Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Carta Nazionale dei Servizi
CNS

File System

CRONOLOGIA DELLE VERSIONI	
Num. versione	**Sintesi delle variazioni**
01	Prima emissione 28 Gennaio 2005
02	Seconda emissione 25 febbraio 2005
03	Terza emissione 11 marzo 2005
04	Quarta emissione 1 aprile 2005
05	Quinta emissione 4 aprile 2005
06	Sesta emissione 25 maggio 2005
07	Settima emissione 30 settembre 2005
08	Ottava emissione 21 novembre 2005
09	Nona emissione 16 dicembre 2013
10	Decima emissione 10 giugno 2016

VERSIONE	MODIFICA
09	Eliminati limiti divulgativi del documento Utilizzo componente firma digitale attraverso applet Java
10	Inserito il paragrafo 6 per l'applicazione DPCM 18 gennaio 2016 afferente il Modello AT elettronico

INDICE DEI CONTENUTI

1 SCOPO DEL DOCUMENTO

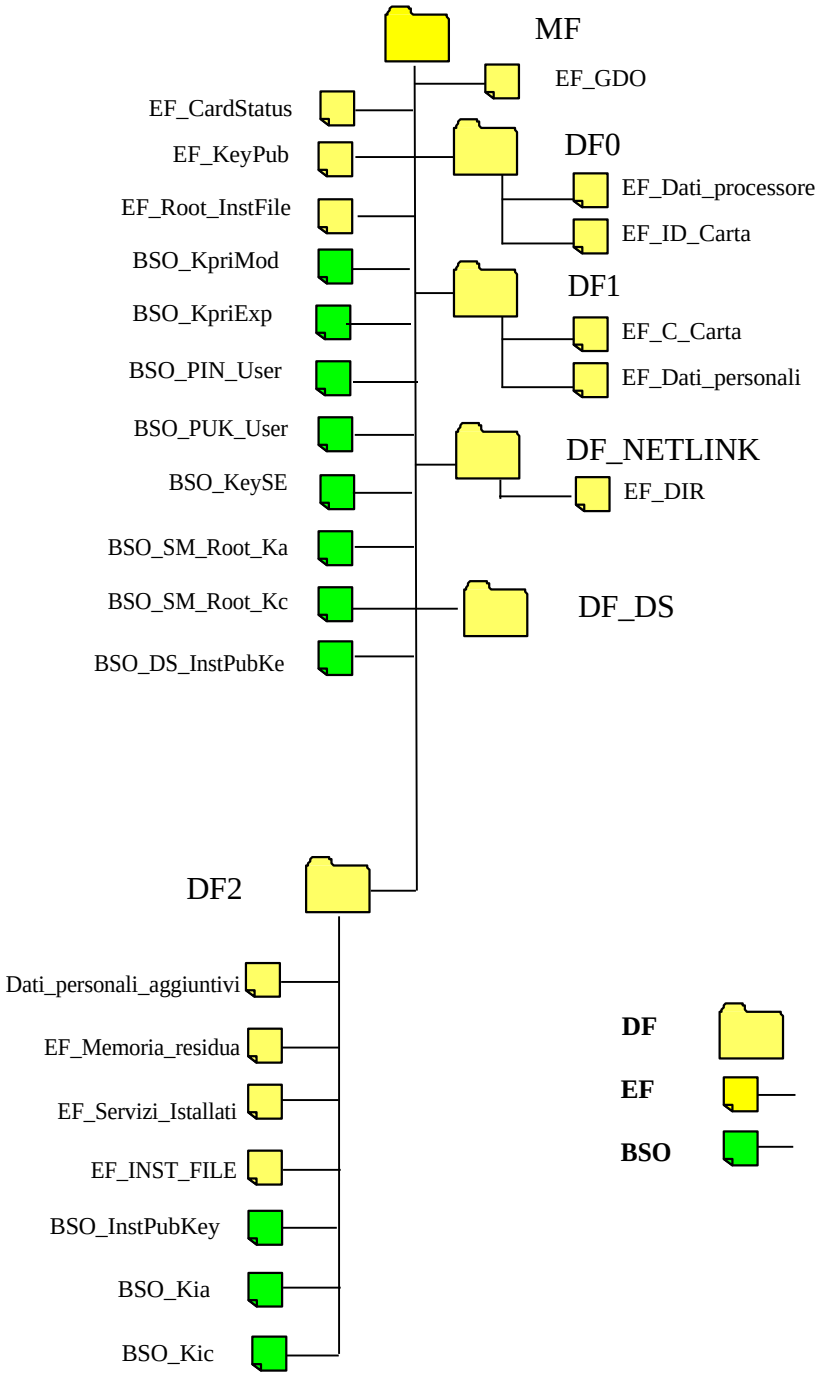
Questo documento contiene le specifiche del File System da adottare per la realizzazione di una Carta Nazionale dei servizi ai sensi del decreto 9 dicembre 2004 “Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale dei Servizi” ed in particolare ne definisce:

- L’organizzazione, specificando i vari elementi che lo compongono e le relazioni gerarchiche che tra essi intercorrono;
- La struttura, definendo gli identificativi dei file e degli oggetti di sicurezza;
- Le condizioni di accesso;
- Le condizioni di utilizzo del Security Messaging.

2 IL FILE SYSTEM

Nei paragrafi successivi è fornita l'organizzazione del File System della carta CNS e sono specificati gli identificativi dei singoli "file" (DF ed EF) e degli oggetti di sicurezza (BSO). Inoltre sono fornite le condizioni di accesso e di utilizzo per la smart card.

2.1 Organizzazione del File System



2.2 Specifiche della struttura del File System

Carta Nazionale dei Servizi - CNS						
File/Object Name	**Parent**	**Description**	**FID/ID (hex)**	**Type**	**Algorithm**	**Net Size**
MF	**----**	**Root**	**3F00**	**DF**		
EF.GDO		Netlink description file	2F02	EF_T		105
BSO_KpriMod		Authentication Private Key Modulus	2001	BSO_RSA_PRI	RSA_PURE(0Ch)	128
BSO_KpriExp		Authentication Private Key Exponent	2101	BSO_RSA_PRI	RSA_PURE(0Ch)	128
BSO_PIN_USR		User PIN	10	BSO_PIN		8
BSO_PUK_USR		Unblocks the User PIN	11	BSO_PIN		8
BSO_KeySE		Security Environment Key	0003	BSO_SE		6
EF_KeyPub		Authentication Public Key	3F01	EF_TLV		300
BSO_SM_Root_Ka		SM Authentication Key for DS installation	0004	BSO_SM	3DES-24 auth	24
BSO_SM_Root_Kc		SM Confidentiality Key for DS installation	0005	BSO_SM	3DES-24 cypher	24
EF_Root_InstFile		RootKIC|RootKIA cyphered with DS_Inst_CypherPub	0405	EF_T		128
EF_CardStatus		Mantains the card status – filled with 00h	3F02	EF_T		20
BSO_DS.InstPubKeyMod		Authentication key to install the DS service	0003	BSO_RSA_PUB		128
BSO_DS.InstPubKeyExp		Authentication key to install the DS service	0103	BSO_RSA_PUB		3
DF0	***MF***	***Card description data***	***1000***	DF		
EF.Dati_processore		Chip Data	1002	EF_T		54
EF.ID_Carta		Card Serial Number	1003	EF_T		16
DF1	***MF***	***Cardholder data***	***1100***	DF		
EF.C_Carta		Cardholder Certificate	1101	EF_T		2.048
EF.Dati_personali		Cardholder data	1102	EF_T		400
DF.NETLINK A000000073	***MF***	***DF Netlink***	***D000***	DF		
EF.DIR		Netlink Dir File	2F00	EF_T		22
EF.NETLINK		Netlink pointers	D002	EF_T		65
EF.NETKITA		National pointers	D004	EF_T		30
EF.NKCF		Card free data	D003	EF_T		64
DF.NKAF	***DF.NETLINK***		***D100***	**DF**		
EF.NKAF		**Administrative free data**	**D101**	**EF_T**		**700**
BSO_NKAF_KEY_W		**Authentication key**	**04**	**BSO_Auth**	**3DES 16**	**16**
DF.NKEF	***DF.NETLINK***		***D200***	**DF**		
EF.NKEF		**Emergency free data**	**D201**	**EF_T**		**2.000**
BSO_NKEF_KEY_W		**Authentication key**	**04**	**BSO_Auth**	**3DES 16**	**16**
DF.NKAP	***DF.NETLINK***		***D300***	**DF**		
EF.NKAP		**Administrative protected data**	**D301**	**EF_T**		**1.200**
BSO_NKAP_KEY_W		**Authentication key**	**04**	**BSO_Auth**	**3DES 16**	**16**
BSO_NKAP_KEY_R		**Authentication key**	**02**	**BSO_Auth**	**3DES 16**	**16**
BSO_Test_NKAP_R		**NKAP_KEY_R or PIN**	**06**	**BSO_Auth**		**16**
DF.NKEP	***DF.NETLINK***		***D400***	**DF**		
EF.NKEP		**Emergency protected data**	**D401**	**EF_T**		**2.000**
BSO_Test_NKEP_R		**NKEP_KEY_R or PIN**	**06**	**BSO_Auth**		**16**
BSO_Test_NKEP_W		**NKEP_KEY_W and PIN**	**05**	**BSO_Auth**		**16**
BSO_NKEP_KEY_W		**Authentication key**	**04**	**BSO_Auth**	**3DES 16**	**16**
BSO_NKEP_KEY_R		**Authentication key**	**02**	**BSO_Auth**	**3DES 16**	**16**
DF.NKPP	***DF.NETLINK***		***D500***	**DF**		
EF.NKPP		**Pointers protected data**	**D501**	**EF_T**		**100**
BSO_NKPP_KEY_W		**Authentication key**	**04**	**BSO_Auth**	**3DES 16**	**16**
BSO_NKPP_KEY_R		**Authentication key**	**02**	**BSO_Auth**	**3DES 16**	**16**
BSO_Test_NKPP_R		**NKPP_KEY_R or PIN**	**06**	**BSO_Auth**		**16**
DF_DS	***MF***	***Digital Signature DF***	***1400***	**DF**		**112**

DF2	*MF*	*Additional Services*	*1200*	DF		
EF.Dati_personali_aggiuntivi		filled with 00h	1201	EF_T		100
EF.Memoria_residua		Value= 4800h (18kb) SPAZIO LIBERO TOTALE	1202	EF_T		2
EF.Servizi installati		filled with 00h	1203	EF_T		160
EF.INST FILE		KIC|KIA ciphered with InstCypherPub	4142	EF_T		128
BSO_InstPubKeyMod		Authentication key to load additional services	0003	BSO_RSA_PUB		128
BSO_InstPubKeyExp		Authentication key to load additional services	0103	BSO_RSA_PUB		3
BSO_Kia		SM Authentication Key for additional services	01	BSO_SM	3DES-24 auth	24
BSO_Kic		SM Confidentiality Key for additional services	02	BSO_SM	3DES-24 cypher	24

2.3 Condizioni di accesso a DF ed EF

	Access Conditions: DF						Access Conditions: EF					
File/Object Name	Update	Append	Deactivate	Activate	Admin	Create	Read	Update	Append	Deactivate	Activate	Admin
MF	**nev**	**nev**	**nev**	**nev**	**nev**	**Nev**						
EF.GDO							alw	nev	nev	nev	nev	nev
BSO_KpriMod												
BSO_KpriExp												
BSO_PIN_USR												
BSO_PUK_USR												
BSO_KeySE												
EF_KeyPub							alw	nev	nev	nev	nev	nev
BSO_SM_Root_Ka												
BSO_SM_Root_Kc												
EF_Root_InstFile							alw	alw	nev	nev	nev	nev
EF_CardStatus							alw	PIN_USR	nev	nev	nev	nev
BSO_DS.InstPubKeyMod												
BSO_DS.InstPubKeyExp												
DF0	***nev***	***nev***	**nev**	**nev**	***Nev***	***Nev***						
EF.Dati_processore							alw	nev	nev	nev	nev	nev
EF.ID_Carta							alw	nev	nev	nev	nev	nev
DF1	***nev***	***nev***	**nev**	**nev**	***Nev***	***Nev***						
EF.C_Carta							alw	nev	nev	nev	nev	nev
EF.Dati_personali							alw	nev	nev	nev	nev	nev
DF.NETLINK A000000073	***nev***	***Nev***	**nev**	**nev**	***Nev***	***Nev***						
EF.DIR							alw	nev	nev	nev	nev	nev
EF.NETLINK							alw	nev	nev	nev	nev	nev
EF.NETKITA							alw	nev	nev	nev	nev	nev
EF.NKCF							alw	nev	nev	nev	nev	nev
DF.NKAF	***nev***	***nev***	**nev**	**nev**	***nev***	***nev***						
EF.NKAF							alw	NKAF_KEY_W	nev	nev	nev	nev
BSO_NKAF_KEY_W												
DF.NKEF	***nev***	***nev***	**nev**	**nev**	***nev***	***nev***						
EF.NKEF							alw	NKEF_KEY_W	nev	nev	nev	nev
BSO_NKEF_KEY_W												
DF.NKAP	***nev***	***nev***	**nev**	**nev**	***nev***	***nev***						
EF.NKAP							Test_NKAP_R	NKAP_KEY_W	nev	nev	nev	nev
BSO_NKAP_KEY_W												
BSO_NKAP_KEY_R												
BSO_Test_NKAP_R												
DF.NKEP	***nev***	***nev***	**nev**	**nev**	***nev***	***nev***						
EF.NKEP							Test_NKEP_R	Test_NKEP_W	nev	nev	nev	nev
BSO_Test_NKEP_R												
BSO_Test_NKEP_W												
BSO_NKEP_KEY_W												
BSO_NKEP_KEY_R												
DF.NKPP	***nev***	***nev***	**nev**	**nev**	***nev***	***nev***						
EF.NKPP							Test_NKPP_R	NKPP_KEY_W	nev	nev	nev	nev
BSO_NKPP_KEY_W												

BSO_NKPP_KEY_R												
BSO_Test_NKPP_R												
DF_DS	**DSInstPubKey**	**DSInstPubKey**	**nev**	**nev**	**DSInstPubKey**	**DSInstPubKey**						
DF2	alw	alw	**nev**	**nev**	alw	**InstPubKey**						
EF.Dati_personali_aggiuntivi							alw	nev	nev	nev	nev	nev
EF.Memoria_residua							alw	alw	nev	nev	nev	nev
EF.Servizi istallati							alw	alw	nev	nev	nev	nev
EF.INST FILE							alw	alw	nev	nev	nev	nev
BSO_InstPubKeyMod												
BSO_InstPubKeyExp												
BSO_Kia												
BSO_Kic												

2.4 Condizioni di utilizzo BSO

	Access Conditions: BSO			
File/Object Name	**Use**	**Change**	**Unblock**	**GenKeyPair**
MF				
EF.GDO				
BSO_KpriMod	PIN_USR	nev	nev	nev
BSO_KpriExp	PIN_USR	nev	nev	nev
BSO_PIN_USR	alw	PIN_USR	PUK_USR	nev
BSO_PUK_USR	alw	nev	nev	nev
BSO_KeySE	alw	alw	nev	nev
EF_KeyPub				
BSO_SM_Root_Ka	alw	alw	nev	nev
BSO_SM_Root_Kc	alw	alw	nev	nev
EF_Root_InstFile				
EF_CardStatus				
BSO_DS.InstPubKeyMod	alw	nev	nev	nev
BSO_DS.InstPubKeyExp	alw	nev	nev	nev
DF0				
EF.Dati_processore				
EF.ID_Carta				
DF1				
EF.C_Carta				
EF.Dati_personali				
DF.NETLINK A000000073				
EF.DIR				
EF.NETLINK				
EF.NETKITA				
EF.NKCF				
DF.NKAF				
EF.NKAF				
BSO_NKAF_KEY_W	alw	nev	nev	nev
DF.NKEF				
EF.NKEF				
BSO_NKEF_KEY_W	alw	nev	nev	nev
DF.NKAP				
EF.NKAP				
BSO_NKAP_KEY_W	alw	nev	nev	nev
BSO_NKAP_KEY_R	alw	nev	nev	nev
BSO_Test_NKAP_R	alw	nev	nev	nev
DF.NKEP				
EF.NKEP				
BSO_Test_NKEP_R	alw	nev	nev	nev
BSO_Test_NKEP_W	alw	nev	nev	nev

BSO_NKEP_KEY_W	alw	nev	nev	nev
BSO_NKEP_KEY_R	alw	nev	nev	nev
DF.NKPP				
EF.NKPP				
BSO_NKPP_KEY_W	alw	nev	nev	nev
BSO_NKPP_KEY_R	alw	nev	nev	nev
BSO_Test_NKPP_R	alw	nev	nev	nev
DF_DS				
DF2				
EF.Dati_personali_aggiuntivi				
EF.Memoria_residua				
EF.Servizi istallati				
EF.INST FILE				
BSO_InstPubKeyMod	alw	nev	nev	nev
BSO_InstPubKeyExp	alw	nev	nev	nev
BSO_Kia	alw	alw	nev	nev
BSO_Kic	alw	alw	nev	nev

2.5 Secure Messaging

	SM Conditions: DF			SM Conditions: EF					SM Conditions: BSO	
	blank means no SM			blank means no SM					blank means no SM	
File/Object Name	**Upd/Append**	**Admin**	**Create**	**Read OUT**	**Update**	**Append**	**Admin**	**Read IN**	**Use IN**	**Change**	**Unblock**
MF	**nev**	**nev**	**nev**								
EF.GDO											
BSO_KpriMod											
BSO_KpriExp											
BSO_PIN_USR											
BSO_PUK_USR											
BSO_KeySE											
EF_KeyPub											
BSO_SM_Root_Ka										SIG:SM_Root_Ka ENC:SM_Root_Kc	
BSO_SM_Root_Kc										SIG:SM_Root_Ka ENC:SM_Root_Kc	
EF_Root_InstFile					SIG:SM_Root_Ka ENC:SM_Root_Kc						
EF_CardStatus											
BSO_DS.InstPubKeyMod											
BSO_DS.InstPubKeyExp											
DF0											
EF.Dati_processore											
EF.ID_Carta											
DF1											
EF.C_Carta											
EF.Dati_personali											
DF.NETLINK A000000073											
EF.DIR											
EF.NETLINK											
EF.NETKITA											
EF.NKCF											
DF.NKAF											
EF.NKAF											
BSO_NKAF_KEY_W											
DF.NKEF											
EF.NKEF											
BSO_NKEF_KEY_W											
DF.NKAP											
EF.NKAP											
BSO_NKAP_KEY_W											
BSO_NKAP_KEY_R											
BSO_Test_NKAP_R											
DF.NKEP											
EF.NKEP											
BSO_Test_NKEP_R											
BSO_Test_NKEP_W											

BSO_NKEP_KEY_W											
BSO_NKEP_KEY_R											
DF.NKPP											
EF.NKPP											
BSO_NKPP_KEY_W											
BSO_NKPP_KEY_R											
BSO_Test_NKPP_R											
DF_DS	**SIG: SM_Root_Kia ENC:SM_Root_Kic**	**SIG: SM_Root_Kia ENC:SM_Root_Kic**	**SIG: SM_Root_Kia ENC:SM_Root_Kic**								
DF2	**SIG: SM_Kia ENC:SM_Kic**	**SIG: SM_Kia ENC:SM_Kic**	**SIG: SM_Kia ENC:SM_Kic**								
EF.Dati_personali_aggiuntivi											
EF.Memoria_residua					SIG:SM_Kia ENC:SM_Kic						
EF.Servizi istallati					SIG:SM_Kia ENC:SM_Kic						
EF.INST FILE					SIG:SM_Kia ENC:SM_Kic						
BSO_InstPubKeyMod											
BSO_InstPubKeyExp											
BSO_Kia										SIG:SM_Kia ENC:SM_Kic	
BSO_Kic										SIG:SM_Kia ENC:SM_Kic	

3 ANSWER TO RESET

Le informazioni seguenti sono dedotte, a titolo di esempio, dal Progetto SISS (Sistema Informativo Socio Sanitario) della Regione Lombardia.
Tali informazioni devono essere modificate in base al contesto specifico e in particolare al fornitore della maschera e del chip della smart card.
Qualora la pubblica amministrazione emittente si avvalga di due o più fornitori per la realizzazione della CNS, la risposta al reset è differenziata in funzione del produttore della maschera e del produttore del chip. Inoltre la CNS contiene informazioni sanitarie secondo le specifiche Netlink e quindi adotta le chiavi di gruppo del Ministero della Salute e la risposta al reset reca informazioni sul set di chiavi adottato per l'emissione della carta.
Di seguito, a titolo esemplificativo e non esaustivo, vengono riportati i due ATR relativi ai fornitori di CNS della Regione Lombardia.
Si ricorda che un ATR che non contiene il riferimento alla CNS deve causare un rifiuto funzionale da parte delle applicazioni che utilizzano la smart card.

3.1 ATR relativo alle Carte cittadino emesse

3B.xF.xx.x1.31.xx.xx

.00	HB – Historical bytes (15)
.6B	TPI
.xx	ICM – IC manufacturer (ISO)
.0y	ICT – Mask manufacturer (CNS)
.xxxx	OSV – Operating system version (2 bytes)
.01	DD1 – ATR coding version
.11	DD2 – Netlink card type
.01	DD3 – Certification tag
.43	DD4 – 'C'
.4E	DD5 – 'N'
.53	DD6 – 'S'
.(valore ≥ 10)	DD7 – Application version
.3180	CPDO – Direct application selection
.xx	TCK – Check character

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
3B	**FF**	**18**	**00**	**FF**	**C1**	**0A**	**31**	**FE**	**55**	**00**	**6B**	**05**	**08**	**C8**	**05**	**01**	**11**	**01**	**43**	**4E**	**53**	**10**	**31**	**80**	**0C**
TS	T0	TA1	TB1	TC1	TD1	TC2	TD2	TA3	TB3	H1	H2	H3	H4	H5	H6	H7	H8	H9	H10	H11	H12	H13	H14	H15	TCK

ATR PDC MI1 Reale - Infineon/Siemens

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
3B	**FF**	**18**	**00**	**FF**	**81**	**31**	**FE**	**55**	**00**	**6B**	**02**	**09**	**02**	**00**	**01**	**11**	**01**	**43**	**4E**	**53**	**11**	**31**	**80**	**8F**
TS	T0	TA1	TB1	TC1	TD1	TD2	TA3	TB3	H1	H2	H3	H4	H5	H6	H7	H8	H9	H10	H11	H12	H13	H14	H15	TCK

ATR PDC MI1 Reale - ST/Incard

4 CONTENUTO DELLA CNS

4.1 DF Netlink

Il contenuto del DF relativo a Netlink e dei relativi EF, non evidenziato nel presente documento, è conforme alle specifiche elencate nel seguito:

- NK/4/FNS/T/3/1.1 Specifiche PDC
- NK/4/FNS/T/4/1.9 Dati PDC
- NK/4/FNS/T/21/1.11 Serial Number delle Carte Sanitarie e successive versioni

4.2 ID_Carta

Rappresentazione ASCII ed esadecimale del contenuto del File EF_ID_Carta, conforme alle raccomandazioni Netlink. A titolo esemplificativo e non esaustivo si riporta di seguito l'ID_Carta utilizzato nelle CNS emesse dalla Regione Lombardia nell'ambito del Progetto SISS.

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	***Byte***
6	**0**	**3**	**0**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**0**	**x**	**ASCII**
36	**30**	**33**	**30**	**3x**	**3x**	**3x**	**3x**	**3x**	**3x**	**3x**	**3x**	**3x**	**3x**	**30**	**3x**	**HEX**
				Numero progressivo									**CD1**			

CD1: check digit dei precedenti 9 byte calcolato secondo la Luhn formula;
CD2: check digit dei precedenti 15 byte calcolato secondo la Luhn formula (per omogeneità con le raccomandazioni Netlink);
Byte1: identifica il tipo di carta (cittadino reale) e il livello di distribuzione (regionale);
Byte 2,3,4: 030 codice Regione Lombardia;
Byte 5: se la CNS è anche una Tessera Sanitaria Nazionale il valore di tale byte deve essere maggiore o uguale a 1.

4.3 ALTRI EF

EF.Dati_Personali – il file è conforme al Decreto 9 dicembre 2004 “Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della carta nazionale dei servizi”.

Dettagli sulla struttura sono riportati nel documento del Centro Nazionale per l’informatica nella pubblica amministrazione “LINEE GUIDA PER L’EMISSIONE E L’UTILIZZO DELLA CARTA NAZIONALE DEI SERVIZI”.

EF.Dati_personali_aggiuntivi – l’intero contenuto è posto a ‘00’hex

EF.CardStatus – l’intero contenuto è posto a ‘00’hex

EF.ServiziInstallati – l’intero contenuto è posto a ‘00’hex

EF.INST FILE – contiene le chiavi utilizzate per installare i servizi aggiuntivi:
$RSA_{InstPubKey}$(KIC | KIA), con padding BT02.

EF.Memoria_residua – impostato con il valore della memoria rimanente

EF.Dati_processore – contiene dati di tracciabilità del chip a cura del produttore.

EF.ID_Carta – contiene il Serial Number della carta (16 caratteri ASCII).

4.4 CERTIFICATO DI AUTENTICAZIONE

Il certificato di autenticazione consiste nell'attestato elettronico che assicura l'autenticità delle informazioni necessarie per l'identificazione in rete del titolare della carta nazionale dei servizi.
Il formato del certificato di autenticazione è conforme allo standard ISO/9594-8 (X.509).
Il *Common name* nel certificato deve avere la seguente struttura:

> *codicefiscale/idcarta.hash(ef_dati_personali)*
> dove *idcarta* è il *Serial Number* (16 caratteri ASCII) della carta.

Per *hash(ef_dati_personali)* vanno considerati solo i caratteri utili (escludendo quindi la parte finale riempita a '00'hex), così come appaiono nel file.

5 LA TECNOLOGIA JAVA E LA FIRMA DIGITALE

Le specifiche della Carta Nazionale dei Servizi risalgono ad un periodo durante il quale la tecnologia Java non si era ancora affermata nelle smart card. Ciononostante, le "Linee guida CNS" emesse nel 2006, già prevedevano che le smartcard potessero utilizzare la tecnologia java, chiarendo che "*una CNS REALIZZATA CON TECNOLOGIA java card offre dunque "più gradi di libertà" alle Amministrazioni*".
Il rispetto del cosiddetto set minimo di APDU [1] può essere fondamentale per la gestione e fruizione dei "servizi aggiuntivi", eventualmente per le funzionalità di autenticazione in rete attraverso la CNS, non anche per la generazione della firma digitale. La firma digitale, infatti, è generata localmente, attraverso il middleware fornito con la carta (PKCS#11 e CSP).
L'utilizzo delle chiavi crittografiche, le modalità di accesso e protezione delle stesse, sono gestite dal middleware.
Anche con le Java card, per utilizzare dette funzionalità è utilizzato un apposito middleware *(PKCS#11 e CSP)*, fornito dal produttore delle stesse. In questo caso le chiavi non si trovano all'interno di un file dedicato, ma all'interno di un applet dedicato a tale scopo.

In considerazione dell'evoluzione tecnologica delle smartcard basate su tecnologia Java, della possibilità di garantire l'assenza di conseguenze in termini di usabilità, nulla osta che si utilizzi un applet dedicato per la firma digitale alle seguenti condizioni:

1. L'applet deve essere dedicato alla firma digitale;
2. L'applet deve essere certificato quale dispositivo sicuro, *nell'ambiente che la ospita,* per la generazione della firma conforme all'allegato III della Direttiva 1999/93/EU;
3. L'applet deve quantomeno consentire attraverso il middleware la generazione delle chiavi crittografiche necessarie, la generazione di richieste di certificati PKCS#10, la generazione della firma digitale, il caricamento del certificato qualificato, la gestione del PIN, la visualizzazione dei certificati presenti, le funzionalità di blocco a fronte di un determinato numero di inserimenti errati del PIN;
3. Il middleware fornito, che deve essere liberamente e gratuitamente utilizzabile, deve consentire l'accesso e la fruibilità delle funzionalità di cui al punto precedente;
4. L'applet di firma deve essere istanziata tramite il processo di "Installation" effettuato in fase di pre-personalizzazione o personalizzazione e attivata tramite selezione da parte del middleware crittografico.
5. Qualora la componente CNS non sia nativa ma anch'essa realizzata tramite applet, questa deve possedere i privilegi di selezione e quindi essere automaticamente selezionata al reset.

Alle condizioni elencate, è quindi consentito utilizzare un applet dedicato ad ospitare le informazioni per la firma digitale in alternativa alla modalità classica che prescrive l'uso di un file dedicato (DF/DS) a tale scopo. La struttura del file system deve comunque rispettare quanto previsto al paragrafo 2.1, pertanto, il file DF_DS deve comunque essere presente, sebbene non ospiti le informazioni necessarie alla firma digitale.
L'applet java fornisce funzionalità e sicurezza necessarie per la firma digitale, il middleware deve rendere trasparente l'uso di tutte le funzioni necessarie per dotare la CNS della firma digitale e garantirne la fruibilità.

[1] Pubblicate con il documento CNS – Carta Nazionale dei Servizi Functional Specification

Inizializzazione della firma digitale

L'inizializzazione della firma digitale deve essere conforme a quanto attualmente realizzato dagli Enti emettitori delle CNS e pertanto devono essere previste le seguenti quantità generate durante il processo di emissione:

- "BSO_SM_Root_Ka e BSO_SM_Root_Kc" che condizionano almeno la generazione della coppia di chiavi di sottoscrizione; questi oggetti di sicurezza devono contenere chiavi 3DES diversificate con il numero seriale della CNS (Id_carta); possono essere contenuti nell'Applet di firma Digitale;
- EF_Root_InstFile che contiene le chiavi dei precedenti oggetti di sicurezza crittografate con la chiave pubblica dell'ente emettitore; questo file deve essere contenuto nella componente CNS a livello di root;
- BSO_DS_InstPubKeyMod e BSO_DS_InstPubKeyExp che contengono la chiave pubblica dell'Ente emettitore dedicata all'autenticazione esterna; questi oggetti di sicurezza possono essere contenuti nella componente CNS a livello di root, in questo caso non condiziona l'accesso a nessun componente dell'Applet di firma ma consente all'Ente emettitore accertarsi di interagire con una propria carta.

6 USO DELLE CHIAVI CRITTOGRAFICHE RSA A 2048 BIT NEI MODELLI AT ELETTRONICI

Le modifiche apportate al DPCM 24 maggio 2010 (recante le "*Regole tecniche delle Tessere di riconoscimento (mod. AT) di cui al D.P.R. n. 851 del 1967 rilasciate con modalità elettronica dalle Amministrazioni dello Stato, ai sensi dell'articolo 66, comma 8, del decreto legislativo n. 82 del 2005*") dal DPCM 18 gennaio 2016 fissano a 10 anni la durata del modello AT elettronico, disponendo che i certificati di autenticazione siano basati su chiavi RSA con lunghezza di 2048 bit.
Tale scelta scaturisce dalla necessità di evitare un fondato rischio di compromissione delle chiavi crittografiche durante il periodo di validità prescritto.
Si prevede che, all'attuale tasso di crescita della capacità di elaborazione, le chiavi RSA a 2048 bit possano rimanere sufficientemente sicure fino al 2030, pertanto è logica la scelta del legislatore di imporre l'uso di chiavi di tale lunghezza.
In considerazione di ciò, visto che per l'emissione del modello AT elettronico trovano applicazione le presenti specifiche tecniche afferenti la CNS, è necessario un aggiornamento per consentire l'utilizzo di chiavi RSA a 2048 bit, sia per l'autenticazione che per la firma digitale, ove presente.
L'aggiornamento delle specifiche funzionali CNS nell'ottica di normare l'utilizzo di chiavi almeno a 2048 bit è in corso ma è piuttosto complesso, poiché mentre la specifica funzionale per l'uso di chiavi a 1024 è essenzialmente già contenuta nell'ISO 7816, e costituisce un sottoinsieme di essa, l'uso di chiavi a 2048 bit impone delle scelte non univoche in termini di gestione di dati la cui lunghezza eccede quella esprimibile con un singolo byte. Ciò impatta non solo la gestione del singolo comando APDU, per il quale esistono estensioni standard ISO come il command chaining o le APDU estese, ma anche le strutture dati usate per memorizzare le quantità di sicurezza, come il TLV. Le soluzioni presenti sul mercato al mese di giugno 2016, infatti, utilizzano sistemi eterogenei per superare questi limiti.
Un'ulteriore considerazione riguarda l'utilizzo delle chiavi di autenticazione, soprattutto nell'ottica dei requisiti di interoperabilità che sono alla base delle specifiche funzionali CNS. L'autenticazione del client tramite certificato digitale ha uno scenario di applicazione che nella quasi totalità dei casi avviene durante l'uso di un'applicazione web in cui il software utilizzato lato client è un browser standard, che non ha una conoscenza specifica della tecnologia con la quale è conservata e utilizzata la chiave privata, ma demanda tale conoscenza a uno strato software intermedio (middleware), sia esso un CSP o un PKCS#11.
Un'applicazione che utilizza una CNS pertanto non richiede, di norma, l'accesso diretto alla chiave di autenticazione, quanto, più probabilmente, la lettura del file dei dati personali o l'accesso a specifici servizi aggiuntivi. Considerando che possono tuttavia essere stati sviluppati applicativi che accedono alle funzioni crittografiche senza utilizzare il middleware, si sta procedendo all'aggiornamento dei comandi APDU necessari allo scopo.
Stanti tali premesse, ritenendo indispensabile consentire da subito l'uso delle chiavi crittografiche della lunghezza prevista dal DPCM 18 gennaio 2016, si stabilisce che:

- L'uso della chiave di autenticazione a 2048 bit sulla CNS può avvenire con modalità specifiche del chip;
- Gli oggetti necessari per la gestione di tale chiave e relativo certificato possono essere inseriti nella parte del file system CNS non normato dalla presente specifica (es.: DF_DS, un DF dedicato o un applet). In tal caso gli oggetti del file system CNS EF_KeyPub, EF_C_Carta, BSO.KPri sono sostituiti dagli omologhi oggetti nei DF di cui sopra, garantendo equivalenti livelli di sicurezza;

- L’uso delle chiavi deve essere gestito dal middleware messo a disposizione dal fornitore, eventualmente anche attraverso comandi APDU non definiti nelle CNS functional specifications;
- Il middleware deve essere reso gratuitamente disponibile per lo sviluppo di applicazioni che interagiscono con le smartcard e ai titolari delle smartcard congiuntamente ad una procedura che ne consenta una semplice installazione;

Il middleware deve permettere la generazione della chiave crittografica di autenticazione, la generazione di richieste di certificati PKCS#10, la generazione della firma elettronica, il caricamento del certificato a bordo del *chip*.
Il middleware deve consentire il processo di autenticazione del client tramite i browser più diffusi.
Deve essere garantito l’uso della chiave di firma digitale non solo tramite il PKCS#11, ma anche attraverso i servizi CSP.