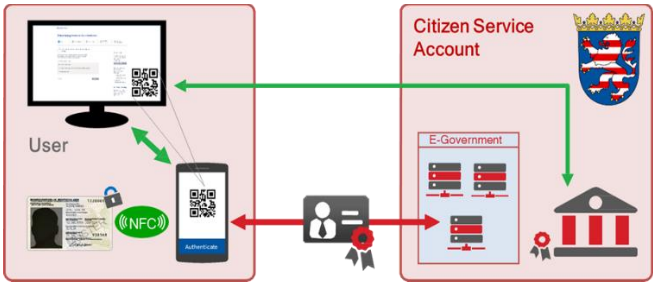


Figure 4. High level overview of the stationary authentication of a citizen

The corresponding step-by-step process for the stationary authentication of a citizen with the quick response code (QR) solution is shown in Figure 5 below:

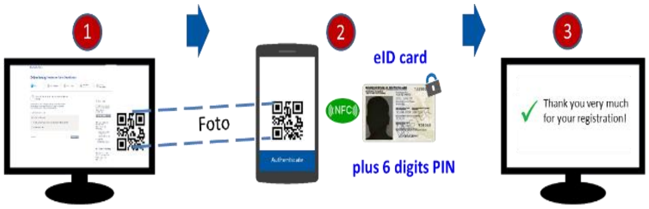


Figure 5. Step-by-step process for the stationary authentication of a citizen

In the stationary authentication approach the user performs the actual login process via the website of the e-government service account and uses the Citizen Service Account App only to scan the generated QR and set the displayed TAN into the corresponding field in the website.

As prerequisite the citizen has to download and install the citizen service account app first on a NFC-enabled Android smartphone. Then the step-by-step process for the stationary authentication of a citizen continues as following:

Step (1): The citizen opens the website of the e-government service account on the desktop PC or notebook and wants to register for the service account as a citizen for the first time.

Step (2): A QR code is then displayed on the website of the e-government service account. The citizen opens the service account app on its smartphone and scans the QR code of the website. It thus establishes a link between the smartphone's service account app and the browser-based website on the PC. He then legitimates himself with the German eID of his ID card and the corresponding 6-digit PIN.

Step (3): After successful authentication the process is terminated in the browser of the PC or Notebook.

Rest–Server: To enable a platform-independent communication with various terminals, a REST server based on the Jersey framework [16] was developed as a server application. The task of the REST interface basically consists of two parts. On one hand, it is used to authenticate a customer, using the new ID card. It can also be used to log off a vehicle after successful authentication. Further applications are possible and could be integrated into the e-government architecture.

REST contains the following five core principles:

- Unique identification (e.g., http://example.com/customers/1234)
- Links / Hypermedia (for example links and forms)
- Standard methods (GET, POST, PUT, DELETE, HEAD, OPTIONS)
- Resources and Representations (Set data format for output, such as XML, JSON)
- Stateless communication (no savings of session status)

VII. SECURITY EVALUATION OF THE REST-INTERFACE

Possible attack vectors and threats against the REST-interface are:

A. *Distributed-Denial-of-Service (DDoS) attack:*

A DDoS attack on a system with a REST interface is aimed at exploiting the limit of the API keys. Often developers do not set a limit on requests to the API when implementing the REST interface. If an attacker finds out such a REST interface, he is able to paralyze the system with frequent requests.

B. *Cross Site Request Forgery (CSRF) attack:*

In a CSRF attack, a user is given a command for a web application (e.g., in the form of a link in a guest book) by an attacker. If the user follows this link, the command is sent to the web application and executed in the context of that user. If the user is logged on to the web application, the user's trust relationship with the web application is exploited and the command is executed with the rights of the user.

C. *Countermeasure Cross Site Request Forgery (CSRF):*

As a safeguard against a CSRF attack, a secret token can be introduced that is difficult to guess by the attacker. Each time the web application views the page, that token is passed as a parameter in URLs or as a hidden field on forms (double submit cookies). For each client request, the web application checks whether the transmitted token matches the value stored for the session. If an error occurs, the requested call is rejected. Without knowledge of this token an attacker cannot adjust a valid HTTP request. For high-security web applications, consider creating the token for each request so that each time the web application is called, a new token is sent to the client, which must then be used in the subsequent request [19].

VIII. SECURITY EVALUATION OF THE HTTPS-INTERFACE

All HTTPS connections of the prototype are implemented and realized with TLS 1.2. The current version TLS 1.2 is specified in RFC 5246. Unlike its predecessor Secure Sockets Layer (SSL), TLS uses the cryptographically more secure keyed-hash message authentication code (HMAC) method to calculate message authentication code (MAC) values. TLS also uses a modified key generation method, which provides greater robustness against attacks on hash values used in key generation as pseudo-random number generators. TLS has also extended the amount of alert messages, with all extensions classified as fatal alerts. Examples of such extensions are the warnings that an unknown Certification Authority (CA) has been specified, or that a decryption operation has failed.

One possible attack vector and threat against the HTTPS-interface shall be discussed here in more detail. The Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext (BREACH) attack is a security exploit against HTTPS when using HTTP compression. [18]

The BREACH attack was discovered in 2013. This type of data theft exploits the data compression and data encryption used by websites to speed up page load times, save bandwidth, and secure data during transmission. While the BREACH attack does not directly address SSL security, it compromises the privacy goals of SSL because HTTPS is used only to encrypt page headers and disclose other content. Hackers use a combination of brute-force attacks and divide-and-conquer methods in BREACH attacks to gain access to credentials, email addresses, and other sensitive and personal information from SSL-enabled sites. BREACH attacks work with all versions of the SSL and TLS protocol and with any type of ciphers collection, as long as the following conditions are met:

- The web application is served via HTTP-level compression and contains user-provided data and a static secret in the HTTP response text.
- The attacker knows what he is looking for and is able to monitor the traffic between the user and the web application to get the length of the HTTP responses.
- The attacker can persuade the user to visit a malicious scripting site and then inject a man-in-the-browser malware that can send requests to the target site.

By injecting plain text into an HTTPS request and observing the length of the compressed HTTPS responses, an attacker is able to iteratively guess and derive plaintext secrets from an SSL stream. [18]
BREACH attacks only require a few thousand queries and can be completed in less than 60 seconds. There is no practical way to turn off the attack.

Some countermeasures in order to give a higher protection against BREACH attacks are:

- One possible safeguard is to disable HTTP compression. This leads to reduced performance and increased bandwidth usage.
- Other measures include the separation of secrets and user input or a limitation of the rate limit for queries to the server. Most protections against BREACH attacks are application-specific or require improved information security practices to handle sensitive data.
- As a further preventive measure, security management for web applications can be implemented and a web application firewall can be used to detect and block malicious clients. [18]

In the following subsections, we discuss some additional countermeasures in order to protect the implemented HTTPS and TLS1.2 connections.

A. *Countermeasure TLS backward compatibility (TLS):*

Incorrect configuration of the TLS 1.2 interface allows entry into the connection. If the connection is broken, there is the potential for man-in-the-middle attacks and phishing attacks. A correct configuration of the extensive TLS connection ensures long-term protection against these intrusion attempts.

By default, TLS 1.2 allows backward compatibility with older versions of TLS. Older versions of TLS offer more vulnerabilities and poorer cryptographic properties. It is advisable to only accept TLS 1.2 and to block all clients with older versions in case of a handshake at the beginning of the connection.

B. *Countermeasure Cipher Suites (TLS):*

The range of cipher suites is large at TLS 1.2, but some are no longer safe. The BSI recommends either Galois / Counter Mode (GCM) or Cipher Block Chaining (CBC). Both are currently considered safe and must continue to be supported until at least 2023. The TLS connection should be set to GCM at least for machine-to-machine connection. With GCM, the real key is never transferred and the temporary key is destroyed. This means that even if an attacker breaks the connection and obtains the private key, unlike CBC, he cannot make the content. Furthermore, the BSI recommends the Elliptic Curve Digital Signature Algorithm (ECDSA) which uses elliptic curve cryptography. ECDSA is recommended here due to the short keys and good performance.

C. *Countermeasure DDoS on HTTPS:*

It is strongly recommended, that the IP range allowed for HTTPS connections shall be truncated, so that only the IP addresses of legitimate connection partners will remain.

IX. CONCLUSION AND OUTLOOK

The new approach and solution has implemented a mobile strong two-factor authentication with German eID card and the corresponding 6-digit PIN, whereby a NFC-enabled Android smartphone will be used. The new mobile solution overcomes the need to buy an expensive NFC card reader. Instead, the NFC-enabled Android smartphone will be used as ubiquitous NFC card reader.

The new approach shall be used for the quick mobile authentication of citizens in order to get access onto electronic government services with trust level "high", like, e.g., the citizen service account.

Advantages for the citizens and users are:

- Mobile and stationary web-based use
- Identification within seconds
- Easily proof of the citizens identity with legal security
- Without biometry, texting, and media breaks.
- Replacement of expensive card reader
- Save the way to the government agency and the long waiting times,

Advantages for the government:

- Sovereign digital identity data
- Strong two-factor authentication suitable for all government services with trust level "high" (and below)
- No media disruption
- High processing speed
- Cost savings and reductions
- High satisfaction of citizens and users

Future work: The new approach will be implemented and used for the de-registration of a vehicle as off the road.

ACKNOWLEDGMENTS

This work was supported by the Hessian Ministry of the Interior and Sports (HMdIS, Government of the Federal State of Hessen) [14], Project "Mobiles Servicekonto Hessen".

REFERENCES

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI): Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token (2015). https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-2-V2_2.pdf. Last accessed 06th Dec 2017.

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI): Technische Richtlinie 03112 – Das eCard-API-Framework (2014). https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03112/index_htm.html. Last accessed 06th Dec 2017.

[3] Bender, J., Dagdelen, Ö., Fischlin, M. and Kügler, D.: "Security analysis of the pace key-agreement protocol." International Conference on Information Security. Springer Berlin Heidelberg (2009).

[4] Bender, J., Dagdelen, Ö., Fischlin, M., and Kügler, D.: "The PACE— AA protocol for machine readable travel documents, and its security." International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg (2012).

[5] http://www.gfk.com, last access 9th Dec 2017.
GfK SE (2015) Fünf Prozent nutzen den elektronischen Personalausweis. http://www.gfk.com/insights/news/fuenf-prozent-nutzen-elektronischen-personalausweis. Last accessed: 06th Dec 2017.

[6] Österreichische Staatsdruckerei GmbH, MIA – My Identity App. https://www.mia.at. Last accessed 06th Dec 2017.

[7] Swisscom Mobile ID, https://www.swisscom.ch/de/business/mobile-id/overview.html. Last accessed 06th Dec 2017.

[8] Florian Otterbein, Tim Ohlendorf, and Marian Margraf: "Mobile Authentication with German eID", IFIP Summer School 2016.

[9] http://www.egov4dev.org/success/definitions.shtml, last access 4th Dec 2017.

[10] http://nearfieldcommunication.org/, last access 6th Dec 2017.

[11] http://www.investopedia.com/terms/q/quick-response-qr-code.asp, last access 7th Dec 2017.

[12] REST: www.restapitutorial.com/lessons/whatisrest.html, last access 9th Dec 2017.

[13] AusweisApp2 can be downloaded for free at: www.ausweisapp.bund.de, last access 7th Dec 2017.

[14] https://english.hessen.de, last access 6th Dec 2017

[15] https://mariadb.org, last access 8th Dec 2017

[16] https://jersey.github.io, last access 8th Dec 2017.

[17] http://www.json.org, last access 8th Dec 2017.

[18] „Akamai BREACH-Attack" [Online]. Available: https://www.akamai.com/de/de/resources/breach-attack.jsp Last access 11st Dec 2017

[19] BSI, Prevention of Cross-Site Request Forgery https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04403.html Last access 11st Dec 2017

ISBN: 978-1-61208-615-6