Secure and User-friendly De-Registration of a Vehicle as Off The Road Using Mobile Authentication with German eID 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— **Digitization is as important to public administration as it is to the economy. Therefore, the German authorities currently see an enormous need for action for digitization and cybersecurity. Provided by the German electronic identity (eID) solution, every German citizen has the ability to identify himself against various electronic and mobile government services. In this paper, we will present a new approach for a mobile de-registration of a vehicle as off the road. The new mobile de-registration service of a vehicle as off the road is secure and user-friendly. The new approach implements a strong two-factor authentication with German eID card and the corresponding 6-digits personal identification number (PIN), whereby a Near Field Communication (NFC) enabled Android smartphone will be used as ubiquitous NFC card reader.**

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

I. INTRODUCTION AND MOTIVATION

Digital identities have gained more and more importance due to the rapid increase of digitalization within our administration, business, industry, and information society. In this paper, we present a new mobile e-government application using the new German National Identity Card with the electronic identity (eID) function for Internet use. In cooperation with the Hessian Ministry of the Interior (Government of the Federal State of Hessen) [10], as well as AUTHADA GmbH [11] and the ekom21 KGRZ Hessen [12], a secure and user-friendly de-registration of a car as off the road mobile e-government service will be presented.

The consumer research company GfK [13] determined in May 2015 that only 5% of all Germans used their eID function of the National Identity Card for online authentication services within the past 12 months [6]. Most probably, there are two main reasons for that disappointing result: First, there are only few services (164 in total, 2015-05) with eID support available on the market. Thus, the German citizen may not see a significant benefit in using eID. Second, for the online authentication, there is a special eID card reader needed, which costs between 30 and 160 Euros. For eID card holders, the need of an expensive card reader may be the biggest barrier. We will overcome this barrier and present a new approach where an NFC-enabled Android smartphone is used as ubiquitous eID card reader.

In order to demonstrate a significant benefit for the citizens and users, we implemented the new approach for a very popular and useful online service, namely, the de-registration of a vehicle as off the road. Therefore, an Android app and a Website were implemented in order to be able to carry out the complete process of the vehicle de-registration in a mobile and user-friendly way in order to provide the Hessian citizens the possibility to avoid the annoying paperwork and the long waiting time. The de-registration of a vehicle as off the road is also a good best-practice example of an electronic government service with required trust level “high”. The paper is structured as follows. In Section II, some definitions of terms are given. Section III shows the stationary Internet-based de-registration of a vehicle as off the road. Following this, Section IV introduces the new German National Identity Card with eID function for Internet use. The stationary online authentication process is shown in Section V. In Section VI, the new mobile authentication process is presented in detail. Section VII ends this paper with a conclusion and outlook on future work.

II. DEFINITIONS AND FUNDAMENTALS

Electronic government (e-government) [1] is the use of electronic communications devices, computers and the Internet to provide public services to citizens and other persons in a country or region. Electronic authentication [2] is the process of establishing confidence in user identities, electronically presented to an information system. Digital authentication or e-authentication may be used synonymously when referring to the authentication process that confirms or certifies a person's identity and works.

AUTHADA ID Service [5] is a server operated by the company AUTHADA GmbH. This provides the authentication process via an API, or a software development kit (SDK). The AUTHADA ID service serves as an interface to a certified e-ID server, which is authorized to read the data from the personal ID card. Within the implemented representational state transfer (REST) server [5], a Java library was included, which contains the calls to the AUTHADA service. Near field communication (NFC) [3] is a set of communication protocols which allow the communication between two devices by bringing them within 4 cm of each other. Quick Response Code (QR code) [4] is a machine-readable optical label that contains information about the item to which it is attached. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to efficiently store data. Representational state transfer (REST) [5] relies on a stateless, client-server, cacheable communications protocol -- and in virtually all cases, the Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS) 1.2 is used, also known as HTTP Secure (HTTPS). REST is often used in mobile applications, social networking Web sites, mashup tools and automated business processes. The REST style emphasizes that interactions between clients and services is enhanced by having a limited number of operations (verbs). Flexibility is provided by assigning resources (nouns) their own unique universal resource indicators (URIs).

III. INTERNET-BASED DE-REGISTRATION OF A VEHICLE AS OF THE ROAD

Since January 1st 2015, it is possible to request the de-registration of a motor vehicle (car) as off the road online.

The following prerequisites are hereby necessary:

- New German National Identity card (Figure 5) with activated online eID function for Internet use and a correspondent card reader.
- Certificate of approval Part I ("vehicle registration", in German "Fahrzeugschein") with concealed security code, see Figure 1.
- License plates (front and back) with new stamped chain with concealed security code (vehicles which have been registered or re-registered since January 1st, 2015), see Figure 3.

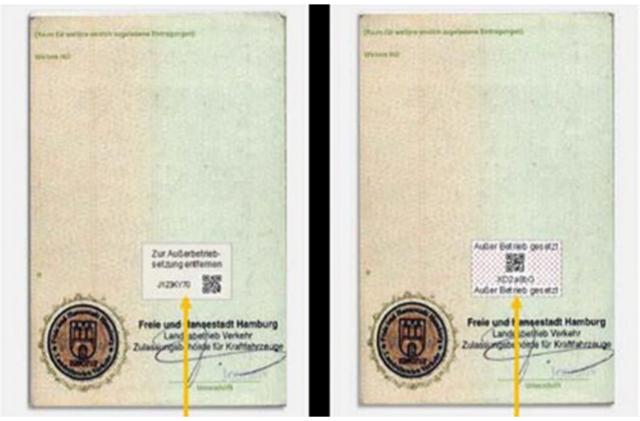

Zur Außerbetrieb-setzung entfernen
Außer Betrieb gesetzt
Außer Betrieb gesetzt
Freie und Hansestadt Hamburg
Landesbetrieb Verkehr
Zulassungsbehörde für Kraftfahrzeuge
Freie und Hansestadt Hamburg
Landesbetrieb Verkehr
Zulassungsbehörde für Kraftfahrzeuge

Figure 1. Certificate of Approval Part I ("vehicle registration") with concealed (left) and uncovered (right) security code.

The application is as follows:

(1) Take the Certificate of approval Part I ("vehicle registration", see Figure 1). On the backside of the approval certificate Part I ("vehicle registration") there is a seal label with the concealed security code (a security code example is shown in Figure 2).

(2) Figure 2 shows three different states of scratching and un-coveing the 7-digits security code of the seal label: (On the left) original seal label on Certificate of Approval Part I ("vehicle registration"), (middle) scratched and partly un-covered security code, and (right) the 7-digits security code completely scratched and un-covered.

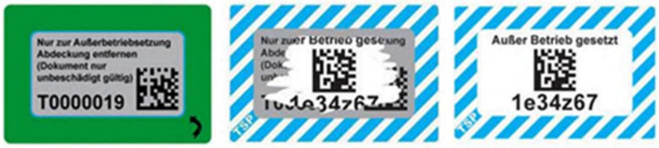

Nur zur Außerbetriebsetzung Abdeckung entfernen (Dokument nur unbeschädigt gültig)
T0000019
Nur zur Betrieb gesetzung
1e34z67
Außer Betrieb gesetzt
1e34z67
TSP
TSP

Figure 2. Seal label on Certificate of Approval Part I ("vehicle registration",)

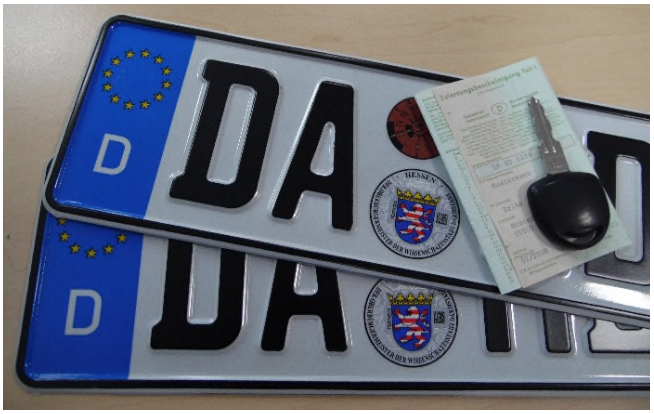


Figure 3. License plates with seal labels, which contains the concealed 3-digits security codes, and Certificate of Approval Part I ("vehicle registration", see Figure 1) with concealed 7-digits security code.

(3) Take both license plates (front and back) with the seal labels, which contain the concealed security codes. Scratch and un-cover the two 3-digits security codes of the seal labels. (One security code is shown in Figure 4).

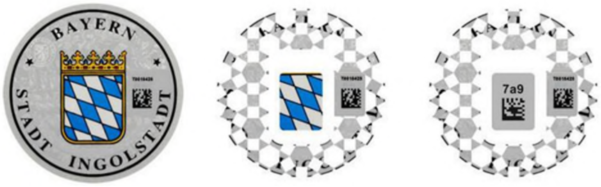


Figure 4. Seal label on license plate (left), scratching and un-cover the security code (middle), 3-digits security code (right).

(4) Scan the security code or scan it as a data matrix code (QR code).

(5) Online-Identification of the vehicle owner using the German identity card (eID) with online function, or electronic residence permit (eAT) with online function, on the Website of the central, municipal or national portal.

(6) Enter the vehicle registration code and the three security codes in the application form of the portal.

(7) Pay by ePayment system.

(8) A click and the vehicle is logged off and de-registered as off the road with the date of the processing in the approval authority after the data has been transferred to the relevant approval authority (determined by the indicator).

(9) The statutory off road notification (SORN) is served by electronic mail.

The new German National Identity Card is therefore mandatory for the Internet-based de-registration of a motor vehicle (car) as off the road in order to secure the identity of the car owner.

IV. THE GERMAN NATIONAL IDENTITY CARD

One of the main problems in the implementation and realization of electronic and mobile government services is the secure and user-friendly authentication of the citizens. Many administrative government services still require the written form. However, the Administrative Procedure Act (Verwaltungsverfahrensgesetz VwVfG) §3a allows the written form to be replaced by the electronic form provided that the law does not specify otherwise. A mandatory prerequisite for this is that the sender can be unambiguously identified and the integrity of the data is guaranteed. One possibility for this is the electronic identity-proof using the new German National Identity Card (eID), see Figure 5.

BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE
PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE
T22000129
Name/Surname/Nom
MUSTERMANN
GEB. GABLER
Vornamen/Given names/Prénoms
ERIKA
Geburtstag/Date of birth/Date de naissance
12.08.1964
Staatsangehörigkeit/Nationality/Nationalité
DEUTSCH
Geburtsort/Place of birth/Lieu de naissance
BERLIN
Gültig bis/Date of expiry/Date d'expiration
31.10.2020
938568
Unterschrift der Inhaberin/des Inhabers - Signature of bearer - Signature de la titulaire/du titulaire
MUSTER

Figure 5. German National eID Card

The new German National Identity Card was introduced on November 1st, , 2010.
It looks different from the former ID card

- Smartcard format
- Integrated NFC-chip
- eID function for Internet use, vending machines or terminals
- Stored biometric passport photograph and voluntary storage of fingerprints to clearly match the ID card with the ID card holder
- Electronic signature function to electronically sign binding contracts, applications, documents, etc. (must be purchased separately)
- Enhanced security features
- Special protection of biometric data

A) *Data printed on the ID card*

Like the former ID card, the national ID card with eID function is an official photo ID with the personal data of the ID card holder printed on the document: family name, name at birth, given names, doctoral degree, date of birth, place of birth, photograph, signature, height, eyes color, address, postal code, citizenship, serial number, religious, stage or pen name if applicable.

B) *Data stored in the NFC-Chip*

The new German national ID card also contains a contactless, readable biometric passport NFC-chip. This NFC-chip stores all data which are printed on the ID card. Additionally, this NFC-chip stores a biometric passport photograph of the card holder and, if desired the biometric fingerprints. The cardholder decides whether the fingerprint data will be stored on the ID card or not.

C) *Applications of the eID Online Function*

The eID online function is offered by service providers that wish to make registration procedures easier and more secure for users. This includes, for example, the online services of banks and insurance companies. However, also public authorities offer online identification, for instance when you register your car or apply for child benefits. Users can identify themselves not only on the Internet, but also at vending machines and the self-service terminals in public authorities.

V. STATIONARY ONLINE AUTHENTICATION PROCESS

As prerequisites for the strong two-factor online authentication process of a German citizen there are the following ingredients needed: The new German eID card with an activated online eID function and a corresponding NFC card reader, or an NFC-enabled Android-smartphone.

A secure connection between the user's eID card and the eID authentication system of the service provider is established for online identification. The eID server ensures reciprocal authentication of both sides.

The online authentication process with the eID card is as follows (using the example of a Web service):

(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-digits 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.

VI. MOBILE AUTHENTICATION APPROACH IN DETAIL

The high level architecture of the mobile de-registration of a vehicle as off the road service is shown in Figure 6 below. At the beginning of authentication, the user has two options available. Either he performs the complete process through our Android app or he uses our QR Code Website solution.

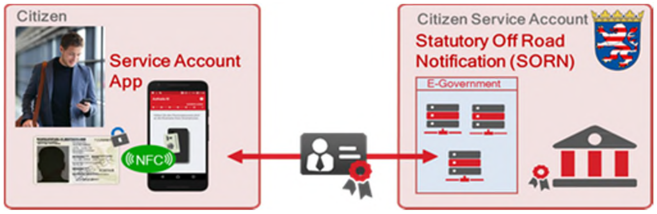


Figure 6. High level overview of the mobile de-registration of a vehicle as off the road service

1. Authentication through our Website

The complete process of de-registration of a vehicle as off the road can be done with our QR code solution. This means that the user performs the actual login process via our Website and uses the app only to scan the generated QR and set the displayed transaction number (TAN) into the corresponding field in the Website.

A) Technical infrastructure

A Linux-based virtual machine from Darmstadt University is used as server platform. A Tomcat Web server was installed on this site, which serves as a container for all developed Web applications. A MariaDB SQL database [14] is used to store the authentication procedures, as well as the vehicle data and log-off procedures. An AUTHADA service is used as a third-party system for identification with the new ID card.

B) Rest – Server

To enable platform-independent communication with various terminals, a REST server based on the Jersey framework [15] 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 architecture. A sequence and message flow of the strong two-factor online authentication of a citizen in order to logout of a vehicle can be seen in Figure 7.

C) Process

The authentication is started at AUTHADA via an integrated library. The obtained data from AUTHADA are first stored in a database and then passed to the caller. With the information obtained, the actual authentication process is now started via the smartphone app or via the Website. The customer identifies himself with his personal ID using the AUTHADA e-Service.

The result of the authentication is a so-called result token. Together with the session information from the first step, the result token is now sent to the server, which in return transfers this information to the AUTHADA e-service and, as a result, receives the read-out customer data from the personal ID card. This data is then stored in the database and linked to the current session. As a result, the REST interface provides only here whether the process was successful or not. In the next step, the customer data that belongs to the respective session can then be retrieved. After this step, the customer's authentication is completed and the vehicle log-off process can be started. In order to request a vehicle cancellation, the vehicle data must first be transmitted together with the session ID. These data must contain at least the label, as well as the necessary security codes. After transmission, the system checks whether the transmitted security codes match the codes stored in the database. For this purpose, some fictitious test codes including security codes were created in the database. Furthermore, it must, of course, be checked whether the authenticated customer is at all entitled to cancel the desired vehicle.

2. Authentication via an NFC-enabled Android app

The complete authentication message flow between the Android App and the eID authentication Server (eID-Server) is shown in detail in Figure 7. The complete process of the de-registration of a vehicle as off the road can also be done with an Android using the AUTHADA SDK and an NFC-enabled mobile, which serves as a reading device to the new German identity card.

After the user decides to execute the login process via the app, he has to accept the privacy policy. Only after this he will be able to do the authentication. After a successful

ISBN: 978-1-61208-605-7

authentication the personal ID data are displayed and the user receives an application form, which must be completed. Before submitting the form, the user's inputs are immediately validated on the client side looking for an error (for example, a security code can only be 3 digits), and the corresponding input validation errors are displayed under the input fields. If the form is valid, the user gets a list of the charges incurred (data coming from the server). If he accepts the costs by touching the button "Compulsory vehicle logout", the log-off process is completed. The user is shown a Success page and then redirected to the start page. In addition, all transactions information (session token) stored until then are removed from the shared preferences (application stored data).

At each step, the user can safely cancel or terminate the vehicle logout by tapping the back button. For this, a dialog is displayed on his mobile terminal with the text "Do you want to terminate the vehicle de-registration?". If the user confirms this dialog with "Yes", he returns to the start page. The session token is also removed from the shared preferences. The following main steps are used to communicate with the eID authentication server (also called eID-Server), see Figure 7:

- Request of an Auth and Session Token
- Transmission of the 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 was implemented, which is able to address the specified REST API of our server. The required data between the app and the server are exchanged in JavaScript Object Notation (JSON) [15] format. Before any request to the server, a check is made as to whether an active Internet connection is available. If this is not the case, the user is shown a message that he must activate his mobile data or WLAN to continue and also he has the possibility to open the settings directly from the app.

All HTTPS connections are implemented and realized with TLS 1.2. If the server is not reachable, or if the response cannot be processed or properly desterilized by the server, the user receives an error message with the request to try again later. From here, he has only the possibility to close the process completely and then reaches the start page. The user is then shown the message that he is not authorized to log off this vehicle and can adjust his inputs again. In order to still be able to use the app in the case of the inadequate availability of our server or to run the logoff process, a mock was developed for test purposes in addition to the real implementation. Before the start of the vehicle logging process, you have the possibility to choose for real or mocked implementation. In the case of the muted variant, the authentication is completely skipped by means of the personal ID card. In addition, the REST requests do not run against our server, but against a mock server [9], which provides static data to successfully test the logoff process.

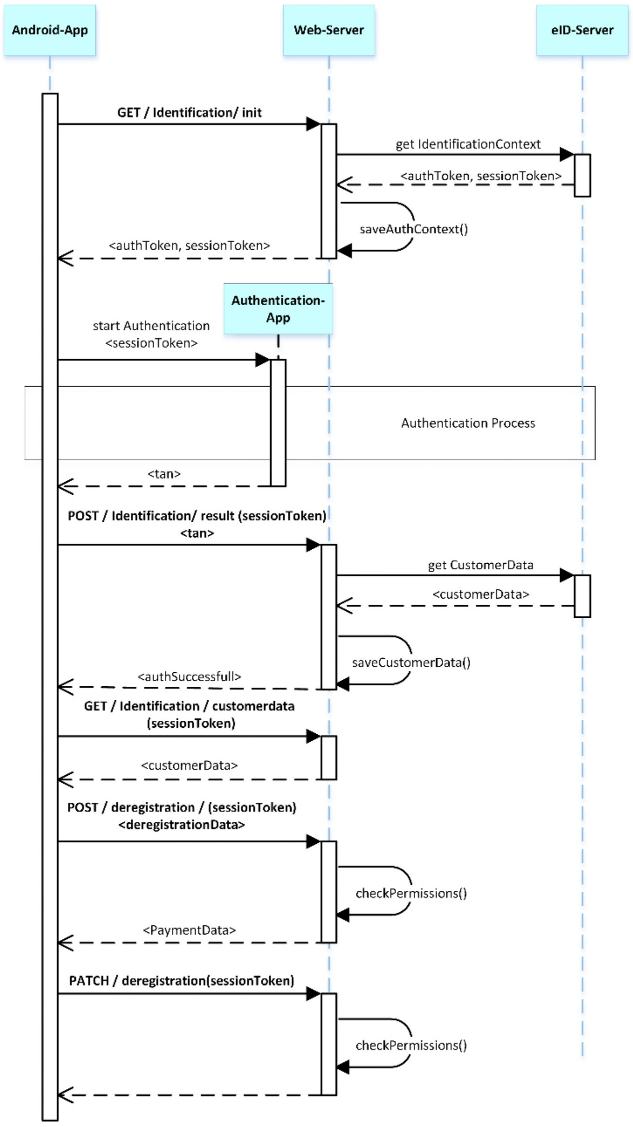


Figure 7. Detailed authentication message flowchart between Android App and eID Authentication Server

VII. CONCLUSION AND OUTLOOK

We presented a new approach for a mobile de-registration of a vehicle as off the road. The new mobile de-registration service of a vehicle as off the road is secure and user-friendly.

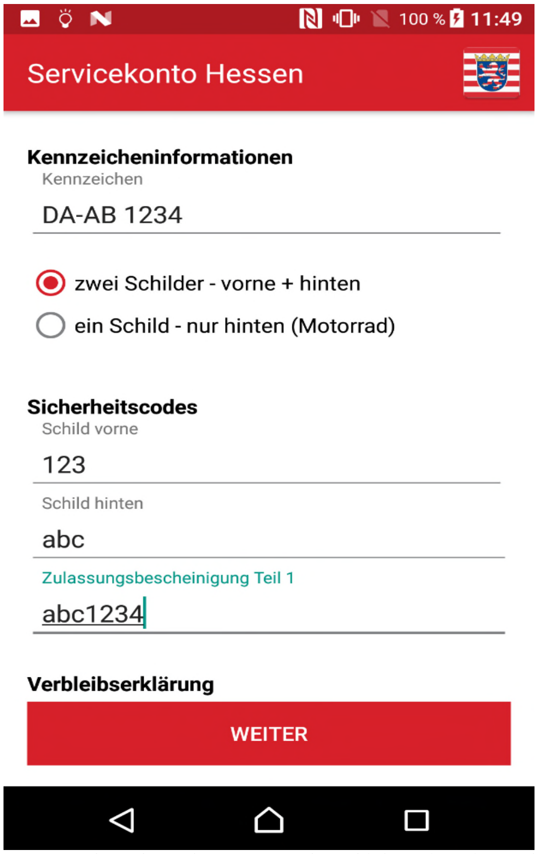
The new approach implements a strong two-factor authentication with German eID card and the corresponding 6-digits PIN, whereby a NFC-enabled Android smartphone will be used as ubiquitous NFC card reader. The new solution overcomes the need to buy a specific NFC card reader. Instead, a NFC-enabled Android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

The big advance for the citizen and users are, in summary: They need not to drive to the government agency, and they save the long waiting times at the agency. So in practice, the citizen save to spend a vacation day for the de-registration of a vehicle as off the road and the Statutory Off Road Notification (SORN). The mobile de-registration service allows the citizens to register their vehicle as off the road (SORN) easily via an Android Smartphone App. In doing so, the electronic identity (eID) of their German eID card will be transmitted via NFC directly via the Android smartphone. Just a few clicks later, the user has registered his/her vehicle as off the road (SORN).

Therefore, here is what the citizen and user needs, in detail: An Android smartphone with enabled NFC functionality, the German eID card with activated online-function and the associated 6-digit PIN, as well as the number/registration plates and vehicle registration license (after 01.01.2015) with three security codes.

The user will find the three security codes on the back of the vehicle registration license, and under the vehicle seal labels on the license plates (front and back).

A strong two-factor authentication ensures the necessary safety and unambiguous identification of the vehicle owner.



Servicekonto Hessen

Kennzeicheninformationen

Kennzeichen

DA-AB 1234

● zwei Schilder - vorne + hinten

○ ein Schild - nur hinten (Motorrad)

Sicherheitscodes

Schild vorne

123

Schild hinten

abc

Zulassungsbescheinigung Teil 1

abc1234

Verbleibserklärung

Figure 8. Screenshot of App how to enter the vehicle registration code and the three security codes in the application form.
Kennzeicheninformationen =license plate information
Sicherheitscodes = security codes from seal labels on the license plates (front and back), as well as from seal label on Certificate of Approval Part I ("vehicle registration")

A screenshot of the new app, how to enter the vehicle registration code and the three security codes in the application form, is shown in Figure 8. The main advantages of the new mobile government solution (as short overview) are the following:

- Quick and easily Statutory Off Road Notification (SORN) of the Vehicle
- Mobile and secure using the Android smartphone app.
- Strong 2-factor authentication (with eID card + PIN).
- No need for an expensive eID card reader.
- Without biometry, TAN and media breaks.

ACKNOWLEDGMENTS

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

REFERENCES

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

[2] https://www.cryptomathic.com/news-events/blog/digital-authentication-the-basics, last access 4th November 2017.

[3] http://nearfieldcommunication.org/, last access 4th November 2017.

[4] http://www.investopedia.com/terms/q/quick-response-qr-code.asp, last access 4th November 2017.

[5] http://rest.elkstein.org/, last access 4th November 2017.

[6] GfK SE (2015) http://www.gfk.com/insights/news/fuenf-prozent-nutzen-elektronischen-personalausweis, last access 4th November 2017.

[7] F. Otterbein, T. Ohlendorf, and M. Margraf: "Mobile Authentication with German eID", IFIP Summer School 2016.

[8] AusweisApp2 for download: www.ausweisapp.bund.de, last access 4th November 2017.

[9] http://www.mocky.io, last access 4th November 2017.

[10] https://english.hessen.de, last access 4th November 2017.

[11] https://www.authada.de, last access 4th November 2017.

[12] https://ekom21.de, last access 4th November 2017.

[13] http://www.gfk.com, last access 4th November 2017.

[14] https://mariadb.org, last access 4th November 2017.

[15] https://jersey.github.io, last access 4th November 2017.

[16] http://www.json.org, last access 4th November 2017.