Tecnologie
Telematiche
Trasporti
Traffico
Torino

5T S.r.l. – Via Bertola, 34 - 10122 Torino
tel. 011-227.4101
telefax 011-227.4201
e-mail: info@5t.torino.it
Posta Certificata: direzione5t@legalmail.it
Sito WEB: www.5t.torino.it
Cod. fisc. e Part. IVA 06360270018
C.C.I.A.A. Torino 2825/1992
Capitale sociale € 100.000,00

Nota Tecnica

Firma e Verifica COP

Doc_ID	SP_1950
Versione	1.2
Riassunto	Questo documento descrive i comandi e le operazioni necessarie ad implementare le procedure di firma e verifica di un titolo di viaggio su supporto chip on paper.
Numero di pagine	9

	Nome	Ruolo	Data	Firma
Autore	D. Migliasso	System Engineer	28-mar-2012	N/A
Revisione	C. Giacobbe	Project Manager		N/A
Approvazione	R. Panero	Direttore 5T		N/A

Storia del documento

Template: 5T-Nota_Tecnica 1.0.0

Data	Versione	Autore	Riassunto dei cambiamenti
28-mar-2012	0.1		Prima bozza
30-mar-2012	1.0	**D. Migliasso**	
12-set-2012	1.1	**D. Migliasso**	• Corretto footer • aggiunto dettaglio chiavi di firma da utilizzare • aggiunto par. modalità di firma • aggiunto esempio di comandi di calcolo e verifica firma
18-feb-2014	1.2	**A. Giglio** **L. Giuliani**	• aggiunto par. verifica firma validazione • corretto par. verifica firma emissione

Lista di distribuzione

Sommario

1 Introduzione

1.1 Definizioni ed Acronimi

Acronimo	Definizione
BIP	Bigliettazione Integrata Piemonte
SAM	Secure Application Module
MAC	Message Authentication Code
KIF	Key Function
KVC	Key Version & Category
APDU	Application Protocol Data Unit
TDVE	Titolo di viaggio elettronico
SC	Smart card
COP	Chip on paper

1.2 Riferimenti

Riferimento	Descrizione
[1]	5T-Nota_Tecnica_BIP_Tabella_Operatori

2 Chiavi di firma

2.1 Introduzione

Per garantire l'autenticità di un contratto presente sul COP, in modo tale da assicurare che un dato contratto è valido, che è stato emesso dall'azienda che dichiara di essere e che non è stato modificato da terzi, è stata introdotta la firma del contratto ovvero un numero che rappresenta in modo univoco una sequenza di byte di lunghezza generica.

2.2 Chiavi operatore

Ognuna delle aziende aderenti al progetto BIP possiede una propria chiave di firma aziendale, identificata con la sigla CKD_SIGNXX (dove XX è il codice dell'azienda) e abilitata per firmare una sequenza di byte. Le rimanenti chiavi aziendali saranno abilitate alla sola verifica di una firma in modo da poter verificare le firme apposte da altri operatori afferenti al BIP.

La discriminante tra chiave di firma/verifica da quella di sola verifica è nei parametri della chiave (che sono raggruppati da PAR1 a PAR10), in particolare in PAR1 e PAR5. Tali parametri si possono ottenere con il comando al SAM denominato "SAM Read Key Parameters".

Per una chiave di firma/verifica devono essere presenti le seguenti condizioni:

- CipherEnableBit=1 in PAR1, autorizzato per ciphering.
- PsoEnableBit=1 in PAR5, autorizzato per operazioni PSO.
- CertifComputeEnableBit=1 in PAR1, autorizzato per l'operazione "PSO Compute Signature".

Per una chiave di sola verifica devono essere presenti le seguenti condizioni:

- CipherEnableBit=1 in PAR1, autorizzato per ciphering.
- PsoEnableBit=1 in PAR5, autorizzato per operazioni PSO.

3 Firma di un COP

3.1 Introduzione

La firma digitale viene calcolata tramite il modulo SAM che contiene l'algoritmo e le chiavi di firma utili a tale scopo. La chiave di firma usata dal SAM è discriminata dal codice azienda. Il CDM COP prevede l'utilizzo di due firme: una da 4 byte calcolata in fase di emissione e una da 2 byte calcolata in fase di validazione. Calypso offre diverse modalità di calcolo della firma digitale che ne rafforzano la sicurezza:

- Busy mode (sempre attiva)
- Traceability mode (attiva solo per la firma di emissione)

3.2 Busy Mode

Questa modalità scongiura il pericolo di attacchi di *brute force* per forzare il sistema di crittografia, infatti dopo un tentativo fallito di verifica della firma il SAM rimane *busy* per qualche secondo (max.10) nei quali è quindi impossibile ulteriori altri tentativi.

3.3 Traceability Mode

Questa modalità inserisce automaticamente, all'offset specificato nel comando di calcolo o verifica della firma, SAM ID (4byte) e SAM Counter (3byte). Tali dati sono univoci a livello planetario e permettono di individuare chi e quando è stata effettuata la firma digitale.

3.4 Calcolo firma di emissione

Viene calcolata con il comando APDU diretto alla SAM denominato "**PSO Compute Signature**" in modalità tracciamento (*traceability mode*) nelle condizioni di chiavi sopra elencate (CipherEnableBit=1 in PAR1, PsoEnableBit=1 in PAR5, CertifComputeEnableBit = 1 in PAR1). La lunghezza della firma in questo caso è di 4 byte.

La chiave di firma varia a seconda dell'operatore (CKD_SIGNxx dove xx rappresenta il numero dell'azienda) vedi documento [1].

Il SAM restituirà i dati con all'interno, all'offset specificato nel comando, SAM serial number e SAM counter e, alla fine, la firma.

Per ulteriori dettagli fare riferimento alla documentazione ufficiale Calypso.

Un **esempio** di sintassi del comando è:

Field	Size	Value (hex)	Description
CLA	1	94	Anche 0x80 è accettato.
INS	1	2A	
P1	1	9E	
P2	1	9A	
LC	1	21	Lunghezza dei byte che seguono.
Sign key reference	1	FF	
KIF	1	xx	KIF della signing key , per l'azienda 1 , GTT vale 2C.
KVC	1	xx	KVC della signing key, per l'azienda 1 , GTT vale 61.
OpMode	1	E4	firma con tracciabilità e busy mode + lunghezza in byte della firma.
Offset	2	xxxx	Offset al quale si trovano SAM s/n e counter (in Message) espresso in bit.
DataIn	7	s/n	Seriale chip-on-paper
	20	Message	Dati

La risposta al comando è:

Field	Size	Description
DataOut	7	Seriale del chip-on-paper
	20	Dati
	4	Firma
Status	2	90 00 se il comando è stato eseguito con successo

Per gli altri possibili valori fare riferimento al SAM user manual.

3.5 Calcolo firma di validazione

Viene calcolata con il comando APDU diretto al SAM denominato "**PSO Compute Signature**" senza modalità tracciamento (*traceability mode*). La lungheza della firma in questo caso è di 2 byte.

La chiave di firma è CKD_DEBIT (KIF= 2Bh KVC=6Ch).

Il SAM restituirà la firma.

Per ulteriori dettagli fare riferimento alla documentazione ufficiale Calypso.

Un **esempio** di sintassi del comando è:

Field	Size	Value (hex)	Description
CLA	1	94	Anche 0x80 è accettato.
INS	1	2A	
P1	1	9E	
P2	1	9A	
LC	1	1D	Lunghezza dei byte che seguono.
Sign key reference	1	FF	
KIF	1	2B	KIF della signing key (CKD_DEBIT)
KVC	1	6C	KVC della signing key (CKD_DEBIT)
OpMode	1	82	Firma con busy mode + lunghezza in byte della firma.
DataIn	4	OTP	OTP bytes
	7	s/n	Seriale chip-on-paper
	26	Message	Dati

La risposta al comando è:

Field	Size	Description
DataOut	2	Firma
Status	2	90 00 se il comando è stato eseguito con successo

Per gli altri possibili valori fare riferimento al SAM user manual.

4 Verifica di una firma

4.1 Introduzione

La verifica di una firma viene eseguita attraverso il comando APDU diretto al SAM denominato "**PSO Verify Signature**", nelle condizioni di chiavi sopra elencate (CipherEnableBit=1 in PAR1, PsoEnableBit=1 in PAR5).

Il terminale deve indicare al SAM gli stessi parametri utilizzati per generare la firma. Con lo stesso comando quindi è possibile, variandone opportunamente i parametri (lunghezza firma, chiavi, etc.), verificare sia la firma di emissione che quella di validazione.

Attenzione: dopo il reset del SAM o dopo una verifica errata della firma il comando PSO Verify Signature fallisce con lo status "busy" (SW=0x6982) per un breve periodo di tempo. In questo caso il terminale dovrà ripetere il comando fino a che il SAM uscirà dallo stato "busy". Tipicamente questo stato dura non più di dieci secondi. Questo accorgimento scoraggia eventuali attacchi *brute force* per individuare la firma corretta.

4.2 Verifica firma di emissione

Viene effettuata tramite il comando APDU diretto al SAM denominato "**PSO Verify Signature**", abilitando le modalità *traceability mode* e *busy mode*. La lunghezza della firma considerata in questo caso è pari a 4 byte.

La chiave necessaria per la verifica firma deve essere la stessa utilizzata nel calcolo della stessa firma. Tale chiave varia a seconda dell'operatore (CKD_SIGNxx dove xx rappresenta il numero dell'azienda) vedi documento [1].

Il SAM restituirà un comando di tipo 90 00 nel caso in cui la verifica è stata eseguita con successo.

Un **esempio** di sintassi del comando per la verifica della firma di emissione è:

Field	*Size*	*Value (hex)*	*Description*
CLA	1	94	Anche 0x80 è accettato.
INS	1	2A	
P1	1	00	
P2	1	A8	
LC	1	25	Lunghezza dei byte che seguono.
Sign key reference	1	FF	
KIF	1	xx	KIF della signing key (per l'azienda 1, GTT vale 2C).
KVC	1	xx	KVC della signing key (per l'azienda 1, GTT vale 61).
OpMode	1	E4	firma con tracciabilità e busy mode + lunghezza in byte della firma.
Offset	2	xxxx	Offset al quale si trovano SAM s/n e counter (in Message) espresso in bit.

DataIn	7	s/n	Seriale del chip-on-paper.
	20	Message	Tracciato contratto da firmare.
	4	Sign	Firma del contratto

La risposta al comando è:

Field	Size	Description
Status	2	90 00 se il comando è stato eseguito con successo

Per gli altri possibili valori fare riferimento al SAM user manual.

4.3 Verifica firma di validazione

Viene effettuata tramite il comando APDU diretto al SAM denominato "**PSO Verify Signature**", con la differenza che in questo caso bisogna disabilitare la modalità di tracciamento (*traceability mode)* attiva solo per la firma di emissione. La lunghezza della firma in questo caso è pari a 2 byte.

La chiave necessaria per la verifica firma deve essere la stessa utilizzata nel calcolo della stessa, ovvero CKD_DEBITp (KIF= 2Bh KVC=6Ch).

Il SAM restituirà un comando di tipo 90 00 nel caso in cui la verifica è stata eseguita con successo.

Un **esempio** di sintassi del comando per la verifica della firma di validazione è:

Field	Size	Value (hex)	Description
CLA	1	94	Anche 0x80 è accettato.
INS	1	2A	
P1	1	00	
P2	1	A8	
LC	1	2B	Lunghezza dei byte che seguono.
Sign key reference	1	FF	
KIF	1	2B	KIF della signing key (CKD_DEBIT)
KVC	1	6C	KVC della signing key (CKD_DEBIT)
OpMode	1	82	firma con busy mode + lunghezza in byte della firma.
DataIn	4	OTP	OTP bytes.
	7	s/n	Seriale del chip-on-paper.
	26	Message	Tracciato contratto da firmare.
	2	Sign	Firma del contratto.

La risposta al comando è:

Field	Size	Description
Status	2	90 00 se il comando è stato eseguito con successo

Per gli altri possibili valori fare riferimento al SAM user manual.