Security improvements for the Estonian ID card

Arnis Parsovs
University of Tartu

June 17, 2022

1 Introduction

The Estonian state is currently in the process of preparing a procurement specification for ID card manufacturing for the period 2023–2028. Since the planned procurement can possibly result in a new ID card manufacturer and a new chip technology, this may be a good time for planning the introduction of significant changes to the ID card manufacturing, personalization and post-issuance procedures.

In this paper we have described several proposals that should improve the security guarantees and add convenience and security features to the Estonian ID card in the context of its eID functionality.

In particular, we discuss the solutions to: (1) ensure that the private keys can occur only in the ID card chip; (2) increase the assurance that the cardholder is the only one who knows the PIN codes; (3) prevent the abuse of the ID card when it is out of the cardholder's control; and (4) increase the convenience for receiving eID issuance and maintenance services.

The proposals may seem ambitious, but since the Estonian ID card is the base eID of the Estonian e-state and is the front runner of its kind, we believe that the Estonian ID card must set high security standards.

2 Proposals

The proposals listed above, in theory, are independent and hence can be implemented separately. However, some of them support each other and hence need to be implemented together to achieve a sufficient level of security.

2.1 Removal of private key import/export functionality

Problem. The core function of the security chip used by the Estonian ID card is to ensure that the cardholder's authentication and digital signature private keys can only ever occur in a single copy inside the protected memory of the ID card chip. In practice, this is realized by generating the cardholder's asymmetric keys inside the ID card chip and ensuring that there are no technical means that could be used to extract the private key from the chip.

In the history of the Estonian ID card there has been at least one publicly documented incident, where an ID card manufacturer has ignored the security requirements and has personalized ID cards by importing copies of private keys generated outside the ID card (see Section 6.8.2 in [1]).

Such misbehavior can occur relatively easy due to the fact that the private key import and export functions are standard features of a JavaCard platform (operating system). This means that the eID applet and other applets loaded in the ID card can implement the private key import and export functionality. This leads to a situation where the use of this high-risk feature in the ID card personalization process can only be prevented through organizational measures that can be easily bypassed leaving no trace for discovery.

Solution. To reduce the risk of accidental or intentional use of the private key import/export functionality, the state should purchase an ID card chip platform which, on the operating system level, does not provide the asymmetric private key import and export feature. This should ensure that the only way applets loaded into the ID card could use asymmetric private key operations is by generating the private keys on-card such that the private key never leaves the chip.

To confirm that the ID card chip platform supplied by the ID card manufacturer does not provide such a private key import/export functionality, the chip platform (or its configuration) has to be Common Criteria certified. The certification report must explicitly state that the evaluation facility has verified that the JavaCard operating system enables private key operations only with on-card generated keys and that these keys cannot be exported. The certification report must also clearly specify how the product which meets these requirements can be unambiguously and publicly identified, e.g., by querying the Card Production Life Cycle (CPLC) data of the card using the GlobalPlatform `GET DATA` command.

Security benefits. The main security benefit would be that the applets loaded on the ID card would not be able to use the asymmetric private key import or export functionality either accidentally or intentionally. Since this would be enforced on the operating system level, it would also apply to the asymmetric private keys used by the eMRTD applet (see Section 2.7).

In theory, a maliciously crafted JavaCard applet could bypass this operating system restriction by implementing its own asymmetric crypto library with private key import or export functionality in an applet using standard math operations provided by JavaCard (e.g., see JCMathLib [2]). However, such an asymmetric crypto implementation would be noticeably slower than the one provided by the operating system and hence would risk being detected.

Of course, the implementation of this proposal will not prevent an attack where a malicious ID card manufacturer supplies a smart card chip whose operating system indicates that the asymmetric key import/export functionality is not supported, while in practice it is supported (or, alternatively, the chip operating system contains other backdoors).

However, such a smart card chip forgery requires a greater amount of conspiracy and if detected cannot be plausibly denied by claiming that the ID card private keys were copied by a local sub-contractor without the ID card manufacturer being aware of it [3].

Impact assessment. To our knowledge there are no JavaCard platforms that have been certified with the absence of private key import and export features. This means that the ID card manufacturer will have to recertify a ready-made JavaCard platform, the evaluation facility ensuring that the calls to JavaCard functions that enable private key import and export return an error condition.

We note that these changes to the operating system do not require any changes to the potential applets that will be loaded into the ID card, because the JavaCard API will not change. Therefore, applets can still contain private key import or export code, but when called, these operations will simply not succeed.

2.2 Removal of the "police key"

Problem. The so-called "police key" [4] is used to implement the PIN bypass feature that enables cardholders to unblock and change forgotten PIN codes in PPA customer service points (see Section 2.11.4 in [1]).

Since the police key has to be loaded into the ID card and has to be used to establish a secure channel with the card in the PIN renewal process, the ID card manufacturer must be able to process plaintext values of the police key. This means that the ID card manufacturer can only protect the confidentiality of the police key through procedural measures[1].

While the official use of the police key requires physical verification of a cardholder's identity, the parties that are in possession of this key and have gained physical or logical (e.g., remote) access to an ID card, can recover the values of the ID card's PIN codes and set new values without leaving any trace, as the use of the key is an offline operation that does not leave any audit records inside the ID card.

Solution. To eliminate the risk of potential abuse of the police key, the ID card should not support the functionality provided by the police key. In fact, there should be no technical means for the ID card manufacturer or any other party (other than the cardholder using their PUK code) to discover the PIN code values or reset them. The manufacturer should be able to set the PIN codes only once in the initialization process of the ID card's eID instance.

The PIN renewal service should instead be implemented by initializing the ID card with a new eID instance, which involves the generation of fresh authentication and digital signature keys and issuance of the corresponding X.509 certificates.

Of course, a malicious ID card manufacturer will still be able to impersonate a cardholder by creating a fresh eID instance on behalf of the cardholder. This, however: (1) requires issuance of new certificates and hence will leave a cryptographic trace; and (2) does not enable access to the current instance of the cardholder's keys and hence the ability to decrypt documents encrypted for these keys.

Impact assessment. From the cardholder's perspective, the only difference is that after the PIN renewal process the cardholder will receive not only a new PIN envelope, but also a new set of keys and certificates. This means that cardholders will not be able to decrypt documents encrypted for the previous keys, but the ID card based document encryption is not meant for long-term document storage anyway.

The added key generation and certificate loading process should add just a couple tens of extra seconds. Depending on the ID card manufacturing contract, the issuance of new certificates may result in additional expenses for the state, but these costs could then be included in the service fee for the PIN renewal service.

[1] A procedural measure is a weak form of security measure, as it essentially means that the information is available to parties, but the parties promise to "not look at it", or if they have seen it, they promise to "not abuse it".

2.3 Removal of the certificate suspension mechanism

Problem. The certificate suspension mechanism enables the possibility to temporarily suspend the validity of ID card certificates (see Section 2.15 in [1]). The suspension mechanism is supposed to prevent the abuse of the ID card's eID functionality while the certificates are suspended.

Unfortunately, the suspension of certificates does not prevent an attacker from creating digital signatures during the time when the certificates are suspended. This is because the attacker can produce a cryptographic signature with the ID card while the certificates are in a suspended state, but later, once the certificates becomes valid, produce a valid digital signature by obtaining a positive certificate validity confirmation.

This results in a security issue and allows the validity of any digital signature created with the Estonian ID card to be challenged, as the validation process set out in eIDAS Article 32(1) cannot provide assurance that the digital signature was given when the signatory's certificate was valid [5].

Solution. As a solution, the certificate suspension mechanism should be removed. If a cardholder loses control over their ID card, they should still be able to call the ID card helpline and request that the certificates be blocked. However, the certificate validity should not be suspended, but instead the certificates should be irrevocably revoked.

To provide cardholders with an option similar to the termination of certificate suspension, the cardholders should be provided with an option to renew revoked certificates in PPA customer service points.

In principle, it should be sufficient to load only new certificates in the ID card retaining the same asymmetric keys and PIN codes. However, it would be safer to fully reinitialize the ID card's eID instance. This would also allow PPA to reuse the same workflow as used for the PIN renewal service (see Section 2.2).

Impact assessment. From the cardholder's perspective, the only difference is that instead of being able to unblock the same certificates, the cardholder has to present the affected ID card to a PPA employee and new certificates are loaded in the ID card.

From the state's perspective, the cost of the service will slightly increase as new certificates have to be loaded in the ID card. To solve this problem, the state can introduce a service fee similarly as it has been introduced for the PIN renewal service.

2.4 Certificate issuance on the first use of eID

Problem. To prevent the abuse of the ID card's eID functionality before the card is handed out to the cardholder, the ID cards are manufactured in an inactive state. In technical terms this is implemented by issuing the ID card certificates in a suspended state and terminating the certificate suspension once the ID card has been handed out to the cardholder.

Unfortunately, this security measure is not able to prevent the creation of digital signatures with a cardholder's ID card before it has been handed out to the cardholder (see Section 6.11 in [1]), since it relies on the same certificate suspension mechanism and therefore carries the same security and legal issues as described in Section 2.3.

Solution. To prevent the abuse of the ID card's eID functionality before the card is handed out to the cardholder, the ID card should be handed out without certificates. On the cardholder's first use of the ID card, the ID card software should obtain fresh certificates and load them into the ID card. The ID card activation process by PPA must ensure that the issuance of ID card certificates is enabled only after the ID card has been handed out to the cardholder.

We note that a similar process is used for the issuance of Mobile-ID certificates, where the certificates are issued after the cardholder has confirmed that the Mobile-ID SIM card is in their possession.

Preferably, this remote ID card initialization process should also involve the generation of the cardholder's asymmetric authentication and digital signature keys. The remote personalization of the ID card keys should provide transparency and hence a higher assurance that the keys have been generated inside the ID card and have not been exported afterwards.

Impact assessment. The introduction of this change would require cardholders to perform an additional step before the eID functionality of the card can be used. However, this process could be seamlessly integrated as a part of the PIN initialization process described in Section 2.5.

The drawback of this change is that it will not be possible to send encrypted documents to cardholders before they have activated the eID functionality of their ID cards.

On the other hand, if another ROCA type of vulnerability is found, the attack exposure will be limited to only those cardholders who use the eID functionality of the card. This also allows the state to obtain more precise statistics about the cardholders who have used the eID functionality of their ID cards.

From the technical perspective, this change requires the design of a secure protocol for such a remote ID card initialization and such a feature has to be implemented in the ID card software.

2.5 Introduction of transport PIN

Problem. In the current setup, the ID card PIN codes are set by the ID card manufacturer in the ID card personalization phase. Since the PIN code value has to be loaded into the ID card and printed for inclusion in a PIN envelope, the ID card manufacturer must be able to process plaintext values of the ID card PIN codes. This means that the ID card manufacturer can protect the confidentiality of the cardholder's PIN codes only through procedural measures.

An additional challenge is the protection of PIN codes while they are in transit, i.e., during their delivery to the cardholders. The PIN codes are delivered to cardholders in a closed PIN envelope, which in theory should prevent third parties from learning the codes without damaging the envelope. However, in practice we have seen incidents where PIN codes inside the envelope are visible without opening the envelope (see Section 6.11 in [1]). Furthermore, the use of PIN envelopes does not prevent a slightly more sophisticated attack where the PIN codes are learned by opening the envelope, but the codes are then resealed in a new envelope that is then delivered to the cardholder. The detection of such an attack is unlikely, as the PIN envelope does not carry any physical security features and even if it did, the cardholders do not know how an authentic PIN envelope should look.

Currently, the ID card holders are not forced to change the initial PIN codes, therefore, it is very likely that only a handful of cardholders have changed their PIN codes (including PUK) in the life cycle of their ID cards. This means that the knowledge of the initial PIN codes gives an attacker the possibility to exploit this knowledge throughout the life cycle of the ID card, assuming that at some point the attacker is able to gain physical or logical (e.g., remote) access to the ID card.

Furthermore, currently, by knowing the PIN codes, it is possible to create digital signatures with a cardholder's ID card before it has been handed out to the cardholder and there are no technical means for the cardholder to discover this afterwards (see Section 6.11 in [1]).

Solution. The proposed solution is to introduce a transport PIN, which must be used by a cardholder to set PIN codes before the first use of the ID card's eID functionality.

To implement it, in the card personalization phase the PIN1 and PIN2 codes should be left blocked and unset. The ID card should be handed out to a cardholder with a PIN envelope which only contains an "activation code", which in technical terms is the traditional random 8-digit PUK code.

On the first use of the ID card, the ID card software should request that the cardholder enter the activation code, after which the software should configure the ID card with new random values for the PIN1, PIN2 and PUK codes, displaying the values to the cardholder and asking the cardholder to write them down (see Figure 1).

The configuration of new PIN codes can be an offline operation, technically implemented as if the cardholder has manually changed the values using the PUK code. However, a different set of APDU commands should be used by the card in order to enable the usage of smart card readers with a PIN pad and PIN firewall (see Section 2.14.1 in [1]). Preferably, a single APDU command should be used to set the new values for all 3 PIN codes in a single transaction,

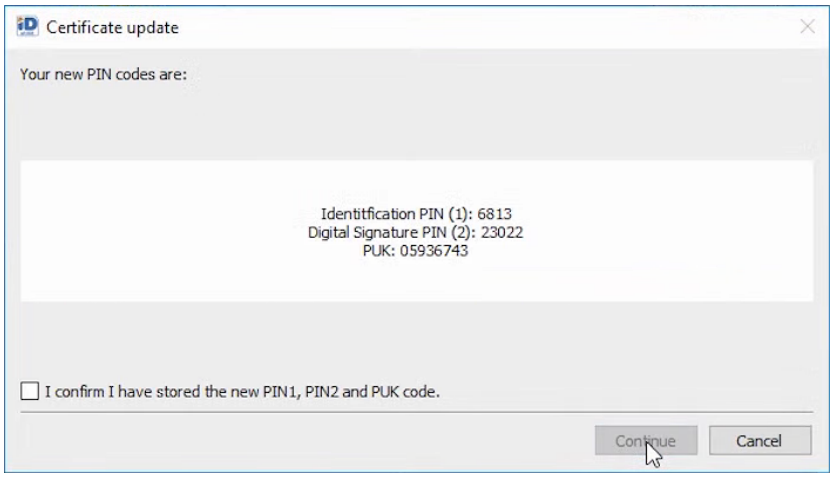

Figure 1: The ID card software UI window for new PIN codes. (Screenshot from the remote ID card update process [6].)

as to provide atomicity for this procedure. The use of this procedure must be possible only once in the life cycle of the card's eID instance.

We recommend that the ID card software generate the new codes rather than asking for the new codes to be entered by the cardholder. This provides two benefits: (1) randomly generated codes will be more random than the codes chosen by a cardholder; and (2) writing down the generated values is a cognitively easier task and less prone to failure, compared to choosing ones own values and remembering to write them down as they have been entered.

Security benefits. The introduction of the transport PIN provides two main security benefits. First, the confidentiality requirements for the transport PIN are slightly weaker compared to the confidentiality requirements for PIN codes. This is because the transport PIN can not be [directly] used to access the eID functionality of the card and the confidentiality of the transport PIN matters only temporarily, until the cardholder has used it to set the new PIN values.

The second benefit of the transport PIN is that it allows a cardholder to detect if someone has used the eID functionality of the card before the cardholder, because in such a case the cardholder will not be able to set the PIN codes to use the eID functionality of the card. In order to be able to investigate such cases, the proposal described in Section 2.4 should be implemented, which should enable the discovery of the time and the IP address of the computer that was used to initialize the eID functionality of the ID card.

This, together with the removal of the "police key" (Section 2.2), enables a strong security claim to be made. Namely, that the ID card holder who is using the eID functionality of the card is the only one who knows the second factor (PIN codes) of the eID solution, as only the cardholder themselves could have set these values.

Another security benefit is that the transport PIN provides better protection against PIN brute-force attacks for ID cards whose PIN values have not yet been set using the transport PIN. This is because the chance of guessing an 8-digit

transport PIN is considerably less likely than guessing 4-digit PIN1 or 5-digit PIN2 values (see Section 2.11.2 in [1]).

Impact assessment. The introduction of a transport PIN would require cardholders to perform two additional steps before the eID functionality of the card can be used: (1) entering the 8-digit activation code; and (2) writing down the new PIN1, PIN2 and PUK codes.

We consider this to be an insignificant one-time inconvenience and note that a similar concept of a transport PIN is used for national identity cards in Finland [7] and Germany [8]. Furthermore, for a significant part of the Estonian ID card holders, the concept of writing down PIN codes is not new, as a similar concept (see Figure 1) was used in the remote ID card update process that was performed by several hundred thousand cardholders during the period from June 2016 to May 2019 (see Section 5.4 in [1]).

However, it is safe to expect that, at least initially, there will be a number of support requests asking what to do with the activation code. It is also likely that the use of the PIN renewal service provided by PPA will slightly increase due to cardholders who have skipped writing down the PIN codes or have written them down incorrectly or illegibly.

From the technical perspective, such a feature has to be implemented in the ID card software and the ID card's eID applet has to be configured or extended to enable such a feature.

2.6 Remote ID card issuance and maintenance

Problem. According to the current procedure, to receive a new ID card, a cardholder has to visit a PPA customer service point or an Estonian foreign representation in person. Alternatively, a cardholder can appoint a representative who is authorized to collect the new ID card, but this option is available only if the cardholder applies for the ID card in person (see Section 2.2.2 in [9]). The PIN renewal service and the service for termination of certificate suspension are provided only in person.

The requirement of physical presence is a significant challenge for people with severe movement disabilities and for those Estonians and e-residents living abroad, whose closest Estonian foreign representation is hundreds, if not thousands of kilometers away [10].

The current situation does not meet the convenience standards of a modern state and hence the state should look for secure solutions to enable remote eID issuance and maintenance for their citizens and (e)-residents.

Solution. A seemingly straightforward solution for a remote ID card issuance would be to deliver the new ID card with PIN envelope using a secure courier service. However, the ID card should be delivered to a cardholder in an unusable state[2], as otherwise any person in the delivery chain could abuse the eID functionality of the card to its full extent.

After receiving the ID card, the cardholder would have to activate the card by logging in to a PPA self-service portal using the cardholder's existing eID solution. We note that almost the same approach is currently used by the state in the issuance of Mobile-ID, with the only difference being that in the case of Mobile-ID the physical identity verification of the cardholder is performed by a mobile operator's representative and not a courier.

However, we see two reasons why this might not be the best approach for a remote ID card issuance:

1. Cardholders who do not have access to a functional state-issued eID solution will not be able to active the card. The state could increase the accessibility of the activation service by enabling activation using Smart-ID. However, the reliance on a derived third-party eID solution for the issuance of the state's base eID solution degrades the security level of the base eID solution.

2. Cardholder's identity verification performed by a foreign courier service employee is unlikely to meet the same assurance level as that performed by an Estonian state official.

To maintain equivalent assurance in terms of reliability to physical presence (eIDAS Article 24(1)(d)), we suggest providing the ID card activation service in a form of a face-to-face video meeting. The ID card would be activated after a PPA official has performed manual facial identity verification and orally verified the cardholder's intent to activate the card. Preferably, the manual facial verification process should be supplemented by a machine-performed facial verification.

[2]Preferably, with the certificates not yet issued (see Section 2.4).

By using the ID card's eMRTD functionality (see Section 2.7), in the ID card activation process it is possible to remotely verify whether the ID card attached to the cardholder's computer is the authentic ID card that was delivered to the cardholder. Since the cardholder's possession of the ID card can be cryptographically verified[3], the use of a secure courier service for the ID card delivery might not be required and hence a much cheaper regular mail could be used instead.

The same online face-to-face service could also be used to remotely provide the eID maintenance services: (1) the PIN renewal service; and (2) the termination of certificate suspension (or the renewal of revoked certificates – see Section 2.3). The remote provision of these services would require a PPA employee to open the PIN envelope and disclose the transport PIN to the cardholder. However, this does not introduce a significant security risk in practice, as the transport PIN will lose its significance as soon as the cardholder uses it to set the new PIN codes for the card (which in most cases is likely to take place shortly after using the service).

Design considerations. The online face-to-face service can be implemented as a web service using standard video conferencing solutions. However, the video recording of the meeting must be stored by PPA for auditing purposes and as evidence in case of disputes.

To provide PPA with remote access to the cardholder's ID card, the Web eID browser extension [12] should be extended to provide a feature for raw smart card access from a set of whitelisted websites (e.g., `taotlus.politsei.ee`).

The technical solution should enable the appointment of a video meeting with a PPA employee only after the web service has verified the presence of the cardholder's authentic ID card in a smart card reader and, possibly, after the cardholder has paid for the service.

Impact assessment. The provision of remote eID services will have a positive impact on the public perception of Estonia as a modern state. Due to the COVID-19 pandemic, people have adjusted to moving their activities online and hence today participation in video meetings can be assumed to be a standard capability of the average IT user.

The introduction of such a service will require significant development efforts on the part of PPA. The cost of the service, however, should not increase, as the provision of a remote service should not take more time for a PPA employee than provision of the same service in a PPA customer service point.

The ability to provide eID issuance and maintenance services remotely is a crucial contingency measure for an e-state and hence may turn out to be a decisive factor when facing the next pandemic or similar crises where free movement of people is restricted.

[3]This prevents an attack where somewhere in the delivery chain the ID card chip is replaced with a fake one (see Section 4.3 in [11]), and as a result, the cardholder activates the ID card chip that actually is in the attacker's possession.

2.7 eMRTD loading in all types of ID cards

Problem. The smart card chips of some types of ID cards implement the eMRTD (Electronic Machine Readable Travel Document) function. This function is implemented as a smart card applet which stores digitally signed information about the identity document and its holder (including the facial image of the document holder). In addition, the eMRTD applet provides a challenge-response mechanism that enables cryptographic verification of the chip's authenticty (i.e., prevents chip cloning).

While the eMRTD technology has been primarily targeted towards travel documents for enabling automated border crossing, in practice it enables a wide variety of other use cases. It can be used to provide secure authentication to a machine (Section 6 in [11]), to implement biometric access control systems [13], to perform remote biometric verification (e.g., remote onboarding for Smart-ID), and to prove to websites the possession of the ID card without the need to enter PIN codes[4] [14].

From the five types of ID cards issued by the Estonian state, currently the eMRTD function is only provided for the *identity card* and the *residence permit card*. The eMRTD function is not available for the *digital identity card*, the *e-resident's digital identity card* and the *diplomatic identity card*. As a result, the holders of these types of ID cards are currently unable to benefit from solutions that rely on the eMRTD function.

Solution. The solution is to also add the eMRTD function to the *digital identity card*, the *e-resident's digital identity card* and the *diplomatic identity card*.

Preferably, the visual design of the cards should be extended with the machine-readable zone (MRZ) in order to enable optical reading of the Basic Access Control (BAC) key that is required to communicate with the eMRTD applet. However, we note that Estonian ID card-specific solutions can construct the BAC key more conveniently, i.e., by reading the entries of the personal data file stored in the ID card's eID applet (see Section 3.3.4 in [1]).

Impact assessment. Since the chips of all types of ID cards have the same technical specification, the loading of the eMRTD applet should only require changes to the ID card personalization workflows. In practice, it would add a couple tens of extra seconds to the personalization of the ID card. The introduction of MRZ would also require changes to the visual design of the ID cards.

[4] The proposal described in Section 2.6 relies on such a feature.

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

References

[1] Arnis Parsovs. *Estonian Electronic Identity Card and its Security Challenges*. PhD thesis, University of Tartu, 2021. https://dspace.ut.ee/handle/10062/71481.

[2] OpenCrypto Project. JCMathLib cryptographic library for Java Card, August 15, 2017. https://github.com/OpenCryptoProject/JCMathLib.

[3] ERR News. Declassified documents reveal ID-card crisis from decade ago, November 26, 2021. https://news.err.ee/1608415676/declassified-documents-reveal-id-card-crisis-from-decade-ago.

[4] Geenius. New ID cards can be accessed with a "police key": what is it for? (in Estonian), December 21, 2018. https://digi.geenius.ee/rubriik/uudis/uutele-id-kaartidele-paaseb-ligi-politsei-votmega-milleks-see-moeldud-on/.

[5] Tõnu Mets and Arnis Parsovs. Time of signing in the Estonian digital signature scheme. *Digital Evidence and Electronic Signature Law Review*, 16:40–50, 2019. https://journals.sas.ac.uk/deeslr/article/view/5076.

[6] Estonian Information System Authority. Renewal of the Estonian ID card certificates 2017, June 22, 2016. https://www.youtube.com/watch?v=BRGFSSoW-Xc.

[7] Digital and Population Data Services Agency. Activation of the Citizen Certificate, April 18, 2022. https://dvv.fi/en/activation-of-the-citizen-certificate.

[8] Federal Ministry of the Interior and Community. German National Identity Card: PIN, PUK and Blocking Code, April 21, 2021. https://www.personalausweisportal.de/Webs/PA/EN/citizens/electronic-identification/pin-puk-blocking-code/pin-puk-blocking-code-node.html.

[9] Estonian Police and Border Guard Board. Estonian eID scheme: ID card. Technical specifications and procedures for assurance level high for electronic identification. Version 1.1, September 30, 2019. https://ec.europa.eu/digital-building-blocks/wikis/download/attachments/62885749/EE%20eID%20LoA%20mapping%20-%20ID%20card%20v1.1.pdf.

[10] ERR News. Applying for, receiving Estonian passports, IDs abroad to be simplified, August 1, 2019. https://news.err.ee/966949/applying-for-receiving-estonian-passports-ids-abroad-to-be-simplified.

[11] Danielle Morgan and Arnis Parsovs. Using the Estonian Electronic Identity Card for Authentication to a Machine (Extended Version). Cryptology ePrint Archive, Report 2017/880, 2017. https://eprint.iacr.org/2017/880.

[12] Mart Sõmermaa. Web eID: electronic identity cards on the Web, March 15, 2022. https://github.com/web-eid/web-eid-system-architecture-doc.

[13] Burak Can Kus. *Use of Electronic Identity Documents for Multi-Factor Authentication*. MSc thesis, University of Tartu, 2021. https://comserv.cs.ut.ee/ati_thesis/datasheet.php?id=72515&year=2021.

[14] UT Institute of Computer Science Graduation Theses Topics Registry. Web eID authentication extension for biometric passports / ID cards, 2021. https://comserv.cs.ut.ee/ati_thesis_offers/datasheet.php?id=73756&year=0.