Estonia ID1 Chip/App 2018

Technical Description

Document Release Version: V0.8

Table for Document Version History		
Date	Version	Changes/notices
09.08.2018	0.1	Draft and document
10.09.2018	0.2	APPENDIX - APDU commands and responses
25.09.2018	0.3	APPENDIX - DF PERSONAL DATA format
01.10.2018	0.4	APPENDIX - DF PERSONAL DATA file for DigiID, Resident Permit cards
16.11.2018	0.5	Updated APPENDIX
19.11.2018	0.6	Updated APPENDIX added : • APDU message command-response pair • INTERNAL AUTHENTICATE for Client/Server Authentication • Compute Digital Signature
21.11.2018	0.7	Updated APPENDIX
04.12.2018	0.8	Updated APPENDIX Added : • “Personal data” - transparent files, examples of reading APDU

CONTENTS

1 JAVA GLOBAL PLATFORM

ID-One™ Cosmo v8.1 is certified as an open platform CC EAL5+ including application loading mechanism. As a result, even if a non-evaluated applet is loaded the security is not compromised and the certificate remains valid. The certification of an external application is also strongly simplified by this existing certificate by simple composition on the platform. The Cosmo is compliant with the latest international standards:

- JavaCard™ 3.0.4 Classic Edition
- Global Platform v2.2.1 (ID Configuration v1.0)
- ISO/IEC 7816 parts 1, 2, 3, 4, 5, 6, 8 and 9
- ISO/IEC 14443 Type A

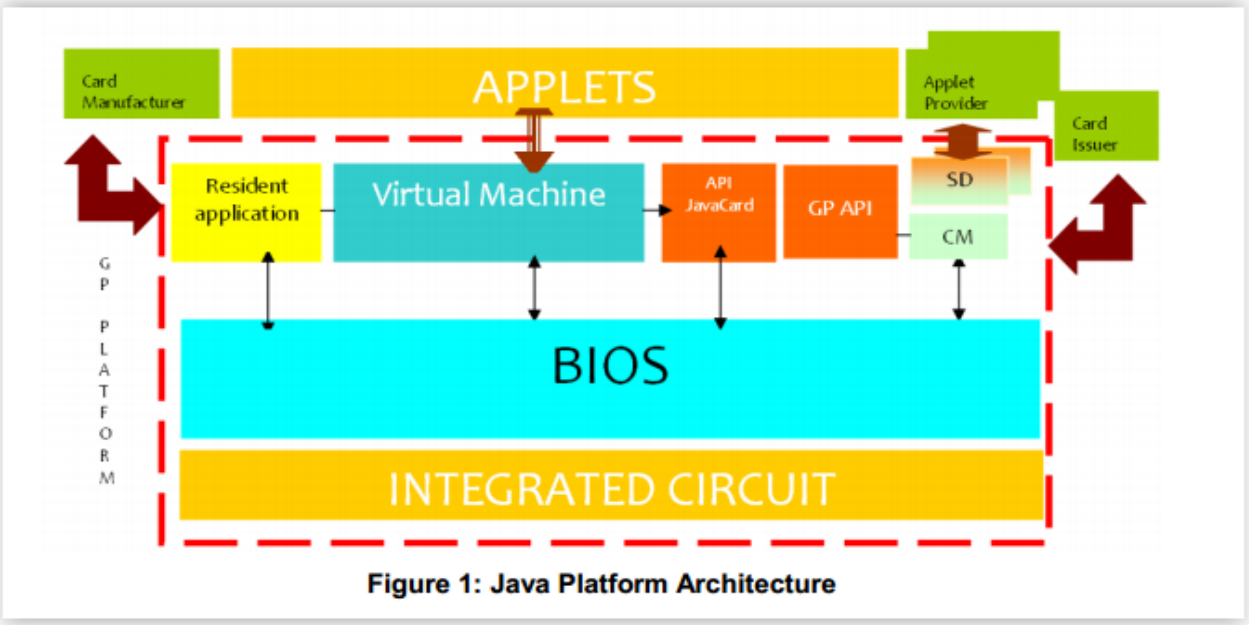

Figure 1: Java Platform Architecture

JAVA GLOBAL PLATFORM CONFIGURATION

CARD MANAGER AID

`A0000001510000 (Standard Global Platform value)`

SECURE CHANNEL PROTOCOLS

Available choices:

		Selected
SCP03 - AES 128 / AES 256		**Description**
60	pseudo-random, R-MAC and R-ENC support	✓

CONTACT INTERFACE

The main choices are :

Choice	Default	Estonia
Communication Protocol		T=0 and T=1
Default Communication Protocol		T=1
Historical Bytes	0031C16408402130	4553544F4E49412D654944 (ESTONIA-eID)

TS	’3B’								
Protocol bytes	T0	TA1	TC1	TD1	TD2	TA3	TB3	TD3	TA15
	’DB’	’96’	’00’	’80’	‘B1’	‘FE’	‘45’	‘1F’	‘83’
Historical bytes	T1	T2	T3	T4	T5	T6	T7	T8	
	’00’	’31’	’C1’	‘64’	‘084021’				
Additional bytes	STATE	SW1	SW2	TCK					
	’00’	’90’	’00’	‘XX’					

TABLE 1: DEFAULT ATR

The ATR resulting from default choices is detailed below:

- TA1=’96’: F=512, D=32, i.e. 307 200 bauds,
- TC1=’00’: No Extra Guard time (specific to T=0 protocol - character time = 12 etu),
- TD1=’80’: Card bi-protocol T=0/T=1,
- TA3=’FE’: IFSC=254 bytes (specific to T=1 protocol),
- TB3=’45’: Waiting times BWI=4, CWI=5 (specific to T=1 protocol),
- TA15=’83’: Clock stop indicator state H (high) and class A & B (class C is not supported)
- Historical Bytes: 0012233053654944 0F 9000
    - Category Indicator: 0x00
    - Country Code (ISO 3166-1): 0x233F (Estonia)
    - Card’s issuer data: 0x654944 (“eID”)
    - LCS: 0x0F (Termination State)
    - SW: 0x9000
- TCK: 0xF1

The resulting specific ATR to Estonia is:

```
3B DB 96 00 80 B1 FE 45 1F 83 00 12 23 3F 53 65 49 44 0F 9000 F1
```

CONTACTLESS INTERFACE

(ATS): Enable / Disable / Frozen

speed rate (kbit/s): 848 / 424 / 212 / 106

Historical bytes: Default (same as contact) / Other (between 0 and 15 bytes)

Default parameters are:

- Baud rate = symmetrical 848 kb/s,
- FWI + CID:
  - FWI = 'C', FWT = 1.237s,
  - CID supported,
- Historical Bytes: 0012233053654944 0F 9000
  - Category Indicator: 0x00
  - Country Code (ISO 3166-1): 0x233F (Estonia)
  - Card's issuer data: 0x654944 ("eID")
  - LCS: 0x0F (Termination State)
  - SW: 0x9000

VHBR (Very High Baud Rate) is activated.

The resulting specific ATS to Estonia is:

```
3B 8B 80 01 00 12 23 3F 53 65 49 44 0F 90 00 A0
```

2 PKI APPLICATION

The application offering PKI functionalities for Estonia eID Documents is IAS-ECC, a sophisticated but standardized solution conforming to CEN TS 15480-2 (European eID) with extra features, everything detailed in the inter-industry standard "EUROPEAN CARD FOR e-SERVICES AND NATIONAL e-ID APPLICATIONS – Technical Specifications" (rev. 1.0.1).

IAS-ECC, which stands for Identification Authentication Signature - European Citizen Card, is a PKI application QSCD certified according to the following Protection Profiles:

- CEN/EN 14169-2 (EN 419211-2) – Device with key generation
- CEN/EN 14169-3 (EN 419211-3) – Device with key import
- CEN/EN 14169-4 (EN 419211-4) – Extension for device with key generation and trusted communication with certificate generation application
- CEN/EN 14169-5 (EN 419211-5) – Extension for device with key generation and trusted communication with signature creation application
- CEN/EN 14169-6 (EN 419211-6) – Extension for device with key import and trusted communication with signature creation application

The several features available in IAS-ECC are for final user or for securing the usage on field.

In Estonia eID documents, four final user features will be made available:

1. Data Storage
2. Digital Signature
3. Client/Server Authentication
4. Asymmetric key generation

through a set of digital security features which will guarantee the needed security level, according to the use case:

1. User Authentication
2. Role Authentication (external authentication for obtaining a privilege)
3. Device Authentication (mutual authentication with or without Secure Channel opening)
4. Secure Messaging

The configuration of IAS-ECC application aims to implement on card the all the elements needed to fulfill Estonia eID use cases in term of functionality and security level.

3 ENTITIES INTERACTING WITH ESTONIA EID

According to use cases, several entities will interact with Estonia eID Documents, with different privileges and security requirements. In the following sections each of the entities will be described for role, privileges, security requirements and relations with other entities.

Characteristics of entities will reflect on IAS-ECC configuration with the creation of special objects linked to the entity itself.

CARDHOLDER

The cardholder is the natural person to whom authentication key belongs, and to whom the usage is reserved. The cardholder can authenticate himself to his document thanks to a secret he knows (PIN1 code).

In Estonia use cases, Cardholder, Signatory and Administrator cardholder are the same natural person, to whom PIN1, PIN2 and PUK are given.

CARDHOLDER	
Authentication type	**User Authentication**
Object Name	PIN1
Type	PIN
Try Counter	3 (rem.) / 3 (max)
Usage Counter	Infinite / Infinite
Format	Numeric
Length (bytes)	4 (min) – 12 (max)
Initial Value	Production value: random number of 4 digits Test value: 1111
Change Condition	Always allowed
Reset Condition	Administrator Cardholder (PUK) or Administrator Police (Police Key)
Privileges granted	- Internal Authenticate on active Authentication Private Key

SIGNATORY

The signatory is the natural person to whom signature key belongs, and to whom the usage is reserved. The signatory can authenticate himself to his document thanks to a secret he knows (PIN2 code).

In Estonia use cases, Cardholder, Signatory and Administrator cardholder are the same natural person, to whom PIN1, PIN2 and PUK are given.

SIGNATORY	
Authentication type	**User Authentication**
Object Name	PIN2
Type	PIN
Try Counter	3 (rem.) / 3 (max)
Usage Counter	Infinite / Infinite
Format	Numeric
Length (bytes)	5 (min) – 12 (max)
Initial Value	Production value: random number of 5 digits Test value: 22222
Change Condition	Always allowed
Reset Condition	Administrator Cardholder (PUK) or Administrator Police (Police Key)
Privileges granted	- PSO Compute Digital Signature on active Signature Private Key

ADMINISTRATORS

An administrator is an entity (natural or a machine) which manages the content of the card, but has not the right to use credentials. Several operations can be performed under supervision of an administrator:

- Key generation;
- Key import;
- Key export;
- PIN personalization;
- PIN reset retry counter

In Estonia documents, there are administrators **with different privileges granted:**

- Cardholder
- Police

In Estonia use cases, Cardholder, Signatory and “Administrator cardholder” are the same natural person, to whom PIN1, PIN2 and PUK are given.

CARDHOLDER	
Authentication type	User Authentication
Object Name	PUK
Type	PIN
Try Counter	3 (rem.) / 3 (max)
Usage Counter	Infinite / Infinite
Format	Numeric
Length (bytes)	8 (min) – 12 (max)
Initial Value	Production value: random number of 8 digits Test value: 99999999
Change Condition	Always allowed
Reset Condition	Administrator Police (Police Key)
Privileges granted	- Reset Retry Counter on PIN1 - Reset Retry Counter on PIN2

POLICE	
Authentication type	Device Authentication
Object Name	Police Key
Type	Symmetric
Try Counter	5 (rem.) / 5 (max)
Usage Counter	Infinite / Infinite
Format	AES – SHA256
Length	32 bytes (256 bit)
Initial Value	Key references are: GAK.2B3B7ED0.AES256.POLICE.KENC.00000001 GAK.2B3B7ED0.AES256.POLICE.KMAC1.00000001
Change Condition	Never allowed
Reset Condition	Never allowed
Privileges granted	- PIN1 First Personalization - PIN2 First Personalization - PUK First Personalization - Reset Retry Counter PIN1 - Reset Retry Counter PIN2 - Reset Retry Counter PUK - Authentication Keypair generation; - Authentication Public Key export; - Authentication Certificate import; - Signature Keypair generation; - Signature Public Key export; - Signature Certificate import

IFD (INTERFACE DEVICE)

The IFD is the interface device used in contactless and it is in charge of sending the data to Estonia eID documents in a manner ensuring privacy.

The remote IT entity corresponding to IFD has to be created and should be enforced whenever in contactless. In such case, it shall be unique and it replaces any middleware key.

INTERFACE DEVICE	
Authentication type	PACE v2 (Unauthenticated Diffie Hellmann)
Object Name	N/A
Type	PACE Java Applet
Format	IAS MRZ and CAN
Initial Value	IAS MRZ = 8 random bytes IAS CAN = ICAO CAN id-PACE-Nist-P256 AES-CBC-CMAC-256
Privileges granted	- To exchange APDU in Contactless with PKI application in a secure channel. No applicative privileges are granted.

4 PKI DATA STRUCTURE

Estonia eID has a fixed and predetermined content, so any object could be pre-created in personalization phase, enforcing security conditions in factory.

In use phase objects can only be used.

```
IAS-ECC Root
|-- Document Number
|-- EF.Dir
|-- EF.CardAccess
|-- PIN1
|-- PUK
|-- Police Key
|-- DF Personal Data
|        |-- PD1 (Surname)
|        |-- PD2 (First Name)
|        |-- PD3 (Sex)
|        |-- PD4 (Citizenship ISO3166 alpha-3)
|        |-- PD5 (Date and place of birth)
|        |-- PD6 (Personal Identification Code)
|        |-- PD7 (Document Number)
|        |-- PD8 (Expiry Date)
|        |-- PD9 (Date and place of Issuance)
|        |-- PD10 (Type of residence permit)
|        |-- PD11 (Notes Line 1)
|        |-- PD12 (Notes Line 2)
|        |-- PD13 (Notes Line 3)
|        |-- PD14 (Notes Line 4)
|        |-- PD15 (Notes Line 5)
|-- ADF AWP
|        |-- Authentication Public Key 1
|        |-- Authentication Private Key 1
|        |-- Authentication Certificate 1
|        |-- Authentication Public Key 2
|        |-- Authentication Private Key 2
|        |-- Authentication Certificate 2
|        |-- ISO 7816-15 data structure
|-- ADF QSCD
         |-- PIN2
         |-- Signature Public Key 1
         |-- Signature Private Key 1
         |-- Signature Certificate 1
         |-- Signature Public Key 2
         |-- Signature Private Key 2
         |-- Signature Certificate 2
         |-- ISO 7816-15 data structure
```

IAS-ECC ROOT

It is the master file containing any other object. It is not shared with MRTD MF.

Object Type	**ADF**						
Object ID	3F00						
Object AID	A0 00 00 00 77 01 08 00 07 00 00 FE 00 00 01 00						
Object size	N/A						
Condition	Delete	Terminate	Activate	Deactivate	DF Creation	EF Creation	SDO Creation
Contact	NEVER	NEVER	NEVER	NEVER	NEVER	NEVER	NEVER
Contactless	NEVER	NEVER	NEVER	NEVER	NEVER	NEVER	NEVER

DOCUMENT NUMBER

It is a transparent file holding the document number as per Estonia specifications: two prefix letters and a seven digits unique number for the given prefix.

The Document Number is generated during personalization phase.

Ex: AB1234567

The document number is stored in the chip in ASCII encoding, inside tag 04:

Ex: 0x04 09 414231323334353637

Object Type	**Transparent EF**						
Object ID	D003						
Object size	11 bytes						
Condition	Delete	Terminate	Activate	Deactivate	RFU	Update	Read
Contact	NEVER	NEVER	NEVER	NEVER	-	NEVER	ALWAYS
Contactless	NEVER	NEVER	NEVER	NEVER	-	NEVER	IFD

EF.CARDACCESS

It is a transparent containing the relevant SecurityInfos that are required for PACE.

- PACEInfo
- PACEDomainParameterInfo

The PACE algorithm encoded in Estonia eID Documents is:

PACEInfo: Id-PACE-ECDH-GM-AES-CBC-CMAC-256

PACEDomainParameterInfo: BRAINPOOL_P384_R1 (BrainpoolP384r1)

Object Type	**Transparent EF**						
Object ID	011C						
Object size	48 bytes						
Condition	Delete	Terminate	Activate	Deactivate	RFU	Update	Read
Contact	NEVER	NEVER	NEVER	NEVER	-	Police	ALWAYS
Contactless	NEVER	NEVER	NEVER	NEVER	-	Police	ALWAYS

DF PERSONAL DATA

It is the DF containing Personal Data transparent files

Object Type	**DF**						
Object ID	5000						
Object size	N/A						
Condition	Delete	Terminate	Activate	Deactivate	DF Creation	EF Creation	SDO Creation
Contact	NEVER	Police	Police	Police	Police	Police	Police
Contactless	NEVER	Police AND IFD	Police AND IFD	Police AND IFD	Police AND IFD	Police AND IFD	Police AND IFD

PERSONAL DATA EFS

All personal data files are transparent files holding the cardholder personal data as it is printed on the card surface.

They are all mandatorily presents in the card.

In case the personal data field is empty, the corresponding Data File exists, has a one-byte size and contains the 0x00 byte.

In case the personal data field is present, the data length defines personal data file size

.

File	Content
PD1	Surname
PD2	First name
PD3	Sex
PD4	Citizenship (3 letters) Pursuant to ISO 3166-1 alpha-3.
PD5	Date and place of birth
PD6	Personal identification code
PD7	Document number
PD8	Expiry date
PD9	Date and place of issuance
PD10	Type of residence permit
PD11	Notes line 1
PD12	Notes line 2
PD13	Notes line 3
PD14	Notes line 4
PD15	Notes line 5

Object Type	**Transparent EF**						
Object ID	50XX (5001, 5002… , 500F)						
Object size	Fit to personalization data						
Condition	Delete	Terminate	Activate	Deactivate	RFU	Update	Read
Contact	Police	Police	Police	Police	-	Police	ALWAYS
Contactless	Police AND IFD	Police AND IFD	Police AND IFD	Police AND IFD	-	Police AND IFD	IFD

ADF AWP

It is the application DF containing credential objects not related to QSCD (authentication and encryption)

Object Type	**ADF**						
Object ID	ADF1						
Object AID	"AWP Application"						
Object size	N/A						
Condition	Delete	Terminate	Activate	Deactivate	DF Creation	EF Creation	SDO Creation
Contact	Police	Police	Police	Police	Police	Police	Police
Contactless	Police AND IFD	Police AND IFD	Police AND IFD	Police AND IFD	Police AND IFD	Police AND IFD	Police AND IFD

AUTHENTICATION CREDENTIALS

Authentication credentials are composed by public/private keypair objects and a certificate object, logically linked.

In order to mitigate consequences of a failed credential renewal process, the renewal process could be achieved according the following sequence:

1. Key pair generation on the inactive keypair;
2. Resize of the inactive certificate container
3. Certificate import in the inactive certificate container;
4. In case of success, logical deletion of previous keypair and certificate;
5. In case of failure, logical deletion of tentative keypair and certificate.

Object Type	**EC Private Asymmetric Key**						
Object ID	01						
Object size	384 bit						
Algorithm	ECDSA-SHA-384 over NIST P-384 (secp384r1)						
Non Repudiation	FALSE						
Usage Counter	Unlimited / Unlimited						
Condition	PSO CDS	Internal Auth	PSO Decipher	Gen Key Pair	RFU	Put Data	Get Data
Contact	NEVER	Cardholder	Cardholder	Police	-	NEVER	ALWAYS
Contactless	NEVER	Cardholder AND IFD	Cardholder AND IFD	Police AND IFD	-	NEVER	IFD

Object Type	EC Public Asymmetric Key						
Object ID	01						
Object size	384 bit						
Algorithm	ECDSA-SHA-384 over NIST P-384 (secp384r1)						
Non Repudiation	FALSE						
Condition	PSO Verify	External Auth	PSO Encipher	Gen Key Pair	RFU	Put Data	Get Data
Contact	NEVER	NEVER	NEVER	Police	-	NEVER	Police
Contactless	NEVER	NEVER	NEVER	Police AND IFD	-	NEVER	Police AND IFD

Object Type	Transparent EF (Certificate)						
Object ID	3401						
Object size	Fit to certificate size						
Condition	Delete	Terminate	Activate	Deactivate	RFU	Update	Read
Contact	NEVER	NEVER	NEVER	NEVER	-	Police	ALWAYS
Contactless	NEVER	NEVER	NEVER	NEVER	-	Police AND IFD	IFD

Object Type	EC Private Asymmetric Key						
Object ID	02						
Object size	512 bit						
Algorithm	ECDSA-SHA-512 over brainpoolP512r1						
Non Repudiation	FALSE						
Usage Counter	Unlimited / Unlimited						
Condition	PSO CDS	Internal Auth	PSO Decipher	Gen Key Pair	RFU	Put Data	Get Data
Contact	NEVER	Cardholder	Cardholder	Police	-	NEVER	ALWAYS
Contactless	NEVER	Cardholder AND IFD	Cardholder AND IFD	Police AND IFD	-	NEVER	IFD

Object Type	EC Public Asymmetric Key						
Object ID	02						
Object size	512 bit						
Algorithm	ECDSA-SHA-512 over brainpoolP512r1						
Non Repudiation	FALSE						
Condition	PSO Verify	External Auth	PSO Encipher	Gen Key Pair	RFU	Put Data	Get Data
Contact	NEVER	NEVER	NEVER	Police	-	NEVER	Police
Contactless	NEVER	NEVER	NEVER	Police AND IFD	-	NEVER	Police AND IFD

Object Type	Transparent EF (Certificate)						
Object ID	3402						
Object size	1 byte						
Condition	Delete	Terminate	Activate	Deactivate	RFU	Update	Read
Contact	NEVER	NEVER	NEVER	NEVER	-	Police	ALWAYS
Contactless	NEVER	NEVER	NEVER	NEVER	-	Police AND IFD	IFD

ADF QSCD

It is the application DF containing credential objects not related to QSCD (authentication and encryption)

Object Type	ADF						
Object ID	ADF2						
Object AID	"QSCD Application"						
Object size	N/A						
Condition	Delete	Terminate	Activate	Deactivate	DF Creation	EF Creation	SDO Creation
Contact	NEVER	Police	Police	Police	Police	Police	NEVER
Contactless	NEVER	Police AND IFD	Police AND IFD	Police AND IFD	Police AND IFD	Police AND IFD	NEVER

SIGNATURE CREDENTIALS

Signature credential is composed by public/private keypair objects and a certificate object, logically linked.

In order to mitigate consequences of a failed credential renewal process, a couple of signature containers is created, so that the renewal process could be achieved according the following sequence:

1. Key pair generation on the inactive keypair;
2. Resize of the inactive certificate container
3. Certificate import in the inactive certificate container;
4. In case of success, logical deletion of previous keypair and certificate;
5. In case of failure, logical deletion of tentative keypair and certificate.

The fact that containers have to be created in initialization phase enforces key type, algorithm and size of objects in advance. No change on these characteristics is allowed in use phase, even on renewal containers.

Object Type	**EC Private Asymmetric Key**						
Object ID	1F						
Object size	384 bit						
Algorithm	ECDSA-SHA-384 over NIST P-384 (secp384r1)						
Non Repudiation	TRUE						
Usage Counter	Unlimited / Unlimited						
Condition	PSO CDS	Internal Auth	PSO Decipher	Gen Key Pair	RFU	Put Data	Get Data
Contact	Signatory	NEVER	NEVER	Police	-	NEVER	ALWAYS
Contactless	Signatory AND IFD	NEVER	NEVER	Police AND IFD	-	NEVER	IFD

Object Type	**EC Public Asymmetric Key**						
Object ID	1F						
Object size	384 bit						
Algorithm	ECDSA-SHA-384 over NIST P-384 (secp384r1)						
Non Repudiation	TRUE						
Condition	PSO Verify	External Auth	PSO Encipher	Gen Key Pair	RFU	Put Data	Get Data
Contact	NEVER	NEVER	NEVER	Police	-	NEVER	Police
Contactless	NEVER	NEVER	NEVER	Police AND IFD	-	NEVER	Police AND IFD

Object Type	**Transparent EF (Certificate)**						
Object ID	341F						
Object size	Fit to Certificate Size						
Condition	Delete	Terminate	Activate	Deactivate	RFU	Update	Read
Contact	NEVER	NEVER	NEVER	NEVER	-	Police	ALWAYS
Contactless	NEVER	NEVER	NEVER	NEVER	-	Police AND IFD	IFD

Object Type	**EC Private Asymmetric Key**						
Object ID	1E						
Object size	512 bit						
Algorithm	ECDSA-SHA-512 over brainpoolP512r1						
Non Repudiation	TRUE						
Usage Counter	Unlimited / Unlimited						
Condition	PSO CDS	Internal Auth	PSO Decipher	Gen Key Pair	RFU	Put Data	Get Data
Contact	Signatory	NEVER	NEVER	Police	-	NEVER	ALWAYS
Contactless	Signatory AND IFD	NEVER	NEVER	Police AND IFD	-	NEVER	IFD

Object Type	**EC Public Asymmetric Key**						
Object ID	1E						
Object size	512 bit						
Algorithm	ECDSA-SHA-512 over brainpoolP512r1						
Non Repudiation	TRUE						
Condition	PSO Verify	External Auth	PSO Encipher	Gen Key Pair	RFU	Put Data	Get Data
Contact	NEVER	NEVER	NEVER	Police	-	NEVER	Police
Contactless	NEVER	NEVER	NEVER	Police AND IFD	-	NEVER	Police AND IFD

Object Type	**Transparent EF (Certificate)**						
Object ID	341E						
Object size	1 byte						
Condition	Delete	Terminate	Activate	Deactivate	RFU	Update	Read
Contact	NEVER	NEVER	NEVER	NEVER	-	Police	ALWAYS
Contactless	NEVER	NEVER	NEVER	NEVER	-	Police AND IFD	IFD

ISO 7816-15 STRUCTURE

At personalization phase, ISO 7816-15 data are recorded onto the card. These data are not accessed by the card application(s). They are intended for interoperability purposes to inform the IFD about the way to access files and to handle cryptographic objects present in the card including SDO. These data reflect the rules governing all of part of the security objects hosted in the card, thereby enabling the IFD to perform transactions with the card.

5 APPENDIX

This appendix contains logs of real life operations of the card application, which should give a better overview of the commands. The following operations are performed in a test environment of the card application by using transmission protocol T1 with Le always present.

RESET THE CHIP ATR/ATS

Contact Interface. Chip responds with ATR.

3B DB 96 00 80 B1 FE 45 1F 83 00 12 23 3F 53 65 49 44 0F 9000 F1

```
TS = 0x3B          Direct Convention
T0 = 0xDB          Y(1): b1101, K: 11 (historical bytes)
TA(1) = 0x96       Fi=512, Di=32, 16 cycles/ETU (250000 bits/s at 4.00 MHz, 312500 bits/s for fMax=5 MHz)
TC(1) = 0x00       Extra guard time: 0
TD(1) = 0x80       Y(i+1) = b1000, Protocol T=0
----
TD(2) = 0xB1       Y(i+1) = b1011, Protocol T=1
----
TA(3) = 0xFE       IFSC: 254
TB(3) = 0x45       Block Waiting Integer: 4 - Character Waiting Integer: 5
TD(3) = 0x1F       Y(i+1) = b0001, Protocol T=15
----
TA(4) = 0x83       Clock stop: state H - Class accepted by the card: (3G) A 5V B 3V
----
Historical bytes   00 12 23 3F 53 65 49 44 0F 90 00
Category indicator byte: 0x00       (compact TLV data object)
Tag: 1, Len: 2 (country code, ISO 3166-1)
Country code: 23 3F
Tag: 5, Len: 3 (card issuer's data)
Card issuer data: 65 49 44 "eID"
Mandatory status indicator (3 last bytes)
LCS (life card cycle): 15 (Termination state)
SW: 90 00 ()
TCK = 0xF1         correct checksum
```

Contactless Interface. Chip responds with ATS.

3B 8B 80 01 00 12 23 3F 53 65 49 44 0F 9000 A0

```
TS = 0x3B          Direct Convention
T0 = 0x8B          Y(1): b1000, K: 11 (historical bytes)
TD(1) = 0x80       Y(i+1) = b1000, Protocol T=0
----
TD(2) = 0x01       Y(i+1) = b0000, Protocol T=1
----
Historical bytes   00 12 23 3F 53 65 49 44 0F 90 00
Category indicator byte: 0x00       (compact TLV data object)
Tag: 1, Len: 2 (country code, ISO 3166-1)
Country code: 23 3F
Tag: 5, Len: 3 (card issuer's data)
Card issuer data: 65 49 44 "eID"
Mandatory status indicator (3 last bytes)
LCS (life card cycle): 15 (Termination state)
```

SW: 90 00 ()
TCK = 0xA0 correct checksum

APDU MESSAGE COMMAND-RESPONSE PAIR

Command APDU		
Field name	**Length (bytes)**	**Description**
CLA	1	Instruction class - indicates the type of command, e.g. interindustry or proprietary
INS	1	Instruction code - indicates the specific command, e.g. "write data"
P1-P2	2	Instruction parameters for the command, e.g. offset into file at which to write the data
L_c	0, 1 or 3	Encodes the number (N_c) of bytes of command data to follow 0 bytes denotes N_c=0 1 byte with a value from 1 to 255 denotes N_c with the same value 3 bytes, the first of which must be 0, denotes N_c in the range 1 to 65 535 (all three bytes may not be zero)
Command data	N_c	N_c bytes of data
L_e	0, 1, 2 or 3	Encodes the maximum number (N_e) of response bytes expected 0 bytes denotes N_e=0 1 byte in the range 1 to 255 denotes that value of N_e, or 0 denotes N_e=256 2 bytes (if extended L_c was present in the command) in the range 1 to 65 535 denotes N_e of that value, or two zero bytes denotes 65 536 3 bytes (if L_c was not present in the command), the first of which must be 0, denote N_e in the same way as two-byte L_e
Response APDU		
Response data	N_r (at most N_e)	Response data
SW1-SW2 (Response trailer)	2	Command processing status, e.g. 90 00 (hexadecimal) indicates success

PIN1, PIN2 AND PUK OPERATIONS

VERIFY

This command allows

- Verifying a candidate PIN
- Devalidating a PIN

<table>
<tr><th>COMMAND PARAMETER</th><th>MEANING</th></tr>
<tr><td>CLA
INS
P1
P2</td><td>ISO
‘20’
‘00’ (verification) or ‘FF’ (for devalidation)
P2 is encoded as follows:

<table>
<tr><td>b8</td><td>b7</td><td>b6</td><td>B5</td><td>b4</td><td>B3</td><td>b2</td><td>b1</td><td>Meaning</td></tr>
<tr><td>1</td><td>-</td><td>-</td><td>-</td><td>-</td><td>-</td><td>-</td><td>-</td><td>Local reference data (Application)</td></tr>
<tr><td>0</td><td>-</td><td>-</td><td>-</td><td>-</td><td>-</td><td>-</td><td>-</td><td>Global reference data (Card)</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>x</td><td>x</td><td>x</td><td>x</td><td>x</td><td>User authentication DO reference</td></tr>
<tr><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>Forbidden</td></tr>
</table>
</td></tr>
<tr><td>L_c field</td><td>Variable</td></tr>
<tr><td>Data field</td><td>Candidate PIN (P1 = ‘00’ and the command is used to submit a PIN)
Or
Empty (P1 = ‘FF’ or P1 = ‘00’ and the command is used to audit the validation status)</td></tr>
<tr><td>L_e field</td><td>Absent</td></tr>
</table>

RESPONSE PARAMETER	MEANING
Data field	Absent

SW1-SW2	‘6A86’ - P1 ≠ ‘00’ and P1 ≠ ‘FF’ ‘6700’ - PIN length is out of valid boundaries [2*Lmin - 2*Lmax]” ‘6A88’ - Referenced PIN not found ‘6982’ - Security Status not satisfied ‘6983’ - Referenced PIN not successfully verified AND no subsequent tries are allowed (remaining tries counter reached 0) ‘6984’ - Referenced PIN usage counter reached 0 ‘6300’ - No retry limit : User authentication failed (if Pin verification) or PIN is not validated (if Lc=0) ‘63Cx’ - x = remaining tries : User authentication failed (if Pin verification) or PIN is not validated (if Lc=0). ‘9000’ - user authentication successful.

Verify PIN1:

>> 00A40400 10 A0000000770108000700000FE00000100 - Select Main AID
<< 9000 - OK
>> 00200001 0C 31323334FFFFFFFFFFFFFFFF – Verify
<< 9000 – OK

Verify PIN2:

>> 00A4040C 10 51534344204170706C69636174696F6E - Select QSCD AID
<< 9000 - OK
>> 00200085 0C 3132333435FFFFFFFFFFFFFFF - Verify
<< 9000 – OK

Verify PUK:

>> 00A40400 10 A0000000770108000700000FE00000100 - Select Main AID
<< 9000 - OK
>> 00200002 0C 3132333435363738FFFFFFFFFF - Verify
<< 9000 – OK

Block PIN1:

>> 00A40400 10 A0000000770108000700000FE00000100 - Select Main AID
<< 9000 – OK
>> 00200001 0C 31323330FFFFFFFFFFFFFFFF – Verify
<< 63C2 – [Warning] Verify fail, 2 retries left.
>> 00200001 0C 31323330FFFFFFFFFFFFFFFF – Verify
<< 63C1 – [Warning] Verify fail, 1 retries left.
>> 00200001 0C 31323330FFFFFFFFFFFFFFFF – Verify
<< 6983 – [Error] Authentication method blocked.

Block PIN2:

>> 00A4040C 10 51534344204170706C69636174696F6E - Select QSCD AID
>> 00200085 0C 3132333430FFFFFFFFFFFFFFF - Verify
<< 63C2 – [Warning] Verify fail, 2 retries left.
>> 00200085 0C 3132333430FFFFFFFFFFFFFFF - Verify
<< 63C1 – [Warning] Verify fail, 1 retries left.
>> 00200085 0C 3132333430FFFFFFFFFFFFFFF - Verify
<< 6983 – [Error] Authentication method blocked.

Block PUK:

>> 00A40400 10 A0000000770108000700000FE00000100 - Select Main AID
<< 9000 – OK
>> 00200002 0C 3132333435363730FFFFFFFFFF - Verify
<< 63C2 – [Warning] Verify fail, 2 retries left.

>> 00200002 0C 3132333435363730FFFFFFFFFF - Verify
<< 63C1 – [Warning] Verify fail, 1 retries left.
>> 00200002 0C 3132333435363730FFFFFFFFFF - Verify
<< 6983 – [Error] Authentication method blocked.

PIN1 Tries left:

>> 00A40400 10 A0000000770108000700000FE00000100 - Select Main AID
<< 9000 – OK
>> 0020000100 – Verify
<< 63C3 – [Warning] Verify fail, 3 retries left.

PIN2 Tries left:

>> 00A4040C 10 51534344204170706C69636174696F6E - Select QSCD AID
<< 9000 – OK
>> 0020008500 – Verify
<< 63C3 – [Warning] Verify fail, 3 retries left.

PUK Tries left:

>> 00A40400 10 A0000000770108000700000FE00000100 - Select Main AID
<< 9000 – OK
>> 0020000200 - Verify
<< 63C3 – [Warning] Verify fail, 3 retries left.

CHANGE REFERENCE DATA

This command allows changing PIN.

COMMAND PARAMETER	MEANING
CLA INS P1 P2	ISO '24' '00' See §23.5.1
L_c field	Variable
Data field	Current PIN || New PIN
L_e field	Absent

RESPONSE PARAMETER	MEANING
Data field	Absent

SW1-SW2	'6A81' - Command not supported (state selectable) '6A86' - P1 ≠ '00' '6A88' - Referenced PIN not found '63Cx' - Referenced PIN not successfully verified AND subsequent tries are allowed (error counter not null), x = remaining tries allowed '6700' - Lc ≠ '00' – PIN length is out of valid boundaries. '6983' - Referenced PIN not successfully verified AND no subsequent tries are allowed (remaining tries counter reached 0) '6984' - Referenced PIN usage counter reached 0 '6982' - Security status not satisfied

When this command is received

- The application retrieves the current length L (stored within the SDO body length of the selected PIN P)
- The current password is considered to be the first L bytes of the data field.
- Performs the PIN verification by checking P value and the current password.
- Update P with the new reference data
- If needed, update L with the new PIN length. The length of the new password is :

  Lnew = Lc — Lold

Change PIN1:

>> 00A40400 10 A0000000770108000700000FE00000100 - Select Main AID
<< 9000 – OK
>> 00240001 18 31323334FFFFFFFFFFFFFFFFFF1323334FFFFFFFFFFFFFFFFFF 00 – Change PIN1

Change PIN2:

>> 00A4040C 10 51534344204170706C69636174696F6E - Select QSCD AID
<< 9000 – OK
>> 00240085 18 3132333435FFFFFFFFFFFFFFFF3132333435FFFFFFFFFFFFFFFF 00 - Change PIN2
<< 9000 – OK

Change PUK:

>> 00A40400 10 A0000000770108000700000FE000001 00 - Select Main AID
<< 9000 – OK
>> 00240002 18 3132333435363738FFFFFFFFFF3132333435363738FFFFFFFFFF 00 – Change PUK
<< 9000 – OK

RESET RETRY COUNTER

This command allows:

- unblocking the PIN;
- devalidating the PIN;
- unblocking and changing the PIN

COMMAND PARAMETER	MEANING
CLA	ISO
INS	'2C'
P1	'02' (to unblock and change PIN) or '03' (to unblock only) or 'FF' (to devalidate PIN)
P2	b8 b7 b6 B5 b4 B3 b2 b1 Meaning 1 - - - - - - - Local reference data (Application) 0 - - - - - - - Global reference data (Card) - - - x x x x x User authentication DO reference 0 0 0 0 0 0 0 0 Forbidden
L_c field	Variable
Data field	Absent (P1 = '03' or 'FF') or new reference data (P1 = '02')
L_e field	Absent

RESPONSE PARAMETER	MEANING
Data field	Absent

SW1-SW2	'6A81' - Command not supported (state selectable) '6A86' - P1 ≠ '02', P1 ≠ '03' and P1 ≠ 'FF' '6A88' - Referenced PIN not found '6700' - The length of the new reference data doesn't match with the length of the PIN reference container length (P1 = '02') or Lc ≠ '00' (P1 = '03' or 'FF'). '6984' - Reference data not usable – Usage counter of referenced PIN raised 0. '6982' - Security status not satisfied

Reset PIN1:

>> 00A40400 10 A0000000770108000700000FE00000100 - Select Main AID
<< 9000 – OK
>> 00200002 0C 3132333435363738FFFFFFFFFF – Verify PUK
<< 9000 – OK
>> 002C0201 0C 31323334FFFFFFFFFFFFFFFFFF – Reset PIN1
<< 9000 – OK

Reset PIN2:

>> 00A40400 10 A0000000770108000700000FE00000100 - Select Main AID
<< 9000 – OK
>> 00200002 0C 3132333435363738FFFFFFFFFF – Verify PUK
<< 9000 – OK
>> 00A4040C 10 51534344204170706C69636174696F6E - Select QSCD AID
<< 9000 – OK
>> 002C0085 0C 3132333435FFFFFFFFFFFFFFFF 00 - Reset
<< 9000 – OK

READ PERSONAL DATA TRANSPARENT FILES

DF ID 5000_{hex} (Personal Data transparent files)

SELECT

COMMAND PARAMETER	MEANING
CLA INS P1 P2	ISO 'A4' **See Table 1** **See Table 2**
L_c field	Absent or length of command data field '02' – to pass a FID 'xx' – to pass DF name or relative path (shall be modulo 2)
Data field	FID, DF name or relative path
L_e field	Variable

Table 1: Selection, file and life cycle commands P1 possible values

B8	B7	B6	B5	B4	B3	B2	B1	MEANING	COMMAND DATA FIELD
0	**0**	**0**	**0**	**0**	**0**	X	x	**Selection by file identifier**	
						0	0	- Select MF	MF identifier
						0	1	- Select child DF	DF identifier
						1	0	- Select EF under the current DF	EF identifier
						1	1	- Select parent DF of the current DF. Upper limit = ADF or MF	None
				0	**1**	X	x	**Selection by name**	
						0	0	- Select by DF name (ADF or MF)	AID
				1	**0**	X	x	**Selection by path**	
						0	1	- Select from the current DF	Path without the current DF identifier

Table 2: Selection, file and life cycle commands P2 possible values

B8	B7	B6	B5	B4	B3	B2	B1	MEANING
0	0	0	0	-	-	x	x	**File occurrence**
				-	-	0	0	- First or only occurrence
				x	X	-	-	**File control Parameters**
				0	0	-	-	Not supported
				0	1	-	-	- Return FCP template, mandatory use of FCP tag and length
				1	1	-	-	- No data in response field

RESPONSE PARAMETER	MEANING
Data field	Absent or FCP

Template	Length	Value field			Presence		
62	L62	**Tag**	**Length**	**content**	**ADF**	**DF**	**EF**
		'80'	'02'	File length.	**-**	**-**	**M**
		'82'	'01'	File descriptor byte	**M**	**M**	**M**
		'83'	'02'	File identifier	**M**	**M**	**M**
		'84'	'05' to '10'	DF name (AID)	**M**	**-**	**-**
		'88'	'00' or '01'	Short file identifier	**-**	**-**	**O**
		'8A'	'01'	Life cycle status byte	**M**	**M**	**M**
		'A1'	Var.	Security attributes in proprietary format	**M**	**M**	**M**
		'A5'	Var.	Issuer discretionary data in BER-TLV format	**O**	**O**	**O**
		'85'	Var.	Issuer discretionary data in NON BER-TLV format	**O**	**O**	**O**

CLASSICAL READ BINARY

<table>
<tr><th>COMMAND PARAMETER</th><th>MEANING</th></tr>
<tr><td>CLA
INS
P1-P2</td><td>ISO
'B0'
<table>
<tr><th colspan="7">P1</th><th colspan="8">P2</th></tr>
<tr><th>B8</th><th>B7</th><th>B6</th><th>B5</th><th>B4</th><th>B3</th><th>B2</th><th>B1</th><th>B8</th><th>B7</th><th>B6</th><th>B5</th><th>B4</th><th>B3</th><th>B2</th><th>B1</th></tr>
<tr><td>0</td><td colspan="15">Offset in the currently selected file over 15 bits
'00' <= Offset <= '7FFF'</td></tr>
<tr><td>1</td><td>0</td><td>0</td><td colspan="4">Short File Identifier
1 <= SFI <= 30</td><td colspan="8">Offset in the file over 8 bits</td></tr>
</table></td></tr>
<tr><td>Le field</td><td>Number of bytes to read</td></tr>
</table>

RESPONSE PARAMETER	MEANING
Data field	Data read

SW1-SW2	'6282' - End of file reached before reading 'Ne' bytes '6981' - Command incompatible with file structure '6982' - Security status not satisfied '6985'- Current DF is "deactivated" or "terminated" / MF was not created '6A80'- Wrong data '6A82' - File not found (no current EF) '6B00' - Wrong parameters P1-P2 : Offset + length is beyond the end of file

Select DF ID 5000_{hex} (Personal Data transparent files) known issues

Selecting DF 5000 twice:

>> 00A40400 10 A000000077010800070000FE00000100 - Select Main AID
<< 9000 – OK
>> 00A4010C025000 – Select DF 5000
<< 9000 – OK
>> 00A4010C025000 – Select DF 5000
<< 6A82 – [Error] File not found

Read contents:

>> 00A40400 10 A0000000770108000700000FE00000100 - Select Main AID
<< 9000 – OK
>> 00A4010C 02 5000 – Select DF 5000
<< 9000 – OK
>> 00A4010C 02 5001 – Select Transparent EF 5001
<< 9000 – OK
>> 00B00000 00 – Read Binary
<< 4A C3 95 45 4F 52 47 9000 – OK (JÕEORG)
>> 00A4010C025002 – Select Transparent EF 5002
<< 9000 – OK
>> 00B00000 00 – Read Binary
<< 4A 41 41 4B 2D 4B 52 49 53 54 4A 41 4E 9000 – OK (JAAK-KRISTJAN)
>> 00A4010C025003 – Select Transparent EF 5003
<< 9000 – OK
>> 00B00000 00 – Read Binary
<< 4D 9000 – OK (M)
>> 00A4010C025004 – Select Transparent EF 5004
<< 9000 – OK
>> 00B00000 00 – Read Binary
<< 45 53 54 9000 – OK (EST)
>> 00A4010C025005 – Select Transparent EF 5005
<< 9000 – OK
>> 00B00000 00 – Read Binary
<< 30 38 20 30 31 20 31 39 38 30 20 45 53 54 9000 – OK (08 01 1980 EST)
>> 00A4010C025006 – Select Transparent EF 5006
<< 9000 – OK
>> 00B00000 00 – Read Binary
<< 33 38 30 30 31 30 38 35 37 31 38 9000 – OK (38001085718)
>> 00A4010C025007 – Select Transparent EF 5007
<< 9000 – OK
>> 00B00000 00 – Read Binary
<< 41 53 39 39 39 31 30 37 32 9000 – OK (AS9991072)
>> 00A4010C025008 – Select Transparent EF 5008
<< 9000 – OK
>> 00B00000 00 – Read Binary
<< 32 33 20 31 30 20 32 30 32 33 9000 – OK (23 10 2023)
>> 00A4010C025009 – Select Transparent EF 5009F
<< 9000 – OK
>> 00B00000 00 – Read Binary
<< 32 33 20 31 30 20 32 30 31 38 9000 – OK (23 10 2018)
>> 00A4010C02500A – Select Transparent EF 500A
<< 9000 – OK
>> 00B00000 00 – Read Binary
<< 00 9000 – OK (NUL)

>> 00A4010C02500B – Select Transparent EF 500B
<< 9000 – OK
>> 00B00000 00 – Read Binary
<< 00 9000 – OK (NUL) 9000
>> 00A4010C02500C – Select Transparent EF 500C
<< 9000 – OK
>> 00B00000 00 – Read Binary
<< 00 9000 – OK (NUL)
>> 00A4010C02500D – Select Transparent EF 500D
<< 9000 – OK
>> 00B00000 00 – Read Binary
<< 00 9000 – OK (NUL)
>> 00A4010C02500E – Select Transparent EF 500E
<< 9000 – OK
>> 00B00000 00 – Read Binary
<< 00 9000 – OK (NUL)
>> 00A4010C 02 500F – Select Transparent EF 500F
<< 9000 – OK
>> 00B00000 00 – Read Binary
<< 00 9000 – OK (NUL)

Known responses with some driver versions:

>> 00A40400 10 A0000000770108000700000FE00000100 - Select Main AID
<< 9000 – OK
>> 00A4010C025000 – Select DF 5000
<< 9000 – OK

>> 00A4010C 02 5001 – Select Transparent EF 5001
<< 9000 – OK
>> 00B00000 00 – Read Binary
<< 6B 00 – [Error] Wrong parameter(s) P1-P2 (Issue may be caused duo to removing 00 from command)

>> 00B00000 01 – Read Binary. Response length 1 byte.
<< 4B 9000 – OK (J)
>> 00B00000 02 – Read Binary. Response length 2 bytes.
<< 4B C3 9000 – OK (J?)
>> 00B00000 03 – Read Binary. Response length 3 bytes.
<< 4B C3 95 9000 – OK (JÕ)
>> 00B00000 04 – Read Binary. Response length 4 bytes.
<< 4B C3 95 45 9000 – OK (JÕE)
>> 00B00000 05 – Read Binary. Response length 5 bytes.
<< 4B C3 95 45 4F 9000 – OK (JÕEO)
>> 00B00000 06 – Read Binary. Response length 6 bytes.
<< 4B C3 95 45 4F 52 9000 – OK (JÕEOR)

>> 00B00000 07 – Read Binary. Response length 7 bytes.
<< 4B C3 95 45 4F 52 47 9000 – OK (JÕEORG)

>> 00B00000 08 – Read Binary. Response length 8 bytes.
<< 4B C3 95 45 4F 52 47 6282 – End of file/record reached before reading Le bytes (JÕEORG)
…
>> 00B00000 FF – Read Binary. Response length 255 bytes.
<< 4B C3 95 45 4F 52 47 6282 – End of file/record reached before reading Le bytes (JÕEORG)

The answer with the latest drivers:

>> 00B00000 08 – Read Binary. Response length 8 bytes.
<< 4B C3 95 45 4F 52 47 9000 – OK bytes (JÕEORG)
…
>> 00B00000 FF – Read Binary. Response length 255 bytes.
<< 4B C3 95 45 4F 52 47 9000 – OK (JÕEORG)

ID CARD PERSONAL DATA FILE DATA EXAMPLE:

DF Personal Data elements	Test data (HEX)	Values	Character encoding	Data format
PD1 (Surname)	4A C3 95 45 4F 52 47	JÕEORG	ASCII/UTF-8	Xn
PD2 (First Name)	4A 41 41 4B 2D 4B 52 49 53 54 4A 41 4E	JAAK-KRISTJAN	ASCII/UTF-8	Xn
PD3 (Sex)	4D	M	ASCII/UTF-8	X
PD4 (Citizenship ISO3166 alpha-3)	45 53 54	EST	ASCII/UTF-8	XXX
PD5 (Date and place of birth)	30 38 20 30 31 20 31 39 38 30 20 45 53 54	08 01 1980 EST	ASCII/UTF-8	DD MM YYYY XXX
PD6 (Personal Identification Code)	33 38 30 30 31 30 38 35 37 31 38	38001085718	ASCII/UTF-8	99999999999
PD7 (Document Number)	41 53 30 30 31 30 33 39 32	AS0010392	ASCII/UTF-8	XX9999999
PD8 (Expiry Date)	31 33 20 30 38 20 32 30 32 33	13 08 2023	ASCII/UTF-8	DD MM YYYY
PD9 (Date of Issuance)	31 33 20 30 38 20 32 30 31 38	13 08 2018	ASCII/UTF-8	DD MM YYYY
PD10 (Type of residence permit)	00		ASCII/UTF-8	
PD11 (Notes Line 1)	00		ASCII/UTF-8	
PD12 (Notes Line 2)	00		ASCII/UTF-8	
PD13 (Notes Line 3)	00		ASCII/UTF-8	
PD14 (Notes Line 4)	00		ASCII/UTF-8	
PD15 (Notes Line 5)	00		ASCII/UTF-8	

Digital Identity Card (eResident) PERSONAL DATA file data example:

DF Personal Data elements	Test data (HEX)	Values	Character encoding	Data format
PD1 (Surname)	4A C3 95 45 4F 52 47	JÕEORG	ASCII/UTF-8	Xn
PD2 (First Name)	4A 41 41 4B 2D 4B 52 49 53 54 4A 41 4E	JAAK-KRISTJAN	ASCII/UTF-8	Xn
PD3 (Sex)	00		ASCII/UTF-8	
PD4 (Citizenship ISO3166 alpha-3)	00		ASCII/UTF-8	
PD5 (Date and place of birth)	00		ASCII/UTF-8	
PD6 (Personal Identification Code)	33 38 30 30 31 30 38 35 37 31 38	38001085718	ASCII/UTF-8	99999999999
PD7 (Document Number)	4E 53 30 30 30 30 30 30 39	NS0000009	ASCII/UTF-8	XX9999999
PD8 (Expiry Date)	31 33 20 30 38 20 32 30 32 33	13 08 2023	ASCII/UTF-8	DD MM YYYY
PD9 (Date of Issuance)	31 33 20 30 38 20 32 30 31 38	13 08 2018	ASCII/UTF-8	DD MM YYYY
PD10 (Type of residence permit)	00		ASCII/UTF-8	
PD11 (Notes Line 1)	00		ASCII/UTF-8	
PD12 (Notes Line 2)	00		ASCII/UTF-8	
PD13 (Notes Line 3)	00		ASCII/UTF-8	
PD14 (Notes Line 4)	00		ASCII/UTF-8	
PD15 (Notes Line 5)	00		ASCII/UTF-8	

Residence Permit Card PERSONAL DATA file data example:

DF Personal Data elements	Test data (HEX)	Values	Character encoding	Data format
PD1 (Surname)	4A C3 95 45 4F 52 47	JÕEORG	ASCII/UTF-8	Xn
PD2 (First Name)	4A 41 41 4B 2D 4B 52 49 53 54 4A 41 4E	JAAK-KRISTJAN	ASCII/UTF-8	Xn
PD3 (Sex)	4D	M	ASCII/UTF-8	X
PD4 (Citizenship ISO3166 alpha-3)	55 4B 52	UKR	ASCII/UTF-8	XXX
PD5 (Date and place of birth)	30 38 20 30 31 20 31 39 38 30 20 55 4B 52	08 01 1980 UKR	ASCII/UTF-8	DD MM YYYY XXX
PD6 (Personal Identification Code)	33 38 30 30 31 30 38 35 37 31 38	38001085718	ASCII/UTF-8	99999999999
PD7 (Document Number)	50 53 30 30 30 30 30 33 38	PS0000038	ASCII/UTF-8	XX9999999
PD8 (Expiry Date)	31 33 20 30 38 20 32 30 32 33	13 08 2023	ASCII/UTF-8	DD MM YYYY
PD9 (Date and place of Issuance)	31 33 20 30 38 20 32 30 31 38 20 50 50 41	08 2018 PPA	ASCII/UTF-8	DD MM YYYY XXX
PD10 (Type of residence permit)	50 49 4B 41 41 4A 41 4C 49 4E 45 20 45 4C 41 4E 4B	PIKAAJALINE ELANK	ASCII/UTF-8	Xn
PD11 (Notes Line 1)	00		ASCII/UTF-8	
PD12 (Notes Line 2)	00		ASCII/UTF-8	
PD13 (Notes Line 3)	00		ASCII/UTF-8	
PD14 (Notes Line 4)	00		ASCII/UTF-8	
PD15 (Notes Line 5)	00		ASCII/UTF-8	

Diplomatic Identity Card PERSONAL DATA file data example:

DF Personal Data elements	Test data (HEX)	Values	Character encoding	Data format
PD1 (Surname)	54 48 4F 4D 50 53 4F 4E	THOMPSON	ASCII/UTF-8	Xn
PD2 (First Name)	53 54 45 56 45 4E 20 50 41 55 4C	STEVEN PAUL	ASCII/UTF-8	Xn
PD3 (Sex)	00		ASCII/UTF-8	
PD4 (Citizenship ISO3166 alpha-3)	00		ASCII/UTF-8	
PD5 (Date of birth)	31 31 20 30 38 20 31 39 37 35	11 08 1975	ASCII/UTF-8	DD MM YYYY
PD6 (Personal Identification Code)	33 37 35 30 38 31 31 30 33 38 37	37508110387	ASCII/UTF-8	99999999999
PD7 (Document Number)	41 31 39 30 30 30 31 39 35	A19000195	ASCII/UTF-8	X99999999
PD8 (Expiry Date)	31 33 20 30 38 20 32 30 32 33	13 08 2023	ASCII/UTF-8	DD MM YYYY
PD9 (Date and place of Issuance)	32 38 20 30 38 20 32 30 31 38	28 08 2018	ASCII/UTF-8	DD MM YYYY
PD10 (Type of residence permit)	00		ASCII/UTF-8	
PD11 (Notes Line 1)	00		ASCII/UTF-8	
PD12 (Notes Line 2)	00		ASCII/UTF-8	
PD13 (Notes Line 3)	00		ASCII/UTF-8	
PD14 (Notes Line 4)	00		ASCII/UTF-8	
PD15 (Notes Line 5)	00		ASCII/UTF-8	

READ CERTIFICATE FILES

READ AUTHENTICATION CERTIFICATE USING MULTIPLE C-APDUS:

>> 00A40400 10 A000000077010800070000FE00000100 - Select Main AID
<< 9000 – OK
>> 00A4000C 00 – Select DF
<< 9000 – OK
>> 00A4010C 02 ADF1 – Select ADF (AWP Application)
<< 9000 – OK
>> 00A4010C 02 3401 – Select Transparent EF (Certificate)
<< 9000 – OK
>> 00B00000 00 – Read Binary (1 part)
<< 30 82 04 0E 30 82 03 6F A0 03 02 01 02 02 10 34 8A 5C 43 AB 6B 21 D6 5B 88 E7 8D 6F CA 6A 8D 30 0A 06 08 2A 86 48 CE 3D 04 03 04 30 60 31 0B 30 09 06 03 55 04 06 13 02 45 45 31 1B 30 19 06 03 55 04 0A 0C 12 53 4B 20 49 44 20 53 6F 6C 75 74 69 6F 6E 73 20 41 53 31 17 30 15 06 03 55 04 61 0C 0E 4E 54 52 45 45 2D 31 30 37 34 37 30 31 33 31 1B 30 19 06 03 55 04 03 0C 12 54 45 53 54 20 6F 66 20 45 53 54 45 49 44 32 30 31 38 30 1E 17 0D 31 38 30 38 33 31 30 37 30 30 32 39 5A 17 0D 32 33 30 38 32 37 32 31 35 39 35 39 5A 30 7D 31 0B 30 09 06 03 55 04 06 13 02 45 45 31 29 30 27 06 03 55 04 03 0C 20 54 48 4F 4D 50 53 4F 4E 2C 53 54 45 56 45 4E 20 50 41 55 4C 2C 33 37 35 30 38 31 31 30 33 38 37 9000 - OK

>> 00B01000 00 – Read Binary (2 part)
<< 55 04 2A 0C 0B 53 54 45 56 45 4E 20 50 41 55 4C 31 1A 30 18 06 03 55 04 05 13 11 50 4E 4F 45 45 2D 33 37 35 30 38 31 31 30 33 38 37 30 76 30 10 06 07 2A 86 48 CE 3D 02 01 06 05 2B 81 04 00 22 03 62 00 04 7C 27 9A 30 D4 C5 1F 19 39 6D CE A5 57 4A 0A B4 19 52 F4 5B 93 15 44 76 A5 3D D2 74 E0 90 A9 45 6A BB D5 38 AA 5E 0D B1 CF 48 DE 27 5C CC EE 86 3A DC A7 70 C3 F1 31 FA 6C 3E 00 1C 5C F2 73 75 78 CD CB 00 05 ED 4F 09 5D CF 81 E5 16 86 E8 52 14 3B C7 F3 7C A5 12 92 20 2B 58 7E CA 4B F8 25 A3 82 01 CF 30 82 01 CB 30 09 06 03 55 1D 13 04 02 30 00 30 0E 06 03 55 1D 0F 01 01 FF 04 04 03 02 03 88 30 47 06 03 55 1D 20 04 40 30 3E 30 32 06 0B 2B 06 01 04 01 83 91 7F 01 02 01 30 23 30 21 06 08 9000 - OK
>> 00B02000 00 – Read Binary (3 part)
<< 65 65 2F 43 50 53 30 08 06 06 04 00 8F 7A 01 02 30 1F 06 03 55 1D 11 04 18 30 16 81 14 33 37 35 30 38 31 31 30 33 38 37 40 65 65 73 74 69 2E 65 65 30 1D 06 03 55 1D 0E 04 16 04 14 C0 74 5B 4B FE E3 C5 53 86 98 A0 04 4C 8D 8D EE 3F 38 1D ED 30 61 06 08 2B 06 01 05 05 07 01 03 04 55 30 53 30 51 06 06 04 00 8E 46 01 05 30 47 30 45 16 3F 68 74 74 70 73 3A 2F 2F 73 6B 2E 65 65 2F 65 6E 2F 72 65 70 6F 73 69 74 6F 72 79 2F 63 6F 6E 64 69 74 69 6F 6E 73 2D 66 6F 72 2D 75 73 65 2D 6F 66 2D 63 65 72 74 69 66 69 63 61 74 65 73 2F 13 02 45 4E 30 20 06 03 55 1D 25 01 01 FF 04 16 30 14 06 08 2B 06 01 05 05 07 03 02 06 08 2B 06 01 05 05 07 03 04 30 1F 06 03 55 1D 23 04 18 30 16 80 14 C0 84 99 29 C4 9000 - OK
>> 00B03000 00 – Read Binary (4 part)
<< 01 01 04 73 30 71 30 2C 06 08 2B 06 01 05 05 07 30 01 86 20 68 74 74 70 3A 2F 2F 61 69 61 2E 64 65 6D 6F 2E 73 6B 2E 65 65 2F 65 73 74 65 69 64 32 30 31 38 30 41 06 08 2B 06 01 05 05 07 30 02 86 35 68 74 74 70 73 3A 2F 2F 73 6B 2E 65 65 2F 75 70 6C 6F 61 64 2F 66 69 6C 65 73 2F 54 45 53 54 5F 6F 66 5F 45 53 54 45 49 44 32 30 31 38 2E 64 65 72 2E 63 72 74 30 0A 06 08 2A 86 48 CE 3D 04 03 04 03 81 8C 00 30 81 88 02 42 00 AC E7 11 5D 44 61 85 BB B5 9C 55 79 68 28 99 32 BF D4 C9 75 60 98 26 4E E6 EE 0A 16 50 C9 99 60 50 62 0D 72 C8 09 2D 17 F4 E8 BE B8 0B D8 F5 98 1F F5 3C 74 ED CA 29 81 0B 87 C5 D0 BB C4 DB 35 0B 02 42 01 28 7D 17 B0 72 4E C9 47 7C 6E 63 14 9E 44 68 CE E0 78 CF B4 63 35 9000 - OK
>> 00B04000 00 – Read Binary (5 part)
<< 50 FF E8 DC F0 E5 5E 17 15 42 A9 B8 C0 51 A4 6A 93 70 9000 - OK
>> 00B05000 00 – Read Binary (6 part)
>> 6B00 – Error (Wrong parameter(s) P1-P2)

READ SIGNATURE CERTIFICATE USING MULTIPLE C-APDUS:

>> 00A4040010A000000077010800070000FE00000100 - Select Main AID
<< 9000 - OK
>> 00A400 0C – Select DF
<< 9000 - OK
>> 00A4020C 02 ADF2 – Select ADF QSCD
<< 9000 - OK
>> 00A4020C 02 341F - Select Transparent EF (Certificate)
<< 9000 - OK
>> 00B0000000 - Read Binary (1.1 part)
<< 30 82 03 EB 30 82 03 4D A0 03 02 01 02 02 10 51 03 B2 48 F2 38 87 C6 5B CF 27 24 63 32 60 6D 30 0A 06 08 2A 86 48 CE 3D 04 03 04 30 60 31 0B 30 09 06 03 55 04 06 13 02 45 45 31 1B 30 19 06 03 55 04 0A 0C 12 53 4B 20 49 44 20 53 6F 6C 75 74 69 6F 6E 73 20 41 53 31 17 30 15 06 03 55 04 61 0C 0E 4E 54 52 45 45 2D 31 30 37 34 37 30 31 33 31 1B 30 19 06 03 55 04 03 0C 12 54 45 53 54 20 6F 66 20 45 53 54 45 49 44 32 30

31 38 30 1E 17 0D 31 38 31 30 32 33 31 33 35 30 32 38 5A 17 0D 32 33 31 30 32 32 32 31 35 39 35 39 5A 30 7F 31 0B 30 09 06 03 55 04 06 13 02 45 45 31 2A 30 28 06 03 55 04 03 0C 21 4A C3 95 45 4F 52 47 2C 4A 41 41 4B 2D 4B 52 49 53 54 4A 41 4E 2C 33 38 30 30 31 30 38 35 37 31 9000 - OK

>> 00B000E719 - Read Binary (1.2 part)

<< 38 31 10 30 0E 06 03 55 04 04 0C 07 4A C3 95 45 4F 52 47 31 16 30 14 06 03 9000 – OK

>> 00B0010000 - Read Binary (2.1 part)

<< 55 04 2A 0C 0D 4A 41 41 4B 2D 4B 52 49 53 54 4A 41 4E 31 1A 30 18 06 03 55 04 05 13 11 50 4E 4F 45 45 2D 33 38 30 30 31 30 38 35 37 31 38 30 76 30 10 06 07 2A 86 48 CE 3D 02 01 06 05 2B 81 04 00 22 03 62 00 04 1F A4 C0 5E 8A 2F 80 0C 58 8C 51 10 49 74 33 4A 3C 20 E2 78 98 DE 30 B2 D5 2A 12 DF 2E 82 94 23 C8 11 91 97 EC DE F6 72 CC B7 EB DF CD F6 D0 26 EE 25 37 0C 3F 66 35 82 FF 76 1A 05 20 54 BE 91 CE 50 D7 3D 50 71 AB AB B3 82 C9 28 55 61 3A F1 DB B6 06 B8 6D BF F7 C7 BF 65 1B 15 2B CB 8B CA A3 82 01 AB 30 82 01 A7 30 09 06 03 55 1D 13 04 02 30 00 30 0E 06 03 55 1D 0F 01 01 FF 04 04 03 02 06 40 30 48 06 03 55 1D 20 04 41 30 3F 30 32 06 0B 2B 06 01 04 01 83 91 21 01 02 01 30 23 30 21 9000 - OK

>> 00B001E719 - Read Binary (2.2 part)

<< 06 08 2B 06 01 05 05 07 02 01 16 15 68 74 74 70 73 3A 2F 2F 77 77 77 2E 73 9000 - OK

>> 00B0020000 - Read Binary (3.1 part)

<< 6B 2E 65 65 2F 43 50 53 30 09 06 07 04 00 8B EC 40 01 02 30 1D 06 03 55 1D 0E 04 16 04 14 79 79 6B 20 FC FF 6F 16 67 93 E0 0E 79 02 B1 A4 81 4B 2C 12 30 81 8A 06 08 2B 06 01 05 05 07 01 03 04 7E 30 7C 30 08 06 06 04 00 8E 46 01 01 30 08 06 06 04 00 8E 46 01 04 30 13 06 06 04 00 8E 46 01 06 30 09 06 07 04 00 8E 46 01 06 01 30 51 06 06 04 00 8E 46 01 05 30 47 30 45 16 3F 68 74 74 70 73 3A 2F 2F 73 6B 2E 65 65 2F 65 6E 2F 72 65 70 6F 73 69 74 6F 72 79 2F 63 6F 6E 64 69 74 69 6F 6E 73 2D 66 6F 72 2D 75 73 65 2D 6F 66 2D 63 65 72 74 69 66 69 63 61 74 65 73 2F 13 02 45 4E 30 1F 06 03 55 1D 23 04 18 30 16 80 14 C0 84 99 29 C4 4E 9F 3B 02 34 F6 99 E1 0A 56 00 08 29 3E 7B 30 73 06 08 2B 06 01 9000 - OK

>> 00B002E719 - Read Binary (3.2 part)

<< 05 05 07 01 01 04 67 30 65 30 2C 06 08 2B 06 01 05 05 07 30 01 86 20 68 74 9000 – OK

>> 00B0030000 - Read Binary (4.1 part)

<< 74 70 3A 2F 2F 61 69 61 2E 64 65 6D 6F 2E 73 6B 2E 65 65 2F 65 73 74 65 69 64 32 30 31 38 30 35 06 08 2B 06 01 05 05 07 30 02 86 29 68 74 74 70 3A 2F 2F 63 2E 73 6B 2E 65 65 2F 54 65 73 74 5F 6F 66 5F 45 53 54 45 49 44 32 30 31 38 2E 64 65 72 2E 63 72 74 30 0A 06 08 2A 86 48 CE 3D 04 03 04 03 81 8B 00 30 81 87 02 41 3D C0 EB E3 51 9F EA DF 33 42 59 62 EE CF E7 1E C9 CF 84 6E ED 36 10 E4 F0 AA 0A 37 BF 00 FD 07 00 76 67 28 FA 90 0F AC 0F D4 41 FA B4 FD 67 F0 EF BC 1C 5D B3 4B 53 75 0A 7A 5F B6 2A 5F 0B 80 F5 02 42 01 DA B9 D3 55 98 F2 A0 70 7C A2 A4 09 C3 4C D0 FD 1F 76 16 59 09 BF EA 84 BE EB E3 2F 04 71 63 69 A8 FB 00 6A 2A 15 4E 0C BB A8 E1 AA F9 45 9D 9F 3F 0E F9 6B 2C F0 48 F3 0E 9000 - OK

>> 00B003E719 - Read Binary (4.2 part)

<< 3E 6E 34 C8 FF 6D 57 3F 6282 (End of file/record reached before reading Le bytes)

>> 00B0040000 - Read Binary (5 part)

<< 6B00 (Wrong parameter(s) P1-P2.)

INTERNAL AUTHENTICATE FOR CLIENT/SERVER AUTHENTICATION

This command is used for the client/server authentication.

COMMAND PARAMETER	MEANING
CLA INS P1 P2	ISO '88' '00' '00'
L_c field	Variable
Data field	**Data** **For RSA scheme** The length of data shall not exceed the maximum threshold set during personalisation of [Applet]. The default value is set to 40% of the authentication key modulus : • '33' for 1024 bits • '4C' for 1536 bits • '66' for 2048 bits **For ECDSA scheme** The length of data shall not exceed the length in bits of the order of the generator
L_e field	Variable

RESPONSE PARAMETER	MEANING
Data field	Authentication cryptogram

SW1-SW2	'6700' Wrong length; no further indication. '6982' Security status not satisfied '6984' SDO not usable '6985' SE content doesn't allow processing the command. '6A81' Command not supported (state selectable) '6A86' P1P2 ≠ '0000' '6A88' Reference data needed for internal authenticate not found

```
>> 00A40400 10 A000000077010800070000FE00000100 – Select Main AID
<< 9000 - OK
>> 00200001 0C 31323334FFFFFFFFFFFFFFFF – Verify PIN1
<< 9000 - OK
>> 00A4040C 0D E828BD080FF2504F5420415750 – Select AWP AID
<< 9000 - OK
>> 002241A4 09 8004FF200800840181 – Set ENV
<< 9000 - OK
>> 00880000 07 4AC395454F5247 00 – Perform Security Operation (INTERNAL AUTHENTICATE)
JÕEORG

<<
EC495AAA2E2EDAC61365BCB6DE99561F5033F2A3CFD1EE8F08B0E1572FC487BBB1FEE4257BA7C662BF9FEDC
E47DAADD01013A363D1EA7962AD139E565702FBB796BBC64125D56AB3678052FA72CAED92626D53BD750CAF
FE80955B1ADE43A478 9000 - OK
```

COMPUTE DIGITAL SIGNATURE

This command performs the digital signature creation.

COMMAND PARAMETER	MEANING
CLA INS P1 P2	ISO '2A' '9E' '9A'
L_c field	**For off card hashing :** Data field length (in case of hash off card) : 0x14 for SHA-1 0x1C for SHA-224 0x20 for SHA-256 0x30 for SHA-384 0x40 for SHA-512 **For last round hashing and on card hashing :** empty
Data field	Hash of data Or Absent
L_e field	Variable

RESPONSE PARAMETER	MEANING
Data field	Digital signature

SW1-SW2	'6984' - SDO not usable '6985' - No hash available '6A81' - Command not supported (state selectable) '6A88' - Current SE problem '6A86' - Incorrect P1-P2 '6982' - Security status not satisfied

```
>> 00A40400 10 A0000000770108000700000FE00000100 – Select Main AID
<< 9000
>> 00A4040C 10 515343442041707 06C69636174696F6E – Select QSCD AID
<< 9000 – OK
>> 00200085 0C 3132333435FFFFFFFFFFFFFF – Verify PIN2
<< 9000 – OK
>> 00A4040C 10 515343442041707 06C69636174696F6E - Select QSCD AID
<< 9000 – OK
>> 002241B6 09 8004FF15080084019F – Set ENV
<< 9000 – OK
SHA-384("JÕEORG"):
A053E7B6A279D215B67407E392ED62684B6D65965B7B2191AEA33638607BDE2B30B6015D843032D1824BC03
888C89762
>> 002A9E9A 30
A053E7B6A279D215B67407E392ED62684B6D65965B7B2191AEA33638607BDE2B30B6015D843032D1824BC03
888C89762 00 – Perform Security Operation (COMPUTE DIGITAL SIGNATURE)
<<
7F864FCAFCA6E4D72EE713483991E4A23C8A6D1680D2D049D645F9616606EC2CBE1C8D28A65FBD5530AAAA5
13079A03E4ABAC19FE1E48A9296B095761EA3F3FF712DE59719B27C82ED44F8D14B9252A30D8CE0B8D5EF19
E4A7E61A5A587A75AE 9000 – OK
```