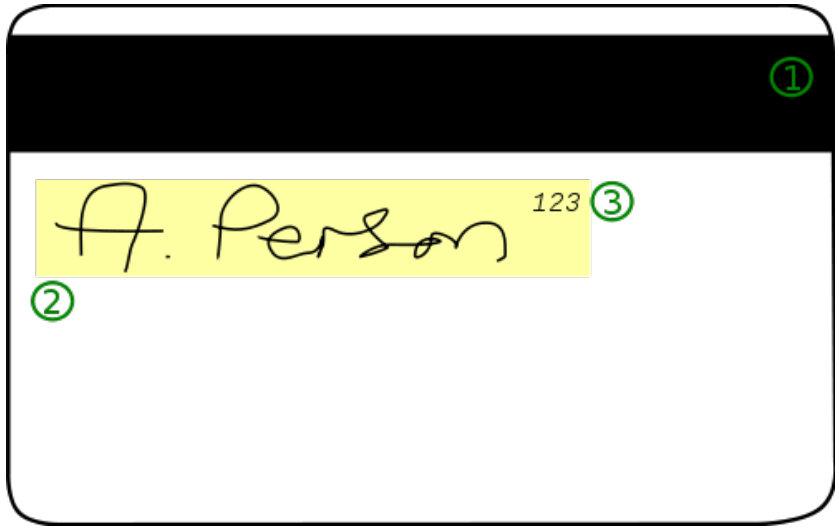
MTAT.07.017
Applied Cryptography

Smart Cards 1

University of Tartu

Spring 2015

Magnetic Stripe Card

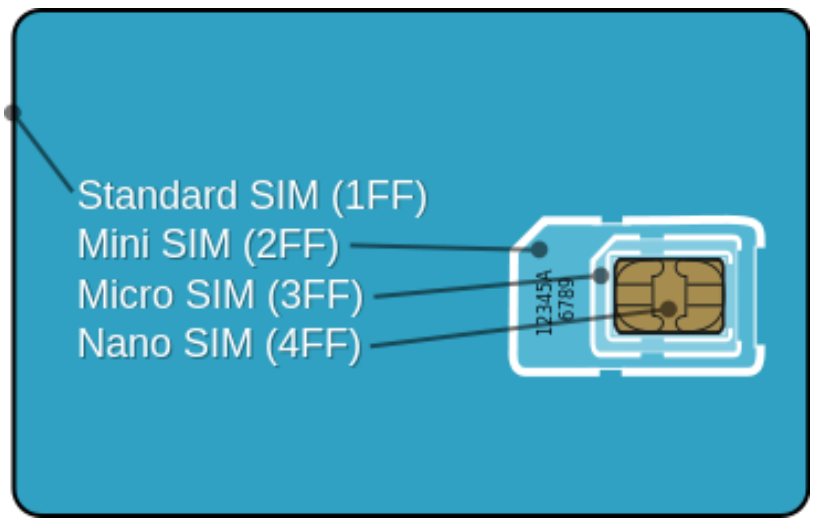


- Not a smart card!
- Three-track stripe:
  - Track 1 holds 79 6-bit plus parity bit characters
  - Track 2 holds 40 4-bit plus parity bit characters
  - Track 3 holds 107 4-bit plus parity bit characters
- Easily modifiable and cloneable
- Magnetic stripe and cryptography

Smart Card

A.K.A. chip card or integrated circuit card (ICC)
Contains protected non-volatile memory and microprocessor

ISO/IEC 7816 defines dimentions and location of the contacts, electrical interface, transmission protocols, etc.



- Contact smart cards
- Contactless smart cards
- Hybrids

Smart Card Communication

APDU: Application Protocol Data Unit

terminal $\longrightarrow$ card: command
terminal $\longleftarrow$ card: response

- Command APDU:
  Header (4 bytes) + data (0 ... 255 bytes)
  `[CLA]` `[INS]` `[P1]` `[P2]` $[L_c]$ $[C_{data}]$ ... $[L_e]$

  `00 b2 01 0c ff`
  `00 a4 01 0c 02 ee ee 00`

- Response APDU:
  Data (0 ... 256 bytes) + status word (2 bytes)
  $[R_{data}]$ ... `[SW1]` `[SW2]`

  `6a 82`
  `45 53 54 90 00`

Standard Commands

ClaIns P1 P2	Lc Send Data	Le Recv Data	Specification	Description
A0 04 00 00 00			3GPP TS 11.11	INVALIDATE
84 16 00 00 xx MAC			VSDC	CARD BLOCK
A0 20 00 xx 08 CHV Value			3GPP TS 11.11	VERIFY
00 82 00 xx 06 Manual			GEMPLUS MPCOS-EMV	EXTERNAL AUTHENTICATE
00 84 xx xx		08 Rnd Num	GEMPLUS MPCOS-EMV	GET CHALLENGE
00 88 XX xx 0A Manual			GEMPLUS MPCOS-EMV	INTERNAL AUTHENTICATE
A0 88 00 00 10 RAND : Rnd num		xx SRES(4B)	3GPP TS 11.11	RUN GSM ALGORITHM
A0 A2 00 xx xx Pattern		xx	3GPP TS 11.11	SEEK
00 A4 04 00 xx AID		00	GlobalPlatform	SELECT
00 A4 00 xx xx File ID || Name		00 Manual	VSDC	SELECT
A0 A4 00 00 02 File ID			3GPP TS 11.11	SELECT
A0 B0 xx xx		xx	3GPP TS 11.11	READ BINARY
00 B2 xx		00	VSDC	READ RECORD
A0 B2 xx xx		xx	3GPP TS 11.11	READ RECORD
00 C0		1C Key Info	GlobalPlatform	GET RESPONSE
A0 C0 00 00		xx	3GPP TS 11.11	GET RESPONSE
80 CA xx xx xx			VSDC	GET DATA
80 D0 xx xx xx Data to be written in EEPROM			VSDC	LOAD STRUCTURE
A0 D6 xx xx xx Data to be written in EEPROM			3GPP TS 11.11	UPDATE BINARY
00 DA xx xx xx Data			VSDC	PUT DATA
00 DC xx xx xx Data (and MAC)			VSDC	UPDATE RECORD
A0 DE 00 00 03 Data			3GPP TS 11.11	LOAD AoC(SICAP)
80 E0 xx xx xx FCI length			3GPP TS 11.11	CREATE FILE
00 E2 00 00 xx Record			3GPP TS 11.11	APPEND RECORD
A0 E4 00 00 02 xx xx			3GPP TS 11.11	DELETE FILE
...			...	...

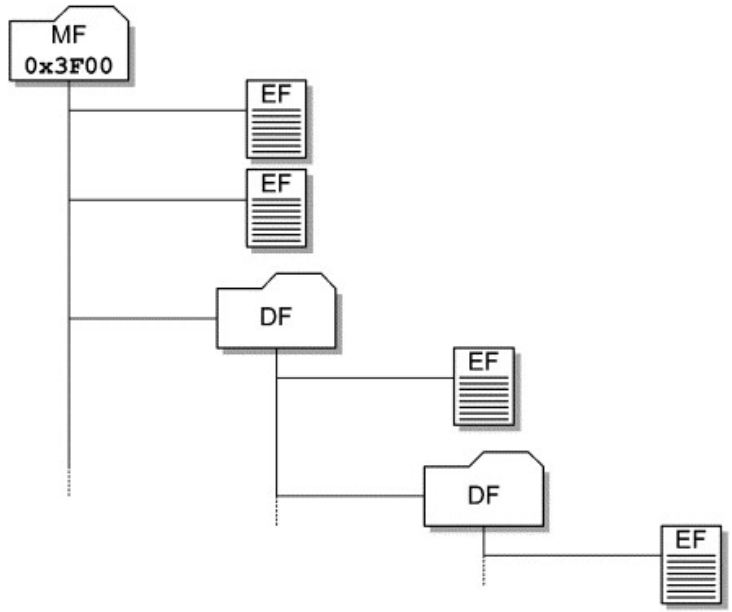
http://web.archive.org/web/20090630004017/http://cheef.ru/docs/HowTo/APDU.info

Standard Status Words

SW1 SW2	Message
'6X XX'	Transmission protocol related codes
'61 XX'	SW2 indicates the number of response bytes still available
'62 00'	No information given
'62 81'	Returned data may be corrupted
'62 82'	The end of the file has been reached before the end of reading
'62 83'	Invalid DF
'62 84'	Selected file is not valid. File descriptor error
'63 00'	Authentification failed. Invalid secret code or forbidden value
'63 81'	File filled up by the last write
'6A 00'	Bytes P1 and/or P2 are incorrect.
'6A 82'	File not found
'6A 83'	Record not found
'6A 84'	There is insufficient memory space in record or file
'6A 85'	Lc inconsistent with TLV structure
'6A 86'	Incorrect parameters P1-P2
'6A 87'	The P3 value is not consistent with the P1 and P2 values.
'6A 88'	Referenced data not found.
'9F XX'	Success, XX bytes of data available to be read via "Get_Response" task.
...	...

http://web.archive.org/web/20090623030155/http://cheef.ru/docs/HowTo/SW1SW2.info

Smart Card File System



- Adressable objects:
  - MF – Master File (root directory)
  - DF – Dedicated File (directory)
  - EF – Elementary File (data file)
- 2 byte file identifier (FID)
- EF has a header that contains metadata

There is no `ls`/`dir` command!

Answer To Reset (ATR)

"The ATR conveys information about the communication parameters proposed by the card, and the card's nature and state."

Can be used to identify the card:

- Cold ATR
- Warm ATR

```
$ pcsc_scan
  ATR: 3B DE 18 FF C0 80 B1 FE 45 1F 03 45 73 74 45 49 44 20 76 65 72 20 31 2E 30 2B
+ TS = 3B --> Direct Convention
+ T0 = DE, Y(1): 1101, K: 14 (historical bytes)
  TA(1) = 18 --> Fi=372, Di=12, 31 cycles/ETU
    129032 bits/s at 4 MHz, fMax for Fi = 5 MHz => 161290 bits/s
  TC(1) = FF --> Extra guard time: 255 (special value)
  TD(1) = C0 --> Y(i+1) = 1100, Protocol T = 0
  TC(2) = 80 --> Work waiting time: 960 x 128 x (Fi/F)
  TD(2) = B1 --> Y(i+1) = 1011, Protocol T = 1
  TA(3) = FE --> IFSC: 254
  TB(3) = 45 --> Block Waiting Integer: 4 - Character Waiting Integer: 5
  TD(3) = 1F --> Y(i+1) = 0001, Protocol T = 15 - Global interface bytes following
  TA(4) = 03 --> Clock stop: not supported - Class accepted by the card: (3G) A 5V B 3V
+ Historical bytes: 45 73 74 45 49 44 20 76 65 72 20 31 2E 30
  Category indicator byte: 45 (proprietary format)
+ TCK = 2B (correct checksum)
Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):
3B DE 18 FF C0 80 B1 FE 45 1F 03 45 73 74 45 49 44 20 76 65 72 20 31 2E 30 2B
Estonian Identity Card (EstEID v1.0 2006 cold)

>>> "\x45\x73\x74\x45\x49\x44\x20\x76\x65\x72\x20\x31\x2E\x30"
'EstEID ver 1.0'
```

Preparation: Hardware

- Get a smart card reader
  - Without a pin pad
  - Can buy one in Swedbank ~~or SEB~~ for EUR 5.75
  - Problems with built-in readers on DELL laptops
- Plug the reader into the USB port
  - If using VirtualBox forward USB to guest Ubuntu
  - Check if smart card reader detected by Ubuntu

```
$ dmesg
[ 1599.744116] usb 4-2: new full-speed USB device number 3 using uhci_hcd
[ 1599.921740] usb 4-2: New USB device found, idVendor=08e6, idProduct=3437
[ 1599.921751] usb 4-2: New USB device strings: Mfr=1, Product=2, SerialNumber=0
[ 1599.921760] usb 4-2: Product: USB SmartCard Reader
[ 1599.921767] usb 4-2: Manufacturer: Gemplus

$ lsusb
Bus 002 Device 002: ID 413c:a005 Dell Computer Corp. Internal 2.0 Hub
Bus 004 Device 003: ID 08e6:3437 Gemplus GemPC Twin SmartCard Reader   <--- external USB
Bus 005 Device 002: ID 03f0:0324 Hewlett-Packard SK-2885 keyboard
Bus 002 Device 003: ID 0b97:7761 O2 Micro, Inc. Oz776 1.1 Hub
Bus 002 Device 004: ID 0b97:7762 O2 Micro, Inc. Oz776 SmartCard Reader <--- DELLs built-in
```

Preperation: Software

- Install pcscd (this will allow us to send APDUs to smart card):

```
$ sudo apt-get install pcscd pcsc-tools
$ dpkg --list | grep -i pcsc
ii  libpcsc-perl   Perl interface to the PC/SC smart card library
ii  libpcsclite1   Middleware to access a smart card using PC/SC (library)
ii  pcsc-tools     Some tools to use with smart cards and PC/SC
ii  pcscd          Middleware to access a smart card using PC/SC (daemon side)

$ pcsc_scan -n
Scanning present readers...
0: O2 Micro Oz776 00 00
1: Gemalto PC Twin Reader 01 00
Reader 0: O2 Micro Oz776 00 00
  Card state: Card removed,
Reader 1: Gemalto PC Twin Reader 01 00
  Card state: Card inserted,
  ATR: 3B DE 18 FF C0 80 B1 FE 45 1F 03 45 73 74 45 49 44 20 76 65 72 20 31 2E 30 2B
Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):
Estonian Identity Card (EstEID v1.0 2006 cold)

$ scriptor -r "Gemalto PC Twin Reader 01 00"
Reading commands from STDIN
0a0a
> 0a 0a
< 6F 00 : No precise diagnosis.
```

Preperation: Software

- Install pyscard (we want to send APDUs using python):

```
$ sudo apt-get install python-pyscard
$ dpkg --list | grep -i pyscard
ii  python-pyscard Python wrapper above PC/SC API

$ python
>>> import smartcard
>>> smartcard.System.readers()
['02 Micro Oz776 00 00', 'Gemalto PC Twin Reader 01 00']
>>> connection = smartcard.System.readers()[1].createConnection()
>>> connection.connect()
>>> connection.getATR()
[59, 222, 24, 255, 192, 128, 177, 254, 69, 31, 3, 69, 115, 116, 69, 73, 68, 32, 118, 101, 1
>>> connection.transmit([0x0a, 0xa4, 0x00, 0x00, 0x02])
([], 110, 0)
>>> connection.getATR()
Traceback (most recent call last):
  File "/usr/lib/python2.7/dist-packages/smartcard/pcsc/PCSCCardConnection.py", line 163, i
    SCardGetErrorMessage(hresult))
smartcard.Exceptions.CardConnectionException: Failed to get status: Card was removed.
```

http://pyscard.sourceforge.net/pyscard-usersguide.html

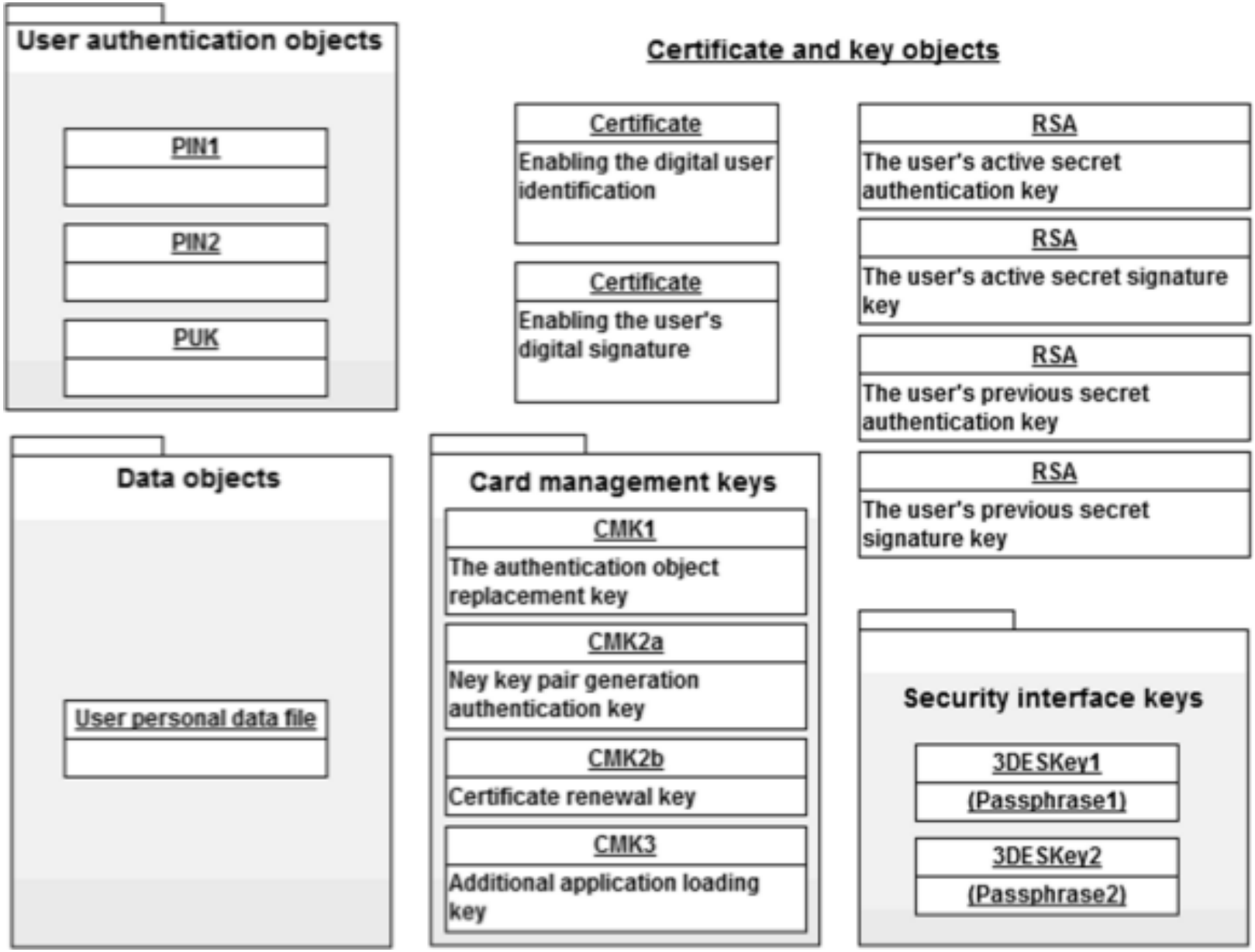
Estonian ID card

There are several versions of smart cards.

EstEID specification in English (includes examples):

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

Objects on security chip (spec page 11)



Security chip operations (spec page 12)

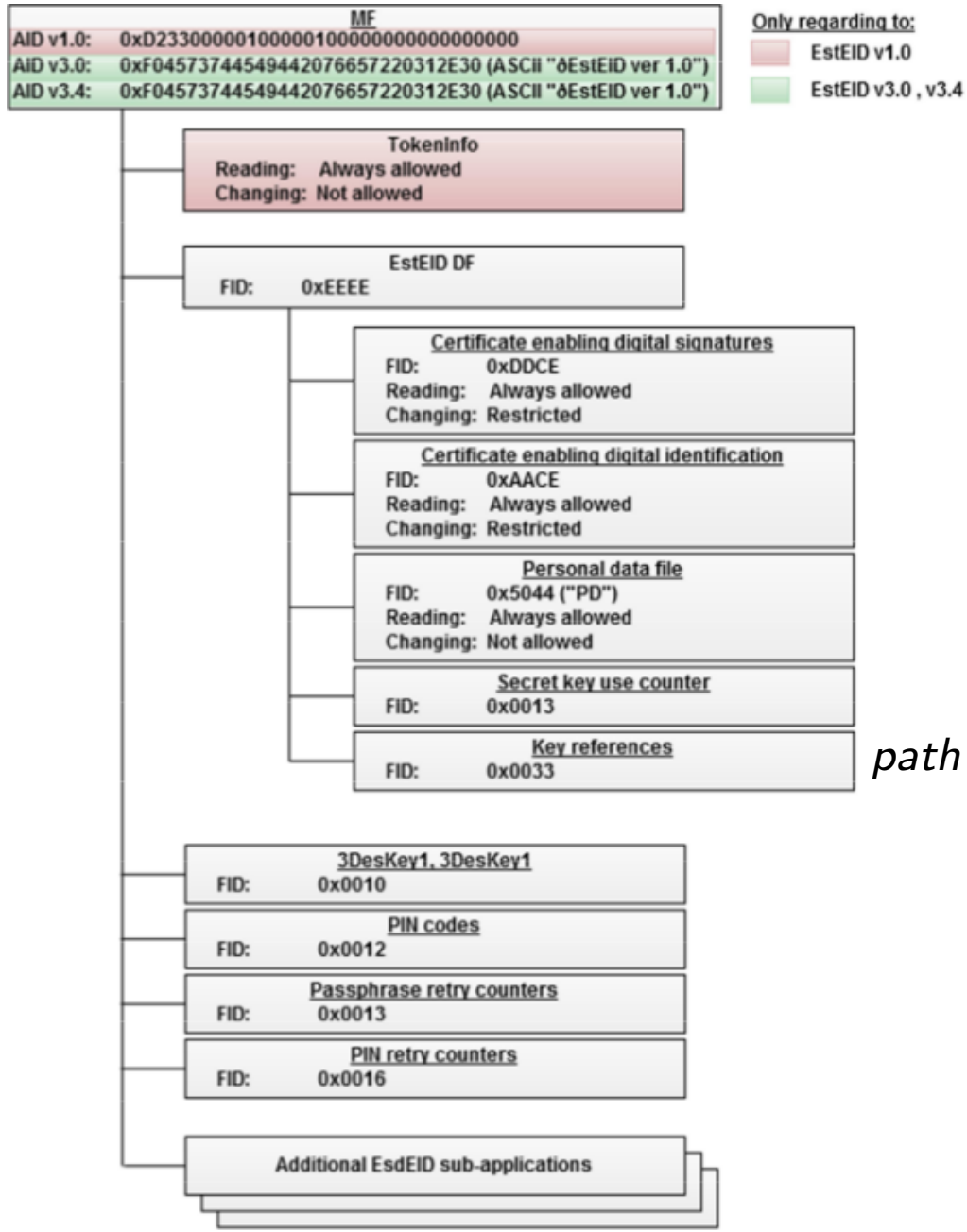
EstEID enables execution of the following operations:

1. The certificate and data reading operations
   a. Reading certificates; Certificate retrieval
   b. Reading the card user personal data file.
2. The administration of the card user authentication objects
   a. Changing the values of PIN1, PIN2 and PUK;
   b. Resetting the consecutive incorrect entries of PIN1 and PIN2;
   c. Assigning values to 3DESKeys.
3. Card user authentication
   a. card user authentication with PIN1, PIN2 and PUK;
   b. card user authentication with 3DESKey1 and 3DESKey2.
4. Operations with secret keys (sign/decrypt)
5. Card management operations
   a. Replacing authentication objects;
   b. Generating new key pairs;
   c. Loading certificates;
   d. Loading and deleting additional applications;
   e. Forming secure loading command series.

Chip versions (spec page 13)

Table 2-1 EstEID card application versions' properties				
	v1.0 and v1.0 since 2006	**v1.1 (DigiID)**	**v3.0 and v3.4 since 18.01.2011**	**v3.4**
Implementation platform	MICARDO	Multos	Java Card	
RSA module length	1024 bits		2048 bits	1024, 1280, 1536, 1984, 2048 bits
Hash algorithm support	SHA-1, SHA-224	SHA-1, SHA-224, SHA-256, SHA-384, SHA-518		
ECC module lengths	Not supported		**160** bits **192** bits **224** bits **256** bits	The RSA key length of the same security level ~1024 bits ~1536 bits ~2048 bits ~3072 bits
PKCS#1 padding support	v1.5			
Protocol support	T=0, T=1	T=0	T=0, T=1	T=0, T=1

EstEID file system (spec page 105)



$path = MF/EEEE/0013$

APDU commands (spec page 117)

Appendix Table 1-1 APDU commands			
Command	**INS**	**Brief description**	**See page**
CHANGE REFERENCE DATA	´24´	Changes the password for cardholder authentication	112
CREATE FILE	´E0´	Creates a directory or data field	115
EXTERNAL AUTHENTICATE /MUTUAL AUTHENTICATE	´82´	Authenticates the external world / external world and chip card	116
GENERATE PUBLIC KEY PAIR	´46´	Generates the public and the private part of a RSA key pair.	118
GET CHALLENGE	´84´	Generates and outputs a random number	120
GET RESPONSE	´C0´	Reads out the response data (T=0)	121
INTERNAL AUTHENTICATE	´88´	Authenticates the chip card or application	112
MANAGE SECURITY ENVIRONMENT	´22´	Passes on key references, random numbers, and data to be used for key derivation	123
PERFORM SECURITY OPERATION	´2A´	Various functions using symmetrical and asymmetrical keys: - COMPUTE DIGITAL SIGNATURE - DECIPHER - HASH	125 126 128 129
READ BINARY	´B0´	Reads from a transparent data field	131
READ RECORD	´B2´	Reads from a formatted data field	133
RESET RETRY COUNTER	´2C´	Resets the counter of failed attempts	134
SELECT FILE	´A4´	Selects a directory or data field	136
UPDATE BINARY	´D6´	Modifies a transparent data field	137
UPDATE RECORD	´DC´	Modifies a formatted data field	139
VERIFY	´20´	Authenticates the cardholder	140

Establishing connection

```
import sys
from smartcard.CardType import AnyCardType
from smartcard.CardRequest import CardRequest
from smartcard.CardConnection import CardConnection
from smartcard.util import toHexString, HexListToBinString

# this will wait until card inserted in any reader
channel = CardRequest(timeout=10, cardType=AnyCardType()).waitforcard().connection

# using T=0 for compatibility (i.e., DigiID) and simplicity
channel.connect(CardConnection.T0_protocol)

print "[+] Selected reader:", channel.getReader()

# detect and print EstEID card type (EstEID spec page 15)
atr = channel.getATR()
if atr == [0x3B,0xFE,0x94,0x00,0xFF,0x80,0xB1,0xFA,0x45,0x1F,0x03,0x45,...]:
    print "[+] EstEID v1.0 on Micardo Public 2.1"
elif atr == [0x3B,0xDE,0x18,0xFF,0xC0,0x80,0xB1,0xFE,0x45,0x1F,0x03,...]:
    print "[+] EstEID v1.0 on Micardo Public 3.0 (2006)"
elif atr == [0x3B,0x6E,0x00,0x00,0x45,0x73,0x74,0x45,0x49,0x44,0x20,...]:
    print "[+] EstEID v1.1 on MultiOS (DigiID)"
elif atr == [0x3B,0xFE,0x18,0x00,0x00,0x80,0x31,0xFE,0x45,0x45,0x73,...]:
    print "[+] EstEID v3.x on JavaCard"
else:
    print "[-] Unknown card:", toHexString(atr)
    sys.exit()
```

Transmitting APDUs

```
from smartcard.util import toHexString, HexListToBinString
def send(apdu):
    data, sw1, sw2 = channel.transmit(apdu)

    # success
    if [sw1,sw2] == [0x90,0x00]:
        return data
    # T=0 signals that there is more data to read
    elif sw1 == 0x61:
        return send([0x00, 0xC0, 0x00, 0x00, sw2]) # GET RESPONSE of sw2 bytes
    # probably error condition
    else:
        print "Error: %02x %02x, sending APDU: %s" % (sw1, sw2, toHexString(apdu))
        sys.exit()
```

- APDU commands and responses are lists containing integers (e.g., `[0,50,199,255]`)
- For pretty-printing a list of integers can be converted to hex string with spaces (i.e., `toHexString([0,50,199,255])=="00 32 C7 FF"`)
- To convert list of integers to byte string use `HexListToBinString([97,0x98,67])=="abC"`.

Using SELECT FILE (spec page 24 and 141)

To change pointer to Dedicated File EEEE:
`send([0x00, 0xA4, 0x01, 0x0C, 0x02, 0xEE, 0xEE])`

- CLA - `0x00`
- INS - `0xA4` (*command* - SELECT FILE)
- P1 - *what type of object to select*
  - `0x00` - Master File (root)
  - `0x01` - Dedicated File (directory)
  - `0x02` - Elementary File (data file)
  - `0x04` - Card Application (chip applet)
- P2 - *type of response*
  - `0x00` - Include object description FCI (FCP+FMD)
  - `0x04` - Include object description FCP (file control parameters)
  - `0x08` - Include object description FMD (file management data)
  - `0x0C` - Do not respond with description
- Lc - *length of file identifier (if present)*
- Data - *file identifier for EF, DF or application (if present)*

Task 1

Implement utility that displays personal data file, PIN retry and key usage counters on ID card.

```
$ ./esteid_info.py
[+] Selected reader: Gemalto PC Twin Reader 00 00
[+] EstEID v1.0 on Micardo Public 3.0 (2006)
[+] Personal data file:
        [1]Surname: PARŠOVS
        [2]First name line 1: ARNIS
        [3]First name line 2:
        [4]Sex: M
        [5]Nationality: LVA
        [6]Birth date: 05.08.1986
        [7]Personal identification code: 38608050013
        [8]Document number: E0044894
        [9]Expiry date: 26.08.2015
        [10]Place of birth: LÄTI / LVA
        [11]Date of issuance: 01.09.2010
        [12]Type of residence permit: ELAMISÕIGUSE LIIK / TYPE OF RIGHT OF RESIDENCE
        [13]Notes line 1: EL KODANIK / EU CITIZEN
        [14]Notes line 2: TÄHTAJALINE ELAMISÕIGUS KUNI 26.08.2015
        [15]Notes line 3: TEMPORARY RIGHT OF RESIDENCE UNTIL 26.08.2015
        [16]Notes line 4: EI VAJA TÖÖTAMISEKS TÖÖLUBA
[+] PIN retry counters:
        PIN1: 3 left
        PIN2: 3 left
        PUK: 3 left
[+] Key usage counters:
        signature key v1: 196 times
        signature key v2: 0 times
        authentication key v1: 972 times
        authentication key v2: 0 times
```

Put your output in `esteid_info.out` on your repository!

Task 1: Personal data file (spec page 24)

- Select MF/EEEE/5044
- Read all personal data file records with READ RECORD
  - Ignore the specification – read all 16 records
- Decode them to unicode using CP1252 codepage (i.e., `"somestring".decode("cp1252")`)

Example for obtaining personal identification code:

```
send([0x00, 0xA4, 0x00, 0x0C]) # SELECT FILE (MF)
send([0x00, 0xA4, 0x01, 0x0C]+[0x02, 0xEE, 0xEE]) # MF/EEEE
send([0x00, 0xA4, 0x02, 0x0C, 0x02, 0x50, 0x44]) # MF/EEEE/5044
record = send([0x00, 0xB2, 0x07, 0x04]) # READ RECORD 7th
print "Personal identification code:", HexListToBinString(record).decode("cp1252")
```

Task 1: PIN retry counters (spec page 28)

- Select MF/0016
- With READ RECORD read PIN1, PIN2, PUK records (records 0x01, 0x02, 0x03 respectively)
- Record's 5th byte will contain integer value of how many retries left

Task 1: Key usage counters (spec page 33)

- Select MF/EEEE/0013
- With READ RECORD read sign1, sign2, auth1 and auth2 key records (records 0x01, 0x02, 0x03, 0x04 respectively)
  - Card might have two sign and auth keys if certificates were renewed
- Record bytes 12th, 13th and 14th joined together contain 3 byte (Big-Endian) integer counter that describes how many times key may be used
  - Initial value 0xFFFFFF (i.e., key may be used 16 million times)
  - 3 byte integer can be calculated by $12th \cdot 256^2 + 13th \cdot 256^1 + 14th \cdot 256^0$

Task 2

Implement utility that downloads authentication and digital signature certificates stored on ID card.

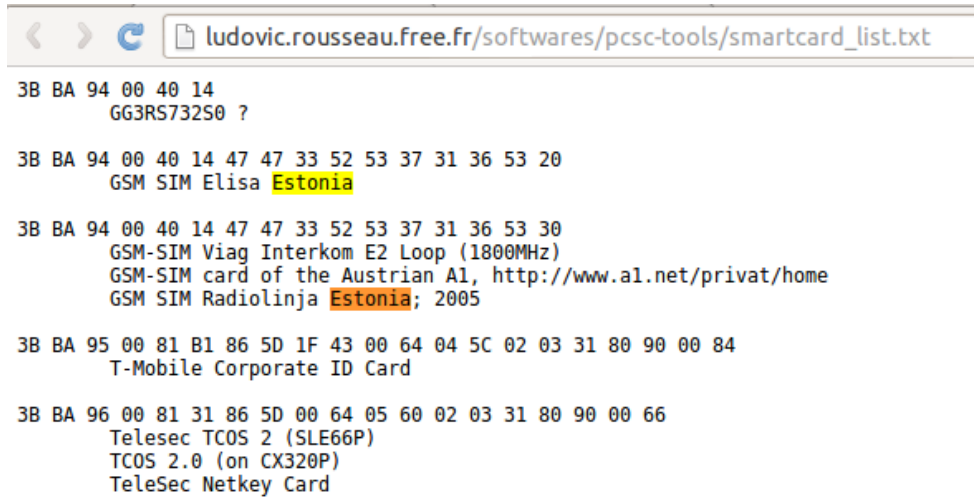
```
$ ./esteid_getcert.py --cert auth --out auth.pem
[+] Selected reader: OMNIKEY CardMan 1021 00 00
[+] EstEID v1.0 on Micardo Public 3.0 (2006)
[=] Retrieving auth certificate...
[+] Certificate size: 1116 bytes
[+] Certificate stored in auth.pem
$ openssl x509 -in auth.pem -text | grep O=ESTEID
        Subject: C=EE, O=ESTEID, OU=authentication, CN=...

$ ./esteid_getcert.py --cert sign --out sign.pem
[+] Selected reader: OMNIKEY CardMan 1021 00 00
[+] EstEID v1.0 on Micardo Public 3.0 (2006)
[=] Retrieving sign certificate...
[+] Certificate size: 1052 bytes
[+] Certificate stored in sign.pem
$ openssl x509 -in sign.pem -text | grep O=ESTEID
        Subject: C=EE, O=ESTEID, OU=digital signature, CN=...

$ wget https://sk.ee/upload/files/ESTEID-SK_2007.pem.crt
$ wget https://sk.ee/upload/files/ESTEID-SK_2011.pem.crt
$ openssl verify -CAfile ESTEID-SK_2007.pem.crt sign.pem
$ openssl verify -CAfile ESTEID-SK_2011.pem.crt sign.pem
sign.pem: OK
```

Put your output from these commands in `esteid_getcert.out`!

Task 2: Retrieve certificate (spec page 35)

- Select MF/EEEE/AACE (authentication certificate)
- Select MF/EEEE/DDCE (digital signature certificate)
- Certificate is stored in a DER form with garbage appended in a transparent file which is of fixed size
  - With READ BINARY (spec page 137) read first 10 bytes of certificate
  - Calculate certificate length by parsing length field of certificate ASN.1 SEQUENCE structure
- Read whole certificate (in a loop) using READ BINARY
  - On one READ BINARY only 0xFF bytes can be read
  - Offset must be specified as two byte integer specifying most significant byte in P1 and least significant byte in P2
  - Two byte integer can be split into [MSByte, LSByte] by `[i/256, i%256]` or by bit operations `[i>>8, i&0xFF]` or by `int_to_bytestring(i, 2)[0]`, `int_to_bytestring(i, 2)[1]`

ATR Collecting Party




```
$ wget http://ludovic.rousseau.free.fr/softwares/pcsc-tools/smartcard_list.txt
--output-file=~/.smartcard_list.txt
$ pcsc_scan
Reader 0: Gemalto PC Twin Reader 00 00
  Card state: Card inserted, Shared Mode,
  ATR: 3B 6D 00 00 00 31 C0 71 D6 64 19 16 01 00 84 90 00
Possibly identified card (using ~/.smartcard_list.txt):
        NONE
Your card is not present in the database. If your ATR is still not in the latest version
then please send a mail to <ludovic.rousseau@free.fr> containing:
- your ATR
- a card description (in english)
```

http://smartcard-atr.appspot.com/