Belgian Electronic Identity Card content

Table of content

1. Scope

This standard describes the specifications of the Belgian Electronic Identity Card files and objects. Only the ***DF(BelPIC)*** and the ***DF(ID)*** are covered in this document.

1.1. Terms and definitions

For the purposes of this document, the following definitions apply:

authentication object directory file optional elementary file containing information about authentication objects known to the PKCS#15 application

binary coded decimal Number representation where a number is expressed as a sequence of decimal digits and then each decimal digit is encoded as a four bit binary number.

Example – Decimal 92 would be encoded as the eight bit sequence 1001 0010.

cardholder person for whom the card was issued

card issuer organization or entity that issues smart cards and card applications

certificate directory file optional elementary file containing information about certificate known to the PKCS#15 application

data object directory file optional elementary file containing information about data objects known to the PKCS#15 application

dedicated file file containing file control information, and, optionally, memory available for allocation, and which may be the parent of elementary files and/or other dedicated files

directory (DIR) file optional elementary file containing a list of applications supported by the card and optional related data elements

elementary file set of data units or records that share the same file identifier, and which cannot be a parent of another file

file identifier 2-byte binary value used to address a file on a smart card

master file mandatory unique dedicated file representing the root of the structure

NOTE – The MF typically has the file identifier 3F00

object directory file elementary file containing information about other directory files in the PKCS #15 application

path concatenation of file identifiers without delimitation

NOTE – If the path starts with the MF identifier (3F00), it is an absolute path; otherwise it is a relative path. A relative path shall start with the identifier ‘3FFF’ or with the identifier of the current DF.

personal identification number (PIN) 4 to 12 digit number entered by the cardholder to verify that the cardholder is authorized to use a functionality of the card

private key directory file optional elementary file containing information about private keys known to the PKCS#15 application

provider authority who has or who obtained the right to create the MF or a DF in the card

public key directory file optional elementary file containing information about public keys known to the PKCS#15 application

record string of bytes which can be handled as a whole by the card and referenced by a record number or by a record identifier

private key directory file optional elementary file containing information about private keys known to the PKCS#15 application

token portable device capable of storing persistent data

1.2. Symbols, abbreviated terms and document conventions

1.2.1. Symbols

DF(x)	Dedicated file *x*
EF(x)	Elementary file *x*

1.2.2. Abbreviated terms

For the purposes of this document, the following abbreviations apply:

AID	Application Identifier
AODF	Authentication Object Directory File
BCD	Binary-Coded Decimal
CDF	Certificate Directory File
DER	Distinguished Encoding Rules
DF	Dedicated File (directory)
DODF	Data Object Directory File
EF	Elementary File
MF	Master File
ODF	Object Directory File
PIN	Personal Identification Number
PrKDF	Private Key Directory File
PuKDF	Public Key Directory File

2. Versions

2.1. *Applet version*

Some objects are hard coded into the applet and are therefore linked to the version of the applet used. These objects are:

- The PINs
- The public and private keys
- The MF, DF(BELPIC) and DF(ID) directories

When applicable, we will refer in this document to **"Applet version x"**. This version can be received with the command **"GetCardData"** that can be sent to the card and that returns a.o. the applet version.

2.2. *Card content versions*

The main version of the card content is located in the file ***TokenInfo*** (see 5.3.1).

Two versions are available:

- ***Electrical personalisation version***: this number increases at every change – even minor – in the personalisation format or personalisation options
- ***Electrical personalisation interface version***: this number increases when a change in the personalisation format or personalisation options introduces an incompatibility (e.g. of the file structure, of PIN identifiers,..).

An application can thus use newer cards if the interface version will be the same.

Note that individual files may have an internal version number corresponding to the data in the file. The "***Electrical personalisation interface version***" should be used to check the file structure, the internal file version should be used to check the fields format in the file.

2.3. *Electrical Personalisation Versions History*

Version (Hexa)	Interface Version (Hexa)	Date	Description
00	00		▪ Initial version
01	00	01-01-2004	▪ New ATR: 3B 98 94 40 **0A** A5 03 01 01 01 AD 13 10 ▪ PKCS#15 files size adaptations ▪ Address file length extended to 117 bytes
02	00	13-12-2004	▪ New ATR: 3B 98 **13** 40 0A A5 03 01 01 01 AD 13 **11**
03	00	26-10-2009	▪ New chip
04	00	01-09-2020	▪ New ATR: 80 31 80 65 b0 85 04 01 20 12 0f ff 82 90 00

3. Security Objects

3.1. Convention about PIN and key references

Some keys and PIN become global in the BelPIC application. ISO 7816 imposes a strict convention for referencing global objects. As these objects are also local, they actually have two references.

ISO 7816 standardises the references as follow:

b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0	**Meaning**
0	0	0	0	0	0	0	0	No information is given (RFU)
0	-	-	-	-	-	-	-	Global reference data
1	-	-	-	-	-	-	-	Local reference data
-	X	X	-	-	-	-	-	‘00’ others are RFU
-	-	-	X	X	X	X	X	Data object number

3.2. PIN

	PIN reference (Java Object)	**Max. trials before blocked**
PIN$_{\textbf{Cardholder}}$	01	3

3.3. Keys and Certificates

3.3.1. Keys and certificates relationships

	Private Key **(Java Object)**	**Public Key**	**X.509 Certificates** **(Transparent file)**
Basic	PrK#1	In EF(PuK#1)	
Authentication	PrK#2	In Cert#2	Cert#2
Non-repudiation	PrK#3	In Cert#3	Cert#3
Citizens CA		In Cert#4	Cert#4
Root		In Cert#6	Cert#6
Government CA		In Cert#4	Cert#4
RRN			Cert#8

Each key or certificate is indicated by means of a reference number (#). Some keys do not have a corresponding private/public key or certificate.

3.3.2. Keys Access Control

Command on key	***Reference (hex)***	***PSO: Compute Digital Signature***	***Internal Authenticate***
PrK#1 (basic)	81	✗	ALW
PrK#2 (authentication)	82	CHV($\text{PIN}_{\text{Cardhoilder}}$)	✗
PrK#3 (non-repudiation)	83	CHV($\text{PIN}_{\text{Cardholder}}$)	✗

✗	Not possible (forbidden by the card Operating System/applet)
ALW	Always
CHV(x)	Card Holder Verification with PIN ‘**x**’

4. Files

All EF file types are transparent, as defined in ISO/IEC 7816–4, sub–clause 5.1.3.

Files in the EID card is organised into a hierarchical structure according to ISO/IEC 7816–4.

The electronic signature and electronic identification applications are separated in the card by means of two application directories: ***DF(BELPIC)*** and ***DF(ID)***. Other applications DF might be added later.

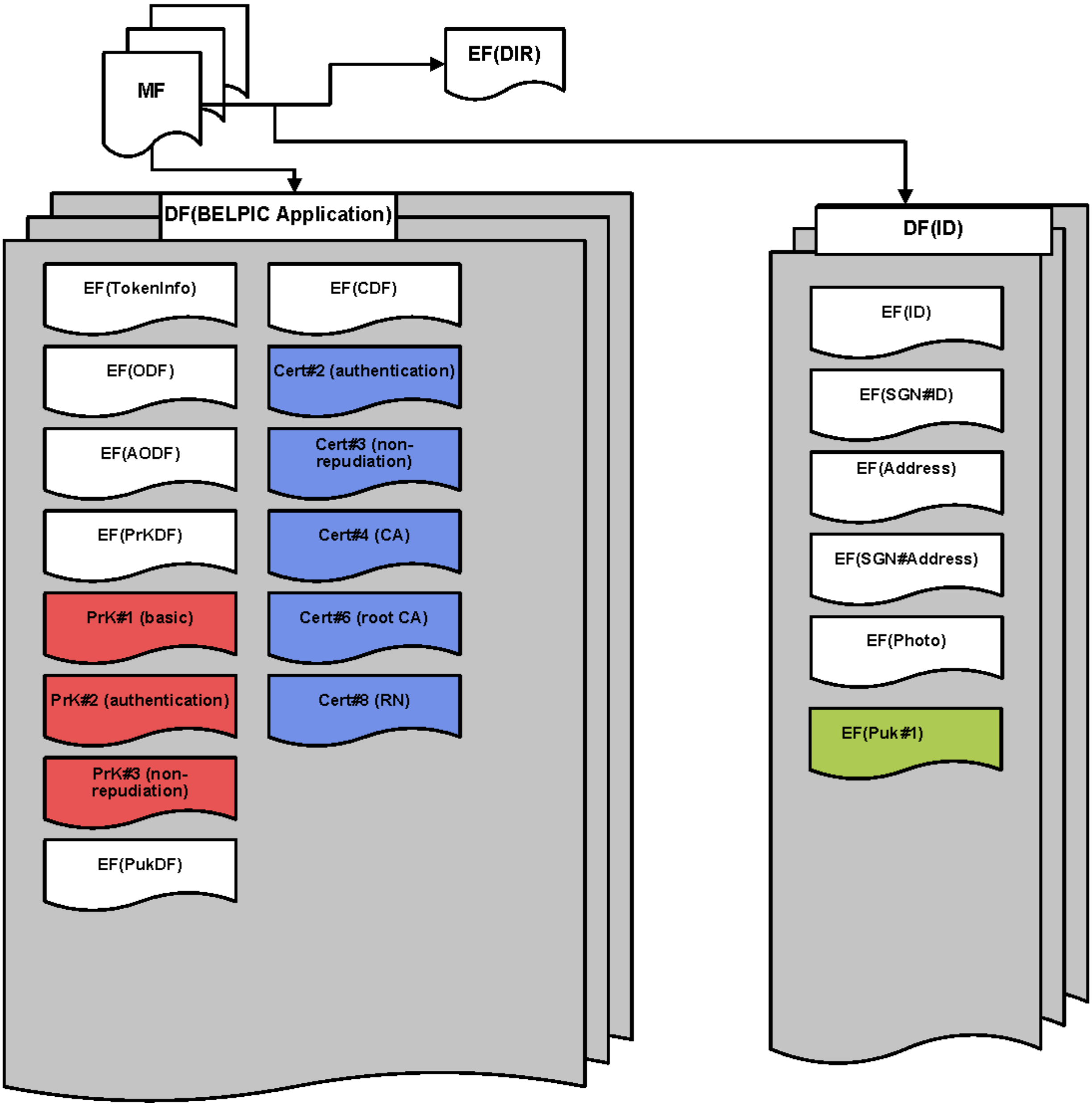
Remark: the maximum size of the files is only indicated when they can be updated later and they have to be created with a maximum size larger than the current one.

The files that can never be modified are created with the exact size to fit the content.

In case a file can be modified, its size is specified in the document.

4.1. File structure

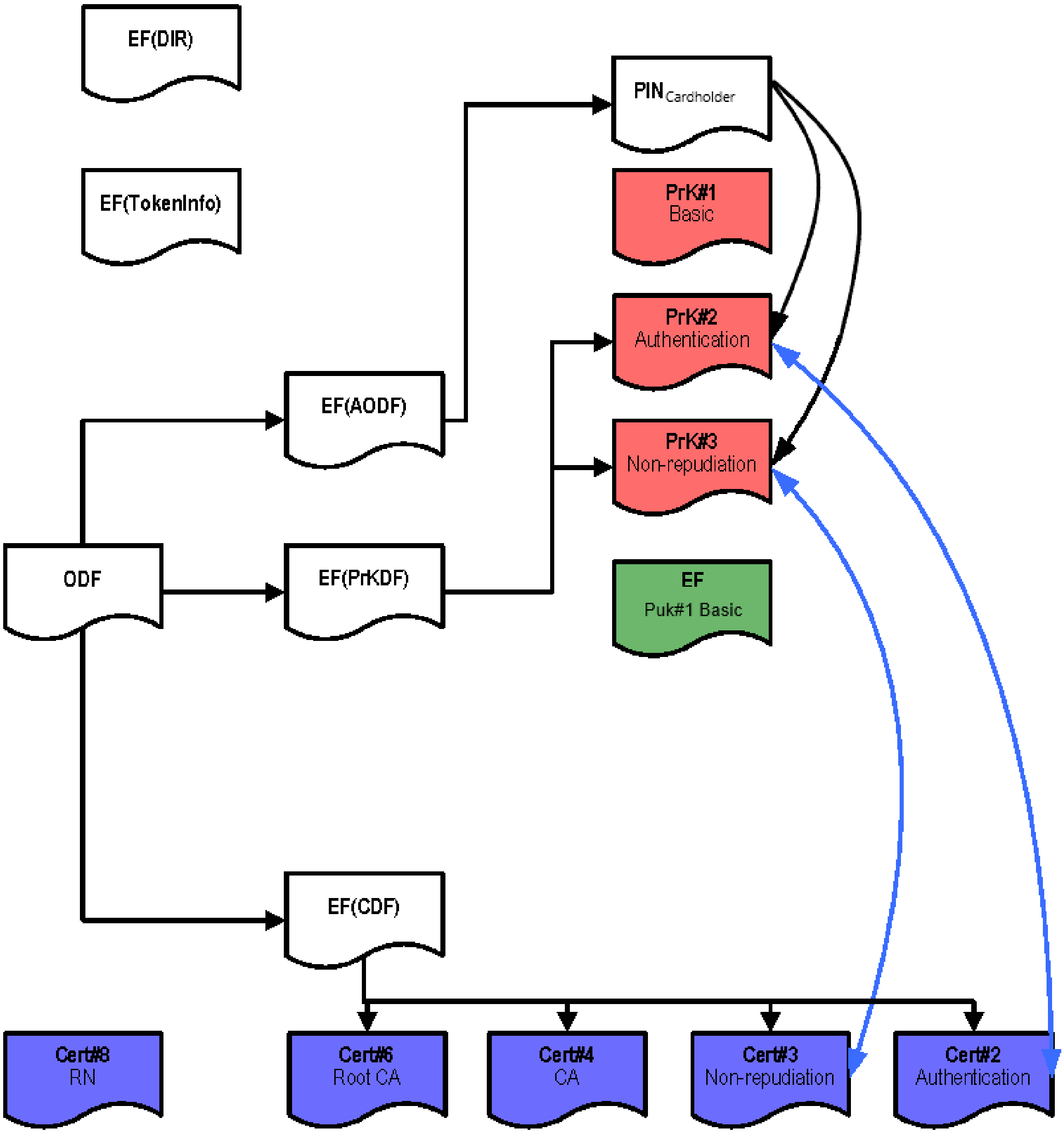
The file structure of the card is described in the figure below.



4.2. PKCS#15 files

The content of the ***DF(BELPIC)*** application directory files is compliant with PKCS#15 v1.1.

A directory file, ***EF(DIR)***, containing the AID (ISO/IEC 7816–5) for each application in the EID card is present in the ***Master File***.



The purpose of the figure above is to show the relationship between certain files ***EF(ODF)***, ***EF(AODF)***, ***EF(PrKDF)*** and ***EF(CDF)*** in the ***DF(BELPIC)*** Directory. ***EF(ODF)*** points to other EFs.

EF(PrKDF) contains cross-reference pointers to an authentication object (PIN) used to protect access to the keys. Arrows between PIN and Private Keys indicate this.

Some certificates (***Cert#2*** & ***Cert#3***) contain a public key whose private key also resides on the card, so these certificates contain the same identifier as the corresponding private key. Arrows between Certificates and Private Keys indicate this.

4.3. *Files identifiers and read permissions*

✗	Not possible (forbidden by the card Operating System/applet)
ALW	Always

	Reference (hexa)	**Read Binary**
MF	3F00	✗
EF(DIR)	2F00	ALW
- DF(BELPIC)	DF00	✗
EF(ODF)	5031	ALW
EF(TokenInfo)	5032	ALW
EF(AODF)	5034	ALW
EF(PrKDF)	5035	ALW
EF(CDF)	5037	ALW
EF(Cert#2) (auth)	5038	ALW
EF(Cert#3) (non-rep)	5039	ALW
EF(Cert#4) (CA)	503A	ALW
EF(Cert#6) (Root CA)	503B	ALW
EF(Cert#8) (RRN)	503C	ALW
- DF(ID)	DF01	✗
EF(ID#RRN)	4031	ALW
EF(SGN#ID#RRN)	4032	ALW
EF(ID#Address)	4033	ALW
EF(SGN#Adress#RRN)	4034	ALW
EF(ID#Photo)	4035	ALW
EF(Puk#1 Basic)	4040	ALW

4.5. Note for non-eID cards

The name Belpic does not only refer to the Belgian eID cards. All DFs, files, PINs and keys are also present on **Kids cards** and the **resident cards for EU and non-EU citizens**.

In some cases however, the contents of certain files may differ.
For example, the **EF(ID#RRN)** file contains extra fields on resident cards for EU and non-EU citizens.
Or for Kids cards, the **EF(Cert#2) (auth)** file may be empty, depending on the age of the child.

5. PKCS#15 information detail

5.1. *PKCS#15 application selection*

The EID card supports direct application selection as defined in ISO/IEC 7816–4, Section 9 and ISO/IEC 7816–5, Section 6 (the full AID is to be used as parameter for a ‘SELECT FILE’ command).

The operating system of the card keeps track of the currently selected application and only allows the commands applicable to that particular application while it is selected.

When several PKCS#15 applications reside on one card, they are distinguished by their object identifier in their application template in ***EF(DIR)***.

5.2. *MF directory contents*

5.2.1. *EF(DIR)*

This file contains all application templates as defined in ISO/IEC 7816–5. Each application template (tag ‘61’H) for a PKCS#15 application must at least contain the following Data Objects:

- ***Application Identifier***: tag ‘4F’, UTF-8 encoded
- ***Path***: tag ‘51’, DER-encoded

Other tags from ISO/IEC 7816–5 may, at the application issuer’s discretion, be present as well. In particular, it is recommended that application issuers include the following Data Objects:

- ***Application Label***: tag ‘50’, UTF-8 encoded
- ***Discretionary Data Objects***: tag ‘51’, DER-encoded

Encoding	ASN.1 Syntax
	Belpic (One entry per application)
	-- [APPLICATION 1] IMPLICIT SEQUENCE
	Application ID
4F 0C	-- [APPLICATION 15] IMPLICIT OCTET STRING
A0 00 00 01 77 50 4B 43 53 2D 31 35	
	Label
50 06	-- [APPLICATION 16] IMPLICIT UTF8 String
42 45 4C 50 49 43	-- 'BELPIC'
	Path
51 04	-- [APPLICATION 17] IMPLICIT OCTET STRING
3F 00 DF 00	*-- MF/Belpic*
	Discretionary Data Object
73 05	-- [APPLICATION 19] IMPLICIT SEQUENCE
	ObjectID
06 03	-- OBJECT IDENTIFIER
60 38 02	-- belgian citizen (2.16.56.2)

Remark: the Object Identifier ***2.16.56.2*** was originally intended to signify “Belgian citizen”. However, since this Object Identifier is also used for **Kids cards** and resident **cards for EU and non-EU citizens**, it should now be interpreted more generally as “Belpic card”.

5.3. DF(BELPIC) Application directory contents

This DF is the directory of the BelPIC application.

No operation is available on this data file.

5.3.1. EF(TokenInfo)

This file contains generic information about the token as such and its capabilities. This information includes the token's serial number, file types for object directory files, algorithms implemented on the token, etc.

OFFSE	Encoding	ASN.1 Syntax
00	30 27	– SEQUENCE
		Version
02	02 01	– INTEGER
04	00	– 0
		Serial Number
05	04 10	– OCTET STRING
07	**{16 bytes}**	**-- chip serial number**
		Application Label
17	**80** 06	**-- [0] Label IMPLICIT UTF8 String**
19	42 45 4C 50 49 43	– "BELPIC"
		TokenFlags
1F	03 02	– BIT STRING
21	04 30	– prnGeneration(2), eidCompliant (3)
23	9E 04	**-- [30] BELPIC Application IMPLICIT INTEGER**
25	**{4 bytes}**	**-- Version**

Versio

n bytes:

- Graphical personalisation version (default = 0)
- Electrical personalisation version (default = 0)
- Electrical personalisation interface version[1] (default = 0)
- Reserved for future use (40)

[1] This is used to indicate to an application which file system organisation is used. This value only changes when a new version is no more compatible with the previous one. (see Error: Reference source not found)

5.3.2. EF(ODF)

The Object Directory File (***ODF***) is a transparent elementary file, which contains pointers to other elementary files (***PrKDF***, ***PuKDF***, ***CDF***, ***AODF***) of the EID card. The information is presented in ASN.1 syntax according to PKCS #15.

An application using the EID card must use this file to determine how to perform security services with the card.

OFFSET	Encoding			ASN.1 Syntax		
00	A0 0A			-- [0] Private Keys		
					Path	
02		30 08			-- SEQUENCE	
						Path
04			04 06			-- OCTET STRING
06			***3F 00 DF 00 50 35***			***-- MF/Belpic/PrKDF***
0C	A4 0A			-- [4] Certificates		
					Path	
0E		30 08			-- SEQUENCE	
						Path
10			04 06			-- OCTET STRING
12			***3F 00 DF 00 50 37***			***-- MF/Belpic/CDF***
18	A8 0A			-- [8] Authentication Objects		
					Path	
1A		30 08			-- SEQUENCE	
						Path
1C			04 06			-- OCTET STRING
1E			***3F 00 DF 00 50 34***			***-- MF/Belpic/AODF***

Remark: The AODF path might be removed in a future version, as it is the default path.

5.3.3. EF(AODF)

This elementary file (Authentication Object Directory File) contains generic authentication object attributes such as allowed characters, PIN length, PIN padding character, etc. It also contains the pointers to the authentication objects themselves (in the case of PINs, pointers to the DF in which the PIN file resides). The authentication objects are used to control access to other objects such as keys. The content of this file is according to PKCS#15.

```
                                                   Common Object Attributes
02    30 0F                                        -- SEQUENCE
                                                      Label
04          0C 09                                     -- UTF8 String
06          42 61 73 69 63 20 50 49 4E                -- "Basic PIN"
                                                      Common Object Flags
0F          03 02                                     -- BIT STRING
11          06 C0                                     --  private(0), modifiable(1)
                                                   Common Authentication Object Attributes
13    30 03                                        -- SEQUENCE
                                                      Authority ID
15          04 01                                     -- OCTET STRING
17          01                                        -- '01'
18    A1 1B                                        -- [1] Pin Attributes
1A          30 19                                     -- SEQUENCE
                                                         Pin Flags
1C                03 02                                  -- BIT STRING
1E                02 0C                                  -- initialized(4), needs-padding(5)
                                                         PinType
20                0A 01                                  -- ENUMERATED
22                00                                     -- bcd(0)
                                                         Min Length
23                02 01                                  -- INTEGER
25                04                                     -- 4
                                                         Stored Length
26                02 01                                  -- INTEGER
28                08                                     -- 8 bytes
29                80 01                                  -- [0] Pin Reference IMPLICIT INTEGER
2B                01                                     -- 1
                                                         Pad Char
2C                04 01                                  -- OCTET STRING
2E                FF                                     -- 'FF'
                                                         Path
2F                30 04                                  -- SEQUENCE
                                                            Path
30                      04 02                               -- OCTET STRING
33                      3F 00                               -- 'MF'
35
```

5.3.4. EF(PrKDF)

This transparent elementary file (Private Key Directory File) contains general key attributes such as labels, intended usage, identifiers etc. It also contains the pointers to the keys themselves. The keys reside in the BELPIC application directory on the card.

OFFSET	Encoding	ASN.1 Syntax
		Private Authentication Key
00	A0 3A	– [0] Private EC Key Attributes
		Common Object Attributes
02	30 17	– SEQUENCE
		Label
04	0C 0E	-- UTF8 String
06	41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E	– "Authentication"
		Common Object Flags
14	03 02	-- BIT STRING
16	06 C0	-- private(0), modifiable(1)
		Authority ID
18	04 01	-- OCTET STRING
1A	01	-- '01'
		Common Key Attributes
1B	30 0F	– SEQUENCE
		Identifier
1D	04 01	-- OCTET STRING
1F	02	-- '02'
		KeyUsageFlags
20	03 02	-- BIT STRING
22	05 20	-- Sign(2)
		Key Access Flags
24	03 02	-- BIT STRING

26	03 B8	-- sensitive(0)
		alwaysSensitive(2)
		neverextractable(3)
		local(4)

		KeyReference
28	02 02	-- INTEGER
2A	00 82	-- '82'
2C	**A1 0E**	-- [1] Private EC Key Attributes
		Path
2E	30 0C	-- SEQUENCE
		Path
30	30 06	-- SEQUENCE
		Path
32	04 04	-- OCTET STRING
34	**3F 00 DF 00**	**-- MF**
		Key Info
38	02 02	-- INTEGER
3A	**01 80**	**-- 384 bit length**

OFFSET	Encoding	ASN.1 Syntax
		Private Non-repudiation Key
3C	A0 39	**-- [0] Private EC Key Attributes**
		Common Object Attributes
3E	30 15	-- SEQUENCE
		Label
40	0C 09	-- UTF8 String
42	53 69 67 6E 61 74 75 72 65	-- "Signature"
		Common Object Flags
4C	03 02	-- BIT STRING
4E	06 C0	-- private(0), modifiable(1)
		Authority ID
50	04 01	-- OCTET STRING
52	01	-- '01'
		UserConsent
53	02 01	-- INTEGER
55	01	-- 15
		Common Key Attributes
56	30 10	-- SEQUENCE
		Identifier
58	04 01	-- OCTET STRING
5A	03	-- '02'
		KeyUsageFlags
5B	03 03	-- BIT STRING
5D	06 00 40	-- NonRepudiation(9)
		Key Access Flags
60	03 02	-- BIT STRING

62	03 B8	-- sensitive(0)
		alwaysSensitive(2)
		neverextractable(3)
		local(4)

		KeyReference
64	02 02	-- INTEGER
66	00 83	-- '83'
68	**A1 0E**	**-- [1] Private EC Key Attributes**
		Path
6A	30 0C	-- SEQUENCE
		Path
6C	30 06	-- SEQUENCE
		Path
6E	04 04	-- OCTET STRING
70	**3F 00 DF 00**	**-- MF**
		Key Info
74	02 02	-- INTEGER
76	**01 80**	**-- 384**

5.3.5. EF(PuKDF)

This transparent elementary file (Public Key Directory File) can be regarded as directories of public keys known to the PKCS #15 application. They contain general key attributes such as labels, intended usage, identifiers, etc. When applicable, it contains cross-reference pointers to authentication objects used to protect access to the keys. Furthermore, they contain pointers to the keys themselves. Private keys corresponding to public keys must share the same identifier. The keys reside in the BELPIC application directory on the card.

As no public keys are used through the PKCS#15 interface, this file does not exist.

5.3.6. *EF(CDF)*

This transparent elementary file contains attributes and pointers to the authentication certificate (Cert #2), non-repudiation signature certificate (Cert #3), CA certificate (Cert#4) and root certificate (Cert #6). Information in this file contains certificate attributes such as labels, key identifiers, pointers to certificate files etc. The format of the file is specified in PKCS#15.

Depending on the citizen’s choice or the type of card, there can be 3 cases:

- **All certificates are present**: In this case, the ***EF(CDF)*** is exactly as show below.
- **No Non-repudiation certificate is present**. In this case, the information about the *Non-repudiation certificate* (bytes *30 27 30 12 ... DF 00 50 29*) is not present. The information about the *Intermediate CA certificate* immediately follows the information about the *Authentication certificate*, and the remainder of the file is filled with zero bytes. Additionally, the *Non-repudiation certificate* file is filled with 2500 zero bytes.
- **No Authentication and Non-repudiation certificates are present**. In this case, the information about the *Authentication* and *Non-repudiation certificates* is not present. The file starts with the information about the *Intermediate CA certificate* (bytes *30 23 30 3B ...*), and the remainder of the file is filled with zero bytes. Additionally, the *Authentication* and *Non-repudiation certificate* files are filled with 2500 zero bytes.

OFFSET	Encoding	ASN.1 Syntax
		Authentication Certificate
00	30 32	– SEQUENCE
		Common Object Attributes
02	30 17	-- SEQUENCE
		Label
04	0C 0E	-- UTF8String
06	41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E	-- "Authentication"
		Common Object Flags
14	03 02	-- BIT STRING
16	06 40	-- modifiable(1)
		AuthID
18	04 01	-- OCTET STRING
1A	01	-- '01'
		Common Certificate Attributes
1B	30 06	-- SEQUENCE
		Identifier
1D	04 01	-- OCTET STRING
1F	02	-- '02'
20	83 01	**--[3] ImplicitTrust IMPLICIT BOOLEAN**
22	00	-- False
23	**A1 0C**	**-- [1] 509CertificateAttributes**
		Path
25	30 0A	-- SEQUENCE
		Path
27	30 08	-- SEQUENCE
		Path
29	04 06	-- OCTET STRING
2B	**3F 00 DF 00 50 38**	**-- MF/Belpic/Cert#2(auth)**

OFFSET	Encoding	ASN.1 Syntax
		Non-Repudiation Certificate
31	30 2A	-- SEQUENCE
		Common Object Attributes
33	30 12	-- SEQUENCE
		Label
35	0C 09	-- UTF8String
37	53 69 67 6E 61 74 75 72 65	-- "Signature"
		Common Object Flags
40	03 02	-- BIT STRING
42	06 40	-- modifiable(1)
		AuthID
44	04 01	-- OCTET STRING
46	01	-- '01'
		Common Certificate Attributes
47	30 06	-- SEQUENCE
		Identifier
49	04 01	-- OCTET STRING
4B	03	-- '03'
4C	**83 01**	**--[3] ImplicitTrust IMPLICIT BOOLEAN**
4E	00	-- False
4F	**A1 0C**	**-- [1] X509CertificateAttributes**
		Path
51	30 0A	-- SEQUENCE
		Path
53	30 08	-- SEQUENCE
		Path

OFFSET	Encoding	ASN.1 Syntax
		Certification Authority Certificate
5D	30 26	-- SEQUENCE
		Common Object Attributes
5F	30 0B	-- SEQUENCE
		Label
61	0C 02	-- UTF8String
63	43 41	-- "CA"
		Common Object Flags
65	03 02	-- BIT STRING
67	06 40	-- modifiable(1)
		AuthID
69	04 01	-- OCTET STRING
6B	01	-- '01'
		Common Certificate Attributes
6C	30 09	-- SEQUENCE
		Identifier
6E	04 01	-- OCTET STRING
70	04	-- '04'
		Authority
71	01 01	-- BOOLEAN
73	FF	-- True
74	**83 01**	**--[3] ImplicitTrust IMPLICIT BOOLEAN**
76	00	-- False
77	**A1 0C**	**-- [1] X509CertificateAttributes**
		Path
79	30 0A	-- SEQUENCE
		Path
7B	30 08	-- SEQUENCE
		Path

OFFSET	Encoding	ASN.1 Syntax
		Root Certificate
85	30 28	-- SEQUENCE
		Common Object Attributes
87	30 0D	-- SEQUENCE
		Label
89	0C 04	-- UTF8String
8B	52 6F 6F 74	-- "Root"
		Common Object Flags
8F	03 02	-- BIT STRING
91	06 40	-- modifiable(1)
		AuthID
93	04 01	-- OCTET STRING
95	01	-- '01'
		Common Certificate Attributes
96	30 09	-- SEQUENCE
		Identifier
98	04 01	-- OCTET STRING
9A	06	-- '06'
		Authority
9B	01 01	-- BOOLEAN
9D	FF	-- True
9E	**83 01**	**--[3] ImplicitTrust IMPLICIT BOOLEAN**
A0	00	-- False
A1	**A1 0C**	**-- [1] X509CertificateAttributes**
		Path
A3	30 0A	-- SEQUENCE
		Path
A5	30 08	-- SEQUENCE
		Path

6. Application information detail

6.1. *TLV format*

Some files are encoded in a simplified ***TLV*** format:

- a tag identifying the data: 1 byte
- the length of the data[2]:
  - < 255: 1 byte
  - >= 255: multiple bytes:
    - $\boxed{\text{FF}}\boxed{x - 255}$
    - $\boxed{\text{FF}}\boxed{\text{FF}}\boxed{x - 510}$
    - $\boxed{\text{FF}}\boxed{\text{FF}}\boxed{\text{FF}}\boxed{x - 765}$
    - …
- the data: *x* bytes

Encoding type:

- All data is either pure binary, or UTF-8 containing Unicode characters.
- UTF-8 strings are not null-terminated.
- UTF-8 containing multi-byte characters is referred as ***UTF-8***.
- When data contains only 7-bits characters, it is referred as ***ASCII***, although they are fully compatible with the ***UTF-8/Unicode*** conventions.
- The actual data may be followed by padding bytes (‘0’). They have to be ignored.

[2] Nor the tag, nor the length are counted in this length.

6.2. Identity data

6.2.1. DF(ID)

This transparent data file contains all files related to the citizen and to information that is managed by the National Register.

6.2.2. EF(ID#RN)

This transparent elementary file contains all permanent information about the citizen, such as issuing country, issuing authority, issuing date, validity period, name, address, birth date, etc. This is known as the ‘ID file’.

This file contains most of the information that is graphically personalised on the card plastic.

It is formatted in simplified ***TLV*** format (see 6.1).

The file structure version corresponding to this document is 2.

The contents of this file are documented in a separate document.

6.2.3. EF(SGN#ID)

This transparent elementary file contains the signature of the ***EF(ID#RN)*** by the National Register.

As the ***EF(ID#RN)*** file contains the hash of the picture, the picture is also implicitly signed.

Signature format: ECDSA P-384 with SHA-2-384.

6.2.4. EF(ID#Address)

This transparent elementary file contains the information about the citizen‘s residence.

It is formatted in simplified ***TLV*** format (see 6.1).

The file structure version corresponding to this document is 2

The contents of this file are documented in a separate document.

6.2.5. EF(SGN#Address)

This transparent elementary file contains the signature of the ***EF(ID#Address)*** by the National Register.

EF(SGN#ID) is first appended to ***EF(ID#Address)*** before signing, in order to ensure the consistency with the file ***EF(ID#RN)***. If zero bytes are present at the end of ***EF(ID#Address)***, they need to be removed first.

Signature format: ECDSA P-384 with SHA-2-384

6.2.6. EF(ID#Photo)

This transparent elementary file contains the citizen’s picture in the standard JPEG format.

As the ***EF(ID#RN)*** file contains the hash of the picture, the picture is also implicitly signed when signing this file.

Current picture resolution: width: 140 pixels, height: 200 pixels, grey levels: 8 bits

Remark: The resolution and colour encoding are included in the JPEG format. It is advisable to dynamically use these, as they could change in the future.

6.2.7. EF(PuK#1 ID)

This transparent elementary file contains the public card key. As the ***EF(ID#RN)*** file contains the hash of the public card key, the public card key is also implicitly signed when signing this file.

OFFSE	Encoding	ASN.1 Syntax
		Authentication Certificate
00	30 76	-- SEQUENCE
02	30 10	-- SEQUENCE
		Label
04	06 07	-- OBJECT_ID
06	2A 86 48 CE 3D 02 01	EcPublicKey (1 2 840 10045 2 1)
0D	06 05	-- OBJECT_ID
0F	2B 81 04 00 22	Secp384r1 (1 3 132 0 34)
14	03 62	-- BIT_STRING (98 bytes)
16	00	-- no bits unused in the final byte
17	04	compression byte
18	**{48 bytes}**	**– X coordinate**
48	**{48 bytes}**	**– Y coordinate**

7. Public and Private Keys detail

7.1. PrivateKey #1

This file contains the private ***Basic Key***. It is involved in the ***Internal Authentication*** process.

7.2. Public Key #1

This file contains the public ***Basic Key***. It can be used to check the signature of the ***Internal Authentication*** process.

7.3. PrivateKey #2

This file contains the private RSA ***Authentication Key***.

7.4. Private Key #3

This file contains the private ***Non-Repudiation Key***.

The userConsent element in ***PrKDF*** contains value 1 for this key i.e. the cardholder must manually enter the corresponding PIN for each private key operation.

8. Certificates detail

All certificates stored in the card are DER encoded (not Base 64).

8.1. Certificate #2

This file contains the citizen’s X.509 ***Authentication Certificate*** containing the public key corresponding to the private ***Authentication Key*** (Private Key #2). When the file is created and written to during personalisation, 1100 zero bytes are appended to it. If **no authentication certificate** is issued for this person, this file consists of 2500 zero bytes.

8.2. Certificate #3

This file contains the citizen’s X.509 ***Non-Repudiation Certificate*** containing the public key corresponding to the private ‘***Non-Repudiation Key***’ (Private Key #3). When the file is created and written to during personalisation, 1100 zero bytes are appended to it. If **no non-repudiation certificate** is issued for this person, this file consists of 2500 zero bytes.

8.3. Certificate #4

This file contains the X.509 ***Citizen’s CA Certificate*** or ***Foreigner’s CA Certificate*** used to sign the ***Authentication Certificate*** (#2) and the ***Non-Repudiation Certificate*** (#3). When the file is created and written to during personalisation, 50 zero bytes are appended to it.

In the case of a resident **card for an EU or non-EU citizen**, this file contains the **Foreigner CA certificate** Instead.

8.4. Certificate #6

This file contains the X.509 ***ROOT CERTIFICATE*** used to sign the ***Citizen’s CA certificate*** (#4) or the **Foreigner CA certificate**(#4) and the **RRN certificate** (#8)

8.5. Certificate #8

This file contains the X.509 ***RRN Certificate***. This certificate corresponds to the private key used to sign the files ***EF(ID#RN)*** and ***EF(ID#Address)***.