Using the Estonian Electronic Identity Card for Authentication to a Machine

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

[1]Tallinn University of Technology, Tallinn, Estonia

[2]Software Technology and Applications Competence Center, Tartu, Estonia

[3]University of Tartu, Tartu, Estonia

November 9, 2017

Estonian ID card

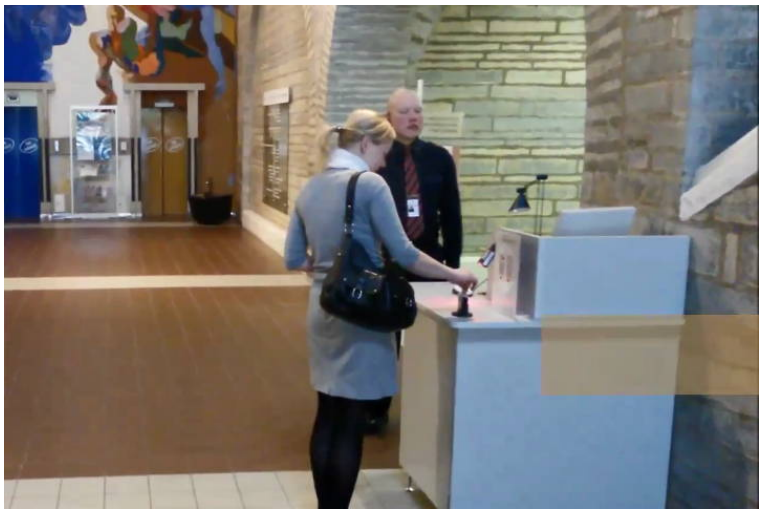
There are several types of electronic ID cards:

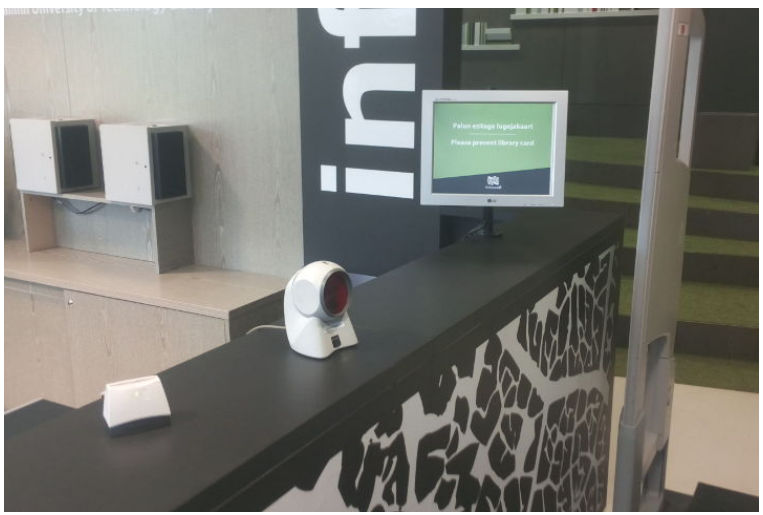
EstEID specification in English:

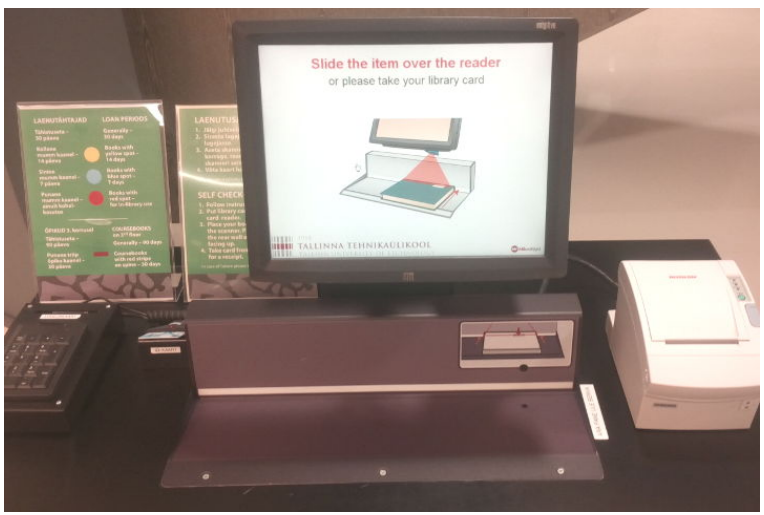
`http://www.id.ee/public/TB-SPEC-EstEID-Chip-App-v3.4.pdf`

Authentication to a Machine

Authentication to a Machine (cont.)







Research Questions

1. How is the chip authenticated?
2. Can we impersonate the chip by building an ID card emulator?
3. How could the security of card authentication be improved?

The analysis of fraud feasibility is not in the scope of this study.

Card Authentication

Personal data file:

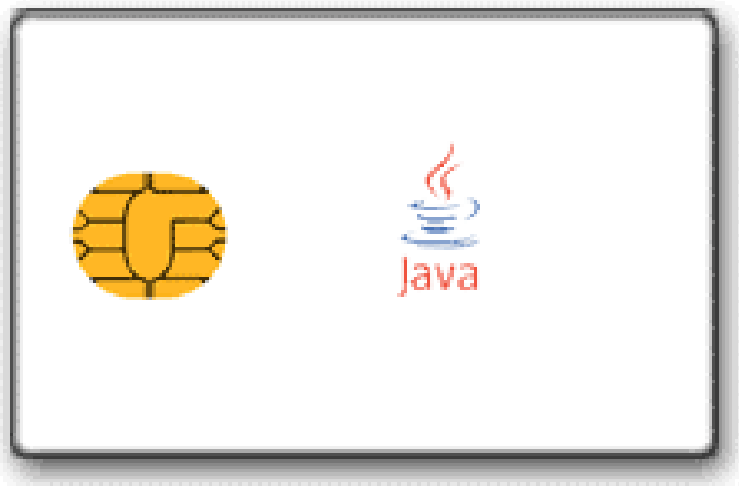
No.	Content	Example	Length (bytes)
1	Surname	ŽAIKOVSKI	Max 28
2	First name line 1	IGOR	Max 15
3	First name line 2		Max 15
4	Sex	M	1
5	Nationality code	POL	3
6	Date of birth	01.01.1971	10
7	Personal ID code	37101010021	11
8	Document number	X0010536	8 or 9
9	Expiry date	13.08.2019	10
10	Place of birth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

APDU commands for reading the 5th record:

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

ID card emulator/logger

Emulates the Estonian ID card as much as possible[1]



- Implemented using a programmable JavaCard
- Based on Martin Paljak's FakeEstEID.java applet
- Logs command APDUs received from the terminal
- Passes chip authentication in all the terminals tested

[1] Private key operations cannot be emulated.

Card ATR Adjustment

"Answer To Reset (ATR): bytes returned by a contact smart card on power up. Conveys information about the parameters proposed by the card."

```
$ pcsc_scan
ATR: 3B FA 18 00 00 80 31 FE 45 FE 65 49 44 20 2F 20 50 4B 49 03
```

- Historical bytes can be set using `GPSystem.setATRHistBytes()`
- The ATR prefix cannot be changed
- A JavaCard with the same ATR prefix was found:
  - G&D SmartCafe Expert 6.0 80K (15 GBP from `https://www.smartcardfocus.com/`)

Visual Imitation

Chip Transplantation

Card Authentication in Practice

- The emulator was tested in the most popular public deployments.
- Each terminal was tested using four different fake ID cards:
  1. A perfect ID card emulator to obtain the APDU trace
  2. A card with a random ATR to check if ATR is validated
  3. An expired card with an invalid document number
  4. A card to check if the terminal supports the T=0/T=1 protocol
- In total 15 terminals were tested from May to July 2017.

Sample APDU Trace (Prisma)

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

Payment Terminals

- Ingenico iPP320

- Apollo
- Apotheka
- Grossi Toidukaubad
- Olerex

- VeriFone Vx805/Vx820

- Lido
- Rahva Raamat

- Worldline YOMANI

- K-Rauta
- Prisma

Results

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

- Most of the terminals read more data than required.
- None of the terminals do expiration and revocation checks.
- Not all terminals validate a card's ATR.
- Both protocols supported, T=0 preferred.

Possible Improvements

- A card authentication key
  - Accessible without a PIN
  - The terminal requires signing a random challenge
  - Certificate includes signed cardholder data
  - Can be installed remotely as an additional applet
  - Performance (ECDSA P-256): 1.5s (2011), 0.6s (2014)
- Signed facial image
  - Simplify cardholder verification
  - Feature already provided by ICAO ePassports
- Contactless interface
  - Convenient for using an ID card as an entrance card
  - Privacy concerns
  - Next-generation ID cards (starting from 2019)

Conclusions

1. The current mechanism is not suited for high-risk transactions
2. An ID card emulator is not expensive to build nowadays
3. The chip cannot be trusted even if ID card is visually authentic
4. Terminals process more personal data than needed
5. Expiration and revocation checks are not performed

Thank you!