Fig.1 (Smart card INCRIPTO 34)
(le nuove carte di test successivamente al 2009 sono identiche originali, graficamente a quelle non riportano più la scritta
Smart Card di Prova né Fac Simile)

Indice:

1. Scopo del documento

Scopo del seguente documento è quello di descrivere brevemente il contenuto delle Smart Card di test che SIAE rilascia per conto dell'Agenzia delle Entrate, al fine di poter provare il funzionamento dei Sistemi di Emissione Titoli d'Accesso. Qui di seguito si forniscono anche indicazioni sulle modalità d'uso del software a corredo e sulle modalità di accesso ai dati della SC (SmartCard).
Tale documento fornisce informazioni sul materiale fornito da produttore delle SmartCard. Si tratta di software in vari formati e di documentazione. Per evidenti motivi, tale materiale è passibile di correzioni ed integrazioni che saranno rese disponibili sul sito SIAE all'indirizzo:

https://online.siae.it/site/DownloadSoftware/erario.asp?link_page=DownloadSoftware/Erario_SIETA_SoftwareLicenze.htm&open_menu=yes&search=no&click_level=0900.0500.0800 al quale si raccomanda di fare riferimento.
Le integrazioni e correzioni verranno fornite in file separati indicanti la versione e/o la data di aggiornamento cui si riferiscono.

2. Descrizione fisica

La Smart Card al momento in uso è il modello INCRIPTO 34 (Smartcard MCU With Modular Arithmetic Processor & 34 KBytes High Density EEPROM) della InCard.

La descrizione del chip a bordo della carta con le caratteristiche e le specifiche è demandata all'apposito documento Bd19xl34.pdf

3. Differenze tra la SC di Test (prova) e quella distribuita ai Titolari.

Le differenze tra le SC di TEST (d'ora in poi SCT) e quelle effettivamente distribuite ai Titolari di biglietterie automatizzate, consistono nei seguenti punti:

- I certificati a bordo delle SCT sono di una CA SIAE di Test mentre a bordo delle carte d'attivazione definitive il certificato di firma è di un certificatore DigitPA.
- I dati a bordo delle SCT sono quelli del produttore di sistemi di emissione e non di un titolare di Biglietteria Automatizzata come nell'ambiente di produzione.
- Il codice sistema (primo campo del file EFFF) seguirà il "pattern": Pxxxxxxx es: P0001234 invece di xxxxxxxx es: 00001234 delle carte di attivazione reali date ai Titolari.
- Le chiavi 3Des del sigillo fiscale sono casuali e non soddisfano le verifiche di sigillo essendo diverse da quelle dell'ambiente di produzione.

4. Contenuto della Smart Card (SC)

Ciascuna Smart Card verrà corredata, all'atto della personalizzazione da parte di SIAE, delle seguenti informazioni:

1. Una chiave triplo DES. Tale chiave **non** può essere letta ma solo utilizzata implicitamente invocando il comando opportuno *computeSigillo* (dove i vari * mascherano le varianti alla chiamata standard)
2. Il certificato di firma del Titolare del sistema di emissione ovvero del Richiedente la SC
3. la chiave privata RSA relativa al Titolare/richiedente del sistema di emissione. Tale chiave non può essere letta ma solo utilizzata implicitamente invocando il comando opportuno
4. la chiave pubblica RSA relativa al Titolare/richiedente del sistema di emissione
5. Il certificato pubblico del server SIAE.

6. Il certificato pubblico CA emittente (*issuer*) del certificato del server SIAE.
7. Contatore del numero dei biglietti emessi (EF_CNT) con valore iniziale pari a 0 con incremento unitario automatico per ogni richiesta di sigillo fiscale. Esternamente tale contatore è disponibile in sola lettura.
8. Contatore del numero degli importi registrati (EF_CNT_BALANCE) con valore iniziale pari a 0 con incremento automatico per ogni richiesta di sigillo fiscale con l'importo inserito per il titolo emesso espresso con un intero rappresentante il totale in centesimi di euro (es: un biglietto da 10,00 euro andrà passato il valore 1000 (mille centesimi). Esternamente tale contatore è disponibile in sola lettura.
9. Un insieme di informazioni anagrafiche contenute in un file (EFFF) organizzato in record di lunghezza variabile. Tale file è inserito nel dominio PKCS#11 ed i record contengono delle stringhe di caratteri ASCII.
10. Il numero di serie della carta che risulta anche stampato sull'involucro plastico. Tale valore è inserito in uno specifico file binario all'interno del master file della carta.

Nel seguito è indicato il file con le informazioni anagrafiche. Il file ha identificativo EF FF e si trova nel DF PKCS (11 11). Tale file è leggibile ma non modificabile:

File Identifier: EFFFh
Type: EF Linear Variable Record
Presence: Mandatory
Body Size: variable

Access Conditions (AC)

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

Il file si compone di una serie di informazioni elencate nel seguito.

Le smart card di test fornite, conterranno al loro interno i valori (ragione sociale, nome e cognome richiedente etc.) del produttore di sistemi di emissione anziché del titolare come succede nel caso delle carte di attivazione dell'ambiente di produzione.

In particolare si fa riferimento alla tabella qui sotto per capire cosa sarà possibile ottenere dalla lettura del file di personalizzazione della SC:

Campi presenti sul file EF FF e loro ordine nelle SmartCard definitive (Carte d'attivazione).

Fields order	DE DTD Field:	Description:	SC field length (indicativo)	Notes:
1	systemId	**Codice** univoco del **Sistema**	8	Es: 99999999 Nel caso invece di SmartCard di Prova Pxxxxxxx es: P0001234
2	ContactName	Nome del firmatario (**richiedente**)	40	
3	ContactLastName	Cognome del firmatario (**richiedente**)	40	
4	contactCodFis	Codice Fiscale del firmatario (**richiedente**)	18	
5	SystemLocation	Ubicazione del sistema	100	
6	ContactEmail	Indirizzo e-mail da associare al certificato digitale (associato quindi al **richiedente** ovvero al Titolare per conto del quale il richiedente ha ottenuto la SmartCard)	50	Titolarex@wind.it
7	SiaeEmail	Indirizzo **e-mail del server SIAE** a cui inviare posta	40	Es nel caso di SmartCard di prova: servertest2@batest.siae.it
8	partnerName	**Titolare**, ovvero ragione sociale oppure Nome e cognome [in unico campo nel caso di persona fisica]	60	Es: Giochi Scommesse e Ballo S.p.A.
9	partnerCodFis	Codice Fiscale o partita Iva della società (del **Titolare**)	18	
10	partnerRegistroImprese	Numero di Iscrizione al registro delle imprese (REA ex CCIAA) del **Titolare**	18	
11	partnerNation	Nazione della società (**Titolare**) con codifica ISO 3166	2	Es: IT
12	systemApprCode	Num. Di protocollo della delibera approvazione del sistema di emissione da parte della Agenzia delle Entrate	20	Data di rilascio della SC di prova nel caso di uso della SC di prova: testo libero
13	systemApprDate	Data delibera approvazione sistema di emissione	20	In formato di testo libero: Es: 15/Apr/2003 oppure 15/04/2003 ovvero 15/04/03
14	contacRepresentationType	Tipo di rappresentanza legale: I→ Titolare del sistema (Imprenditore) T→ Titolare del sistema (Non Imprenditore) L→ Legale Rappresentante N→ Procura Notarile P→ Poteri Statutari	1	
15	userDataFileVersion	Stringa contenente la versione del presente file	5	Prima versione: 1.0.0

I campi descritti qui sopra saranno scritti sul file EFFF presente nella SmartCard nel dominio PKCS#11 con struttura a **record variabili,** a tal fine bisogna tenere presente che le dimensioni dei campi indicate nella tabella nella colonna "SC field length" sono puramente **indicative**. Solo nel caso di dati eccedenti le dimensioni esposte (qualora possibile) tali numeri indicano il numero massimo dei caratteri ammessi.

Se in futuro dovesse essere necessario aggiungere dei campi questo sarà fatto a partire dal 16° campo in poi (attualmente non previsto) si raccomanda di leggere quindi il file fino al raggiungimento dell'EOF (End Of File) al fine di visualizzarne comunque tutto il contenuto. In tale eventualità, il campo " userDataFileVersion" (campo 15) sarà impostato a qualcosa di diverso da 1.0.0 che è il valore impostato a partire da aprile 2003 in base allo schema qui sopra riportato.

5. Note sul “comportamento” della SmartCard

5.1 PIN e PUK di default

Quando la SmartCard di test viene inizializzata, le viene assegnato il PIN ed un PUK che saranno indicati nella lettera di accompagnamento spedita insieme alle SC.

Attenzione ad eseguire sempre il VerifyPIN (della LibSIAEcard.dll) prima di eseguire operazioni “protette” come il calcolo del sigillo (ComputeSigillo) sulla SmartCard.

5.2 Utilizzazione del sigillo fiscale ottenuto dalla SC

La funzione ComputeSigillo e le varianti ottimizzate a questa chiamata presenti nella LibSIAEcard.dll restituiscono in output oltre al valore del contatore progressivo del biglietto emesso (con quella SC) anche il sigillo fiscale in 8 byte.
La **rappresentazione degli 8 byte è eseguita in esadecimale** utilizzando per ciascun byte una coppia di caratteri nell'insieme 0 (zero) - F (effe maiuscola) che pertanto verranno stampigliati sul biglietto emesso in tale rappresentazione. Pertanto utilizzando la notazione esadecimale di una richiesta di sigillo che restituisca i seguenti bytes (in decimale nell’intervallo dei codici ASCII 0 - 255):

022-223-095-250-176-000-112-001

Sarà stampata sul biglietto nel modo seguente:

16-DF-5F-FA-B0-00-70-01

5.3 Gestione contatori interni alla SC e decremento non consentito.

La SC fornita è dotata al proprio interno di due contatori:

EF_CNT che tiene traccia di tutti i sigilli emessi (“biglietti” reali, o annullamenti di biglietti)

e

EF_ CNT_BALANCE che somma i prezzi di tutti i biglietti emessi (“biglietti” reali, o annullamenti di biglietti).

L’operazione di emissione di sigillo automaticamente esegue un incremento di entrambi i contatori. Per evidenti motivi di sicurezza non è possibile in alcun modo annullare l’emissione da parte della SmartCard di un sigillo, pertanto **non esistono funzioni di decremento né dell’uno né dell’altro contatore**.
In caso di necessità andrà eseguita una operazione di annullamento che agirà sul LOG delle transazioni e richiederà alla SC un apposito sigillo di annullamento con importo pari a quello del biglietto da annullare.
In caso di SC difettosa, si puo’ tranquillamente procedere all’annullamento di una emissione mediante sigillo di annullamento emesso da una SC differente da quella utilizzata per l’emissione del titolo da annullare **purché facente riferimento al medesimo sistema**.

6 Descrizione materiale fornito a corredo del SIAE TEST CARD KIT

Il pacchetto SIAE TEST CARD KIT è composto di hardware, software e documentazione in formato digitale, ed in particolare da:

1. massimo N. 2 carte di attivazione (SC) di test;
2. documentazione tecnica Smart Card di test per progetto biglietterie automatizzate (presente documento);
3. descrizione fisica del chip presente a bordo della smart card INCRIPTO 34 V1: Bd19xl34.pdf;
4. un file compresso contenente una serie di informazioni / software distribuiti dal produttore. Il contenuto di tale file è il seguente:

Cartella Documentazione:

- CSP_SIAEp.pdf	Descrizione del modulo SW che implementa le MScryptoAPI
- FileSystemSIAE105bp.pdf	Descrizione del File System SIAE
- libSIAEcard_103p.pdf	Manuale del programmatore della libreria in ANSI C, disponibile in codice sorgente per il supporto di piattaforme diverse da Windows
- licenzaeGaranziaCSP180p.pdf	Licenza e Garanzia del modulo CSP
- licenzaegaranziaPKCS11180.pdf	Licenza e Garanzia del modulo PKCS11
- PKCS#11_SIAEp.pdf	Descrizione del modulo SW che implementa le API standard PKCS#11
- UserManualIncrypto34p.pdf	Manuale del programmatore della smartcard Incrypto34

Cartella software:

- SysGillo PKCS#11 Interfaces.zip	Modulo SW PKCS#11 librerie per ambiente windows
- SysGillo CSP Interfaces.zip	Modulo SW CSP librerie per ambiente windows
- libSIAECard.zip	Codici sorgenti della libreria ANSI C

Attenzione: il file libSIAEcard_103p.pdf è stato reso obsoleto dalla nuova versione (al momento 1.1.0 del 10 marzo 2014) direttamente scaricabile sul link sopra indicato al par. 1Scopo del documento. Idem dicasi per il CSP ora in versione 1.3.1.1).

I file e la documentazione sono accessibili mediante protocollo https protetto da userID/password fornita ai produttori che avranno fatto richiesta delle Smart Card di Prova.

In caso di problemi relativi alla SC e connessi alla firma digitale è stata istituita una casella e-mail (distribution list): SIETA.Tecnologia@siae.it mentre per dubbi riguardanti le norme concernenti le biglietterie automatizzate è disponibile la casella (distribution list): SIETA.Normativa@siae.it .

--------- end of document --------