Security requirements for the successor of the Estonian Mobile-ID

Arnis Parsovs
University of Tartu

April 11, 2022

Abstract

The Estonian state is looking to replace the current SIM-card-based Mobile-ID solution with a next generation mobile-app-based electronic identity (eID) solution. The planned eID solution will play a tremendous role in protecting the digital identity of the Estonian citizens and (e-)residents. However, the procurement specification published by the state does not delve into the security requirements for the solution, leaving the security aspects of it up to the potential contracting parties. This paper aims to fill this gap by introducing a list of general security requirements and principles that are desirable for the next generation eID solution. Most of the points discussed in this paper have been motivated by the shortcomings of the existing Mobile-ID and Smart-ID solutions that are currently used in Estonia.

1 Introduction

On 2020-08-17, the Estonian state opened a public procurement for obtaining a full mobile electronic identity service [1] (hereinafter – Mobile-eID[1]).

The list of security requirements in the procurement's technical specification [2] are essentially limited to two requirements: (1) the proposed authentication solution must correspond to the level "high" in the eIDAS framework of levels of assurance; and (2) the digital signature solution must have a Qualified Signature Creation Device (QSCD) certificate.

Unfortunately, as we can see from the case of the Smart-ID solution (and also the existing Mobile-ID solution), a formal compliance to these requirements does not guarantee that the higher level protocols and user workflows used by the solution are able to provide sufficient security properties in practice [3].

Since the planned eID solution will be backed by the state, it will have the same legal status as the state-issued Estonian ID card. This means that it will be universally accepted as a way to access state-provided e-services, including internet voting, which is the core e-service protecting the Estonian democracy. Therefore, it is crucial for the planned eID solution to provide at least the same security level as the state-issued Estonian ID card.

[1] We propose "Mobile-eID" as the marketing name for the planned solution, as the close similarity to "Mobile-ID" may help in keeping it recognizable by the existing user base, while also indicating that it is the succession of an existing solution.

Moreover, as the planned solution does not have the inherent necessity to rely on trusted parties and blackbox components for the management of users' private keys, the next generation eID solution has the potential to solve the fundamental trust issues that the Estonian ID card currently has [4].

In this paper, we have listed several security requirements and principles to which the next generation Mobile-ID solution should comply, in order to reach the security level of the ID card and even above that.

1.1 Background

The existing Mobile-ID solution was introduced in 2007 by a company known as SK ID Solutions (hereinafter – SK) together with Estonian mobile operators. In the Mobile-ID solution, the eID functionality is implemented on a phone SIM card using SIM Application Toolkit (STK), which is supported by almost all mobile phones that have been produced. The SIM card stores asymmetric private keys and is able to create cryptographic signatures using these keys. The data that has to be signed and the produced cryptographic signature is sent to and from the phone using SMS (Short Message Service).

In 2011, the Estonian state concluded a contract with SK to provide the Mobile-ID solution as an electronic identity document that is issued by the Estonian state. In practice, the state's involvement in the issuance of Mobile-ID is limited to maintaining a website, in which the Mobile-ID holders have to authenticate with their Estonian ID card to activate the use of their Mobile-IDs.

The Mobile-ID contract concluded between the state and SK was set to expire on 2021-12-31. However, because of the prolonged procurement process for a new Mobile-ID solution, the existing contract was extended for 6 months until 2022-06-30. After this date, the existing Mobile-ID instances will remain valid until they expire (up to 5 years), but no new Mobile-IDs in the form of a state-issued electronic identity document will be issued.

Theoretically, the existing Mobile-ID solution could be used for another decade or more. However, SK is not willing to extend the Mobile-ID contract with the state any further, and the use of the existing Mobile-ID solution for digital signing is in a legal gray zone, as the Mobile-ID solution has not passed the QSCD security certification, which is currently required by the eIDAS framework.

Meanwhile, in 2017 SK introduced a new eID solution – Smart-ID. The higher level protocols and user workflows of Smart-ID are based on Mobile-ID, with the main difference being that the eID functionality in Smart-ID is implemented in a smartphone application. The user's private keys in Smart-ID are split, part of the key being stored in the user's mobile device and the other part in a server-side Hardware Security Module (HSM) operated by SK.

Soon after being introduced, the Smart-ID solution gained a dominant position in its use in Estonia. This was mainly thanks to the banks, who promoted Smart-ID as a replacement for password authentication, which at that time was the most popular authentication method for online banking, but was being actively phased out by the banks. Later, due to the growing user demand, other private e-service providers and the state followed the banks and implemented support for Smart-ID in their e-services.

In the public Mobile-eID procurement, opened on 2020-08-17, the state was looking for a next generation Mobile eID service that would not rely on a phone's SIM card. In this procurement, two companies submitted their offers – the Estonian company "SK ID Solutions" and the Belgian company "Belgian Mobile ID". However, on 2021-12-08, the procurement process was closed without declaring a winner. [5]

2 General requirements

Before discussing the security requirements, we have to agree on the general concept of the planned Mobile-eID solution. Since the general concept of the existing eID solutions has proven to be successful, we follow the same concept when defining the general requirements for the planned solution.

At its core, the Mobile-eID solution must provide two functions. The ability for a Mobile-eID user to: (1) prove their identity to e-services (authentication); and (2) create Qualified Electronic Signatures (digital signing). Both functions should be implemented using standard asymmetric cryptography algorithms and the users' cryptographic keys should be bound to their identities using X.509 certificates and the corresponding public key infrastructure (PKI).

Preferably, both functions should be provided by a single mobile app. The mobile app should be developed for, currently, the two most popular mobile platforms – Android and iOS.

Authentication. The user workflow should enable the possibility to authenticate the actions initiated by a Mobile-eID user on the Mobile-eID device itself, as well as the user's actions initiated on another device trusted by the user.

Digital signing. The digital signature creation process should result in a Qualified Electronic Signature that conforms to the signature file formats stipulated by the eIDAS framework (i.e., XAdES).

3 Security requirements

The security requirements discussed above have been motivated by the shortcomings of the existing Mobile-ID and Smart-ID solutions. The discussion has been kept generalized, as to provide flexibility for the potential technical solutions aimed at satisfying the particular requirement.

3.1 Transaction initiation

Transactions must be initiated by the actions of an authenticated Mobile-eID user. The Mobile-eID user must not be required to react on transaction requests initiated by other parties, even if these parties may know some semi-private information about the Mobile-eID user. Meeting this requirement is necessary to avoid user disturbance attacks and increase the complexity of phishing attacks.

3.2 Human factors

The solution must not require the user to perform security-critical checks, such as comparison of some control codes or verification of the authenticity of a relying party (e-service provider). Such security checks must be performed by the technological solution itself. All the actions that need to be performed by the user must be intuitive and free from potential confusion.

This requirement is paramount as the human factor is the weakest link in any type of security system.

3.3 Authentication

The authentication process must be bound to a secure channel that is established between a Mobile-eID user and an authenticated relying party (e-service provider). In practice, this would be largely limited to the use case, where a user authenticates to a TLS-authenticated website of an e-service provider by cryptographically signing a challenge provided by the website. Other authentication use cases, where the cryptographic identity of a relying party cannot be established (e.g., authentication over a phone call) must not be supported, as in these cases man-in-the-middle relay impersonation attacks cannot be prevented.

The authentication process must be secure against phishing attacks. That is, when a Mobile-eID user is authenticating to a malicious phishing website, the attacker must not be able to impersonate the user in another website.

The ID card authentication (both on TLS level and Web eID) is secure against such attacks. The existing Mobile-ID and Smart-ID solutions are vulnerable to such attacks, which is the central cause for the hundreds of successful banking scams that have taken place in Estonia for the last couple of years [6].

3.4 Digital signing

What You See Is What You Sign. The user must be able to inspect the exact content that is to be signed before the signature is given. The inspection must be possible in an electronic environment trusted by the user and must not require significant extra effort from the user.

In the existing Mobile-ID and Smart-ID solutions, the user has no credible means to see the data that they are requested to sign. This allows relying parties (e-service providers) to obtain the user's signature on arbitrary content. As a result, such "blind" signatures are not able to achieve the main purpose of a signature – i.e., the ability to prove the signatory's intent.

3.5 Private key generation and protection

The key generation and storage must be performed by a trusted component under the user's control (i.e., a mobile app running on the user's phone). This component must be publicly auditable and verifiable to the highest extent possible (see Section 3.7).

The cryptographic operations performed with the key have to be authorized by a PIN code. An attacker who has gained full physical and logical control of the user's Mobile-eID device, should not be able to bruteforce the PIN code or perform security operations with the user's keys without knowing the PIN code.

To prevent the user's private key from being cloned, a part of the user's private key can be generated and stored by a publicly untrusted blackbox component operated by a semi-trusted third party, as long as it is mathematically ensured that this third party cannot use the user's secret to perform any security operations on behalf of the user[2].

3.6 Intermediary service

An intermediary service in this context is a service that serves as an intermediary between a Mobile-eID user and a relying party (e-service provider), or assists a Mobile-eID user in the creation of a cryptographic signature.

Trust aspects. The entire security of the solution must not rely on the trustworthiness of this component. I.e., an entity that has full control of it must not be able to forge signatures or be able to impersonate the Mobile-eID user in e-services. Unfortunately, the intermediary services used in the existing Mobile-ID and Smart-ID solutions do not satisfy this requirement.

This component may be trusted for less critical tasks, such as enforcing the security policy of the number of allowed incorrect PIN tries and the requirement that the Mobile-eID holder must interact with this service in order to perform cryptographic operations with their keys.

3.7 Mobile app

Transparency and verifiability. The mobile app component running in the Mobile-eID user's device must be a fully open and transparent component. The protocols and APIs must be publicly documented, supporting the creation of alternative app implementations.

The source code of the official app has to be public and the build system has to implement reproducible builds, enabling the possibility to verify that the binary distribution of the app has been built using the source code that has been published.

The app must be self-contained, meaning that the app must not implement remote runtime code or configuration that can affect the security of the app.

The app should use best practices to protect itself from other (potentially malicious) apps running on the mobile device.

If there is an additional software component that runs in the Mobile-eID user's computer, the same requirements should apply to that component as well.

3.8 Enrollment

The number of digital identities. A person should only be able to have a single Mobile-eID account valid at a time. When applying for a new Mobile-eID account, the previous Mobile-eID account of the person should be revoked. This is necessary to avoid the situation where another Mobile-eID instance is used by a fraudster without (or even with) the Mobile-eID user's knowledge.

[2] In general, this would require the use of threshold cryptography in a similar fashion as used by the existing Smart-ID solution.

Remote enrollment. In the case of a remote Mobile-eID enrollment, a remote facial biometric verification of the person must be performed by the issuer. The biometric verification procedure must not only verify the presence of the person, but also the person's intent to be enrolled for a Mobile-eID account.

The use of automated facial verification solutions should be encouraged, but only to support the human operator performing the verification, as the automated solutions are inherently susceptible to various spoofing attacks.

The use of notified digital identities. The person, in whose name the Mobile-eID account has been created, has to be notified of this fact through a secure notification service[3] maintained by an independent party.

Mobile-eID identities which have not been communicated to (and, possibly, confirmed by) the corresponding person, should not be accepted by the relying parties.

This measure prevents the provider of the Mobile-eID service (and possibly other parties) from creating and using temporary identities issued in the name of a person without the person's knowledge[4].

For the most part, this measure is important in the context of authentication to e-services, as in the existing high-risk eID use cases, digital signing is only used once a successful authentication of a user has taken place (e.g., online banking, i-voting).

4 Development considerations

The unsuccessful Mobile-eID procurement process has shown that the potential providers of the Mobile-eID solution are not particularly interested in the opportunity to provide an innovative and secure eID solution for the Estonian society. Rather, they are interested in the opportunity to use the exclusive position granted by the state to freely determine the price that the e-service providers will have to pay them for each Mobile-eID transaction made [5, 8]. This, of course, is not surprising, as the main objective for these companies is profit.

However, we stress that the question of how a secure eID should look is too important for the Estonian society for it to be left to entities, whose decision making process is mainly driven by their financial interests. Therefore, we urge the state to take an active role in steering the development of this next generation eID solution. The intellectual property of the solution (to the highest extent possible) should be owned by the state. If some parts of the solution have to be outsourced to a private service provider, the state should maintain the possibility to change the service provider whenever needed. This should prevent a vendor lock-in and would also let the state retain control over the pricing policy for the Mobile-eID users and e-service providers[5].

When building a new eID solution, the most time consuming part is the security certification of the cryptographic engine in order to meet the legal

[3] A notification service in such a form currently does not exist, but the need for such a service is also motivated by the necessity to introduce a secure feedback channel to notify a voter that they have cast an i-vote [7].

[4] This idea is derived from the concept of Certificate Transparency.

[5] For instance, in Latvia, to encourage the use of the national eID solutions, the solutions are provided to users and e-service providers free of charge [9].

requirements for Qualified Signature Creation Devices (QSCDs). We note, however, that it is possible to license an already certified cryptographic engine[6] and build unique eID solutions on top of it.

To move forward with the development of the next generation eID solution, we invite the state to announce a public competition for the prototype of a solution that meets the security requirements described in this paper. The security properties listed above can be achieved using different security architectures. However, the architecture and implementation that provides the best user experience and relies on the least security assumptions should be chosen as the winner. To decide on the optimum balance between the two, we encourage the state to make this a public process, inviting contributions from the Estonian cyber security community.

Acknowledgements. This research has been carried out with financial support from the European Social Fund through the IT Academy programme and from the Estonian Ministry of Economic Affairs and Communications.

We would like to thank Semjon Kravtsenko for the fruitful discussions on this topic.

References

[1] Police and Border Guard Board. Procurement 224626: A full mobile electronic identity service (in Estonian), August 17, 2020. `https://riigihanked.riik.ee/rhr-web/#/procurement/2063672/documents?group=B`.

[2] Police and Border Guard Board. Technical specification for the Mobile-ID procurement, August 17, 2020. `https://riigihanked.riik.ee/rhr-web/#/procurement/2063672/documents/source-document?group=B&documentOldId=14814095`.

[3] Postimees. The application, created for security reasons, has become a trap for Estonians (in Estonian), December 4, 2021. `https://majandus.postimees.ee/7400602/turvalisuse-huvides-loodud-rakendusest-on-saanud-uus-eestlaste-petuloks`.

[4] Arnis Parsovs. Estonian Electronic Identity Card: Security Flaws in Key Management. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1785–1802. USENIX Association, August 2020.

[5] ERR News. Estonia's Mobile-ID procurement fails, December 10, 2021. `https://news.err.ee/1608431867/estonia-s-mobile-id-procurement-fails`.

[6] ERR News. Phone fraud on the rise, July 25, 2021. `https://news.err.ee/1608288237/phone-fraud-on-the-rise`.

[6] For example, Cybernetica's SplitKey [10] technology that is currenty used by the Smart-ID solution.

[7] Arne Koitmäe, Jan Willemson, and Priit Vinkel. Vote secrecy and voter feedback in remote voting – can we have both? In *Electronic Voting*, pages 140–154, Cham, 2021. Springer International Publishing.

[8] Geenius. SK, which has been developing Mobile-ID for decades, will not be developing a new digital identity for the state (in Estonian), November 5, 2021. https://digipro.geenius.ee/rubriik/uudis/aastakumneid-mobiil-id-d-arendanud-sk-ei-jatka-digitaalse-isikutunnistuse-arendamist/.

[9] LV portāls. eID is becoming a universal digital identification tool (in Latvian), December 1, 2021. https://lvportals.lv/skaidrojumi/335301-eid-klust-par-universalu-digitalo-identifikacijas-lidzekli-2021.

[10] Cybernetica AS. SplitKey: Next generation digital ID technology, December 15, 2021. https://cyber.ee/products/splitkey/.