Carta di Identità Elettronica (C.I.E)

File System

v2.0.3

1. Revision History

Version	Description	Issuing Date
2.0.3	DF_DS: SM bytes corrected. 02 / 01 values for BSO_SM_Root_Kc / BSO_SM_Root_Ka replaced with 05 / 04	2008/08/25
2.0.2	EF_DatiPersonali: file size corrected in table (04b0h instead of 01cch) Address Tag for BSOs have been corrected (83h instead of 82h)	2008/05/21
2.0.1	EF_C_Carta AC_Read set to ALWAYS	2008/05/19
2.0	First Issue	2007/05/14

2. Reference Documents

1. ISO/IEC 7816-3 second edition: Signal and transmission protocols
2. ISO/IEC 7816-4 Interindustry commands for interchange
3. ISO/IEC 7816-5 Numbering System and registration procedure for application identifiers
4. ISO/IEC 7816-8 Security related interindustry commands
5. ISO/IEC 7816-9 Additional interindustry commands and security attributes
6. Carta d' Identità Elettronica, Specifiche dei Comandi del Sistema Operativo (APDU), version 1.0 (January 11, 2000)
7. AIPA CNS Working Group May 23, 2002 Meeting Report
8. CIE – Functional Specification v 2.0
9. D.M. “Regole Tecniche sulla C.I.E.” pubblicato sulla Gazzetta Ufficiale n.261 del 9/11/2007

Table of Contents

3. File System Overview

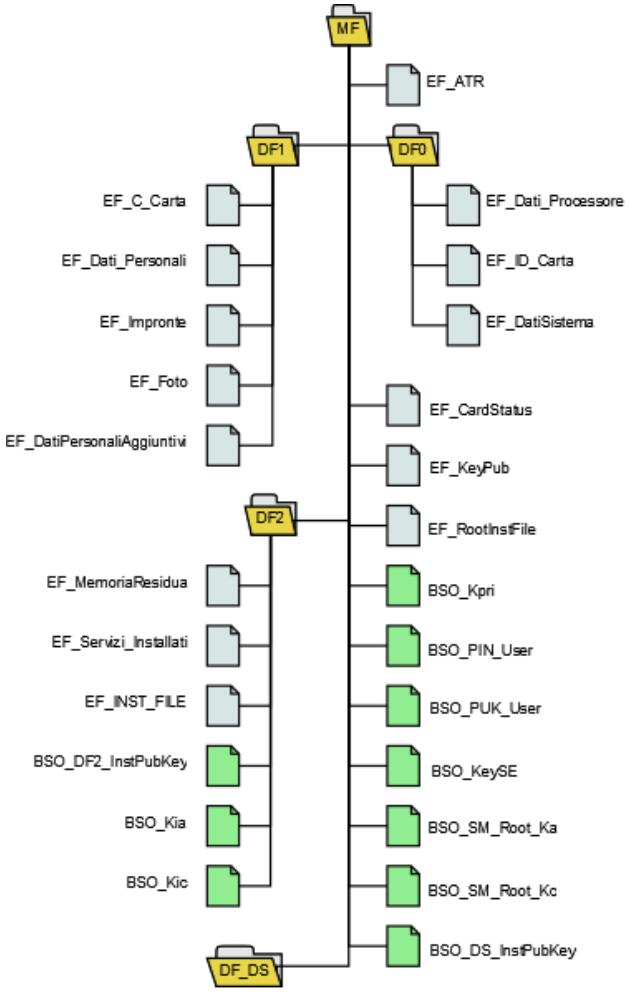

Figure 1: C.I.E. File System representation

4. File System Description

4.1Master File (MF)

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	RFU	FF	N/A
2	AC_UPDATE	FF	NEVER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER
8	AC_CREATE	FF	NEVER
9	RFU	FF	N/A

Table 1: MF Access Conditions table

4.2EF_ATR

FCI Nr.	T	L	Value	Description
1	80H	2	XX XX	File Size
2	82H	3	01 FF FF	File type: EF Transparent
3	83H	2	2F 01	File ID: ‘2F01’
4	85H	1	01	MUST be set to 01
5	86H	9	AC Bytes	See EF_ATR Access Conditions table
6	CB	24	SM Bytes	No operation is set in SM for this object

Table 2: EF_ATR file control information (FCI)

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	AC_READ	00	ALWAYS
2	AC_UPDATE	FF	NEVER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 3: EF_ATR Access Conditions table

Secure Messaging: no operation is set in SM for this object.

4.3BSO_KeySE

SECI Nr.	T	L	V	Description
1	83h	1	03	SEO ID: 03
2	86h	2	00	AC_RESTORE: ALWAYS
				RFU
3	8Fh	6	00	RFU
				COMP_CDS
			00	Not used
				COMP_CON
				COMP_Ext_Auth
			00	Not used

Table 4: BSO_KeySE description

4.4BSO_PUK_User

OCI Nr.	T	L	V	Description
1	83h	2	00	CLASS (PIN)
			11H	ID: 11h
2	85h	8	02	OPTIONS (PIN Object)
			03	FLAGS (preset Max Retry Counter=3)
			87H	ALGORITHM (PIN)
			03	ERROR COUNT
			FF	USE COUNT (Unlimited use)
			FF	RFU
			00	VALIDITY COUNTER (Unlimited Use)
			16	MINIMUM LENGTH
3	86h	7	AC bytes	See BSO_PUK_User AC table
4	CBh	16	SM bytes	No operation is set in SM for this object
5	8Fh	16	16 bytes	PUK Value filled with FF

Table 5: BSO_PUK_User description

Byte Nr.	Access Condition	Value	Meaning
1	AC_USE	00	ALWAYS
2	AC_CHANGE	FF	NEVER
3	AC_UNBLOCK	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A

7	AC_GENKEYPAIR	FF	NEVER

Table 6: BSO_PUK_User AC table

4.5BSO_PIN_User

OCI Nr.	T	L	V	Description
1	83h	2	00	CLASS (PIN)
			10H	ID: 10h
2	85h	8	02	OPTIONS (PIN Object)
			03	FLAGS (preset Max Retry Counter=3)
			87H	ALGORITHM (PIN)
			03	ERROR COUNT
			FF	USE COUNT (Unlimited use)
			FF	RFU
			00	VALIDITY COUNTER (Unlimited Use)
			08	MINIMUM LENGTH
3	86h	7	AC bytes	See BSO_PIN_User AC table
4	CBh	16	SM bytes	No operation is set in SM for this object
5	8Fh	08	8 bytes	PIN Value filled with FF

Table 7: BSO_PIN_User description

Byte Nr.	Access Condition	Value	Meaning
1	AC_USE	00	ALWAYS
2	AC_CHANGE	10H	PIN_USER
3	AC_UNBLOCK	11H	PUK_USER
4	RFU	FF	N/A
5	RFU	FF	N/A

6	RFU	FF	N/A
7	AC_GENKEYPAIR	FF	NEVER

Table 8: BSO_PIN_User AC table

4.6Card Status (EF_CardStatus)

FCI Nr.	T	L	Value	Description
1	80H	2	00 20H	File Size: 32 byte
2	82H	3	01 FF FF	File Type: EF Transparent
3	83H	2	3F 02	File ID: '3F02'
4	85H	1	01	MUST be set to 01
5	86H	9	AC Bytes	See EF_CardStatus Access Conditions table
6	CB	24	SM Bytes	No operation is set in SM for this object

Table 9: EF_CardStatus

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	AC_READ	00	ALWAYS
2	AC_UPDATE	10H	PIN_USER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 10: EF_CardStatus Access Conditions Table

This file is filled with 32 bytes set to 0.

4.7EF_KeyPub

FCI Nr.	T	L	Value	Description
1	80H	2	01 2C	File Size: 300 byte
2	82H	3	05 FF FF	File Type: EF TLV
3	83H	2	3F 01	File ID: ‘3F01’
4	85H	1	01	MUST be set to 01
5	86H	9	AC Bytes	See EF_KeyPub Access Conditions table
6	CB	24	SM Bytes	No operation is set in SM for this object

Table 11: EF_KeyPub description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	AC_READ	00	ALWAYS
2	AC_UPDATE	FF	NEVER
3	AC_APPEND	11H	PUK_USER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	11H	PUK_USER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 12: EF_KeyPub AC table after Initialization phase

Byte Nr.	AC Description	Personalization Phase (IPZS)

		Value (Hex)	Meaning
1	AC_READ	00	ALWAYS
2	AC_UPDATE	FF	NEVER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 13: EF_KeyPub AC table after Personalization phase

4.8BSO_SM_ Root_Ka

OCI Nr.	T	L	V	Description
1	83h	2	10H	CLASS (3DES_SM)
			04	ID: 04
2	85h	8	83H	OPTIONS (3DES SM)
			00	FLAGS (No meaning)
			82H	ALGORITHM (SM Authentication)
			0F	ERROR COUNT (No meaning)
			FF	USE COUNT (Unlimited use)
			FF	RFU
			00	VALIDITY COUNTER (Unlimited Use)
			24	24 bytes 3DES Key
3	86h	7	AC bytes	See BSO_SM_Root_Ka AC table

4	CBh	16	SM bytes	See BSO_SM_Root_Ka SM description
5	8Fh	24	24 bytes	SM_Root_Ka value

Table 14: BSO_SM_Root_Ka description

Byte Nr.	Access Condition	Value	Meaning
1	AC_USE	00	ALWAYS
2	AC_CHANGE	00	ALWAYS
3	AC_UNBLOCK	FF	N/A
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_GENKEYPAIR	FF	N/A

Table 15: BSO_SM_Root_Ka AC table

Byte Nr.	SM Condition	Value	Meaning
1	ENC USE IN	FF	No SM
2	SIG USE IN	FF	No SM
3	ENC CHANGE	05	BSO_SM_Root_Kc
4	SIG CHANGE	04	BSO_SM_Root_Ka
5	ENC UNBLOCK	FF	No SM
6	SIG UNBLOCK	FF	No SM
7..14	RFU	FF	No SM
15	ENC USE OUT	FF	No SM
16	SIG USE OUT	FF	No SM

Table 16: BSO_SM_Root_Ka SM description

4.9BSO_SM_Root_Kc

OCI Nr.	T	L	V	Description
1	83h	2	10H	CLASS (3DES_SM)
			05	ID: 05
2	85h	8	83H	OPTIONS (3DES SM)
			00	FLAGS (No meaning)
			03	ALGORITHM (SM Cipher)
			0F	ERROR COUNT (No meaning)
			FF	USE COUNT (Unlimited use)
			FF	RFU
			00	VALIDITY COUNTER (Unlimited Use)
			24	24 bytes 3DES Key
3	86h	7	AC bytes	See BSO_SM_Root_Kc AC table
4	CBh	16	SM bytes	See BSO_SM_Root_Kc SM description
5	8Fh	24	24 bytes	SM_Root_Kc value

Table 17: BSO_SM_Root_Kc description

Byte Nr.	Access Condition	Value	Meaning
1	AC_USE	00	ALWAYS
2	AC_CHANGE	00	ALWAYS
3	AC_UNBLOCK	FF	N/A
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_GENKEYPAIR	FF	N/A

Table 18: BSO_SM_Root_Kc AC table

Byte Nr.	SM Condition	Value	Meaning
1	ENC USE IN	FF	No SM
2	SIG USE IN	FF	No SM
3	ENC CHANGE	05	BSO_SM_Root_Kc
4	SIG CHANGE	04	BSO_SM_Root_Ka
5	ENC UNBLOCK	FF	No SM
6	SIG UNBLOCK	FF	No SM
7..14	RFU	FF	No SM
15	ENC USE OUT	FF	No SM
16	SIG USE OUT	FF	No SM

Table 19: BSO_SM_Root_Kc SM description

4.10BSO_DS_InstPubKey (Modulus)

OCI Nr.	T	L	V	Description
1	83h	2	00	CLASS (RSA KPub Ext. Auth. 1st component)
			03	ID: 03
2	85h	8	21H	OPTIONS (RSA public key Modulus for Ext. Authentication)
			0A	FLAGS (Preset Error Count: 10)
			88H	ALGORITHM (RSA public key for EXT. AUTH.)
			0A	ERROR COUNT (10)
			FF	USE COUNT (Unlimited use)
			FF	RFU
			00	VALIDITY COUNTER (Unlimited Use)
			00	MINIMUM LENGTH

3	86h	7	AC bytes	See BSO_DS_InstPubKey (modulus) AC table
4	CBh	16	SM bytes	No operation is set in SM for this object
5	8Fh	130	130 bytes	BSO_DS_InstPubKey Modulus bytes

Table 20: BSO_DS_InstPubKey (modulus) description

Byte Nr.	Access Condition	Value	Meaning
1	AC_USE	00	ALWAYS
2	AC_CHANGE	FF	NEVER
3	AC_UNBLOCK	FF	N/A
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_GENKEYPAIR	FF	N/A

Table 21: BSO_DS_InstPubKey (modulus) AC table

4.11BSO_DS_InstPubKey (Exponent)

OCI Nr.	T	L	V	Description
1	83h	2	01	CLASS (RSA KPub Ext. Auth. 2nd component)
			03	ID: 03
2	85h	8	01	OPTIONS (RSA public key Exponent for Ext. Authentication)
			0A	FLAGS (Preset Error Count: 10)
			88H	ALGORITHM (RSA public key for EXT. AUTH.)
			0A	ERROR COUNT (10)
			FF	USE COUNT (Unlimited use)
			FF	RFU
			00	VALIDITY COUNTER (Unlimited Use)

			00	MINIMUM LENGTH
3	86h	7	AC bytes	See BSO_DS_InstPubKey (exponent) AC table
4	CBh	16	SM bytes	No operation is set in SM for this object
5	8Fh	130	130 bytes	BSO_DS_InstPubKey Exponent bytes

Table 22: BSO_DS_InstPubKey (exponent) description

Byte Nr.	Access Condition	Value	Meaning
1	AC_USE	00	ALWAYS
2	AC_CHANGE	FF	NEVER
3	AC_UNBLOCK	FF	N/A
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_GENKEYPAIR	FF	N/A

Table 23: BSO_DS_InstPubKey (exponent) AC table

4.12EF_RootInstFile

FCI Nr.	T	L	Value	Description
1	80H	2	01 00H	File Size: 256 byte
2	82H	3	01 FF FF	EF Transparent
3	83H	2	04 05	File ID: ‘0405’
4	85H	1	01	MUST be set to 01
5	86H	9	AC Bytes	See EF_RootInstFile Access Conditions table
6	CB	24	SM Bytes	See EF_RootInstFile SM description table

Table 24: EF_RootInstFile description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	AC_READ	00	ALWAYS
2	AC_UPDATE	00	ALWAYS
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 25: EF_RootInstFile Access Conditions table

Byte Nr.	SM Condition	Value	Meaning
1	ENC READ OUT	FF	No SM
2	SIG READ OUT	FF	No SM
3	ENC UPDATE	05	SM_Root_Kc
4	SIG UPDATE	04	SM_Root_Ka
5	ENC APPEND	FF	No SM
6	SIG APPEND	FF	No SM
7..12	RFU	FF	N/A
13	ENC ADMIN	FF	No SM
14	SIG ADMIN	FF	No SM
15..22	RFU	FF	N/A
23	ENC READ IN	FF	No SM
24	SIG READ IN	FF	No SM

Table 26: EF_RootInstFile SM description

4.13BSO_KPri (Modulus)

OCI Nr.	T	L	V	Description
1	83h	2	20H	CLASS (RSA KPri for ENC/DEC and DS 1st component)
			01	ID: 01
2	85h	8	22H	OPTIONS (RSA private key Modulus for ENC/DEC and DS)
			00	FLAGS (No meaning)
			0C	ALGORITHM (RSA PURE)
			0F	ERROR COUNT (No meaning)
			FF	USE COUNT (Unlimited use)
			FF	RFU
			00	VALIDITY COUNTER (Unlimited Use)
			00	MINIMUM LENGTH
3	86h	7	AC bytes	See BSO_KPri (Modulus) AC table
4	CBh	16	SM bytes	No operation is set in SM for this object
5	8Fh	130	130 bytes	BSO_KPri Modulus bytes

Table 27: BSO_KPri (Modulus) description

Byte Nr.	Access Condition	Value	Meaning
1	AC_USE	10H	PIN_USER
2	AC_CHANGE	FF	NEVER
3	AC_UNBLOCK	FF	N/A
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A

7	AC_GENKEYPAIR	11H	PUK_USER

Table 28: BSO_KPri (Modulus) AC table

4.14BSO_KPri (Exponent)

OCI Nr.	T	L	V	Description
1	83h	2	21H	CLASS (RSA KPri for ENC/DEC and DS 2nd component)
			01	ID: 01
2	85h	8	02	OPTIONS (RSA private key Exponent for ENC/DEC and DS)
			00	FLAGS (No meaning)
			0C	ALGORITHM (RSA PURE)
			0F	ERROR COUNT (No meaning)
			FF	USE COUNT (Unlimited use)
			FF	RFU
			00	VALIDITY COUNTER (Unlimited Use)
			00	MINIMUM LENGTH
3	86h	7	AC bytes	See BSO_KPri (Exponent) AC table
4	CBh	16	SM bytes	No operation is set in SM for this object
5	8Fh	130	130 bytes	BSO_KPri Exponent bytes

Table 29: BSO_KPri (Exponent) description

Byte Nr.	Access Condition	Value	Meaning
1	AC_USE	10H	PIN_USER
2	AC_CHANGE	FF	NEVER
3	AC_UNBLOCK	FF	N/A
4	RFU	FF	N/A
5	RFU	FF	N/A

6	RFU	FF	N/A
7	AC_GENKEYPAIR	11H	PUK_USER

Table 30: BSO_KPri (Exponent) AC table

4.15Card Data DF (DF0)

FCI Nr.	T	L	Value	Description
1	81H	2	N/A N/A	File Size: N/A
2	82H	3	38H FF FF	File Type: Dedicated File
3	83H	2	10H 00	File ID: ‘1000’
4	85H	1	01	MUST be set to 01
5	86H	9	AC Bytes	See DF0 Access Conditions table
6	CB	24	SM Bytes	No operation is set in SM for this object

Table 31: DF0 description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	RFU	FF	N/A
2	AC_UPDATE	FF	NEVER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER
8	AC_CREATE	FF	NEVER
9	RFU	FF	N/A

Table 32: DF0 Access conditions table

4.15.1 Chip Data EF (EF_DatiProcessore)

FCI Nr.	T	L	Value	Description
1	80H	2	00 36	File Size: 54 byte
2	82H	3	01 FF FF	File Type: EF Transparent
3	83H	2	10H 02	File ID: ‘1002’
4	85H	1	01	MUST be set to 01
5	86H	9	AC Bytes	See EF_DatiProcessore Access Conditions table
6	CB	24	SM Bytes	No operation is set in SM for this object

Table 33: EF_DatiProcessore description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	AC_READ	00	ALWAYS
2	AC_UPDATE	FF	NEVER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 34: EF_DatiProcessore Access Conditions table

4.15.2 Card ID EF (EF_IDCarta)

FCI Nr.	T	L	Value		Description
1	80H	2	00	10H	File Size: 16 byte

2	82H	3	01	FF	FF	File Type: EF Transparent
3	83H	2	10H	03		File ID: ‘1003’
4	85H	1	01			MUST be set to 01
5	86H	9	AC Bytes			See EF_IDCarta Access Conditions table
6	CB	24	SM Bytes			No operation is set in SM for this object

Table 35: EF_IDCarta description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	AC_READ	00	ALWAYS
2	AC_UPDATE	FF	NEVER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 36: EF_IDCarta Access Conditions table

4.15.3 System's Data EF (EF_DatiSistema)

FCI Nr.	T	L	Value			Description
1	80H	2	00	C8		File Size: 200 byte
2	82H	3	01	FF	FF	File Type: EF Transparent
3	83H	2	10H	04		File ID: ‘1004’
4	85H	1	01			MUST be set to 01

5	86H	9	AC Bytes	See EF_DatiSistema Access Conditions table
6	CB	24	SM Bytes	No operation is set in SM for this object

Table 37: EF_DatiSistema description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	AC_READ	00	ALWAYS
2	AC_UPDATE	11H	PUK_USER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	11H	PUK_USER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 38: EF_DatiSistema Access Conditions table after initialization

Byte Nr.	AC Description	Personalization Phase	
		Value (Hex)	Meaning
1	AC_READ	00	ALWAYS
2	AC_UPDATE	FF	NEVER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER

8	RFU	FF	N/A
9	RFU	FF	N/A

Table 39: EF_DatiSistema Access Conditions table after personalization

4.16Card Holder's Data DF (DF1)

FCI Nr.	T	L	Value	Description
1	81H	2	N/A N/A	File Size: N/A
2	82H	3	38H FF FF	File Type: Dedicated File
3	83H	2	11H 00	File ID: '1100'
4	85H	1	01	MUST be set to 01
5	86H	9	AC Bytes	See DF1 Access Conditions table
6	CB	24	SM Bytes	No operation is set in SM for this object

Table 40: DF1 description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	RFU	FF	N/A
2	AC_UPDATE	FF	NEVER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER
8	AC_CREATE	FF	NEVER
9	RFU	FF	N/A

Table 41: DF1 Access conditions table

4.16.1 Card Holder's Certificate EF (EF_C_Carta)

FCI Nr.	T	L	Value	Description
1	80H	2	08 00	File Size: 2KB
2	82H	3	01 FF FF	File Type: EF Transparent
3	83H	2	11H 01	File ID: '1101'
4	85H	1	01	MUST be set to 01
5	86H	9	AC Bytes	See EF_C_Carta Access Conditions table
6	CB	24	SM Bytes	No operation is set in SM for this object

Table 42: EF_C_Carta description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	AC_READ	00	ALWAYS
2	AC_UPDATE	11H	PUK_USER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	11H	PUK_USER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 43: EF_C_Carta AC table after Initialization phase

Byte Nr.	AC Description	Personalization Phase	
		Value (Hex)	Meaning
1	AC_READ	00	ALWAYS

2	AC_UPDATE	FF	NEVER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 44: EF_C_Carta AC table after Personalization phase

4.16.2 Card Holder's Personal Data EF (EF_DatiPersonali)

FCI Nr.	T	L	Value	Description
1	80H	2	04 B0	File Size: 1200 bytes
2	82H	3	01 FF FF	File Type: EF Transparent
3	83H	2	11H 02	File ID: '1102'
4	85H	1	01	MUST be set to 01
5	86H	9	AC Bytes	See EF_DatiPersonali Access Conditions table
6	CB	24	SM Bytes	No operation is set in SM for this object

Table 45: EF_DatiPersonali description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	AC_READ	10H	PIN_USER
2	AC_UPDATE	11H	PUK_USER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A

5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	11H	PUK_USER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 46: EF_DatiPersonali AC table after Initialization phase

Byte Nr.	AC Description	Personalization Phase	
		Value (Hex)	Meaning
1	AC_READ	10H	PIN_USER
2	AC_UPDATE	FF	NEVER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 47: EF_DatiPersonali AC table after Personalization phase

4.16.3 Card Holder's Notes EF (EF_DatiPersonali_Annotazioni)

FCI Nr.	T	L	Value	Description
1	80H	2	01 00	File Size: 256 bytes
2	82H	3	01 FF FF	File Type: EF Transparent
3	83H	2	11H 03	File ID: '1103'
4	85H	1	01	MUST be set to 01

5	86H	9	AC Bytes	See EF_DatiPersonali_Annotazioni Access Conditions table
6	CB	24	SM Bytes	No operation is set in SM for this object

Table 48: EF_DatiPersonali_Annotazioni description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	AC_READ	10H	PIN_USER
2	AC_UPDATE	11H	PUK_USER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	11H	PUK_USER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 49: EF_DatiPersonali_Annotazioni AC table after Initialization phase

Byte Nr.	AC Description	Personalization Phase	
		Value (Hex)	Meaning
1	AC_READ	10H	PIN_USER
2	AC_UPDATE	FF	NEVER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER

8	RFU	FF	N/A
9	RFU	FF	N/A

Table 50: EF_DatiPersonali_Annotazioni AC table after Personalization phase

4.16.4 Fingerprints EF (EF_Impronte)

FCI Nr.	T	L	Value	Description
1	80H	2	0C 00	File Size: 3072 bytes
2	82H	3	01 FF FF	File Type: EF Transparent
3	83H	2	11H 04	File ID: ‘1104’
4	85H	1	01	MUST be set to 01
5	86H	9	AC Bytes	See EF_Fingerprints Access Conditions table
6	CB	24	SM Bytes	No operation is set in SM for this object

Table 51: EF_Impronte description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	AC_READ	TBD	TBD
2	AC_UPDATE	11H	PUK_USER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	11H	PUK_USER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 52: EF_Impronte AC table after Initialization phase

Byte Nr.	AC Description	Personalization Phase	
		Value (Hex)	Meaning
1	AC_READ	TBD	TBD
2	AC_UPDATE	FF	NEVER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 53: EF_Impronte AC table after Personalization phase

4.16.5 Photo EF (EF_Foto)

FCI Nr.	T	L	Value	Description
1	80H	2	30H 00	File Size: 12288 bytes
2	82H	3	01 FF FF	File Type: EF Transparent
3	83H	2	11H 05	File ID: ‘1105’
4	85H	1	01	MUST be set to 01
5	86H	9	AC Bytes	See EF_Fingerprints Access Conditions table
6	CB	24	SM Bytes	No operation is set in SM for this object

Table 54: EF_Foto description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	AC_READ	TBD	TBD

2	AC_UPDATE	11H	PUK_USER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	11H	PUK_USER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 55: EF_Foto AC table after Initialization phase

Byte Nr.	AC Description	Personalization Phase	
		Value (Hex)	Meaning
1	AC_READ	TBD	TBD
2	AC_UPDATE	FF	NEVER
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 56: EF_Foto AC table after Personalization phase

4.17Additional Services DF (DF2)

FCI Nr.	T	L	Value		Description
1	81H	2	N/A	N/A	File Size: N/A

2	82H	3	38H	FF	FF	File Type: Dedicated File
3	83H	2	12H		00	File ID: ‘1200’
4	85H	1	01			MUST be set to 01
5	86H	9	AC Bytes			See DF2 Access Conditions table
6	CB	24	SM Bytes			See DF2 SM description

Table 57: DF2 description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	RFU	FF	N/A
2	AC_UPDATE	00	ALWAYS
3	AC_APPEND	00	ALWAYS
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	00	ALWAYS
8	AC_CREATE	03	BSO_DF2_InstPubKey
9	RFU	FF	N/A

Table 58: DF2 Access conditions table

Byte Nr.	SM Condition	Value	Meaning
1..2	RFU	FF	Set to FFh
3	ENC UPDATE/APPEND (objects)	02	BSO_Kic
4	SIG UPDATE/APPEND (objects)	01	BSO_Kia
5..12	RFU	FF	Set to FFh
13	ENC ADMIN	02	BSO_Kic

14	SIG ADMIN	01	BSO_Kia
15	ENC CREATE	02	BSO_Kic
16	SIG CREATE	01	BSO_Kia
17..24	RFU	FF	Set to FFh

Table 59: DF2 SM description

4.17.1 Card's Free Memory EF (EF_MemoriaResidua)

FCI Nr.	T	L	Value	Description
1	80H	2	00 04	File Size: 4 bytes
2	82H	3	01 FF FF	File Type: EF Transparent
3	83H	2	12H 02	File ID: '1202'
4	85H	1	01	MUST be set to 01
5	86H	9	AC Bytes	See EF_MemoriaResidua Access Conditions table
6	CB	24	SM Bytes	See EF_MemoriaResidua SM description

Table 60: EF_MemoriaResidua description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	AC_READ	00	ALWAYS
2	AC_UPDATE	00	ALWAYS
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER
8	RFU	FF	N/A

9	RFU	FF	N/A

Table 61: EF_MemoriaResidua AC table

Byte Nr.	SM Condition	Value	Meaning
1	ENC READ OUT	FF	No SM
2	SIG READ OUT	FF	No SM
3	ENC UPDATE	02	BSO_Kic
4	SIG UPDATE	01	BSO_Kia
5	ENC APPEND	FF	No SM
6	SIG APPEND	FF	No SM
7..12	RFU	FF	Set to FFh
13	ENC ADMIN	FF	No SM
14	SIG ADMIN	FF	No SM
15..22	RFU	FF	Set to FFh
23	ENC READ IN	FF	No SM
24	SIG READ IN	FF	No SM

Table 62: EF_MemoriaResidua SM description

4.17.2 Installed Services List EF (EF_ServiziInstallati)

FCI Nr.	T	L	Value	Description
1	80H	2	01 40	File Size: 320 bytes
2	82H	3	01 FF FF	File Type: EF Transparent
3	83H	2	12H 03	File ID: ‘1203’
4	85H	1	01	MUST be set to 01
5	86H	9	AC Bytes	See EF_ServiziInstallati Access Conditions table
6	CB	24	SM Bytes	See EF_ServiziInstallati SM description

Table 63: EF_ServiziInstallati description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	AC_READ	00	ALWAYS
2	AC_UPDATE	00	ALWAYS
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 64: EF_ServiziInstallati AC table

Byte Nr.	SM Condition	Value	Meaning
1	ENC READ OUT	FF	No SM
2	SIG READ OUT	FF	No SM
3	ENC UPDATE	02	BSO_Kic
4	SIG UPDATE	01	BSO_Kia
5	ENC APPEND	FF	No SM
6	SIG APPEND	FF	No SM
7..12	RFU	FF	Set to FFh
13	ENC ADMIN	FF	No SM
14	SIG ADMIN	FF	No SM
15..22	RFU	FF	Set to FFh
23	ENC READ IN	FF	No SM
24	SIG READ IN	FF	No SM

Table 65: EF_ServiziInstallati SM description

4.17.3 EF_INST_FILE

FCI Nr.	T	L	Value	Description
1	80H	2	01 00	File Size: 256 bytes
2	82H	3	01 FF FF	File Type: EF Transparent
3	83H	2	41H 42H	File ID: ‘4142’
4	85H	1	01	MUST be set to 01
5	86H	9	AC Bytes	See EF_INST_FILE Access Conditions table
6	CB	24	SM Bytes	See EF_INST_FILE SM description

Table 66: EF_INST_FILE description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	AC_READ	00	ALWAYS
2	AC_UPDATE	00	ALWAYS
3	AC_APPEND	FF	NEVER
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	FF	NEVER
8	RFU	FF	N/A
9	RFU	FF	N/A

Table 67: EF_INST_FILE AC table

Byte Nr.	SM Condition	Value	Meaning
1	ENC READ OUT	FF	No SM

2	SIG READ OUT	FF	No SM
3	ENC UPDATE	02	BSO_Kic
4	SIG UPDATE	01	BSO_Kia
5	ENC APPEND	FF	No SM
6	SIG APPEND	FF	No SM
7..12	RFU	FF	Set to FFh
13	ENC ADMIN	FF	No SM
14	SIG ADMIN	FF	No SM
15..22	RFU	FF	Set to FFh
23	ENC READ IN	FF	No SM
24	SIG READ IN	FF	No SM

Table 68: EF_INST_FILE SM description

4.17.4 BSO_DF2_InstPubKey (Modulus)

OCI Nr.	T	L	V	Description
1	83h	2	00	CLASS (RSA KPub Ext. Auth. 1st component)
			03	ID: 03
2	85h	8	21H	OPTIONS (RSA public key Modulus for Ext. Authentication)
			0A	FLAGS (Preset Error Count: 10)
			88H	ALGORITHM (RSA public key for EXT. AUTH.)
			0A	ERROR COUNT (10)
			FF	USE COUNT (Unlimited use)
			FF	RFU
			00	VALIDITY COUNTER (Unlimited Use)
			00	MINIMUM LENGTH
3	86h	7	AC bytes	See BSO_DF2_InstPubKey (modulus) AC table

4	CBh	16	SM bytes	No operation is set in SM for this object
5	8Fh	130	130 bytes	BSO_DF2_InstPubKey Modulus bytes

Table 69: BSO_DF2_InstPubKey (modulus) description

Byte Nr.	Access Condition	Value	Meaning
1	AC_USE	00	ALWAYS
2	AC_CHANGE	FF	NEVER
3	AC_UNBLOCK	FF	N/A
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_GENKEYPAIR	FF	N/A

Table 70: BSO_DF2_InstPubKey (modulus) description

4.17.5 BSO_DF2_InstPubKey (Exponent)

OCI Nr.	T	L	V	Description
1	83h	2	01	CLASS (RSA KPub Ext. Auth. 2nd component)
			03	ID: 03
2	85h	8	01	OPTIONS (RSA public key Exponent for Ext. Authentication)
			0A	FLAGS (Preset Error Count: 10)
			88H	ALGORITHM (RSA public key for EXT. AUTH.)
			0A	ERROR COUNT (10)
			FF	USE COUNT (Unlimited use)
			FF	RFU
			00	VALIDITY COUNTER (Unlimited Use)
			00	MINIMUM LENGTH

3	86h	7	AC bytes	See BSO_InstPubKey (exponent) AC table
4	CBh	16	SM bytes	No operation is set in SM for this object
5	8Fh	130	130 bytes	BSO_InstPubKey Exponent bytes

Table 71: BSO_DF2_InstPubKey (exponent) description

Byte Nr.	Access Condition	Value	Meaning
1	AC_USE	00	ALWAYS
2	AC_CHANGE	FF	NEVER
3	AC_UNBLOCK	FF	N/A
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_GENKEYPAIR	FF	N/A

Table 72: BSO_DF2_InstPubKey (exponent) AC table

4.17.6 BSO_Kia

OCI Nr.	T	L	V	Description
1	83h	2	10H	CLASS (3DES_SM)
			01	ID: 01
2	85h	8	83H	OPTIONS (3DES SM)
			00	FLAGS (No meaning)
			82H	ALGORITHM (SM Authentication)
			0F	ERROR COUNT (No meaning)
			FF	USE COUNT (Unlimited use)
			FF	RFU
			00	VALIDITY COUNTER (Unlimited Use)

			24	24 bytes 3DES key
3	86h	7	AC bytes	See BSO_Kia AC table
4	CBh	16	SM bytes	See BSO_Kia SM description
5	8Fh	24	24 bytes	Kia bytes

Table 73: BSO_ Kia description

Byte Nr.	Access Condition	Value	Meaning
1	AC_USE	00	ALWAYS
2	AC_CHANGE	00	ALWAYS
3	AC_UNBLOCK	FF	N/A
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_GENKEYPAIR	FF	N/A

Table 74: BSO_ Kia AC table

Byte Nr.	SM Condition	Value	Meaning
1	ENC USE IN	FF	No SM
2	SIG USE IN	FF	No SM
3	ENC CHANGE	05	BSO_Kic
4	SIG CHANGE	04	BSO_Kia
5	ENC UNBLOCK	FF	No SM
6	SIG UNBLOCK	FF	No SM
7..14	RFU	FF	No SM
15	ENC USE OUT	FF	No SM
16	SIG USE OUT	FF	No SM

Table 75: BSO_ Kia SM description

4.17.7 BSO_Kic

OCI Nr.	T	L	V	Description
1	83h	2	10H	CLASS (3DES_SM)
			02	ID: 02
2	85h	8	83H	OPTIONS (3DES SM)
			00	FLAGS (No meaning)
			03	ALGORITHM (SM Cipher)
			0F	ERROR COUNT (No meaning)
			FF	USE COUNT (Unlimited use)
			FF	RFU
			00	VALIDITY COUNTER (Unlimited Use)
			24	24 bytes 3DES Key
3	86h	7	AC bytes	See BSO_Kic AC table
4	CBh	16	SM bytes	See BSO_Kic SM description
5	8Fh	24	24 bytes	Kic bytes

Table 76: BSO_Kic description

Byte Nr.	Access Condition	Value	Meaning
1	AC_USE	00	ALWAYS
2	AC_CHANGE	00	ALWAYS
3	AC_UNBLOCK	FF	N/A
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A

7	AC_GENKEYPAIR	FF	N/A

Table 77: BSO_Kic AC table

Byte Nr.	SM Condition	Value	Meaning
1	ENC USE IN	FF	No SM
2	SIG USE IN	FF	No SM
3	ENC CHANGE	05	BSO_Kic
4	SIG CHANGE	04	BSO_Kia
5	ENC UNBLOCK	FF	No SM
6	SIG UNBLOCK	FF	No SM
7..14	RFU	FF	No SM
15	ENC USE OUT	FF	No SM
16	SIG USE OUT	FF	No SM

Table 78: BSO_Kic SM description

4.18Digital Signature DF (DF_DS)

FCI Nr.	T	L	Value	Description
1	81H	2	N/A N/A	File Size: N/A
2	82H	3	38H FF FF	File Type: Dedicated File
3	83H	2	14H 00	File ID: ‘1400’
4	85H	1	01	MUST be set to 01
5	86H	9	AC Bytes	See DF_DS Access Conditions table
6	CB	24	SM Bytes	See DF_DS SM description

Table 79: DF_DS description

Byte Nr.	AC Description	Initialization Phase (IPZS)	
		Value (Hex)	Meaning
1	RFU	FF	N/A
2	AC_UPDATE	03	BSO_DS_InstPubKey
3	AC_APPEND	03	BSO_DS_InstPubKey
4	RFU	FF	N/A
5	RFU	FF	N/A
6	RFU	FF	N/A
7	AC_ADMIN	03	BSO_DS_InstPubKey
8	AC_CREATE	03	BSO_DS_InstPubKey
9	RFU	FF	N/A

Table 80: DF_DS Access conditions table

Byte Nr.	SM Condition	Value	Meaning
1..2	RFU	FF	Set to FFh
3	ENC UPDATE/APPEND (objects)	05	BSO_SM_Root_Kc
4	SIG UPDATE/APPEND (objects)	04	BSO_SM_Root_Ka
5..12	RFU	FF	Set to FFh
13	ENC ADMIN	05	BSO_SM_Root_Kc
14	SIG ADMIN	04	BSO_SM_Root_Ka
15	ENC CREATE	05	BSO_SM_Root_Kc
16	SIG CREATE	04	BSO_SM_Root_Ka
17..24	RFU	FF	Set to FFh

Table 81: DF_DS SM description