S.I.A.E. Card

File System Specification

Document Version 1.0.5b

INDICE

1. Document Revision History

Version	Date	Subject	Issued by	Authorized by
1.0.0 (DRAFT)	Apr. 29, 2002	Edizione	L.Consiglio	A. Scognamiglio
1.0.1 (DRAFT)	Mag. 29, 2002	Modifiche al file system concordate con SIAE il 21/5/2002	A. Scognamiglio	A. Scognamiglio
1.0.2	Giu. 03, 2002	Consolidamento delle specifiche secondo quanto concordato con mail SIAE del 03/06	A. Scognamiglio	A.Scognamiglio
1.0.3	Giu. 05, 2002	Consolidamento delle specifiche secondo quanto concordato con mail SIAE del 04/06. In particolare condizioni never su private Keys, ridefinizione atr, inserimento dei file card info e label.	A. Scognamiglio	A.Scognamiglio
1.0.4	Giu. 11,2002	Correzione dimensione file atr	A. Scognamiglio	A. Scognamiglio
1.0.5	Lug. 16,2002	Revisione Contenuto file	L.Consiglio	A.Scognamiglio

		di attributi		
1.0.5b	Lug. 16,2002	Revisione per la distribuzione	L.Consiglio	A.Scognamiglio

2. Glossario

AC Access Condition

AID Application Identifier

Alg-ID Algorithm Reference

ALW Always

ASN.1 Abstract Syntax Notation One

ATR Answer-to-Reset

AUT Authentication

BCD Binary Coded Digit

BER Basic Encoding Rules

BSO Base Security Object (oggetti chiavi, PIN, PUK)

C Certificate

CA Certification Authority

CBC Cipher Block Chaining

CH Cardholder

CMS Card Management System

DER Distinguished Encoding Rules

3DES Data Encryption Standard, triple DES

DF Dedicated File

EF Elementary File

FCI File Control Information (Acces Condition dei file)

FID File Identifier

GDO Global Data Object

ICC Integrated Circuit(s) Card

ICCSN ICC Serial Number

ID Identifier

Key Cryptographic Key

KID Key ID

MAC Message Authentication Code

MF Master File

P11 PKCS#11

PIN Personal Identification Number

PKCS Public Key Cryptography Standards

PUK PIN Unblock

RC Retry Counter

RFC Request for Comment

RFU Reserved for future use

RND Random Number

RSA Algorithm of Rivest, Shamir, Adleman

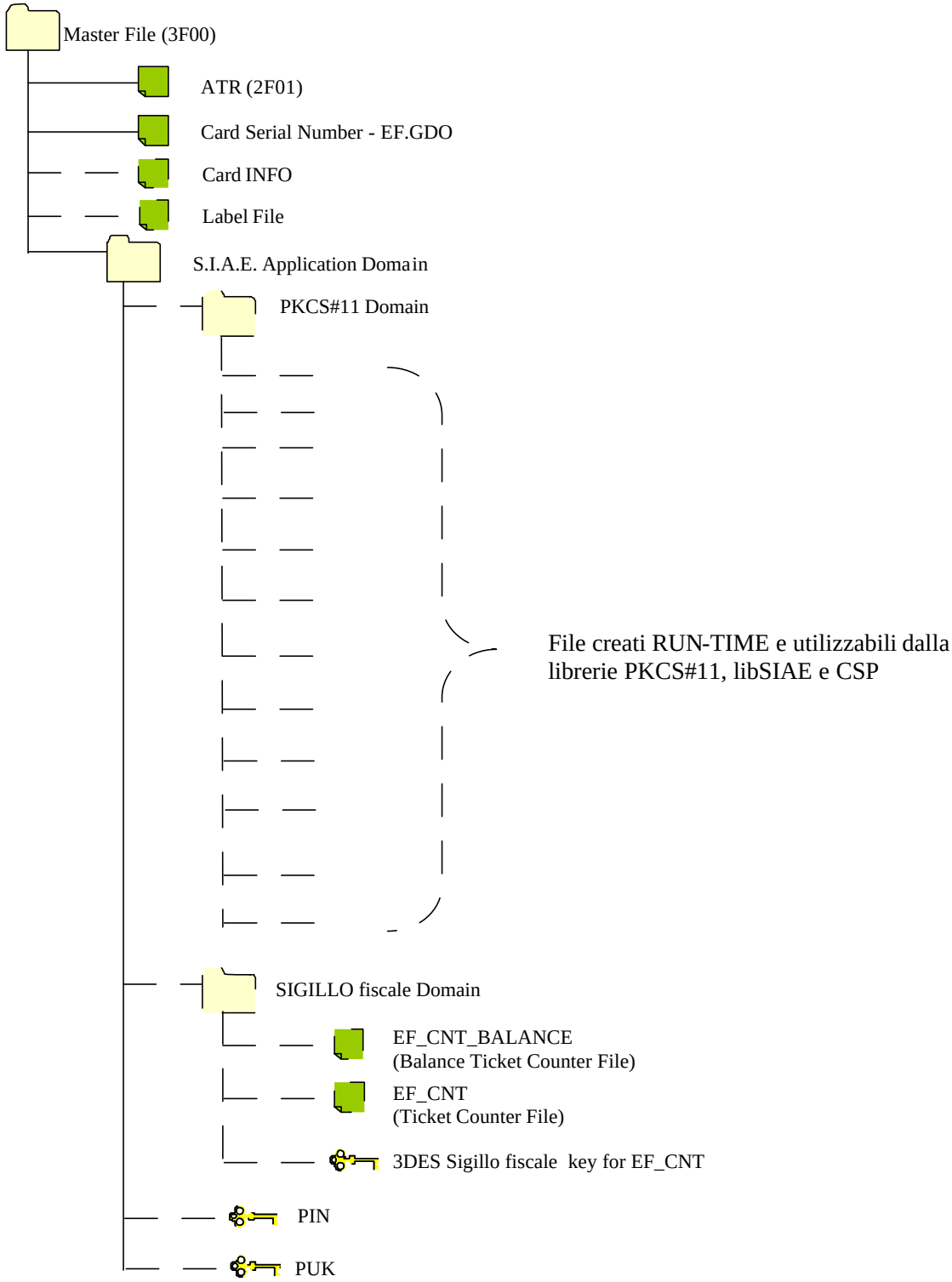
SE Security environment

TLV Tag-Length-Value

X.509 Public Certificate Standard

3. Struttura File System

La figura seguente mostra la struttura file system complessiva per la carta SIAE.



4. Master File (3F00)

Il Master File rappresenta la *root* della struttura file system della carta SIAE.

File Identifier: 3F00h
Type: MF
Presence: Mandatory
BodySize: All available capacity

Access Conditions (AC)

Access Condition	Value
Create files (AC_CREATE)	Never
Delete files (AC_DELETE)	Never
Append BSO (AC_APPEND)	Never
Update BSO (AC_UPDATE)	Never
Admin FCI (AC_ADMIN)	Never

4.1 ATR (2F01)

L'ATR (Answer To Reset) è il file dal quale la carta legge i byte da fornire in risposta ad un comando di reset. E' un dato personalizzato dal produttore.

File Identifier: 2F01
Type: Binary File
Presence: Mandatory
BodySize: 15h bytes

File Contents

Value	Symbol	Description
0x3B	TS	Direct Convention (Z = 1 and lsb first)

0xFB	T0	Codes Y1 and K. Y1 = 1111 TA1 present TB1 present TC1 present TD1 present K = 1011 (11 Historical bytes)
0x11	TA1	Standard Fi=1 Di=1
0x00	TB1	II = 00 PI1 = 00000 (Vpp not electrically connected to the card)
0xFF	TC1	N extra guard time N = 11111111 (255) see ISO 7816-4 p.12: the minimum delay between the leading edge od two consecutive chars is the same in both direction. 12 etu (T= 0) / 11 etu (T=1)
0x81	TD1	Y2 = 1000 TA2 not present TB2 not present TC2 not present TD2 present T = 0001 First offered protocol is T = 1
0x31	TD2	Y3 = 0011 TA3 present TB3 present TC3 not present TD3 not present T = 0001 Protocol T = 1
0x80	TA3	IFSC (Information Field Size Card)
0x55	TB3	BWICWI
0x00	T1	CI Category Indicator
0x68	T2	TPI (Tag Pre-issuing Data)
0x02	T3	ICM

0x00	T4	ICT
0x10	T5	OSV 1-st byte (Versione OS InCrypto34 V1.0)
0x10	T6	OSV 2-st byte (Versione Package SIAE V1.0)
0x53	T7	Ascii “S”
0x49	T8	Ascii “I”
0x41	T9	Ascii “A”
0x45	T10	Ascii “E”
0x00	T11	CLS (Card Life Cycle) default 0x00
0x04	TCK	Check Character

Control Access Conditions

Access Condition	**Value**
Read (AC_READ)	Always
Update (AC_UPDATE)	Never
Delete (AC_DELETE)	Never
Admin (AC_ADMIN)	Never

4.2 Card Serial Number File - EF.GDO - (2F02)

Il file binario EF.GDO (Global Data Object) contiene le informazioni relative al numero di serie del chip (traceability) e della carta (numero emesso dall’emettitore, SIAE). Tali informazioni sono codificate in TLV secondo la seguente specifica:

File Identifier: 2F02
Type: EF bynary
Presence: Mandatory
BodySize: 1Ah bytes

File Contents

Il Serial Number è un numero univoco di carta valorizzato come segue:

Byte#	**Field description**	**InitValue (HEX)/Value**

1	Tag (ICC_Traceability)	5A
2	Lunghezza (ICC_Traceability)	0D
3-8	ICC_Traceability	D2 76 00 00 00 00
9-15	ICC_ Traceability Number	Xx xx xx xx xx xx xx (Tale valore deve essere letto dall'output dei primi 7 byte del GET CARD TRACEABILITY COMMAND)
16-17	Tag (ICC_Card_Number)	5F 20
18	Lunghezza (ICC_Card_Number)	08
19-26	ICC_Card_Number	65 yy yy yy yy yy yy yy (tale valore è calcolato come un contatore progressivo unitario inizializzato a 1. yy è codificato in ASCII)[1]

Access Conditions

Access Condition	**Value**
Read (AC_READ)	Always
Update (AC_UPDATE)	Never
Delete (AC_DELETE)	Never
Admin (AC_ADMIN)	Never

4.2 Card Info - (2F03)

Il file binario Card Info contiene le informazioni relative all' applicazione per la quale la carta è stata emessa.

File Identifier: 2F03
Type: EF bynary
Presence: Mandatory
BodySize: 0Eh bytes

File Contents

Il File contiene la seguente stringa codificata in ASCII:

```
AE - SIAE CARD
```

[1] Per le carte di test il valore è il seguente "TEST000x" codificato in ASCII

Access Conditions

Access Condition	Value
Read (AC_READ)	Always
Update (AC_UPDATE)	Never
Delete (AC_DELETE)	Never
Admin (AC_ADMIN)	Never

4.2 Label - (5F0A)

Il file binario Label contiene le informazioni relative alla Label così come definita dallo standard PKCS#11.

File Identifier: 5F0A
Type: EF bynary
Presence: Mandatory
BodySize: 20h bytes

File Contents

Il File contiene la seguente stringa codificata in ASCII:

```
SysGillo
Il carattere di Fill è 00 hex
```

Access Conditions

Access Condition	Value
Read (AC_READ)	Always
Update (AC_UPDATE)	PIN
Delete (AC_DELETE)	Never
Admin (AC_ADMIN)	Never

5. SIAE Application Domain (0000)

Questa directory contiene l'applicazione SIAE. E' composta dal dominio PKCS#11 e dal dominio Sigillo fiscale.

File Identifier: 0000h
Type: DF
Presence: Mandatory
Body Size: max available capacity

Access Conditions (AC)

Access Condition	**Value**
Create files (AC_CREATE)	Never
Delete files (AC_DELETE)	Never
Append BSO (AC_APPEND)	Never
Update BSO (AC_UPDATE)	Never
Admin FCI (AC_ADMIN)	Never

5.1 PIN

Questo oggetto (BSO) contiene il PIN dell'utente finale, che consentirà all'utente di autenticarsi alla carta.

Key Identifier: 01h
Type: BSO PIN
Presence: Mandatory
Retry Counter:05h

BSO value

Tale BSO sarà creato in Incard con valore uguale per tutte le carte e sarà diversificato carta per carta dal CMS SIAE.

Init value (hex)	**Value (hex)**
31 32 33 34 35 36 37 38	XX…..XX

Access Conditions

Access Condition	Value
Verify (AC_USE)	Always
Change (AC_Change)	PIN
Reset Retry Counter (AC_Append)	PUK
GenKeyPair (AC_GENKEYPAIR)	Never

5.2 PUK

Questo oggetto (BSO) contiene il PUK della carta che consente di sbloccare la carta in caso di raggiungimento del numero massimo di tentativi errati di presentazione PIN.

Key Identifier: 02h
Type: BSO PIN
Presence: Mandatory
Retry Counter: 0Ah

BSO value

Tale BSO sarà creato in Incard con valore uguale per tutte le carte e sarà diversificato carta per carta dal CMS SIAE.

Init value (hex)	Value (hex)
38 37 36 35 34 33 32 31	XX…..XX

Access Conditions

Access Condition	Value
Verify (AC_USE)	Always
Change (AC_Change)	Never
Reset Retry Counter (AC_Append)	Never
GenKeyPair (AC_GENKEYPAIR)	Never

5.3 PKCS#11 Application Domain (1111)

Questa directory contiene gli oggetti PKCS#11.

File Identifier: 1111h
Type: DF
Presence: Mandatory
Body Size: max available capacity

Access Conditions (AC)

Access Condition	Value
Create files (AC_CREATE)	PIN
Delete files (AC_DELETE)	PIN
Append BSO (AC_APPEND)	PIN
Update BSO (AC_UPDATE)	Never
Admin FCI (AC_ADMIN)	Never

5.4 Sigillo Fiscale Domain (1112)

Questa directory contiene gli oggetti che implementano il sigillo fiscale.

File Identifier: 1112h
Type: DF
Presence: Mandatory
Body Size: max available capacity

Access Conditions (AC)

Access Condition	Value
Create files (AC_CREATE)	Never
Delete files (AC_DELETE)	Never
Append BSO	Never

(AC_APPEND)	
Update BSO (AC_UPDATE)	Never
Admin FCI (AC_ADMIN)	Never

5.4.1 3DES Sigillo Fiscale key for EF_CNT

Questo è il BSO 3DES CRYPT/DECRYPT. Tale chiave è utilizzata per il calcolo del Sisgillo Fiscale (lanciando il comando Increase with MAC computation).

Key Identifier: 03h
Type: BSO 3DES CRYPT/DECRYPT
Presence: Mandatory

BSO value

Tale BSO sarà creato in Incard con valore uguale per tutte le carte e sarà diversificato carta per carta dal CMS SIAE.

Init value (hex)	Value (hex)
38 37 36 35 34 33 32 31 38 37 36 35 34 33 32 31	XX…..XX

Access Conditions

Access Condition	Value
Verify (AC_USE)	PIN
Change (AC_Change)	Never
Reset Retry Counter (AC_Append)	Never
GenKeyPair (AC_GENKEYPAIR)	Never

5.4.2 Balance Ticket Counter File – EF_CNT_BALANCE (1001)

Il file di EF_CNT_BALANCE viene utilizzato come contatore di biglietti emessi in termini di saldo valorizzato in centesimi di EURO.

File Identifier: 1001
Type: EF Counter
Presence: Mandatory
BodySize: C8h bytes

File Contents

Il File sarà inizializzato a 0 in fase di personalizzazione in Incard.

Access Conditions

Access Condition	Value
Read (AC_READ)	Always
Update (AC_UPDATE)	Never
Delete (AC_DELETE)	Never
Admin (AC_ADMIN)	Never
Increase (AC_INCREASE)	PIN
Decrease (AC_DECREASE)	Never

5.4.3 Ticket Counter File EF_CNT (1000)

Il file di EF_CNT viene utilizzato come contatore di numero di biglietti emessi.

File Identifier: 1000
Type: EF Counter
Presence: Mandatory
BodySize: C8h bytes

File Contents

Il File sarà inizializzato a 0 in fase di personalizzazione in Incard.

Access Conditions

Access Condition	Value
Read (AC_READ)	Always
Update (AC_UPDATE)	Never
Delete	Never

(AC_DELETE)	
Admin (AC_ADMIN)	Never
Increase (AC_INCREASE)	PIN
Decrease (AC_DECREASE)	Never