Real-World Identification: Towards a Privacy-Aware Mobile eID for Physical and Offline Verification

Michael Hölzl
JRC u'smile and Johannes Kepler University Linz, Institute of Networks and Security
michael.hoelzl@usmile.at

Michael Roland
JRC u'smile
University of Applied Sciences Upper Austria
michael.roland@usmile.at

René Mayrhofer
JRC u'smile and Johannes Kepler University Linz, Institute of Networks and Security
rene.mayrhofer@usmile.at

ABSTRACT

There are many systems that provide users with an electronic identity (eID) to sign documents or authenticate to online services (e.g. governmental eIDs, OpenID). However, current solutions lack in providing proper techniques to use them as regular ID cards that digitally authenticate their holders to another physical person in the real world. We envision a fully mobile eID which provides such functionality in a privacy-preserving manner, fulfills requirements for governmental identities with high security demands (such as driving licenses, or passports) and can be used in the private domain (e.g. as loyalty cards). In this paper, we present potential use cases for such a flexible and privacy-preserving mobile eID and discuss the concept of privacy-preserving attribute queries. Furthermore, we formalize necessary functional, mobile, security, and privacy requirements, and present a brief overview of potential techniques to cover all of them.

CCS Concepts

•**Software and its engineering** → **Requirements analysis;** •**Security and privacy** → *Pseudonymity, anonymity and untraceability;* •**Applied computing** → E-government;

Keywords

Electronic identities, privacy, mobile eID, requirements

1. INTRODUCTION

Electronic identities (eID) allow users to electronically authenticate to service providers or to digitally sign documents. Many governments already provide their citizens with eID systems to handle administrative tasks like doing taxes, applying for subsidies, or registering a business. The Estonian[1] and Finnish[2] governments even provide their citizens with mobile eIDs integrated in SIM-cards on mobile phones.

OpenID[3] as well as the Fast Identity Online (FIDO)[4] specification are examples of systems in the private domain that work beyond system boundaries. OpenID provides the capability to authenticate a user to numerous different services without the requirement to register at every service; and FIDO allows a more user-friendly authentication.

However, these existing systems all rely on the concept of an online service as a verifier of an identity. For example, eID holders verify their identity against an e-government service; users want to login to an online mail server, etc. This restriction results in systems that do not allow identity verification in the same way as regular identification cards. A practical example would be a bouncer at a disco who checks for the proper age of visitors. While this is a trivial task with regular identification cards, it can become troublesome with eID tokens (i.e. eID cards). Potential challenges that might arise include that the system requires online connectivity, the interface to an eID token requires special reader equipment connected to a PC, each verifier needs special certification to read the token, login credentials by the holder of an eID need to be entered on the verifying device, etc.

As a result, existing solutions fail to replace regular identification cards as a simple physical identity proof. Especially challenging thereby is the requirement of online connectivity during verification. We refer to these properties as *real-world identification* and *offline verification*.

Furthermore, the usage of an electronic identity token bears many additional problems concerning the privacy of the user. As information is digitally processed, users lose control over their data. They cannot be sure that their data is adequately protected, only used for the claimed purpose (of identification), and not stored or passed on to other parties. Hence, with regard to the privacy of the user it is important that as little information as necessary is given to verifiers. For example, it is sufficient for the bouncer at the disco to know that the user is above 18 years old. The exact date of birth or even further attributes, such as name, address, social security number, etc. are not relevant.

The main motivation of this paper is to further elaborate the vision of an eID system that provides both: real-world identification and privacy-preserving attribute checks. We aim for providing a mobile eID system that fulfills the requirements of government issued identities with high security demands, such as driving licenses or passports. Furthermore, we strive for an eID that can be used as central authentication token for numerous use cases without loosing privacy,

[1] Estonian: `http://e-estonia.com/component/mobile-id/`
[2] Finnish: `http://www.mobiilivarmenne.fi/`
[3] `https://openid.net/`
[4] `https://www.fidoalliance.org`

MoMM '16, November 28 - 30, 2016, Singapore, Singapore

ISBN 978-1-4503-4806-5/16/11...$15.00

DOI: `http://dx.doi.org/10.1145/3007120.3007158`

such as a loyalty card, a public transport ticket, etc.

As a first step towards such a privacy-preserving eID system with high security demands and flexibility, we formalize the essential requirements in this paper. A special focus lies in the capability of direct physical interaction in the verification phase (i.e. real-world identification) as well as the offline and mobile capabilities. We also define exemplary use cases which need to be covered with such a system and discuss the general concept of privacy-preserving attribute queries that do not reveal unnecessary information about the eID holder. Finally, we give an outlook on future steps towards a system that fulfills all requirements.

2. RELATED WORK

Many countries already provide their citizens with eID cards. In European countries, this is often realized with smart cards which allow the generation of qualified and binding signatures. A survey of available governmental eIDs in the European Union by Lehman et al. [8] shows that none of them provides anonymous and privacy-preserving verification methods. Only the Austrian and German eID cards support notable features for protecting users' privacy by pseudonym generation and selective attribute disclosure.

The techniques that are most often used for privacy-preserving eID systems in the literature are pseudonym-based signatures [1, 2] and group signature protocols [4, 5, 11]. The latter allow members of a group to sign messages on behalf of the whole group without revealing their identity within that group. Pseudonym-based signatures rely on public-key cryptography (e.g. RSA, ECC) and provide each member with a list of pseudonyms to sign messages.

Attribute based signatures by Maji et al. [10] are a modification to group signatures and allow a signer to endorse that she owns a certain attribute. Hence, the verifier does not acquire the actual attribute but only gets the confirmation if the attribute has a certain value or not.

A specification for eIDs that has recently become well-known is provided by the Fast Identity Online (FIDO) alliance. They are an industry consortium with the goal to improve usability of user authentication on the Internet by reducing the reliance on passwords. With one specification for such a passwordless authentication and one for second factor authentication, they provide schemes for secure identity verification on any online service.

Nyman et al. [12] define an eID architecture that is based on the use of so-called Trusted Platform Modules (TPM). They build upon version 2.0 of the TPM specification and evaluate its feasibility as an identity token on PC as well as mobile platforms. They also provide a formal definition of requirements for eID systems, with a focus on online services.

We build upon the definitions in all of this previous work (especially on the definitions of an eID system by Nyman et al. [12] and the privacy properties by Camenisch et al. [4]). However, we further extend them with requirements that result from the practical use cases of real-world identification with mobile eIDs, as outlined in the remainder of this paper.

3. PRIVACY-PRESERVING MOBILE eID

In this section we outline an eID system that provides real-world identification and privacy-preserving attribute check. Particularly, we refine the stakeholders and attribute checks which shall be possible in such a system.

3.1 Stakeholders

We consider four main stakeholders of an eID system:

- The *eID issuer* is the central authority that controls the enrollment of eIDs and provides an interface for verifiers to acquire system information.
- The *prover* is the actual holder of an eID and possesses techniques to authenticate her identity to a verifier. The architecture of an eID system may require the prover to carry a physical eID token (e.g. smart card, mobile device, etc.) where data attributes (e.g. name, address, etc.) about the holder are stored.
- The *verifier* is interested in identifying and authenticating eID holders. This could be another person who wants to validate that the eID holder has certain attributes. Note that a verifier does not necessarily need to involve a human (e.g. automatic vending machine).
- A *verifier group* can be an online service or any domain which provides services to provers. The group is able to add attributes to the eID and all verifiers of the group can validate them. Nonmembers should not be able to acquire any information about these attributes. For example, the point-of-sale in a shop (i.e. verifier group member) wants to verify that an eID is a member of a customer loyalty program. A competitor should not be able to acquire that information.

3.2 Privacy-preserving Attribute Queries

In order to protect the privacy of the eID holders, an attribute query should not reveal information unnecessary for a specific task. For that purpose, we define three privacy-preserving queries which shall only return a binary result:

Attribute equality query. With this type of query, the verifier finds out if an attribute on the eID token has a certain reference value. If the actual value is not known by the verifier, it cannot be determined with such a query.

Input: attribute, reference value

Output: $1 \,|\, 0$

Attribute inequality query. With this type of query, the verifier can determine if a certain attribute on the eID is larger or smaller than a given reference value.

Input: attribute, reference value, operator $(<, \leq, >, \geq)$

Output: $1 \,|\, 0$

Group membership check. With this type of query, the verifier can determine if a holder is member of a certain group (e.g. loyalty program).

Input: group identifier

Output: $1 \,|\, 0$

3.3 Exemplary Use Cases

A privacy-preserving mobile eID offers many potential real-world use cases. The following represents a selection where privacy-preserving attribute queries are useful:

Parcel collection address check. Due to absence at delivery, the parcel of an eID holder got forwarded to the post office. When collecting the parcel, the eID holder is asked to

Table 1: Overview of requirements.

1. Functional	(a) Real-world identification
	(b) One-to-many relationship
	(c) Revocation
	(d) Scalability
2. Mobility	(a) Offline
	(b) Power-off
	(c) Scalability
3. Security	(a) Key confidentiality/code isolation
	(b) Unforgeability/attribute authenticity
	(c) Communication protection
	(d) State-of-the-art cryptography
4. Privacy	(a) Privacy-preserving signatures
	(b) User control
	(c) Privacy-preserving attribute queries

verify that he is the true recipient and lives at the delivery address. In order to verify that, the verifier (i.e. post officer) uses a mobile device running the eID application to send an *attribute equality query* with the requested name and address to the eID token. In return, the post officer gets a binary result if the address and name match the eID attributes.

Age verification. A bouncer at a disco only allows access to people who are above 18 years old. In order to prove that the holder of an eID is old enough, the bouncer uses a mobile device to send an *attribute inequality query* with the date 18 years behind the current date as reference value as well as the $\leq$ operator. If the date of birth stored on the eID token is less or equal to the reference value, the holder is older than 18 and the result of the query is 1.

Loyalty program membership. A shop offers special discounts for loyalty program members. eID holders can join this program using the eID application on the mobile device to exchange all relevant information (i.e. group identifier). The point-of-sale terminal in the shop sends the group identifier in a *group membership check* and gets a binary result. Hence, the terminal learns if the customer is program member without the need of additional data (e.g. name, age, etc.)

4. FORMAL REQUIREMENTS

We base the requirements of a mobile eID system on the definitions by Nyman et al. [12]. According to them, they can be classified in three categories: *functional*, *security*, and *privacy* requirements. While we build upon their requirements, we defined multiple additional ones that especially concern the real-world identification and mobile scenarios. Most notable requirements in [12] which we build upon are the *one-to-many relationship*, *confidentiality of the identity keys*, *code isolation*, as well as the *cryptographic requirements*. In addition, we consider the category of mobility requirements. An overview of all requirements is shown in Table 1.

4.1 Functional Requirements

(a) Real-world identification: The eID shall allow identity verification in the same way as regular identification documents. This real-world identification between prover and verifier should be possible with everyday technology, such as mobile phones, tablets, etc. A practical example is the police officer who checks the driving license stored on the eID in a mobile phone of the prover or the bouncer at a disco who checks for the proper age of the visitors using a tablet.

(b) One-to-many relationship: The identity of one physical person should be able to enroll to many domains. That is, it shall be possible for the user to be a member of numerous verifier groups (e.g. loyalty programs) with the same eID. These groups should thereby have the possibility to extend attributes in the eID tokens (e.g. store information about a public transport ticket, insert loyalty program details, etc.)

(c) Revocation shall be possible for the owner of the eID (e.g. user lost the identity token), the eID issuer (e.g. citizen deceased) as well as the verifier group (e.g. service provider revoking membership). Considering a governmental identity with the capability to perform sensitive tasks, such revocation measures need to be effective almost in real-time. The scheme also needs to consider scalability as revocation may happen often. For example, according to [9] a nationwide Belgian eID lists 375,000 revoked identities for a population of just 10 million citizens. Thus, a simple certificate revocation list downloaded by every verifier might not be feasible.

(d) Scalability: Besides revocation, the system should scale in all other integral parts of the eID architecture such as enrollment and verification.

4.2 Mobility Requirements

(a) Offline: Verification should be possible with offline devices on both prover and verifier side. In other words, both should not require online connectivity to a central service during verification. However, they may still connect from time to time to get system updates. Also the revocation checks (Req. 1.c) should be possible in mobile and offline scenarios. For example, police officers should not have the need to get network connectivity in order to be able to verify the validity of a driving license.

(b) Power-off: Verification should not require the device of the prover to be powered on. Hence, availability of an eID that is for example located in a mobile device should not be affected by an empty battery.

(c) Scalability: Similar to the functional requirement in Req. 1.d, scalability is also a central requirement for the mobility of prover and verifier. In order to keep the system usable for mobile devices, the amount of data that needs to be processed shall stay manageable on devices with constrained resources even with a large population.

4.3 Security Requirements

(a) Key confidentiality and code isolation: The secret cryptographic keys of an identity need to be protected with hardware specifically designed to provide high confidentiality and integrity assurances (e.g. smart cards). Any operation using these keys shall be executed within this environment.

(b) Unforgeability and attribute authenticity: Only eID tokens enrolled in the system should be able to provide valid identity proofs and eID attributes should be modifiable only by the issuer. The verifier needs be able to detect maliciously created identity claims as well as modified attributes.

(c) Communication protection: The confidentiality and integrity of data attributes needs to be protected when they are transmitted between the eID and the verifier/issuer.

(d) State-of-the-art cryptography: For mentioned data protection requirements, state-of-the-art cryptographic techniques and key sizes shall be used. According to [3], current minimum requirements are equivalents to 256 bit elliptic curve and SHA-256. However, the system shall be able to adapt to future advancements in cryptographic primitives and key sizes. This is a property especially important considering governmental IDs, such as driving licenses, which are often valid for over 10 years. Consequently, the security of such identity tokens with long validity shall be future-proof.

4.4 Privacy Requirements

(a) Privacy-preserving signatures: As already elaborated in the related work section, group signatures are a good candidate for providing privacy-protective techniques to create signatures in an eID system. As discussed in [4], a well designed scheme should thereby provide the principles of *anonymity*, *unforgeability*, and *unlinkability*. Note that unforgeability is already listed as a security requirement in Req. 3.b. Furthermore, we consider *backward unlinkability* as defined by Nakanishi et al. [11] as an essential requirement:

- *Anonymity*: Users' identity shall not be determinable within the whole population (k-anonymity with k as the population size). That is, a signature created by an eID should not reveal the identity of the user.
- *Unlinkability*: Signatures created in a verification process or revocation information of the same user shall not be linkable. That is, an eID holder should not be traceable across verifications.
- *Backward unlinkability*: Even when an eID has been revoked, the anonymity and unlinkability property of that identity shall not be relinquished.

(b) User control: The holder of an eID has to stay in control of the data. Hence, the user shall have the possibility to authorize which data attributes can be retrieved by a verifier and which attributes shall remain secret.

(c) Attribute queries: In order not to reveal unnecessary additional attributes, the eID system shall support special privacy-preserving queries. Rather than giving out the actual content, binary results for specific queries are preferred (cf. Section 3.2). Note that while these queries already reveal some information, they might still be eligible to additional user control (Req. 4.b).

5. CONCLUSIONS

In this paper we introduced the vision of a privacy-preserving mobile eID which can be used for real-world identification similar to regular ID documents and that provides extensibility for the use in private domains. As a first step towards that vision, we described the general outline of such a system and presented multiple practical use cases. We also introduced the concept of privacy-preserving attribute queries and discussed all necessary requirements for a system that would also fulfill high security demands of governmental eIDs such as driving licenses or passports.

To the best of our knowledge, there currently exists no solution that fulfills all these requirements. However, a solution would most probably combine the usage of multiple techniques: NFC secure elements (SE) for confidentiality, code isolation and power-off support, group signatures for privacy-preserving identity proofs, a scheme as in [7] for scalable, unlinkable and offline revocation checks, a secure channel protocol as in [6] for confidentiality and integrity when communicating with the SE, etc.

6. ACKNOWLEDGMENTS

This work has been carried out within the scope of *u'smile*, the Josef Ressel Center for User-Friendly Secure Mobile Environments, funded by the Christian Doppler Gesellschaft, A1 Telekom Austria AG, Drei-Banken-EDV GmbH, LG Nexera Business Solutions AG, NXP Semiconductors Austria GmbH, and Österreichische Staatsdruckerei GmbH.

7. REFERENCES

[1] J. Bringer, H. Chabanne, R. Lescuyer, and A. Patey. Efficient and Strongly Secure Dynamic Domain-Specific Pseudonymous Signatures for ID Documents. In *Financial Cryptography and Data Security*, pages 255–272. Springer, 2014.

[2] J. Bringer, H. Chabanne, R. Lescuyer, and A. Patey. Hierarchical Identities from Group Signatures and Pseudonymous Signatures. In *The New Codebreakers*, pages 457–469. Springer, 2016.

[3] BSI. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Technical Report TR-02102-1 v2016-1, Feb. 2016.

[4] J. Camenisch and M. Stadler. Efficient group signature schemes for large groups. In *Advances in Cryptology*, CRYPTO '97, pages 410–424. Springer, Aug. 1997.

[5] D. Chaum and E. Van Heyst. Group signatures. In *Advances in Cryptology*, EUROCRYPT '91, pages 257–265. Springer, 1991.

[6] M. Hölzl, E. Asnake, R. Mayrhofer, and M. Roland. A Password-authenticated Secure Channel for App to Java Card Applet Communication. *International Journal of Pervasive Computing and Communications (IJPCC)*, 11:374–397, Oct. 2015.

[7] V. Kumar, H. Li, J.-M. J. Park, K. Bian, and Y. Yang. Group Signatures with Probabilistic Revocation: A Computationally-Scalable Approach for Providing Privacy-Preserving Authentication. In *Proc. CCS 2015*, pages 1334–1345. ACM, 2015.

[8] A. Lehmann et al. Survey and Analysis of Existing eID and Credential Systems. FutureID Deliverable D32.1, Apr. 2013.

[9] W. Lueks, G. Alpár, J.-H. Hoepman, and P. Vullers. Fast revocation of attribute-based credentials for both users and verifiers. In *ICT Systems Security and Privacy Protection*, pages 463–478. Springer, 2015.

[10] H. K. Maji, M. Prabhakaran, and M. Rosulek. Attribute-Based Signatures. In *Topics in Cryptology*, CT-RSA 2011, pages 376–392. Springer, Feb. 2011.

[11] T. Nakanishi and N. Funabiki. Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps. In *Advances in Cryptology*, ASIACRYPT 2005, pages 533–548. Springer, Dec. 2005.

[12] T. Nyman, J.-E. Ekberg, and N. Asokan. Citizen electronic identities using TPM 2.0. In *Proceedings of the 4th International Workshop on Trustworthy Embedded Devices*, pages 37–48. ACM, 2014.