EMV (Chip & PIN) Protocol

Märt Bakhoff
Supervised: Arnis Paršovs

Objective

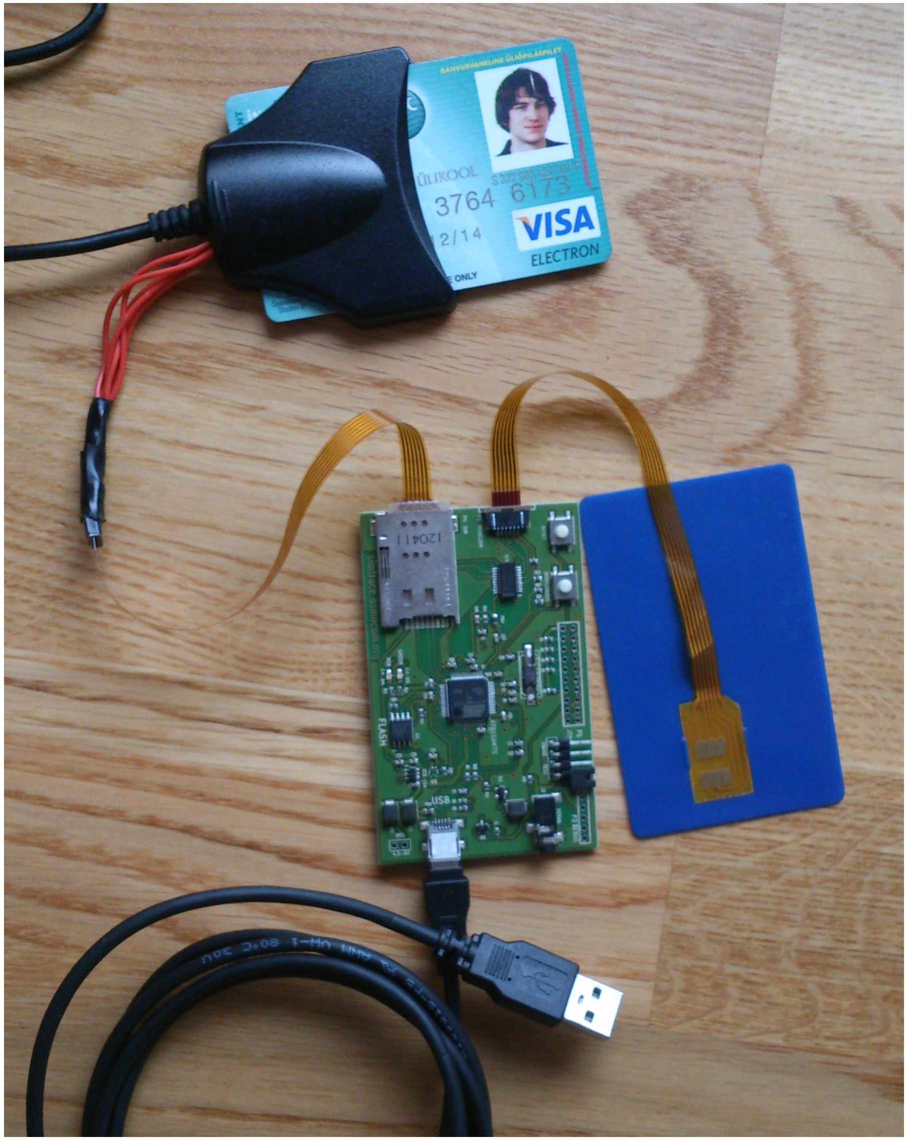
observe and describe a real world transaction

Agenda

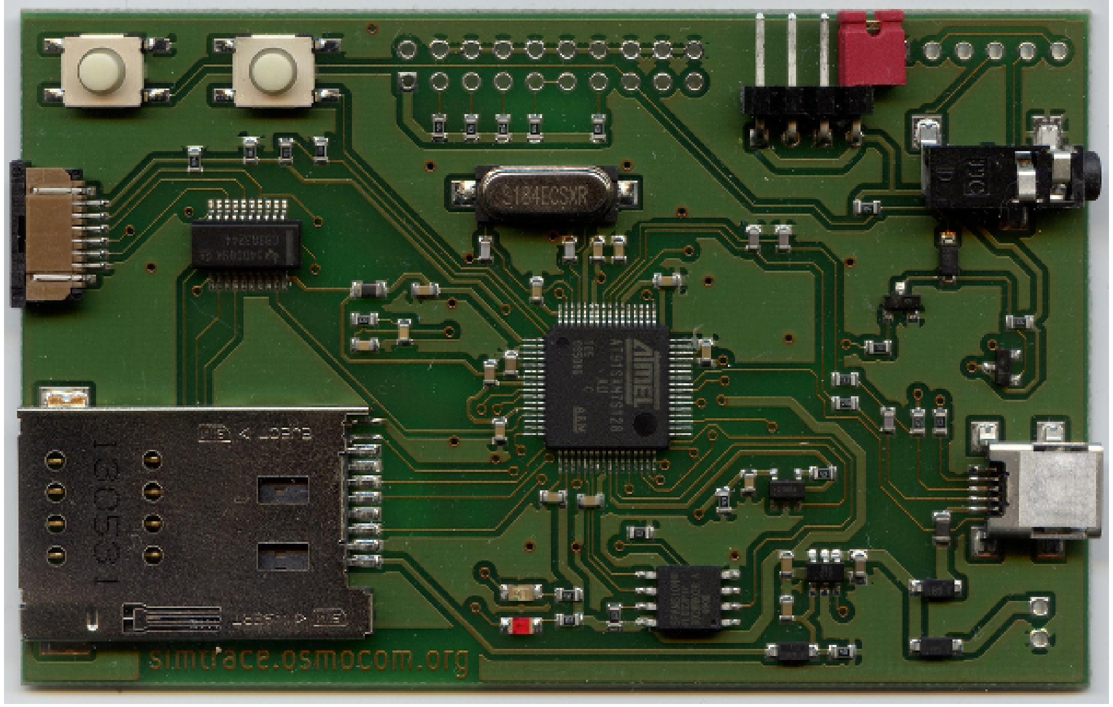
- Tools & setup
- Quick overview of transaction processing
- High level overview of captured data

Tools & setup

- Osmocom Simtrace
- “upgraded” cardreader
- Visa Electron card
- friendly merchant



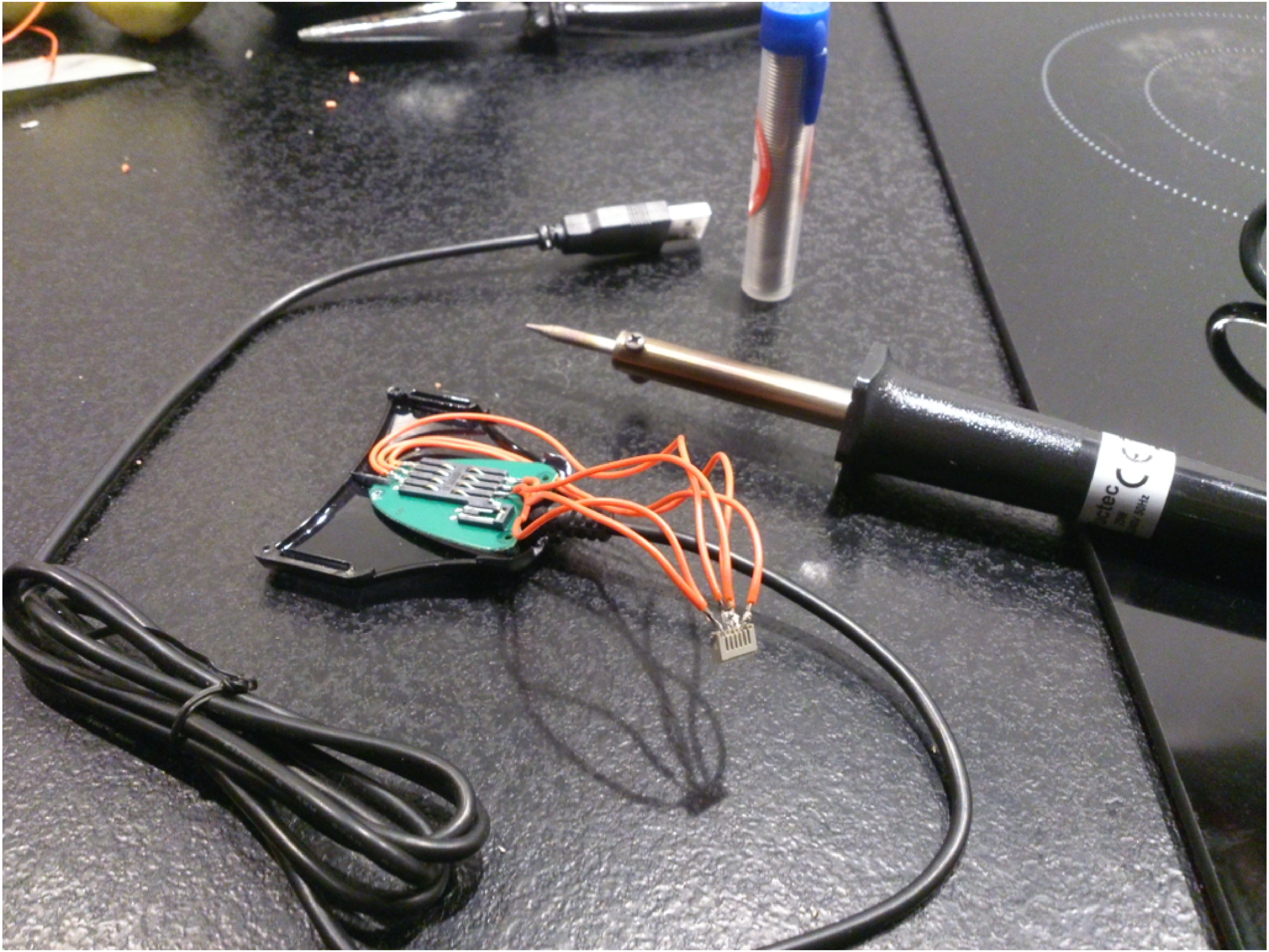
Simtrace
MITM board for SIM cards

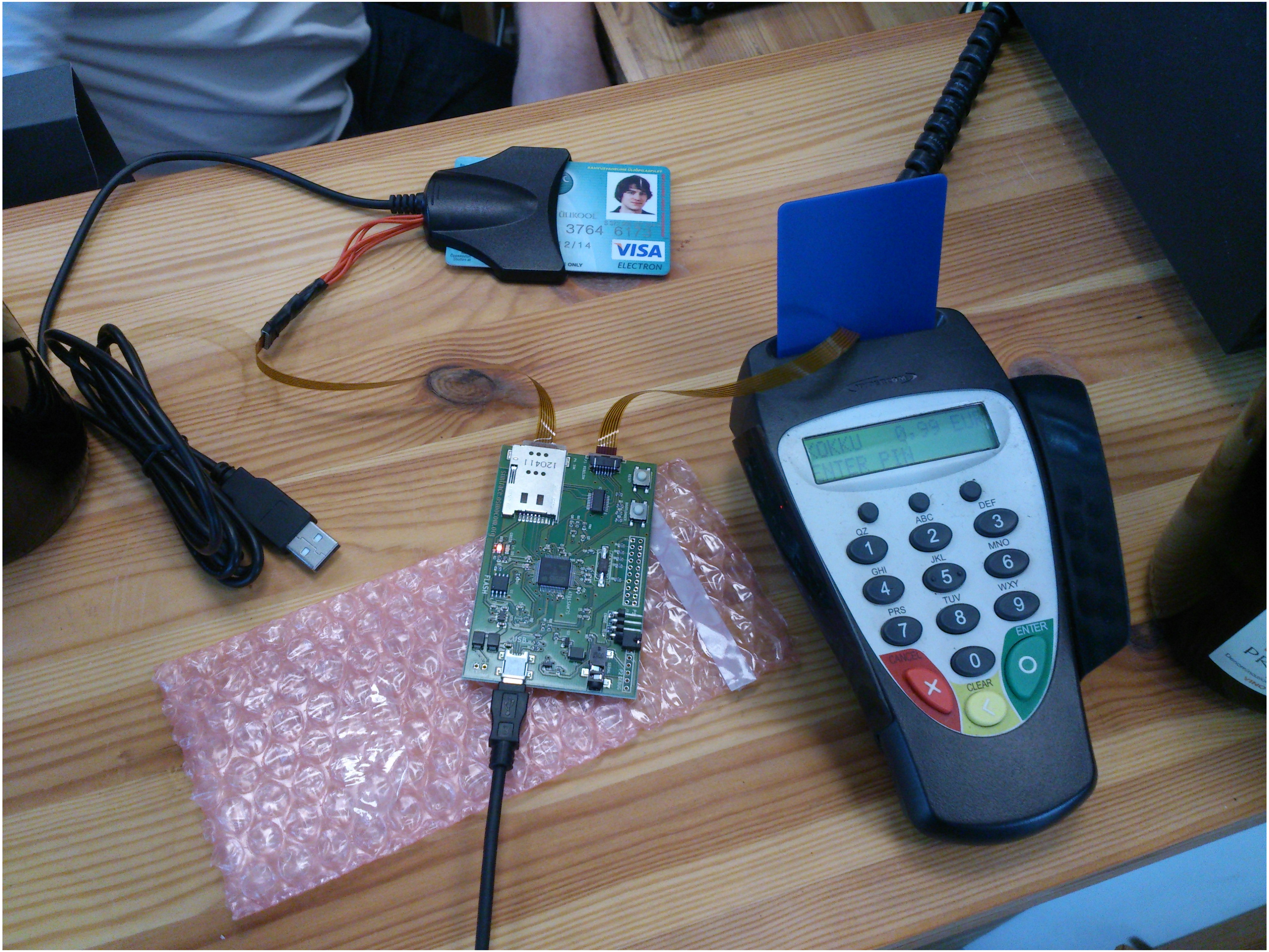


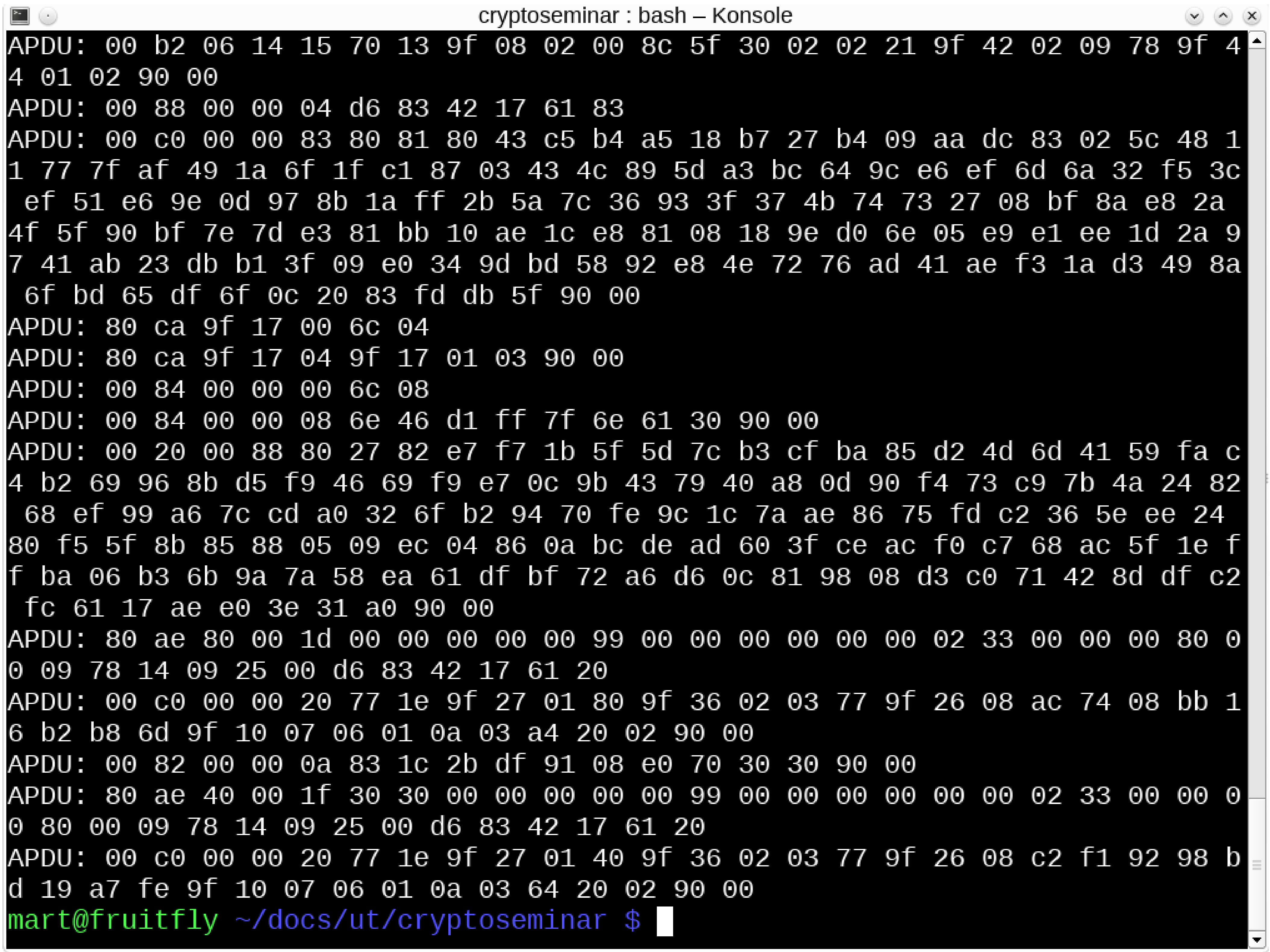
TERMINAL >

CHIP >

< PC


ctec


ÜLIKOOL
3764 6173
12/14
VISA
ELECTRON
KOKKU 0.99 EUR
ENTER PIN
QZ 1
ABC 2
DEF 3
GHI 4
JKL 5
MNO 6
PRS 7
TUV 8
WXY 9
0
CANCEL
CLEAR
ENTER
simtrace.osmocom.org
120411
USB
FLASH



```
APDU: 00 b2 06 14 15 70 13 9f 08 02 00 8c 5f 30 02 02 21 9f 42 02 09 78 9f 4
4 01 02 90 00
APDU: 00 88 00 00 04 d6 83 42 17 61 83
APDU: 00 c0 00 00 83 80 81 80 43 c5 b4 a5 18 b7 27 b4 09 aa dc 83 02 5c 48 1
1 77 7f af 49 1a 6f 1f c1 87 03 43 4c 89 5d a3 bc 64 9c e6 ef 6d 6a 32 f5 3c
 ef 51 e6 9e 0d 97 8b 1a ff 2b 5a 7c 36 93 3f 37 4b 74 73 27 08 bf 8a e8 2a
4f 5f 90 bf 7e 7d e3 81 bb 10 ae 1c e8 81 08 18 9e d0 6e 05 e9 e1 ee 1d 2a 9
7 41 ab 23 db b1 3f 09 e0 34 9d bd 58 92 e8 4e 72 76 ad 41 ae f3 1a d3 49 8a
 6f bd 65 df 6f 0c 20 83 fd db 5f 90 00
APDU: 80 ca 9f 17 00 6c 04
APDU: 80 ca 9f 17 04 9f 17 01 03 90 00
APDU: 00 84 00 00 00 6c 08
APDU: 00 84 00 00 08 6e 46 d1 ff 7f 6e 61 30 90 00
APDU: 00 20 00 88 80 27 82 e7 f7 1b 5f 5d 7c b3 cf ba 85 d2 4d 6d 41 59 fa c
4 b2 69 96 8b d5 f9 46 69 f9 e7 0c 9b 43 79 40 a8 0d 90 f4 73 c9 7b 4a 24 82
 68 ef 99 a6 7c cd a0 32 6f b2 94 70 fe 9c 1c 7a ae 86 75 fd c2 36 5e ee 24
80 f5 5f 8b 85 88 05 09 ec 04 86 0a bc de ad 60 3f ce ac f0 c7 68 ac 5f 1e f
f ba 06 b3 6b 9a 7a 58 ea 61 df bf 72 a6 d6 0c 81 98 08 d3 c0 71 42 8d df c2
 fc 61 17 ae e0 3e 31 a0 90 00
APDU: 80 ae 80 00 1d 00 00 00 00 00 99 00 00 00 00 00 00 02 33 00 00 00 80 0
0 09 78 14 09 25 00 d6 83 42 17 61 20
APDU: 00 c0 00 00 20 77 1e 9f 27 01 80 9f 36 02 03 77 9f 26 08 ac 74 08 bb 1
6 b2 b8 6d 9f 10 07 06 01 0a 03 a4 20 02 90 00
APDU: 00 82 00 00 0a 83 1c 2b df 91 08 e0 70 30 30 90 00
APDU: 80 ae 40 00 1f 30 30 00 00 00 00 00 99 00 00 00 00 00 00 02 33 00 00 0
0 80 00 09 78 14 09 25 00 d6 83 42 17 61 20
APDU: 00 c0 00 00 20 77 1e 9f 27 01 40 9f 36 02 03 77 9f 26 08 c2 f1 92 98 b
d 19 a7 fe 9f 10 07 06 01 0a 03 64 20 02 90 00
mart@fruitfly ~/docs/ut/cryptoseminar $
```

Reading binary dumps for the win?

- EMV = Europay, Mastercard, Visa
- standardized payment cards (currently v4.3)
- released as 4 “books” with a total of 747 pages

Transaction flow

Candidate list creation

iterate applications on the card

read application ids

Candidate List Creation

Application Selection

Read Application Data

Data Authentication

Cardholder Verification

Processing Restrictions

Terminal Risk Management

Card Action Analysis

Online Processing

Final Action Analysis

Transaction flow

Application selection

select the application in the terminal

activate application in the chip

Candidate List Creation

Application Selection

Read Application Data

Data Authentication

Cardholder Verification

Processing Restrictions

Terminal Risk Management

Card Action Analysis

Online Processing

Final Action Analysis

Transaction flow

Candidate List Creation

Application Selection

Read Application Data

Data Authentication

Cardholder Verification

Processing Restrictions

Terminal Risk Management

Card Action Analysis

Online Processing

Final Action Analysis

Read Application Data

expiration date

pin options

online/offline support

crypto keys

Transaction flow

Data authentication

offline mode:
verify data on the card
using digital signature

online mode:
challenge&response
with card's private key

Candidate List Creation

Application Selection

Read Application Data

Data Authentication

Cardholder Verification

Processing Restrictions

Terminal Risk Management

Card Action Analysis

Online Processing

Final Action Analysis

Transaction flow

Cardholder verification

online pin / offline pin / handwritten signature

pinpad->icc encrypted

Candidate List Creation
Application Selection
Read Application Data
Data Authentication
Cardholder Verification
Processing Restrictions
Terminal Risk Management
Card Action Analysis
Online Processing
Final Action Analysis

Transaction flow

Processing restrictions

check expiration date

check “application usage controls”

Candidate List Creation

Application Selection

Read Application Data

Data Authentication

Cardholder Verification

Processing Restrictions

Terminal Risk Management

Card Action Analysis

Online Processing

Final Action Analysis

Transaction flow

Terminal risk management

decide online/offline

“floor limits”

Candidate List Creation

Application Selection

Read Application Data

Data Authentication

Cardholder Verification

Processing Restrictions

Terminal Risk Management

Card Action Analysis

Online Processing

Final Action Analysis

Transaction flow

Card action analysis

decide online/offline/reject

can upgrade to online

can't upgrade to offline

Candidate List Creation

Application Selection

Read Application Data

Data Authentication

Cardholder Verification

Processing Restrictions

Terminal Risk Management

Card Action Analysis

Online Processing

Final Action Analysis

Transaction flow

Online processing

send ARQC to issuer

send response to chip

can downgrade to offline

Candidate List Creation

Application Selection

Read Application Data

Data Authentication

Cardholder Verification

Processing Restrictions

Terminal Risk Management

Card Action Analysis

Online Processing

Final Action Analysis

Transaction flow

Final card analysis

verify issuer online response

decide to accept/reject

generate transaction certificate (TC)

Candidate List Creation

Application Selection

Read Application Data

Data Authentication

Cardholder Verification

Processing Restrictions

Terminal Risk Management

Card Action Analysis

Online Processing

Final Action Analysis

Captured data

(19 request/response pairs)

00 A4 SELECT

Request:
file '1PAY.SYS.DDF01'

Response:
ShortFileIdentifier of directory element: 1
language preference: et,en,ru,de

00 B2 READ RECORD

Request:
ShortFileIdentifier: 1; record: 1

Response:
application identifier: VISA electron
application priority: 1

00 B2 READ RECORD

Request:
ShortFileIdentifier: 1; record: 2

Response:
File not found

00 C0 GET RESPONSE

Request:
empty

Response:
application id: Visa Electron
application priority: 1
language preference: et,en,ru,de
issuer url: 0x9f4d020b14

80 A8 GET PROCESSING OPTS

Request:
empty list

Response:
dynamic data authentication (DDA) supported,
cardholder verification supported,
perform terminal risk mgmt supported,
issuer authentication supported
locations of data records:
  SFI1, record 1-1
  SFI2, record 1-6

00 B2 READ RECORD

Request:
SFI:1, record: 1

Response:
card number: xx xx xx xx 37 64 61 73
expiration date: 14 12
cardholder name: BAKHOFF/MART

00 B2 READ RECORD

Request:
SFI:2, record: 1

Response:
Application Effective Date: 12 10 01
Application Expiration Date: 14 12 31
Application Usage Control: all allowed
Primary Account Number: xxxx xxxx 3764 6173
CDOL1, CDOL2, CVM
Issuer country code: 0x0233

00 B2 READ RECORD

Request:
SFI:2, record: 2

Response:
Issuer Public Key Certificate
Issuer Public Key Exponent
Issuer Public Key Remainder

00 B2 READ RECORD

Request:
SFI:2, record: 3

Response:
DDOL
ICC Public Key Exponent

00 B2 READ RECORD

Request:
SFI:2, record: 4

Response:
ICC Public Key Certificate

00 B2 READ RECORD

Request:
SFI:2, record: 5

Response:
ICC PIN Encipherment Public Key Certificate
ICC PIN Encipherment Public Key Exponent

00 B2 READ RECORD

Request:
SFI:2, record: 6

Response:
Application Version Number: 0x008c
Service Code: 0x0221
Application Currency Code: 0x0978
Application Currency Exponent: 2

00 88 INTERNAL AUTHENTICATE

Request:
(DDOL) 4 bytes nonce 0xd6834217

Response:
Signed Dynamic Application Data

80 CA GET DATA

Request:
pin try counter

Response:
PIN Try Counter: 3 remaining

00 84 GET CHALLENGE

Request:
empty

Response:
6e 46 d1 ff 7f 6e 61 30
(8-byte nonce generated by the ICC)

00 20 VERIFY

Request:
encrypted pin

Response:
ok

80 AE GENETATE AC

Request:
request ARQC (online mode)
amount: 0.99
terminal country code: 0x0233
TVR: transaction exeeds floor limit
transaction date: 14 09 25
nonce: 4 bytes

Response:
Application Transaction Counter (ATC): 0x0377
Application Cryptogram: ac 74 08 bb 16 b2 b8 6d

00 82 EXTERNAL AUTHENTICATE

Request:
Issuer Authentication Data:
83 1c 2b df 91 08 e0 70 30 30

Response:
ok

80 AE GENERATE AC

Request:
request transaction certificate
authorization response code: 0x3030
amount: 0.99
terminal country code: 0x0233
TVR: transaction exeeds floor limit
transaction date: 14 09 25
nonce: 4 bytes

Response:
Application Transaction Counter (ATC): 0x0377
Application Cryptogram: c2 f1 92 98 bd 19 a7 fe

Q/A

References

- www.emvco.com/specifications.aspx
- www.level2kernel.com/flow-chart.html
- cotignac.co.nz/emv-offline-data-authentication