Using the Estonian Electronic Identity Card for Authentication to a Machine (Extended Version)*

Danielle Morgan[1] and Arnis Parsovs[2,3]

[1] Tallinn University of Technology, Tallinn, Estonia
[2] Software Technology and Applications Competence Center, Tartu, Estonia
[3] University of Tartu, Tartu, Estonia
arnis@ut.ee

Abstract. The electronic chip of the Estonian ID card is widely used in Estonia to identify the cardholder to a machine. For example, the electronic ID card can be used to collect rewards in customer loyalty programs, authenticate to public printers and self-checkout machines in libraries, and even unlock doors and gain access to restricted areas.
This paper studies the security aspects of using the Estonian ID card for this purpose. The paper shows that the way the ID card is currently being used provides little to no assurance to the terminal about the identity of the cardholder. To demonstrate this, an ID card emulator is built, which emulates the electronic chip of the Estonian ID card as much as possible and is able to successfully impersonate the real ID card to the terminals deployed in practice. The exact mechanisms used by the terminals to authenticate the ID card are studied and possible security improvements for the Estonian ID card are discussed.

1 Introduction

The state of Estonia issues several types of credit card-sized identity documents that contain a contact-type smart card chip. These are the identity card, the residence permit card, the digital identity card and the e-resident's digital identity card [28]. The common term "ID card" is used in this paper to refer to all these chip cards.

The main purpose of the electronic chip embedded in the ID card is to perform cryptographic operations with two RSA 2048-bit keys stored on the chip. One key is used for authentication and the other for digital signatures. The authentication key can be used to sign TLS client certificate authentication challenges and to decrypt encrypted documents sent to the cardholder, while the digital signature key can be used by the cardholder to create eIDAS-compatible [33] qualified electronic signatures (QES). Cryptographic operations require that the cardholder authenticate using a PIN.

In Estonia, it is a widespread practice to use the ID card as a credential to electronically identify oneself to a machine. Several large merchants in Estonia allow the ID card to be used as a customer loyalty card [7], providing access to rewards once the ID card is inserted in the merchant's terminal. Similarly, the ID card can be used to authenticate to self-service printing machines and self-checkout machines in libraries. Pharmacies use the ID card chip to look up the drugs prescribed using the digital prescription system. In some public and less public security installations the ID card can be used as an entrance card to unlock the door and gain access to restricted areas [6]. Using the ID card is convenient, as every Estonian resident is supposed to have one, and using such a universal identification token means that people do not need to carry around a large number of service provider-specific identification tokens.

---

* This paper is an extended version of a paper from NordSec 2017.

However, one common characteristic observed in this type of identification is that the ID card is authenticated without the cardholder being required to enter a PIN. This means that the cryptographic capabilities provided by the card are not used to authenticate the chip. The card terminal simply reads a cardholder identifier stored on the card and uses it to decide if access to the service should be granted.

This paper studies how the smart card terminals deployed authenticate the ID card chip in practice. This is done by building an ID card emulator, which emulates the chip of the real ID card as much as possible and logs the commands received from the terminal. We discuss the security aspects of using this type of chip authentication and also analyze the risks faced by the cardholder when inserting their ID card in an untrusted terminal. We acknowledge that for certain ID card use cases discussed in this paper, the risk of fraud is so low that a secure authentication solution may not be needed. The analysis of fraud feasibility, however, is not in the scope of this study.

The paper is structured as follows. Section 2 describes the current ID card chip authentication mechanism and the related issues. Section 3 analyzes the security risks faced by the cardholder when inserting their card in a malicious terminal. Section 4 describes the design of the ID card emulator. Section 5 describes the results of using the ID card emulator in the terminals deployed in practice. Section 6 discusses possible improvements to the current card authentication mechanism. Finally, Section 7 concludes the paper.

2 Card Authentication

To identify the cardholder, the terminals deployed in practice read the publicly readable personal data file that resides on the chip of the Estonian ID card. The records contained in the personal data file are shown in Table 1.[4] To read the records, the terminal has to send several Application Protocol Data Unit (APDU) commands to the smart card and read the responses. An example of reading the 5th record (nationality code) from the personal data file is shown in Table 2. In practice, the process of reading the whole personal data file takes half a second.

Table 1. Contents of a personal data file stored on an ID card [34, Sect. 10]

No.	Content	Example	Length (bytes)
1	Surname	ŽAIKOVSKI	Max 28
2	First name line 1	IGOR	Max 15
3	First name line 2		Max 15
4	Sex	M	1
5	Nationality code	POL	3
6	Date of birth	01.01.1971	10
7	Personal ID code	37101010021	11
8	Document number	X0010536	8 or 9
9	Expiry date	13.08.2019	10
10	Place of birth	POOLA / POL	Max 35
11	Date of issuance	13.08.2014	10
12	Permit type		Max 50
13	Notes line 1	EL KODANIK / EU CITIZEN	Max 50
14	Notes line 2	ALALINE ELAMISÕIGUS	Max 50
15	Notes line 3	PERMANENT RIGHT OF RESIDENCE	Max 50
16	Notes line 4	LUBATUD TÖÖTADA	Max 50

[4] The digital identity cards issued before December 2014 only have the document number (field No. 8) filled. These cards will expire by December 2017.

Table 2. APDU commands for reading the 5th record from the personal data file

Command	Command APDU	Response APDU	Description
`SELECT FILE`	00 A4 01 0C 02 EE EE	90 00	Select EstEID DF
`SELECT FILE`	00 A4 02 0C 02 50 44	90 00	Select personal data file
`READ RECORD`	00 B2 05 04 00	61 03	Read 5th record
`GET RESPONSE`	00 C0 00 00 03	50 4F 4C 90 00	Retrieve 3-byte response

For the purpose of identifying the cardholder, the personal ID code (record No. 7) is the best option. The personal ID code does not change during the cardholder's lifetime and is the standard identifier used by Estonian information systems to uniquely identify a person. The personal ID code, however, is not just a unique identifier – it also reveals the person's date of birth, sex, and the district where the code was issued.

2.1 Document Expiration and Revocation Checks

To verify that the card has not expired and is not revoked, the terminal can check the expiry date (record No. 9) and use the document number (record No. 8) to run an online check against the public online document validity service provided by the Estonian Police and Border Guard Board [8]. Alternatively, the terminal can check the validity of X.509 certificates stored on the card using the OCSP service provided by the CA free of charge. However, since the certificates on the card can be revoked without revoking the identity document, the validity status of certificates may not reflect the validity status of the document. For example, the cardholder could have revoked the certificates only to disable the card's cryptographic functionality. On the other hand, in case a card is lost or stolen the validity of certificates is often suspended temporarily in hopes of finding the card later, at which time the suspension can be terminated. The validity life-cycle of the identity document, however, does not allow temporarily suspending the validity of the document.

2.2 Card Impersonation

The data records stored in the personal data file are not cryptographically protected, therefore the terminal has to trust that the data received has not been modified and is read from an authentic ID card. With cheap programmable smart cards available on the market, this assumption of trust does not hold in practice. In Sect. 4 we demonstrate the design of a fake ID card chip that is able to trick the terminals into accepting the fake chip as a genuine ID card, and respond to the terminal with arbitrary data contained in the personal data file. This makes the schemes relying on chip authentication vulnerable to cardholder impersonation attacks.

2.3 Barcodes and Machine-Readable Zone

An alternative method for automated ID card identification is to scan the barcode or the machine-readable zone available on some types of ID cards.

The identity cards and residence permit cards issued since 2011 have two barcodes (see Fig. 1) on the back of the card. The first (topmost) encodes the personal ID code of the cardholder, but the second encodes the document number. The data in the barcodes is encoded using the "Code 128" barcode format. The digital identity cards and the e-resident's digital identity cards have only the barcode encoding of the document number on the back of the card.

All ID cards, except digital identity cards and e-resident's digital identity cards have a machine-readable zone (MRZ) in the travel document "Type 1" format on the back of the card (see Fig. 1). The data in the MRZ encodes the code of the issuing country, the document number, the date of birth, sex, the expiry date, the nationality code and the name of the cardholder. Since the data encoded in the MRZ follows the ICAO standard for machine-readable travel documents, the data does not include the country-specific Estonian personal ID code, not even in the optional fields of the MRZ. Hence, the MRZ on ID cards is not well suited for the purpose of cardholder identification.

Some merchants in Estonia scan the barcode to identify the cardholder (e.g., Euroapteek and Euronics). This type of card authentication may provide better protection against card impersonation, assuming that the operator processing the card performs a thorough card inspection and is able to spot a forged barcode. The focus of this paper, however, is solely on the card authentication methods that interact with the chip of the ID card.

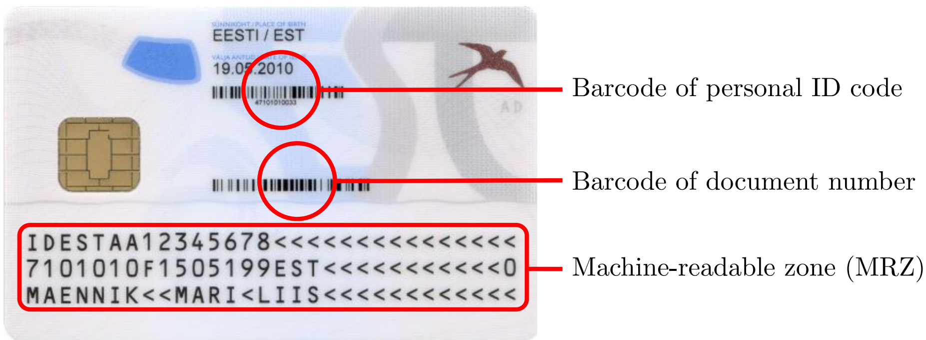


Fig. 1. Back of the identity card (cards issued since 2011) [10]

3 Attacks by Malicious Terminals

The lack of cryptographic assurance in the chip authentication process allows a malicious cardholder to deceive the terminal. However, the cardholder also faces security risks if the ID card is inserted in a malicious terminal. These risks will be discussed in this section.

3.1 Compromising the Cardholder's Privacy

While their personal ID code is the only record needed to identify the cardholder, a malicious terminal can read other records from the personal data file, such as place of birth or information about a residence permit. There may be a legitimate reason for reading the expiry date and document number, if the document expiration and revocation checks are to be performed (see Sect. 2.1). Without the data stored in the personal data file, there is also other publicly readable information available on the chip, such as X.509 public key certificates, private key usage counters and PIN retry counters.

The X.509 certificates stored on the ID card [34, Sect. 13] do not contain any personal information other than the personal ID code and name of the cardholder. The certificates can also be obtained from the public LDAP directory maintained by the CA. Instead of reading the personal data file, the ID code to authenticate the cardholder could be extracted from the certificate. This approach, however, is not used in practice, since it is faster and easier to read a single record from the personal data file. On the other hand, by verifying the signature on the certificate, the terminal could at least obtain a cryptographic assurance that a person with such a name and personal ID code exists.

Private key usage counters [34, Sect. 12.4] show how many private key operations have been performed with a particular private key. The terminal can use this information to find out how active the cardholder is in using the ID card for authentication and digital signatures.

The PIN and PUK code retry counters [34, Sect. 12.2] show the remaining PIN tries, which lets the terminal find out how many times the particular PIN or PUK code has been entered incorrectly. Note that the retry counter is reset to 3 after each successful PIN/PUK verification, and hence these counters are unlikely to have any other value except 3.

Privacy Risk for Residence Permit Card Holders. Residence permit cards are ID cards issued to Estonian residents who are not citizens of the European Union [9]. These cards contain an additional contactless smart card chip that runs the ICAO compliant ePassport application storing digitally signed cardholder data, including biometric data. However, to read that information wirelessly, the terminal has to authenticate to the ePassport chip using the Basic Access Control (BAC) mechanism. To create the BAC key, the reader has to optically read the machine-readable zone (MRZ) and extract the document number, expiration date and date of birth. However, since the fields comprising the BAC key are also stored on the contact chip in the personal data file, a malicious terminal – if equipped with an additional contactless reader – can read the data stored on the ePassport chip without needing to scan the MRZ. The additional personal information that can be obtained this way are the cardholder's facial image and two fingerprints[5].

We note that the reading of the facial image may be useful for the purpose of cardholder verification (see Sect. 6.2), although the wireless reading of 20 KB 480x640 pixel facial image from the residence permit card takes around 15 seconds.

3.2 Denial-of-Service Attacks

A malicious terminal can execute denial-of-service attacks against the card, leaving the card in an impaired state. The most straightforward attack is to decrease the PIN/PUK retry counters to 0. This will block the cardholder's access to cryptographic operations, forcing the cardholder to visit the ID card customer service point to obtain a new PIN envelope. Such a service does not exist for holders of the e-resident's digital identity card, which means that their only option is to apply for a new ID card. Similarly, a malicious terminal can block the GlobalPlatform [12] applet management key, which will prevent the cardholder from renewing the applet in ID card customer service points or over the Internet.

One could argue that these logical denial-of-service attacks against the ID card should not be of concern, since a malicious terminal can always cause damage, for example, by supplying excessive voltage to the electronic chip. In practice, however, the attacker may have gained only a logical control over the terminal, leaving application-level attacks against the smart card the only option available.

3.3 Unauthorized Use of Private Keys

A malicious terminal could also try to perform private key operations by guessing the 4-digit PIN1 protecting the authentication key or the 5-digit PIN2 protecting the digital signature key. The probabilities of guessing a random 4-digit or 5-digit PIN in 3 tries are 0.03% and 0.003%, respectively. In practice, however, the probability of successfully guessing the PIN can be several times higher, since some of the cardholders may have updated the random PIN generated by the card issuer with a PIN of their choice. Bonneau and others in [2, Table 3] show that compared to randomly generated PINs, for human-chosen PINs the probability of successfully guessing a 4-digit PIN increases from 0.03% to 5.52% if 3 guesses are allowed.

[5] Fingerprints on cards issued after 3 November 2014 are additionally protected using the Extended Access Control (EAC) mechanism, which requires terminal authentication.

While this type of an attack has quite a low success probability for a targeted attack, an opportunistic attacker in contact with thousands of cards can succeed in guessing the PIN for some of the cards. Instead of performing 3 guesses per PIN (which will cause the PIN to be blocked), the attacker can perform only one try per PIN. The cardholder is unlikely to notice that after inserting the card in a terminal, the PIN retry counter has decreased. In fact, the malicious terminal can continue the attack once the cardholder returns with the PIN retry counter reset.

Nevertheless, the probability of guessing both PINs for the same cardholder is negligible. Therefore, high-risk transactions should always involve both the authentication as well as the digital signing operation.

4 Design of ID Card Emulator

In this section, we show the design of the ID card emulator that we used in the experiments performed in Sect. 5. The purpose of the ID card emulator is to emulate the chip of a real ID card as closely as possible. Since the private keys from the real chip cannot be extracted, the operations performed with the private keys cannot be emulated. However, as discussed before, for the purpose of card authentication, the emulation of private key operations is not needed. As the experiments will show, in practice the terminals only use the personal data file feature.

To implement ID card functionality in a smart card, a programmable smart card supporting JavaCard technology was chosen. The JavaCard technology allows smart card applications to be written using a subset of the Java programming language. Nowadays, most of the smart cards on the market run applications written using the JavaCard technology. The Estonian ID cards issued starting from 2011 also use the JavaCard technology to implement the required functionality. The source code of the EstEID JavaCard applet, which is installed on the ID cards in the card personalization stage, is the intellectual property of the card personalizer Trüb Baltic AS and is not public [4]. However, a detailed specification for terminal and chip communication is provided in [34] and [35]. Furthermore, there is an open source implementation of the EstEID applet called FakeEstEID [22], on which we based our ID card emulator. The FakeEstEID applet was modified to implement the APDU command logging functionality, add support for the arbitrary applet application identifier (AID), implement the `GET RESPONSE` emulation for T=0 Case 2 APDUs, and to emulate the EstEID v3.5 personal data file format.

4.1 Card ATR Adjustment

Whenever the power or the reset signal is supplied to a card, the card responds with a sequence of bytes called Answer To Reset (ATR). These bytes identify communication parameters supported by the card and may contain historical bytes that typically hold some kind of a card identifier. Several generations of Estonian ID cards in circulation respond with different ATRs. Each generation of ID card responds with two different ATRs, cold and warm ATR, depending on whether the power or the reset signal has been supplied to the card.

Since the ATR returned by the card can be used by the terminal to verify if the inserted card is the Estonian ID card, the ID card emulator had to be adjusted to respond with the ATR of the real ID card. The historical bytes of ATR can be changed within the applet using the JavaCard API call `GPSystem.setATRHistBytes()`. However, the ATR prefix, which encodes the electrical communication parameters of the card, cannot be changed. The solution was to find a blank JavaCard whose ATR prefix would match the prefix of the Estonian ID card.

Fortunately, a blank JavaCard "G&D SmartCafe Expert 6.0 80K Dual" [11] sold for under 15 pounds in small quantities by a UK-based seller [32] was found to have the ATR[6] whose ATR

[6] `3B FE 18 00 00 80 31 FE 45 53 43 45 36 30 2D 43 44 30 38 31 2D 6E 46 A9` (ATR of SmartCafe Expert 6.0).

prefix `3B F? 18 00 00 80 31 FE 45` matched the ATR prefix of Estonian identity cards issued since 2011. Since this blank JavaCard returns a single ATR value for both the cold and warm ATR, we chose to configure the ID card emulator to respond with the cold ATR[7] of the Estonian identity card version issued from October 2014. The inability to emulate both ATRs at the same time is a deficiency of our ID card emulator. The terminals deployed in practice, however, are unlikely to validate both ATRs.

4.2 APDU Logging Functionality

The purpose of the APDU logging functionality is to study how the terminals deployed in practice interact with the ID cards. The logging functionality of the emulator applet writes the received APDU commands on the card's EEPROM storage and later releases them when a specific command is received.

Since in the JavaCard each APDU received from the terminal is passed to the selected applet's `process()` method, this method is the central place where all the APDU commands received are logged. The smart card technology allows several applications to reside on one card; however, only one applet on the card can be set as the implicitly selected (default) applet. To communicate with another applet, an explicit `SELECT FILE` APDU has to be sent, specifying the application identifier (AID) for the applet that should be selected. For the ID card emulator, the emulator applet is set as the default applet. This means that all the commands, including applet selection commands containing non-existent AIDs, will be received and logged by the emulator applet. In addition to logging the received APDUs, the emulator applet logs invocations of the applet's `select()` and `deselect()` methods.

The applet's `select()` method is invoked automatically when the first APDU is received from the terminal and before it is passed to the applet's `process()` method. The logging of `select()` invocation allows detecting if the card has been reset in the middle of an APDU trace. Note that if the terminal powers up the card just to read the ATR, this fact will not be logged, because the `select()` method is invoked only when the first APDU is to be processed. Since the smart card does not have a built-in clock, the timing of the APDUs received cannot be logged either.

The Estonian ID card being emulated supports both electrical transport protocols T=0 and T=1 defined by ISO 7816. To find out which communication protocol the terminal prefers, the applet's `select()` method logs the protocol used in the communication. The protocol used is obtained using the `APDU.getProtocol()` JavaCard API call.

The invocation of the applet's `deselect()` method is also logged. This method is invoked whenever the terminal selects the emulator applet or some other applet residing on the card. The possibility that the applet's deselection is caused by the terminal's explicit selection of the emulator applet itself can be ruled out, because the AID of the emulator applet is set to a random value. The only other selectable applet on the card is the Issuer Security Domain (ISD) with the standard AID `A000000003000000`, which is used for GlobalPlatform's [12] applet management purposes. A legitimate terminal should not communicate with the ISD. However, if it does, this fact is logged and detected.

From the 80 KB of the card's total EEPROM size, a 4 KB memory buffer was allocated to store logged APDU commands. The amount allocated is more than enough to store the APDU trace of a usual interaction between terminal and card.

[7] `3B FA 18 00 00 80 31 FE 45 FE 65 49 44 20 2F 20 50 4B 49 03` (cold ATR of EstEID v3.5 (10.2014)).

4.3 Visual Imitation of ID Card

Since we wanted to avoid drawing attention to our fake ID card when it was used in supervised terminals, the white blank of the fake ID card had to be disguised to imitate the design of the real ID card. To avoid the potential legal problems associated with imitating a physical identification document, we decided to imitate the visual design of the digital identity card. The digital identity card does not serve the purpose of physical identification and hence has neither a facial image nor any security features on it.

We used a scanner to scan the original digital identity card and printed the scan on a sticker paper, which was then glued onto both sides of the fake ID card. Visually, the results were not bad, but the added layer created issues when the card was inserted into some terminals and the paper got wet and dirty very fast. A much better result was obtained using the Zebra ZXP Series 3 card printer to print the scanned image on both sides of the white plastic.

Chip Transplantation. A perfect visual imitation of the real ID card could be obtained if the chip from the fake ID card was transplanted onto the plastic of the real ID card. This way even a thorough inspection of the card's security features along with the verification of the cardholder's facial image would give no signs that the card's electronic communication was inauthentic. The only way to detect the inauthentic behavior of the card would be to compare the data read from the chip with the data printed on the surface of the card.

Since we did not wish to experiment with a real identity card, we tested the feasibility of chip transplantation using the ID card test cards obtained from SK ID Solutions AS [31]. The test card fully replicates the visual appearance of the identity card, including all the security features on it. The only difference from the real identity card is that the test card has the word "SPECIMEN" placed diagonally on the front of the card and the identity information on the card is that of a fictitious cardholder. We removed the fake ID card chip from the white blank card by heating the back of the card with a lighter for a few seconds. To remove the chip from the test card, we used a utility knife to carefully cut out the chip without damaging the plastic around the chip. The fake ID card chip was then glued to the test card. We found the chip transplantation process (Fig. 2) to be straightforward and reliable, and the end result (Fig. 3) had no visible traces of chip replacement other than the different contact pad layout of the fake chip.

Fig. 2. Cards with the chips removed

Fig. 3. Original vs. transplanted card

5 Card Authentication in Practice

To study the exact mechanisms used by the terminals to authenticate a card, we used the ID card emulator in the most popular public deployments where the ID card is used for authentication to a machine. The protocol trace logged by the ID card emulator was later retrieved from the card and analyzed. Each terminal was tested using four slightly different fake ID cards.

1. The first card was a perfect ID card emulator described in Sect. 4. The card was used to test if the terminal accepts the fake ID card and to obtain APDU commands received from the terminal.
2. The second card was the same as the first card, but with the ATR historical bytes set to random values. This card was used to test if the terminal validates the ATR against the list of ATRs for the ID cards in circulation.
3. The third card was the same as the first card, but with a document expiry date that has already passed and an invalid document number. This card was used to test if the terminal performs document validity checks described in Sect. 2.1.
4. The fourth card was used to test if the terminal supports both ISO 7816 electrical transport protocols. If the terminal preferred the T=0 protocol to communicate with the first card, the fourth card was the card with the arbitrary ATR supporting only the T=1 protocol, and vice versa. It is not particular important which protocol the terminal supports, since all ID cards in circulation support both protocols.[8]

The results of the tests are summarized in Table 3. In total 15 terminals were tested from May to July 2017. A more detailed description of the terminals analyzed is documented in the subsections below. The raw APDU traces obtained from the terminals are provided in the Appendix.

As expected, our ID card emulator was accepted by all the terminals tested. This shows that the terminals are vulnerable to card impersonation attacks. The results show that all the terminals perform cardholder identification based on data from the personal data file and not from the certificates. Most of the terminals read more records from the personal data file than required for cardholder identification. While we do not know if the personal data read is retained by the systems, this practice of excessive personal data reading is troubling.

As we can see from Table 3, not all of the terminals check the ATR of the ID card. ATR validation makes ID card forgery more challenging (see Sect. 4.1), however, in the past it has resulted in newer-generation ID cards being rejected temporarily [25]. Our tests with the third card show that none of the terminals tested perform the ID card expiration and revocation checks described in Sect. 2.1. Almost all the terminals support both smart card communication protocols, but T=0 is widely preferred.

Use of ID Cards in Payment Terminals. Using the ID card as a loyalty card is a popular authentication method in Estonia.[9] To avoid the need for a separate smart card reader, the merchants tested in this study communicate with the ID card chip using the point-of-sale (POS) terminal. Support for the ID card has been implemented in the firmware of payment terminals, and the merchant's systems only receive the predefined records of the personal data file. We found three payment terminal models that were used by Estonian merchants to communicate with an ID card. These are: Ingenico iPP320 (Apollo, Apotheka, Grossi Toidukaubad, Olerex), VeriFone Vx805/Vx820 (Lido, Rahva Raamat) and Worldline YOMANI (K-Rauta, Prisma).

[8] The exception is the digital identity cards issued before 2014, which support T=0 only.

[9] For various reasons, not all merchants in Estonia accept the ID card as a loyalty card [24]. These merchants provide their own loyalty cards, which are usually magnetic stripe cards or contactless chip cards [18].

Table 3. The results of using the ID card emulator in terminals deployed in practice

Terminal	Records read	ATR check	Protocol
Apotheka (PC reader)	First nine records	No	T=0 pref.
Apotheka (prescr. lookup)	Name, ID code, doc. No.	No	T=1 pref.
Ektaco ARGOS	Doc. No.	Yes	T=0 pref.
Ingenico iPP320	All records	Yes	T=0 pref.
National Library	All records	No	T=1 pref.
Pilveprint	Doc. No.	No	T=0 only
TUT library entrance	All records	No	T=1 pref.
TUT library checkout	ID code	Yes	T=1 pref.
VeriFone Vx805/Vx820	Name, ID code, doc. No., expiry date	No	T=0 pref.
Worldline YOMANI	ID code, doc. No., expiry date	Yes	T=0 pref.

5.1 Apotheka (PC reader)

The Apotheka pharmacy chain in Estonia unites more than 180 pharmacies under the Apotheka trademark. In addition to the magnetic stripe card offered by the merchant, people can use their ID card as a loyalty card. As an alternative to the payment terminal, the client can insert the ID card in a separate smart card reader connected to the pharmacist's computer. When the card is inserted, the terminal reads the first nine records from the personal data file in a nonconsecutive order. It is odd to see that the first APDU sent to the card is `A0 A4 00 00 02 7F 20`, which is the `SELECT DF.GSM` command from the GSM standard. The APDU traces were collected from Apotheka pharmacies located in Tartu.

Digital Prescription Lookup. The card reader connected to the pharmacist's computer is also used to automate the lookup of drugs prescribed to the patient in the digital prescription system [5]. For the prescription lookup process, the cardholder's surname, first name (both lines) and personal ID code are read from the personal data file. The document number is then read in a loop, probably to detect the insertion of a new card. Just like in the case of using the ID card as a loyalty card, ATR is not verified. However, the digital prescription lookup application establishes T=1 connection to the ID card.

We noted that contrary to the legal requirement, in the process of prescription lookup the pharmacist used our ID card emulator without asking for any physical identification document. However, even if a physical identification document was verified, the identity read from the chip would likely not be verified with the information printed on the card, and thus the chip transplantation (Sect. 4.3) could allow impersonating another person.

5.2 Ektaco ARGOS

The Estonian company Ektaco has developed an ARGOS-series access control system where the ID card can be used as a key. According to Ektaco, by using the DIP switch the system can be configured to authorize door unlocking either using the personal ID code or the document number from the ID card. The access control system does not have the capability to perform document expiry or validity checks. The APDU traces were collected from unsupervised Ektaco terminals installed on the side gate of TTK University of Applied Sciences and the front door of Tudengimaja. As we can see from the traces, both access control systems are configured to use the document number for authorization.

5.3 Ingenico iPP320

Ingenico iPP320 is a payment terminal with personal data file reading functionality implemented by the company Voicecom OÜ. The payment terminal returns to the POS system all personal data file records read from the chip using the PosXML protocol [36, Sect. 2.4.2]. Before reading the personal data file, the terminal performs the EMV application discovery process by sending EMV application selection APDUs to the card. We found that the ID card reading functionality of the terminal was used by the following merchants: Apollo, Apotheka, Grossi Toidukaubad and Olerex.

Apollo is a cinema and bookstore chain with 10 stores in Estonia. In 2005, Apollo was the first merchant in Estonia to accept the ID card as a loyalty card [1]. The APDU traces were collected in the Apollo Lõunakeskus bookstore in Tartu.

Grossi Toidukaubad is a grocery store chain with 54 stores all over Estonia. The ID card can be used in the capacity of a loyalty card as an alternative to the magnetic stripe card offered by the merchant. The APDU traces were collected in the Grossi Toidukaubad store in Tartu.

Olerex is an Estonian oil company that has 80 filling stations across Estonia. The ID card can be used as a loyalty card or as a credit card [27]. To register the ID card as a credit card, a credit agreement has to be digitally signed in the Olerex self-service portal. The registration process requires the cardholder to select a 4-digit PIN, which is stored in the Olerex payment system. The PIN has to be entered in the payment terminal whenever the ID card is used as a credit card (the ID card has to be removed from the terminal before the PIN is entered). The APDU traces for using the ID card as a credit card and as a loyalty card are the same. The APDU traces were collected in the Olerex filling station in Tartu.

5.4 National Library

Libraries in Estonia make heavy use of ID cards for client identification as an alternative to barcode-based library cards [15]. The National Library of Estonia allows the use of the ID card as a library card [20]. A reader has to insert their ID card in a card reader when entering the library. The security guard checks the screen to see if the person has registered as a reader and has access to the library.

5.5 Pilveprint

Pilveprint is a cloud printing service with public printing machines located in educational institutions and libraries all over Estonia. The documents to be printed can be uploaded to the Pilveprint self-service portal. To release and print a document, the user has to insert their ID card in the printing machine. Before they are able to use the ID card in a printing machine, the user has to enter the self-service portal and manually bind the document number of their ID card to their Pilveprint user account. The APDU traces were collected from the printing machine located in the University of Tartu building at Lossi 3.

5.6 TUT Library

The readers of the library of the Tallinn University of Technology can use their ID card as a library card. The reader has to insert their ID card in the smart card reader when entering the library. A librarian supervises this action and a different signal sounds depending on whether or not the inserted ID card is accepted.

The library also has two self-checkout machines that the readers can use to borrow books. The ID card has to be inserted into the machine, after which the barcode of the book can be scanned. The APDU traces were collected from the self-checkout machine located on the second (entrance) floor of the library.

5.7 VeriFone Vx805/Vx820

VeriFone Vx805/Vx820 is a payment terminal with personal data file reading functionality implemented by the company Verifone Baltic SIA. The terminal does not perform ATR verification and the EMV application discovery process is not visible in APDU traces. Because of this, in order to read the ID card the POS system has to be switched to the ID card reading mode. We found that the ID card reading functionality of the terminal was used by the merchants Lido and Rahva Raamat.

Lido is a restaurant and bistro chain with three restaurants in Tallinn. The APDU traces were collected in the Lido Mustamäe Center restaurant.

Rahva Raamat is a bookstore chain with 10 stores in Estonia. The APDU traces were collected in the Rahva Raamat store located in the Tasku Center in Tartu.

5.8 Worldline YOMANI

Worldline YOMANI is a payment terminal with personal data file reading functionality implemented by the company Verifone Finland Oy. Before reading the personal data file the terminal performs the EMV application discovery process. After that, the card is reset and three records from the personal data file are read. We found that the ID card reading functionality of the terminal was used by the merchants K-Rauta and Prisma.

K-Rauta is a chain of construction and home furnishings department stores with eight stores in Estonia. The ID card can be used as a loyalty card as an alternative to the magnetic stripe card offered by the merchant. The APDU traces where collected in the K-Rauta store in Tartu.

Prisma is a hypermarket chain owned by the SOK corporation with eight stores in Estonia. Prisma offers the biggest ID card-based loyalty program in Estonia, which is estimated to be used by at least 150 000 customers. The ID card has to be inserted in the payment terminal. At the end of the EMV application discovery, the terminal attempts to select an unknown AID FFFFFFFFFF0111. The terminal then tries to select AID A0000003790000, which corresponds to the AID of the Finnish S-Etukortti SOK loyalty card used in Finland. The insertion of the card that supports only the T=1 protocol causes the terminal to reboot after the EMV application discovery is performed. The APDU traces were collected in the Prisma Sõbra store in Tartu and a self-checkout terminal of the Prisma Kristiine store in Tallinn.

6 Discussion: Improvements

As demonstrated in the previous sections, the chip authentication mechanism currently used can be abused by a malicious cardholder to execute card impersonation attacks. Using the cryptographic capabilities provided by the current ID cards, while assuring the terminal, would make authentication and digital signature keys open to abuse by a malicious terminal (Sect. 3.3). In this section, we discuss the ID card's possible technological improvements that could improve its security and usability, therefore enabling wider use of the ID card as a physical authentication token.

6.1 Cloning Prevention

To prevent a card impersonation attack, the card authentication process should verify that the unclonable private key objects are on the chip. To achieve this, the terminal should require the card to sign a random challenge and verify it using the certificate. To prevent the abuse of the authentication or digital signature keys, the ID card should contain a separate card authentication key and the corresponding certificate. The key should be used only for card authentication purposes and should be operable without the requirement to enter a PIN. The data in the personal data file or its hash should be embedded in the card authentication certificate to prove its integrity. The validity information of the card authentication certificate should correspond to the validity of the document, thereby enabling reliable document validity checking (Sect. 2.1). This chip cloning prevention feature is similar to the FIPS 201-2 (PIV card) "card authentication key (CAK)" [21], and Active Authentication in the ICAO ePassport [13]. The card authentication feature can be remotely deployed as an additional JavaCard applet on the ID cards that have already been issued. The use of a separate applet provides flexibility, since then the applet will not have to be Common Criteria certified, which is a requirement for applets used to create eIDAS-compatible QESs. To make use of the cryptographic feature, the terminal owners will have to invest in adapting the terminal software. The software, however, will have to be updated to some extent anyway, since the new-generation ID cards (to be issued starting from 2019) will have a new ATR, and due to the eIDAS certification requirements, the EstEID applet will have to be replaced with the internationally developed IAS-ECC applet [23, slide 14]. It is not yet known if it will support the Estonian personal data file feature in its current form.

Performance. To evaluate the performance of the suggested card authentication feature, we performed measurements using two ID card generations in circulation: the chip of ID cards issued since 2011 and the newest-generation chip in ID cards issued since October 2014. The results are shown in Table 4. To summarize, if the ECDSA is used, the cryptographic card authentication process takes around 1.5 seconds on the ID cards issued after 2011, but only 0.6 seconds on the cards issued after October 2014. By utilizing the certificate caching mechanisms, this time could be decreased to be under 200 ms on the latest generation of ID cards. This would considerably improve the user experience when using the ID card as an entrance card.

Table 4. The performance of two ID card chip generations

Measurement	2011 (ms)	2014 (ms)
Reading the personal ID code	150	150
Reading the entire personal data file	625	450
Reading the 1.5 KB certificate	440	380
RSA-2048 signing	1500	385
ECDSA with NIST P-256	1000	160

Relay Attacks. While the card authentication process would prevent the use of ID card forgeries, a more sophisticated relay attack where the fraudulent card relays card authentication commands to the legitimate card is still possible. Relay attacks are not easy to prevent. The EMV contactless payment card specification tries to prevent them using distance bounding protocols, which are far from easy to implement in the actual physical hardware [19].

To some extent, the relay attacks are more applicable to universal credentials such as the ID card, since the terminal-specific authentication tokens are presented and hence accessible only to the owner of the terminal that issued the respective token.

6.2 Cardholder Verification

Verification Using a PIN. Basic protection against the unauthorized use of an ID card by a non-owner of the card can be implemented by requiring cardholder verification using an additional PIN3. In practice, however, the added security value may be too insignificant to compensate for the degraded user experience caused by memorizing and entering yet another PIN. Entering a

PIN into a terminal and in an environment controlled by some third party would also greatly increase the risk of the PIN being compromised. In the EMV payment card rollout in the U.S., banks have chosen to abandon PIN verification, because most fraud cases involve counterfeit cards, while fraud related to lost and stolen cards is minimal [16]. The use of lost or stolen cards can instead be prevented by card revocation mechanisms.

Cardholder verification using a PIN does not prevent fraud where the owner of the card has authorized the use of their ID card by some other person. In some fraud schemes (e.g., in some customer loyalty programs) the owner may have a direct or indirect interest in their card being used by someone else.

Verification Using Biometrics. To completely eliminate the use of an ID card by someone who is not the cardholder, the identity of the card user has to be verified. Due to chip transplantation attacks (Sect. 4.3), not only the facial image printed on the identity document has to be verified, but also the personal ID code retrieved electronically should be compared with the personal ID code printed on the document. To automate the verification task as much as possible, the facial image of the cardholder should be stored on the card, indirectly signed by including its hash in the card authentication certificate. The person performing cardholder verification would then only need to compare the digital image retrieved from the chip with the facial features of the card user. This task could be further delegated to a face recognition system.

A similar feature is already provided by the ePassport chip on the residence permit cards (see Sect. 3.1). Therefore, as an alternative to cryptographic improvements for the ID card chip, all types of ID cards could be equipped with the ICAO ePassport chip. The advantage of this solution would be that an internationally standardized method would then be used for cardholder authentication, and in the case of the Estonian ID card, the BAC key would be read from the contact chip without the need for optical character recognition. The disadvantage would be the need for two readers, which complicates the deployment and slows down the speed of card authentication transactions.

6.3 Contactless Interface

With the exception of the residence permit card, which contains a separate contactless ICAO ePassport chip, the current ID cards in circulation do not have a contactless interface. The potential benefits of adding a contactless interface to the ID card have been discussed in [4,14]. A non-public pilot for using NFC-enabled digital identity cards with mobile phones has been described in [17,26].

While the traditional electronic use of ID cards does not benefit much from a contactless interface (except perhaps to interface with mobile devices), the convenience provided by a contactless interface would be especially useful for using the ID card as an entrance card. This would allow making the terminals more vandal-proof and enhancing the convenience of the process.

However, the introduced security risk is that the cardholder's identifiable information could be retrieved covertly from a distance, and covert access to a PIN-less card authentication key would make relay attacks easier to execute. The security risk could be largely solved by introducing an NFC antenna-enabling button to the card [29]. Cards with such buttons, however, are currently not available on the market. The U.S. Department of Defense, for example, has decided to enable contactless interface for CAC cards, but has issued radio frequency shielding sleeves to cardholders [30].

7 Conclusion

We have shown the design of an ID card emulator able to impersonate a real Estonian ID card to the terminals deployed in practice. Building such an ID card emulator today is both feasible and affordable, and therefore the current ID card chip authentication mechanism, which does not involve any cryptographic assurance, should not be used for high-risk transactions. By demonstrating the reliability of the ID card chip transplantation process, we have shown that the authenticity of the data read from the chip should not be trusted even if the chip is part of a visually authentic ID card.

The study of terminals deployed in practice shows that the terminals do not perform document expiration and revocation checks, and most of the terminals read more personal data from the ID card than required for cardholder identification.

We hope that this paper will raise awareness of the risks related to the current ID card chip authentication mechanism and will facilitate the development of a secure and universal authentication solution. Such a solution is highly needed in the current situation in Estonia where a variety of proprietary solutions vulnerable to cloning and replay attacks are ubiquitous [3,18].

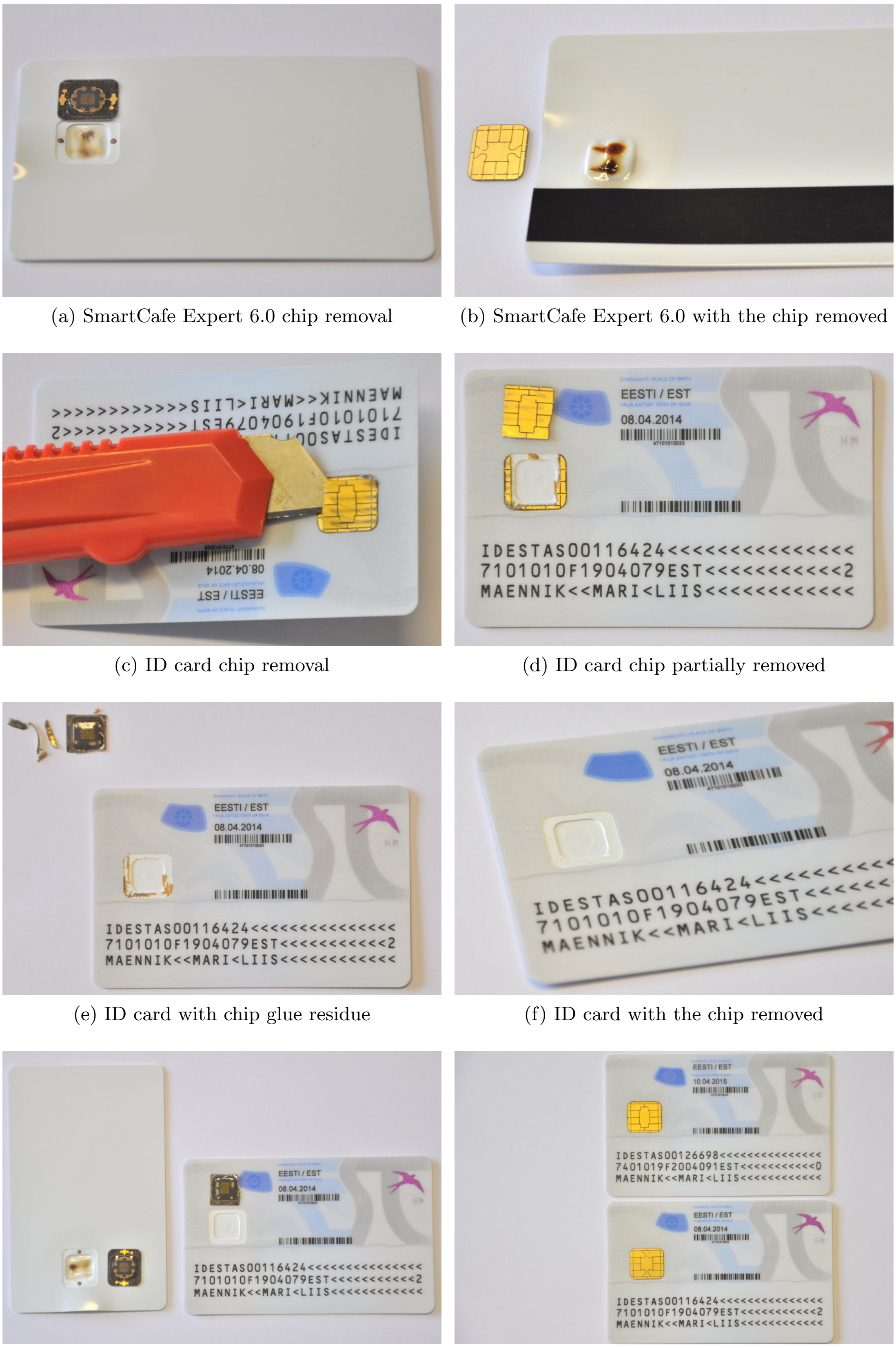
Acknowledgements. We would like to thank Martin Paljak for his feedback and the technical support he provided for this study, and all the people who gave their feedback on this paper. This work was supported by the European Regional Development Fund through the Estonian Centre of Excellence in ICT Research (EXCITE) and the Estonian Doctoral School in Information and Communication Technologies.

References

1. Äripäev: ID-card is used as a loyalty card (in Estonian) (Jun 28, 2006), http://www.aripaev.ee/uudised/2006/06/27/kasuta-kliendikaardina-id-kaarti
2. Bonneau, J., Preibusch, S., Anderson, R.: A birthday present every eleven wallets? The security of customer-chosen banking PINs. In: FC 12: The 16 th International Conference on Financial Cryptography and Data Security (2012), https://doi.org/10.1007/978-3-642-32946-3_3
3. Cybernetica AS: Cryptographic Algorithms Lifecycle Report 2016, chap. Cryptographic protocols over radio connection. (Jun 22, 2016), https://www.ria.ee/public/RIA/Cryptographic_Algorithms_Lifecycle_Report_2016.pdf
4. e-Governance Academy: Study on the functionality of documents in ID-1 format (in Estonian) (Dec 2013), https://www.siseministeerium.ee/sites/default/files/dokumendid/Uuringud/Isikut_toendavad_dokumendid/2013_id-1_formaadis_dokumentide_funktsionaalsuse_uuring.pdf
5. Estonian Health Insurance Fund: Digital Prescription (Jul 2017), https://www.haigekassa.ee/en/digital-prescription
6. Estonian Information System Authority: Electronic Identity Application Guide: ID card as an entrance card (May 2014), https://eid.eesti.ee/index.php/ID_card_as_an_entrance_card
7. Estonian Information System Authority: Electronic Identity Application Guide: Using ID-card as a loyalty card (May 2014), https://eid.eesti.ee/index.php/Using_ID-card_as_a_loyalty_card
8. Estonian Police and Border Guard Board: Online identity document validity check (May 2017), https://www.politsei.ee/en/teenused/inquiries/
9. Estonian Police and Border Guard Board: Residence card (May 2017), https://www.politsei.ee/en/nouanded/residence-card.dot
10. Estonian Police and Border Guard Board: Sample of ID-card issued starting from 01.01.2011 (Jul 2017), https://www.politsei.ee/en/nouanded/dokumentide-naidised/identity-card/identity-cards-issued-since-01012011.dot
11. Giesecke & Devrient: Sm@rtCafé Expert operating systems: Sm@rtCafé Expert 6.0 (Feb 2013), https://www.gd.gd/gd_media/media/en/documents/brochures/mobile_security_2/nb/SmartCafe-Expert.pdf

12. GlobalPlatform Inc.: GlobalPlatform Card Specification, Version 2.1.1 (Mar 2013), http://www.win.tue.nl/pinpasjc/docs/Card%20Spec%20v2.1.1%20v0303.pdf
13. International Civil Aviation Organization: DOC 9303. Machine Readable Travel Documents. Part 11: Security Mechanisms for MRTDs (2015), https://www.icao.int/publications/Documents/9303_p11_cons_en.pdf
14. Joandi, E., Kuusik, A., Tammet, T.: Analysis of potential RFID usage in the context of extending Estonian ID-card (in Estonian) (Jan 2008), https://www.mkm.ee/sites/default/files/rfid_id_analyys_-_koopia.doc
15. Kask, K.: ID card as a customer card: Estonian Libraries Network Consortium Experience (in Estonian) (Oct 18, 2016), http://kliendikaart.publicon.ee/userfiles/RIA/idkaart/Kill_Kask.pdf
16. Krebs, B.: Chip & PIN vs. Chip & Signature (Oct 2014), http://krebsonsecurity.com/2014/10/chip-pin-vs-chip-signature/
17. Lehmann, A.: New Generation of eID Smartcard (Nov 06, 2014), https://sk.ee/upload/files/AK2014_New%20Generation%20of%20eID%20Smartcard_Andreas%20Lehmann.pdf
18. Morgan, D.: Security of Loyalty Cards Used in Estonia. MSc thesis, Tallinn University of Technology (2017), http://kodu.ut.ee/~arnis/loyalty_thesis.pdf
19. Murdoch, S.J.: Do you know what you're paying for? How contactless cards are still vulnerable to relay attack (Aug 2016), https://www.benthamsgaze.org/2016/08/02/do-you-know-what-youre-paying-for-how-contactless-cards-are-still-vulnerable-to-relay-attack/
20. National Library of Estonia: Registration of readers (in Estonian) (Dec 2015), https://www.youtube.com/watch?v=NrouBnYk1dU
21. NIST: FIPS PUB 201-2: Personal Identity Verification (PIV) of Federal Employees and Contractors (Aug 2013), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
22. Paljak, M.: FakeEstEID JavaCard applet (Jan 16, 2015), https://github.com/martinpaljak/esteid-applets/blob/master/docs/FakeEstEID.md
23. Paljak, M.: Off-line ID card (in Estonian) (Oct 18, 2016), http://kliendikaart.publicon.ee/userfiles/RIA/idkaart/Martin_Paljak.pdf
24. Postimees: No plans to connect Kaubamaja Partnercard with ID-card (in Estonian) (Aug 5, 2011), http://www.postimees.ee/521494/partnerkaarti-id-kaardiga-uhendada-ei-kavatse
25. Postimees: The new ID-cards will be refused (in Estonian) (Jan 23, 2015), http://tarbija24.postimees.ee/3067299/uued-id-kaardid-voivad-torkuda
26. Postimees: Contactless Estonian ID-card has been built (in Estonian) (Mar 5, 2016), http://tehnika.postimees.ee/3607697/video-valminud-on-kontaktivaba-eesti-id-kaart
27. Postimees: Gas station chain created credit card capability for ID-card (in Estonian) (Apr 25, 2016), http://tarbija24.postimees.ee/3668981/tanklakett-loi-id-kaardile-krediitkaardi
28. Riigi Teataja: Identity Documents Act (2000), https://www.riigiteataja.ee/en/eli/504112013003/consolide/current
29. Roland, M., Hlzl, M.: Evaluation of Contactless Smartcard Antennas (Jun 2015), https://arxiv.org/abs/1507.06427
30. SecureIDNews: Defense Department order RF shields from National Laminating (Nov 2010), https://www.secureidnews.com/news-item/defense-department-order-rf-shields-from-national-laminating/
31. SK ID Solutions AS: Cards for testing (Jul 01, 2017), https://sk.ee/en/services/testcard/
32. Smartcard Focus: Giesecke & Devrient: SmartCafe Expert 6.0 80K Dual (Apr 11, 2017), https://www.smartcardfocus.com/shop/ilp/id~684/smartcafe-expert-6-0-80k-dual-/p/index.shtml
33. The European Parliament and the Council of the European Union: Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (2014)
34. Trüb Baltic AS: EstEID v3.4 card specification (Jun 11, 2012), http://www.id.ee/public/TB-SPEC-EstEID-Chip-App-v3.4.pdf
35. Trüb Baltic AS: EstEID v3.5 card specification (Mar 14, 2017), http://www.id.ee/public/TB-SPEC-EstEID-Chip-App-v3.5-20170314.pdf
36. Voicecom OÜ: PosXML Protocol Specification v7.1 (2012), https://voicecom.ee/media/filer_public/2013/01/22/vcomt2appl_posxml_71_std.pdf

Appendix A: ID Card Chip Transplantation Process



(a) SmartCafe Expert 6.0 chip removal (b) SmartCafe Expert 6.0 with the chip removed

(c) ID card chip removal (d) ID card chip partially removed

(e) ID card with chip glue residue (f) ID card with the chip removed

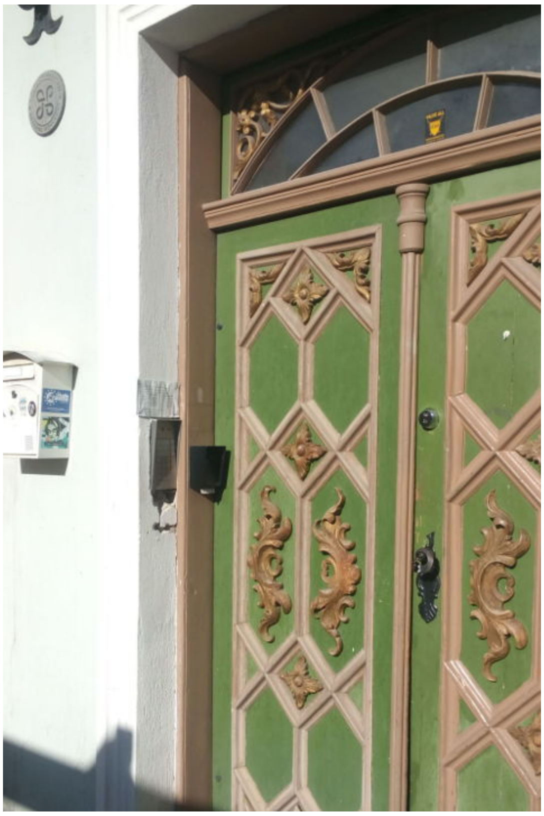
(g) Cards with the removed chips (h) Original (top) vs. transplanted (bottom)

Fig. 4. Chip transplantation process

Appendix B: Some of the Terminals Tested in This Study

(a) Ektaco terminal (Pärnu mnt 62, Tallinn)

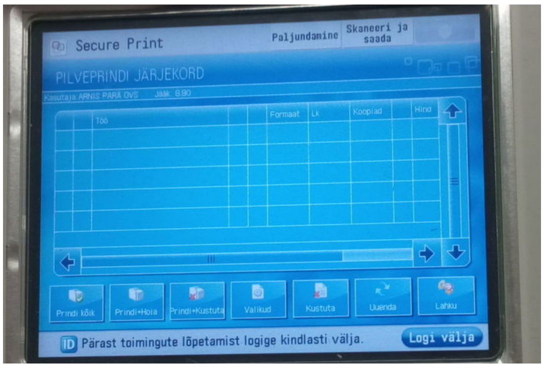
(b) Ektaco terminal (from the inside area)



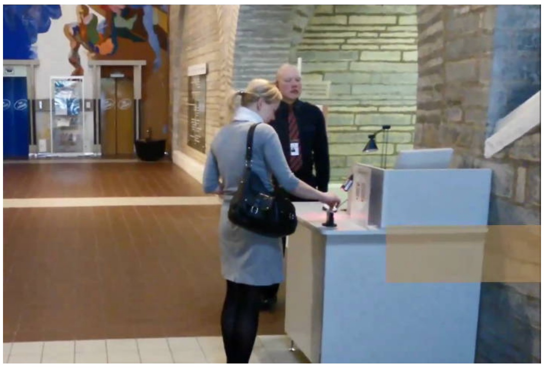
(c) Tudengimaja (Raekoja plats 16, Tallinn)

(d) Tudengimaja Ektaco terminal

(e) Pilveprint printer (Lossi 3, Tartu)

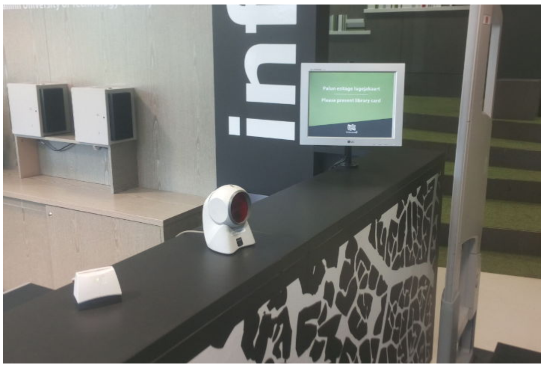


(f) Printer menu for authenticated users

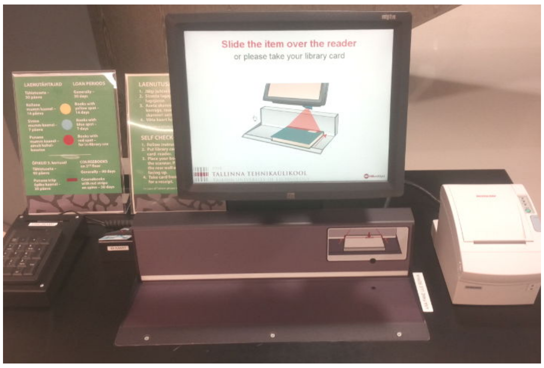


(g) National Library entrance (from [20])

(h) National Library entrance terminal



(i) TUT library entrance terminal



(j) TUT library self-checkout machine

Fig. 5. Some of the tested terminals

Appendix C: Collected APDU Traces

APDU trace 1.1. Apotheka PC reader (loyalty card reading)

```
T=0
A0 A4 00 00 02 7F 20
00 A4 00 0C 00
00 A4 01 0C 02 EE EE
00 A4 02 04 02 50 44
00 B2 07 04 00
00 C0 00 00 0B
00 B2 09 04 00
00 C0 00 00 0A
00 B2 08 04 00
00 C0 00 00 09
00 B2 05 04 00
00 C0 00 00 03
00 B2 04 04 00
00 C0 00 00 01
00 B2 01 04 00
00 C0 00 00 07
00 B2 02 04 00
00 C0 00 00 05
00 B2 03 04 00
00 C0 00 00 01
00 B2 06 04 00
00 C0 00 00 0A
```

APDU trace 1.2. Apotheka PC reader (digital prescription lookup)

```
T=1
00 A4 04 00 0B A0 00 00 03 97 43 49 44 5F 01 00
00 CA 7F 68 00
00 A4 04 00 09 A0 00 00 03 08 00 00 10 00
00 A4 04 00 09 A0 00 00 03 97 42 54 46 59
00 A4 00 0C 00
00 A4 01 0C 02 EE EE
00 A4 02 0C 02 50 44
00 B2 01 04 1C
00 B2 02 04 0F
00 B2 03 04 0F
00 B2 07 04 0B
00 A4 00 08 00
00 A4 00 08 00
00 A4 01 08 02 EE EE
00 A4 02 04 02 50 44
00 B2 08 04 00
00 A4 00 08 00
00 A4 00 08 00
00 A4 01 08 02 EE EE
00 A4 02 04 02 50 44
00 B2 08 04 00
00 A4 00 08 00
```

APDU trace 1.3. Ektaco ARGOS (TTK University of Applied Sciences, Tudengimaja)

```
T=0
00 A4 01 0C 02 EE EE
00 A4 02 04 02 50 44
00 B2 08 04 00
00 C0 00 00 09
```

APDU trace 1.4. Ingenico iPP320 (Apollo)

```
T=0
00 A4 04 00 0E 31 50 41 59 2E 53 59 53 2E 44 44 46 30 31
00 A4 04 00 06 A0 00 00 00 25 01
00 A4 04 00 07 A0 00 00 00 03 20 20
00 A4 04 00 07 A0 00 00 00 04 10 10
00 A4 04 00 07 A0 00 00 00 04 30 60
00 A4 04 00 07 A0 00 00 00 03 10 10
00 A4 04 00 07 A0 00 00 00 03 20 10
00 A4 01 0C 02 EE EE
00 A4 02 04 02 50 44
00 B2 01 04 00
00 C0 00 00 07
00 B2 02 04 00
00 C0 00 00 05
00 B2 03 04 00
00 C0 00 00 01
00 B2 04 04 00
00 C0 00 00 01
00 B2 05 04 00
00 C0 00 00 03
00 B2 06 04 00
00 C0 00 00 0A
00 B2 07 04 00
00 C0 00 00 0B
00 B2 08 04 00
00 C0 00 00 09
00 B2 09 04 00
00 C0 00 00 0A
00 B2 0A 04 00
00 C0 00 00 0A
00 B2 0B 04 00
00 C0 00 00 0A
00 B2 0C 04 00
00 C0 00 00 01
00 B2 0D 04 00
00 C0 00 00 17
00 B2 0E 04 00
00 C0 00 00 13
00 B2 0F 04 00
00 C0 00 00 1C
00 B2 10 04 00
00 C0 00 00 0F
```

APDU trace 1.5. Ingenico iPP320 (Apotheka, Grossi Toidukaubad, Olerex)

```
T=0
00 A4 04 00 0E 31 50 41 59 2E 53 59 53 2E 44 44 46 30 31
00 A4 04 00 07 A0 00 00 00 03 10 10
00 A4 04 00 07 A0 00 00 00 03 20 10
00 A4 04 00 07 A0 00 00 00 03 20 20
00 A4 04 00 07 A0 00 00 00 04 10 10
00 A4 04 00 07 A0 00 00 00 04 30 60
00 A4 04 00 05 A0 00 00 00 25
00 A4 01 0C 02 EE EE
00 A4 02 04 02 50 44
00 B2 01 04 00
00 C0 00 00 07
00 B2 02 04 00
00 C0 00 00 05
00 B2 03 04 00
00 C0 00 00 01
00 B2 04 04 00
00 C0 00 00 01
00 B2 05 04 00
00 C0 00 00 03
00 B2 06 04 00
00 C0 00 00 0A
00 B2 07 04 00
00 C0 00 00 0B
00 B2 08 04 00
00 C0 00 00 09
00 B2 09 04 00
00 C0 00 00 0A
00 B2 0A 04 00
00 C0 00 00 0A
00 B2 0B 04 00
00 C0 00 00 0A
00 B2 0C 04 00
00 C0 00 00 01
00 B2 0D 04 00
00 C0 00 00 17
00 B2 0E 04 00
00 C0 00 00 13
00 B2 0F 04 00
00 C0 00 00 1C
00 B2 10 04 00
00 C0 00 00 0F
```

APDU trace 1.6. National Library

```
T=1
00 A4 01 0C 02 EE EE
00 A4 02 04 02 50 44
00 B2 01 04 1C
00 B2 02 04 0F
00 B2 03 04 0F
00 B2 04 04 01
00 B2 05 04 03
```

```
00 B2 06 04 0A
00 B2 07 04 0B
00 B2 08 04 09
00 B2 09 04 0A
00 B2 0A 04 23
00 B2 0B 04 0A
00 B2 0C 04 32
00 B2 0D 04 32
00 B2 0E 04 32
00 B2 0F 04 32
00 B2 10 04 32
```

APDU trace 1.7. Pilveprint

```
T=0
00 A4 01 04 02 EE EE
00 A4 02 04 02 50 44
00 B2 08 04 00
00 C0 00 00 09
```

APDU trace 1.8. TUT library entrance

```
T=1
00 A4 01 0C 02 EE EE
00 A4 02 04 02 50 44
00 B2 01 04 1C
00 B2 02 04 0F
00 B2 03 04 0F
00 B2 04 04 01
00 B2 05 04 03
00 B2 06 04 0A
00 B2 07 04 0B
00 B2 08 04 09
00 B2 09 04 0A
00 B2 0A 04 23
00 B2 0B 04 0A
00 B2 0C 04 32
00 B2 0D 04 32
00 B2 0E 04 32
00 B2 0F 04 32
00 B2 10 04 32
```

APDU trace 1.9. TUT library self-checkout

```
T=1
00 A4 00 0C 80
00 A4 01 0C 02 EE EE
00 A4 02 04 02 50 44
00 B2 07 04 00
```

APDU trace 1.10. VeriFone Vx805/Vx820 (Lido, Rahva Raamat)

```
T=0
00 A4 04 0C 0F D2 33 00 00 00 45 73 74 45 49 44 20 76 33 35
00 A4 00 0C 00
```

```
00 A4 01 0C 02 EE EE
00 A4 02 04 02 50 44
00 B2 08 04 00
00 C0 00 00 09
00 B2 02 04 00
00 C0 00 00 05
00 B2 01 04 00
00 C0 00 00 07
00 B2 09 04 00
00 C0 00 00 0A
00 B2 07 04 00
00 C0 00 00 0B
```

APDU trace 1.11. Worldline YOMANI (K-Rauta)

```
T=0
00 A4 04 00 0E 31 50 41 59 2E 53 59 53 2E 44 44 46 30 31
00 A4 04 00 07 A0 00 00 00 03 10 10
00 A4 04 00 07 A0 00 00 00 03 20 10
00 A4 04 00 07 A0 00 00 00 03 20 20
00 A4 04 00 07 A0 00 00 00 04 10 10
00 A4 04 00 07 A0 00 00 00 04 30 60
CARD RESET
T=0
00 A4 01 0C 02 EE EE
00 A4 02 04 02 50 44
00 B2 07 04 00
00 C0 00 00 0B
00 B2 08 04 00
00 C0 00 00 09
00 B2 09 04 00
00 C0 00 00 0A
```

APDU trace 1.12. Worldline YOMANI (Prisma)

```
T=0
00 A4 04 00 0E 31 50 41 59 2E 53 59 53 2E 44 44 46 30 31
00 A4 04 00 07 A0 00 00 00 03 10 10
00 A4 04 00 07 A0 00 00 00 03 20 10
00 A4 04 00 07 A0 00 00 00 03 20 20
00 A4 04 00 07 A0 00 00 00 04 10 10
00 A4 04 00 07 A0 00 00 00 04 30 60
00 A4 04 00 07 FF FF FF FF FF 01 11
00 A4 04 00 07 A0 00 00 03 79 00 00
CARD RESET
T=0
00 A4 01 0C 02 EE EE
00 A4 02 04 02 50 44
00 B2 07 04 00
00 C0 00 00 0B
00 B2 08 04 00
00 C0 00 00 09
00 B2 09 04 00
00 C0 00 00 0A
```