CYBERNETICA

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti
tuleviku heaks

Analysis of the Possibility to Use ID1 Card's NFC Interface for Authentication and Electronic Signing

Analysis
Version 1.1
11th October 2022
61 pages
Doc. D-26-7

Project leaders: Tõnis Reimo (Estonian Information System Authority)
Andrei Kargin (Estonian Information System Authority)
Katrin Kivi (Estonian Information System Authority)
Kaija Kirch (Cybernetica)
Liis Peets (Cybernetica)

Contributing authors: Aivo Kalu (Cybernetica)
Aleksander Kamenik (Cybernetica)
Burak Can Kuş (Cybernetica)
Valentyna Tsap (Cybernertica)
Triin Siil (Cybernetica)

Estonian Information System Authority, Pärnu maantee 139a, 15169 Tallinn, Estonia.
Email: ria@ria.ee, Web: https://www.ria.ee, Phone: +372 663 0200.

Cybernetica AS, Mäealuse 2/1, 12618 Tallinn, Estonia.
E-mail: info@cyber.ee, Web: https://www.cyber.ee, Phone: +372 639 7991.

Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

NFC (Near-Field Communication) is a technology used daily. A large majority of interactions between devices and smartcards are contactless payments. NFC is also used as a standardised technology requirement for passports which lets people travel to countries all over the world. Since November 2018, Estonia has started issuing ID cards equipped with a contactless interface (ISO/IEC 14443 Type A). This creates a new opportunity for performing authentication and electronic signing without the card holder having to insert the smartcard into a smartcard reader. However, this function is currently not in use, due to uncertainties about the legality and security.

1.2 Project goal

Any changes to the existing national eID ecosystem must be carefully analysed for any additional or changed risks. This project studies the potential usage of the Estonian ID-card via NFC for authentication and electronic signing. The aim is to identify and map the risks and threats, evaluate them, propose risk mitigation tools as a list of requirements that may ensure a secure deployment and usage of ID cards via NFC.

This report only studies ID-cards with IAS ECC applet and ID-One Cosmo v8.2 platform, issued since November 2018. In this report, we only focus on authentication and electronic signing use-cases. The loyalty card use-case of an ID-card is not in the scope of this report.

In this report, ID-card is used as a general term to describe all different types of ID1 format documents issued by the Estonian Police and Border Guard Board. Also terms ”smartcard” or ”card” may be used.

In order to illustrate how authentication and electronic signing can be done via NFC we have included some fictional components to the process description (see Chapter 5). One of such fictional components is the eID app which in practice does not yet exist.

1.3 Acronyms

BAC

Basic Access Control

CAN

Card Access Number. 4-digit number, which is printed on the ID-card and used to establish a secure PACE tunnel with the ID-card applet.

DTBS/R

Data To Be Signed Representation. Cryptographic hash of the data to be signed by the user.

eIDAS

Euroopa Parlamendi ja Nõukogu määrus e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul (in Estonian: ‘**origtitle**’) [9]

eMRTD

Electronic Machine Readable Travel Documents

EUTS

Electronic Identification and Trust Services for Electronic Transactions Act (in Estonian: ‘E-identimise ja e-tehingute usaldusteenuste seadus’) [6]

HID

Human Interface Device

ITDS

Identity Documents Act (in Estonian: ‘Isikut tõendavate dokumentide seadus’) [22]

MRZ

Machine-Readable Zone

NFC

Near-Field Communication. Wireless communication protocol between electronic devices over a distance of 4 cm or less.

OCR

Optical Character Recognition

PACE

Password Authenticated Connection Establishment

PIN

Personal Identification Number, used as knowledge-based factor for authenticating the person. Estonian ID-cards have two PIN numbers. PIN1 is a 4-digit number, which is protecting access to the authentication key pair. PIN2 is a 5-digit number, which is protecting access to the signing key pair.

PP

Protection Profile. A document used as part of the certification process according to ISO/IEC 15408 and the Common Criteria (CC). Provides implementation (specific product) independent specification of security requirements. A PP is combination of threats, security objectives, assumptions, security functional requirements (SFRs), security assurance requirements (SARs) and rationales.

QSCD

Qualified Signature Creation Device

RFID

Radio-Frequency Identification

RIA

Information System Authority (`www.ria.ee`)

SCA

Signature Creation Application. Application, which is running on PC or mobile device and which is handling the ASiC containers, computing the DTBS/R and communicating with the QSCD. One example is the DigiDoc application, which is widely used in Estonia.

TOE

Target of Evaluation. The product or system that is the subject of the evaluation.

VAD

Verification Authentication Data. Data, such as PIN, which is passed to QSCD device in order to authenticate the user.

2 System Description

The Estonian ID-card has an NFC interface but currently there is no supporting ecosystem that would allow to use it, as well as no planned architecture or design documents. For interim purposes, in this chapter we will describe one possible option for an eID system, components of this system and how the user functions could be implemented, so that the following security analysis can be based on this example.

We include two assumed additional components to the existing system in order to explain how the process of electronic signing and authentication would take place in contactless mode. These are smartphone components:

- eID app – an application that will enable the communication of the NFC-enabled smartphone with the ID-card and provide APIs to other apps.
- DigiDoc app – a mobile version of the existing desktop application that will also create ASiC containers (it could also include eID app's functionality)

In the future, some eID system components or interfaces could be implemented differently, or it could be decided that some additional functions will be included. In such a case, the applicability of the current analysis could come into question and some parts of it could require updating.

2.1 System Components

For analysis purposes, our simplified model of the eID system consists of a smartcard and a smart device (smartphone, tablet). To be able to conclude whether signing and authenticating using NFC capability are secure actions to perform, we need to look at the components that the smartcard and the phone consist of and which of those are the main actors/parties in transactions.

Components of the smartcard:

1. JavaCard platform (operating system) on the smart-card – ID-One Cosmo V8.2;
2. eID applet on the JavaCard platform – IAS ECC V2;
3. Third party applets on the JavaCard platform (for example, LDS applet);
4. Wired communication interface (USB interface);
5. Contactless communication interface (NFC radio);

Components of the smartphone:

1. eID app – the assumed additional component (see above in the description of Chapter 2);
2. DigiDoc app – the assumed additional component (see above in the description of Chapter 2);
3. Third party apps, installed on the user's smartphone;
4. Mobile operating system (providing NFC API, for example);
5. Contactless communication interface (NFC radio);

For comparison purposes we also model a desktop computer with the following components:

1. DigiDoc application – responsible for creating signed ASiC containers;

2. ID-card middleware and drivers – responsible for asking user's consent and PIN's, providing API to other applications (e.g. DigiDoc or browsers) and communicating with the ID-card over USB interface with the help of the smartcard reader.

Components are depicted in figure 1.

2.2 System Use Cases

This section gives a short overview of the eID system functions, in the form of use cases. For analysis purposes, we only show a simplified version of the use cases, without exceptions or alternative flows.

Please note that the popular identification use case, where the ID-card is used as an alternative to a customer loyalty card, is not considered a useful example of how to use the NFC interface. The personal data file is read from the ID-card via USB interface, but the data file itself is not accessible without using the card's CAN number and therefore this use case would be impractical.

2.2.1 Adding CAN into the eID App

In order to use the smartcard's NFC functionality for signing and authentication on a phone, the user must first enter the CAN into the eID app so the phone, via its NFC reader, can establish a secure channel with the user's smartcard (Fig. 2).

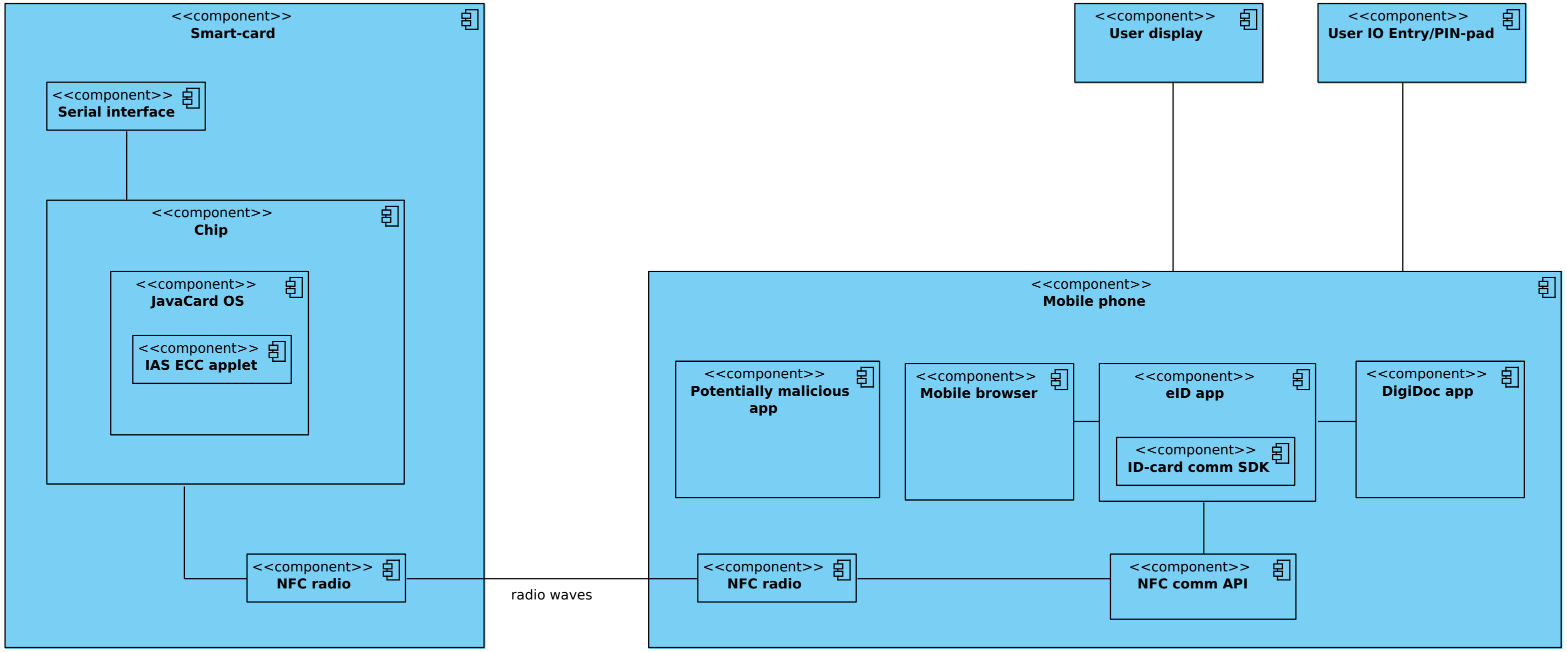


Figure 1: Scope of components involved in contactless mode of communication

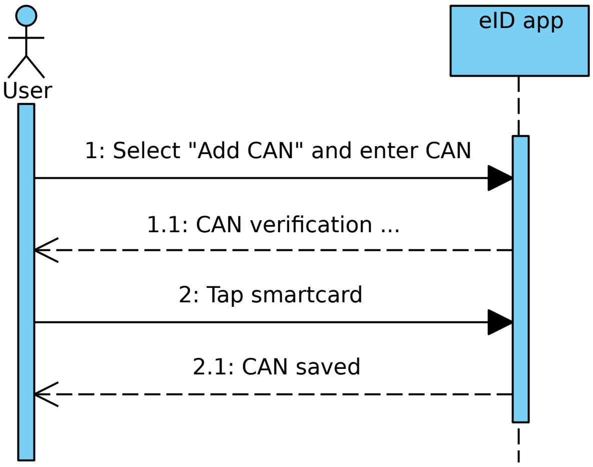


Figure 2: Adding CAN

Main flow of the use case:

1. The user opens the eID app on their phone.
2. The user chooses option “Add CAN”.
3. The user enters the CAN.
4. The app verifies the CAN by asking the user to bring the smartcard close to the phone.
5. The eID app saves the CAN.

The result is that the CAN number is now saved on the user’s phone so during electronic signing or authentication the card is be ready to be used. No manual entry of CAN will be required again unless the eID app is removed or the user is issued a new smartcard.

2.2.2 Electronic Signing over NFC

The goal is to electronically sign a document the user has on their phone using the smartcard’s NFC functionality (Fig. 3). The user must have previously installed a mobile version (an app) of the DigiDoc application which acts as the Signature Creation Application and creates a container with the electronic signature produced by the IAS ECC applet.

It is also possible that the DigiDoc signature creation functionality is embedded in the eID app or vice versa.

Main flow of the use case:

1. The user chooses the file they want to sign from their phone’s directory.
2. The DigiDoc app starts preparing the ASiC container and asks for the user’s certificate via the eID app.
3. The eID app asks the user to bring the smartcard close to the phone.
4. The user taps the smartcard on the smartphone.
5. The eID app creates a PACE tunnel with the smartcard, reads the user’s certificate and returns it to the DigiDoc app.

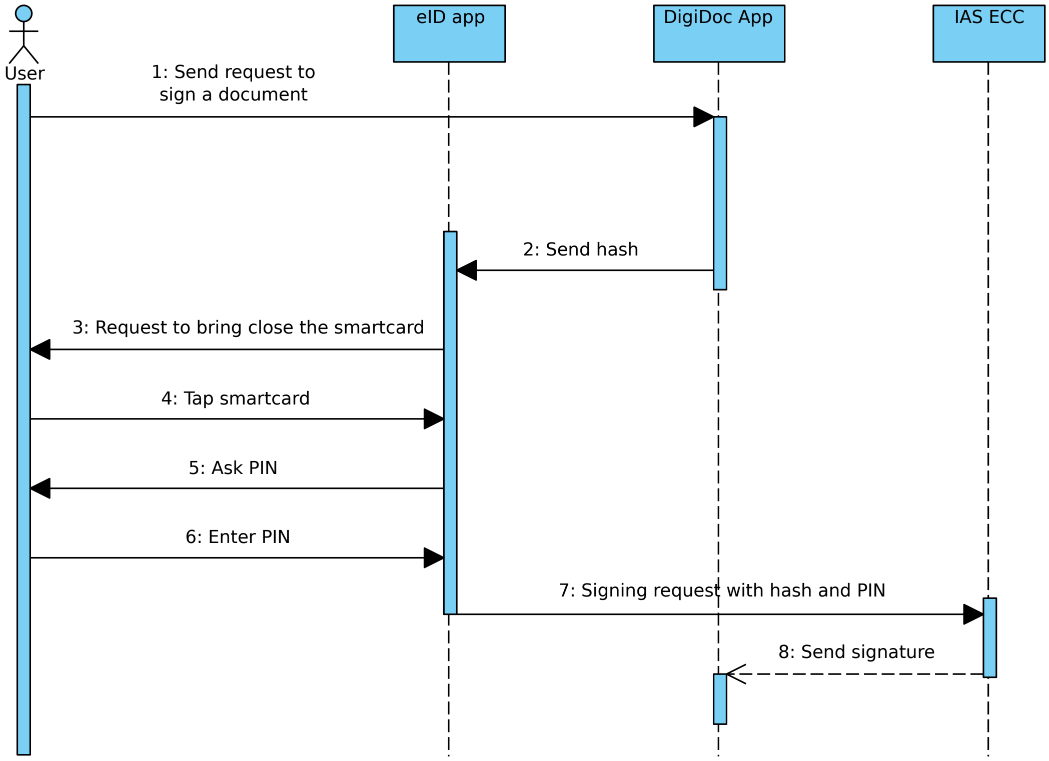

User
eID app
DigiDoc App
IAS ECC
1: Send request to sign a document
2: Send hash
3: Request to bring close the smartcard
4: Tap smartcard
5: Ask PIN
6: Enter PIN
7: Signing request with hash and PIN
8: Send signature

Figure 3: Signing over NFC

6. The DigiDoc app finalises the ASiC container, creates the hash to be signed and sends it to the eID app.
7. The eID app asks the user to enter PIN2.
8. The user enters PIN2 into the eID app on their phone.
9. The eID app creates a PACE tunnel with the smartcard and sends the signing request with the hash and PIN2 to the IAS-ECC applet.
10. The applet creates a cryptographic signature and returns it to the eID app.
11. The eID app returns the signature to the DigiDoc app.
12. The DigiDoc app completes the ASiC container with a signature.

2.2.3 Authenticating over NFC

The goal is to authenticate to a third party website using the smartcard's NFC functionality.

The eID app creates a signature for the authentication request (Fig. 4). The process of how the authentication request reaches the eID app from the browser is outside of the scope of this project. There could be several options, such as Universal Links, App Links, QR-code, or push notification.

Main flow of the use case:

1. The user chooses to log in to a website using the option "ID card via NFC".

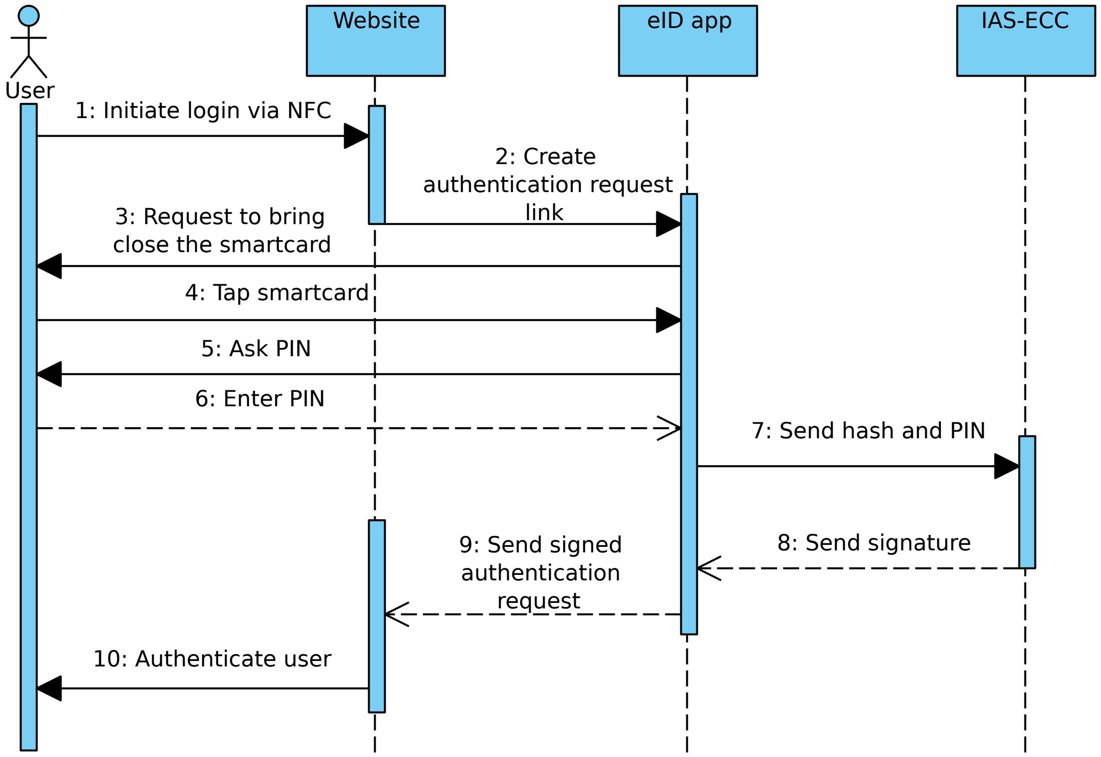

User
Website
eID app
IAS-ECC
1: Initiate login via NFC
2: Create authentication request link
3: Request to bring close the smartcard
4: Tap smartcard
5: Ask PIN
6: Enter PIN
7: Send hash and PIN
8: Send signature
9: Send signed authentication request
10: Authenticate user

Figure 4: Authentication over NFC

2. The website creates an authentication request and invokes the eID app with the authentication request.
3. The eID app asks the user to bring the smartcard close to the phone.
4. The user taps the smartcard on the smartphone.
5. The eID app asks the user to enter PIN1.
6. The user enters PIN1 in the eID app on their phone.
7. The eID app creates a PACE tunnel with the smartcard and sends the hash to be signed and PIN1 to the IAS-ECC applet.
8. The IAS-ECC applet creates the signature and sends it back to the eID app.
9. The eID app sends the signed authentication request back to the website.
10. The website creates an authentication session with the user's browser.

3 Vulnerabilities

In this section, we discuss the vulnerabilities that can be exploited and the potential costs for the attackers.

When using the NFC interface with a mobile app, there are two main areas of concern:

1. Attacker, who is in the vicinity of the ID-card, could start attacking the card at any time, without the knowledge of or action from the card holder. This is in contrast with the current situation. Currently, attacking the ID-card requires physical possession of the card by the attacker or connecting the ID-card to a computer, which is controlled by the attacker.

2. Attacker, who remotely controls a malicious app installed on the user's phone, could present fake dialogs to the user and start communicating with the card on behalf of legitimate apps.

We will discuss these concerns and vulnerabilities in the following sections.

3.1 NFC Skimming

In the following sections, we present an overview of literature that reports on communication with RFID or NFC tags over longer distances than the standard $\approx$ 10 cm. Since NFC communication is relying on the same radio frequencies as the RFID ISO-14443 standard, we include both results.

3.1.1 Theoretical Model

A theoretical research paper from 2005 [24] uses NEDAP, which is a system model for RFID systems. NEDAP includes a C program to simulate the physical communication characteristics of RFID systems. The parameters of the RFID tag (card), reader and antenna are given as input to the model which then combines them with the effects of external noises and sources to simulate the reading ranges. In this research, the attacker is assumed to ignore any regulatory limitations. Researchers find that instead of official, $\approx$ 10 cm range, they can increase the range of the attacker to the RFID tag (or ID card with NFC interface) to $40 - 50$ cm using typical ISO-14443 type B parameters and the optimal antenna dimensions are 40x40 cm^2.

The leech in the following quote [24, p. 8] refers to the tag reader.

> Figure 5 shows the basic schema structure of a leech using an NFC device: wrap a magnetic coupling around the NFC device, using a looped wire. In transmission operations, the gain stage amplifies the outgoing transmitted signals to a high-power-signal. In receive operations the gain stage amplifies the weak received signals to the level required by NFC device and filters out-of-band noises. The gain stage is connected to an antenna with optimal size, which transmits and receives signals to/from the card.

The paper presents a table with estimated costs for different setup options (see figure 6) for various distances. However, in the next research paper we see that the range can be increased further in practical scenarios.

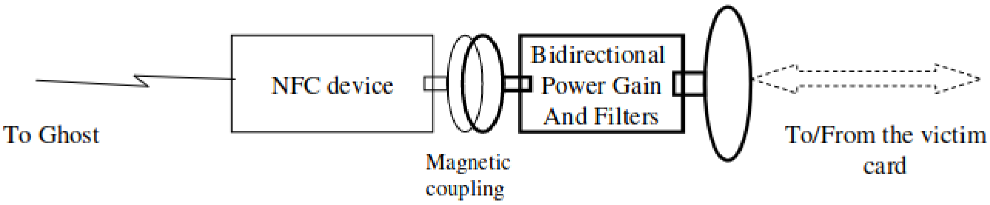


Figure 5: Theoretical model for a NFC leech (from [24])

Method	Property			
	Max Distance	Extra Cost (beyond NFC)	Availability	Attacker Knowledge
Standard	10 cm	0$	High	Low
Current + Antenna	40 cm	< 100$	High	Medium
Current + Antenna + Software	50 cm	< 100$	Medium	High
Current + Antenna + Signal-Processing	55 cm	> 5000$	Low	Very High

Figure 6: Estimated distance and attack costs for NFC skimming (from [24, p. 9])

3.1.2 Experimental Results

A paper from 2006 [25] picks up from where the first paper left off and the authors build a cheap RFID skimmer that can work from a distance of ≈25 cm range.

> ...[it] uses a lightweight 40cm-diameter copper-tube antenna, is powered by a 12V battery — and requires a budget of ≈ $100. We believe that, with some more effort, we can reach ranges of ≈ 35 cm, using the same skills, tools, and budget.

A paper from 2011 reports an activation distance of 27 cm:

> ...describe the implementation of an RFID receiver kit that could be constructed for less than £50, which can be used to observe RFID communication. Even though the self-build RF receiver did not achieve the same results as commercial equipment it does illustrate that eavesdropping is not beyond the means of the average attacker.

A paper from 2015 'describes a novel antenna design for communicating with ISO/IEC 14443A RFID cards at longer distances than the normal 5-10 cm.' The way they achieve this is by having 'two antennas, placed 100 cm apart, form an RFID gate that can communicate with cards in the middle of the gate. This is a substantial improvement of the maximum skimming distance of 25 cm reported in literature.' [12]

In the first experiments of the mentioned paper [12], 'Putting two amplifiers in cascade it was possible to power a 50 x 50 cm, transformer-matched, magnetic loop antenna with 60 W. This resulted in a successful skimming distance of approximately 40 cm' [12] but they found that this setup is not really stable as components heat over $120°C$ and the antenna and the reader break.

However, in later stages of their research in their main findings, they use higher harmonics and a square activation antenna in combination with a round receiving antenna to achieve a 100 cm gate that can be used to skim RFID tags. They point out that running a 100cm gate requires a large amount of power and using it successfully is not quite realistic, because the orientation of the tag easily changes the results. They also point out that tags that require high

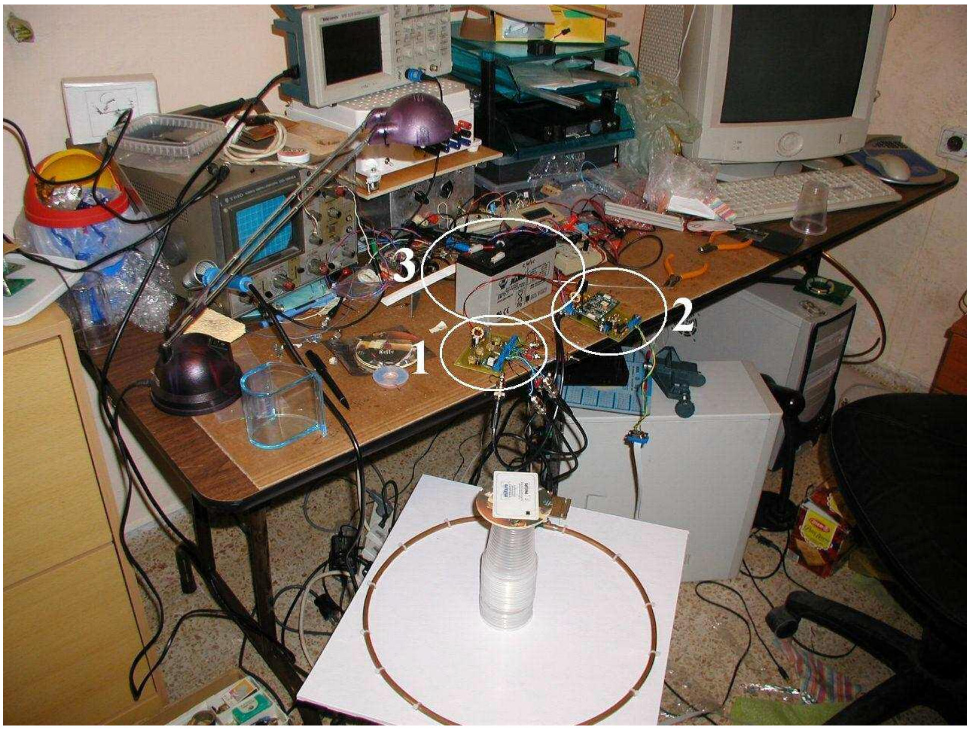


Figure 7: NFC antenna tuning process. Note the tag placed over a stack of plastic cups and beer coasters in the centre of the antenna. The power amplifier is marked as item 1, the reader base board is marked as item 2 and the battery is marked as item 3. [25, p. 11]

computing powers, such as the programmable Java Card they used for testing, might fail when their distance from the gates changes. In their tests with RSA, DES and AES computations, the card computations failed when they moved the card away from the activation antenna. Experimental RFID skimming gate and distance results can be seen in figures 8 and 9.

The authors conclude that in this paper no digital signal processing was done and with better filtering techniques and a different low-noise amplifier, longer distances can be achieved.

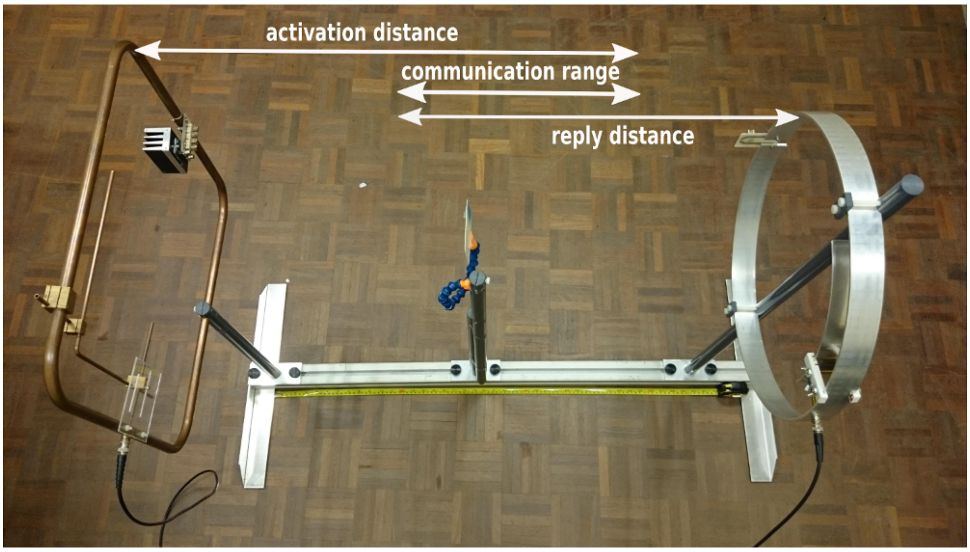
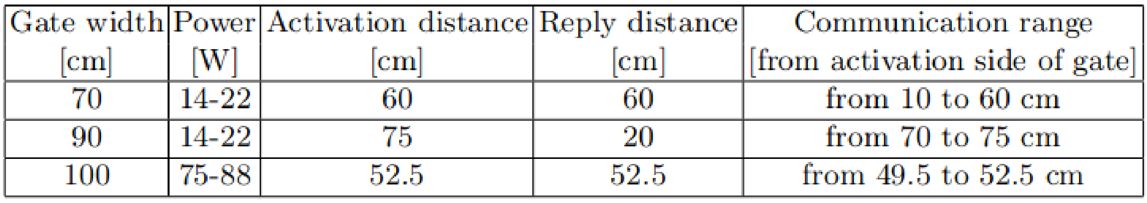


Figure 8: Picture of an experimental RFID skimming gate (from [12, p. 14])



Gate width [cm]	Power [W]	Activation distance [cm]	Reply distance [cm]	Communication range [from activation side of gate]
70	14-22	60	60	from 10 to 60 cm
90	14-22	75	20	from 70 to 75 cm
100	75-88	52.5	52.5	from 49.5 to 52.5 cm

Figure 9: Results for RFID skimming gate, where the communication range is measured from the side of the gate formed by the activation antenna, i.e. the left side of the gate in figure 8 (from [12, p. 14])

For the cost of this setup no information is given in the paper, but we could guess that the cost of such an attack is in the ballpark of 10 000 EUR.

3.1.3 Conclusion

Based on the sources, we believe that it is very feasible to build a 70 to 100 cm wide gate to skim NFC cards or RFID tags. We don't know however, if such attacks can perform full PACE handshake and private key operations from such distances.

3.2 Damaging NFC Cards Over Distance

One of our findings during this research was that it is also possible to permanently damage cards running on ID-Cosmo platform version 8.1. This happens when establishing a PACE protocol is attempted using the wrong MRZ or CAN number 10 times consecutively. This attack leaves the PACE protocol with a 15 second delay that won't disappear even if the right MRZ or CAN is given [29, p. 75]. This kind of attack could easily damage a large number of ID cards if deployed in an area with high traffic, such as between the aisles of shopping malls.

3.3 Communicating with Multiple NFC Cards

In this section we discuss the possibility of attackers targeting a single ID card among multiple ID cards. Since the Estonian ID card contactless interface uses ISO/IEC 14443 Type A, and the ISO/IEC 14443-3 [23] describes anti-collision methods to be used with these cards, the readers and cards support anti-collision and the reader can choose which card to interact with.

For more information and examples see ISO/IEC 14443-3 [23] and 'Smart Card Handbook' by Rankl and Effing [41, p. 304].

3.4 ID-card Public Identifiers over NFC

In this section we perform a literature review of identifying RFID tags. Focusing on cards operating under ISO/IEC 14443 Type A. This would be a case of an attacker with a clandestine reader, possibly tracking people. A theoretical attack would be that the attacker could activate a card, generate an identifier for this card and store it in a database. After building a database of identifiers the attacker could use it to identify the same card if they come across it again.

3.4.1 Physical-layer Device Identification

In [47] the authors can identify 20 different cards from 4 different manufacturers, 5 cards from each manufacturer of the same batch. Their calculations and results require millimetre precision and we find that it is unfeasible in actuality.

In [5], 50 RFID cards are identified, with a low error rate of 2.43%. However, their results also require a controlled environment. In this controlled environment they can generate identifiers of 120 bytes for cards in around 2 seconds.

In [46], 20 RFID cards are identified by their manufacturers by using the electromagnetic measurements on the reader end as each card effects the electromagnetic signal. They use an oscilloscope connected to the test setup and a commercially available testing fixture designed for ISO 10373-6. Their results also require precise placement and we find it unfeasible to carry out practically.

In [27], the authors identify 50 ISO/IEC 14443A RFID cards by training a deep learning model and then using the model to identify the cards. Their data collection times are quite long (18 minutes) for each tag and their setup also requires precise card placement.

3.4.2 Logical-layer Device Identification

A related attack is logical-layer device identification.

In [2], the authors first record a successful encrypted communication between the e-passport and the reader. Then they can, without breaking the encryption, replay the messages to older versions of French e-passports.[1] Using the replies from the e-passport chip and the timing of these replies, they can track a specific e-passport among many. In [13], the authors claim eavesdropping distances of 2 to 3 meters with different setups. If these results can also be achieved in more difficult conditions (airports, supermarkets etc.) we believe that the communication with an authorised reader can be captured.

We have verified that the latest generation of Estonian temporary residence permit cards are not vulnerable to this kind of attack. Whether it is a wrong APDU or a replayed APDU, the ID cards return the same error: `[0x63 0x00]`. We have not tested the timings for the different results, but they might give a clue about the identity of the card.

In [45], the authors can distinguish e-passports of ten different countries by sending valid and invalid commands. Since some of the e-passports return different answers for invalid commands, it is possible to distinguish them. This might be applicable to ID cards of different generations if the application within them is updated or changed.

In [10], the authors illustrate an attack that 'identify the e-passport that has most recently interacted with a specific reader device (which need not be under adversary control). For example, in an airport, the attacker may wish to identify people who have travelled through the priority lane, as they are more likely to be airline staff or other people of interest.' [10]. For their attack to work, OCR process has to be done by an honest reader, so this attack only works after BAC has been attempted by an honest reader.

3.4.3 Conclusion

Literature research and our tests with residence permit cards show that on the logical-layer, there's no publicly readable identifier for Estonian ID cards. However, a synthesised identifier could be deduced from the timing information or other properties of physical-layer communication. In controlled environments, different cards from the same manufacturer and of same batches can be identified. The research results we have discussed show that even though these identifiers can be found, in real life they might be very difficult/unfeasible to exploit.

[1] Older version of French passports send a different error message depending on which part of BAC the process fails. That's why it's more trivial to track these passports.

One more important thing to note is that all the studies we have mentioned use a very limited number of tags (e.g. 20, 50, 200) and we think that scaling this to millions might prove unfeasible. However, novel or improved techniques might allow the exploitation of analog differences in the ID card communications that stem from the manufacturing processes and that could successfully identify ID cards even in real life and in large numbers.

3.5 Vulnerabilities of Mobile Platforms

The nature of mobile platforms brings along some additional concerns such as the ones described in the sections below.

3.5.1 Trojan Apps Controlled by an Attacker

Trojan apps are mobile apps, which perform their advertised function and don't try to appear as other trusted apps. For example, after the user has installed a tic-tac-toe game from the app store, the app displays its own icon, name and the game design UI. It looks like a proper game app. However, even if the app is fulfilling all its advertised functions, users don't have any way of making sure that the app is not doing something extra in the background.

Android phones have a system of app privileges. In order to use NFC communications, apps have to request a permission `android.permission.NFC`[2] and during installation Android operating systems will ask if the user grants this permission. In practice, we doubt that many users understand what this privilege actually means and whether they should grant it or not. Therefore, we can assume that some attacker provided apps on a user's device can communicate with the smartcard as well.

Even when this app doesn't try to trick the user into revealing the CAN number or PIN numbers, it can still simply try out a few CAN and PIN numbers when it discovers that a smartcard is near the phone. When the app is popular and installed on the phones of a wide user base, it can try this with many users. In case the correct CAN number and correct PIN number are found by this kind of distributed brute-force-attack, the app could signal back to the attacker that he has found an available smartcard, along with the X.509 certificate. The Attacker can then send back a hash to be signed from the attacker's authentication session or corresponding to some digital document and the trojan app will return the unauthorised signature.

CAN numbers have 6 digits, which means that with 14 tries (which doesn't impose the 3-second delay yet) the attacker finds the correct CAN with probability $14 \cdot \frac{1}{1000000} = 0.000014$. With 100 000 users and perhaps one user in ten having the smartcard next to the phone (i.e. with 10 000 tries), the attacker can discover around 0.14 smartcards with associated CAN numbers. Maybe more if the attack is continued for a longer period of time.

Let's assume that the attacker already has access to the user's smartcard. The attacker now also has to guess the correct PIN1. With PINs, attacker only has 2 tries before the IAS-ECC applet locks up and therefore, the probability of success could olny be around 0.002. We estimate it to be a bit higher, because the user could have changed the randomly generated PIN into something more convenient and thusly the distribution of PIN numbers is no longer uniform.

Therefore, with installed user population of 100 000 users, we estimate that the attacker is able to get access to at least one smartcard's authentication function with a probability of ≈ 0.0003 and to at least one smartcard's signing function with a probability of around ≈ 0.00003. Developing and distributing such kind of trojan app would cost around 1 000 – 10 000 EUR.

We haven't verified, if such NFC communication attempts are completely invisible to the user. Extra dialogs by operating systems will diminish the success probability. Also, mobile

[2] `https://developer.android.com/guide/topics/connectivity/nfc/nfc#manifest`

platforms perform security analysis and scanning of the apps that are uploaded to the app store. This could hopefully detect such programmed code and the trojan app would be rejected.

3.5.2 Fake Apps Controlled by An Attacker

The next level of trojan apps is the kind that try to trick the user into entering the CAN number and PIN numbers. Sometimes they randomly present authentic-looking dialogs which confuse the user; sometimes they try to hook into the user's flow between the DigiDoc and eID apps; sometimes they claim that they offer some useful smartcard related service to the user. In some instances attackers combine such apps with phishing phone calls and they actively instruct and guide the user to download and run the app controlled by attackers on their mobile phone. It is not impossible that they could convince the user to tap the smartcard on the phone as well, etc.

It is much more difficult to estimate the success probability of such kind of attacks, because all possible variants of tricks is not known. However, the success probability of this combined approach is surely higher than just random trying as described in the previous section.

We estimate that this kind of a phishing campaign, targeting around 10 000 users, could lead to the attacker getting access to at least 10 – 100 users' smartcards. Keeping such a campaign a secret is probably impossible and it will attract the attention of law enforcement officials pretty soon. However, some damage could already be done by that time.

4 Risk Analysis

4.1 Methodology

We use Microsoft STRIDE [48] and NIST SP800-30 [11] for the risk analysis in this report.

The Microsoft STRIDE method is a part of a systematic approach in threat modelling developed by the Security, Engineering and Communications groups at Microsoft. To ensure the security of the system in our scope, it must have the following properties: Confidentiality, Integrity, Availability, Authentication, Authorization, Non-repudiation. Threat modelling and STRIDE are used to challenge these security properties with the corresponding threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.

We break down the system in our scope into its components; data objects and flows between them; analyse them for susceptibility to threats; evaluate the risks, describe the attacks and the attacker's goals. We propose a list of system requirements as risk mitigation tools presented in section 5.

The components of the system in our scope are presented in figure 1. Such components as the chip, IAS ECC applet, and ID-One Cosmo v8.2 platform are Common Criteria (CC) certified. CC certification provides assurance that a computer security product has gone through a rigorous evaluation and testing process which resulted in confirming the product's compliance with the claims and meeting the security functional requirements.

We study and analyse the Security Target documents of the CC certified components within our system scope to obtain relevant information about applicable threats and risks. The risk analysis of the system in scope includes those threats and risks, plus security measures which are directly related to the components, data objects, data flows, and communication channels between the components.

Combining STRIDE and CC materials allows simplifying the identification of threats. The threats addressed in the Security Target of the CC certified components are sorted to relate to the corresponding group of STRIDE.

4.2 Identified and Evaluated Risks

The risks are given in the table 1 on page 25.

Each risk derives from the data objects and flows that are involved in the process of signing or authentication within the defined scope.

Each column contains the following record:

- The identifier of the risk.
- The type of threat according to STRIDE threat modelling approach.
- Threat description, i.e., what the attacker does to the data object or flow. The source of vulnerability that is potentially the cause of the attack is also indicated here.
- Scenario that describes the chain of actions and circumstances that facilitate the risk and attack to occur.
- Possibility (applicability) of the attack to occur when signing or authenticating via USB.

In order to evaluate the identified risks, we use the "Guide for Conducting Risk Assessments" by NIST (National Institute of Standards and Technology) [11]. Specifically, we implement the assessment scale for evaluating the impact of the attack events (see sections 4.2.1, 4.2.2, 4.2.3). The guidelines are developed to be universal and focus mostly on higher organisational levels when describing subjects, their functioning and interaction between each other. We have adjusted the assessment scale to our system scope and its domain. The evaluated risks are presented in table 2 on page 32.

The risk assessment is conducted on the information system level according to NIST guidelines [11]. The identified threats are targeted at one user at a time due to the NFC technology being used as a communication protocol in a smartcard. We adapt the NIST guidelines regarding the determination of likelihood to fit our scope.

4.2.1 Determining Launch Probability

When assessing launch probability of an attack, a score is given based on the available evidence, experience, and our expert judgement.

We assess the launch probability and how likely it is that the attack will be initiated.

We apply a qualitative assessment using a range of 5 levels:

"Very high" – The attacker is almost certain to launch the attack. The vulnerability is very easy to exploit. The attacker requires only a short amount of time for preparation and reasonable technical capabilities to launch the attack. The likelihood of favourable conditions required to launch the attack manifesting and the attacker using this opportunity is very high.

"High" – The attacker is highly likely to launch the attack. The vulnerability is easy to exploit. The attacker requires short time for preparation and average technical capabilities to launch the attack. The likelihood of favourable conditions required to launch the attack manifesting and the attacker using this opportunity is high.

"Moderate" – The attacker is somewhat likely to launch the attack. The vulnerability is moderately likely to be exploited. The attack requires a relatively short time for preparation and substantial technical capabilities. The likelihood of favourable conditions required to launch the attack manifesting and the attacker using this opportunity is moderate.

"Low" – The attacker is unlikely to launch the attack. The vulnerability is complex and is unlikely to be exploited. The attack requires a substantial amount of time for preparation and strong technical capabilities. The likelihood of favourable conditions required to launch the attack manifesting and the attacker using this opportunity is low.

"Very low" – The attacker is highly unlikely to launch the attack. The attack requires a deterring amount of time for preparation and vast technical capabilities to exploit the vulnerability. The likelihood of circumstances and favourable conditions for the attack aligning is very low.

4.2.2 Damage Probability Assessment

We assess the damage probability or how likely the attack will result in an adverse impact, regardless of the damage scale that can be expected.

We apply a qualitative assessment using a range of 5 levels:

"Very high"' – Catastrophic damage. The attacker is able to impersonate any and all Estonian PKI users at will without any other prerequisites. Comparable threat event examples could be the compromise of the issuing CA key pair or catastrophic breakdown of the cryptographic algorithms, so that after the attack, attacker can easily create a private key out of the public key, without significant additional resources.

"High" – Severe damage. The attacker is able to impersonate many and multiple Estonian PKI subscribers. The attacker would need to target each user individually, but once the attack succeeds, it is possible to use the subscriber's key pair freely, multiple times. The attacker is able to target multiple users at the same.

"Moderate" – Serious damage. The attacker is able to create single fraudulent authentication or single fake digital signature on behalf of the user, without the user's consent. The attacker would need to target each user individually and practical considerations limit the number of impacted users to perhaps 10 or 1000 or 10 000.

“Low” – Limited damage. All digital identities are still safe, but perhaps the authentication or signing function doesn’t work for some time for the user. The user needs to replace the physical smart-card because of physical damages. The software might not function and needs to be updated. The certificates might need to be suspended or revoked.

“Very low” – Negligible damage. All key pairs are safe, all knowledge authentication factors (PIN) are safe and every user is able to continue the business as usual, without concerns.

4.2.3 Damage Scale Assessment

We apply a semi-qualitative assessment using a range of 5 levels:

“Very high” – 10000 or more ID card users affected;
“High” – 1000 to 10000 ID card users affected;
“Moderate” – 100 to 1000 ID card users affected;
“Low” – 10 to 100 ID card users affected;
“Very low” – 1 to 10 ID card user(s) affected.

The majority of identified risks are left out of consideration in the following analysis since they are assessed as “Very low” or “Low”, and/or the source of vulnerability is covered by CC certification, and/or identical attack can occur in the USB mode.

The impact levels “Very low” and “Low” mean that the critical data objects such as key pairs and PIN(s) remain safe and digital identity theft cannot be committed. The number of affected users is relatively low – up to 1000. If the attack succeeds, the users must perform routine procedural actions in order to remove or fix the damage caused by the attack.

If the risk/threat is identical to one which can occur in the USB mode, it is disregarded. Only those attacks which have a success probability higher if launched in NFC mode, require further consideration.

If the impact (or damage scale) of the threat is assessed as ”Very low”, we neglect the probability of this threat causing damage due to its insignificance.

4.3 Attacker’s Goals

This section gives an overview of the attacker’s potential goals, which we consider in the following analysis.

4.3.1 GOAL-FAKE-SIG

The attacker’s goal is to sign a document on behalf of the user. In order to achieve this goal successfully, the attacker can do the following:

- have physical access to the smartcard and/or know the CAN and PIN;
- trick the user into installing a malicious eID or DigiDoc app;
- slip the user a fake ID card;
- perform a skimming attack when the user is nearby.

If the attacker has the user’s smartcard, they therefore have the access to the CAN number. If the PIN is not known, the attacker may guess it. However, the likelihood of a correct guess is very low. If the attacker has the smartcard and knows the PIN, they can give signatures on behalf of the user unlimited number of times. The alternative variant of this goal is authentication, which requires the same actions but a different PIN.

If the user installs a malicious app, the attacker might obtain various data including the CAN, PIN, hashes, signature, etc. Depending on the knowledge and the resources the attacker has, this data can be further used to give a signature of behalf of the user.

If the attacker posesses a fake ID card, then it is possible that they would swap it with the user's original one. The user will use the fake when signing a document and once the attacker swaps the cards back they can read the fake ID card and obtain the PIN.

If the attacker skims the user's smartcard trying different CAN and PIN combinations - at a certain scale after a certain amount of times, the attacker may succeed.

4.3.2 GOAL-PRIVACY-LEAK

The attacker's goal is to obtain personal and possibly sensitive data which can further be stored, copied and published. In order to achieve this goal successfully, the attacker can do the following:

- have physical access to the smartcard and/or know the CAN;
- trick the user into installing a malicious eID or DigiDoc app;
- eavesdrop on user's transactions using an antenna.

If the attacker simply sees the CAN on the user's smartcard, they may further disseminate this data.

If the attacker has physical access to the user's smartcard, they may further read the data off the eMRTD applet and further disseminate this data.

If the attacker has physical access to the user's smartcard and they know the PIN, they can exploit this data to authenticate and obtain access to the user's personal information online.

If the user installs a malicious app, the attacker may obtain various data including the CAN, PIN, hashes, signature, etc. Depending on the knowledge and the resources the attacker has, this data can be further used to disseminate personal data.

If the attacker uses antennae, they can eavesdrop on the data transmitted during the transaction and obtain personal data.

4.3.3 GOAL-DOS

The attacker's goal is to damage either permanently or temporarily the smartcard contactless interface functionalities or target the app(s). In order to achieve this goal, the attacker can do the following:

- trick the user into installing a malicious eID or DigiDoc app;
- damage the smartcard.

If the user installs a malicious app, the attacker can halt the app functioning and/or damage the documents and hashes.

If the attacker wants to damage the smartcard, he can simply break it, burn the circuits inside the card using powerful antennae, or lastly, block the card by entering wrong PINs or perform brute-force attacks [29, 26].

4.4 Attack Descriptions

This section describes in details the assumed steps attacker may take in order to reach the attack goal by taking advantage of the risks we have identified.

Table 1: Risk descriptions

ID	Threat type	Threat	Scenario	Countered by ST?
CAN-TAMP-1	Tampering	Attacker hacks the eID app and modifies the stored CAN so the user cannot use the card over NFC. Source: eID app.	The attacker gets access to the eID app of the user where the user is storing the CAN, the attacker can modify the CAN, so once the user wants to use the card for sign/auth over NFC, he cannot do it. The user needs to enter CAN again.	No
CAN-INFO-1	Information Disclosure	Attacker sees or knows the CAN, he can get access to the smartcard. Source: Physical ID card.	The attacker has temporary access to the card of the user and reads the card with an NFC reader. The card is read, the secure channel is established, but the card provides only the public file that does not contain sensitive data such as private keys and PIN.	No
CAN-INFO-2	Information Disclosure	Attacker hacks the eID app and copies the CAN. Source: eID app.	The attacker gets access to the eID app of the user where the user is storing the CAN, the attacker can obtain the CAN.	No
CAN-DENIAL-1	Denial of Service	CAN number on card is modified or not readable, the smartcard cannot be accessed over NFC. Source: Physical ID card.	The attacker has temporary access to the smartcard of the user and visually destroys or covers the CAN appearance on the surface of the card, once the user wants to use the card for sign/auth over NFC, he cannot do it. Eventually, the card needs to be replaced.	No
CAN-DENIAL-2	Denial of Service	Attacker hacks the eID app and deletes the CAN so the user cannot use the card over NFC. Source: eID app.	The attacker gets access to the eID app of the user where the user is storing the CAN, the attacker can delete the CAN, so once the user wants to use the card for sign/auth over NFC, he cannot do it. The user needs to enter CAN again.	No

Risk descriptions

ID	Threat type	Threat	Scenario	Countered by ST?
PIN-SPOOF-1	Spoofing	Attacker impersonates the eID app the user installs on their device, the PIN can be disclosed. Source: Third-party application.	The attacker develops a fake application that impersonates the eID app. The user is tricked into installing the fake eID app. During the process of sign/auth the fake eID intercepts the PIN that the user entered. The attacker obtains the PIN and can further use it via hacked eID app.	No
PIN-SPOOF-2	Spoofing	Attacker impersonates the IAS ECC applet and installs it on the user's card, the PIN can be disclosed. Source: Third-party applet.	The attacker develops a fake applet that impersonates the IAS ECC applet. The user is tricked into installing the fake applet onto their smart-card. During the process of sign/auth the fake applet pretends to sign/auth and intercepts the PIN(s).	Yes
PIN-SPOOF-3	Spoofing	User uses a fake smart-card, the attacker can find out the PIN. Source: Physical smart-card.	The attacker forges the user's smart-card and replaces it. During the process of sign/auth the user enters the PIN while it is recorded into the fake card's memory. The attacker then can obtain the PIN and can further use and leak it.	Yes
PIN-TAMP-1	Tampering	Attacker modifies the eID app, the PIN code can be disclosed. Source: Third-party application.	The attacker modifies the eID app by tricking the user into installing a malicious patch or an update. During the process of sign/auth the malicious eID app intercepts the PIN that the user entered. The attacker obtains the PIN and can further use and leak it.	No
PIN-TAMP-2	Tampering	Attacker modifies the IAS ECC applet, the PIN can be disclosed. Source: Third-party application.	The attacker modifies the IAS ECC applet by tricking the user into installing a malicious patch or an update. During the process of sign/auth the malicious IAS ECC applet intercepts the PIN that the user entered. The attacker obtains the PIN and can further use and leak it.	Yes

Risk descriptions

ID	Threat type	Threat	Scenario	Countered by ST?
PIN-TAMP-3	Tampering	Attacker modifies the javacard platform, the PIN can be disclosed. Source: Third-party application.	The attacker tricks the user into installing a malicious patch or an update for the smart-card's operational platform. During the process of sign/auth the malicious card platform modifies the functioning of the platform's firewall and eventually intercepts the PIN that the user entered. The attacker obtains the PIN and can further use and leak it.	Yes
PIN-REPU-1	Repudiation	Attacker finds out the PIN and has access to the user's card. He can sign documents and perform transactions the user did not intend to do.	The attacker finds out the PIN(s) of the user. The attacker obtains the user's smartcard and can start using it on behalf of the user by signing documents and performing transactions that the user did not intend to do.	No
PIN-INFO-1	Information Disclosure	Attacker finds out the PIN and can disclose it to others.	The attacker finds out the PIN(s) of the user. The attacker leaks the PIN(s) online and/or offline which can lead to further attacks.	No
PIN-DENIAL-1	Denial of Service	A wrong PIN code is entered 3 timesand the card is blocked.	The user wants to sign/auth via NFC and enters a wrong PIN code 3 times. The card is blocked, the user cannot use it.	No
HASH-SPOOF-1	Spoofing	A fake version of DigiDoc deliberately creates a corrupted hash for the document the user intends to sign. Source: DigiDoc.	The attacker tricks the user into installing a fake DigiDoc app. The app is programmed to create wrong hashes for the documents that the user wants to sign. As a result the user ends up signing potentially repudiated content.	Env
HASH-TAMP-1	Tampering	A malicious eID app alters the hash of the document to be signed. Source: eID app.	A fake or malicious eID app developed by the attacker corrupts the hash created for the document to be signed. The user then signs content different to the one they intended to.	Env

Risk descriptions

ID	Threat type	Threat	Scenario	Countered by ST?
HASH-REPU-1	Repudiation	A malicious eID app creates an altered hash of the document or transaction different to the one that the user intends to sign. Source: eID app.	The attacker hacks the eID app on the user's device or tricks him into installing a fake eID app or a malicious patch or update for the eID app. The malicious eID app creates a hash that does not correspond to the content of the document or transaction that the user intends to sign.	Env
HASH-REPU-2	Repudiation	A hash is created for the document or transaction that has been corrupted by a malicious eID app. Source: eID app.	A fake or malicious eID app developed by the attacker corrupts the document to be signed. Hence, a hash is created for a document different from the one that the user intends to sign.	Env
HASH-INFO-1	Information Disclosure	A malicious eID app leaks the hash of the document or transaction to be signed. Source: eID app.	A fake or malicious eID app developed by the attacker created the hash for the document to be signed and leaks it (also possible to leak together with the document to be signed itself).	Env
HASH-INFO-2	Information Disclosure	A fake or malicious eID app leaks the received DigiDoc hash of the document to be signed. Source: eID app.	The user has installed a fake or malicious eID app developed or hacked by the attacker on their device. It receives the hash from DigiDoc from PC and then leaks it.	Env
HASH-DENIAL-1	Denial of Service	A malicious eID app does not produce a correct format of hash. Source: eID app.	A fake or malicious eID app developed by the attacker is programmed to produce a hash in a format different to the required one. Once the user puts the card close to the NFC reader of their device, unknown errors occurs. As a result, the signature cannot be added.	Env
HASH-DENIAL-2	Denial of Service	A malicious eID app does not produce a hash. Source: eID app.	A fake or malicious eID app developed by the attacker is programmed to not produce a hash for the document or transaction or remains unresponsive. The user cannot sign/auth.	Env

Risk descriptions

ID	Threat type	Threat	Scenario	Countered by ST?
HASH-PRIV-1	Elevation of Privilege	An eID app enables permissions for access to it without user's knowledge or consent. Source: eID app.	A fake or malicious eID app developed or hacked by the attacker introduces or modifies permissions of the application to access it by third-party apps and/or send and/or receive data without the user's knowledge or consent.	Env
SIG-SPOOF-1	Spoofing	A malicious eID app receives the signature from IAS ECC applet and replaces the signed file with a damaged or corrupted file. Source: eID app.	A fake or malicious eID app developed or hacked by the attacker receives the correct signature from the smartcard. The eID app replaces the signature with an incorrect signature and sends this to the signature creation application (DigiDoc). The resulting digital signature container will be invalid and the attacker has prevented the user from successfully creating a valid digital signature.	Env
SIG-SPOOF-2	Spoofing	A malicious DigiDoc app receives the signature from IAS ECC applet and replaces the signed file with a damaged or corrupted file. Source: DigiDoc.	A fake or malicious eID app developed or hacked by the attacker receives the correct signature from the smart-card. The eID app replaces the signature with an incorrect signature and sends it to the signature creation application (DigiDoc). The resulting digital signature container will be invalid and the attacker has prevented the user from successfully creating a valid digital signature.	Env

Risk descriptions

ID	Threat type	Threat	Scenario	Countered by ST?
SIG-TAMP-1	Tampering	A malicious eID app receives the signature from IAS ECC and damages the signed file. Source: eID app.	A fake or malicious eID app developed or hacked by the attacker receives the correct signature from the smart-card. The eID app replaces the signature with an incorrect signature and sends this to the signature creation application (DigiDoc). The resulting digital signature container will be invalid and the attacker has prevented the user from successfully creating a valid digital signature.	Env
SIG-REPU-1	Repudiation	A malicious eID receives the signature from IAS ECC applet and alters it. Source: eID app.	A fake or malicious eID app developed or hacked by the attacker receives the correct signature from the smartcard. The eID app changes the signature and sends this to the signature creation application (DigiDoc). The resulting digital signature container will be invalid and attacker has prevented the user from successfully creating a valid digital signature.	Env
SIG-INFO-1	Information Disclosure	A malicious eID app receives the signature and leaks and/or copies the data. Source: eID app.	A fake or malicious eID app developed or hacked by the attacker receives the signature from the smartcard and leaks it to third parties.	Env
SIG-DENIAL-1	Denial of Service	A malicious eID app receives the signature from IAS ECC applet and replaces the signed file with a damaged or corrupted file. Source: eID app.	A fake or malicious eID app developed or hacked by the attacker receives the correct signature from the smartcard. The resulting digital signature container will be invalid and the attacker has prevented the user from successfully creating a valid digital signature.	Env
SIG-DENIAL-2	Denial of Service	A malicious eID app receives the signature from IAS ECC applet and deletes the signed file. Source: eID app.	A fake or malicious eID app developed or hacked by the attacker receives the signature from the smartcard. As a result the user is not able to create a signature and sign the intended document.	Env

Risk descriptions

ID	Threat type	Threat	Scenario	Countered by ST?
WIRELESS-REPU-1	Repudiation	The attacker can eavesdrop on the wireless connection using an antenna and can sign documents and perform transactions using the CAN and PIN. Source: NFC.	The attacker is able to see the CAN. Being in close proximity to the user, the attacker uses an antenna to connect to the user's smartcard using the CAN number. The attacker knows the PIN and can sign and/or authenticate on behalf of the user.	No
WIRELESS-INFO-1	Information Disclosure	The attacker can eavesdrop on the wireless connection using an antenna. Source: NFC.	The attacker uses an antenna to eavesdrop and intercept the data transmitted through wireless communication.	No
WIRELESS-INFO-2	Information Disclosure	The attacker can eavesdrop on the wireless connection using an antenna and gets access to the data using the CAN. Source: NFC.	The attacker is able to see the CAN. Being in close proximity to the user, the attacker uses an antenna to connect to the user's smartcard using the CAN number and read the data file with PII.	No

Table 2: Risk evaluation table

ID	Launch probability	Damage probability	Damage scale	Same risk for PC/USB

CAN number

CAN-TAMP-1	Very low	Very low	Very low	No
CAN-INFO-1	Very low	Very low	Very low	No
CAN-INFO-2	Very low	Low	Very low	No
CAN-DENIAL-1	Very low	Very low	Low	No
CAN-DENIAL-2	Very low	Very low	Very low	No

PIN code

PIN-SPOOF-1	Very low	Low	Moderate	Yes
PIN-TAMP-1	Very low	Moderate	Moderate	Lower than PC
PIN-REPU-1	Moderate	High	Moderate	Yes
PIN-INFO-1	Low	Moderate	Moderate	Yes
PIN-DENIAL-1	Low	Low	Low	Yes

Hash of the document to be signed

HASH-SPOOF-1	Very low	Moderate	Low	Yes
HASH-TAMP-1	Very low	Low	Low	Yes
HASH-REPU-1	Very low	Moderate	Moderate	Yes
HASH-REPU-2	Low	Moderate	Moderate	Yes
HASH-INFO-1	Low	Moderate	Moderate	Yes
HASH-INFO-2	Low	Low	Low	Yes
HASH-DENIAL-1	Low	Low	Low	Yes
HASH-DENIAL-2	Low	Low	Low	Yes
HASH-PRIV-1	Very low	Moderate	Low	Yes

Signature

SIG-SPOOF-1	Very low	Very low	Very low	Yes
SIG-SPOOF-2	Very low	Very low	Very low	Yes

ID	Launch probability	Damage probability	Damage scale	Same risk for PC/USB
SIG-TAMP-1	Very low	Very low	Very low	Yes
SIG-REPU-1	Very low	Very low	Very low	Yes
SIG-INFO-1	Very low	Very low	Low	Yes
SIG-DENIAL-1	Very low	Very low	Very low	Yes
SIG-DENIAL-2	Very low	Very low	Very low	Yes

Wireless connection

WIRELESS-REPU-1	Low	Low	Low	No
WIRELESS-INFO-1	Low	Low	Low	No
WIRELESS-INFO-2	Very low	Low	Low	No

4.4.1 PIN-SPOOF-1

Attack goal: GOAL-FAKE-SIG. An attacker tries to create one or more fake signatures on behalf of the user who has not given their consent.

Attack assumptions:

1. The attacker can trick the user into installing attacker-controlled apps on the user's mobile phone.
2. The attacker-controlled app appears to function as a legitimate official app.
3. The attacker-controlled app is capable of recording and storing data (CAN, PIN, hashes, files and signed documents) entered by the user. Related threats: CAN-INFO-1, CAN-INFO-2, PIN-INFO-1, HASH-INFO-2, SIG-INFO-1.
4. The attacker can continue receiving leaked data. Related threats: CAN-INFO-1, CAN-INFO-2, HASH-INFO-2, SIG-INFO-1, WIRELESS-TAMP-1, WIRELESS-INFO-3.
5. The attacker can continue signing documents on behalf of the user when the attacker and the user are in sufficient proximity for a skimming attack. Related threats: WIRELESS-REPU-2.
6. The attacker can perform other attacks to achieve GOAL-PRIVACY-LEAK, GOAL-DOS.

Attack steps:

1. The user confuses the attacker's app with the eID App.
2. The user starts the signing process from the attacker-controlled app.
3. The user enters the CAN and PIN into the attacker-controlled app.
4. The Attacker's app records and stores the entered CAN and PIN. Related threats: CAN-INFO-1, CAN-INFO-2.
5. The Attacker's app sends the hash to be signed and PIN to the ID-card.
6. The ID-card signs the hash and returns the signature.

4.4.2 PIN-SPOOF-3

Attack goal: GOAL-FAKE-SIG. An attacker tries to create one or more fake signatures on behalf of the user who has not given their consent.

Attack assumptions:

1. The fake smartcard needs to be perceived as a genuine smartcard by the user.
2. The fake smartcard must have capabilities to record and store the entered PIN. Related threats: PIN-REPU-1.
3. The fake smartcard may be recognised by the signature creation application and produce signatures in order to be perceived as a genuine smartcard.
4. The attacker must be able to slip in as well as take back the fake smartcard from the user in order to obtain the PIN.

5. The attacker can use the obtained PIN to sign documents on the user's behalf when the user is in sufficient proximity for a skimming attack. Related threats: WIRELESS-REPU-1.
6. The attacker can leak the obtained PIN and hence perform other attacks to achieve GOAL-PRIVACY-LEAK, GOAL-DOS.

Attack steps:

1. The attacker slips in the fake smartcard to the user.
2. The user confuses the fake smartcard with the genuine smartcard.
3. The user starts the signing process with the fake smartcard.
4. The user enters the PIN which is recorded into the smartcard's memory.
5. The attacker gets the fake smartcard with the recorded PIN back.

4.4.3 WIRELESS-REPU-1 or Skimming

Attack goal: GOAL-FAKE-SIG. The attacker tries to create one or more fake signatures by using antennae on behalf of the user who has not given their consent.

Attack assumptions:

1. The attacker assembles an antenna(e) which is capable of activating the smartcard and reading the answer.
2. The attacker knows or guesses the CAN and can establish a connection with the smartcard. Related threats: CAN-INFO-1.
3. The attacker knows or guesses the PIN. Related threats: PIN-REPU-1.
4. The attacker can repeat the attack.
5. The attacker can perform other attacks to achieve GOAL-PRIVACY-LEAK, GOAL-DOS.
6. The attacker can eavesdrop. Related threats: WIRELESS-TAMP-1.

Attack steps:

1. The user is located in the proximity of the attacker's antenna(e).
2. The antenna(e) activates the smartcard.
3. The attacker enters the CAN and PIN.
4. The smartcard returns the signed transaction/document to the attacker without the user's knowledge.

4.5 Conclusion

This section identified risks in table 1 on page 25 and evaluated them in table 2 on page 32. In case damage of the realisation of a risk was estimated as 'very low' or 'low', other characteristics of a risk were not evaluated.

Only the following risks' damage scale were estimated as 'moderate':

1. PIN-SPOOF-1
2. PIN-TAMP-1
3. PIN-REPU-1
4. PIN-INFO-1
5. HASH-REPU-1
6. HASH-REPU-2
7. HASH-INFO-1

This is mostly because we see that there is a possibility for an attacker to spoof the eID or DigiDoc application and then trick the user into entering PIN-codes into the attacker controlled app. However, we must also point out that the same threats and attacks are possible on the PC platform where the user is using a regular smartcard reader and a USB interface.

Therefore, we have not identified any such risks, which are unique to the situation when the ID-card is used via NFC interface and which are on 'moderate' or higher damage scale.

After applying the list of recommended security measures (see chapter 5 on the facing page), we could conclude that the risk level of using an ID-card via NFC interface is not significantly higher than using an ID-card via USB interface.

5 System Requirements

This chapter describes the security requirements (or 'security profile'), which should be taken into account, when amending the current ecosystem of Estonian eID components and enabling the usage of the NFC interface for the ID-card.

Security requirements are essentially a kind of security measure which is needed in order to mitigate some specific threats identified in the chapter 4 on page 21.

They use either 'must', to indicate that this recommendation should be mandatory to follow or 'should', to indicate that this recommendation is for RIA's future consideration.

5.1 Security Requirements for eID App

- Req-App-1: eID App must use secure programming techniques for implementing the API methods and data processing, because the input data could be maliciously crafted.
- Req-App-2: eID App must use the PACE protocol [1, chapter 3.3] when establishing secure connection to the IAS-ECC applet on the ID-card.
- Req-App-3: eID App must use `android:allowBackup="false"` or similar settings in order not to leak the stored CAN number to cloud-based backups, or the eID App must use mobile platform features, such as file encryption[3,4] to protect the stored CAN number.
- Req-App-4: eID App must not cache or store the user's PIN codes.
- Req-App-5: eID App must support multiple ID-cards (ID-card, Digital-ID) of the same person and allow switching between multiple persons and their ID-cards. The eID App must provide convenient and easily understandable user interface.

5.2 Security Requirements for eID Ecosystem Maintainer

- Req-Ops-1: The eID ecosystem maintainer and the eID app publisher have to make sure that the attackers are not able to change the binary of the eID App and upload modified apps. In order to ensure that the maintainer and app published may need to protect the signing key pair of the eID app and/or the login credentials to the app stores of mobile platforms. 2FA login credentials must be used.
- Req-Ops-2: eID ecosystem maintainer should consider following two options to help users to install the correct eID App:
  1. ID-card already has a QR-code on it, which redirects to the document status page at `https://www.politsei.ee/et/paringud/dokumendi-kehtivuse-kontroll?qr=`. This webpage should also include pointers to the correct eID App at the app stores of mobile platforms.
  2. It could be possible to include the same URL in the NDEF message of the NFC tag inside the ID-card, so that when user taps the ID-card with the Android phone, the same web-page with links to correct eID Apps is automatically opened.
- Req-Ops-3: The eID App must be kept up to date (for example, in order to keep up with new versions of mobile platforms) and new eID App versions must be made available in the app stores frequently - at least once every 6 months. Security critical updates must be published more often.

[3] https://developer.android.com/reference/androidx/security/crypto/EncryptedFile

[4] https://developer.apple.com/documentation/uikit/protecting_the_user_s_privacy/encrypting_your_app_s_files

- Req-Ops-4: Feedback for the eID App and comments or complaints in the app stores must be managed and responded to in order to ensure that the rating of the eID App is on par with other trustworthy apps. This helps in a situation when an attacker could try to have the app blocked and generates fabricated malicious feedback, which could be basis for the mobile platforms to remove the app from app stores.
- Req-Ops-5: Incidents must be monitored (for example, blocking the eID App, publishing of fake apps, ...) and handled.

5.3 Security Requirements for RPs

- Req-RP-1: RP must verify the trustworthiness of the eID App on the user's phone and only proceed with ID-card authentication over NFC if it receives and validates the attestation of the vendor of the installed eID App.
- Req-RP-2: RP must use Universal Links/App Links for invoking the function of authentication or signing of the eID App.
- Req-RP-3: DigiDoc app or RP, who is requesting digital signature from the ID-card over the NFC interface, must verify the trustworthiness of the eID App on the user's phone and only proceed with signing function, if it receives and validates the attestation of the vendor of the installed eID App.

5.4 Security Requirements Mapping

Some proposed security measures are related to multiple identified security risks (i.e. they decrease the risk level) and some security risks may need multiple security measures in order to decrease the risk level. For overview, please see the table 3 on the facing page.

Table 3: Mapping security requirements against threats

	Req-App-1	Req-App-2	Req-App-3	Req-App-4	Req-App-5	Req-Ops-1	Req-Ops-2	Req-Ops-3	Req-Ops-4	Req-Ops-5	Req-RP-1	Req-Rp-2
CAN-TAMP-1	YES	–	YES	–	YES	YES	YES	YES	YES	YES	–	–
CAN-INFO-1	–	–	–	–	–	–	–	–	–	–	–	–
CAN-INFO-2	YES	–	YES	–	YES	YES	YES	YES	YES	YES	–	–
CAN-DENIAL-1	YES	–	YES	–	YES	YES	YES	YES	YES	YES	–	–
CAN-DENIAL-2	YES	–	YES	–	YES	YES	YES	YES	YES	YES	–	–
PIN-SPOOF-1	–	–	–	–	–	YES	YES	YES	YES	YES	YES	YES
PIN-SPOOF-2	YES	YES	–	–	–	–	–	–	–	–	–	–
PIN-SPOOF-3	YES	YES	–	YES	–	–	–	–	–	–	–	–
PIN-TAMP-1	–	–	–	YES	–	YES	YES	YES	YES	YES	YES	YES
PIN-TAMP-2	YES	YES	–	YES	–	YES	YES	YES	YES	YES	YES	YES
PIN-TAMP-3	YES	YES	–	YES	–	–	–	–	–	–	–	–
PIN-REPU-1	–	–	–	–	–	–	–	–	–	–	–	–
PIN-INFO-1	–	–	–	–	–	–	–	–	–	–	–	–
PIN-DENIAL-1	–	–	–	–	YES	–	–	–	–	–	–	–
HASH-SPOOF-1	YES	–	–	–	–	–	–	–	–	–	–	–
HASH-TAMP-1	–	–	–	–	–	YES	YES	YES	YES	YES	YES	–
HASH-REPU1	–	–	–	–	–	YES	YES	YES	YES	YES	YES	–
HASH-REPU-2	–	–	–	–	–	YES	YES	YES	YES	YES	YES	–
HASH-INFO-1	–	YES	–	–	–	YES	YES	YES	YES	YES	YES	–

	Req-App-1	Req-App-2	Req-App-3	Req-App-4	Req-App-5	Req-Ops-1	Req-Ops-2	Req-Ops-3	Req-Ops-4	Req-Ops-5	Req-RP-1	Req-Rp-2
HASH-INFO-2	–	YES	–	–	–	YES	YES	YES	YES	YES	YES	–
HASH-DENIAL-1	–	–	–	–	–	YES	YES	YES	YES	YES	YES	–
HASH-DENIAL-2	–	–	–	–	–	YES	YES	YES	YES	YES	YES	–
HASH-PRIV-1	YES	–	–	–	–	YES	YES	YES	YES	YES	YES	–
WIRELESS-REPU-1	YES	YES	–	–	–	–	–	–	–	–	–	–
WIRELESS-INFO-1	YES	YES	–	–	–	–	–	–	–	–	–	–
WIRELESS-INFO-2	YES	YES	–	–	–	–	–	–	–	–	–	–

6 Legal Analysis

In this chapter we analyse the legal requirements of authentication and electronic signing over the contactless NFC interface. In broad terms, the purpose of this analysis is to clarify whether authentication and electronic signing over the contactless NFC interface have the same legal effect as authentication and electronic signing when using a smartcard reader. More specifically, we are looking to answer two questions:

1. Is an electronic signature generated by means of the Estonian ID-card (a certified QSCD) via contactless NFC interface considered a qualified electronic signature?
2. Would an authentication, which is carried out by means of the Estonian ID-card (electronic identification means issued under an electronic identification scheme at assurance level high) via contactless NFC interface, correspond to assurance level high?

We answer these questions in three separate sections below:

1. Overview and analysis of the regulatory requirements and technical standards of certifying the Estonian ID-card as a QSCD for electronic signing.
2. Legal analysis of electronic signing by means of the Estonian ID-card over the contactless NFC interface.
3. Legal analysis of authentication by means of the Estonian ID-card over the contactless NFC interface.

6.1 Using QSCD Device over Contactless Interface

This section studies basic underlying questions for upcoming legal and compliance topics. The questions are:

1. Is it allowed that a QSCD can be used via contactless interface to produce qualified signatures?
2. If specific models of the Estonian ID-card also have this security feature.

6.1.1 Protection Profile Requirements for QSCDs

eIDAS regulation [44] and Commission implementing decision 650/2016 [3] specify in the Annex a list of PPs (Protection Profile), which a QSCD (Qualified Signature Creation Device) product must correspond to:

1. EN 419211-1:2014 – Protection profiles for secure signature creation device — Part 1: Overview [31]
2. EN 419211-2:2013 – Protection profiles for secure signature creation device — Part 2: Device with key generation [32]
3. EN 419211-3:2013 – Protection profiles for secure signature creation device — Part 3: Device with key import [34]
4. EN 419211-4:2013 – Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application [36]

5. EN 419211-5:2013 – Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application [38]

6. EN 419211-6:2013 – Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application [30]

Those PPs define threats, assumptions and security features for evaluated products and for the environment, where the products can be used. The question is, whether these PP-s also take into account that communication with a QSCD could be done over the contactless NFC communication channel.

In those PPs, there's no direct mentioning of terms 'NFC' or 'contactless interface'. However, the PP EN 419211-2:2013 does include the following security objectives for the operational environment of a TOE:

1. `OE.HID_VAD` – 'If an external device provides the human interface for user authentication, this device shall ensure confidentiality and integrity of the VAD as needed by the authentication method employed from import through its human interface until import through the TOE interface. In particular, if the TOE requires a trusted channel for import of the VAD, the HID shall support usage of this trusted channel' [32, section 7.2.5]

2. `OE.DTBS_Protect` – 'The operational environment shall ensure that the DTBS/R (Data To Be Signed Representation) cannot be altered in transit between the SCA (Signature Creation Application) and the TOE. In particular, if the TOE requires a trusted channel for import of the DTBS/R, the SCA shall support usage of this trusted channel' [32, section 7.2.7]

in order to counter the following threats and organisational policies:

1. `T.SigF_Misuse` – 'An attacker misuses the signature creation function of the TOE to create SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE' [32, section 6.2.5]

2. `T.DTBS_Forgery` – 'An attacker modifies the DTBS/R sent by the SCA. Thus the DTBS/R used by the TOE for signing does not match the DTBS the signatory intended to sign' [32, section 6.2.6]

3. `P.Sig_Non-Repud` – 'The lifecycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate' [32, section 6.3.4]

EN 419211-5:2013 extends the core PP EN 419211-2:2013 and includes the following security objectives for both the TOE and the operational environment:

1. `OT.TOE_TC_VAD_Imp` – 'The TOE shall provide a trusted channel for the protection of the confidentiality and integrity of the VAD received from the HID as needed by the authentication method employed' [38, section 7.1.2]

2. `OT.TOE_TC_DTBS_Imp` – 'The TOE shall provide a trusted channel to the SCA to detect alteration of the DTBS/R received from the SCA. The TOE shall not generate electronic signatures with the SCD for altered DTBS' [38, section 7.1.3]

3. OE.HID_TC_VAD_Exp – 'The HID provides the human interface for user authentication. The HID will ensure confidentiality and integrity of the VAD as needed by the authentication method employed including export to the TOE by means of a trusted channel' [38, section 7.2.2]

4. OE.SCA_TC_DTBS_Exp – 'The SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS/R cannot be altered undetected in transit between the SCA and the TOE' [38, section 7.2.3]

Application notes 1, 2, 3 and 4 explain this addition in more details [38, p. 11]:

> This security objective for the TOE is partly covering *OE.HID_VAD* from the core PP. While *OE.HID_VAD* in the core PP requires only the operational environment to protect VAD, this PP requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to *OE.HID_TC_VAD_Exp*, the TOE imports VAD at the other end of the trusted channel according to *OT.TOE_TC_VAD_Imp*. Therefore this PP re-assigns partly the VAD protection from the operational environment as described by *OE.HID_VAD* to the TOE as described by *OT.TOE_TC_VAD_Imp* and leaves only the necessary functionality by the HID.

Therefore, [38] describes the situation, when SCA is communicating with the QSCD over an untrusted communication channel and they both need to implement certain security measures and it requires that products claiming conformance to this PP (and in turn, to the eIDAS regulation), need to implement a trusted channel between the product and the SCA application in the operational environment.

We can conclude, that the eIDAS regulation foresees the possibility to use a QSCD over NFC interface and allows this use case, provided that some specific requirements are met.

6.1.2 Estonian ID-card Applet Security Evaluation

6.1.2.1 Estonian ID-card Versions and Configurations

We have found two different versions of IAS ECC applet, used in Estonian ID-cards and residence permit cards:

1. Applet IAS ECC V2, release 1.0, applet ID E002020A, running on top of the JavaCard platform ID-One Cosmo V8.1-N

2. Applet IAS ECC V2, release 1.3, applet ID F0020213, running on top of the JavaCard platform ID-One Cosmo V8.2

Additionally, IAS ECC applet has four different configuration options. All those releases and configurations have corresponding ST documents and different PP conformance claims. Summary of the overall situation is given in table 4.

Table 4: Versions, configurations and claimed conformance of IAS ECC applet

Applet version	Applet ID	Config. #	ST document ID	Claimed conformance to PPs	Claimed conformance to standards
release 1.0	E002020A	#1	110 8711 R3.0	BSI-CC-PP-0059-2009-MA-01	prEN 14169-1:2009
				BSI-CC-PP-0075	prEN 14169-3:2012
				BSI-CC-PP-0071	prEN 14169-4:2012
				BSI-CC-PP-0072	prEN 14169-5:2012
				BSI-CC-PP-0076	prEN 14169-6:2013
release 1.0	E002020A	#2	110 8712 R3.0	BSI-CC-PP-0059-2009-MA-01	prEN 14169-1:2009
				BSI-CC-PP-0075	prEN 14169-3:2012
release 1.0	E002020A	#3	110 8713 R3.0	BSI-CC-PP-0059-2009-MA-01	prEN 14169-1:2009
				BSI-CC-PP-0075	prEN 14169-3:2012
release 1.0	E002020A	#4	110 8714 R3.0	BSI-CC-PP-0059-2009-MA-01	prEN 14169-1:2009
				BSI-CC-PP-0075	prEN 14169-3:2012
				BSI-CC-PP-0071	prEN 14169-4:2012

Applet version	Applet ID	Config. #	ST document ID	Claimed conformance to PPs	Claimed conformance to standards
release 1.3	F0020213	#1	110 9184 R3.0	BSI-CC-PP-0059-2009-MA-01	prEN 14169-1:2009
				BSI-CC-PP-0075	prEN 14169-3:2012
				BSI-CC-PP-0071	prEN 14169-4:2012
				BSI-CC-PP-0072	prEN 14169-5:2012
				BSI-CC-PP-0076	prEN 14169-6:2013
release 1.3	F0020213	#2	110 9185 R3.0	BSI-CC-PP-0059-2009-MA-01	prEN 14169-1:2009
				BSI-CC-PP-0075	prEN 14169-3:2012
release 1.3	F0020213	#3	110 9186 R3.0	BSI-CC-PP-0059-2009-MA-01	prEN 14169-1:2009
				BSI-CC-PP-0075	prEN 14169-3:2012
				BSI-CC-PP-0071	prEN 14169-4:2012
release 1.3	F0020213	#4	110 9187 R3.0	BSI-CC-PP-0059-2009-MA-01	prEN 14169-1:2009
				BSI-CC-PP-0075	prEN 14169-3:2012
				BSI-CC-PP-0071	prEN 14169-4:2012

6.1.2.2 Discrepancy of PP Versions

Formally, ST documents [14, 15, 17, 18, 16, 19, 20, 21] claim conformance to PPs [33, 35, 37, 39, 40], which are not the same documents as [32, 34, 36, 38, 30], which are referenced by [3].

Following conservative interpretation, the applet 'IAS ECC v2', versions 1.0 and 1.3 are not compliant with EU QSCD requirements, because they are evaluated against older versions of PPs.

However, for the purpose of this analysis, we assume that those PP-s are equivalent, because for example the [38] also refers to itself internally, as 'BSI-CC-PP-0071' and not 'BSI-CC-PP-0071-2012-MA-01' (see page 5 of [38]). We assume this discrepancy is simply a clerical error and the references simply haven't been updated on time.

6.1.2.3 Configuration of Estonian ID-card Applet

Document 'Estonia eID Chip Specifications' [7] gives an overview of Estonian eID's technical details and also specifies in the sections 6.1.1 and 6.1.2 whether a trusted channel is used to communicate with the CGA or SCA components. It concludes that a trusted channel is only used when communicating with the CGA and therefore:

> The identified configuration for Estonian ID cards is #4 according to CLYTEMNESTRE *`ADV_PRE`*.

6.1.2.4 Evaluated Security Functions of Applet Version 1.3 and Configuration #4

[21] includes the same set of relevant threats and security policies:

1. `T.SigF_Misuse` – (see section 5.2.1.5)
2. `T.DTBS_Forgery` – (see section 5.2.1.6)
3. `P.Sig_Non-Repud` – (see section 5.3.1.4)

However, [21] claims that `T.SigF_Misuse` is satisfied by the following set of security objectives:

1. `OT.Lifecycle_Security`
2. `OT.Sigy_SigF`
3. `OT.DTBS_Integrity_TOE`
4. `OT.Lifecycle_Management`
5. `OE.HID_VAD`
6. `OE.DTBS_Intend`
7. `OE.DTBS_Protect`
8. `OE.Signatory`

and `T.DTBS_Forgery` by:

1. `OT.DTBS_Integrity_TOE`
2. `OE.DTBS_Intend`

3. OE.DTBS_Protect

The list of relevant security objectives doesn't include OT.TOE_TC_VAD_Imp or OT.TOE_TC_DTBS_Imp. The OT.DTBS_Integrity_TOE doesn't cover this either, because it only focuses on what is happening inside the TOE itself and not on transmitting the VAD or DTBS over the secure channel [21, section 6.1.1.9].

Therefore, security of the 'configuration #4' is only evaluated in the case when contactless interface is used to communicate only with the CGA.

6.1.2.5 Evaluated Security Functions of Applet Version 1.3 and Configuration #1

At the same time, eID applet 'IAS ECC V2' is also evaluated in 'configuration #1', accordance with the ST document [16], which is similar to the [21], but includes all the relevant security objectives, such as OT.TOE_TC_VAD_Imp and OT.TOE_TC_DTBS_Imp.

Therefore, the evaluation results also hold in the case when contactless interface is used to communicate with SCA.

6.1.2.6 Evaluation Reports of Applet Version 1.3

Configurations #1 and #4 have separate certification reports.

Evaluation report 'Rapport de certification ANSSI-CC-2020/50 – IAS ECC v2, version 1.3 in configuration #1 on ID-One Cosmo v8.2 open platform' [42] section 3.1 ('Conclusion') gives us the following statement (machine translation by translate.google.com):

> This certificate certifies that the product 'IAS ECC v2, version 1.3 in configuration #1 on ID-One Cosmo v8.2 open platform, applet identification: F0 02 02 13, hardware identification: 09 11 21, patch identification : 09 42 22' submitted for evaluation meets the security characteristics specified in its security target [ST] for the EAL 5 evaluation level augmented with the *ALC_DVS.2* and *AVA_VAN.5* components.

Evaluation report 'Rapport de certification ANSSI-CC-2020/53 – IAS ECC v2, version 1.3 in configuration #4 on ID-One Cosmo v8.2 open platform' [43] section 3.1 ('Conclusion') gives us the following statement (machine translation by translate.google.com):

> This certificate certifies that the product 'IAS ECC v2, version 1.3 in configuration #4 on ID-One Cosmo v8.2 open platform, applet identification: F0 02 02 13, hardware identification: 09 11 21, patch identification : 09 42 22' submitted for evaluation meets the security characteristics specified in its security target [ST] for the EAL 5 evaluation level augmented with the *ALC_DVS.2* and *AVA_VAN.5* components.

Because the applet identifier (F0020213) is the same for both certificates (and also with the certification reports for the version 1.0), we simply conclude that the applet's binary code is the same for both configurations. Therefore, it doesn't really matter, which configuration is stated by the [7]. In the end, all the security features are still there and they are still evaluated.

6.1.3 Conclusion

Therefore, we can conclude that Estonian eID applet 'IAS ECC V2', both versions 1.0 and 1.3, do implement all the promised security features, including possibility to use a trusted channel to communicate with SCA.

6.2 Signing over the Contactless NFC Interface

6.2.1 Qualified Electronic Signatures

Electronic signatures generated by means of the Estonian ID-card using a smartcard reader are considered as qualified electronic signatures and thus have the equivalent legal effect of a handwritten signature (eIDAS Art 25(2)). In order to give the same legal effect to electronic signatures generated by means of the Estonian ID-card over the contactless NFC interface, they would also have to be considered as qualified electronic signatures.

Qualified electronic signatures are equalled to handwritten signatures in the EU law (eIDAS Regulation Art 25(2)), which has direct applicability in Estonian law. This means that, essentially, the EU law overrules the Estonian law in the same field. For this reason, we shall not analyse the rules of Estonian law concerning electronic or digital signatures and their legal effects. Instead, we shall only focus on analysing the eIDAS rules on qualified electronic signatures.

In what follows, we shall analyse whether an electronic signature generated by means of the Estonian ID-card (a certified QSCD) via contactless NFC interface can be considered a qualified electronic signature. Firstly, the requirements of what constitutes a qualified electronic signature are provided. According to eIDAS Art 3 p 12, a qualified electronic signature must fulfil the following three conditions:

1. it has to be an advanced electronic signature,
2. that is created by a qualified electronic signature creation device (QSCD), and
3. based on a qualified certificate for electronic signatures.

We shall address these conditions in separate subsections below.

6.2.2 Advanced Electronic Signature

The first condition of having a qualified electronic signature is for it to meet the requirements for an advanced electronic signature.

'Advanced electronic signature' means an electronic signature which meets the following four requirements (eIDAS Art 3 p 11 and Art 26):

1. it is uniquely linked to the signatory;
2. it is capable of identifying the signatory;
3. it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
4. it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

As per the general design of the anticipated eID system for the contactless NFC interface (see chapter 2 on page 8), the signature itself, created by means of the Estonian ID-card using a smartcard reader is essentially the same, as compared to the situation when it is created by means of the Estonian ID-card over the contactless NFC interface.

In conclusion, we presume that the first condition of having a qualified electronic signature is fulfilled.

6.2.3 Qualified electronic signature creation device (QSCD)

The second condition of having a qualified electronic signature is for it to be created by means of a qualified electronic signature creation device (QCSD).

Qualified electronic signature creation device (QSCD) means an electronic signature creation device that meets the requirements laid down in Annex II of eIDAS (eIDAS Art 3 p 23). QSCDs shall meet the requirements laid down in Annex II of eIDAS (eIDAS Art 29(1)). Furthermore, compliance with the requirements laid down in Annex II of eIDAS shall be presumed where a QSCD meets the standards that the Commission has established for QSCDs (eIDAS Art 29(2)).

To the best of our knowledge, the Commission has not established any reference numbers of standards for QSCDs under eIDAS Art 29(2). This means that no QSCD can be presumed to meet the requirements of Annex II of eIDAS, because there are no standards established for QSCDs based on eIDAS Art 29(2) that a specific QSCD could be measured against. It also means that there is room for interpretation and thus rather wide discretion for the QSCD provider to demonstrate that its QSCD actually meets the requirements of Annex II of eIDAS.

In practice, service providers have relied on Common Criteria based Protection Profile (PP) requirements, to demonstrate the compliance of their QSCD with the requirements of Annex II of eIDAS. As explained above in Section ”Protection Profile requirements for QSCDs” (see section 6.1.1 on page 41), the Commission has established a list of standards for the security assessment of information technology products under eIDAS Art 30(3) second paragraph. One of those standards is ‘EN 419211 - Protection profiles for secure signature creation device, Parts 1 to 6 — as appropriate’ – it provides security objectives concerning QSCDs. Even though this standard is established by the Commission as a standard for the security assessment of information technology products under eIDAS Art 30(3), and not as a standard for QSCDs under eIDAS Art 29(2), it can still be relied on to demonstrate that a QSCD meets the requirements of Annex II of eIDAS, for the lack of a better alternative.

Another way to provide certainty regarding a QSCD’s compliance with the requirements of Annex II of eIDAS is to have it certified. eIDAS requires the conformity of QSCDs with the requirements laid down in eIDAS Annex II to be certified by appropriate public or private bodies designated by Member States (eIDAS Art 30(1)). The certification can be based on one of the following options:

1. a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in the list established by the Commission Implementing Decision 2016/650 [3] (eIDAS Art 30(3)(a));

2. other process, provided that it uses comparable security levels and provided that the certifying public or private body notifies that process to the Commission. That process may be used only in the absence of standards referred to in the first option above or when a security evaluation process referred to in the first option above is ongoing (eIDAS Art 30(3)(b)).

The certification of the QSCD contained in the Estonian ID-card has been confirmed by ANSSI[42, 43], which is designated by France as an appropriate public or private body to certify QSCDs[5] and notified as such to the Commission ((eIDAS Art 30(2)).[6] The certification of the Estonian ID-card as a QSCD has been done according to the rules explained in the previous section. However, the Estonian ID-card has not been notified as a certified QSCD to

[5] Estonia has not designated any appropriate public or private bodies to certify QSCDs. It remains open for discussion wether eIDAS Art 30(2) requires each Member State to rely on certification of only those bodies which it has designated as appropriate itself or whether it can also rely on the certifications of bodies designated by other Member States. We presume the latter interpretation is correct and Estonia is thus allowed to rely on the certification of a body designated as appropriate by another Member State.

[6] https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/BODIES_QSCD_SSCD

the Commission, as required by eIDAS (eIDAS Art 31(1)), because it relies on a pre-existing QSCD notified to the Commission before implementing it in the Estonian ID-card. For this reason, the Estonian ID-card is not on the list of certified QSCDs published and maintained by the Commission (eIDAS Art 31(2)).[7]

Based on the above circumstances, the following question arises - can an electronic signature generated by means of a QSCD still be considered a qualified electronic signature, if:

1. the QSCD is not certified or is certified against the wrong (e.g. outdated) standard for the security assessment of information technology products (for example, if it is confirmed that the applet 'IAS ECC v2', versions 1.0 and 1.3 are not compliant with eIDAS requirements for QSCDs, because they are evaluated against older version of PPs - see 6.1.2.2 on page 46)), or

2. the QSCD is not in the list of certified QSCDs published and maintained by the Commission?

In order to answer this question, we need to first clarify the legal meaning of 'certification' and 'certified QSCD' under eIDAS. When looking at the very definition of a qualified electronic signature in eIDAS, it does not involve the requirement for the QSCD to be 'certified' (eIDAS Art 3 p 12):

> 'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

At the same time, the rule that a QSCD has to be 'certified' is set out in a different eIDAS norm (eIDAS Art 30(1)):

> Conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States.

Therefore, there can be no doubt that all QSCDs have to be 'certified' at some point, eventually. Here is where the temporal aspect of 'certification' becomes important – is 'certification' of a QSCD required before it can be used to generate legally valid qualified electronic signatures? This question remains unanswered in eIDAS - none of the eIDAS clauses require a QSCD to be 'certified' or notified to the Commission for publication in the list of certified QSCDs or even published in that list before effectively using the QSCD for electronic signing. Prior 'certification' of a QSCD or a QSCD having been 'certified' is not an imperative precondition to create a legally valid qualified electronic signature by means of this QSCD.

Based on the above reasoning, it seems that a QSCD does not need to be 'certified' (not even 'certified' against the correct standard) nor published in the list of certified QSCDs maintained by the Commission in order for it to effectively generate qualified electronic signatures. To sum up, if an advanced electronic signature is created by a QSCD, which demonstrably meets the requirements laid down in Annex II of eIDAS, then it can be a qualified electronic signature even without 'certification' or publication as a 'certified QSCD'.

Even if the opposite is true and 'certification' of a QSCD is considered an imperative precondition for creating legally valid qualified electronic signatures by the relevant supervisory authority or court, it is important to note that the lack of such 'certification' does not necessarily cause an electronic signature to be invalid or cancelled. If an electronic signature does not meet all the requirements for qualified electronic signatures, it can still have legal effect and

[7] https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD

admissibility as evidence in legal proceedings (eIDAS Art 25(1)), although it is no longer equal to a handwritten signature.

In conclusion, we presume that the second condition of having a qualified electronic signature is fulfilled.

6.2.4 Qualified Certificate for Electronic Signatures

The third condition of having a qualified electronic signature is for it to be based on a qualified certificate for electronic signatures.

'Qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in eIDAS Annex I (eIDAS Art 3 p 15). The eIDAS Annex I requires that qualified certificates for electronic signatures shall contain the following:

(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;

(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and:

   1. for a legal person: the name and, where applicable, registration number as stated in the official records,
   2. for a natural person: the person's name;

(c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;

(d) electronic signature validation data that corresponds to the electronic signature creation data;

(e) details of the beginning and end of the certificate's period of validity;

(f) the certificate identity code, which must be unique for the qualified trust service provider;

(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;

(i) the location of the services that can be used to enquire about the validity status of the qualified certificate;

(j) where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.

The last point above (eIDAS Annex I (j)) expressly mentions QSCDs - this means that a qualified certificate for electronic signatures has to include information if the signature is given by means of a QSCD. However, the requirements of eIDAS Annex I also do not presume the QSCD to be certified, thus confirming the conclusions of the previous section.

As per the general design of the anticipated eID system for the contactless NFC interface (see chapter 2 on page 8), the certificate for electronic signatures stored on the Estonian ID-card will remain the same, whether it is used over a smartcard reader or over the contactless NFC interface. According to our understanding, the certificate for electronic signatures currently used in the Estonian ID-card is issued by a qualified trust service provider (SK ID Solutions AS) and meets the requirements laid down in eIDAS Annex I.

In conclusion, we presume that the third condition of having a qualified electronic signature is fulfilled.

6.2.5 Interim Conclusion

As a result of the analysis of the three conditions of a qualified electronic signature above, we conclude that an electronic signature generated by means of the Estonian ID-card (a certified QSCD) via contactless NFC interface can be considered a qualified electronic signature, as long as the requirements of eIDAS Art 3 p 12 remain fulfilled, even if the Estonian ID-card is certified against an older version of the relevant QSCD standard (see section 6.1.2.2 on page 46).

6.3 Authentication over the Contactless NFC Interface

Under Estonian law, there are very few rules concerning the use of digital identity. This concerns also authentication. ITDS regulates the entry of the certificate that enables digital identification into an identity document and provides rules for the suspension, restoration of validity and revocation of the certificate that enables digital identification (ITDS §9^4-9^6), referring to EUTS with regard to the suspension and restoration of validity process (ITDS §9^5). ITDS also provides for the basic rules of verification of identity of a holder of an identity document (ITDS §18^1). EUTS, on the other hand, does include provisions concerning the evaluation of assurance level of electronic identification schemes but these do not apply to electronic identification schemes which are based on (digital) identity documents issued under the ITDS, including the ID-card and Mobile ID (EUTS §1 lg 5).

Therefore, when putting the EU law aside (eIDAS), authentication as such is essentially unregulated in Estonian law. The only legal act that includes technical specifications concerning the electronic identification means in Estonia is a regulation issued by the Minister of Entrepreneurship and Innovation under ITDS § 9 section 5^1 concerning the data medium for digital documents and digital data [49]. According to this regulation, the data medium to which a digital document or the document's digital data may be transferred to, must fulfill the following conditions:

1. the technical characteristics of the data carrier ensure the integrity, authenticity and confidentiality of the data transferred to it;
2. the data medium ensures the storage of the data at least during the period of validity of the certificates that have been transferred to the data medium or are related to it;
3. the data medium is separable from the device, where operations are carried out by means of the digital document;
4. the data medium ensures sufficient endurance to everyday use;
5. the data medium has a standardised data interface;
6. the data medium enables reading of data and writing over an encrypted data exchange channel;
7. the data medium is interoperable with and enables the use of the corresponding digital document in the existing infrastructure;

8. if the technical characteristics of the data medium allow adding and deleting applications to it, this can happen only under the control of the issuer of the digital document.

According to our understanding, the conditions enlisted above remain to be fulfilled in case of the Estonian ID-card (data medium),[8] if the contactless NFC interface is taken into use along the lines of the general design of the anticipated eID system for the contactless NFC interface (see chapter 2 on page 8).

Due to the above considerations, we will focus on analysing the EU law (eIDAS) in the analysis that follows below.

Authentication carried out by means of the Estonian ID-card using a smartcard reader is considered as authentication at assurance level high according to eIDAS. As a result, the Estonian ID-card must be recognised as an electronic identification means in other Member States for the purposes of cross-border authentication in their public sector services which require the use of an electronic identification means and authentication for access to the service, provided that the other Member State has introduced at least one public service which uses assurance level substantial or high in relation to accessing that service online (eIDAS Art 6(1)). In order to give the same legal effect to authentication by means of the Estonian ID-card over the contactless NFC interface, it would also have to be considered as authentication at assurance level high.

In what follows, we shall analyse whether an authentication, which is carried out by means of the Estonian ID-card (electronic identification means issued under an electronic identification scheme at assurance level high) via contactless NFC interface, corresponds to assurance level high. In order to do so, we shall first clarify the legal requirements for electronic identification means at assurance level high. According to eIDAS Art 6(1), the electronic identification means issued in Estonia shall be recognised in another Member State for the purposes of cross-border authentication for a service provided by a public sector body online, provided that the following conditions are met:

1. the electronic identification means must be issued under an electronic identification scheme that is included in the list of the electronic identification schemes which were notified by Estonia and published by the Commission (eIDAS Art 6(1)(a) and eIDAS Art 9);

2. the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the other Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high (eIDAS Art 6(1)(b));

3. the relevant public sector body uses the assurance level substantial or high in relation to accessing that service online in the other Member State (eIDAS Art 6(1)(c)).

For the purposes of the following analysis, we shall presume that the last condition (eIDAS Art 6(1)(c)) is fulfilled, i.e. the public sector service in the other Member State uses at least the assurance level substantial in order to be accessed online. Therefore, we shall focus on the first two conditions and find answers to the following questions:

1) does the Estonian ID-card, which is included in the list of the electronic identification schemes notified to the Commission by Estonia, cover the recently added NFC functionality for contactless authentication?

2) does authentication by means of the Estonian ID-card via contactless NFC interface correspond to assurance level high (eIDAS Art 6(1)(b))?

[8] For some reason, this regulation does not refer to any of the requirements established for a QSCD, although such requirements are also applied to electronic identification means in Estonia.

6.3.1 Notified Electronic Identification Means

The first condition of authenticating via contactless NFC interface at assurance level high is for the relevant electronic authentication means (the Estonian ID-card) to be included in the list of the electronic identification schemes notified by the relevant Member State to the Commission. The Republic of Estonia has notified altogether 6 electronic identification schemes, each of which includes one electronic identification means bearing the same name as the scheme[9]:

1. Estonian eID scheme: ID card
2. Estonian eID scheme: RP card
3. Estonian eID scheme: Digi-ID
4. Estonian eID scheme: e-Residency Digi-ID
5. Estonian eID scheme: Mobiil-ID
6. Estonian eID scheme: diplomatic identity card

The Estonian ID-card is issued as an electronic identification means under the electronic identification scheme 'Estonian eID scheme: ID card' notified by Estonia and published by the Commission [8]. We have concluded above that the most recent generation of ID-cards issued in Estonia have the NFC functionality for contactless authentication available. Thus, what needs to be ascertained is whether this NFC functionality of the Estonian ID-card is also part of the electronic identification means notified to the Commission under the 'Estonian eID scheme: ID card'. In order to do this, the [8] has to be analysed in more detail.

In principle, neither eIDAS nor the Commission Implementing Regulation 2015/1502 [4] pose any limitations to starting the usage of contactless NFC interface functionalities to the electronic identification means in the Estonian ID-card because there are no specific requirements towards the interfaces and communication channels used within the electronic identification means.

At the same time, a Member State is required to notify the Commission if there are any subsequent changes in some of the information included in the notification of an electronic identification scheme (eIDAS Art 9(1)). The obligation to notify changes concerns the following information:

1. a description of the electronic identification scheme, including its assurance levels and the issuer or issuers of electronic identification means under the scheme (eIDAS Art 9(1)(a));
2. the applicable supervisory regime and information on the liability regime with respect to (i) the party issuing the electronic identification means; and (ii) the party operating the authentication procedure (eIDAS Art 9 (1)(b));
3. the authority or authorities responsible for the electronic identification scheme (eIDAS Art 9 (1)(c));
4. information on the entity or entities which manage the registration of the unique person identification data (eIDAS Art 9 (1)(d));
5. a description of how the requirements set out in the implementing acts on the interoperability framework are met (eIDAS Art 9 (1)(e), eIDAS Art 12 (8));
6. a description of the authentication (eIDAS Art 9 (1)(f), eIDAS Art 7 (f));

[9] https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Estonia

7. arrangements for suspension or revocation of either the notified electronic identification scheme or authentication or the compromised parts concerned (eIDAS Art 9 (1)(g)).

Description of how Estonian ID-card is technically used for authentication, is given in the section 2.3.1 – 'Authentication mechanism' of [8]. It is rather high-level, it doesn't say anything about the communication interface of the ID-card itself, and we have to conclude that it fits with general design of the anticipated eID system for the contactless NFC interface (see chapter 2 on page 8). According to our understanding, there will be no changes required in the information that has been notified to the Commission under eIDAS Art 9 (1) concerning the authentication by means of ID-card over currently used smartcard interfaces. However, if the contactless NFC interface is taken into use for authenticating by means of the Estonian ID-card in the future, additional information may need to be notified to the Commission under eIDAS Art 9 (1), e.g. description of the authentication and how the different eIDAS requirements are fulfilled in case of using the contactless NFC interface. This question is out of scope of this legal analysis and should be further analysed in the future.

Based on the above, we conclude that the contactless NFC interface functionality of the Estonian ID-card can be considered as incorporated in the electronic identification means notified to the Commission under the 'Estonian eID scheme: ID card' scheme. To summarise, the first condition of authenticating via contactless NFC interface at assurance level high is fulfilled, if it is verified that no changes are required in the information listed in eIDAS Art 9(1) due to the taking into use of the contactless NFC interface in the future.

6.3.2 Correspondence to Assurance Level High

The second condition of authenticating via contactless NFC interface at assurance level high is that such authentication has to meet the requirements for assurance level high (eIDAS Art 6 (1)(b)). Such requirements are provided in eIDAS Art 8 and the Commission Implementing Regulation (EU) 2015/1502.

All the Estonian schemes are notified as having assurance level high. According to the notification form submitted by Estonia, the electronic identification means characteristics and design are described in section 2.2.1 of the corresponding level of assurance documents [28, section 4.2.2]. The relevant level of assurance document for the Estonian ID-card is made available by Estonia as 'Estonian eID scheme: ID card. Technical specifications and procedures for assurance level high for electronic identification' [8]. As per section 2.2.1 and section 2.3.1 of [8], ID-card fulfils all the minimum technical specifications of assurance levels substantial and high, as stipulated in the Commission Implementing Regulation (EU) 2015/1502 [4] pursuant to eIDAS art 8(3).

Based on the above, we conclude that the uptake of contactless NFC functionality as part of a pre-existing electronic identification means issued at assurance level high (Estonian ID-card) does not change the assurance level of that means, as long as it fulfils the requirements of eIDAS Art 8 and the Commission Implementing Regulation (EU) 2015/1502 for assurance level high.

To summarise, the second condition of authenticating via contactless NFC interface at assurance level high is fulfilled, as long as the ID-card with NFC functionality fulfils the requirements of eIDAS Art 8 and the Commission Implementing Regulation (EU) 2015/1502 for assurance level high.

6.4 Disclaimer

We note that this document does not contain a compliance analysis of the anticipated eID system performing authentication via NFC interface, considering all the specified attacks in the Commission Implementing Regulation (EU) 2015/1502 [4] and assuming attacker with high attack potential. That kind of compliance analysis would probably require a formal security evaluation as specified in a Common Criteria standard.

6.5 Conclusion

In the previous chapters of this document we have concluded that:

1. the contactless NFC functionality will fit into the current ecosystem of Estonian eID components, including the pre-existing electronic identification means contained in the ‘Estonian eID scheme: ID card’ [8], if certain additional security requirements are taken (as concluded in section 5 on page 37, and
2. the contactless NFC functionality will not add significant security risks to the pre-existing electronic identification means contained in the ‘Estonian eID scheme: ID card’ (as concluded in section 4.5 on page 36),

As long as these conclusions remain unchanged for the anticipated eID system performing authentication via NFC interface, we can conclude that:

1. an electronic signature generated by means of the Estonian ID-card (a certified QSCD) via contactless NFC interface can be considered a qualified electronic signature, as long as the requirements of eIDAS Art 3 p 12 remain fulfilled, even if the Estonian ID-card is certified against an older version of the relevant QSCD standard (see section 6.1.2.2 on page 46).
2. an electronic authentication, which is carried out by means of the Estonian ID-card (electronic identification means issued under an electronic identification scheme at assurance level high) via contactless NFC interface, could correspond to assurance level high, as long as the requirements of eIDAS Art 8 and the Commission Implementing Regulation (EU) 2015/1502 remain fulfilled. However, it needs to be verified whether there are any changes required in the information listed in eIDAS Art 9(1) due to the taking into use of the contactless NFC interface in the future.

7 Summary

7.1 Overview

The goal of this analysis is to answer the question ‘whether it is legal and safe to use the ID1 smartcard’s NFC interface for authentication and electronic signing?’

In order to answer that question, we created a draft description of the anticipated system (see section 2 on page 8) and analysed risks, which could arise in such a system. In section 4 on page 21, we identified the risks and evaluated them. We concluded that the situation where ID-card is used via NFC interface is not significantly riskier compared to using ID-card via USB interface.

In section 5 on page 37, we proposed security measures, which should be implemented and followed when using the NFC interface in production.

In section 6 on page 41, we studied the compliance and legal situation. Provided that the conclusions of the previous chapters remain unchanged for the anticipated eID system performing authentication via NFC interface, we concluded that

1. an electronic signature generated by means of the Estonian ID-card (a certified QSCD) via contactless NFC interface can be considered a qualified electronic signature, as long as the requirements of eIDAS Art 3 p 12 remain fulfilled, even if the Estonian ID-card is certified against an older version of the relevant QSCD standard;

2. an electronic authentication, which is carried out by means of the Estonian ID-card (electronic identification means issued under an electronic identification scheme at assurance level high) via contactless NFC interface, could correspond to assurance level high, as long as the requirements of eIDAS Art 8 and the Commission Implementing Regulation (EU) 2015/1502 remain fulfilled. However, it needs to be verified whether there are any changes required in the information listed in eIDAS Art 9(1) due to the taking into use of the contactless NFC interface in the future.

7.2 Conclusion

To summarize, we can conclude that using the Estonian ID-card over NFC interface is safe and there are no significant risks for the confidentiality of the user’s private keys and knowledge-based factors (PINs).

8 References

[1] *Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 1.* Technical Guideline. Version 2.20. TR-03110-1; eMRTDs with BAC/PACEv2 and EACv1. 26th Feb. 2015. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-1_V2-2.pdf;jsessionid=BDB57D1D3800DC098326B59623B86ABE.internet461?__blob=publicationFile&v=1.

[2] Tom Chothia and Vitaliy Smirnov. 'A Traceability Attack against e-Passports'. In: *Financial Cryptography and Data Security.* Ed. by Radu Sion. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 20–34. ISBN: 978-3-642-14577-3.

[3] *Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.* Commission implementing decision. Apr. 2016. URL: https://eur-lex.europa.eu/eli/dec_impl/2016/650/oj.

[4] *Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.* Commission implementing regulation. Sept. 2015. URL: https://eur-lex.europa.eu/eli/reg_impl/2015/1502/oj.

[5] Boris Danev and Thomas S Heydt-Benjamin. 'Physical-layer Identification of RFID Devices'. In: (Jan. 2009), p. 16.

[6] *Electronic Identification and Trust Services for Electronic Transactions Act.* RT I, 25.10.2016, 1 … RT I, 15.10.2021, 1. 12th Oct. 2016. URL: https://www.riigiteataja.ee/en/eli/518102021002/consolide.

[7] *Estonia eID Chip Specifications.* 2017_2000031659 V1.6. IDEMIA, 22nd Feb. 2021.

[8] *Estonian eID scheme: ID card. Technical specifications and procedures for assurance level high for electronic identification.* Police and Border Guard, 30th Sept. 2019. URL: https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Estonia?preview=/62885749/218763054/EE%20eID%20LoA%20mapping%20-%20ID%20card%20v1.1.pdf.

[9] *Euroopa Parlamendi ja Nõukogu määrus e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul.* EU määrus 910/2014. 28th Aug. 2014. URL: https://eur-lex.europa.eu/eli/reg/2014/910/oj.

[10] Ihor Filimonov et al. 'Breaking Unlinkability of the ICAO 9303 Standard for e-Passports Using Bisimilarity'. In: *Computer Security – ESORICS 2019.* Ed. by Kazue Sako, Steve Schneider and Peter Y. A. Ryan. Cham: Springer International Publishing, 2019, pp. 577–594. ISBN: 978-3-030-29959-0.

[11] *Guide for Conducting Risk Assessment.* Technical Guideline. Version 1. NIST Special Publication 800–30 Revision 1. 1st Sept. 2012. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[12] René Habraken et al. 'An RFID Skimming Gate Using Higher Harmonics'. In: 23rd June 2015, pp. 122–137. ISBN: 978-3-319-24836-3. DOI: 10.1007/978-3-319-24837-0_8.

[13] Gerhard P. Hancke. 'Practical eavesdropping and skimming attacks on high-frequency RFID tokens'. In: *Journal of Computer Security* 19.2 (1st Jan. 2011). Publisher: IOS Press, pp. 259–288. ISSN: 0926-227X. DOI: 10.3233/JCS-2010-0407. URL: https://content.iospress.com/articles/journal-of-computer-security/jcs407.

[14] *IAS ECC V2, version 1.0, in configuration #1 on Cosmo V8.1N – Public Security Target.* 110 8711 R3.0. IDEMIA, 24th Apr. 2018. URL: https://www.commoncriteriaportal.org/files/epfiles/anssi-cible-cc-2018_15en.pdf.

[15] *IAS ECC V2, version 1.0, in configuration #2 on Cosmo V8.1N – Public Security Target.* 110 8712 R3.0. IDEMIA, 24th Apr. 2018. URL: https://www.commoncriteriaportal.org/files/epfiles/anssi-cible-cc-2018_16en.pdf.

[16] *IAS ECC V2, version 1.0, in configuration #2 on Cosmo V8.2 – Public Security Target.* 110 9184 R3.0. IDEMIA, 21st Apr. 2020. URL: https://www.commoncriteriaportal.org/files/epfiles/anssi-cible-cc-2020_50en.pdf.

[17] *IAS ECC V2, version 1.0, in configuration #3 on Cosmo V8.1N – Public Security Target.* 110 8713 R3.0. IDEMIA, 24th Apr. 2018. URL: https://www.commoncriteriaportal.org/files/epfiles/anssi-cible-cc-2018_17en.pdf.

[18] *IAS ECC V2, version 1.0, in configuration #4 on Cosmo V8.1N – Public Security Target.* 110 8714 R3.0. IDEMIA, 24th Apr. 2018. URL: https://www.commoncriteriaportal.org/files/epfiles/anssi-cible-cc-2018_18en.pdf.

[19] *IAS ECC V2, version 1.3, in configuration #2 on Cosmo V8.2 – Public Security Target.* 110 9185 R3.0. IDEMIA, 21st Apr. 2020. URL: https://www.commoncriteriaportal.org/files/epfiles/anssi-cible-cc-2020_51en.pdf.

[20] *IAS ECC V2, version 1.3, in configuration #3 on Cosmo V8.2 – Public Security Target.* 110 9186 R3.0. IDEMIA, 21st Apr. 2020. URL: https://www.commoncriteriaportal.org/files/epfiles/anssi-cible-cc-2020_52en.pdf.

[21] *IAS ECC V2, version 1.3, in configuration #4 on Cosmo V8.2 – Public Security Target.* 110 9187 R3.0. IDEMIA, 21st Apr. 2020. URL: https://www.commoncriteriaportal.org/files/epfiles/anssi-cible-cc-2020_53en.pdf.

[22] *Identity Documents Act.* RT I 1999, 25, 365 … RT I, 15.10.2021, 1. 15th Feb. 1999. URL: https://www.riigiteataja.ee/en/eli/501112021001/consolide.

[23] ISO. *ISO/IEC 14443-3:2018 Cards and security devices for personal identification — Contactless proximity objects — Part 3: Initialization and anticollision.* July 2018. URL: https://www.iso.org/standard/73598.html.

[24] Ziv Kfir and Avishai Wool. 'Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems'. In: (2005), p. 14.

[25] Ilan Kirschenbaum and Avishai Wool. 'How to Build a {Low-Cost}, {Extended-Range} {RFID} Skimmer'. In: 15th USENIX Security Symposium (USENIX Security 06). 2006. URL: https://www.usenix.org/conference/15th-usenix-security-symposium/how-build-low-cost-extended-range-rfid-skimmer.

[26] Sander-Karl Kivivare. 'Secure Channel Establishment for the NFC Interface of the New Generation Estonian ID Cards'. MA thesis. University of Tartu, 2020. URL: https://comserv.cs.ut.ee/home/files/Kivivare_ComputerScience_2020.pdf?study=ATILoputoo&reference=87E6E1A14B9BC99ED47533B597228A376CE608E1.

[27] Woongsup Lee, Seon Yeob Baek and Seong Hwan Kim. 'Deep-Learning-Aided RF Fingerprinting for NFC Security'. In: *IEEE Communications Magazine* 59.5 (2021), pp. 96–101. DOI: 10.1109/MCOM.001.2000912.

[28] *Notification form for electronic identity scheme under Article 9(5) of regulation (EU) No. 910/2014*. Police and Border Guard, 30th Sept. 2019. URL: https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Estonia?preview=/62885749/218763046/ESTONIAN%20eID%20NOTIFICATION%20FORM%20FOR%20ELECTRONIC%20IDENTITY%20SCHEME%20UNDER%20ARTICLE%209%20OF%20eIDAS%20REGULATION%20v1.1.pdf.

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

[30] *Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application*. EN 419211-6:2013. European Committee for Standardization (CEN).

[31] *Protection profiles for secure signature creation device — Part 1: Overview*. EN 419211-1:2014. European Committee for Standardization (CEN).

[32] *Protection profiles for secure signature creation device — Part 2: Device with key generation*. EN 419211-2:2013. European Committee for Standardization (CEN).

[33] *Protection profiles for secure signature creation device — Part 2: Device with key generation*. prEN 14169-1:2009. European Committee for Standardization (CEN). URL: https://www.commoncriteriaportal.org/files/ppfiles/pp0059b_pdf.pdf.

[34] *Protection profiles for secure signature creation device — Part 3: Device with key import*. EN 419211-3:2013. European Committee for Standardization (CEN).

[35] *Protection profiles for secure signature creation device — Part 3: Device with key import*. prEN 14169-3:2012. European Committee for Standardization (CEN). URL: https://www.commoncriteriaportal.org/files/ppfiles/pp0075b_pdf.pdf.

[36] *Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application*. EN 419211-4:2013. European Committee for Standardization (CEN).

[37] *Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application*. prEN 14169-4:2012. European Committee for Standardization (CEN). URL: https://www.commoncriteriaportal.org/files/ppfiles/pp0071b_pdf.pdf.

[38] *Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application*. EN 419211-5:2013. European Committee for Standardization (CEN).

[39] *Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application*. prEN 14169-5:2012. European Committee for Standardization (CEN). URL: https://www.commoncriteriaportal.org/files/ppfiles/pp0072b_pdf.pdf.

[40] *Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted communication with signature creation application*. prEN 14169-6:2013. European Committee for Standardization (CEN). URL: https://www.commoncriteriaportal.org/files/ppfiles/pp0076b_pdf.pdf.

[41] Wolfgang Rankl and Wolfgang Effing. *Smart Card Handbook*. 4th ed. Chichester, West Sussex, England ; Hoboken, NJ, USA: J. Wiley, 2010. 1088 pp. ISBN: 978-0-470-74367-6. DOI: 10.1002/9780470660911.

[42] *Rapport de certification ANSSI-CC-2020/50 – IAS ECC v2, version 1.3 in configuration #1 on ID-One Cosmo v8.2 open platform*. ANSSI-CC-2020/50. Agence nationale de la sécurité des systèmes d'information (ANSSI), 9th July 2020. URL: https://www.commoncriteriaportal.org/files/epfiles/anssi-cc-2020_50fr.pdf.

[43] *Rapport de certification ANSSI-CC-2020/53 – IAS ECC v2, version 1.3 in configuration #4 on ID-One Cosmo v8.2 open platform*. ANSSI-CC-2020/53. Agence nationale de la sécurité des systèmes d'information (ANSSI), 9th July 2020. URL: https://www.commoncriteriaportal.org/files/epfiles/anssi-cc-2020_53fr.pdf.

[44] *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. 910/2014. 28th Aug. 2014. URL: https://eur-lex.europa.eu/eli/reg/2014/910/oj?locale=en.

[45] Henning Richter, Wojciech Mostowski and Erik Poll. 'Fingerprinting Passports'. In: *NLUUG Spring Conference on Security*. 2008.

[46] Henry P. Romero et al. 'Electromagnetic Measurements for Counterfeit Detection of Radio Frequency Identification Cards'. In: *IEEE Transactions on Microwave Theory and Techniques* 57.5 (May 2009), pp. 1383–1387. ISSN: 1557-9670. DOI: 10.1109/TMTT.2009.2017318.

[47] Henry P. Romero et al. 'Identifying RF Identification Cards From Measurements of Resonance and Carrier Harmonics'. In: *IEEE Transactions on Microwave Theory and Techniques* 58.7 (July 2010), pp. 1758–1765. ISSN: 1557-9670. DOI: 10.1109/TMTT.2010.2049773.

[48] Adam Shostack. *Threat Modeling – Designing for Security*. Indianapolis, IN: John Wiley & Sons, Inc., 2014.

[49] *Tehnilised nõuded andmekandja kohta, millele võib kanda digitaalse dokumendi või dokumendi digitaalsed andmed*. RT I, 07.12.2021, 25. 10th Dec. 2021. URL: https://www.riigiteataja.ee/akt/107122021025.