A Secure and Flexible Server-Based Mobile eID and e-Signature Solution

Christof Rath, Simon Roth, Manuel Schallar and Thomas Zefferer
Institute for Applied Information Processing and Communications
Graz University of Technology
Graz, Austria
Email: {first name}.{last name}@iaik.tugraz.at

***Abstract*—In our digital society, e-government, e-commerce, and e-business are increasingly gaining importance. Many services of these domains rely on reliable user authentication and electronic signatures. For many years, smart cards have been the technology of choice to implement eID and e-signature solutions. Recently, mobile eID and e-signature solutions have emerged as an attractive alternative, as they provide better usability compared to smart card based approaches while maintaining the same level of security. Unfortunately, most current mobile eID and e-signature solutions are tailored to the needs of specific application scenarios and hence cannot easily be applied to and used for other use cases. This prevents a broad use of mobile eID and e-signature solutions and leads to a situation, in which many services still rely on smart card based approaches with poor usability or even insecure password-based solutions for user authentication. To overcome this issue, we propose an improved mobile eID and e-signature solution. In contrast to existing comparable solutions, the proposed solution has been designed such that compatibility with arbitrary use cases is guaranteed. This way, its integration into arbitrary services and applications is facilitated. The feasibility and applicability of the proposed solution has been successfully evaluated by means of a concrete implementation. This implementation demonstrates that the proposed solution provides a secure and usable alternative to existing eID and e-signature solutions and has the potential to improve the security of various e-government services and applications from private-sector domains.**

Keywords*—eGovernment; eID; electronic identity; electronic signature; identity management; mobile security.

I. INTRODUCTION

With the rise of the digital society, remote identification of users has become an increasing challenge as a growing number of services have been moved to the Internet. This applies to public-sector applications (e-government) as well as to private-sector applications (e-commerce, e-business). Remote identification is usually achieved by means of a unique electronic ID (eID) assigned to the user. An eID can for instance be a unique number, user name, or e-mail address. During authentication, the claimed identity (eID) is proven by the user. Reliance on secret passwords for authentication purposes is still the most popular and most frequently used authentication approach for online services. However, password-based authentication schemes have turned out to be insecure due to their vulnerability against phishing attacks and their poor usability, which often leads to the use of weak passwords that are easy to guess [1] [2].

Transactional online services from the e-government domain and related fields of application typically require reliable remote identification and authentication of users. Given the obvious drawbacks of password-based eID and authentication schemes in terms of security, two-factor authentication schemes have been developed for applications with high security requirements such as transactional e-government services. Current two-factor authentication schemes typically comprise the authentication factors *possession* and *knowledge*.

Popular examples of two-factor authentication schemes are smart card based solutions. During the authentication process, the user proves to be in *possession* of the eID token (i.e., the smart card) and proves *knowledge* of a secret PIN that is specific to this eID token and that protects access to the token and to eID data stored on it. In most cases, smart cards additionally enable users to create electronic signatures (e-signatures). For this purpose, the smart card additionally stores a secret signing key and features hardware-based signature-creation capabilities. Access to the signing key and to the smart card's signature-creation functionality is again protected by means of two-factor authentication.

Smart cards are an ideal technological choice to combine the concepts of eID and e-signature, as they are capable to implement both eID and e-signature functionality. Thus, they are frequently used in security-critical fields of application such as e-business, e-banking, or e-government. For instance, various transactional e-government services that have been launched in Europe during the past years require users to authenticate remotely with a personalized smart card and to complete online transactions by applying an electronic signature with the same card [3]. Unfortunately, smart card based solutions usually lack an appropriate level of usability, as they require users to obtain, install, and use an appropriate card-reading device [4].

Powered by the recent emergence of mobile communication technologies and motivated by the low user acceptance of smart card based eID and e-signature solutions, several mobile eID and e-signature solutions have been developed during the past years [5]. These solutions render the use of smart cards unnecessary, as they cover the authentication factor *possession* by means of the user's mobile phone. This way, mobile eID and e-signature solutions have the potential to significantly improve usability while maintaining the same level of security as smart card based solutions.

Due to their improved usability compared to smart card based authentication schemes [4], mobile eID and e-signature

 ISBN: 978-1-61208-324-7

solutions are in principle also suitable for use cases with lower security requirements. Unfortunately, existing mobile eID and e-signature solutions are usually tailored to the requirements of specific use cases and fields of application. This applies to most mobile eID and e-signature solutions that have been introduced and launched worldwide during the past years. Due to their limitation to specific use cases, these solutions can hardly be used in different fields of application. This leads to a situation, in which most applications cannot benefit from the enhanced security and usability of existing mobile eID and e-signature solutions.

To overcome this problem, we propose a modular and flexible concept for mobile eID and e-signature solutions. The main idea behind the design of the proposed concept was to achieve a flexible solution and to maintain its compatibility to different use cases and application scenarios. Details of the proposed concept are presented in this paper. In Section II, we start with a brief survey of existing mobile eID and e-signature solutions and discuss their strengths and limitations. We then derive requirements of a mobile eID and e-signature solution that is applicable in arbitrary application scenarios in Section III. In Section IV, we introduce a technology-agnostic architecture for a mobile eID and e-signature solution that meets all predefined requirements. Based on the proposed architecture, we model three technology-agnostic processes that cover the functionality of the proposed solution in Section V. The practical applicability and feasibility of the proposed solution is assessed in Section VI by means of a concrete implementation. Finally, conclusions are drawn in Section VII.

II. Related Work

The reliable remote identification and authentication of users by means of two-factor based approaches has been a topic of scientific interest for several years. Two-factor based authentication schemes based on smart cards have been introduced in several security-sensitive fields of application during the past decades. Especially in Europe, various countries, such as Austria [6], Estonia [7], Belgium [8], or Spain [9] have issued personalized smart cards to their citizens in order to reliably identify and authenticate them during transactional e-government procedures [3]. In various fields of application, smart cards also enable users to create electronic signatures during online procedures. For instance, electronic signatures are of special importance in Europe, where electronic signatures can be legally equivalent to handwritten signatures according to the EU Directive 1999/93/EC [10].

While smart cards work fine from a functional point of view, their usability is usually rather poor due to the need for a card-reading device to physically connect the smart card to the user's computer. The need for additional drivers and software to communicate with the smart card and to integrate its functionality into security-critical applications also decreases the usability of smart-card technology in general and of smart card based eID and e-signature solutions in particular [4].

To overcome given usability issues of smart card based solutions, several mobile two-factor based eID and e-signature solutions have been developed during the past years. Surveys of mobile eID and e-signature solutions have for instance been provided by Ruiz-Martinez et al. [5] and Pisko [11]. All these solutions have in common that the factor *possession* is not covered by a smart card but by the user's mobile phone. All mobile eID and e-signature solutions that comply with demanding legal requirements, such as those defined by the EU Signature Directive include some kind of secure hardware element, which is able to securely store eID data and to carry out cryptographic operations. Depending on the realization and location of this secure hardware element, mobile eID and e-signature solutions can be basically divided into the following two categories:

- **SIM-based solutions:** Solutions belonging to this category make use of the mobile phone's SIM (subscriber identity module) to securely store eID data and to carry out cryptographic operations. In most cases, the use of a special SIM is required, as off-the-shelf SIMs do not feature the required cryptographic operations such as the creation of electronic signatures. Access to eID data stored on the SIM and to cryptographic functionality provided by the SIM is typically protected by a secret PIN that is only known to the legitimate user. This PIN covers the factor *knowledge* of the two-factor based authentication scheme.
- **Server-based solutions:** Server-based mobile eID and e-signature solutions implement the secure hardware element centrally e.g., in a hardware security module (HSM). Such a solution has been proposed by Orthacker et al. [12]. The user's mobile phone does neither implement cryptographic functionality, nor store eID data. However, the mobile phone is an integral component of the authentication process that is mandatory in order to gain access to centrally stored eID data and to carry out electronic signatures. In most cases, the mobile phone acts as receiver for one-time passwords (OTP), which have then to be sent by the user to the central HSM in order to prove *possession* of the mobile phone and to complete the authentication process.

For both above-mentioned categories, concrete mobile eID and e-signature solutions have been developed and rolled-out on a large scale. For instance, SIM-based mobile eID and e-signature solutions have been set into productive operation in Estonia [13] and Norway [14]. A server-based mobile eID and e-signature solution has been in productive operation in Austria since 2009 [15]. Most existing solutions are tailored to a specific legal framework (e.g., national laws) or to a certain identity system (e.g., to a specific national eID system). For instance, the Austrian mobile eID and e-signature solution has been purpose-built for the Austrian official eID infrastructure and bases on data structures, protocols, and registers that are specific to the Austrian use case. Deploying this solution in other countries would require major adaptations and cause additional costs. Similar limitations apply to most mobile eID and e-signature solutions that have been set into productive operation so far. This renders an application of these solutions in different fields of application difficult and expensive, and prevents that all applications can benefit from the improved security and usability of mobile eID and e-signature solutions.

III. Requirements

The conducted survey on existing mobile eID and e-signature solutions has identified a lack of dynamically adaptable solutions that can easily be applied to arbitrary use cases. To remove this issue, we propose a mobile eID and e-signature solution that can easily be used in arbitrary application sce-

 ISBN: 978-1-61208-324-7

narios. We have designed the proposed solution, which will be introduced in Sections IV and V in detail, according to a set of requirements. These requirements have been extracted from an analysis of existing solutions and from published evaluations of these solutions such as [4]. The derived requirements (R1-R5) are discussed in the following in more detail.

- **R1:** **Flexibility regarding external components:** Mobile eID and e-signature solutions typically rely on external parties and components. Common examples for such components are certification authorities (CA), which bind a user's identity to her signing key, or identity databases (e.g., official person registers or company databases), which are required to derive eIDs for users. A generic mobile eID and e-signature solution must not be limited to certain external components but provide flexible means to integrate different external components (e.g., different CAs).
- **R2:** **Avoidance of token roll-outs:** Long-term experience with smart card based solutions has shown that the roll-out of eID and e-signature tokens (e.g., smart cards, SIMs) causes additional (financial) effort and hence reduces user acceptance. Avoidance of necessary roll-outs of such tokens is hence a key requirement for usable mobile eID and e-signature solutions.
- **R3:** **Usability:** The often disappointing user acceptance of smart card based solutions shows that usability is an important success factor of eID and e-signature solutions. For mobile eID and e-signature solutions, the following aspects need to be considered in particular in order to achieve an appropriate level of usability:
  - **R3a:** **Avoidance of installations:** Usable solutions must not require the user to obtain, install, and maintain additional hardware or software, as this causes additional effort.
  - **R3b:** **Platform and device independence:** Usable solutions must not be restricted to certain computing platforms, operating systems, or end-user devices, as users want to access services everywhere and at any time irrespective of their current execution environment.
  - **R3c:** **Location independence:** Usable mobile eID and e-signature solutions must not be bound to a certain mobile network but must also be accessible when roaming in foreign networks.
- **R4:** **Security:** Security is an important requirement, as mobile eID and e-signature solutions are mainly applied in security-sensitive fields of application such as e-government or e-commerce. Hence, mobile solutions must assure the same level of security as other two-factor based eID and e-signature solutions and must be able to comply with given legal requirements such as the EU Signature Directive.
- **R5:** **Easy and flexible deployment and operation:** From the service operator's point of view, mobile signature solutions should support an easy and flexible deployment as well as an efficient operation, in order to save installation, set-up, and operation costs.

Based on these requirements, we propose a generic and adaptable mobile eID and e-signature solution, which removes limitations of current solutions. We introduce and discuss the concept of our solution in the next sections before providing details on its implementation in Section VI.

IV. ARCHITECTURE

As discussed in Section II, mobile eID and e-signature solutions follow either a SIM-based or a server-based approach to store eID data and to create electronic signatures. Other approaches would be possible on smartphones but cannot be applied on standard mobile phones due to their limited capabilities. Considering the requirements defined in Section III, we have decided to follow a server-based approach for our solution. This means, that a central hardware security module (HSM) stores all eID data and computes electronic signatures. Since solutions based on server-side signatures have very limited hardware requirements on the user side, they are comparatively cheap, user-friendly, and flexible in their deployment, as no roll-out of tokens is required (R2). There are no up-front investments in dedicated SIM cards and no requirements towards the MNOs, hence, the targeted user group is not limited to a single, or certain MNOs. Advantages of server-based signature-creation approaches in terms of usability and user acceptance have also been discussed by Zefferer et al. in [4]. Thus, reliance on a server-based approach assures that requirements regarding usability (R3) are met.

A theoretic concept of a server-based mobile signature solution and a solution to store users private keys in a secure manner on a remote server has been proposed by Orthacker et al. [12] in 2010. The proposed solution fulfills the requirements of *qualified electronic signatures* as defined by EU Directive 1999/93/EC [10], which emphasizes the suitability of this concept for security-critical application scenarios. Furthermore, a server-based mobile eID and e-signature solution that is compliant to the EU Directive 1999/93/EC has been in productive operation in Austria for several years. This provides evidence that server-based solutions are capable to meet given security requirements (R4).

On a high level view, our solution defines the three processes: *registration*, *activation* and *usage*. These processes have different properties regarding computational effort and security constraints. During registration, which is mainly a matter of legal and organizational requirements, the identity of the user is verified. Usually, it is sufficient to perform the registration only once per user. During activation, a new eID and a signing key and certificate are created for a registered user. Activation is required once per life span of an eID. In the usage process, created eIDs and signing keys are used by the user for authentication purposes and to create electronic signatures. Details of the three processes will be provided in the following section.

The architecture of our mobile eID and e-signature solution, which is shown in Fig. 1, basically reflects the three processes defined above. The entire architecture is split into an inner part and an outer part. Components implementing functionality of the activation and the usage processes are divided between these two parts. As shown in Fig. 1, each part has its own database to store required internal data.

This way, the architecture is mainly composed of two databases and the four core components *Activation Outer*, *Activation Inner*, *Usage Outer*, and *Usage Inner*. The split between inner and outer components is a security feature as it reduces the impact of a data loss in case a service connected to the outer world gets compromised. Communication between

 ISBN: 978-1-61208-324-7

outer and inner components happens via a limited, pre-defined set of commands over an encrypted channel. The separation of the core components allows for a very flexible deployment where, e.g., the activation parts can run on different machines, a different network or, if the business process allows/demands it, without a remote access at all. Additionally, access rights can be granted more restrictively, as only the activation process requires write access to many fields in the databases. On the other hand, it is theoretically also possible to deploy the complete service on a single machine, if this is the preferred deployment scenario. This way, the chosen architecture meets the requirements of security (R4) and also the requirements for easy and flexible deployment, and efficient operation (R5).

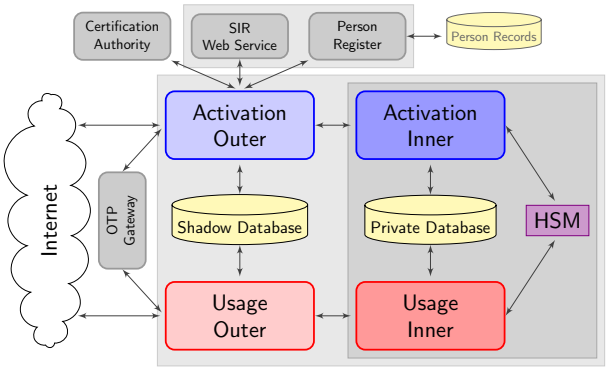


Figure 1: Overview of Core Components

In addition to the four core components, the proposed architecture additionally defines two internal and two external components. The external component *OTP Gateway* is required during the activation and the usage processes to send OTPs to users. The internal component *SIR Web Service* is used during the registration phase and is part of our solution. The *Person Register* and the *Certification Authority (CA)* are services that are required during the activation process. While the CA is an external component, the Person Register is an internal component, which usually connects to an external database. By clearly separating potential external components from the core components of our solution, we can meet the requirement for flexibility regarding external components already on architectural level (R1). The three processes, which build up our solution and cover its functionality as well as all involved components are described in the following section in detail.

V. Processes

The functionality of the proposed technology-agnostic mobile eID and e-signature solution is basically covered by the the processes, *registration*, *activation* and *usage*. The purpose of these processes is discussed in the following subsections in more detail.

A. Registration Process

During the registration process, the identity of a user is verified. Each user has to run the registration process once, before being able to use the proposed solution. In order to allow for a flexible setup of the registration process and to cover a broad range of legal and organizational requirements regarding the registration process, the registration process has been designed to support different types of registration. In particular, the following types of registration have been defined. These types of registration cover use cases from the e-government domain as well as use cases from related domains such as e-commerce or e-business. Also, the proposed architecture is flexible enough to allow for an easy integration of further alternative registration types, in case this is required by the given use case.

- **Registration via registration officer:** The registration officer (RO) is a trusted user, who verifies the identity of the user face-to-face using official IDs, e.g., a passport. After manual verification of the user's identity, the RO manually registers the user in the system.
- **Self registration:** Self registration is carried out by the user herself with the help of an existing eID (e.g., a smart card). The systems verifies the user's ID by means of the provided eID and afterwards registers the user.
- **Offline registration:** To support offline registration, the proposed solution supports registration of users via so-called *Standard Identification Records (SIR)*. A SIR contains information to identify a person, information about the ID used to verify the identity of the applicant, a binding towards a hardware token, i.e., a mobile phone for the use case at hand, and the digital signature of a RO or a trusted partner, e.g., a bank or a university. During the registration process, the system verifies the validity of a provided SIR that has been created offline, i.e. checks that the signature is valid and that the signer of the SIR is a legitimate RO or trusted partner.

Support of different types of registration allows for a very flexible setup of the registration process and covers a broad range of legal and organizational requirements regarding the registration process. This, in turn, contributes to a flexible operation of the proposed solution, which has been identified as key requirement (R5).

B. Activation Process

After successful registration, users can run the activation process to create a new eID. Our solution supports multiple eIDs for each user. Hence, the activation process can be run multiple times by each user. During the activation process, the unique identifier of the applicant is bound to the mobile phone, or more precisely, to the signing certificate that is issued during the activation process.

To activate a new eID, the applicant has to prove possession of the specified mobile phone. This is achieved by means of OTPs that are sent to the user through an OTP Gateway.

When the user has proven possession of her mobile phone, a signing key-pair is generated for the user inside the server-side HSM. The public key and the filtering criteria to find the applicant, e.g., name and date of birth, is sent to the Person Register. The Person Register is a component that connects to a database containing potential users of the service. Depending on the deployment and application scenario, this can be an existing official database like a central register of residence maintained by a public authority, an existing domain-specific database like the database of employees of a private-sector company, or a database specifically for this service that grows with every new registration.

If the user has been found unambiguously in the database, the Person Register returns a signed data structure that contains

 ISBN: 978-1-61208-324-7

the unique eID of the applicant within the register and the public key of the created signature key-pair. Thus, it is possible to link a signature to a person for means of identification without the need to embed the unique eID directly in the signing certificate. By clearly separating eID functionality from e-signature functionality, users' privacy is assured. A similar concept is already successfully applied in existing national eID solutions [16].

Subsequently, a end-user certificate is requested from the certification authority (CA). The certificate, the wrapped private key, and the created eID data are stored encrypted in the database. The encryption of user data is based on a secret signature password, which the applicant chooses during the activation process. Our solution relies on hybrid encryption schemes, in order to encrypt data on behalf of the user without knowledge of the signature password. The decryption, however, requires the consent of the user, which she gives by providing the signature password. By choosing different signature passwords, a user can activate different eIDs for the same mobile phone number. Each eID can be managed separately. This enables users to have eIDs for different purposes, e.g., private and official purposes.

C. Usage Process

After successful completion of the activation process, the user can use the created eID and signing key to securely and conveniently authenticate at services and to create electronic signatures. To issue an electronic signature, the user has to enter her phone number and signature password. The signature password is used to decrypt a private key that is part of the hybrid encryption mentioned above. Thus, neither the activation of the user's signature key has to take place before the two-factor authentication is complete, nor must the signature password be stored in a session.

Next, the service sends a OTP via the OTP Gateway to verify possession of the mobile phone. After the user has been successfully authenticated, the user data is read from the database and decrypted using the user's private key of the hybrid encryption. Then, the still-wrapped private key of the signing key-pair is loaded into the HSM where it is unwrapped. Finally, the unwrapped key is used to create an electronic signature. After successful completion of the signature-creation process, the unwrapped key is discarded.

VI. Evaluation

Based on the proposed architecture, we implemented a prototype to evaluate and demonstrate the applicability of our solution. We built our implementation on a set of well-known and production-ready frameworks and libraries. The foundation of all modules is the Spring Framework [17], which greatly supports the development of modular and flexible software solutions. Access to databases happens through Hibernate [18], an object-relational mapping (ORM) library. Thus, the access to a database is mostly independent from its implementation. This gives us the freedom to adapt the databases to the needs of a certain deployment scenario. For cryptographic operations we use the IAIK JCE and iSaSiLk libraries [19]. Messages between the modules are exchanged using Apache ActiveMQ [20]. As means to deliver OTPs our implementation uses random transaction numbers (TAN) delivered by an SMS gateway.

To assure its security, we have assessed our implementation by means of a security analysis. To follow an approved approach, the implementation has been evaluated regarding the most recent critical risks according to OWASP [21] using a white-box testing approach. This approach allows the auditor having knowledge of the internal structure of the project, like the knowledge of libraries and frameworks in use, as well as having access to the source code.

The developed and assessed implementation covers the three processes defined in Section V. The realization of these processes is discussed in the following subsections.

A. Registration Process

In this step, the applicant has to prove her identity. Our implementation supports the three types of registration defined in Section V. In a traditional setup this happens at the office of the RO. For this scenario, our implementation provides a web-based UI, through which the RO can register the applicant in the system.

However, in some situations it might be beneficial if the RO travels from applicant to applicant (offline registration). We developed different front-ends to simplify this type of registration. Initially, we developed a simple, yet comprehensive, stand-alone application based on Spring MVC. This application can be used on mobile devices in case of traveling ROs and supports the RO in creating SIRs. Furthermore, we developed a proof-of-concept where a traveling RO takes the picture of the ID of an applicant. The required data is extracted using optical character recognition (OCR). Additionally, our implementation provides a web service that accepts these externally created SIRs.

To cover the third registration type, our implementation provides a UI for the applicant. This UI allows the applicant to carry out a self registration in case she has already a trusted eID (e.g., smart card).

B. Activation Process

In this step, the applicant creates and activates a new mobile eID. A pre-registered applicant can perform this step on her own and independent of the registration process.

The activation process offers again a web-based interface. It has been developed using JSF 2.1 [22] and Primefaces [23]. The decision to use a different technology to create the UI is based on the rich set of UI components that is part of Primefaces. Thus, a flexible, easy to use, role/permission-based interface has been developed in a short amount of time.

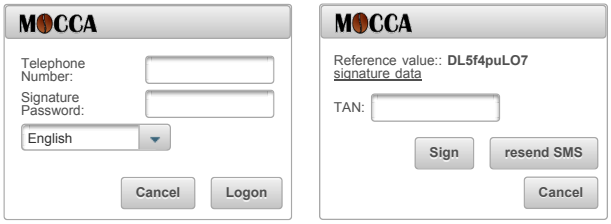
Apart from the actual activation process, this module offers interfaces for several other tasks. Registration officers can perform activations on behalf of someone else. Hence, the activation process has been extended by the registration tasks. Furthermore, we developed interfaces to manage eIDs, both for the owner and a support team. An administration UI allows the definition and assignment of roles.

C. Usage Process

The usage process was developed alongside the activation and therefore is built on the same technologies, i.e., Java Server Faces [22] and Primefaces [23]. The interfaces are reduced to the bare minimum required for authenticating users and authorizing the creation of signatures. This facilitates an easy integration of our solution into arbitrary third-party applications. The two main forms for the two-factor authentication are shown in Fig. 2.

First, the signer provides her phone number and signature password. If the authentication was successful, two random

 ISBN: 978-1-61208-324-7



(a) Login (b) TAN Verification

Figure 2: Interface of the Usage Process

values are generated: the reference value, which is shown in the TAN verification form (Fig. 2(b)) and in the SMS to provide a link between TAN and signature, and the TAN itself, which is only sent by SMS.

After verifying the reference value received by SMS against the reference value prompted in the TAN verification form, the user enters the received TAN. If the correct TAN is entered, the signature is created. This form also provides a link to display the signature data, to verify what data will be signed.

VII. Conclusions

In this paper, we have proposed an enhanced eID and e-signature solution. The practical applicability of the proposed solution has been successfully evaluated and demonstrated by means of a concrete implementation. A test deployment of this implementation is publicly available online and can be accessed for test purposes [24].

By relying on a server-side HSM for storage of users' eID data and for realization of cryptographic functionality, our solution is one of few mobile eID and e-signature solutions that rely on a server-based approach. In contrast to existing server-based eID and e-signature solutions, our solution has not been tailored to requirements of a specific use case or application scenario but has been based on an abstract architecture. This assures that the proposed solution is applicable for different use cases and fields of operation.

Furthermore, the proposed solution shows that secure two-factor based user authentication can be achieved in a user-friendly way and does not necessarily require the cumbersome handling of additional security tokens such as smart cards. This way, the proposed solution provides a promising way to enhance the usability of transactional e-government services while maintaining a high level of security.

Due to its easy integrability and high degree of usability, the proposed solution is not limited to e-government-related use cases. It can also be an attractive alternative for less security-critical services such as e-commerce or social networking. If also these services take the opportunity to provide users a higher degree of security while maintaining a high degree of usability by integrating the proposed mobile eID and e-signature solution, insecure password-based authentication schemes will hopefully be history in the future.

Acknowledgements: The authors have been supported by the European Commission Seventh Framework Programme through project *FutureID*, grant agreement number 318424.

References

[1] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," Commun. ACM, vol. 47, no. 4, Apr. 2004, pp. 75–78. [Online]. Available: http://doi.acm.org/10.1145/975817.975820

[2] D. Florencio and C. Herley, "A large-scale study of web password habits," in Proceedings of the 16th International Conference on World Wide Web, ser. WWW '07. New York, NY, USA: ACM, 2007, pp. 657–666. [Online]. Available: http://doi.acm.org/10.1145/1242572.1242661

[3] S. Arora, "National e-id card schemes: A european overview," Inf. Secur. Tech. Rep., vol. 13, no. 2, May 2008, pp. 46–53. [Online]. Available: http://dx.doi.org/10.1016/j.istr.2008.08.002

[4] T. Zefferer and V. Krnjic, "Usability evaluation of electronic signature based e-government solutions," in Proceedings of the IADIS International Conference WWW/INTERNET 2012, 2012, pp. 227 – 234.

[5] A. Ruiz-Martinez, D. Sanchez-Martinez, M. Martinez-Montesinos, and A. F. Gomez-Skarmeta, "A survey of electronic signature solutions in mobile devices." JTAER, vol. 2, no. 3, 2007, pp. 94–109. [Online]. Available: http://dblp.uni-trier.de/db/journals/jtaer/jtaer2.html#Ruiz-MartinezSMG07

[6] "Handy Signatur und Buergerkarte," 2013, [retrieved: November, 2013]. [Online]. Available: http://www.buergerkarte.at/

[7] "Estonia eID," 2013, [accessed November, 2013]. [Online]. Available: http://www.id.ee/?lang=en

[8] "Belgium eID," 2013, [accessed November, 2013]. [Online]. Available: http://eid.belgium.be/en/

[9] "Spanish eID," 2013, [accessed November, 2013]. [Online]. Available: http://www.dnielectronico.es/

[10] European Parliament and Council, "Directive 1999/93/ec on a community framework for electronic signatures," December 1999.

[11] E. Pisko, "Mobile electronic signatures: Progression from mobile service to mobile application unit." in ICMB. IEEE Computer Society, 2007, p. 6. [Online]. Available: http://dblp.uni-trier.de/db/conf/icmb/icmb2007.html#Pisko07

[12] C. Orthacker, M. Centner, and C. Kittl, "Qualified mobile server signature," in Security and Privacy – Silver Linings in the Cloud, ser. IFIP Advances in Information and Communication Technology, K. Rannenberg, V. Varadharajan, and C. Weber, Eds., vol. 330. Springer Berlin Heidelberg, 2010, p. 103–111. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-15257-3_10

[13] "Estonia mobile eID," 2013, [accessed November, 2013]. [Online]. Available: http://mobiil.id.ee/

[14] "Norway eID," 2013, [accessed November, 2013]. [Online]. Available: https://www.bankid.no/

[15] "Austrian Handy Signatur," 2013, [accessed November, 2013]. [Online]. Available: https://www.handy-signatur.at/

[16] H. Leitold, A. Hollosi, and R. Posch, "Security architecture of the austrian citizen card concept," in Proceedings of 18th Annual Computer Security Applications Conference (ACSAC'2002), Las Vegas, 9-13 December 2002. pp. 391-400, IEEE Computer Society, ISBN 0-7695-1828-1, ISSN 1063-9527., 2002.

[17] "Spring Framework," 2014, [accessed November, 2013]. [Online]. Available: http://projects.spring.io/spring-framework/

[18] "Hibernate," 2014, [accessed November, 2013]. [Online]. Available: http://hibernate.org/

[19] "IAIK JCE," 2014, [accessed November, 2013]. [Online]. Available: http://jce.iaik.tugraz.at/

[20] "Apache Active MQ," 2014, [accessed November, 2013]. [Online]. Available: http://activemq.apache.org/

[21] The Open Web Application Security Project, "Owasp top 10 - 2013 the ten most critical web application security risks," 2013.

[22] "Java Server Faces," 2014, [accessed November, 2013]. [Online]. Available: https://javaserverfaces.java.net/

[23] "Primefaces," 2014, [accessed November, 2013]. [Online]. Available: http://www.primefaces.org/

[24] "Test deployment of our implementation," 2014, [retrieved: November, 2013]. [Online]. Available: https://pheasant.iaik.tugraz.at:8443/Registration/

 ISBN: 978-1-61208-324-7