TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Danielle Melissa Morgan 156334IVCM

SECURITY OF LOYALTY CARDS USED IN ESTONIA

Master's thesis

Supervisor:	Rain Ottis
	PhD
Co-Supervisor:	Arnis Paršovs
	MSc

Tallinn 2017

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Danielle Melissa Morgan 156334IVCM

EESTIS KASUTATAVATE KLIENDIKAARTIDE TURVALISUS

Magistritöö

Juhendaja:	Rain Ottis
	PhD
Kassjuhendaja:	Arnis Paršovs
	MSc

Tallinn 2017

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Danielle Melissa Morgan

18.05.2017

Tallinn 2017

Abstract

This thesis identifies the card technologies used in loyalty programs across Estonia. These technologies include magnetic-stripe cards, contactless cards (in the form of MIFARE Classic, MIFARE Ultralight, MIFARE DESFire EV1 and low frequency RFID cards) and a smart card known as the Estonian electronic identification card (ID card). Each card type implements its own security features to prevent cloning and/or unauthorized access to the content stored on the card. The contents of each card was read and the method in which it was used in the system analysed. In the cases where possible a clone of the card was created and tested against the real system to verify that it passed the authentication procedures. In the case of the Estonian ID card, a clone of the card was created to log the protocol queries sent by merchant terminals to the card. The study finds that due to the lack of security mechanisms in the technology used, in the majority of cases the loyalty cards provide limited or no protection against card cloning attacks, which makes the loyalty schemes vulnerable to fraud.

Keywords: RFID, NFC, EstEID, Estonian ID card, card technology, loyalty card

This thesis is written in English and is 76 pages long, including 5 chapters, 41 figures and 22 tables.

Abstract

Eestis Kasutatavate Kliendikaartide Turvalisus

Magistritöö eesmärk on uurida erinevaid tehnoloogiaid, mida kasutatakse Eesti ettevõtete kliendikaartide puhul. Uuritud tehnoloogiate loetelu hõlmab järgnevaid kaarituüpe: magnetribaga kaardid, NFC MIFARE Classic, Ultralight ja DESFire tüüpi kaardid, madalsagedusel RFID kaardid ning Eesti elektrooniline isikutunnistus (ID-kaart). Igal kaardil on oma turvaelemendid, mis peaksid takistama kaardi kopeerimist ja/või autoriseerimata ligipääsu kaardile salvestatud andmetele. Töö käigus loeti kaartidele salvestatud infot ning analüüsiti viise, kuidas seda infot boonus-süsteemis kasutatakse. Kloonimist võimaldavatest kaartidest tehti koopia ning testiti seda reaal-süsteemide vastu, et veenduda, kas kloonid läbivad autentimise protseduuri edukalt. Eesti ID-kaardi puhul loodi kloon, mis logiks teenusepakkuja terminali poolt saadetavaid protokolli päringuid. Magistritöö tulemusena tuvastati, et puudulike turvamehhanismide tõttu pole enamik kliendikaarte piisavalt kindlustatud kloonimisrünnakute vastu, mis tähendab, et püsikliendi boonus-programmid on petuskeemide poolt haavatavad.

Märksõnad: RFID, NFC, EstEID, Eesti ID-kaart, kaarditehnoloogia, kliendikaart

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 76 leheküljel, 5 peatükki, 41 joonist, 22 tabelit.

List of abbreviations and terms

3DES	Triple Data Encryption Standard
APDU	Application Protocol Data Unit
ATR	Answer to Reset
CBC	Cipher-Block Chaining
DoS	Denial-of-service
EEPROM	Electrically Erasable Programmable Read-Only Memory
ID	Identification
IEC	International Electrotechnical Commission
ISIC	International Student Identity Card
ISO	International Organization for Standardization
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
PAN	Primary Account Number
QR	Quick Response
RFID	Radio Frequency Identification
RSA	Rivest-Shamir-Adleman cryptosystem
SHA-1	Secure Hash Algorithm 1
TTU	Tallinn University of Technology
UID	Unique Identifier
UT	University of Tartu

Table of Contents

List of Figures

List of Tables

1 Introduction

In Estonia, various merchants have implemented customer loyalty schemes to provide repeat customers with benefits and discounts. To identify the customer, merchants have implemented various card technologies and provide these cards as loyalty cards to their customers. This study seeks to determine what card technologies are used to implement loyalty cards and how they are used in the loyalty scheme. Magnetic-stripe cards, contactless cards (in the form of MIFARE Classic, MIFARE Ultralight, MIFARE DESFire EV1 and low frequency RFID cards) and the Estonian ID card were identified as the main cards used for implementing loyalty schemes.

In this study the contactless public transportation cards are also analysed. While these cards do not fall directly under the category of loyalty cards, they are included in the study as they are still access tokens used to identify the customer.

Currently there have been no comprehensive studies done on the technology used for loyalty cards in Estonia. There is research done about security issues with the MIFARE card technology used in NFC cards, however, this thesis aims to study how the technology is deployed in the loyalty programs provided by Estonian merchants. To highlight the related work done in the context of Estonia, the work of Martin Paljak in documenting the scheme used for the Tallinn public transportation card [16] should be mentioned, as well as the Cryptographic Algorithms Lifecycle Report 2016 [21] ordered by Estonian Information System Authority which discusses the security of radio communication protocols, some of which are used for the loyalty cards in Estonia.

As there are many loyalty schemes available, only the most popular schemes were selected for analysis. The security analysis of the loyalty cards mainly focuses on the cloneability aspects of the cards, because in most cases the card along with its benefits is intended to be used only by the card holder himself. In this aspect, the thesis describes how the cloning experiments were executed, what hardware and software was utilized, and what results were obtained. Since some of the attacks against loyalty programs cannot be tested without brute-force attacks that can lead to unauthorized impersonation, they were not tested to avoid ethical and legal issues.

This work can be used to learn about the technology deployed in practice and the security risks associated with its use. The study can also be used by the users of the loyalty cards to be aware of the risks and hence with this knowledge be able to protect themselves and defend their rights in the event of fraud.

The thesis is structured as follows: Chapter 2 describes the magnetic-stripe cards, explains how they are used and what information is stored on the tracks of the cards. Chapter 3 identifies the different types of contactless cards used, explains the contents of the cards and how the information stored is used, details how the security features available are implemented and finally if the card can be successfully cloned. In Chapter 4, the use of the Estonian ID card as a loyalty card is discussed. To determine the information used by merchants to identify a customer, a clone of the Estonian ID is created and is used to log all commands sent to the card.

2 Magnetic-Stripe Cards

The magnetic-stripe card is one of the first card technology used to store machine readable data encoded on a magnetic stripe. A magnetic stripe contains digitally encoded data which can be read by pulling it across a read head and are usually located at the back of the card. The properties of the magnetic stripe, the coding technique and the locations of the magnetic tracks are specified in ISO standard 7811 [1] . The placement of the track on the card along with the standard size properties can be seen in Figure 1.

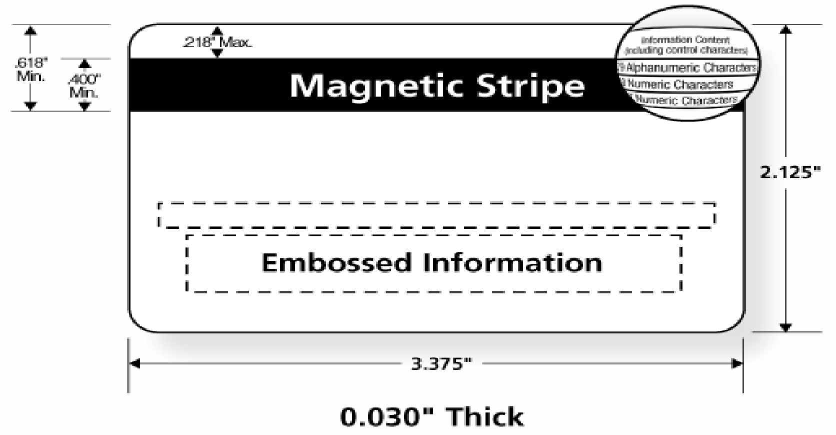
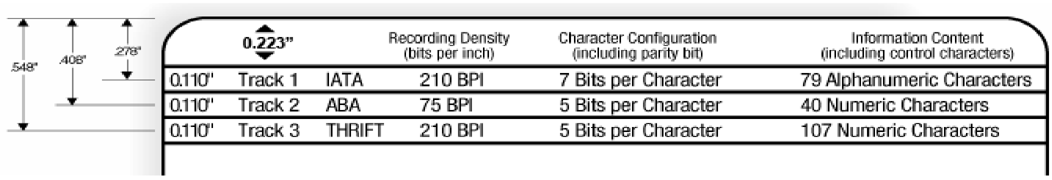


Figure 1. Location of the magnetic stripe on the Magnetic-Stripe Card [2]

The magnetic stripe can contain as many as three tracks, with a storage capacity of more than 1000 bits of data [1] . The number of characters and the number of bits for each character can be seen in Figure 2. As specified by the standard each track is dedicated to storing specific information. Track 1, with a total of 79 alphanumeric characters, stores the account number and the name of the account holder. Track 2, holding 40 numeric characters, stores information relating to the account including the number and expiration date. While Track 1 and 2 are often only used, Track 3 can be used to store additional information but is mostly used in financial transactions.

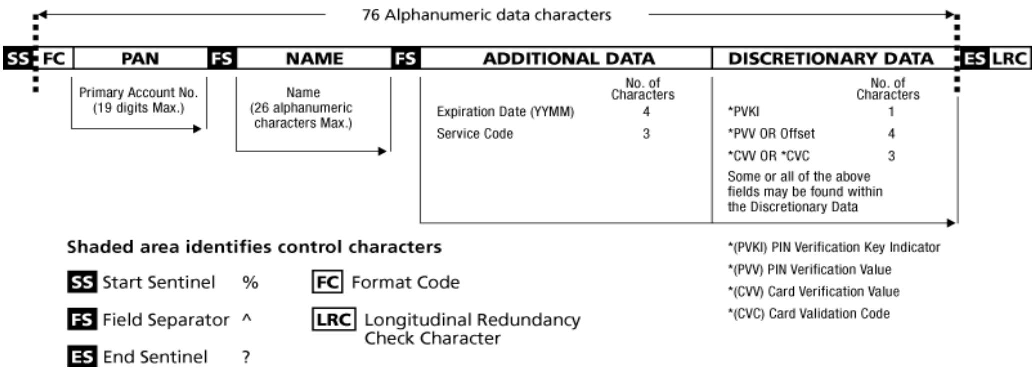


.548"
.408"
.278"
0.223"

			Recording Density (bits per inch)	Character Configuration (including parity bit)	Information Content (including control characters)
0.110"	Track 1	IATA	210 BPI	7 Bits per Character	79 Alphanumeric Characters
0.110"	Track 2	ABA	75 BPI	5 Bits per Character	40 Numeric Characters
0.110"	Track 3	THRIFT	210 BPI	5 Bits per Character	107 Numeric Characters

Figure 2. The Magnetic-Card Track Capacity [2]

In regards to loyalty cards, as opposed to financial cards, magnetic-stripe cards are mainly used for identification, therefore Track 2 is the most used field in practice, with Track 1 and 3 being used on rare occasions. The contents of Track 1, as seen in Figure 3, for typical magnetic-stripe cards are the primary account number with a maximum of 19 digits, the account holder's name (26 alphanumeric characters), expiration (4 characters), service code (3 characters) and discretionary data which can occupy the remaining space. The Longitudinal redundancy check at the end of the track is calculated according to the ISO/IEC 7811-2 standard.



76 Alphanumeric data characters
SS
FC
PAN
FS
NAME
FS
ADDITIONAL DATA
DISCRETIONARY DATA
ES
LRC
Primary Account No. (19 digits Max.)
Name (26 alphanumeric characters Max.)
No. of Characters
Expiration Date (YYMM) 4
Service Code 3
No. of Characters
*PVKI 1
*PVV OR Offset 4
*CVV OR *CVC 3
Some or all of the above fields may be found within the Discretionary Data
Shaded area identifies control characters
SS Start Sentinel %
FS Field Separator ^
ES End Sentinel ?
FC Format Code
LRC Longitudinal Redundancy Check Character
*(PVKI) PIN Verification Key Indicator
*(PVV) PIN Verification Value
*(CVV) Card Verification Value
*(CVC) Card Validation Code

Figure 3. Track 1 Card Data Format for Magnetic-Stripe Cards [2]

The primary account number (PAN), usually adheres to the Luhn Check Algorithm where the last digit of the PAN is calculated using the Luhn formula [3] . The card holder's name follows the format of SURNAME/FIRST and the expiration date follows the format YYMM. Using the above encoding description as a guide and given the information about the card holder Danielle Morgan, with account number 1234 5678 9012 3452 (last digit formatted according to Luhn formula), expiration date May 2018, service code 105 and format code B the Track 1 encoding would be as follows:

%B1234567890123452^DANIELLE/MORGAN
^1805105000000000000000000000000?

Track 2, the most used track for loyalty cards, contains the PAN, expiration date, service code and discretionary data in the format outlined in Figure 4. Using the information from above the Track 2 encoding would appear as follows:

;1234567890123452=18051050000000000000?

In some cases the discretionary data may contain a card validation code or some other identifier the merchant deems necessary to validate the card. The validation information may also be stored on Track 3 in a user-decided format.

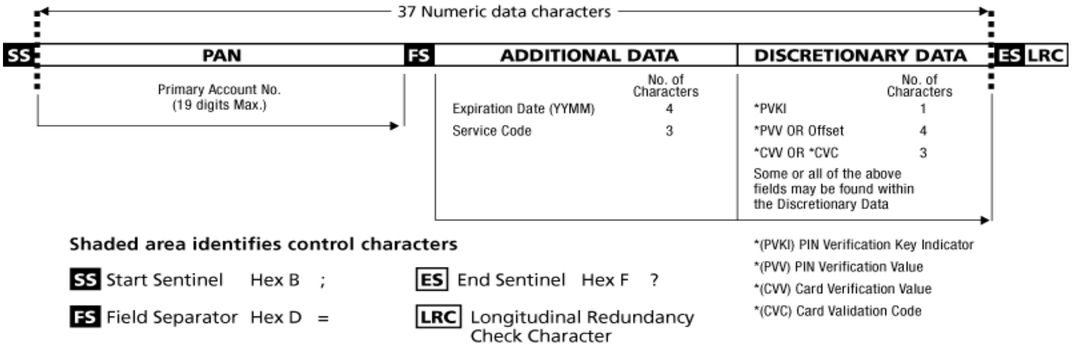

37 Numeric data characters
SS
PAN
FS
ADDITIONAL DATA
DISCRETIONARY DATA
ES
LRC
Primary Account No. (19 digits Max.)
No. of Characters
Expiration Date (YYMM) 4
Service Code 3
No. of Characters
*PVKI 1
*PVV OR Offset 4
*CVV OR *CVC 3
Some or all of the above fields may be found within the Discretionary Data
Shaded area identifies control characters
SS Start Sentinel Hex B ;
FS Field Separator Hex D =
ES End Sentinel Hex F ?
LRC Longitudinal Redundancy Check Character
*(PVKI) PIN Verification Key Indicator
*(PVV) PIN Verification Value
*(CVV) Card Verification Value
*(CVC) Card Validation Code

Figure 4. Track 2 Card Data Format for Magnetic-Stripe Cards [2]

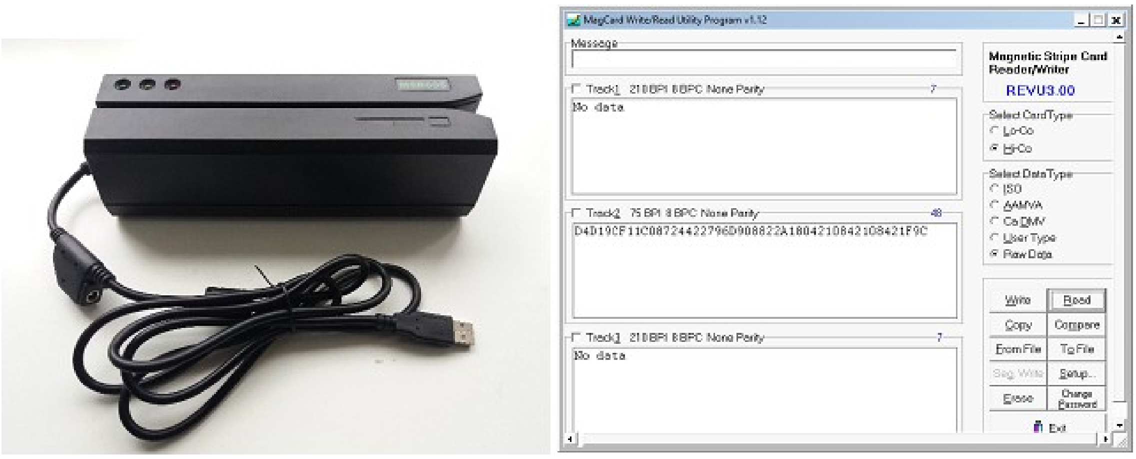
The main disadvantage of magnetic-stripe technology is that the data stored can be easily altered using a standard read/write device and detecting that there has been an alteration can be difficult. In situations where the cards are used in automated systems, such as self-service terminal, a visual inspection of the card cannot be done to detect forgery. A potential criminal having gained valid card data can then duplicate the card and use it in automated machines without having to imitate the card design.

2.1 Methodology

Since the magnetic stripe technology by definition allows data encoded in the stripe to be easily cloned, the investigation into the security measures implemented in the use of magnetic cards as loyalty cards focused mainly on: whether the card could be cloned with the information that was visible on the card or on any receipts gained after proper usage; and whether in the use of the loyalty card the identity of the user was verified to match the identity of the person to whom the card has been issued. The identity verification process, however, may only occur in transactions involving a considerable amount of money, which is hard to determine without access to internal procedures implemented by the merchants. In addition, the information about the price of the card versus the benefits gained from its usage were collected, and whether there was an online solution for the customer to customize or verify any aspects of the card's usage. Another important security check would be to determine if the account numbers assigned to loyalty cards were predictable - for example, if sequential numbers are used. This study, however, does not aim to answer this question, since in order to determine that, the process would require to use the card with modified account numbers, which if done without the account holder's knowledge, may create a legal issue. From a visual inspection of some card numbers, it seems that in some cases predictable sequential numbers are indeed used.

To collect the information described above, the first step was to determine how to acquire the card and what information was required for the process. The second step was applying for the card and receiving the card, which could be delivered to an address or obtained by direct pick up. After gaining the card, it was used as intended to determine the usage and identification process as well as to obtain a receipt from the merchant. Finally, the card data was read using a magnetic stripe reader and an attempt was made to match the information present on the stripe to any information visibly present on the card and/or receipt which would lead to the card be easily cloned using this side information. It should also be noted, that an attacker can follow this same process of acquiring a valid card through the appropriate channels and using it as a starting point instead of trying to imitate the design of the card. The attacker could then replace the account number stored on this card with any other account number seen on other registered cards.

The magnetic stripe reader used in the experiments was the MSR605 3-Track Magnetic Stripe Card Reader Writer Encoder (~80€) and its accompanying software which is shown in Figure 5.



Message

□ Track1 210 BPI 8BPC None Parity 7

```
No data
```

□ Track2 75 BPI 8 BPC None Parity 48

```
D4D19CF11C08724422796D908822A1804210842108421F9C
```

□ Track3 210 BPI 8BPC None Parity 7

```
No data
```

Select CardType
○ Lo-Co
● Hi-Co

Select DataType
○ ISO
○ AAMVA
○ Ca DMV
○ User Type
● Raw Data

(a) (b)

Figure 5. The MSR605 (a) and accompanying software (b)

2.2 Results

The results presented in this section are ordered alphabetically by the name of the loyalty card. The results include: the method of applying for the card and its delivery, the price of the card and its benefits, how the card is used, an image of the card and an analysis of the data stored on the card's tracks.

2.2.1 ABC Card

ABC Loyalty cards are offered by ABC Supermarkets AS and provide customers with discounts at its stores: Delice Food stores at Viimsi Kaubanduskeskus, Pärnu Keskus shopping centres, Solaris Food store at Tallinn Solaris Keskus shopping centre and all Comarket stores[1].

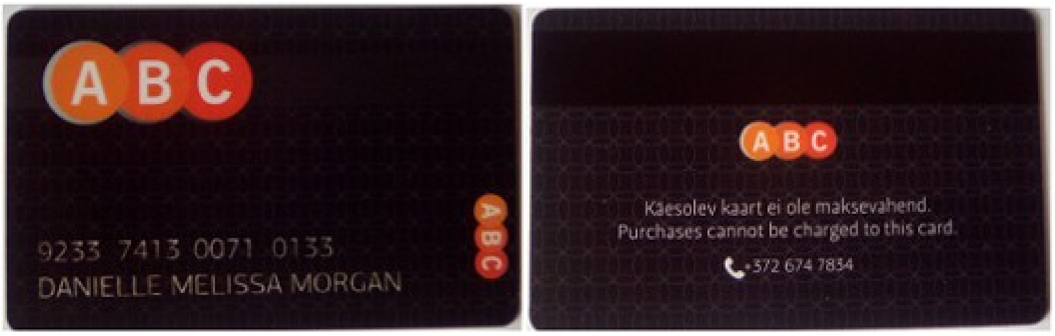
The customer has a choice of 4 cards with each providing a different discount level on regular priced items (the items are not currently discounted). The first card, the ABC Customer card provides the customer with 3% discount and costs 3€ annually. The second card, the ABC Silver Card provides the customer with a 5% discount with a cost of 10€ per year and the third, the ABC Gold Card, provides a 10% discount at a yearly cost of 50€. Both the second and third card apply only to purchases of over 10€. Finally

[1] https://www.abccom.eu/faq

the fourth card, ABC Silver Plus Card for a cost of 30€ per year provides a 5% discount with no purchase limits.

To apply for the card the customer has to fill in an online application form on the company website. To access the self-service portal the user has to log in with either their ID card, Mobile-ID or via their bank. Once the user has successfully logged onto the portal, their name is automatically entered into the application form provided by either their ID card, bank or Mobile-ID. To complete the form a phone number, email address and physical address are required. The user is then allowed to select the desired card, the card selected for this experiment was the ABC Customer card, and the transaction is completed with payment through online banking solutions.

The personalized card is delivered to the address specified within 2 weeks of the application date. Each card has a color scheme associated with its name. The Gold card has a gold background, the Silver card has a dark gray background, the Silver Plus card has a silver background and the Customer card, as seen in Figure 6 uses a black background with white writing. The front of the ABC Customer card (Figure 6 (a)) contains the ABC logo at the top and right side and the card number and customer's name at the bottom. The back of the card (Figure 6 (b)) contains a black magnetic stripe at the top of the card, the ABC logo in the middle and a notice and contact number at the bottom.


ABC
9233 7413 0071 0133
DANIELLE MELISSA MORGAN
ABC
ABC
Käesolev kaart ei ole maksevahend.
Purchases cannot be charged to this card.
+372 674 7834

(a) (b)

Figure 6. The front (a) and back (b) view of the ABC Customer Card

The ABC Customer card utilizes only Track 2 of the magnetic stripe and its contents can be seen in Table 1 in ISO format. The information encoded here include the card number, as seen in Figure 6 (a), in the first field and the second field contains the expiration date (December 2029) and the service code (501).

Table 1. Table showing the ABC Customer Card track information in ISO format

Track	Content
1	No data
2	;9233741300710133=29125010000000000?
3	No data

To use this card the customer presents it to cashier, who swipes it and returns it to the customer. In some cases the customer may be asked to provide proof of identity especially when the higher discounts are applied[1]. After paying, the customer is then handed a receipt of the transaction which shows the customer's loyalty level and the card's expiration date, as seen in Appendix 2 Figure 42, but contains no information about the card number. In addition to allowing for the application of cards, the online self-service portal allows the user to view information on their current card, such as expiration date and number, the transactions including date, time, location, receipt number and price, that have been executed using the card and to update their personal information.

Overall the magnetic stripe on the card is easy to clone as the main data is visually present on the front of the card. The design of the card, however, and the usage method requires that a clone have a high quality print to make it pass a visual and tactile inspection. The lack of personal or card information on the receipt also provides a slightly higher level of security as receipts that are usually discarded without a second thought are of no use to the attacker. A card holder is additionally able to see whether someone has used their card by viewing the online transactions and comparing it with their shopping history. In the event that this occurs, a user is allowed to use the self service portal or other contact methods to replace the lost or stolen card free of cost.

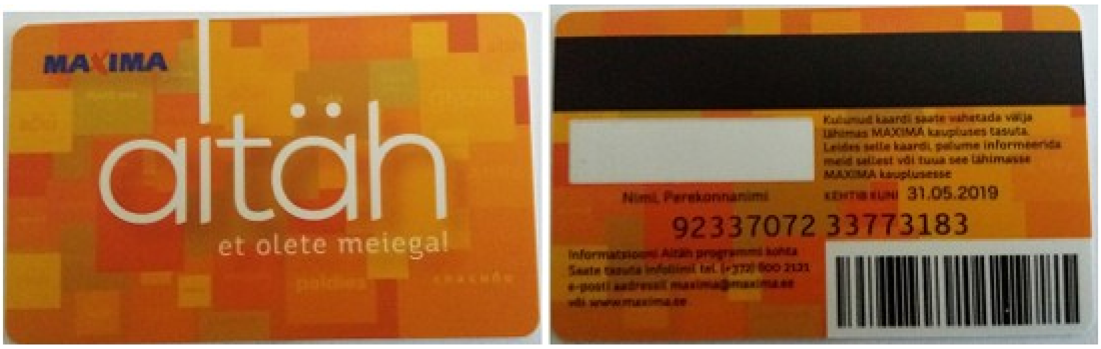
[1] https://www.abccom.eu/faq

2.2.2 Aitäh Card

The Aitäh Loyalty Card is offered by Maixma stores. For a price of 1€, a customer can collect 1% of their purchase in bonus money which can be later used to buy items in Maxima stores as well as gain discounts on special offers[1].

To apply for this card a customer can go to any Maxima stores' information desk and fill out the application form. The information needed are the customer's first and last name, date of birth, phone number, address, email and signature to verify the information and acceptance of terms. The application is then returned to the cashier who registers the card and enters the information into the system. The card can then be used by giving it to the cashier to swipe before paying for purchases or can be used by the customer themselves in the self-service terminals. After this transaction, the customer receives a receipt with the first six and last four digits of the card number presented along with the bonus money acquired, as seen in Appendix 2 Figure 43.

The Aitäh card as seen in Figure 7 uses an orange background with black and white text color scheme. The front of the card (Figure 7 (a)) contains the Maxima and Aitäh card logo while the back of the card (Figure 7 (b)) contains a black magnetic stripe at the top, a field designated for the customer's name, the card's expiration date, the card number, a bar code and information pertaining to the Maxima stores and the Aitäh program.


MAXIMA
aitäh
et olete meiegal
Kulunud kaardi saate vahetada välja lähimas MAXIMA kaupluses tasuta. Leides selle kaardi, palume informeerida meid sellest või tuua see lähimasse MAXIMA kauplusesse
Nimi, Perekonnanimi
KEHTIB KUNI 31.05.2019
92337072 33773183
Informatsiooni Aitäh programmi kohta Saate tasuta infoliinil tel. (+372) 800 2121 e-posti aadressil maxima@maxima.ee või www.maxima.ee

(a) (b)

Figure 7. The front (a) and back (b) view of the Aitäh Loyalty Card

The Aitäh card utilizes only Track 2 of the magnetic stripe. The information can be found in ISO format in Table 2. The information encoded here includes the card number

[1] http://www.maxima.ee/aitah

in the first field and the expiration date in the second field in YYMM format. Both of the fields present on the stripe can be located at the back of the card.

Table 2. Table showing the Aitäh Loyalty Card track information in ISO format

Track	Content
1	No data
2	;9233707233773183=19050000000000000000?
3	No data

The Aitäh card's design of the phrase "Thank you" in several languages embedded in the background of the card is the card's strongest feature against a perfect replica. Taking a picture or scan may not provide enough detail to highlight the fine print on the card. This feature however is only useful when a visual inspection is performed and the use of self-service terminals definitely makes this feature irrelevant. The information encoded on the magnetic stripe is perhaps the feature that can reproduced with the least effort. The card's number is clearly presented on the back in a sizeable font which makes it easy to detect. In addition, while not as large, the card's expiration date can be clearly seen and with this information alone a clone that can be used at the self-service machines can be created. The bar code, decoded as D23377318319057, also contains the last 9 digits of the card number and the expiration date in the format YYMM.

2.2.3 Club One Card

Club One is a Frequent Traveler Program offered by Tallink Silja. Club One customers can accumulate bonus points from ticket and onboard purchases as well as from accommodation in Tallink Hotels. These bonus points can then be later used to book future trips on all Tallink and Silja Line routes. In addition to the bonus points the card can also be used to gain discounts at various other locations such as shops, restaurants, opticians and sports facilities[1].

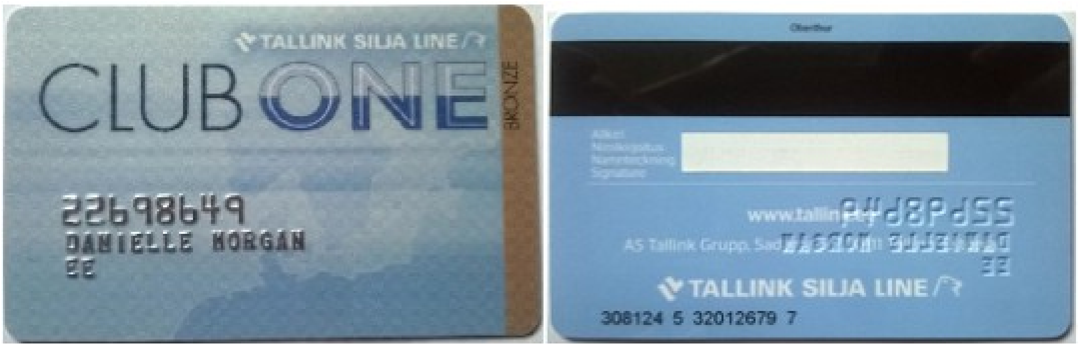
Club One is a three level program: Bronze, Silver and Gold with Bronze being the lowest level and Gold the highest. The main difference between the levels is the number of bonus points gained per euro spent, with Gold producing the most points per euro,

[1] https://www.tallinksilja.com/club-one

and the discounts that are available to the customer. When a customer applies for a card they start at the basic level and can advance to the other levels by gaining a certain level of bonus points (15000 to reach Silver, 60000 to reach Gold) in a 12 month period.

In order to receive a Club One card, a customer must fill in the online form. The requested information includes: first name, family name, birth date, gender, nationality, address, mobile number, email address and optional home and work number[1]. A customer is also then required to create an account, username and password fields which are later emailed in plain text to the client, so that they can track their account and change customer data if necessary. After the application has been submitted the customer receives a personalized card for no charge within a month of the submission date at the address specified in the application.

The Club One Bronze card, as seen in Figure 8, uses a blue background with white text. The front of the card (Figure 8 (a)) has a stripe to the right of the card indicating its level, in this case a bronze stripe. The top of the card contains the Club One and Tallink Silja Line logos. To the left bottom of the card the customer's account number, first and last name and country code are embossed. The back of the card (Figure 8 (b)) contains a black magnetic stripe at the top, a white strip for a signature in the center along with the company's website and logo, and at the bottom left the card number in black is located.



(a) (b)

Figure 8. The front (a) and back (b) view of the Club One Bronze Card

This card breaks the tradition in that the account number, used for online transactions, is not related to the card number, but both however are still printed on the surface of the

[1] https://www.tallinksilja.com/join-club-one

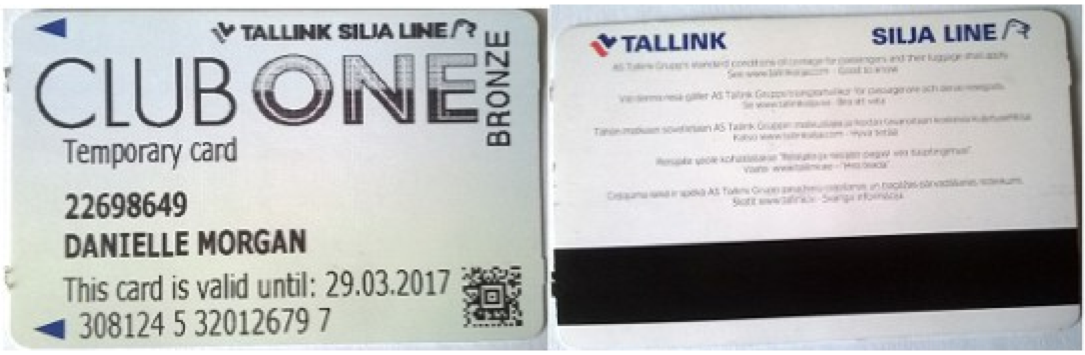
card. The Club One card only utilizes Track 2 of the magnetic stripe and its data in ISO format can be seen in Table 3. The information encoded here is the card number, as presented on the back of the card, in field one and in field two a concatenation of the expiration date (December 2027), service code (777) and discretionary data.

Table 3. The track information available on the Club One Bronze Card in ISO format

Track	**Content**
1	No data
2	;3081245320126797=27127770000040000300?
3	No data

The standard usage of the card in physical cases while on board requires the user to present the card to the cashier before payment so the card can be swiped and bonus points added. On the receipt received, Appendix 2 Figure 44, the card level and number can be found at the top. In the case of online transactions the user is required to enter their account number and first and last name. Entering the user name and account number then allows a person to use their bonus points to pay for trips. The Club One web service, after the user has logged in with username and password, can also be used to change personal information, change login information, transfer bonus points to another Club One member, view reservations and transaction history. Club One also offers a mobile application for Android devices. The information required to log in to this service is the account number and the customer's first and last name as seen on the front of the card. This interface allows the user to book and manage trips but does not allow for the changing of personal data.

In addition to the standard Club One cards, in the event that the client loses the card or forgets it while on a cruise, a temporary card can be ordered from the information desk by presenting the cabin key to the attendant. This card is usually valid for 2 months. The Club One Temporary Card, seen in Figure 9, has the same basic information on its front (Figure 9 (a)) that is present on the real card: account number, name and card number and additionally the expiration date is also present.



(a) (b)

Figure 9. The front (a) and back (b) view of the Club One Temporary Card

The contents of the magnetic stripe of this card can be seen in Table 4 in ISO format. As with the real card, only Track 2 is utilized and the difference between the two lie in the expiration date and the discretionary data differs by only one byte.

Table 4. The contents of the magnetic stripe of the Club One Temporary Card in ISO format

Track	Content
1	No data
2	;3081245320126797=17037770000040000500?
3	No data

Overall, the design of the card is its strongest feature against cloning forgery. However, the fact that all the information necessary to imitate the card can be found on its surface makes writing to the magnetic track easy. The information present also makes using the customer's bonus points to book trips effortless, especially in the case of the mobile application. However, as the customer's name automatically goes on the ticket and email confirmation sent, a person intending to use a customer's points may have to add themselves as a second person, as the standard procedure for checking into the cruise requires the comparing of passports or other identification methods with the data in the system, and to book the trip shortly before the reservation deadline. The temporary card which is probably simply discarded after its expiration date contains valuable information which could lead to the successful making of a cloned card which could allow a person to gain discounts provided by the card. A simple usage case would be a customer with a Bronze card re-writing their track information with that of a customer with a Gold Card. In the event the card is swiped to receive a discount and the cashier does not compare the information on the screen to that on the card, a person would be able to gain discounts of a Gold Card member. These transactions would also not be detected by the real card holder as these are not stored on the Club One system available to card holder in self service portal.

2.2.4 Hesburger Card

Hesburger is a fast food restaurant chain which originated in Finland and has now expanded to 8 other countries, with 42 restaurants located in Estonia alone. The loyalty card offered by Hesburger, provided to the customer for free, has three levels: Silver, Gold and Platinum and a customer can advance to the next level by spending 90€ to reach Gold and 180€ to reach Platinum in 2 consecutive months. The benefits a customer receives from using this card include a free hot beverage and/or a dessert or mayonnaise sauce (level dependent) and bonus points gained on the money spent per month at 2%, 3.5% or 5% for total purchases over 4.39€, 17.49€ and 42.49€ respectively. These bonus points can then be used to purchase goods in all Hesburger restaurants all over Estonia[1].

To apply for the card a customer can fill out an application form[2] stating their first and last name, address, phone, telephone number, date of birth and email address. In addition the customer has to provide a username and password which would allow them to view their account details online. After the card has been ordered, it is delivered to the address specified on the form within 3 weeks of application date.

The Hesburger card (Figure 10) uses a black background and white text color scheme. The front of the card, as seen in Figure 10 (a), has the Hesburger logo in the center and the customer’s first and last name and card number on the front. The back of the card (Figure 10 (b)) has the black magnetic stripe at the top and the registered websites for Hesburger in the Baltic states and Finland.

[1] https://www.hesburger.ee/boonusklubi/boonuskaardi-reeglid

[2] https://www.hesburger.ee/boonusklubi/liituge-boonusklubiga

(a) (b)

Figure 10. The front (a) and back (b) view of the Hesburger loyalty card

The Hesburger card uses only Track 2 of the magnetic stripe. The contents of this track can be seen in ISO format in Table 5. The card number as seen in Figure 10 (a) is encoded in the first field of the track and the second field includes the expiration date (1612, presumably December 2016 but as the card was acquired in 2017 this may be mistake), service code (701) and discretionary data.

Table 5. The track information of the Hesburger Loyalty Card in ISO format

Track	**Content**
1	No data
2	;6009170106791055=16127011000000000100?
3	No data

The standard usage of the card involves the user giving the card to the cashier before paying. The cashier swipes the card, asks the user if they have a desire for any of the bonus products and returns the card. The user then receives a receipt (Appendix 2 Figure 45) that contains the last 8 digits of the card number and the current bonus balance on the card. The day following the purchase the customer is able to log in to the account and view their bonus account balance, bonus level, total visits and purchases in the last 3 months and the bonus account transactions. Additionally in the online environment the user is able to view their card number and change their contact information.

Overall this card presents everything a user needs to clone it on its surface. A user could simply order a card and overwrite the field with their card number with the card number from someone else to obtain their benefits. If the cashier does not ask for photo ID of the person using the card (which is the usual case) and does not compare the name to that on the card, the person may then be able to spend the bonus points of that person.

2.2.5 ISIC Card

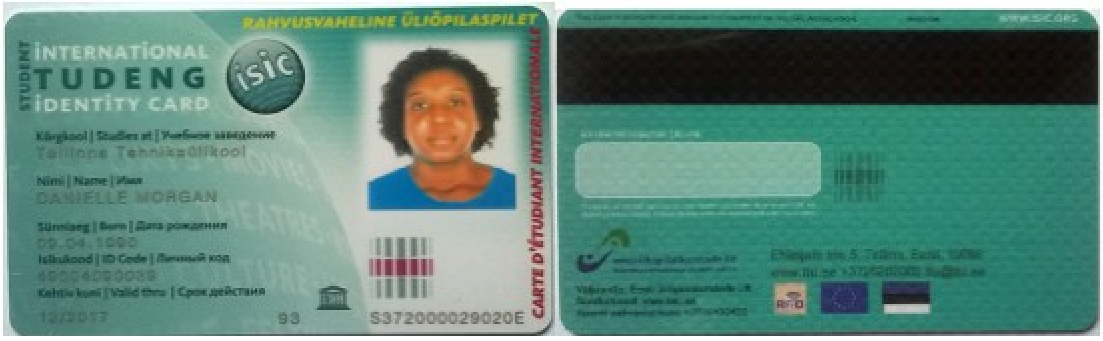
The International Student Identity Card (ISIC) is issued to students and is used to prove their official student status. Through the card a student can gain preferential and discounted access to products, services, and experiences relevant to student life such as software licenses, cinema access, restaurants and public transportation[1].

To apply for this card a student has to submit an application to a local issuer and in the case of Tallinn University of Technology (TTU) students, this would be the Student Union. The application form requires the following information to be completed: first name, last name, name of school (TTU), personal identification number (or passport number), date of birth, email and phone number. After completion the form and a recent photo of the student is then submitted to the Student Union Office along with the payment fee of 2.8€ for a card valid for one year card and 7.9€ for two years on first application and 6.4€ otherwise. The card is available for the student within 10 days and can be collected at the Student Union Office after presenting an identification document or it can delivered to a specified address (on the application form) for an additional fee of 1.1€[2].

The ISIC card (Figure 11) uses a green background and black text color scheme. The front of the card as seen in Figure 11 (a) contains the ISIC logo, the school, name date of birth, personal ID code and photo of the student as well as the card's expiration date and number. The back of the card contains a black magnetic stripe, a signature field and contact information for the ISIC program. This card is also NFC-enabled and its full capabilities are fully discussed in Section 3.5.2.

[1] https://www.isic.org/about-us/

[2] https://ttu.ee/students/university-facilities/student-card-2/


RAHVUSVAHELINE ÜLIÕPILASPILET
STUDENT
INTERNATIONAL
TUDENG
IDENTITY CARD
isic
Kõrgkool | Studies at | Учебное заведение
Tallinna Tehnikaülikool
Nimi | Name | Имя
DANIELLE MORGAN
Sünniaeg | Born | Дата рождения
Isikukood | ID Code | Личный код
Kehtiv kuni | Valid thru | Срок действия
12/2017
93
S372000029020E
CARTE D'ÉTUDIANT INTERNATIONALE
RFID

(a) (b)

Figure 11. The front (a) and back (b) view of the International Student Identity Card

The ISIC card only utilizes Track 2 of the magnetic stripe as seen in Table 6. The information encoded here include the card number in field one and the expiration date in the second field. The expiration date encoded on the stripe matches what is seen on the front of the card in the format of YYYYMM instead of the usual YYMM. The card number, however, does not match what is presented on the front of the card.

Table 6. Track Information for the ISIC card in ISO format

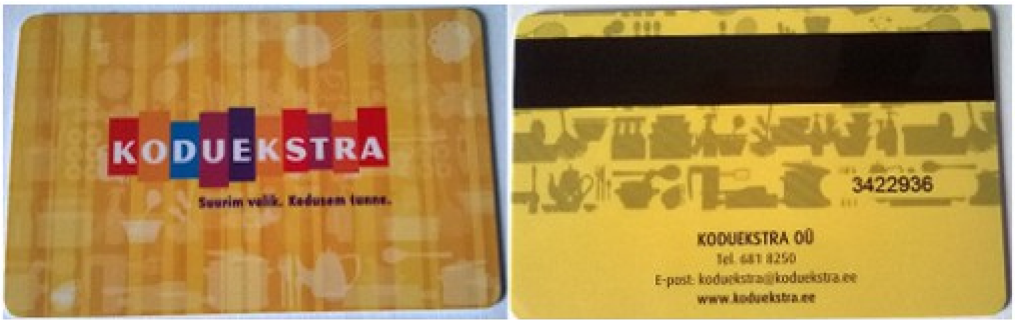
Track	**Content**
1	No data
2	;1702071647000020=20171200000000000000?
3	No data

The ISIC card is mainly used for visual confirmation of student status and for that purpose the magnetic stripe is hardly used. A student can either show the ISIC logo or give the card to the cashier who will verify the image on the document matches the person who is presenting the card. As such, cloning this card may prove to be difficult as the card number is unknown without first swiping it and receipts would generally show an ISIC discount but not the card number to which the discount was provided.

2.2.6 Koduekstra Card

Koduekstra Ltd is a home and household goods retail chain with 26 stores located across Estonia. Koduekstra offers its customers a loyalty card which grants them a 10% discount on all items five days before and after their birthday and access to monthly promotional offers[1]. To acquire this card, customers have to fill out an application form at the cashier's desk which asks for their name, date of birth, address, email address, telephone number, date and signature. The customer's information is then entered into the database, by the cashier, along with the account number that is associated with the card that was chosen from a stack. The card is then given to the customer for a price of 2€ or for free when making a purchase of over 10€.

The Koduekstra card is a non-personalized card which uses a color scheme of a yellow background with black text. The front of the card, pictured in Figure 12 (a), contains the company logo n the center while the back (Figure 12 (b)) contains a black magnetic stripe at the top, the company's contact information at the bottom and the account number to the middle right of the card.


KODUEKSTRA
Suurim valik. Kodusem tunne.
3422936
KODUEKSTRA OÜ
Tel. 681 8250
E-post: koduekstra@koduekstra.ee
www.koduekstra.ee

(a) (b)

Figure 12. The front (a) and back (b) view of the Koduekstra card

The Koduekstra card utilizes one of the three tracks available on the magnetic stripe. Table 7 shows the raw data output that was available for that track. Track 2 contains the card number: a concatenation of the issuer identifier and the account number found on the back of the card, an expiration date (December 2022) and a service code (501).

Table 7. The track information contained on the Koduekstra Loyalty card in ISO format

Track	Content
1	No data
2	;9233727003422936=2212501000000000000?
3	No data

[1] http://www.koduekstra.ee/et/p/kliendikaart

To use this card the customer presents it to cashier, who swipes it and returns it to the customer without any confirmation of identity. After paying, the customer is then handed a receipt, Appendix 2 Figure 46,which contains their name but not the account or card number.

Overall this card can be easily cloned. An attacker, gaining a valid card could replace the account number with the number from another card. By doing this, the attacker can possibly gain a 10% discount every month if customers with varying birth dates are chosen. In addition Koduekstra offers online shopping, where a user, on registration can enter their loyalty card number. A non-card holder could possibly gain the number on the back of the card of a card holder and enter this to gain discounts and access to the monthly specials without having to make a clone of the card.

2.2.7 Partner Card

The Partner Card is a loyalty card which allows the user to collect one bonus point (0.01€) for each euro spent which can be later used to purchase merchandise. This card also gives the user access to discounts and special offers and birthday discounts. Partner Card is offered by Selver supermarkets, Kaubamajas, ILU, ABC King and SHU stores for a price of 1€ and is valid for three years. The card is free for ISIC holders and persons over the age of 65[1].

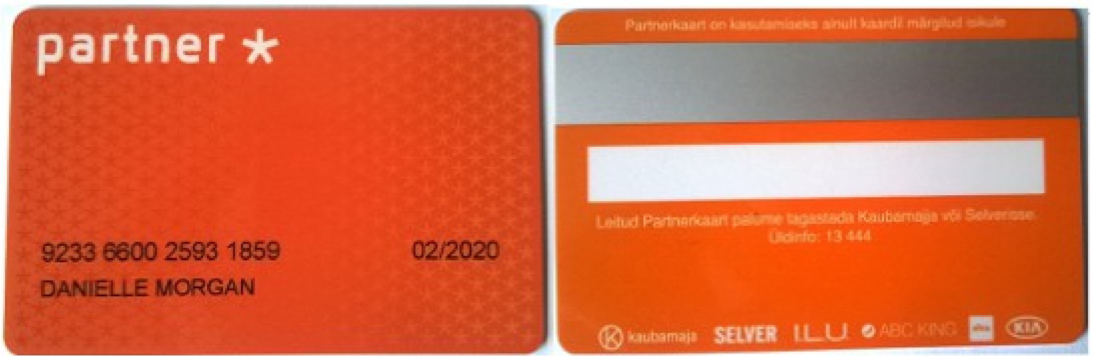
To apply for the card a person submits an application form online with their first and last name, personal ID code, birthday, address, phone number, email address, language and the collection location. Optionally, occupation, type of housing, level of education, marital status and number of family members can also be entered[2]. After the submission, the user receives an email confirming the information has been added to the system and the procedure necessary to collect the card. On collection, the user is expected to provide identification to receive the card and if the user is an ISIC holder, the card is closely inspected to ensure validity and the photo matches the user.

The Partner card, as seen in Figure 13, uses an orange background and white and black text in its color scheme. The front of the card (Figure 13 (a)) has the Partner card logo at

[1] https://www.partnerkaart.ee/et/mis-partnerprogramm

[2] https://www.partnerkaart.ee/join/partnerkaart

the top and the card number, user's name and expiration date in black text at the bottom. The back of the card (Figure 13 (b)) has a gray magnetic stripe at the top, a signature field in the middle and the logos of the stores participating in the scheme at the bottom.


partner
9233 6600 2593 1859
02/2020
DANIELLE MORGAN
Partnerkaart on kasutamiseks ainult kaardil märgitud isikule
Leitud Partnerkaart palume tagastada Kaubamaja või Selverisse.
Üldinfo: 13 444
kaubamaja
SELVER
ILU
ABC KING
KIA

(a) (b)

Figure 13. The front (a) and back (b) view of the Partner card

The Partner card uses only Track 2 of the magnetic stripe and its contents can be seen in Table 8. Track 2 contains the card number, as written on the front of the card, in the first field and the expiration date (February 2020) and the service code (501) in the second field.

Table 8. The track information contained on the Partner Loyalty card in ISO format

Track	**Content**
1	No data
2	;9233660025931859=200250100000000000?
3	No data

Standard usage of the card includes giving the card to the cashier who swipes it and returns it to the customer along with a receipt of the purchase. The user is able to view the last 4 digits of their card and the previous bonus points on the receipt as seen in Appendix 2 Figure 47. To see their bonus points a user can also login to the self-service portal using either their ID card, Mobile-ID, Smart-ID or through their bank. From the self-service portal the user is also able to change personal data, add family members, view transactions and receipts from the last 2 years and disable the card.

In summary, this card does not present any challenge in cloning the magnetic stripe. All data required for a clone is directly visible on the card's front. With the increasing use of self-service terminals in places such as the supermarket a person would be able to use a clone that looks nothing like the original without being detected. If these terminals also allow for bonus points to be used to purchase items then a person would also be able to not only gain a person's discounts but also use their points. The online self-service portal would be able to indicate when and where the card holder's points were spent but would not prevent them from being spent.

2.2.8 PINS Card

The PINS program is owned and operated by Coalition Rewards Ltd, a loyalty management company, based in Northern and Eastern Europe and Russia, which is owned by Air Baltic Corporation. In Estonia, the company offers several loyalty cards to customers to connect to the program: a standard PINS card, a LuxExpress PINS card and four types of airBaltic PINS cards[1]. The card chosen for this experiment was the LuxExpress PINS card. This card offers the client three level of discounts (15%, 30% and 40%) dependent on the number trips undertaken and every euro spent gains PINS points that can be later used to purchase rewards such as trips and electronics from the PINS store.

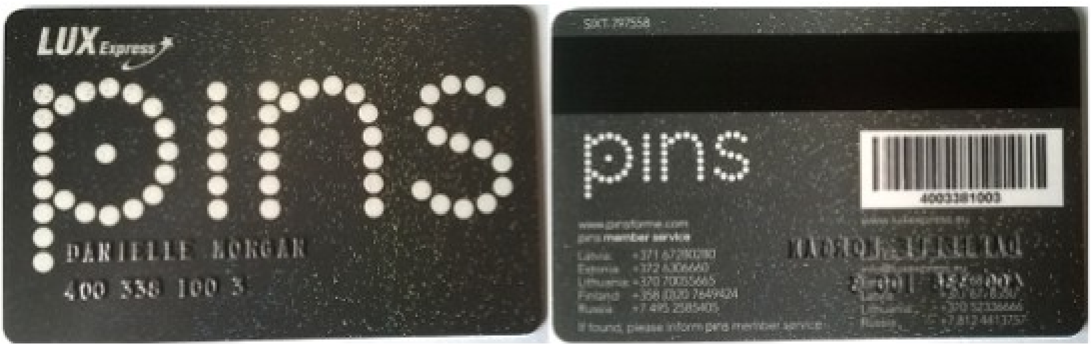
A customer can apply for the LuxExpress card through the PINS mobile application, LUX Express customer service offices and by filling out an online form. The method used to gain the card was by filling out the online application form. The information required for the application include: an email address, name (first and last), date of birth, gender, address and an optional mobile number[2]. After the application has been submitted, the customer receives an email confirmation including their name, address and account number. The personalized card, pictured in Figure 14, is then delivered to the stated address within 2 weeks at no cost to the customer as the card is also free.

The personalized LuxExpress PINS card uses a gray background with with white lettering. The front of the card as seen in Figure 14 (a) contains the LuxExpress and PINS logo as an embossing of the customer's name and account number. The back of the card, pictured in Figure 14 (b), contains a black magnetic stripe at the top, the PINS

[1] https://www.pinsforme.com/en-ee/pins-explained

[2] https://luxexpress.eu/en/register

logo, contact information for customer service and the customer’s account number in bar code format positioned to the middle right of the card.



(a) (b)

Figure 14. The front (a) and back (b) view of the personalized LuxExpress PINS card

The design of this card makes it difficult to cheaply produce a clone that can pass visual inspection as standard usage of the card requires the user to present the card either to the bus driver or another Lux Express employee who swipes the card and verifies that the customer has a valid travel ticket and that the information in the system matches that on the card. Additionally, the customer may be required to present an identification document to verify their identity and age in case of age-related discounts.

The Lux Express card utilizes two of the three tracks on the magnetic stripe, Track 1 and 2. Table 9 displays the encoded information found on these tracks. Track 1 contains an issuer identifier followed by the account number (the card number), as seen on the front and back of the card, in the first field. The second field contains the customer’s name and the third field contains a mixture of information, in the order of: an expiration date (December 2099) followed by the service code, the expiration date again and the account number. Track 2 contains the card number in the first field and in the second field the same data from field three on Track 1 minus the account number.

Table 9. The track information contained on the Lux Express PINS Loyalty card in ISO format

Track	Content
1	%B2106574003381003^DANIELLE/MORGAN ^991279999121000040033810030000O?

2	;2106574003381003=99127999912100000000?
3	No data

Overall the data visibly present on the card gives sufficient knowledge for a clone to be attempted. Another option available, would be to order several cards with varying information to analyze their content as acquiring cards comes at no cost to the customer. Lux Express and PINS also each offers a mobile application where a user can log in to their account and in the event the customer's card is missing or forgotten, a digital representation of the card can be presented via the application. In the case of the Lux Express application the customer's account number is encoded in a QR code and the front of the card (Appendix 2 Figure 49) and in the case of the PINS application the account number is simply presented in both bar code and QR code with the client's name (Appendix 2 Figure 50). A simple replica of these applications can be made, by just knowing the customer's name and account number which are present on the front of the card as well as on the tickets purchased using the card (Appendix 2 Figure 48). The replica can then be used to gain discounts in the event identity is not confirmed (which may occur when the bus driver is the one performing the check). The cloning of the card, however, only allows for the user to gain discounts on trips but gives no access to spending a customer's PINS points.

2.2.9 Rimi Card

The Rimi Loyalty card is offered by Rimi supermarket to its customers and provides them with special offers and discounts and allows them to collect bonus points on every euro spent at the rate of 1%. These bonus points can be later used to pay for products in store[1].

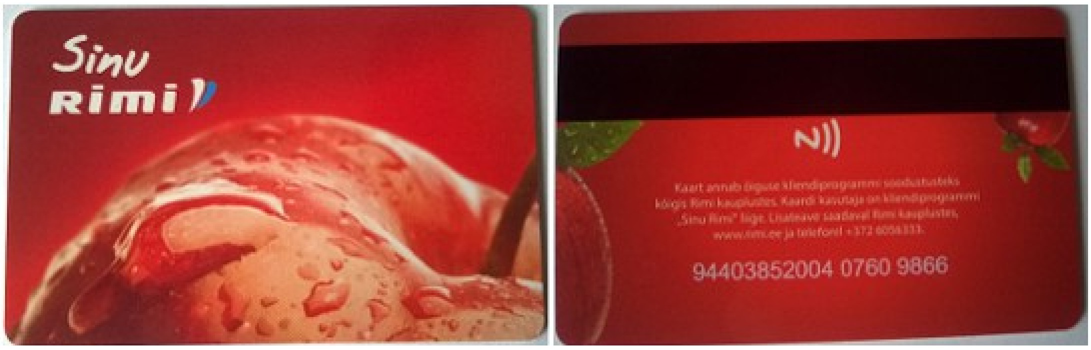
A customer can acquire a Rimi card for 1€ at the information desk located at Rimi supermarkets. The cards can be used in stores to collect points, but in order to gain card discounts and spend the money collected, the card has to be registered at the terminals located in store or on the Rimi website. The fields required to complete registration are first and last name, gender, birthday and mobile number. Once the terms and conditions have been accepted the user can enter contact methods including an email address. An

[1] https://www.rimi.ee/sinurimi

email with a confirmation link (valid for 10 days) is sent to the customer along with their login password, which appears to be randomly generated.

The online self-service portal allows the customer to manage their personal data including adding an address, change their password, view the Rimi money that is available and view previous transactions including time, date, total cost and location. Rimi also offers an Android mobile application for its customers where they can login using their email and password. From the application the user can view their Rimi money, set food preferences and change their address and mobile number.

The Rimi card as seen in Figure 15 uses a red background and white text color scheme. The front of the card (Figure 15 (a)) has the Rimi logo and at the back of the card (Figure 15 (b)) a black magnetic stripe at the top, some information about the card in the middle and the card number at the bottom. Standard usage of this card involves the user swiping it at the terminal to receive discounts and bonus points. The Rimi card is also an NFC enabled card and while the full card cannot be read, some information encoded on the stripe is available. This topic is discussed fully in Section 3.6.



(a) (b)

Figure 15. The front (a) and back (b) view of the Rimi Loyalty card

The Rimi card uses Track 2 and Track 3 of the magnetic stripe and its Raw Data can be seen in Table 10. Track 2 contains the card number, as seen on the back of the card, in field one and in field two the expiration date (December 2020) and service code (101). Track 3 contains a mixture of information which is not at first glance easy to discern. The fields appear to present the following information:

1. Store Location Identifier (4 digits): 9002

2. Identifier (16 digits): Prefix (8 digits) + Last 8 digits of the card number
3. Null Field (9 digits)
4. Card Number Prefix: First 10 digits in card number
5. 01 (2 digits)
6. Null (6 digits)
7. Null (3 digits)
8. Expiration date (6 digits): YYMMDD format
9. Manufacture Date (6 digits): YYMMDD format
10. Country Code Identifier (4 digits): 0233 (Estonia)

Table 10. The track information contained on the Rimi Loyalty Card in ISO format

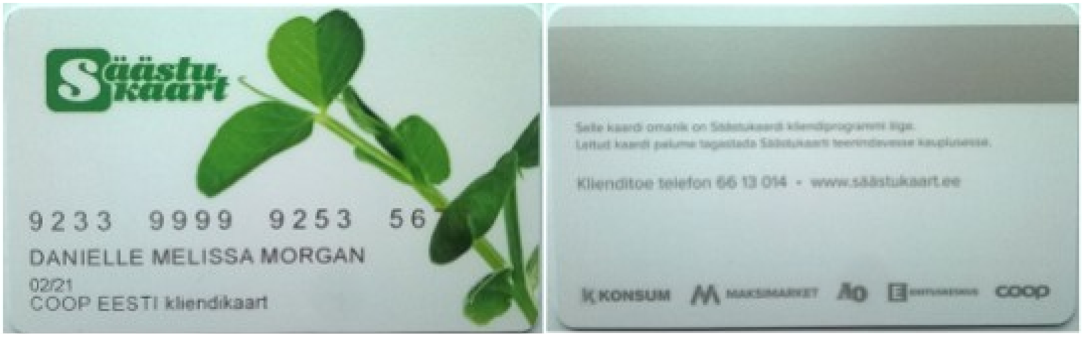
Track	**Content**
1	No data
2	;9440385200407609866=20121010000000000?
3	;9002=1233000107609866=000000000=9440385200=01=000000=000 =201231=160519=0233?

Overall the Rimi card presents a challenge in cloning. The data encoded on the magnetic stripe is not readily available on the surface of the card or the receipt, Appendix 2 Figure 51, which shows the first 6 and last 4 digits of the customer card and the bonus points available. The information present is sufficient to create Track 2 but is not detailed enough for a Track 3 clone. Standard usage of the card dictates that the customer is usually the one who handles the card therefore imitating the design of the card may not be necessary. Additionally, Rimi offers self-service checkouts where the user can freely use the card without scrutiny. If a clone can be indeed successfully executed then the user would be able to spend the bonus points of the victim as well, since these terminals allow for payment by points. However, an interesting security feature of self-service checkouts is that a user can only cover up to 99% of the cost with bonus points and the remainder must be covered by using a payment card.

2.2.10 Säästu Card

Säästukaart is a loyalty card offered to customers for use in Coop Eesti stores including Konsum, Maksimarket, Ehituskeskus and A ja O stores. With this card, for every purchase made, customers can collect bonus points that can be used to pay for future purchases in addition to gaining discount offers and a 10% discount 5 days before and after their birthday[1].

To apply for the Säästukaart, a customer can submit an application online or in any Coop store. To order the card online, the user can login with their ID card, Mobile-ID or through their bank. When ordering the card online the user's name and identification code fields are automatically filled. To complete this form a phone number and address must be entered and optionally an email address can be entered as well. The card which is valid for 4 years is free of charge and is delivered to the address specified within 2 weeks of the submission of the application.


Säästu-
kaart
9233 9999 9253 56
DANIELLE MELISSA MORGAN
02/21
COOP EESTI kliendikaart
Selle kaardi omanik on Säästukaardi kliendiprogrammi liige.
Leitud kaardi palume tagastada Säästukaarti teenindavasse kauplusesse.
Klienditoe telefon 66 13 014 • www.säästukaart.ee
KONSUM
MAKSIMARKET
coop

(a) (b)

Figure 16. The front (a) and back (b) view of the Säästukaart Loyalty card

The personalized card as seen in Figure 16 uses a white background and gray text. The front of the card (Figure 16 (a)) contains the Säästukaart logo at the top followed by the card number (the last 2 digits hidden by the design), the customer's name, the card's expiration date and the name of the description of the card (Coop Eesti client card). The back of the card (Figure 16 (b)) contains a gray magnetic stripe at the top, contact information for card related issues and the logos of the participating stores.

Säästukaart only uses Track 2 of the magnetic stripe and its content can be seen in Table 11. The data encoded here includes the card number as seen on the front of the card in the first field and the expiration date (February 2021) and service code (701) in the second field. Typical use cases of this card involves the user swiping it in the terminal before paying for the purchases. The receipt returned, Appendix 2 Figure 52, details the

[1] https://www.skaart.ee/et/info/uus_boonusprogramm

bonus points gained from the purchase. The user can also login to the self-service portal to check their bonus points or order new cards and change their contact information.

Table 11. Track Information for the Säästukaart Loyalty Card in ISO format

Track	**Content**
1	No data
2	;9233999992535677=21027010000000000000?
3	No data

This card's color scheme (white background) means that a standard blank magnetic stripe card could be mistaken for this card. In addition, since the card is swiped by the user, it is the possible to hide the upper part of the card by hand. The Track 2 encoding does not present a challenge as only the basic data is present and can easily be gained from a simple photo of the card. The method for acquiring a card is, however, somewhat secure as the user needs to present a valid ID document when ordering the card from a store and when ordering online the user's name and personal ID code have been verified by their bank, valid ID card or Mobile-ID.

2.3 Summary

Magnetic stripe cards analyzed in this study usually present the information encoded on the magnetic stripes on the surface of the card. Additionally, in most cases the receipts disclose the card number at least partially, but in several cases the entire card number is printed. This allows the information necessary to create a clone to be obtained from a distance without the need to read the magnetic stripe of the victim's card. Minimizing the information presented on the card and receipts would prevent a clone from being created using that information. This, however, would prevent the use of information printed on the card as a means of backup if the magnetic stripe becomes unreadable. Customization of the card in unique and colorful ways reduces the chances of an exact replica of the design. However, if the identity of the card user is not verified to that printed on the card and read from the stripe, physical security features embedded on the card provide no security.

3 Contactless Cards

As discussed in the introduction section, some merchants in Estonia use contactless cards to provide customer identification in their loyalty schemes. This section first gives a brief overview of contactless technologies in use and later describes particular use of the technology in merchants loyalty program.

3.1 Contactless Technology

The term “contactless card” refers to cards whose data can be read without the card coming into direct contact with the reader. Radio Frequency Identification (RFID) enables identification from a distance by using radio waves. RFID tags support a large set of unique IDs and can include additional data such as manufacturer and product type. In addition, RFID systems can distinguish between many different tags in the same general area of use. [10]

RFID tags fall into two categories: active and passive tags. Active tags require a power source and have a lifespan limited to the energy stored in the power source. Passive tags do not require a battery and have an indefinite lifespan. Passive tags consist of an antenna, a semi-conductor chip attached to the antenna and casing. For passive tags, the reader is responsible for powering and commencing communication with a tag. The tag antenna, after acquiring the energy returns the tag’s UID, coordinated by the chip, while the casing protects the antenna and chip. [10]

RFID includes many standards that operate at different frequencies. These include: low frequency (LF) at around 125kHz, high frequency (HF) at 13.56MHz and ultrahigh frequencies (UHF) at around 900MHz. NFC is a subset of these standards operating in the HF band at 13.56MHz under ISO 14443. The NFC protocol supports communication between an active reader and a passive tag and peer-to-peer communication hence allowing an NFC-enabled phone to both read tags and receive and transmit data to another NFC-capable device. [11]

RFID tags can contain read/write memory allowing for the storage of information. When reading from such a tag, its UID is first obtained and then any corresponding content. To prevent the content from being changed without permission, a security key can be set to restrict access on internal blocks of data. The NFC data stored on the tag is transferred between a reader and tag using an NFC Data Exchange Format (NDEF) message. An NDEF message can be comprised of an arbitrary number of NDEF records with each record containing length and type information which describes its function. There are several record types but one of the more popular ones is the signature type which defines a format for signing a set of NDEF records including the signature algorithm and certificate types used to create the signature.[11]

3.2 Contactless Tools

In order to test the capabilities of a card, a reader with the correct operating frequency must be used. There are several products available but the reader chosen for NFC card communication for this study was the ACR122U USB NFC reader (~36€) shown in Figure 17. This device can be used for accessing ISO 14443-4 Type A and B, MIFARE, ISO 18092 and FeliCa tags. It also has a built in authentication command for MIFARE Classic cards.

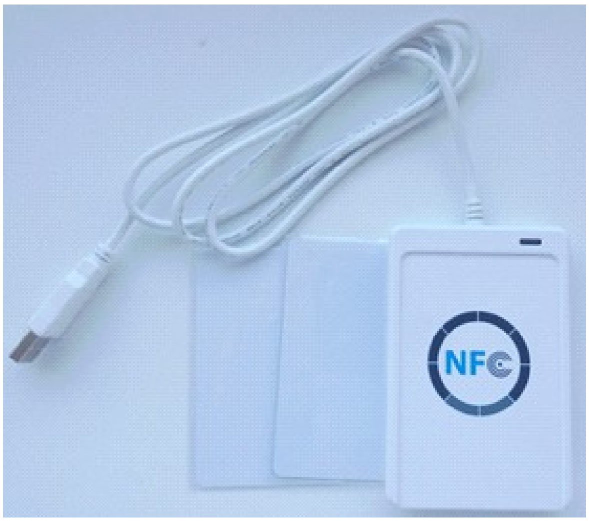
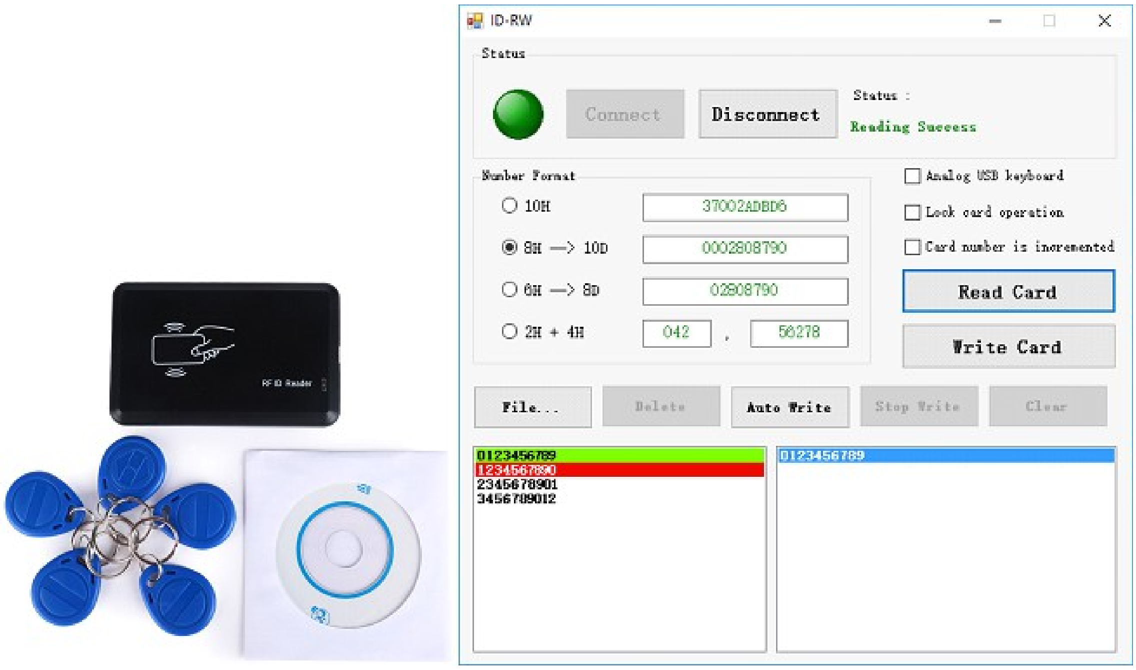


Figure 17. The ACR122U USB reader and the accompanying MIFARE Classic 1K cards

Another reader used in this study is the NFC-enabled smart phone, Samsung Galaxy J5 (2016) running Android OS 6.0.1. There are also several applications available for reading NFC tags, but the two applications used in the following experiments were NFC TagInfo[1] and MIFARE Classic Tool[2] (also available on GitHub [23]). For cards operating at low frequency radio waves, a USB 125Khz RFID Card Reader/Writer/Copier (~22€), as shown in Figure 18, was acquired.



Status : Reading Success

Number Format
○ 10H 37002ADBD6
● 8H —> 10D 0002808790
○ 6H —> 8D 02808790
○ 2H + 4H 042 , 56278

□ Analog USB keyboard
□ Lock card operation
□ Card number is incremented

```
0123456789
1234567890
2345678901
3456789012
```

```
0123456789
```

Figure 18. The 125kHz RFID reader/writer/copier and accompanying software and tags

Another step in card analysis is to test the ability to clone the card and use the clone for authentication. In some experiments a standard MIFARE Classic card was used, but since each card has a unique ID, to trick the systems which check the UID of a card, a special card with a changeable UID can be used. These cards can be obtained cheaply (as low as ~0.35€ per card) from online market places such as aliexpress.com. There are also devices available which imitate the functionality of contactless cards. One such device is the ChameleonMini [24] (~100€) shown in Figure 19, which has an 8 slot memory each with a size of 8kB [27] . Each slot can be configured to emulate card data for different types of cards: MIFARE Classic 1K and 4K both 4-byte and 7-byte UID and MIFARE Ultralight. The ChameleonMini, however, currently cannot be used to imitate MIFARE DESFire or MIFARE Ultralight C cards, but does support

[1] https://play.google.com/store/apps/details?id=at.mroland.android.apps.nfctaginfo

[2] https://play.google.com/store/apps/details?id=de.syss.MifareClassicTool

communication sniffing from the reader to the card. This device was used to imitate the MIFARE Classic cards discovered.

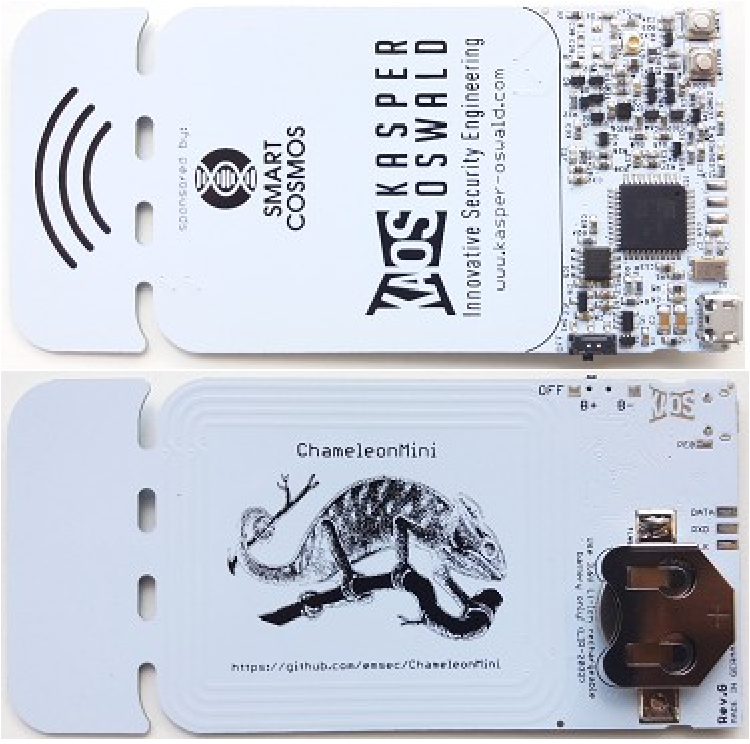


Figure 19. The front and back of the ChameleonMini

3.3 Low Frequency (LF) Cards

The tags in low frequency cards operate at around 125kHz with a read range of about 10cm. These cards generally only store an identifier which is 5-bytes in size with an additional byte used as a checksum. The tag can either be read/write or read-only. The read-only tags can be bought cheaper, but are not suitable if a specific tag ID is needed for a system. Additionally, some systems only utilize the 3 rightmost bytes in the tag as a token ID hence reducing the number of possible unique values. As a consequence, the tag ID may be unique only in the system where it is intended to be used. This can result in the tag ID used by one system matching the one used by another system hence resulting in a collision.

3.3.1 Methodology

The RFID reader/writer/copier shown in Figure 18 was used to read the tag ID of the card and this value was then later used to create a clone. Finally, the device was used to determine if the tag was read/write or read-only.

3.3.2 Results

MyFitness Membership Cards

MyFitness is a sports club which provides its members with a Membership card used to gain access to training facilities. The cost of the card is covered in the joining fee which is 20€ online and 30€ at the club. In case of lost or damaged card a new membership card can be obtained for 5€. The MyFitness card, shown in Figure 20, has no card-specific information printed on the card (such as the card number).

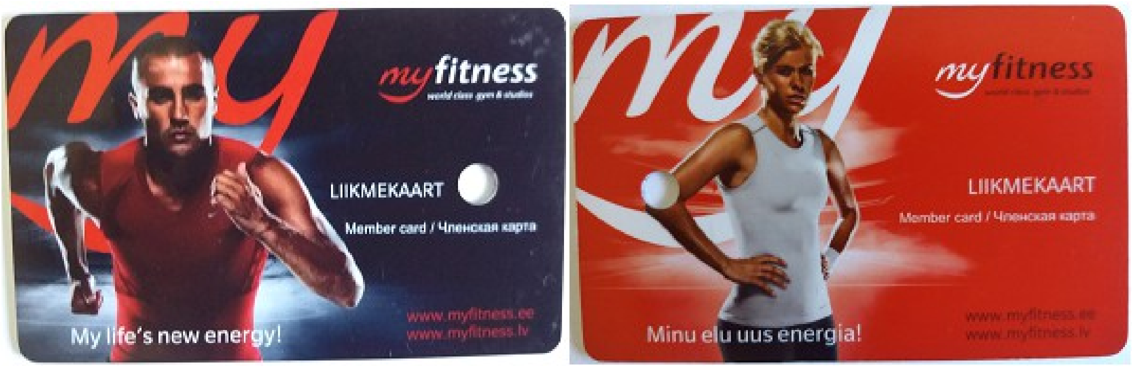


Figure 20. The front and back view of the MyFitness Card

The RFID reader was able to read the tag's ID in different number formats (shown in Table 12). Using the reader, an attempt was made to re-write the tag in the card but was unsuccessful, which shows that the tag is write protected. The card number was then written to one of the LF key fobs provided with the reader. The cloned tag was successfully used to gain entry to the MyFitness gym.

Table 12. The MyFitness Card Tag ID in different number formats

Number Format	**Card Number**
10H	37002ADBD6
8H (10D)	0002808790
6H (8D)	02808790
2H + 4H	042 56278

The lack of security in the technology used in MyFitness cards can be well described by the incident, where the identity of another MyFitness member was unintentionally used to access MyFitness services. It was found that the incident was caused by the unrelated RFID door card residing in the same wallet as the legitimate MyFitness card. The wallet was approximated to the MyFitness reader and, apparently, the reader established connection not with the MyFitness card, but the door card. The card number encoded in the door card, apparently, matched the tag ID stored in the MyFitness card of another member. This incident shows that the card technology used by MyFitness can be compromised even without intention. The incident was discovered most likely because the member whose identity was unintentionally impersonated complained about being billed for service he did not use.

In summary, the MyFitness Membership card can be easily cloned. As the card is read-only, it is protected from a denial-of-service (DoS) attack by covertly overwriting the tag with invalid data. It is, however, entirely possible to accidentally impersonate some other club member if another tag is read at the terminal instead of the MyFitness card.

3.4 MIFARE DESFire EV1

The MIFARE DESFire EV1 card is a contactless smart card with an operating distance of up to 100mm an is ideal for use in public transport schemes, access management, closed-loop e-payment applications, event ticketing or eGovernment applications. It is compliant to all 4 levels of ISO/IEC 14443A and uses optional ISO/IEC 7816-4 commands. A MIFARE DESFire EV1 card can hold up to 28 different applications with 32 files each where file size is defined at creation. MIFARE DESFire is available in memory sizes of 2kB, 4kB and 8kB and has several security features including a unique 7-byte serial number (UID), optional random ID, mutual three pass authentication, one master key for the card and a maximum of 14 keys per application, hardware DES using 56/112/168 bit keys and hardware AES using 128-bit keys. [9]

The unique 7-byte UID, is programmed into a locked part of memory and is write protected after being programmed. This UID cannot be altered to ensure the uniqueness of each device. The UID can therefore be used to derive diversified keys for each ticket which increases the security of the original key. The MIFARE DESFire EV1 can also be configured to return a random ID of 3 bytes. [9]

As mentioned above the file system on the card allows for a maximum of 28 applications, identified by a 3 byte Application Identifier (AID), with up to 32 files each. The file types available are: Standard data files, Backup data files, Value Files with Backup, Linear record files with backup and cyclic record files with backup. These files can either be created during card production or when in use. [9]

Before data transmission can occur a mutual three-pass authentication can be done depending on the configuration specified uising either 56-bit DES, 112-bit 3DES, 168-bit 3DES or AES. The MIFARE DESFire EV1 can be considered as having three operational levels: the card level (PICC level), the application level and the file level. At each level a different command set is available with security related commands being available throughout. On the PICC level the user is allowed to: create, delete and select applications; get application IDs, free memory available, key settings, card UID and version; and release user memory. These commands may only be available after authentication with the master key. The application level commands allow the user to create and delete files, get the file identifiers (FID) and change or get file settings (file access parameters). Once again these commands may only become available after authentication. Once a file is selected a user is able to perform various actions depending on the file type. For Standard files the read and write data commands are available while the get value, credit (increase a value), debit (decrease a value) and limited credit (limited increase of a value) commands are available for Value files. The Cyclic and Linear record files support the commands write, read and clear record and the Backup Data files commit and abort transaction commands. [9]

Currently there are no publicly known practical attacks against the MIFARE DESFire EV1 cards that could be used to recover the cryptographic keys used by the card.

3.4.1 Methodology

The card identified under the category of MIFARE DESFire was first scanned using the NFC TagInfo app. This provided tag information, version information and application information and master key configuration information. LibNFC [20] and LibFreeFare

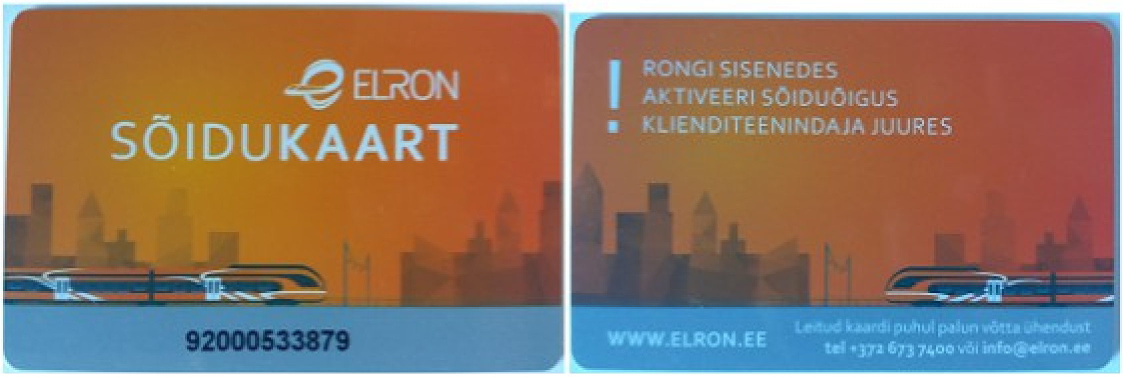
[19] was then used to create a printout of the DESFire information. This information was then used to analyze the security features used on the card.

3.4.2 Results

Elron Farecard

The Elron card as pictured in, Figure 21, is a MIFARE DESFire EV1 4K card which can be used for loading money and buying tickets for travel on Elron trains. This card provides its users with a 10% discount on all ticket prices[1]. The card can be purchased from staff on board the train or from the Baltic and Tartu stations for a price of 2.50€.

The card is orange in color with white text. On the front of the card, Figure 21 (a), the card number is printed at the bottom. This number can be used via the online interface[2] to load money onto the card and view the current account balance and all transactions.



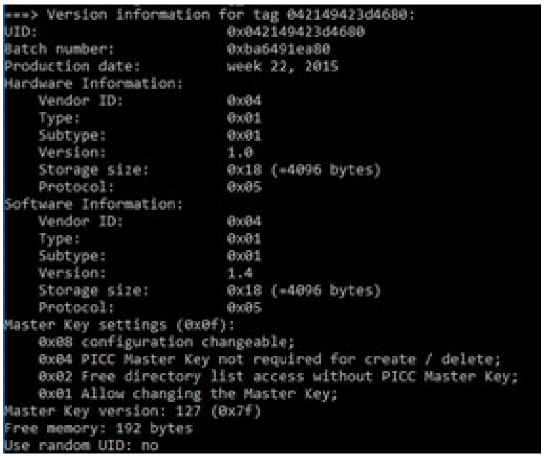
(a) (b)

Figure 21. The front (a) and back (b) view of the Elron Card

The version information about the card can be viewed in Figure 22. From this readout, it can be seen that the card uses the standard 7-byte UID and the size of the memory is 4kB. The master key configuration allows for the listing of AIDs and creation and deletion of applications.

[1] http://elron.ee/en/piletid/elron-soidukaart/

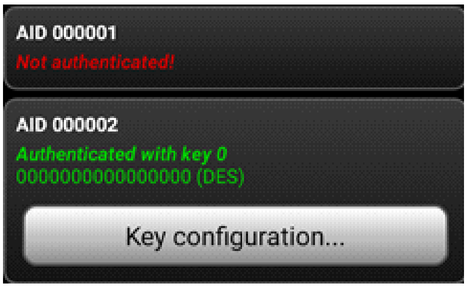
[2] https://pilet.elron.ee/en/Account/Login



```
===> Version information for tag 042149423d4680:
UID:                          0x042149423d4680
Batch number:                 0xba6491ea80
Production date:              week 22, 2015
Hardware Information:
    Vendor ID:                0x04
    Type:                     0x01
    Subtype:                  0x01
    Version:                  1.0
    Storage size:             0x18 (=4096 bytes)
    Protocol:                 0x05
Software Information:
    Vendor ID:                0x04
    Type:                     0x01
    Subtype:                  0x01
    Version:                  1.4
    Storage size:             0x18 (=4096 bytes)
    Protocol:                 0x05
Master Key settings (0x0f):
    0x08 configuration changeable;
    0x04 PICC Master Key not required for create / delete;
    0x02 Free directory list access without PICC Master Key;
    0x01 Allow changing the Master Key;
Master Key version: 127 (0x7f)
Free memory: 192 bytes
Use random UID: no
```

Figure 22. Version Information for the MIFARE DESFire EV1 Elron Card

Executing the AID list command showed that the Elron Application had an AID of 0x000001. On selecting this application, file identifiers could not be obtained as this process required authentication. As the master key was not the default value, the default key could not be used to gain additional information about the application. The card however has 192 bytes of unused memory and with this space an Application with an AID of 0x000002 was successfully created with a null key for authentication (see Figure 23). A file was then added and deleted from the card but further action could not be taken in regards to the card as the memory space available had been used. To reclaim the space of the deleted file a format of the card would be required. This action, however, requires authentication with the master key to be executed. In addition, deletion of the application was not allowed as authentication to delete the application was required. An interesting question is whether this would prevent the Elron application from writing to or updating any of the files in its application (if this is ever done after the card has been issued).



AID 000001
Not authenticated!

AID 000002
Authenticated with key 0
0000000000000000 (DES)

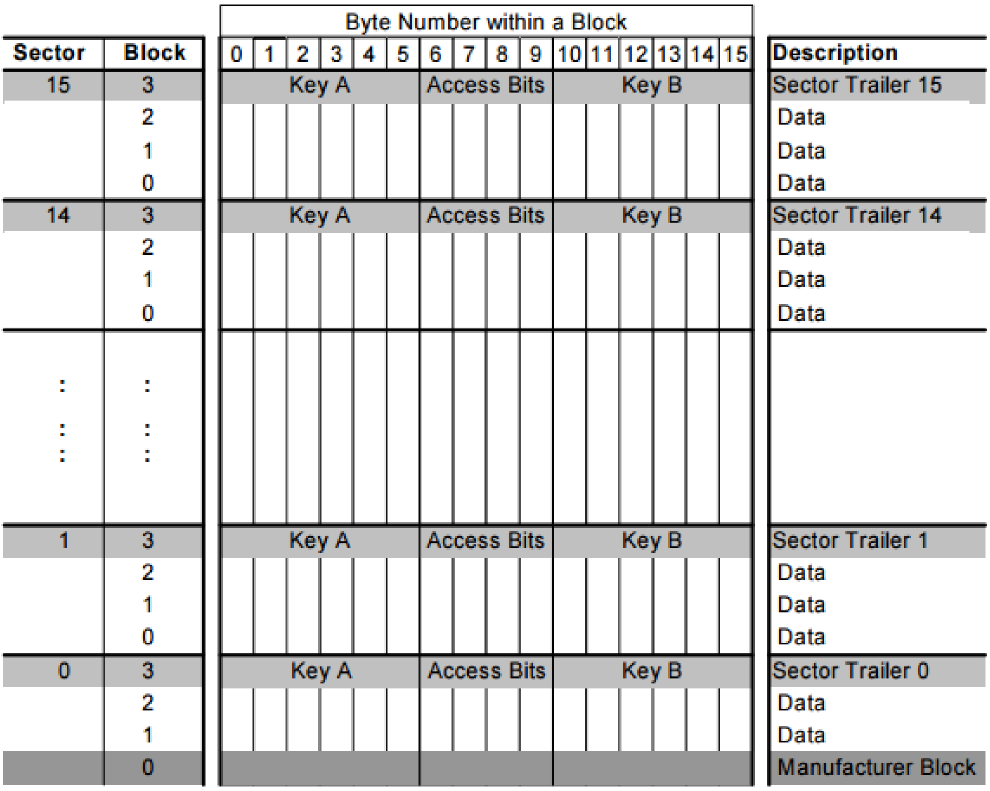
Figure 23. Successful creation of an application on the Elron Card

In summary, with the current knowledge this card cannot be cloned. The key or keys required to read the application files are unknown and hence the contents cannot be emulated. Even if the keys could be recovered, a DESFire UID changeable card would be required (unless UID of the card is not verified). These cards, however, are not readily available and a solution such as the ChameleonMini cannot be used as the ChameleonMini currently does not support DESFire EV1 emulation, and even if it would, the shape of it is not that of a typical card and hence would be rejected by Elron employees. An alternative solution would be to implement the application by emulating a DESFire card using a Java Card applet [25] ,[26] . The DoS attacks cannot be performed either, because to modify the contents of the Elron application, authentication is required. The open issue is whether the ability to create new applications without authorization creates any security risks.

3.5 MIFARE Classic 1K

The MIFARE Classic 1K card is a contactless smart card with an operating distance of up to 100mm designed for use in applications such as public transportation, access control event ticketing and gaming & identity. The card comes with a 1024 bytes EEPROM memory organized into 16 sectors with 4 blocks of 16 bytes each, as shown in Figure 24. The security features available to the card include mutual three pass authentication (ISO/IEC DIS 9798-2), unique serial number for each device and a set of two keys per sector.[6]

The Manufacturer Block is the first data block (block 0) of the the first sector (Sector 0). This block contains the card serial number and other manufacturer data. In the case of 4-byte serial number (UID), the first 4 bytes hold the UID of the card and byte 4 is a check byte which is calculated by XOR-ing the bytes of the UID. In the case of 7-byte UID cards (also known as MIFARE Classic EV1 1K) the first four bytes contain a non-unique UID (NUID), but the first seven bytes together contain the UID of the card. The remaining bytes in both types of cards contain the manufacturer data. This block is programmed and write protected in the production phase. [6] , [7]

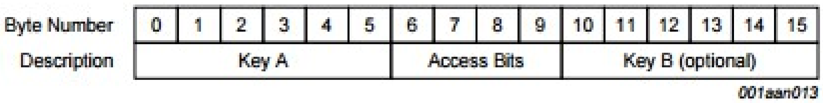


		Byte Number within a Block																
Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Description
15	3	Key A						Access Bits				Key B						Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A						Access Bits				Key B						Sector Trailer 14
	2																	Data
	1																	Data
	0																	Data
:	:																	
:	:																	
:	:																	
1	3	Key A						Access Bits				Key B						Sector Trailer 1
	2																	Data
	1																	Data
	0																	Data
0	3	Key A						Access Bits				Key B						Sector Trailer 0
	2																	Data
	1																	Data
	0																	Manufacturer Block

Figure 24. Memory Organization of the MIFARE Classic 1K card [[6] , Figure 4]

All sectors contain 3 blocks for storing data with the exception of Sector 0, which only contains two data blocks and the read-only manufacturer block. The data blocks can be configured by the access bits to be either read/write block or value blocks, but a successful authentication must be executed to allow any memory operation. [6] , [7]

The last block in every sector is known as the sector trailer and contains the secret keys A (mandatory) and B (optional) which return logical “0”s when read and the access conditions for the blocks of that sector. The access bits also specify the type (read/write or value) of the data blocks. Key A occupies the first 6 bytes of the block, Key B the last 6 bytes and the access bits bytes 6 to 9. Byte 9 is also available for user data. A graphical representation of the sector trailer can be seen in Figure 25. The default value for all keys is FFFF FFFF FFFFh and bytes 6 to 8 of the access bits FF0780h. [6] , [7]

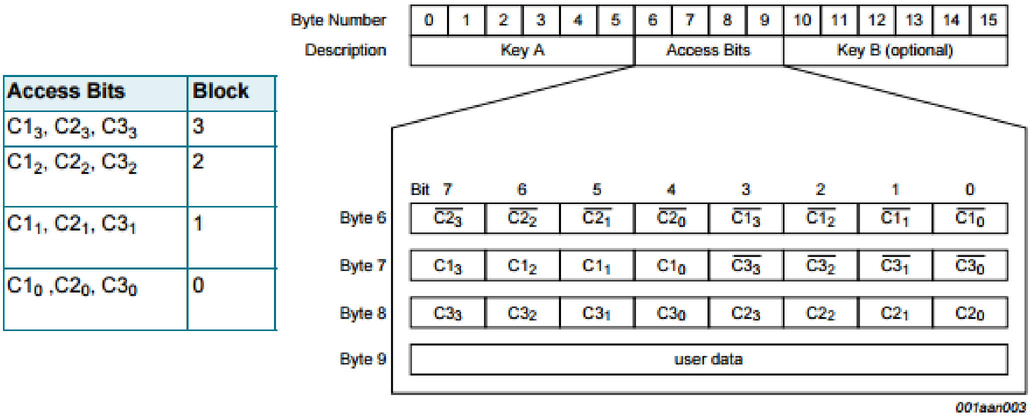


Byte Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Description	Key A						Access Bits				Key B (optional)					

Figure 25. Sector Trailer of MIFARE Classic 1K Card [[7] , Figure 10]

Before any memory operation can be executed the card has to be authenticated first. The memory operations available depend on the key used during authentication and the access conditions stored in the sector trailer. The list of memory operations include: read (read one memory block), write (write one memory block), increment (increments the contents of a block), decrement (decrements the contents of a block), transfer (write contents of the buffer to a block) and restore (reads the contents of a block to the buffer).[6] , [7]

Three bits (C1, C2 and C3), stored inverted and non-inverted in the sector trailer, are used to define the access conditions for every data block and sector trailer. Figure 26 shows the layout of the access bits and the block they affect. The access bits control the rights to memory access using Key A and B and may only be altered once the correct key is known and the current access conditions allows the operation. The valid commands for data blocks include read, write, increment, decrement, transfer and restore and for the sector trailer only the read and write operations are allowed. These commands can only be executed after a successful authentication.[6] , [7]



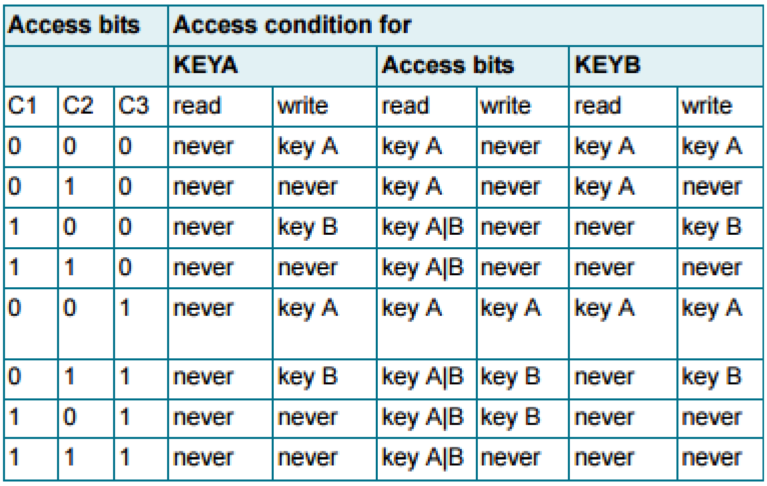
Access Bits	Block
$C1_3, C2_3, C3_3$	3
$C1_2, C2_2, C3_2$	2
$C1_1, C2_1, C3_1$	1
$C1_0, C2_0, C3_0$	0

Byte Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Description	Key A						Access Bits				Key B (optional)					

Bit	7	6	5	4	3	2	1	0
Byte 6	$\overline{C2_3}$	$\overline{C2_2}$	$\overline{C2_1}$	$\overline{C2_0}$	$\overline{C1_3}$	$\overline{C1_2}$	$\overline{C1_1}$	$\overline{C1_0}$
Byte 7	$C1_3$	$C1_2$	$C1_1$	$C1_0$	$\overline{C3_3}$	$\overline{C3_2}$	$\overline{C3_1}$	$\overline{C3_0}$
Byte 8	$C3_3$	$C3_2$	$C3_1$	$C3_0$	$C2_3$	$C2_2$	$C2_1$	$C2_0$
Byte 9	user data							

Figure 26. Access conditions for the MIFARE Classic 1K as detailed by sector trailer [[7] Figure 11, Table 6]

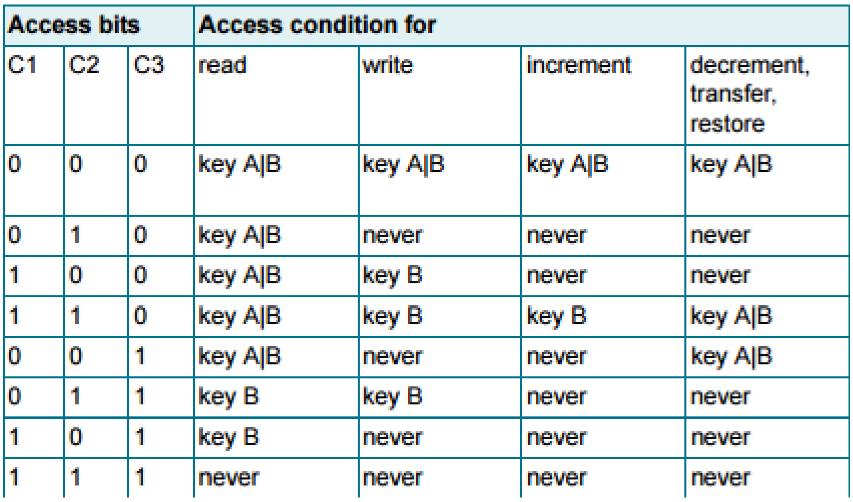
Read/write access to the keys and access bits can be either be dependent on Key A, Key B, Key A or B (A|B) or there could be no access (never). These conditions are dependent on access bits C1, C2 and C3 which affect the sector trailer (Block 3). Figure 27 shows how the combination of these bits allow for access to Block 3.[6] , [7]



Access bits			Access condition for					
			KEYA		Access bits		KEYB	
C1	C2	C3	read	write	read	write	read	write
0	0	0	never	key A	key A	never	key A	key A
0	1	0	never	never	key A	never	key A	never
1	0	0	never	key B	key A|B	never	never	key B
1	1	0	never	never	key A|B	never	never	never
0	0	1	never	key A	key A	key A	key A	key A
0	1	1	never	key B	key A|B	key B	never	key B
1	0	1	never	never	key A|B	key B	never	never
1	1	1	never	never	key A|B	never	never	never

Figure 27. Access conditions for the sector trailer for MIFARE Classic 1K cards [[7] , Table 7]

The access conditions for the data blocks (blocks 0 to 2) have the same dependencies as the sector trailer and its full access conditions can be seen on Figure 28. This information can read in the following way: for C1, C2 and C3 set to “0” for either key A or B can be used in the authentication step to allow for a read, write, increment, decrement, transfer or restore operation and for C2 set to “1” and C1 and C3 to “0” key A or B can be used to perform a read operation but the write, increment, decrement, transfer and restore operations are not allowed.



Access bits			Access condition for			
C1	C2	C3	read	write	increment	decrement, transfer, restore
0	0	0	key A|B	key A|B	key A|B	key A|B
0	1	0	key A|B	never	never	never
1	0	0	key A|B	key B	never	never
1	1	0	key A|B	key B	key B	key A|B
0	0	1	key A|B	never	never	key A|B
0	1	1	key B	key B	never	never
1	0	1	key B	never	never	never
1	1	1	never	never	never	never

Figure 28. Access conditions for the data blocks of the MIFARE Classic 1K cards [[7] , Table 8]

All MIFARE Classic commands typically use the MIFARE CRYPTO1 cipher and require authentication and the available commands can be found in Table 13. In 2008, however, digital security group from Radboud University Nijmegen in the Netherlands, published a paper on the reverse engineering of the MIFARE classic chip and CRYPTO1 cipher by analysing the communication between tag and reader [15] .

Using this as a base, in 2009 Nethemba implemented a card-only nested attack with the MIFARE Classic Offline Cracker (MFOC) tool [18] which can derive all keys on a card by knowing only one key. The nested attack works using the following steps [8] :

1. authenticate the block with default key and read tag's Nt;
2. authenticate to the same block with the default key and read tag's Nt;
3. compute timing distance;
4. guess the Nt value and authenticate to the different block.

Another card-only attack known as the Dark-Side attack was implemented by Andrei Costin with the MiFare Classic Universal toolKit (MFCUK) [17] which recovers at least one key from the card. MFCUK can be used in conjunction with MFOC to obtain the keys of a MIFARE Classic Card.

Table 13. Command set for MIFARE Classic EV1 1K [[7] , Table 9]

Command	**ISO/IEC 14443**	**Command code (hexadecimal)**
Request	REQA	26h (7 bit)
Wake-up	WUPA	52h (7 bit)
Anticollision CL1	Anticollision CL1	93h 20h
Select CL1	Select CL1	93h 70h
Anticollision CL2	Anticollision CL2	95h 20h
Select CL2	Select CL2	95h 70h
Halt	Halt	50h 00h
Authentication with Key A	-	60h
Authentication with Key B	-	61h
Personalize UID Usage	-	40h
SET_MOD_TYPE	-	43h
MIFARE Read	-	30h
MIFARE Write	-	A0h
MIFARE Decrement	-	C0h

MIFARE Increment	-	C1h
MIFARE Restore	-	C2h
MIFARE Transfer	-	B0h

3.5.1 Methodology

The first step in analysing the MIFARE Classic Cards was to read the data that was stored in the memory. As mentioned before, to read each sector a key is required and the access conditions have to be such that reading is allowed with the known key. For MIFARE Classic cards there are common Key A values that can be used to ensure that any application can read the sectors. Some of these values are A0A1A2A3A4A5, D3F7D3F7D3F7, 000000000000 and FFFFFFFFFFFF. To obtain these keys the MIFARE Classic Tool and NFC TagInfo Android Applications were used to scan the cards. From both of the apps, the A keys for each sector were found along with the access conditions.

After obtaining the data stored in the sector the second step was to use MFOC to execute a nested attack against each sector to try to obtain the B keys that can be used to write to the card. In case the keys were obtained, the ACR122U was used to overwrite the data to determine whether the keys obtained were correct.

The data on the card was then examined to determine which parts were used in the systems that used the cards and hence was required to reside on the clone. For example, was the UID of the card the only data required to gain access to the system or was some other section of information required. This analysis was then used to create clones using either the MIFARE Classic 1K cards or the ChameleonMini.

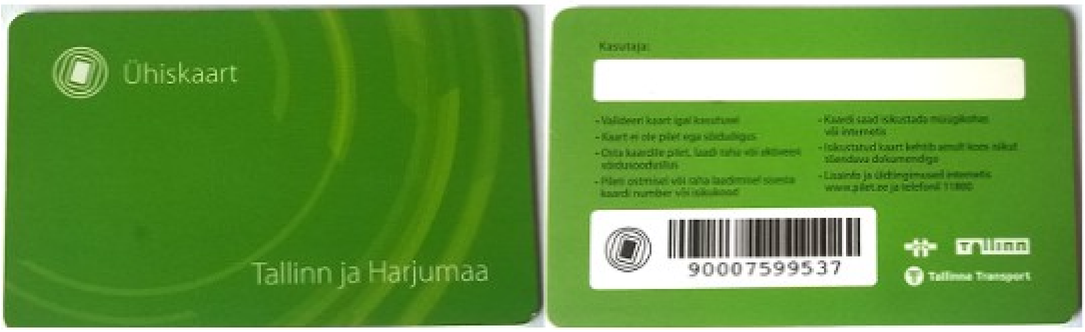
3.5.2 Results

Tallinn Bus Card (Ühiskaart)

The first card obtained that was identified as a MIFARE Classic Card was the Tallinn Bus Card (Ühiskaart). This card can be purchased at various locations including: Selver, Maxima and Prisma supermarkets, all Eesti Post post offices located in Harjumaa and

Tallinn, the Tallinn City Government Service Desk and all R-Kiosk for a price of 2€[1]. This card can be used to buy bus tickets or to prove the user's right to free travel on public transportation in Tallinn. Additionally, tickets for the Tallinn Zoological and Botanic Gardens can be be loaded onto the card and the card used to gain entrance into these venues. The card is also used to release documents from Pilveprint, a public printing service in Estonia, and to lock or unlock a bicycle stored in the Bikeep bicycle locking stations.

The Ühiskaart is a green card with white and black text as shown in Figure 29 below. Relevant information printed on the surface of the card include the card number which is located on the back side of the card at the bottom, Figure 29 (b). Both the front and the back of the card also contain a logo which indicates that the card is contactless.



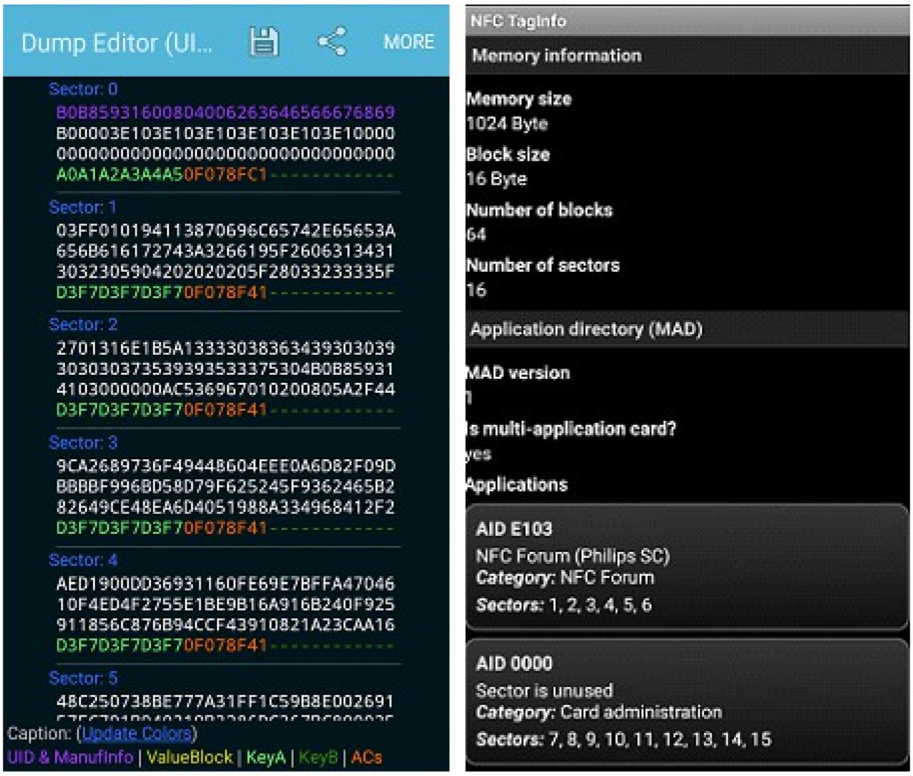
(a) (b)

Figure 29. The front (a) and back (b) view of the Tallinn Bus Card

After the card was scanned by both MIFARE Classic Tool and NFC TagInfo, it was revealed that the card was a 1K card with 1024 bytes of memory, 16 sectors and 64 blocks in total. Outputs from both of these applications are shown in Figure 30. The card contained one Application with the AID of E103 and it occupied sectors 1, 2, 3, 4, 5 and 6 of the card, while sectors 7 to 15 contained the default manufacturing data. The access conditions for sectors 0 to 6 make block 0 to 2 read-only, accessible with either key A or B. Block 3 for each sector can be also read with key A or B, but the access bits and the keys (A and B) can only be changed with key B. The output also showed that key A for Sector 0 was the common key A0A1A2A3A4A5 and for Sector 1 to 6, key A

[1] http://www.tallinn.ee/eng/pilet/Ticket-information-for-tourists

was D3F7D3F7D3F7. The keys found were then used to create a memory dump of the card using the ACR122U which can be seen in Appendix 3 Table 23.



```
Sector: 0
 B0B85931600804006263646566676869
 B00003E103E103E103E103E103E10000
 00000000000000000000000000000000
 A0A1A2A3A4A50F078FC1------------
Sector: 1
 03FF010194113870696C65742E65653A
 656B616172743A3266195F2606313431
 3032305904202020205F28033233335F
 D3F7D3F7D3F70F078F41------------
Sector: 2
 2701316E1B5A13333038363439303039
 303030373539393533375304B0B85931
 4103000000AC5369670102008 05A2F44
 D3F7D3F7D3F70F078F41------------
Sector: 3
 9CA2689736F49448604EEE0A6D82F09D
 BBBBF996BD58D79F625245F9362465B2
 82649CE48EA6D4051988A334968412F2
 D3F7D3F7D3F70F078F41------------
Sector: 4
 AED1900DD36931160FE69E7BFFA47046
 10F4ED4F2755E1BE9B16A916B240F925
 911856C876B94CCF43910821A23CAA16
 D3F7D3F7D3F70F078F41------------
Sector: 5
 48C250738BE777A31FF1C59B8E002691
```

Caption: (Update Colors)
UID & ManufInfo | ValueBlock | KeyA | KeyB | ACs

Memory information

Memory size
1024 Byte
Block size
16 Byte
Number of blocks
64
Number of sectors
16

Application directory (MAD)

MAD version
1
Is multi-application card?
yes
Applications

AID E103
NFC Forum (Philips SC)
Category: NFC Forum
Sectors: 1, 2, 3, 4, 5, 6

AID 0000
Sector is unused
Category: Card administration
Sectors: 7, 8, 9, 10, 11, 12, 13, 14, 15

(a) (b)

Figure 30. Sections of the output from the MIFARE Classic Tool (a) and NFC TagInfo (b)

From the card dump the following information can be determined from Sector 0. The UID of the card B0B85931 can be seen in the first 4 bytes of block 0 and the following bytes ("bcdefghi"), which is the manufacturing data that appears to be common among the Ühiskaart. Block 1 shows that the AID of the bus card application is E103 (in little-endian format) and it starts in Sector 1 (byte 2 and 3) and goes onto Sector 6 (byte 12 and 13). Bytes 14 and 15 of Block 1 and bytes 0 to 15 of Block 2 are 00 which can be read as AID of 00 occupies Sector 7 to 15.

Sector 1 to Sector 6 contain the information that allows the terminal to ascertain that the card is valid for travel. In this description the first byte on the left will be referred to as byte 0 and the numbering continuing until the last byte on the right, byte 15. The information is stored in a Tag, Length, Value (TLV) format with the first byte in block four (0x03) indicating the information is an NDEF message and byte 5 in block 25

(0xFE) acting as the terminator for the data. Bytes 1 to 3 indicate the length of the message, in the 3 byte format (0xFF0101), which is 257 bytes and the message starts at byte 4 and continues to the byte before the terminating 0xFE.

The card stores a cryptographic signature value data along with data that has been signed starting in sector 1 block 4 byte 7 and ending in sector 2 block 9 byte 15. The information embedded in the data that has been signed includes the UID of the card in which the signature was written to, the PAN of the card as well as the card number and the card type. In the case of this card the UID is B0B85931 and can be found as the last 4 digits of block 9. The primary account number, 3086490090007599537, and the card number, 90090007599537 which follows the Luhn algorithm for calculating the last digit (as shown in Figure 29 (b)), stretch from block 8 to block 9. The card type “pilet.ee:ekaart:2” can be found at the end of block 4 and the beginning of block 5.

The value of the cryptographic signature starts in sector 2 block 10 byte 13 and ends in sector 5 block 21 byte 12. The signature is created using an RSA 1024-bit key over SHA-1 hash. To verify the signature the public key certificate is required. The signer’s certificate information can be found starting in block 22 of the memory dump and continuing to block 25. The value, when decoded, shows the location of the certificate to be http://pilet.ee/crt/30864900-0001.crt. This certificate identifies the issuer as the creator of the Ühiskaart.

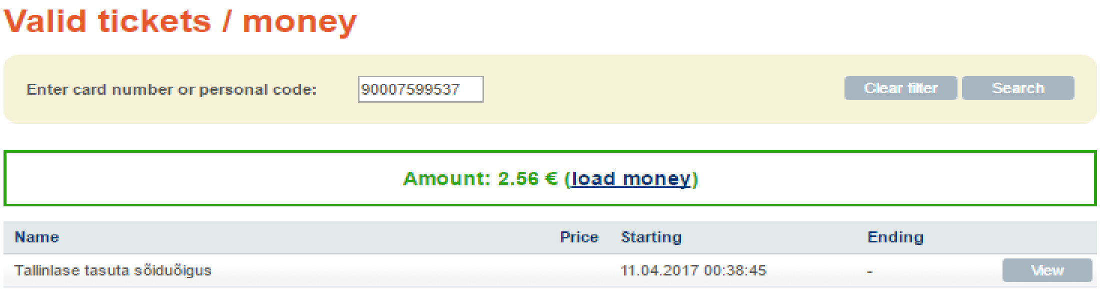
The data stored in the card can be analysed and the relevant information such as the card UID and account number can be easily extracted using yhiskaart[1] (validaator.py), an open source code written by Martin Paljak [16] . To use this program a memory dump of the card is required and can be created using MFOC or a card reader and hex editor. In addition to extracting relevant data the program also verifies the signature of the data. The verification can also be done manually using openssl command line tool. First by copying the signature data to a file (info.txt) and executing the command “openssl dgst -sha1 info.txt”. The output produced is the SHA-1 digest of the signature data. To verify the signature, the signature data has to be saved to a file (sig.txt.sha1) and the certificate (30864900-0001.crt) has to been downloaded. Then the following command has to be executed: “openssl rsautl -verify -certin -in sig.txt.sha1 -inkey 30864900-0001.crt -out

[1] https://github.com/martinpaljak/yhiskaart/blob/gh-pages/py/validaator.py

sigdata.txt". This command will produce the digest of the information signed in Abstract Syntax Notation One (ASN.1) format with the last 20 bytes being the digest. The digest created here can be compared to the digest created with the first command and if they match the signature verification is successful. The use of the digital signature scheme prevents an attacker from copying the information of a valid card and using it to make a clone with a standard MIFARE Card. As the UID in the standard MIFARE card would be write protected, it would not match the UID included in the signature. However, with the availability of UID changeable MIFARE Classic cards, the signature scheme provides no protection against the cloning.

To determine whether the terminal verifies the validity of the signature and the UID of the card, two cards were tested at a terminal on a public transport bus in Tallinn. One card had an invalid signature while the other had a valid signature but the UID of the card was different than that in the signature data. The cards were rejected hence confirming that the terminal in the bus does verify the validity of the signature and that the UID of the card matches the UID in the signature data.

The money available and the status of the card (e.g. "free travel in Tallinn") can be checked online at pilet.ee[12] by simply submitting a card number (or the personal code if the card is personalized). Figure 31 shows the output of the validity for the Ühiskaart used in this experiment. The code found in yhiskaart (pilet.py)[16] can be used for automated generation of valid card numbers and viewing the information about these cards.



Valid tickets / money

Enter card number or personal code: 90007599537

Amount: 2.56 € (load money)

Name	Price	Starting	Ending	
Tallinlase tasuta sõiduõigus		11.04.2017 00:38:45	-	View

Figure 31. Ticket validity check on pilet.ee

[1] https://www.pilet.ee/viipe/uhiskaart/activetickets

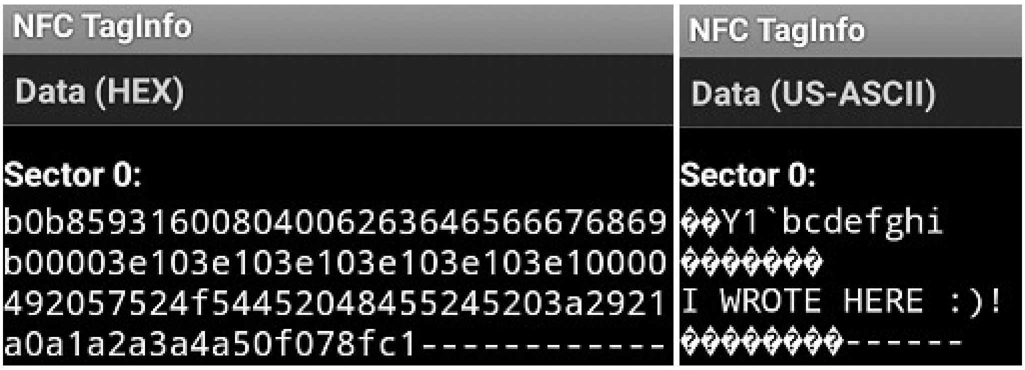
[2] https://tallinn.pilet.ee/tickets/personalcode

After the information on the card was analysed, MFOC was used to crack the B keys of the card. The results were successful and the keys for the six sectors were produced. In an effort to determine whether the keys generated on the card were random, the B keys of 2 other Ühiskaarts were found using MFOC. This process, when executed on a Ühiskaart takes around 15 minutes but varies from card to card, since it is largely dependent on the number of probes needed to discover the key in a sector. The results of the test can be seen in Table 14. The keys appear to be randomly generated as there are no repeating patterns present.

Table 14. Table showing the B keys for Sectors 0 to 6 for three Tallinn Bus Cards

Sector	Card 1	Card 2	Card 3
0	6d 04 7e 00 94 8b	04 fa 1a e6 c9 f2	dd 6b b7 5f 85 e6
1	c2 84 c2 bd 23 d0	ed 3c 68 b7 51 69	b2 30 8b 5b c8 c2
2	34 61 32 40 f6 61	b4 d2 83 88 ad 53	97 71 75 bd 52 51
3	ad ca 21 9d f0 ed	26 e6 12 50 29 97	63 c5 e0 50 88 0a
4	d4 e3 de d6 ef 25	be 36 07 16 18 4b	45 bb 16 c6 a9 44
5	dc 8e 48 14 78 45	dc e7 cb 25 78 0d	5d 43 59 4d 1d 14
6	66 17 09 94 56 52	f1 61 db 8c 25 fb	3c 18 4f 40 2d be

To test whether the keys produced were accurate, Key B for Sector 0 was used to change the access conditions and keys on Block 0. Both key A and B were changed to FFFFFFFFFFFF and the access conditions to allow all operations with key A - reading (except key A), writing, increment and so on. Basically, the default manufacturing access conditions. The new Key A was then used to authenticate the sector, write data to block 2 and then restore the original keys (including B) and the access conditions. The result of the writing experiment was successful and the output, taken using NFC TagInfo, can be viewed in Figure 32.



```
Sector 0:
b0b85931600804006263646566676869
b00003e103e103e103e103e103e10000
492057524f5445204845245203a2921
a0a1a2a3a4a50f078fc1------------
```

```
Sector 0:
��Y1`bcdefghi
�������
I WROTE HERE :)!
��������------
```

Figure 32. Sector 0 of the Ühiskaart after writing operation using Key B recovered with MFOC

One of the basic principles of MIFARE cards is that the sector 0 block 1 is read-only and the UID of the card is unchangeable therefore to clone the Ühiskaart a UID changeable card would be required. The ChameleonMini, with its ability to imitate MIFARE Classic 1K 4-byte UID cards, was used to create a clone of the bus card. The memory dump generated by MFOC, which contained the B keys for sectors 0 to 6, was uploaded to the ChameleonMini. The clone was then tested by tapping it at the validator on a Public Transport Bus in Tallinn. The validator accepted the card and displayed the amount present on the card.

To summarize, the Ühiskaart can be trivially cloned. The DoS attacks against the cards are possible, however, the uniqueness of the B keys on each card requires each card to be cracked individually. The exploitation, however, is not trivial as it requires the attacker to be in contact with the victim's card for a significant amount of time.

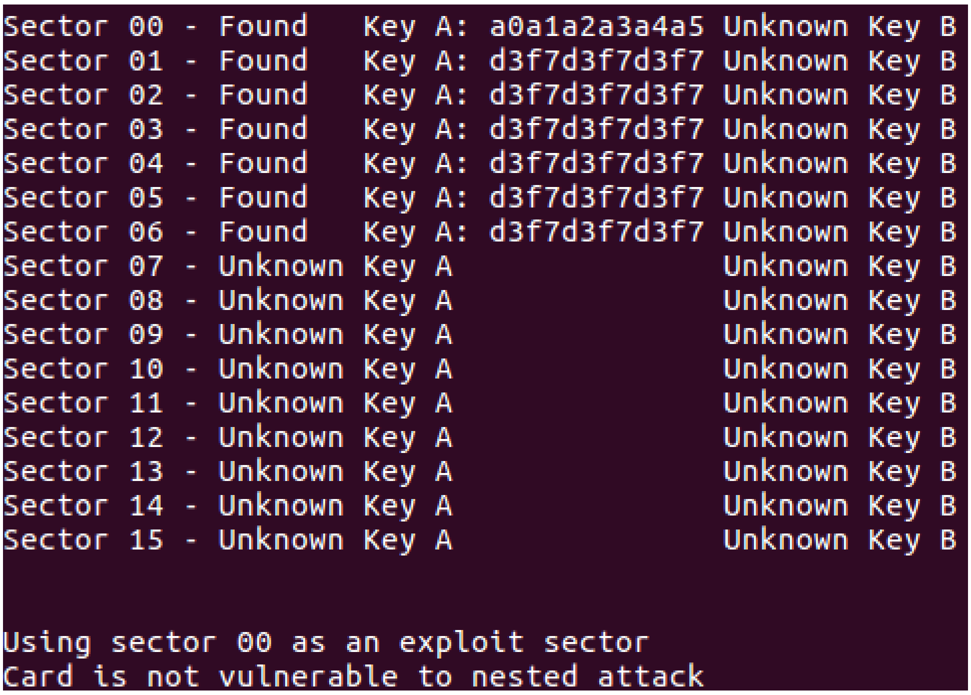
ISIC

The second card discovered to be MIFARE Classic was the ISIC card, described in Section 2.2.5 and shown in Figure 11. Not only is the ISIC a magnetic-stripe card but it is also a MIFARE Classic 1K 7-byte UID card. Older versions of the card, however, are known to have 4-byte UIDs. The contents of this card (keys and data structure) are similar to that of the Ühiskaart and hence it can be used for validation on public transport. The memory dump for the readable sectors can be seen in Appendix 3 Table 24. The notable difference to that of the Ühiskaart's memory dump (Appendix 3 Table 23) is that this card only contains 7 sectors. The other 9 sectors are considered by

MIFARE Classic Tool and NFC TagInfo to be either dead or keys suitable for reading cannot be found.

The important information that can be extracted from the memory dump are the card UID 0477D2BA153C80, card type “pilet.ee:ekaart:2”, card expiration date 1712 in block 6 (shown also on the front of the card in Figure 11), card PAN 9233731680120315877, card number 80120315877 and card’s issuer certificate found at http://pilet.ee/crt/92337316-0001.crt (issuer being identified as a school). It should be noted that unlike the Ühiskaart, the card number found on the front of the card does not match the card number in the signature data. In addition, neither the card number printed on the card nor the one encoded in the token can be used to search for valid tickets on pilet.ee. Instead the personal code of the card user has to be used. It should also be noted that a user is required to login into pilet.ee and associate the ISIC card number with the user’s personal ID code in order to use it as a ticket in public transport.

MFOC was used to try to extract the B keys stored on the ISIC. MFOC, however, was unable to gain the keys giving an error “Card is not vulnerable to nested attack” as shown in Figure 33. MFOC most likely aborted its operation as all the sectors are not readable. This failure also resulted in a memory dump of the card data not being produced.



```
Sector 00 - Found   Key A: a0a1a2a3a4a5 Unknown Key B
Sector 01 - Found   Key A: d3f7d3f7d3f7 Unknown Key B
Sector 02 - Found   Key A: d3f7d3f7d3f7 Unknown Key B
Sector 03 - Found   Key A: d3f7d3f7d3f7 Unknown Key B
Sector 04 - Found   Key A: d3f7d3f7d3f7 Unknown Key B
Sector 05 - Found   Key A: d3f7d3f7d3f7 Unknown Key B
Sector 06 - Found   Key A: d3f7d3f7d3f7 Unknown Key B
Sector 07 - Unknown Key A               Unknown Key B
Sector 08 - Unknown Key A               Unknown Key B
Sector 09 - Unknown Key A               Unknown Key B
Sector 10 - Unknown Key A               Unknown Key B
Sector 11 - Unknown Key A               Unknown Key B
Sector 12 - Unknown Key A               Unknown Key B
Sector 13 - Unknown Key A               Unknown Key B
Sector 14 - Unknown Key A               Unknown Key B
Sector 15 - Unknown Key A               Unknown Key B


Using sector 00 as an exploit sector
Card is not vulnerable to nested attack
```

Figure 33. Failed MFOC operation performed on ISIC card

To test if the card can be successfully cloned, it was used for validation in public transport. A memory dump was created using the readable information and B key values of FFFFFFFFFFFF. The memory dump was then uploaded to the ChameleonMini emulating a MIFARE Classic 1K 7-byte UID card. The clone performed a successful validation in public transport indicating that the missing sectors and B keys are unnecessary for a successful clone.

The ISIC card can be used not only to validate bus rides, but also as a means of gaining access to various student-related locations. The clone used in public transport was also able to pass the validation check to gain entry into the gym at TTU. However, in order to determine the exact information required for the successful validation, the ChameleonMini was used to sniff the communication between the card and the gym reader. The results can be seen in Appendix 1. The output shows that the reader does not read any sectors but instead just requests the UID of the card. To test this hypothesis, the memory dump of a blank MIFARE Classic card was uploaded to the ChameleonMini with the UID set to that of the ISIC card. The validation was successful, indicating that a UID of a valid ISIC card is enough to gain entrance to the TTU gym.

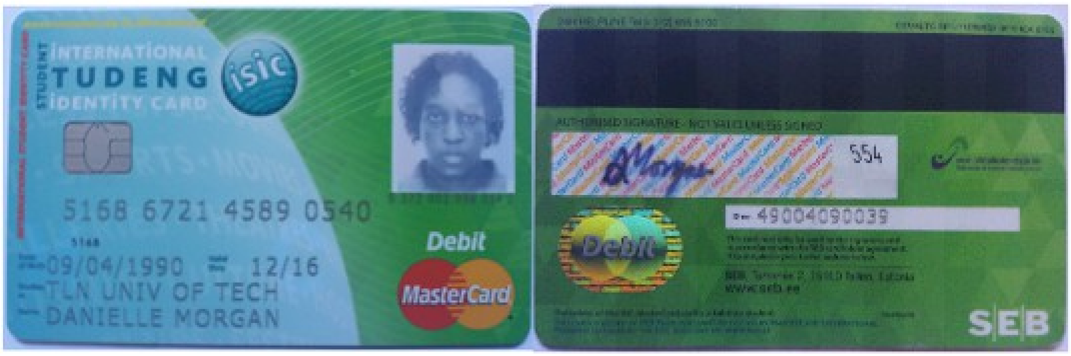
To summarize, a valid clone that can be used in public transport can be created from the readable sectors and keys. The ISIC is not vulnerable to a DoS attack as the B keys for the card are not recoverable. In order to create a clone to access the TTU gym, only the UID emulation is required.

SEB ISIC

The third and final card analysed as a MIFARE Classic card was the SEB ISIC card which is MIFARE Classic 1K 4-byte UID card. This card combines the functionality of an international Student card, international MasterCard debit card and a ticket used in the public transportation system[1]. This card like the previous two has information which is required to use public transportation system and can also be used to gain access to the TTU gym. The visual information that can be gained, as seen in Figure 34 (a), include the ISIC card number, a picture of the card holder, the date of birth, card's expiration

[1] http://www.seb.ee/eng/everyday-banking/debit-cards/isic-and-itic-cards

date and the card holder’s name and school. On the back of the card, Figure 34 (b), the personal ID code of the card holder can be found.



(a) (b)

Figure 34. The front (a) and back (b) of the SEB ISIC card

The memory dump for sectors that could be read can be found in Appendix 3 Table 25. The important information contained in this card are the card UID 4BF2ACF8, card type “pilet.ee:ekaart:2”, card expiration date 1612 (currently expired), card PAN 9233733180140500507, card number 80140500507 and card issuer certificate found at http://pilet.ee/crt/92337331-0002.crt (card issuer can be identified as SEB). Similarly as for the standard ISIC, the card number found on the front of the card does not match the card number in the signature data, therefore the personal ID code of the card user would have to be used to check the valid ticket information online.

Similarly as for the standard ISIC card, this card caused MFOC to abort its operation due to sectors 7 to 15 being classified as dead sectors. The cloning experiment was performed identically to the standard ISIC. The memory dump of a valid SEB ISIC, was created by substituting B keys with the value FFFFFFFFFFFF. The memory dump was then uploaded to the ChameleonMini using the 1K 4-byte UID mode and successfully used at the validator in the public transport as well at the TTU gym.

Pilveprint

As mentioned before, Pilveprint[1] is a public printing service. Pilveprint does not provide its own card to its clients, but allows the use of the Ühiskaart for identification. After creating an account in the self-service portal, a Tallinn Bus Card (Ühiskaart) can be

[1] http://pilveprint.overall.ee/support/

linked to the account by entering the card number that is printed on the back of the Ühiskaart. A user is then able to upload documents to the service and release them by inserting the card into the reader on any printer at the selected print location. Additionally, the user can insert the card and create scans or make copies without having to interact with the web service.

Pilveprint does not utilize all the information present on the card to identify the user and as such, a clone of the Ühiskaart can be made with a standard MIFARE Classic card. Pilveprint compares the UID of the card (first 4 bytes in block 0) with the UID in the signature data (last 4 bytes in block 9) and if there is a match, the card number is extracted without performing signature verification. If the card number exists in the database of registered cards, the user is logged into their account and is able to use the functions of the printer.

Pilveprint explicitly requires the Ühiskaart as the card used for identification. However, since the ISIC and SEB ISIC cards both have similar memory structures to the Ühiskaart, they should also be accepted for identification to the printers. To verify this, the ISIC card number was linked to the Pilveprint account and the card was tested at the printers to determine if access could be obtained. The authentication, however, was unsuccessful, which can be attributed to the difference in UID length, since the Ühiskaart has a 4-byte UID, but the ISIC a 7-byte UID. The test was then repeated using the SEB ISIC which has a 4-byte UID. This card was successfully authenticated allowing access to the printer functions. This shows that the 4-byte ISIC (older version ISIC cards) or the SEB ISIC can be used as a safer substitute for the Ühiskaart, since ISIC cards do not place the card number on the card's surface.

Regarding the fraud detection in Pilveprint, while the history of the documents sent to the printer is kept and can be viewed in the self-service portal, the paid actions such as copying or scanning executed at the printing machine are not registered. Providing more detailed information about activities performed with user's credit would help to investigate such fraud cases.

In summary, Pilveprint can be accessed with either the Ühiskaart, the ISIC card or the SEB ISIC card. However, since Pilveprint does not utilize the digital signature scheme, the clone can be made by writing the card number of a victim's card into a standard Ühiskaart whose B keys have been recovered.

Bikeep Smart Bike Lock

Bikeep Smart Bike Lock[1] is a service in Tallinn and Tartu which allows a user to secure their bicycle at a Bikeep locking station with a rack locking mechanism that is activated and deactivated by tapping the Ühiskaart at the terminal. In order to determine what information is used by the terminal to authenticate the card, the memory dump of a blank MIFARE Classic card was uploaded to the ChameleonMini with the UID set to that of the Ühiskaart. The ChameleonMini was able to successfully unlock the terminal that was locked by the Ühiskaart. This shows that the only parameter used by the bike locking system is the UID of the card. It was verified that the terminals support MIFARE Classic cards with both 7-byte and 4-byte UIDs.

An interesting security feature observed, was that a card (UID) can only lock one rack at a time. This makes a potential DoS attack more expensive, since the attacker cannot use a single card to lock all the racks deployed at a Bikeep station.

In summary, Bikeep Smart Bike Lock uses the UID of MIFARE Classic cards to authenticate the card used to lock the bicycle. This means that in order to make a clone, the UID of the card has to be read from the victim's card and written to a UID changeable MIFARE Classic card.

3.6 MIFARE Ultralight C

The MIFARE Ultralight C is a contactless smart card with an operating distance of up to 100mm designed for use in applications such as public transportation, event ticketing and loyalty applications. The card comes with a 192 bytes EEPROM memory organized into 48 pages of 4 bytes each, as shown in Table 15, and has several security features including 3DES Authentication, a unique 7-byte serial number for each device, a programmable One Time Programmable (OTP) area and a read-only locking function. [4]

[1] https://bikeep.com/smart-commercial-bike-rack/

Table 15. Memory organization of the MIFARE Ultralight C [[4] , Table 5]

Page address		**Byte number**			
Decimal	**Hex**	**0**	**1**	**2**	**3**
0	00h	serial number			
1	01h	serial number			
2	02h	serial number	internal	lock bytes	lock bytes
3	03h	OTP	OTP	OTP	OTP
4 to 39	04h to 27h	user memory	user memory	user memory	user memory
40	28h	lock bytes	lock bytes	-	-
41	29h	16-bit counter	16-bit counter	-	-
42	2Ah	authentication configuration (AUTH0)			
43	2Bh	authentication configuration (AUTH1)			
44 to 47	2Ch to 2Fh	authentication key			

The serial number or UID of the card is 7 bytes in length and has two Block Check Character bytes (BCC). These bytes are programmed into the first 9 bytes of the memory stretching from page 0 to the first byte in page 2. The first BCC, stored in byte 3 of page 0, is calculated by XOR-ing the first 3 bytes of the UID with the cascade tag byte 88h. The second BBC, stored in byte 0 of page 2, is calculated by XOR-ing the last 4 bytes of the UID together. For devices created by NXP the first byte in the UID is 04h. These values are programmed and write protected in the production phase. [4]

Each page from 03h to 0Fh can be individually locked by setting a specific bit to logic 1 in the lock bytes of page 2. The locking mechanism prevents further write access to the page causing it to become read-only memory. In Figure 35, L# refers to the page that is locked when the bit is set to 1. The block-locking bits (BL) are used to prevent further changes to the locking configuration of the corresponding bits. The default value for these 2 bytes are 00 00h.[4]

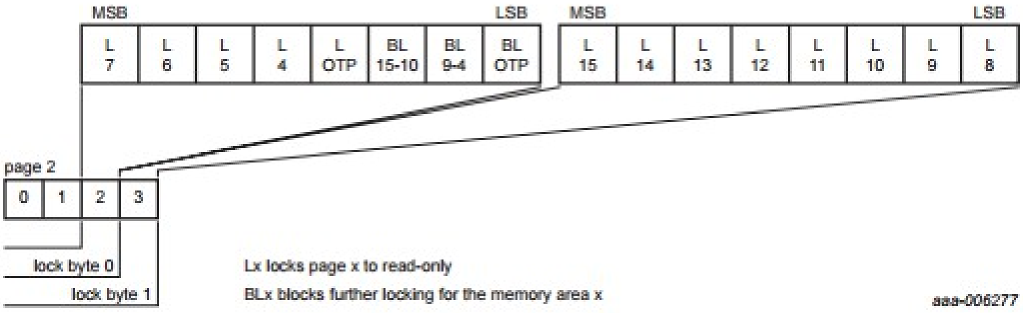


Figure 35. Locking functionality of the lock bytes in page 2 [[4] , Figure 6]

The lock bytes of page 40 are used to lock page 16 to 47. The default value for these bytes is also 00 00h, however, unlike the first 2 lock bytes, each bit here is responsible for locking 4 pages.[4] The locking functionality of each bit can be seen in Figure 36.

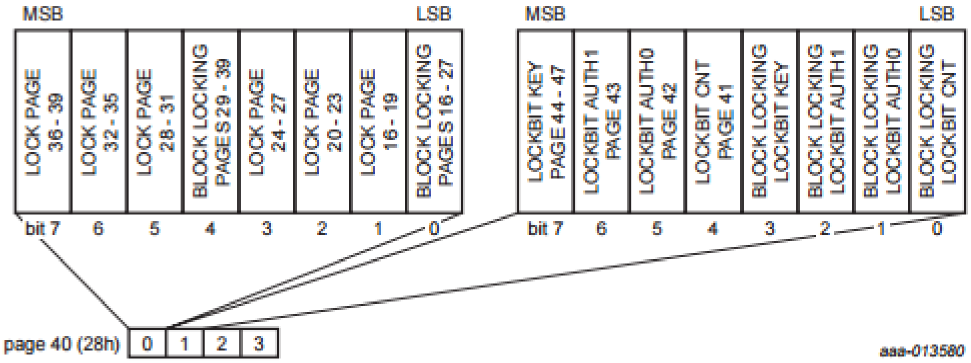


Figure 36. The locking functionality of the lock bytes in page 40 (28h) [[4] , Figure 8]

The OTP area found on page 3 has a default value of 00 00 00 00h. In this area, if a bit is set to “1” it cannot be reset to “0” again with write access being controlled by lock byte 0 as seen in Figure 36. When the card is formatted as a Type 2 Tag in initialised state the OTP bytes are set to E1 10 12 00 with Byte 3 signifying that there is read and write access without any security. [4] , [5]

Memory access rights in the card are dependent on the values that are stored in the authentication configuration pages. In these pages only the first byte is used. AUTH0 on page 42 defines the page address starting from which authentication is required for access. Valid address values range from 03h (3) to 30h (48) where a value of 30h signifies that memory protection has been disabled. AUTH1, page 43, determines if write access or both read and write access is restricted. If the first bit in AUTH1 is set to 1 then only write access is restricted without authentication and if it is set to 0 then both read and write access is restricted. The default value for AUTH0 is 30h and 00h for AUTH1. [4]

Page 41 contains a 16-bit one-way counter which occupies the first 2 bytes and has a default value of 0000h. After the initial write to this area, with a value ranging from 0001h to FFFFh, the counter can be incremented in values from 01h to 0Fh. This area is recommended to be protected by authentication.[4]

The 3DES authentication implemented in the Ultralight C card proves that two entities hold the same secret and communication can occur between the two parties. The applied encryption algorithm is the 2 key 3DES encryption in CBC mode as described in ISO/IEC 10116. The 16 bytes of the 3DES key are stored in page 44 to 47. Key 1 is stored in page 44 and 45 and key 2 in page 46 and 47 with the first key byte stored in the first byte of page 44 and 46, respectively. The authentication key pages are write-only and this feature remains regardless of the configuration settings. [4]

Finally the data pages can be found from page 04h to 27h totalling 144 bytes. The initial state of each byte in this area is 00h. Write access to these pages can be permanently restricted using the lock bytes, while read and write access can be permanently or temporarily restricted using the authentication configuration settings.[4]

The default configuration values on the card allow for complete personalization of the memory without knowledge of the authentication key. All pages and functionality are available since the lock bytes are set to 00h. This configuration, however, means that after personalization the authentication key should be changed and the authentication configuration set to prevent the AUTH bytes and key from being overwritten without authentication.[4]

Currently there are no publicly known practical attacks against the MIFARE Ultralight C cards that could be used to recover the cryptographic keys used by the card.

3.6.1 Methodology

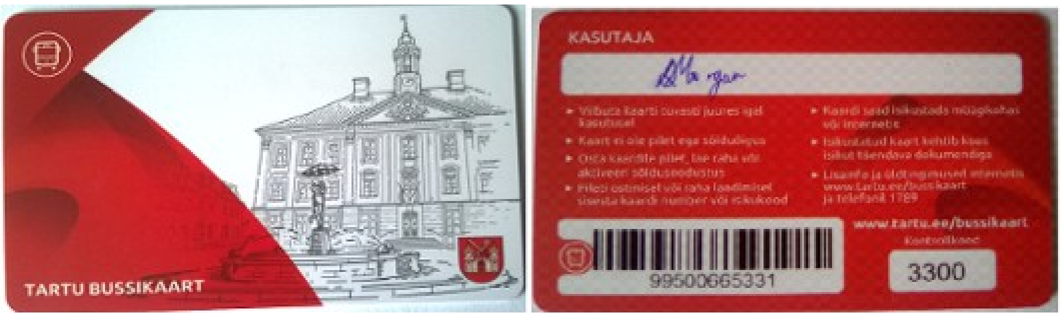
The contents of the cards discovered to be in this category were first scanned with NFC TagInfo mobile application to determine the access conditions on the card and to determine if the authentication key was set to the default value. A memory dump of the card data was then created using the ACR112U and a Python script. The contents of the card were inspected to determine how the information stored is used (at least 2 cards were inspected for comparison) and what security features available were utilized.

3.6.2 Results

Tartu Bus Card (Tartu Bussikaart)

The Tartu Bus card was identified as an MIFARE Ultralight C card. This card can be purchased for 2€ from several locations including supermarkets, R-Kiosks and other market chains[1]. The Tartu Bus card can be used to validate rides on public transport in Tallinn, Tartu and other counties.

The Tartu Bus card is red and white in appearance with white and black text as shown in Figure 37 below. The relevant parts of the card include a signature field and the bus card number along with the accompanying bar code, located on the back of the card, Figure 37 (b).



(a) (b)

Figure 37. The front (a) and back (b) view of the Tartu Bus Card

The Tartu Bus card contains data similar to that seen in the Ühiskaart and its full contents can be viewed in Appendix 3 Table 26. The information that can be extracted from this memory dump includes the card's UID, the signature data (and its relevant information), the signature value, access conditions and authentication key.

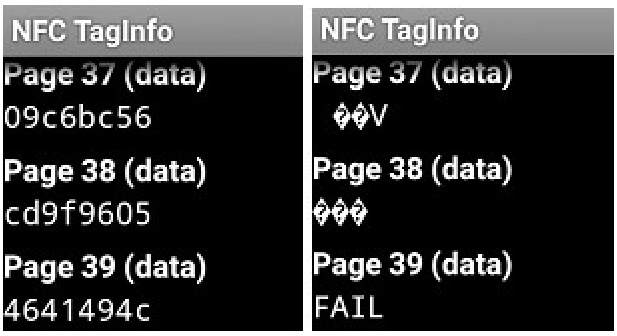
The UID of the card as seen in page 0 and 1 is 047F0DDA8D3A84 with FE being the first BCC. The signature details start in page 4 with the first byte (0x03) indicating the

[1] http://www.tartu.ee/et/bussikaardi-korduma-kippuvad-kusimused

presence of an NDEF and the second byte (0x84) indicating the total length of the message. The signature data, commences at the second byte in page 5 (0x70) and extends to the third byte in page 21 (0x84). Included in the signature data are the card type "pilet.ee:ekaart:3", the PAN 3086490099500665331, the card number 99500665331 as shown on the back of the card and the card UID starting at page 20. The signature starts at page 25, with the first byte 0x36 (54) indicating the length of the field, and extends to page 38. The signature of the Tartu Bus card differs from the Ühiskaart in that the signature was created using Elliptic Curve Digital Signature Algorithm (ECDSA 192-bit key) while the Ühiskaart signature was created using an RSA 1024-bit key. Another notable difference is that the card issuer certificate is not present on this card, possibly because the size of user memory remaining is insufficient to hold this information.

From Table 26, it can be seen that the security features have not been fully utilized on the card. The OTP bytes, E1 10 12 00, identifies the card as being in the initialised state while all the the lock bytes are set to 0x00 indicating that no page is set to read-only mode and block locking has not been enabled. Furthermore, the authentication configuration in page 42 (0x2A) and page 43 (0x2B) are at the default values indicating that memory protection has been disabled. Finally page 41 shows the counter value to be 0 and the authentication key is set to the default value "BREAKMEIFYOUCAN!".

Since this card both possesses the default key and requires no authentication to perform read or write operations, any section of the card can be overwritten with the exception of the read-only areas. A successful write operation to page 39 without providing authentication can be seen in Figure 38. This shows that a valid card can have its data changed to effectively invalidate it.



```
Page 37 (data)
09c6bc56
Page 38 (data)
cd9f9605
Page 39 (data)
4641494c
```

```
Page 37 (data)
  ��V
Page 38 (data)
���
Page 39 (data)
FAIL
```

Figure 38. Successful write operation to the Tartu Bus card

As with the Ühiskaart, the valid tickets or the balance present on the card can be viewed at pilet.ee[12] using either the card number or in the case of a personalized card, the card holder's personal ID code. However, unlike the Ühiskaart, the Tartu bus card cannot be used at Pilveprint and Bikeep Smart Bike Lock.

In summary, the Tartu Bus card can be completely read and overwritten therefore allowing an attacker to perform a DoS attack and giving all the information required to make a clone. A UID changeable card, however, would be needed for the clone to pass the validation check at the bus terminal. The UID changeable Ultralight C cards, however, are not as readily available as the UID Changeable Classic cards. For example, currently on aliexpress.com there is only one merchant who sells UID changeable Ultralight C cards, while there are several merchants selling UID changeable MIFARE Classic cards.

Rimi Card

The Rimi card described in Section 2.2.9 and shown in Figure 15 is not only a magnetic-stripe card but also a MIFARE Ultralight C card. The readable contents of this contactless card can be viewed in Appendix 3 Table 27. The first piece of information learnt is the card UID 04DCABC24A4E80. The second bit of knowledge comes from page 2 were the lock bytes show that no locking restrictions have been placed on pages 3 to page 15. The final bit of information before the data blocks is that the OTP is set to the production value of 0x00000000.

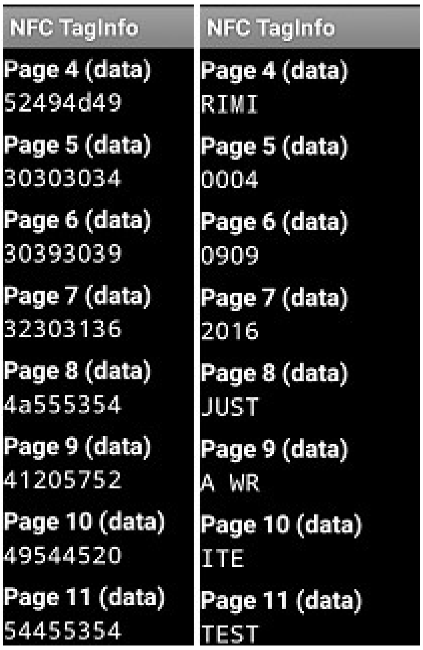
The first 4 pages in the data blocks contain an identifier RIMI0002 and a date 19052016. This identifier may be indicative of the location where the card was acquired and the date may be the card manufacturing date. This date value is also present in field 9 of Track 3 on the magnetic stripe. The data blocks from page 8 to page 21 remain unchanged from the default production value, while pages 22 and 23 repeat the first 2 pages as read by NFC TagInfo. This information was, however, unreadable by the ACR122U. After page 23, however, no more data can be read from the card indicating that the authentication key has been changed from the default value and that AUTH0 has been set to 16h (page 22) and AUTH1 has been set to restrict both read and write

[1] https://tartu.pilet.ee/tickets/personalcode

[2] https://www.pilet.ee/viipe/uhiskaart/activetickets

access without authentication. The counter and the secondary lock bytes cannot be determined due to this read restriction.

The change from the default key means that there is probably one standard authentication key for all cards stored in the terminals in Rimi stores. The problem with this is that once the key is found the security of all cards is compromised. Additionally, the readable data on the card is also writeable, as shown in Figure 39. Therefore, if this data is used to identify the card then an attacker would be able to perform a DoS attack preventing the user from using the NFC capabilities of the card.



```
NFC TagInfo        NFC TagInfo
Page 4 (data)      Page 4 (data)
52494d49           RIMI
Page 5 (data)      Page 5 (data)
30303034           0004
Page 6 (data)      Page 6 (data)
30393039           0909
Page 7 (data)      Page 7 (data)
32303136           2016
Page 8 (data)      Page 8 (data)
4a555354           JUST
Page 9 (data)      Page 9 (data)
41205752           A WR
Page 10 (data)     Page 10 (data)
49544520           ITE
Page 11 (data)     Page 11 (data)
54455354           TEST
```

Figure 39. A successful write operation to the RIMI card

To summarize, with the current knowledge of the Rimi card, it would present a challenge to be successfully cloned. An attacker would be unable to read all the contents of the card without providing authentication and therefore would be unable to write this data to a clone. However, if only the publicly readable data is used for authentication, a successful clone could be made.

3.7 Summary

MIFARE NFC card technology offers more advanced security features than the basic tag identifier storage on Low Frequency RFID cards. However, the use of the security features provided by MIFARE technology has to be considered. If the symmetric keys used for reading the card are not secret, a successful clone can be made.

The two cards (Rimi and Elron) could not be cloned because the keys used to read the cards were unknown. The keys for these cards could be kept secret because there was no need to share the keys outside of that business. To guarantee security in case of multi-purpose use, a better technology using asymmetric key encryption schemes would be required.

4 Estonian Identity Card (EstEID)

The Estonian electronic ID card is a smart card capable to perform cryptographic operations with the authentication and digital signature RSA private key stored in the card [12] . The communication interface between the ID card smart card EstEID application and terminal is well documented in the EstEID technical specification [12] .

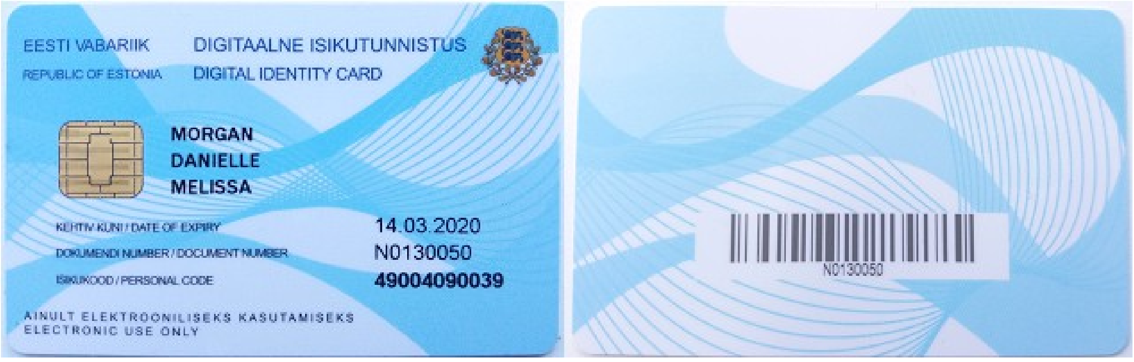
In regards to loyalty schemes, the EstEID card contains a personal data file which can be read by sending the correct APDU (Application Protocol Data Unit) commands to the card. The personal data file contains 16 record fields and their names and lengths can be viewed in Table 16. This information can then be queried from the card to identify the customer. In addition, the card also contains two public key certificates; one for authentication operations and the other for digital signatures, which can also be used to verify the validity of the card.

Table 16. Personal data file stored in ID card v3.5 [[12] , Table 2-1]

Record number	Content	Length
1	Surname	max 28 bytes
2	First name line 1	max 15 bytes
3	First name line 2	max 15 bytes
4	Gender Values: “M” – Male “N” – Female	1 byte
5	Nationality (3 letters)	3 bytes
6	Birth date (dd.mm.yyyy)	10 bytes
7	Personal ID code	11 bytes
8	Document Number	9 bytes
9	Document Expiry Date (dd.mm.yyyy)	10 bytes
10	Place of Birth	max 35 bytes
11	Date of Issuance (dd.mm.yyyy)	10 bytes
12	Type of Residence Permit	max 50 bytes
13	Notes line 1	max 50 bytes

Record number	Content	Length
14	Notes line 2	max 50 bytes
15	Notes line 3	max 50 bytes
16	Notes line 4	max 50 bytes

Suitable identifiers to be used in loyalty schemes is personal ID code and document number. While the personal ID code stays the same for the person, the document number is different for every card issued to the person. It is, however, recommended to use the document number when the card is used in access control systems as the card then can be revoked if the card is lost [13] . Other concerns with use of the loyalty card include the damage to the chip after repeated use. The Digital Identity card (Digi-ID), shown in Figure 40, contains the same file structure as the ID card and can be used to minimize the wear and tear on the ID card chip. The Digi-ID, however, can be used only for electronic identification, because it does not serve physical identification purposes.


EESTI VABARIIK
REPUBLIC OF ESTONIA
DIGITAALNE ISIKUTUNNISTUS
DIGITAL IDENTITY CARD
MORGAN
DANIELLE
MELISSA
KEHTIV KUNI / DATE OF EXPIRY
14.03.2020
DOKUMENDI NUMBER / DOCUMENT NUMBER
N0130050
ISIKUKOOD / PERSONAL CODE
49004090039
AINULT ELEKTROONILISEKS KASUTAMISEKS
ELECTRONIC USE ONLY
N0130050

(a) (b)

Figure 40. The front (a) and back (b) view of the Estonian Digital Identity Card

4.1 Methodology

The Estonian ID card can be used in two ways to prove the membership in loyalty programmes. In the first case, the information present on the surface of the card is scanned or read by the cashier and looked up in the customer database. This, however, requires the cashier to manually enter information unless the bar code is scanned. In the second case the customer identifiable information stored in the ID card is electronically read from the card using contact communication with ID card chip. The object of this study is the second use case, where the customer's ID card is electronically identified. The communication between the ID card and merchant's terminal is analysed using a special card made to imitate the structure of the ID card, but with the additional function of logging the APDUs sent to the card.

4.1.1 Design of Fake ID card

To implement ID card functionality in a smart card, a standard Java-Card [22] compliant smart card Feitian D11CR[1] was used. The first step in creating the Fake ID card was to change the ATR of the card to one recognized as that of an Estonian ID card. The Answer to Reset (ATR) gives information about the electrical communication protocol of the chip. Every contact card responds to reset with the ATR[12] . The ATR can be separated into two parts - the communication protocol configuration and the historical bytes which provide information about the card and can be freely changed. The second byte in the ATR can be used to identify the length of the historical bytes. For example if the byte is 0x6A then there are 10 historical bytes.

The original ATR of the Feitian card was 3B 6A 00 00 09 44 31 31 43 52 02 00 25 C3 with its historical bytes being 09 44 31 31 43 52 02 00 25 C3. The historical bytes of the card was programmatically changed to 45 73 74 45 49 44 20 76 65 72 20 31 2E 30 giving the card an overall ATR of 3B 6E 00 00 45 73 74 45 49 44 20 76 65 72 20 31 2E 30. This new ATR matches the ATR of the Digi-ID Card (EstEID v1.1 “MULTOS” cold). This change was sufficient to trick the terminals into believing that the card was one of the many versions of the Estonian ID card.

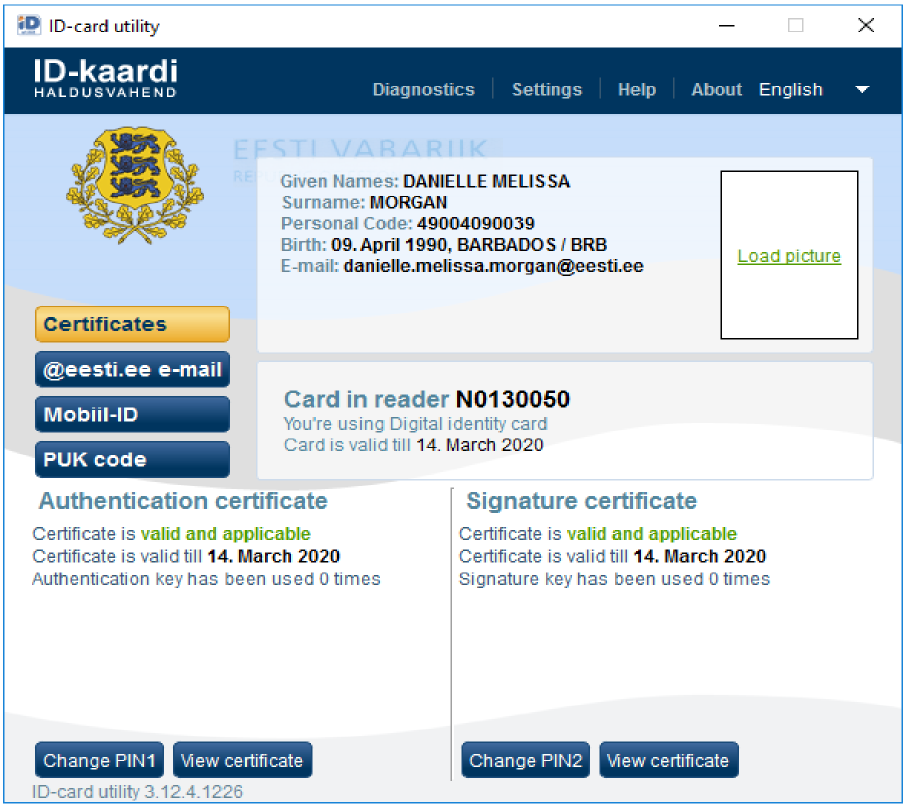
The second step that was required to use the card in the terminals was creating a Java Card applet which imitated that of the one stored on standard Estonian ID cards. To accomplish this task, the open source FakeEstEID.java [14] code written my Martin Paljak was modified to support the current structure of the ID cards. First the File Control Information (FCI), which is a combination of the File Control Parameters (FCP) and the File Management Data (FMD), was updated to the information present on the

[1] http://www.grama.es/en/portfolio-items/feitian-d11cr/

real EstEID v3.5 card. The FCIs were obtained by sending the APDUs to request FCI data to a real Estonian ID card and recording the card's output. Secondly, the size of the byte array used to store the certificates was increased to support the larger certificate sizes.

The logging functionality was the final change made to the applet code. Every APDU sent to the applet was recorded in Type, Length, Value (TLV) structure in smart card's EEPROM. The tag values were: 0x00 representing an APDU sent to the card, 0x01 for a reset, 0x02 for when the applet was selected as the default applet, 0x03 for when the applet was explicitly selected, 0x04 for deselection of the applet, 0x05 to represent communication over T0 protocol and 0x06 for communication over T1 protocol.

Once the applet was loaded to the card, a Python script was used to extract the personal data file values and the certificates from the real Digi-ID card and to write the values onto the FakeID card. The card was then tested in the ID-card utility on the Windows platform, the output of which can be seen in Figure 41, and the APDUs with annotations sent to the card can be viewed in Table 17.



Given Names: DANIELLE MELISSA
Surname: MORGAN
Personal Code: 49004090039
Birth: 09. April 1990, BARBADOS / BRB
E-mail: danielle.melissa.morgan@eesti.ee

Card in reader N0130050
You're using Digital identity card
Card is valid till 14. March 2020

Authentication certificate
Certificate is valid and applicable
Certificate is valid till 14. March 2020
Authentication key has been used 0 times

Signature certificate
Certificate is valid and applicable
Certificate is valid till 14. March 2020
Signature key has been used 0 times

ID-card utility 3.12.4.1226

Figure 41. The ID card utility output from the Fake Digi-ID

Table 17. Edited[1] output of the APDUs sent to the Fake card from the ID card utility in Windows 10

APDU	Description
01	card reset
05	T0_protocol
02	default select
00 a4 04 00 0b a0 00 00 03 97 43 49 44 5f 01 00	Driver discovery process
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 01 08 02 ee ee	
00 a4 02 04 02 50 44	Select Personal Data File
00 b2 08 04 00	Read Document number
00 a4 00 0c 00	Select Master File
00 a4 02 0c 02 00 16	Select Pin retry counter
00 b2 01 04 00	Read PIN1 retries left
00 b2 02 04 00	Read PIN2 retries left
00 b2 03 04 00	Read PUK retries left
00 a4 01 0c 02 ee ee	Select EstEID Dedicated File
00 a4 02 0c 02 00 33	Select Key references file
00 b2 01 04 00	Read key references record 1
00 a4 02 0c 02 00 13	Select Key Use counter
00 b2 03 04 00	Read times Auth key used
00 b2 01 04 00	Read times Signature key used
00 a4 02 0c 02 50 44	Select Personal Data File
00 b2 01 04 00	Read Surname
00 b2 02 04 00	Read First name line 1
00 b2 03 04 00	Read First name line 2
00 b2 04 04 00	Read Gender
00 b2 05 04 00	Read Nationality
00 b2 06 04 00	Read Birth date
00 b2 07 04 00	Read Personal identification code
00 b2 08 04 00	Read Document number
00 b2 09 04 00	Read Expiry date
00 b2 0a 04 00	Read Place of birth
00 b2 0b 04 00	Read Date of issuance
00 b2 0c 04 00	Read Type of residence permit
00 b2 0d 04 00	Read Notes line 1
00 b2 0e 04 00	Read Notes line 2
00 b2 0f 04 00	Read Notes line 3
00 a4 02 00 02 aa ce	Select auth cert
00 b0 00 00 00	Read cert
00 a4 02 00 02 dd ce	Select signature cert
00 b0 00 00 00	Read cert

[1] The GET RESPONSE APDUs and the repeated READ BINARY APDUs for the certificates were removed from the table for readability purpose

In the stores or businesses where the personal data file was read the Fake ID card was inserted into the reader to log the APDUs. The APDUs were then extracted and annotated. The APDU memory store on the Fake ID card was cleared to be used in the next experiment.

4.2 Results

This section describes the results obtained from merchants that use ID card for electronic identification.

4.2.1 Forum Cinemas

Forum Cinemas AS is a cinema operator in Estonia whose cinemas include Coca-Cola Plaza in Tallinn, Ekraan in Tartu and Centrum in Viljandi[1]. Forum Cinemas offers a loyalty program known as the Forum Cinemas Club. Members of this program can purchase tickets and snacks at a cheaper price, gain access to premiers and special sessions and other benefits. To become a member of the club, an application form can be submitted online with the following information: first name, last name, personal ID code, e-mail address and mobile number.

To gain the benefits of the club, when purchasing a ticket at the box office or snacks at the concession stand the user can insert their card into the reader to identify themselves as club members. Alternatively at the concession stand the bar code of the personal ID code located at the back of the card can be scanned. To determine the information that is extracted at the reader the test card was inserted at the concession stand at Coca-Cola Plaza. The full output of the dump can be viewed in Table 18. From the table it can be seen that the entire contents of the personal data file are extracted even though the name and personal ID code are the only fields entered in registration for the loyalty program. The receipts generated include the name of the client, as seen in Appendix 2 Figure 53.

[1] http://www.forumcinemas.ee/eng/Cinemas/ForumCinemas/

Table 18. APDUs sent to the Fake ID card at Forum Cinemas Coca Cola Plaza

APDU	Action
01	card reset
05	T0_protocol
02	select by select()
00 a4 04 00 0e 31 50 41 59 2e 53 59 53 2e 44 44 46 30 31	Card Discovery Process
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	Select EstEID Dedicated File
00 a4 02 04 02 50 44	Select Personal Data File
00 b2 01 04 00	Read Surname
00 c0 00 00 06	Get Response: 6 bytes expected
00 b2 02 04 00	Read First name line 1
00 c0 00 00 08	Get Response: 8 bytes expected
00 b2 03 04 00	Read First name line 2
00 c0 00 00 07	Get Response: 7 bytes expected
00 b2 04 04 00	Read Gender
00 c0 00 00 01	Get Response: 1 bytes expected
00 b2 05 04 00	Read Nationality
00 c0 00 00 03	Get Response: 3 bytes expected
00 b2 06 04 00	Read Birth date
00 c0 00 00 0a	Get Response: 10 bytes expected
00 b2 07 04 00	Read Personal identification code
00 c0 00 00 0b	Get Response: 11 bytes expected
00 b2 08 04 00	Read Document number
00 c0 00 00 08	Get Response: 8 bytes expected
00 b2 09 04 00	Read Expiry date
00 c0 00 00 0a	Get Response: 10 bytes expected
00 b2 0a 04 00	Read Place of birth
00 c0 00 00 0e	Get Response: 14 bytes expected
00 b2 0b 04 00	Read Date of issuance
00 c0 00 00 0a	Get Response: 10 bytes expected
00 b2 0c 04 00	Read Type of residence permit
00 c0 00 00 01	Get Response: 1 bytes expected
00 b2 0d 04 00	Read Notes line 1
00 c0 00 00 01	Get Response: 1 bytes expected
00 b2 0e 04 00	Read Notes line 2
00 c0 00 00 01	Get Response: 1 bytes expected
00 b2 0f 04 00	Read Notes line 3
00 c0 00 00 01	Get Response: 1 bytes expected

4.2.2 Olerex

AS Olerex is an Estonian oil company which offers a loyalty program based on the ID-card that provides customer's discounts on fuel and other services[1]. To register for the program the user is required to provide their first and last name, personal ID code, email address and phone number. To determine the APDUs sent to the card the Fake ID card was used at the Olerex terminal. The APDUs sent to the card can be viewed in Table 19. From this table it can be seen that the entire personal data file is read.

Table 19. APDUs sent to the Fake ID card from the Olerex Terminal

APDU	**Action**
01	card reset
05	T0_protocol
02	select by select()
00 a4 04 00 0e 31 50 41 59 2e 53 59 53 2e 44 44 46 30 31	Card Discovery Process
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	Select EstEID Dedicated File
00 a4 02 04 02 50 44	Select Personal Data File
00 b2 01 04 00	Read Surname
00 c0 00 00 07	Get Response: 7 bytes expected
00 b2 02 04 00	Read First name line 1
00 c0 00 00 05	Get Response: 5 bytes expected
00 b2 03 04 00	Read First name line 2
00 c0 00 00 01	Get Response: 1 bytes expected
00 b2 04 04 00	Read Gender
00 c0 00 00 01	Get Response: 1 bytes expected
00 b2 05 04 00	Read Nationality
00 c0 00 00 03	Get Response: 3 bytes expected
00 b2 06 04 00	Read Birth date
00 c0 00 00 0a	Get Response: 10 bytes expected
00 b2 07 04 00	Read Personal identification code
00 c0 00 00 0b	Get Response: 11 bytes expected
00 b2 08 04 00	Read Document number
00 c0 00 00 09	Get Response: 9 bytes expected
00 b2 09 04 00	Read Expiry date
00 c0 00 00 0a	Get Response: 10 bytes expected
00 b2 0a 04 00	Read Place of birth

[1] http://olerex.ee/en/era/loyalty-program

APDU	Action
00 c0 00 00 0a	Get Response: 10 bytes expected
00 b2 0b 04 00	Read Date of issuance
00 c0 00 00 0a	Get Response: 10 bytes expected
00 b2 0c 04 00	Read Type of residence permit
00 c0 00 00 01	Get Response: 1 bytes expected
00 b2 0d 04 00	Read Notes line 1
00 c0 00 00 17	Get Response: 23 bytes expected
00 b2 0e 04 00	Read Notes line 2
00 c0 00 00 13	Get Response: 19 bytes expected
00 b2 0f 04 00	Read Notes line 3
00 c0 00 00 1c	Get Response: 28 bytes expected
00 b2 10 04 00	Read Notes line 4
00 c0 00 00 0f	Get Response: 15 bytes expected

4.2.3 Pilverprint

The Pilveprint printing service described in Section 3.5.2 can also be configured to work with the Estonian ID card. In the online account the user must specify the document number of the card to link it to the Pilveprint account. The user can then insert the card into the selected printer to release their documents. To determine the APDUs sent to the ID card the Fake ID card was tested at printer Gamma at TTU and printer Oeconomicum at UT. The APDUs registered to the card are shown in Table 20. The results in the table show that the only field read from the card is the document number.

Table 20. APDUs sent to the Fake ID card from printers Gamma and Oeconomicum

APDU	Action
01	card reset
05	T0_protocol
02	select by select()
00 a4 01 04 02 ee ee	Select EstEID Dedicated File
00 a4 02 04 02 50 44	Select Personal Data File
00 b2 08 04 00	Read Document number
00 c0 00 00 08	Get Response: 8 bytes expected

4.2.4 Prisma

Prisma Peremarket offers their customers an ID card based loyalty program known as Prisma Konto. This program allows the customer to gain Prisma bonus money from their purchases amounting from 0.5% to 5%[1]. To register for this program a customer fills out the online application providing their first and last names, Estonian personal ID code, phone number and email address. The customer can later modify their account by adding their gender and address. To show loyalty status a user can insert their card at the terminal before paying for the items both at standard and self-service checkouts. The Fake ID card, tested at the Kristiine and Annelinna shops, was used to capture the APDUs sent to the card and the full results can be seen in Table 21. The table shows that the personal ID code, document number and document expiration date are read from the personal data file.

Table 21. APDUs sent to the Fake ID Card from the Prisma terminal at the Kristiine and Annelinna shops

APDU	Action
01	card reset
05	T0_protocol
02	select by select()
00 a4 04 00 0e 31 50 41 59 2e 53 59 53 2e 44 44 46 30 31	Card Discovery Process
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	
01	card reset
05	T0_protocol
02	select by select()
00 a4 01 0c 02 ee ee	Select EstEID Dedicated File
00 a4 02 04 02 50 44	Select Personal Data File
00 b2 07 04 00	Read Personal identification code
00 c0 00 00 0b	Get Response: 11 bytes expected
00 b2 08 04 00	Read Document number
00 c0 00 00 09	Get Response: 9 bytes expected
00 b2 09 04 00	Read Expiry date
00 c0 00 00 0a	Get Response: 10 bytes expected

[1] http://www.id.ee/index.php?id=36094

4.2.5 TTU Library

To become a user of the library at TTU, a registration card must be filled out with the signature of the new reader. To access the library services, a valid library card is needed. For this purpose the ID card can be used[1]. To enter the library the ID card is inserted in the card reader and its data is read to determine whether the user has a valid library card. The Fake ID card was used to capture the APDUs sent to the card and the full output can be seen in Table 22. From this table it can be seen that the entire personal data file is read before access is granted to the library.

Table 22. APDUs sent to the Fake ID card by the terminal at the TTU library

APDU	Action
01	card reset
05	T0_protocol
02	select by select()
00 a4 01 0c 02 ee ee	Select EstEID Dedicated File
00 a4 02 04 02 50 44	Select Personal Data File
00 b2 01 04 1c	Read Surname
00 b2 02 04 0f	Read First name line 1
00 b2 03 04 0f	Read First name line 2
00 b2 04 04 01	Read Gender
00 b2 05 04 03	Read Nationality
00 b2 06 04 0a	Read Birth date
00 b2 07 04 0b	Read Personal identification code
00 b2 08 04 09	Read Document number
00 b2 09 04 0a	Read Expiry date
00 b2 0a 04 23	Read Place of birth
00 b2 0b 04 0a	Read Date of issuance
00 b2 0c 04 32	Read Type of residence permit
00 b2 0d 04 32	Read Notes line 1
00 b2 0e 04 32	Read Notes line 2
00 b2 0f 04 32	Read Notes line 3
00 b2 10 04 32	Read Notes line 4

4.3 Summary

The experiments show that the Fake ID card was accepted as a valid ID card by all terminals where it was tested. In most of the cases the terminals read the entire Personal Data File even though all the records present are not needed by the system. The personal

[1] https://www.ttu.ee/institutes/library-3/services-2/user-registration/user-registration-2/

ID code and document number are the only fields that should be used to identify the customer with the possibility of the expiration date to determine whether the document is still valid. Fields such as nationality, place of birth, type of permit and the notes should not be processed without customer consent, hence the processing of this data should be reviewed in the context of personal data regulation.

5 Summary and Conclusions

Magnetic stripe cards provide no security for the information stored on the card - the data can be easily read and written with a magnetic-stripe reader. Thus the only measure preventing the creation of a perfect clone is to replicate the design of the card. However, as more and more merchants deploy self-service terminals, the design of the card becomes less relevant. The thesis finds that in most cases the data needed to clone the magnetic stripe is present on the card's surface, therefore allowing to create a clone without the need to read the magnetic stripe.

Contactless card solutions, when deployed correctly, can prevent unauthorized access to the data stored in the card and hence the possibility to create a clone. However, when these cards are used for more than one system (as in the case of the bus cards), the symmetric cryptography used to implement the security features cannot be used and hence the cards become vulnerable to attacks. Perhaps a decade ago, the security of the system could rely on the unforgeability of UIDs. However, with the UID changeable cards and hardware to emulate the chips widely available on the market, the assumption of UID unforgeability does not hold. Since the hardware to read contactless cards is built in even into today's smart phones, the covert reading of a contactless card is easier than ever. The card holders hence should consider using a radio-frequency-blocking shield while storing the card.

As demonstrated by the proof-of-concept Fake ID card, the current method of using Estonian ID card for automated customer identification in loyalty programs provide no security against client impersonation attacks, unless information read from the card is compared to that in the photo ID. The customer privacy can also be at risk by merchant terminals processing more information from the personal data file than required for the purpose of customer identification. While the Estonian ID card has a potential to be used as a cryptographically uncloneable multi-purpose authentication token, the security features provided by the card has to be made available to the merchants and the merchants must deploy their terminals to make use of the features.

When use of loyalty cards provide discounts or allow to spend bonus points collected by the customer, use of cloned loyalty cards could be the most attractive to fraudsters. The possible solutions for a merchant to minimize such occurrences would be to always confirm the identity of the card holder. An optional messaging service (email, text-message etc.) could be employed to inform the customer when the card is used. However, before implementing such measures, the potential of fraud cases occurring should be weighed against the cost of implementing such changes.

The weaknesses described in this thesis, however, are unlikely to be exploited on a large scale, since the benefits provided by typical loyalty schemes are hard to monetize. Furthermore, since the loyalty cards are usually used in merchant premises, in the event of fraud the surveillance camera footage can be used to eventually trace down the possible scam artists.

References

[1] W. Rankl and W. Effing, Smart Card Handbook, 3rd ed., England: John Wiley & Sons, 2004, pp. 16-18.

[2] Q-Card, "ISO Magnetic Stripe Card Standards," Q-Card, 06 May 2015. [Online]. Available: https://www.q-card.com/about-us/iso-magnetic-stripe-card-standards/page.aspx?id=1457. [Accessed 18 April 2017].

[3] L. Padilla, "Track format of magnetic stripe cards," December 2002. [Online]. Available: http://www.gae.ucm.es/~padilla/extrawork/tracks.html. [Accessed April 2017].

[4] NXP Semiconductors N.V., "MF0ICU2 MIFARE Ultralight as Type 2 Tag," 30 June 2014. [Online]. Available: http://www.nxp.com/documents/data_sheet/MF0ICU2.pdf. [Accessed 19 April 2017].

[5] NXP B.V., "AN1303 MIFARE Ultralight as Type 2 Tag," 02 October 2012. [Online]. Available: http://www.nxp.com/documents/application_note/AN1303.pdf. [Accessed 21 April 2017].

[6] NXP Semiconductors, "MF1ICS50 Functional Specification," 14 December 2009. [Online]. Available: http://www.nxp.com/documents/data_sheet/001055.pdf. [Accessed 23 April 2017].

[7] NXP Semiconductors N.V., "MF1S50yyX/V1, MIFARE Classic EV1 1K Mainstream contactless smart card IC for fast and easy solution development," 03 March 2014. [Online]. Available: http://cache.nxp.com/documents/data_sheet/MF1S50YYX_V1.pdf. [Accessed 22 April 2017].

[8] P. Lupták, "Mifare Classic analysis in Czech Republic / Slovakia," 2009. [Online]. Available: https://nethemba.com/resources/mifare-classic-slides.pdf. [Accessed 23 April 2017].

[9] NXP Semiconductors N.V., "MF3ICDx21_41_81 MIFARE DESFire EV1 contactless multi-application IC," 09 December 2015. [Online]. Available: http://www.nxp.com/documents/short_data_sheet/MF3ICDX21_41_81_SDS.pdf. [Accessed 22 April 2017].

[10] R. Want, "An introduction to RFID technology," IEEE Pervasive Computing, vol. 5, no. 1, pp. 25-33, 2006.

[11] R. Want, "Near Field Communication," IEEE Pervasive Computing, vol. 10, no. 3, pp. 4-7, 2011.

[12] Trüb Baltic AS, "EstEID v. 3.5 Estonian Electronic ID–card application specification," AS Sertifitseerimiskeskus, 21 May 2013. [Online]. Available: http://www.id.ee/public/TB-SPEC-EstEID-Chip-App-v3_5-20140327.pdf. [Accessed 30 March 2017].

[13] Estonian Information System Authority, "Electronic Identity (eID) Application Guide: Using the ID card as a loyalty card and in access control systems," 31 October 2012. [Online]. Available: https://eid.eesti.ee/index.php/ID_card_loyalty_access_analysis. [Accessed 22 April 2017].

[14] M. Paljak, “FakeEstEID JavaCard applet,” 16 January 2015. [Online]. Available: https://github.com/martinpaljak/esteid-applets/blob/master/docs/FakeEstEID.md. [Accessed 21 March 2017].

[15] F. D. Garcia, G. de Koning Gans, R. Muijrers, P. van Rossum, R. Verdult, R. W. Schreur and B. Jacobs, “Dismantling MIFARE Classic,” in 13th European Symposium on Research in Computer Security, Málaga, 2008.

[16] M. Paljak, “Tallinna Ühiskaardi,” 31 May 2015. [Online]. Available: https://github.com/martinpaljak/yhiskaart. [Accessed 23 November 2016].

[17] A. Costin, “MiFare Classic Universal toolKit (MFCUK),” 10 January 2014. [Online]. Available: https://github.com/nfc-tools/mfcuk. [Accessed 13 April 2017].

[18] N. Szetei and P. Luptak, “Mifare Classic Offline Cracker (MFOC),” 17 February 2017. [Online]. Available: https://github.com/nfc-tools/mfoc. [Accessed 13 April 2017].

[19] R. Conty and R. Tartière, “Libfreefare,” April 2017. [Online]. Available: https://github.com/nfc-tools/libfreefare. [Accessed 11 April 2017].

[20] R. Verdult et al., “Libnfc,” 20 April 2017. [Online]. Available: https://github.com/nfc-tools/libnfc. [Accessed 11 April 2017].

[21] Estonian Information System Authority, "Cryptographic algorithms lifecycle report 2016," 22 June 2016. [Online]. Available: https://www.ria.ee/public/RIA/Cryptographic_Algorithms_Lifecycle_Report_2016.pdf. [Accessed 14 November 2016].

[22] C. E. Ortiz, “An Introduction to Java Card Technology - Part 1,” Oracle, 29 May 2003. [Online]. Available: http://www.oracle.com/technetwork/java/javacard/javacard1-139251.html. [Accessed 23 April 2017].

[23] G. Klostermeier, “Mifare Classic Tool,” April 2017. [Online]. Available: https://github.com/ikarus23/MifareClassicTool. [Accessed April 2017].

[24] T. Kasper, S. Küppers and D. Oswald, “ChameleonMini,” 05 April 2017. [Online]. Available: https://github.com/emsec/ChameleonMini. [Accessed 04 April 2017].

[25] J. Prado Casanovas and G. Van Damme, “DESfire Emulation Using Java Card,” 2011. [Online]. Available: https://www.esat.kuleuven.be/cosic/publications/article-2206.pdf. [Accessed 12 May 2017].

[26] J. Prado Casanovas, “Java card DESfire emulation,” 28 August 2011. [Online]. Available: https://github.com/Dansf/java-card-desfire-emulation. [Accessed May 2017].

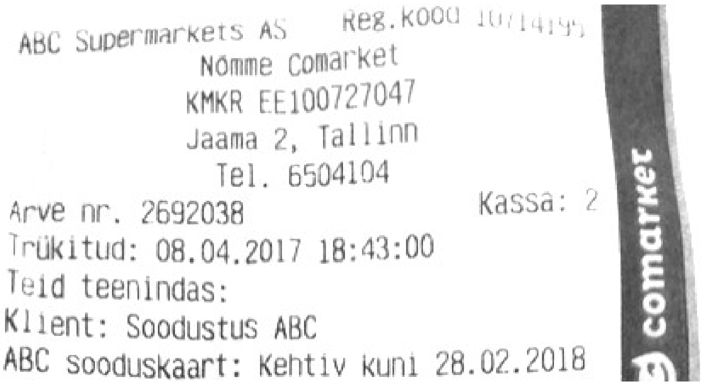
[27] T. Kasper, S. Küppers and D. Oswald, “Chameleon-Mini Documentation,” Kasper & Oswald, 05 April 2017. [Online]. Available: https://rawgit.com/emsec/ChameleonMini/master/Doc/Doxygen/html/index.html. [Accessed 06 April 2017].

Appendix 1 – Communication between TTU gym reader and ISIC card

```
10917 ms <+10917 ms>:CODEC RX      (1   bytes) [52]
10918 ms <    +1 ms>:CODEC RX      (2   bytes) [fd0f]
10918 ms <    +0 ms>:CODEC RX      (2   bytes) [9320]
10919 ms <    +1 ms>:CODEC RX      (4   bytes) [9b1f1072]
10920 ms <    +1 ms>:CODEC RX      (9   bytes) [9370880477d22990a7]
10920 ms <    +0 ms>:CODEC RX      (3   bytes) [fd0001]
10920 ms <    +0 ms>:CODEC RX      (2   bytes) [9520]
10921 ms <    +1 ms>:CODEC RX      (4   bytes) [800f7e3d]
10922 ms <    +1 ms>:CODEC RX      (9   bytes) [9570ba153c801350b3]
10922 ms <    +0 ms>:CODEC RX      (3   bytes) [ff0000]
11003 ms <   +81 ms>:CODEC RX      (1   bytes) [52]
11004 ms <    +1 ms>:CODEC RX      (4   bytes) [500057cd]
11006 ms <    +2 ms>:CODEC RX      (1   bytes) [52]
11006 ms <    +0 ms>:CODEC RX      (2   bytes) [cd1f]
11007 ms <    +1 ms>:CODEC RX      (2   bytes) [9320]
11007 ms <    +0 ms>:CODEC RX      (4   bytes) [bf3f107e]
11008 ms <    +1 ms>:CODEC RX      (9   bytes) [9370880477d22990a7]
11009 ms <    +1 ms>:CODEC RX      (3   bytes) [fd8101]
11009 ms <    +0 ms>:CODEC RX      (2   bytes) [9520]
11010 ms <    +1 ms>:CODEC RX      (4   bytes) [e01f7e7e]
11011 ms <    +1 ms>:CODEC RX      (9   bytes) [9570ba153c801350b3]
11011 ms <    +0 ms>:CODEC RX      (3   bytes) [fb0000]
11088 ms <   +77 ms>:CODEC RX      (1   bytes) [52]
11090 ms <    +2 ms>:CODEC RX      (4   bytes) [500057cd]
11091 ms <    +1 ms>:CODEC RX      (1   bytes) [52]
11092 ms <    +1 ms>:CODEC RX      (2   bytes) [df1f]
11092 ms <    +0 ms>:CODEC RX      (2   bytes) [9320]
11093 ms <    +1 ms>:CODEC RX      (4   bytes) [9f1f7072]
11094 ms <    +1 ms>:CODEC RX      (9   bytes) [9370880477d22990a7]
11094 ms <    +0 ms>:CODEC RX      (3   bytes) [fd0001]
11094 ms <    +0 ms>:CODEC RX      (2   bytes) [9520]
11095 ms <    +1 ms>:CODEC RX      (4   bytes) [80877f3f]
11096 ms <    +1 ms>:CODEC RX      (9   bytes) [9570ba153c801350b3]
11096 ms <    +0 ms>:CODEC RX      (3   bytes) [fb0200]
11131 ms <   +35 ms>:CODEC RX      (1   bytes) [52]
11132 ms <    +1 ms>:CODEC RX      (4   bytes) [500057cd]
11134 ms <    +2 ms>:CODEC RX      (1   bytes) [52]
11134 ms <    +0 ms>:CODEC RX      (2   bytes) [cd0f]
11135 ms <    +1 ms>:CODEC RX      (2   bytes) [9320]
11135 ms <    +0 ms>:CODEC RX      (4   bytes) [9b1f1072]
```

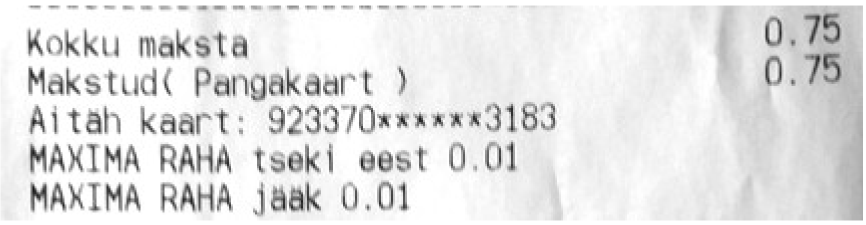
```
11136 ms <    +1 ms>:CODEC RX        (9   bytes) [9370880477d22990a7]
11137 ms <    +1 ms>:CODEC RX        (3   bytes) [fd0001]
11137 ms <    +0 ms>:CODEC RX        (2   bytes) [9520]
11138 ms <    +1 ms>:CODEC RX        (4   bytes) [001f7e7a]
11139 ms <    +1 ms>:CODEC RX        (9   bytes) [9570ba153c801350b3]
11139 ms <    +0 ms>:CODEC RX        (3   bytes) [fb0000]
11216 ms <   +77 ms>:CODEC RX         (1   bytes) [52]
11218 ms <    +2 ms>:CODEC RX        (4   bytes) [500057cd]
11219 ms <    +1 ms>:CODEC RX        (1   bytes) [52]
11220 ms <    +1 ms>:CODEC RX        (2   bytes) [cd0f]
11220 ms <    +0 ms>:CODEC RX        (2   bytes) [9320]
11221 ms <    +1 ms>:CODEC RX        (4   bytes) [9b1f1072]
11222 ms <    +1 ms>:CODEC RX        (9   bytes) [9370880477d22990a7]
11222 ms <    +0 ms>:CODEC RX        (3   bytes) [fd0001]
11222 ms <    +0 ms>:CODEC RX        (2   bytes) [9520]
11223 ms <    +1 ms>:CODEC RX        (4   bytes) [000f7e7a]
11224 ms <    +1 ms>:CODEC RX        (9   bytes) [9570ba153c801350b3]
11224 ms <    +0 ms>:CODEC RX        (3   bytes) [fb0000]
11302 ms <   +78 ms>:CODEC RX         (1   bytes) [52]
11303 ms <    +1 ms>:CODEC RX        (4   bytes) [500057cd]
11305 ms <    +2 ms>:CODEC RX        (1   bytes) [52]
11305 ms <    +0 ms>:CODEC RX        (2   bytes) [cd0f]
11305 ms <    +0 ms>:CODEC RX        (2   bytes) [9320]
11306 ms <    +1 ms>:CODEC RX        (4   bytes) [9b1f1072]
11307 ms <    +1 ms>:CODEC RX        (9   bytes) [9370880477d22990a7]
11307 ms <    +0 ms>:CODEC RX        (3   bytes) [fd0001]
11308 ms <    +1 ms>:CODEC RX        (2   bytes) [9520]
11308 ms <    +0 ms>:CODEC RX        (4   bytes) [000f7e7a]
11309 ms <    +1 ms>:CODEC RX        (9   bytes) [9570ba153c801350b3]
11310 ms <    +1 ms>:CODEC RX        (3   bytes) [fb0000]
```

Appendix 2 – Receipts of purchases using loyalty cards



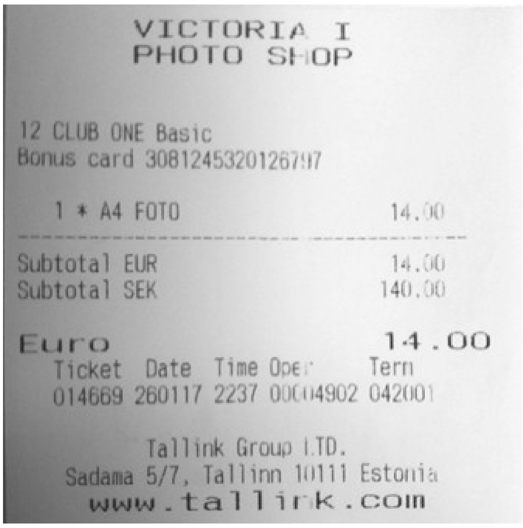
```
ABC Supermarkets AS    Reg.kood 10714195
            Nõmme Comarket
           KMKR EE100727047
           Jaama 2, Tallinn
             Tel. 6504104
Arve nr. 2692038                Kassa: 2
Trükitud: 08.04.2017 18:43:00
Teid teenindas:
Klient: Soodustus ABC
ABC sooduskaart: Kehtiv kuni 28.02.2018
```

Figure 42. Section of the customer receipt after use of the ABC loyalty card at Comarket Supermarket



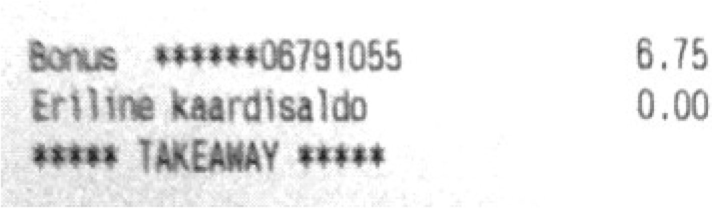
```
---------------------------
Kokku maksta                        0.75
Makstud( Pangakaart )               0.75
Aitäh kaart: 923370******3183
MAXIMA RAHA tseki eest 0.01
MAXIMA RAHA jääk 0.01
```

Figure 43. Section of the customer receipt after use of the Äitah Loyalty card at a self-service terminal at Maxima supermarket



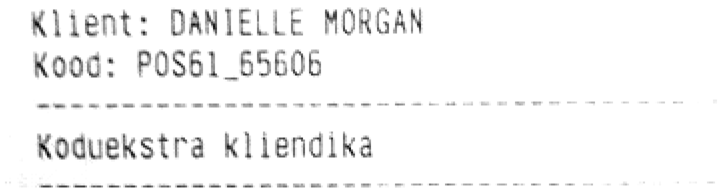
```
          VICTORIA I
          PHOTO SHOP

12 CLUB ONE Basic
Bonus card 3081245320126797

  1 * A4 FOTO                  14.00
------------------------------------
Subtotal EUR                   14.00
Subtotal SEK                  140.00

Euro                          14.00
  Ticket  Date   Time Oper     Term
  014669 260117 2237 00004902 042001

        Tallink Group LTD.
  Sadama 5/7, Tallinn 10111 Estonia
         www.tallink.com
```

Figure 44. Customer Receipt after use of the Club One card on board a Tallink Cruise



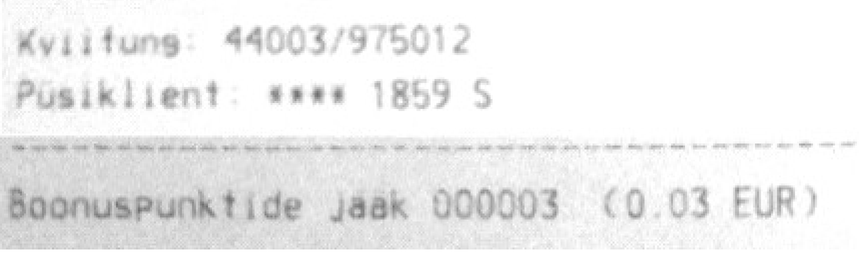
```
Bonus  ******06791055            6.75
Eriline kaardisaldo              0.00
***** TAKEAWAY *****
```

Figure 45. Section of the customer receipt after use of the Hesburger Loyalty card



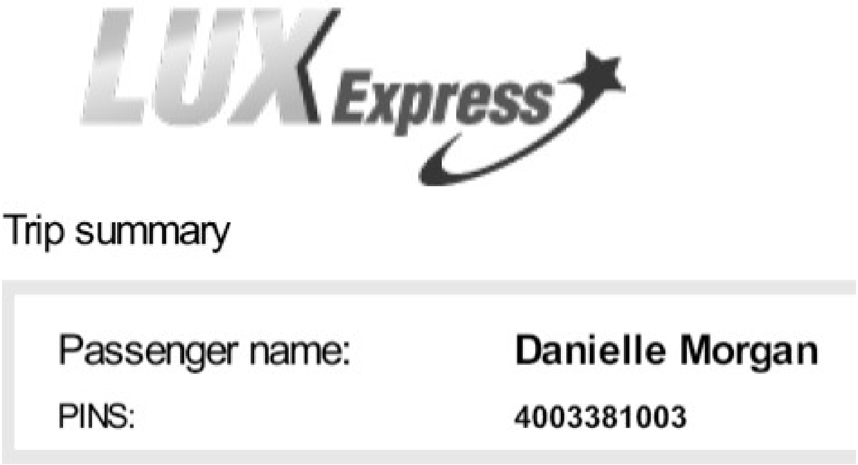
```
Klient: DANIELLE MORGAN
Kood: POS61_65606
-------------------------------------
Koduekstra kliendika
-------------------------------------
```

Figure 46. Section of customer receipt after use of the Koduekstra loyalty card



```
Kviitung: 44003/975012
Püsiklient: **** 1859 S
-------------------------------------------
Boonuspunktide jääk 000003  (0.03 EUR)
```

Figure 47. Select sections of the customer receipt after use of the Partner Loyalty card at Selver supermarket



Trip summary

Passenger name:	**Danielle Morgan**
PINS:	**4003381003**

Figure 48. Section of the Online Ticket received after using the PINS Loyalty card to purchase tickets at LuxExpress

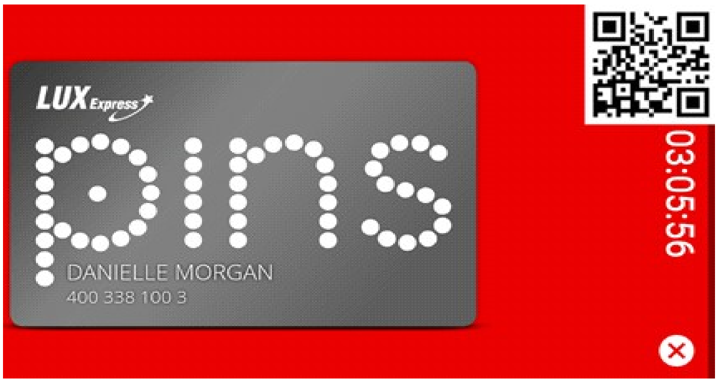


Figure 49. PINS virtual as displayed by the LuxExpress Android mobile application

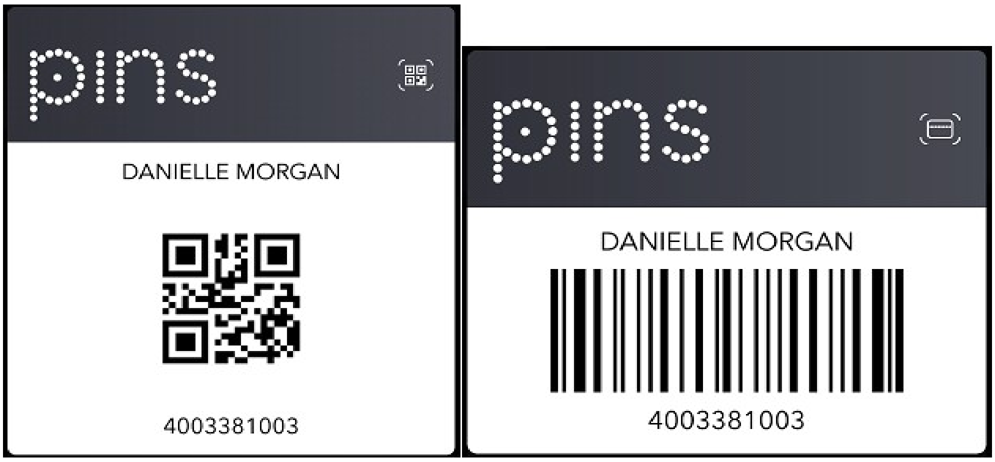
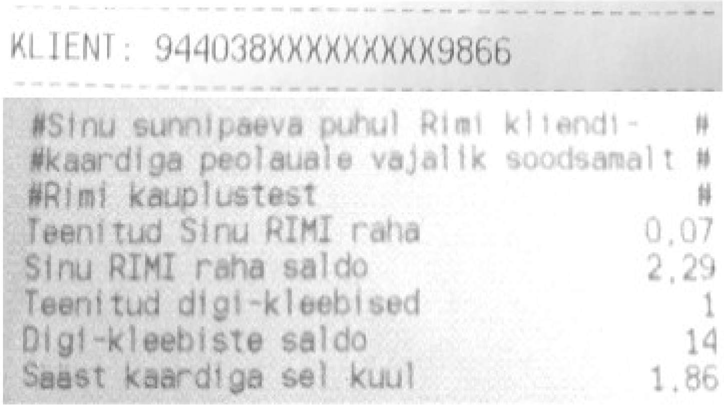
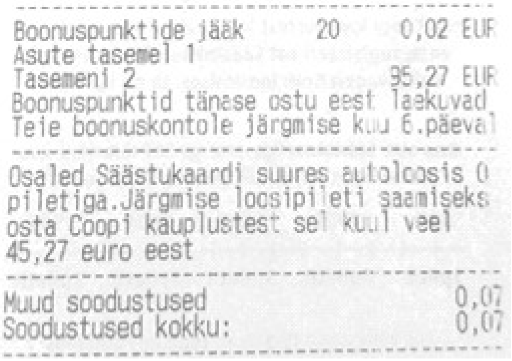


Figure 50. PINS virtual card as displayed by the PINS Android mobile Application



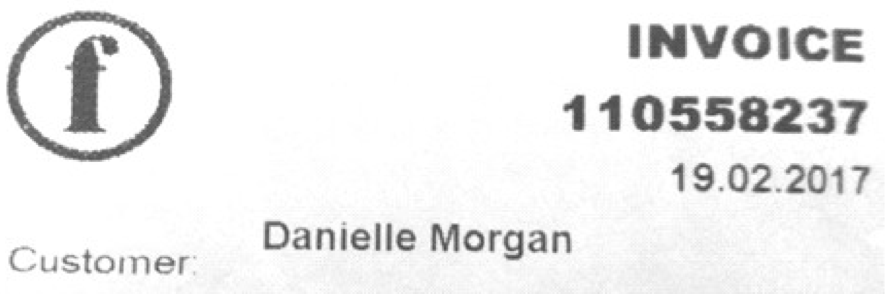
```
KLIENT: 944038XXXXXXXXX9866

#Sinu sunnipaeva puhul Rimi kliendi-   #
#kaardiga peolauale vajalik soodsamalt #
#Rimi kauplustest                      #
Teenitud Sinu RIMI raha             0,07
Sinu RIMI raha saldo                2,29
Teenitud digi-kleebised                1
Digi-kleebiste saldo                  14
Saast kaardiga sel kuul             1,86
```

Figure 51. Sections of the receipt after use of the Rimi Loyalty Card



```
Boonuspunktide jääk      20       0,02 EUR
Asute tasemel 1
Tasemeni 2                       95,27 EUR
Boonuspunktid tänase ostu eest laekuvad
Teie boonuskontole järgmise kuu 6.päeval

Osaled Säästukaardi suures autoloosis 0
piletiga.Järgmise loosipileti saamiseks
osta Coopi kauplustest sel kuul veel
45,27 euro eest

Muud soodustused                      0,07
Soodustused kokku:                    0,07
```

Figure 52. Section of the customer receipt after use of the Säästukaart at Konsum supermarket



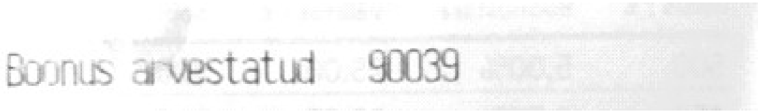
INVOICE

110558237

19.02.2017

Customer: Danielle Morgan

Figure 53. Section of the customer receipt when the Estonian ID card is used to verify loyalty status at Forum Cinemas



Boonus arvestatud 90039

Figure 54. Section of the customer receipt when the Estonian ID card is used to verify loyalty status at Prisma Supermarkets

Appendix 3 – Memory dumps of NFC cards

Table 23. Memory dump of the Tallinn Bus Card

Block		Data Bits	ASCII
Sector 0			
0	***00h***	B0 B8 59 31 60 08 04 00 62 63 64 65 66 67 68 69	..Y1`...bcdefghi
1	***01h***	B0 00 03 E1 03 E1 03 E1 03 E1 03 E1 03 E1 00 00	....
2	***02h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
3	***03h***	00 00 00 00 00 00 0F 07 8F C1 00 00 00 00 00 00	....
Sector 1			
4	***04h***	03 FF 01 01 94 11 38 70 69 6C 65 74 2E 65 65 3A	......8pilet.ee:
5	***05h***	65 6B 61 61 72 74 3A 32 66 19 5F 26 06 31 34 31	ekaart:2f._&.141
6	***06h***	30 32 30 59 04 20 20 20 20 5F 28 03 32 33 33 5F	020Y....._(.233_
7	***07h***	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......
Sector 2			
8	***08h***	27 01 31 6E 1B 5A 13 33 30 38 36 34 39 30 30 39	’.1n.Z.308649009
9	***09h***	30 30 30 37 35 39 39 35 33 37 53 04 B0 B8 59 31	0007599537S...Y1
10	***0Ah***	41 03 00 00 00 AC 53 69 67 01 02 00 80 5A 2F 44	A.....Sig....Z/D
11	***0Bh***	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......
Sector 3			
12	***0Ch***	9C A2 68 97 36 F4 94 48 60 4E EE 0A 6D 82 F0 9D	..h.6..H`N..m...
13	***0Dh***	BB BB F9 96 BD 58 D7 9F 62 52 45 F9 36 24 65 B2	.....X..bRE.6$e.
14	***0Eh***	82 64 9C E4 8E A6 D4 05 19 88 A3 34 96 84 12 F2	.d.........4....
15	***0Fh***	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......
Sector 4			
16	***10h***	AE D1 90 0D D3 69 31 16 0F E6 9E 7B FF A4 70 46	.....i1....{..pF
17	***11h***	10 F4 ED 4F 27 55 E1 BE 9B 16 A9 16 B2 40 F9 25	...O’U.......@.%
18	***12h***	91 18 56 C8 76 B9 4C CF 43 91 08 21 A2 3C AA 16	..V.v.L.C..!.<..
19	***13h***	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......
Sector 5			
20	***14h***	48 C2 50 73 8B E7 77 A3 1F F1 C5 9B 8E 00 26 91	H.Ps..w.......&.

Block		Data Bits	ASCII
21	***15h***	57 FC 79 1B 94 02 19 B3 28 6D C3 67 BC 80 00 25	W.y.....(m.g...%
22	***16h***	68 74 74 70 3A 2F 2F 70 69 6C 65 74 2E 65 65 2F	http://pilet.ee/
23	***17h***	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......
Sector 6			
24	***18h***	63 72 74 2F 33 30 38 36 34 39 30 30 2D 30 30 30	crt/30864900-000
25	***19h***	31 2E 63 72 74 FE 00 00 00 00 00 00 00 00 00 00	1.crt...........
26	***1Ah***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
27	***1Bh***	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......
Sector 7			
28	***1Ch***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
29	***1Dh***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
30	***1Eh***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
31	***1Fh***	00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF	.........i......
Sector 8			
32	***20h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
33	***21h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
34	***22h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
35	***23h***	00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF	.........i......
Sector 9			
36	***24h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
37	***25h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
38	***26h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
39	***27h***	00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF	.........i......
Sector 10			
40	***28h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
41	***29h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
42	***2Ah***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
43	***2Bh***	00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF	.........i......
Sector 11			
44	***2Ch***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
45	***2Dh***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
46	***2Eh***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
47	***2Fh***	00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF	.........i......
Sector 12			

Block		**Data Bits**	**ASCII**
48	***30h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
49	***31h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
50	***32h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
51	***33h***	00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF	.........i......
Sector 13			
52	***34h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
53	***35h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
54	***36h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
55	***37h***	00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF	.........i......
Sector 14			
56	***38h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
57	***39h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
58	***3Ah***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
59	***3Bh***	00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF	.........i......
Sector 15			
60	***3Ch***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
61	***3Dh***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
62	***3Eh***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
63	***3Fh***	00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF	.........i......

Table 24. Memory dump of the ISIC card

Block		**Data Bits**	**ASCII**
Sector 0			
0	***00h***	04 77 D2 BA 15 3C 80 88 44 00 C8 20 00 00 00 00	.w...<..D.......
1	***01h***	B0 00 03 E1 03 E1 03 E1 03 E1 03 E1 03 E1 00 00	....
2	***02h***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
3	***03h***	00 00 00 00 00 00 0F 07 8F C1 00 00 00 00 00 00	....
Sector 1			
4	***04h***	03 FF 01 04 94 11 3B 70 69 6C 65 74 2E 65 65 3A	......;pilet.ee:
5	***05h***	65 6B 61 61 72 74 3A 32 66 19 5F 26 06 31 37 30	ekaart:2f._&.170
6	***06h***	32 30 39 59 04 31 37 31 32 5F 28 03 32 33 33 5F	209Y.1712_(.233_
7	***07h***	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......
Sector 2			

Block		Data Bits	ASCII
8	*08h*	27 01 31 6E 1E 5A 13 39 32 33 33 37 33 31 36 38	’.1n.Z.923373168
9	*09h*	30 31 32 30 33 31 35 38 37 37 53 07 04 77 D2 BA	0120315877S..w..
10	*0Ah*	15 3C 80 41 03 00 00 00 AC 53 69 67 01 02 00 80	.<.A.....Sig....
11	*0Bh*	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......
Sector 3			
12	*0Ch*	40 C0 52 FC BC 9C F4 2D 82 D1 E9 81 B5 39 EA A8	@.R....-.....9..
13	*0Dh*	6F F0 29 83 9F BC 2E A6 30 33 A5 6B 5D 88 65 42	o.).....03.k].eB
14	*0Eh*	BB 8F F5 CF 07 AE 52 8E FD 0C 37 CA B0 92 6C D8	......R...7...l.
15	*0Fh*	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......
Sector 4			
16	*10h*	B8 22 76 9D 64 30 2E 3A F8 71 32 59 90 EF B0 3B	."v.d0.:.q2Y...;
17	*11h*	36 B8 A7 2C 70 A7 19 94 EF 5C 84 6F 1F FB 32 1D	6..,p....\.o..2.
18	*12h*	B6 02 26 E0 8D FF 04 C6 A1 6F E7 F3 9B 0E ED 86	..&......o......
19	*13h*	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......
Sector 5			
20	*14h*	F2 B8 A7 ED 5C 6E 2D 4C A9 01 E0 77 1E 86 BA 5D	....\n-L...w...]
21	*15h*	FD C0 95 61 5E 62 0B 23 82 97 0F 9B 02 70 C6 6A	...a^b.#.....p.j
22	*16h*	80 00 25 68 74 74 70 3A 2F 2F 70 69 6C 65 74 2E	..%http://pilet.
23	*17h*	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......
Sector 6			
24	*18h*	65 65 2F 63 72 74 2F 39 32 33 33 37 33 31 36 2D	ee/crt/92337316-
25	*19h*	30 30 30 31 2E 63 72 74 FE 00 00 00 00 00 00 00	0001.crt........
26	*1Ah*	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
27	*1Bh*	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......

Table 25. Memory dump of SEB ISIC card

Block		Data Bits	ASCII
Sector 0			
0	*00h*	4B F2 AC F8 ED 88 04 00 C0 8E 3E 95 49 20 32 14	K.........>.I.2.
1	*01h*	B0 00 03 E1 03 E1 03 E1 03 E1 03 E1 03 E1 00 00	....
2	*02h*	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
3	*03h*	00 00 00 00 00 00 0F 07 8F C1 00 00 00 00 00 00	....
Sector 1			

Block		**Data Bits**	**ASCII**
4	***04h***	03 FF 01 01 94 11 38 70 69 6C 65 74 2E 65 65 3A	......8pilet.ee:
5	***05h***	65 6B 61 61 72 74 3A 32 66 19 5F 26 06 31 35 30	ekaart:2f._&.150
6	***06h***	39 30 38 59 04 31 36 31 32 5F 28 03 32 33 33 5F	908Y.1612_(.233_
7	***07h***	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......
Sector 2			
8	***08h***	27 01 31 6E 1B 5A 13 39 32 33 33 37 33 33 31 38	’.1n.Z.923373318
9	***09h***	30 31 34 30 35 30 30 35 30 37 53 04 4B F2 AC F8	0140500507S.K...
10	***0Ah***	41 03 00 00 00 AC 53 69 67 01 02 00 80 59 AF 3D	A.....Sig....Y.=
11	***0Bh***	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......
Sector 3			
12	***0Ch***	D2 15 AF 11 D2 FD 6F 6D F2 5E 25 5E 94 C0 24 CB	......om.^%^..$.
13	***0Dh***	8F 18 ED 94 2A 59 29 C7 36 71 49 2C B3 95 D8 9C	....*Y).6qI,....
14	***0Eh***	9D A6 62 6A 6E D2 89 CB 7E 04 13 5B F2 15 1C B7	..bjn...~..[....
15	***0Fh***	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......
Sector 4			
16	***10h***	81 34 B4 DE 39 DF 07 93 81 0D 98 C2 56 D1 C3 9E	.4..9.......V...
17	***11h***	B3 EB 3A 75 19 FD 76 E0 15 95 89 68 92 AE 7E A7	..:u..v....h..~.
18	***12h***	52 6E FD 2A 84 C1 D2 56 AD 20 17 15 73 0C 5F 64	Rn.*...V....s._d
19	***13h***	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......
Sector 5			
20	***14h***	3C 89 6B 7E 16 B8 6E E0 37 08 DE BD FA 96 D1 97	<.k~..n.7.......
21	***15h***	4E D7 11 11 A4 B7 EF FA 3A 41 93 99 8D 80 00 25	N.......:A.....%
22	***16h***	68 74 74 70 3A 2F 2F 70 69 6C 65 74 2E 65 65 2F	http://pilet.ee/
23	***17h***	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......
Sector 6			
24	***18h***	63 72 74 2F 39 32 33 33 37 33 33 31 2D 30 30 30	crt/92337331-000
25	***19h***	32 2E 63 72 74 FE 00 00 00 00 00 00 00 00 00 00	2.crt...........
26	***1Ah***	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
27	***1Bh***	00 00 00 00 00 00 0F 07 8F 41 00 00 00 00 00 00	.........A......

Table 26. Memory dump of the Tartu Bus Card

Page		Bytes B0 B1 B2 B3	ASCII	Page		Bytes B0 B1 B2 B3	ASCII
0	*00h*	04 7F 0D FE	....	*1*	*01h*	DA 8D 3A 84	..:.
2	*02h*	E9 48 00 00	.H..	*3*	*03h*	E1 10 12 00	....
4	*04h*	03 8A 94 11	....	*5*	*05h*	35 70 69 6C	5pil
6	*06h*	65 74 2E 65	et.e	*7*	*07h*	65 3A 65 6B	e:ek
8	*08h*	61 61 72 74	aart	*9*	*09h*	3A 33 66 0F	:3f.
10	*0Ah*	5F 26 06 31	_&.1	*11*	*0Bh*	35 31 30 30	5100
12	*0Ch*	31 59 04 20	1Y..	*13*	*0Dh*	20 20 20 6E	...n
14	*0Eh*	22 5A 13 33	"Z.3	*15*	*0Fh*	30 38 36 34	0864
16	*10h*	39 30 30 39	9009	*17*	*11h*	39 35 30 30	9500
18	*12h*	36 36 35 33	6653	*19*	*13h*	33 31 53 07	31S.
20	*14h*	04 7F 0D DA	....	*21*	*15h*	8D 3A 84 54	.:.T
22	*16h*	02 00 01 51	...Q	*23*	*17h*	03 3B 53 69	.;Si
24	*18h*	67 01 04 00	g...	*25*	*19h*	36 30 34 02	604.
26	*1Ah*	18 19 B7 94	....	*27*	*1Bh*	CA 78 86 9D	.x..
28	*1Ch*	52 14 1E 37	R..7	*29*	*1Dh*	27 BC 13 7B	’..{
30	*1Eh*	0D 1B D6 28	...(	*31*	*1Fh*	0E A3 C9 EC	....
32	*20h*	B4 02 18 55	...U	*33*	*21h*	77 9B BE C1	w...
34	*22h*	4F 06 9C 59	O..Y	*35*	*23h*	1A 45 95 FC	.E..
36	*24h*	A0 D8 8C 2A	...*	*37*	*25h*	34 BD 43 FC	4.C.
38	*26h*	CB F5 F1 00	....	*39*	*27h*	00 00 00 00	....
40	*28h*	00 00 00 00	....	*41*	*29h*	00 00 00 00	....
42	*2Ah*	30 00 00 00	0...	*43*	*2Bh*	00 00 00 00	....
44	*2Ch*	42 52 45 41	BREA	*45*	*2Dh*	4B 4D 45 49	KMEI
46	*2Eh*	46 59 4F 55	FYOU	*47*	*2Fh*	43 41 4E 21	CAN!

Table 27. Memory dump of Rimi Card

Page		Bytes B0 B1 B2 B3	ASCII	Page		Bytes B0 B1 B2 B3	ASCII
0	*00h*	04 DC AB FB	....	*1*	*01h*	C2 4A 4E 80	.JN.
2	*02h*	46 48 00 00	FH..	*3*	*03h*	00 00 00 00	....
4	*04h*	52 49 4D 49	RIMI	*5*	*05h*	30 30 30 32	0002
6	*06h*	31 39 30 35	1905	*7*	*07h*	32 30 31 36	2016

Page		**Bytes B0 B1 B2 B3**	**ASCII**	**Page**		**Bytes B0 B1 B2 B3**	**ASCII**
8	*08h*	00 00 00 00	....	*9*	*09h*	00 00 00 00	....
10	*0Ah*	00 00 00 00	....	*11*	*0Bh*	00 00 00 00	....
12	*0Ch*	00 00 00 00	....	*13*	*0Dh*	00 00 00 00	....
14	*0Eh*	00 00 00 00	....	*15*	*0Fh*	00 00 00 00	....
16	*10h*	00 00 00 00	....	*17*	*11h*	00 00 00 00	....
18	*12h*	00 00 00 00	....	*19*	*13h*	00 00 00 00	....
20	*14h*	00 00 00 00	....	*21*	*15h*	00 00 00 00	....
22	*16h*	04 DC AB FB	....	*23*	*17h*	C2 4A 4E 80	.JN.
24	*18h*	Unable to read	....	*25*	*19h*	Unable to read	....
26	*1Ah*	Unable to read	....	*27*	*1Bh*	Unable to read	....
28	*1Ch*	Unable to read	....	*29*	*1Dh*	Unable to read	....
30	*1Eh*	Unable to read	....	*31*	*1Fh*	Unable to read	....
32	*20h*	Unable to read	....	*33*	*21h*	Unable to read	....
34	*22h*	Unable to read	....	*35*	*23h*	Unable to read	....
36	*24h*	Unable to read	....	*37*	*25h*	Unable to read	....
38	*26h*	Unable to read	....	*39*	*27h*	Unable to read	....
40	*28h*	Unable to read	....	*41*	*29h*	Unable to read	....
42	*2Ah*	Unable to read	....	*43*	*2Bh*	Unable to read	....
44	*2Ch*	Key 1 page 0	....	*45*	*2Dh*	Key 1 page 1	....
46	*2Eh*	Key 2 page 0	....	*47*	*2Fh*	Key 2 page 1	....