S.I.A.E.

INCRYPTO 34

Manuale utente

Cod. Doc. E1001/eS&S

Document Version 1.0.0

Sommario

1 Introduzione

Definizioni

Definizione di AC Per una specifica azione di accesso ad un file o ad un oggetto, una definizione di AC stabilisce quale diritto di accesso deve essere concesso nelle condizioni di sicurezza per eseguire l'azione di accesso (la definizione di AC equivale ad un attributo di sicurezza).
ATR Risposta per il reset.
Backtracking Meccanismo per la ricerca di oggetti.
Oggetto BS Oggetto base di sicurezza (BSO).
CLA Byte di classificazione.
Componente CON Componente di un oggetto SE o CSE che si riferisce ad un oggetto PSO per PSO_DEC o PSO_ENC.
DES Crittografia standard di dati.
Componente DS Componente di un oggetto SE o CSE che si riferisce ad un oggetto PSO per PSO_CDS o PSO_VDS.
FCI Informazione per controllo file.
INS Byte di istruzione.
LSB Byte meno significativo.
LSBit Bit meno significativo.
MAC Codice di autenticazione del messaggio.
Modulo N Componente chiave per chiavi RSA pubbliche e chiavi RSA private.
MSB Byte più significativo.
MSBit Bit più significativo.
OCI Informazione di controllo oggetti.
P1-P2 Byte di parametro.
PIN (Personal Identification Number) Numero di identificazione personale.
PKB Chiave pubblica.
Indicatore_Privato Indicatore della chiave RSA privata.
PSO_DEC PSO per operazioni DECIPHER.
PSO_ENC PSO per operazioni ENCIPHER.
PSO Object Oggetto BS usato per tutti i comandi PSO.
Indicatore_Pubblico Indicatore della chiave RSA pubblica.
RFU rfu Riservato per uso futuro.
Attributo di sicurezza Equivalente alla definizione AC.
SE Ambiente di sicurezza.
SE Object Oggetto dell'ambiente di sicurezza.

Acronimi

AC Condizione di accesso.
AID Identificatore di applicazione (uguale al nome di DF).
CIE Carta d'Identità Elettronica.
CSE Contesto corrente di sicurezza.
DF File dedicato.
EF File elementare.
FID File ID.

MF Master file.
MSE Comando MANAGE SECURITY ENVIRONMENT.
PSO Comando PERFORM SECURITY OPERATION.
SSCE Sistema di Sicurezza del Centro di Emissione.
SW Software.
TBC To Be Confirmed.
TBD To Be Defined.
TLV Etichetta, Lunghezza, Valore.

2 Comandi per la gestione dei file

Select File

Seleziona un file (EF, DF o MF) sulla carta.

CLA	0x00
INS	0xA4
P1	vd. Tabella di seguito
P2	vd. Tabella di seguito
P3	Lc = Length
Data Field	Empty / FID /AID
Le	TBD

Tabella 1

P1	P2	Data Field	Descrizione
00	00	Vuoto	Selezione del Master File
00	00	3F 00	Selezione del Master File
00	00	FID	Selezione del file a partire dal FID
00	01	FID	Viene selezionato il DF figlio avente il FID indicato
00	02	FID	Viene selezionato l'EF figlio avente il FID indicato
00	03	Vuoto	Viene selezionato il DF padre del DF corrente
00	04	AID	Viene selezionato il DF avente l'AID indicato nel data field
00	08	PATH del file	Selezione del file indicato dal PATH presente nel data field

Tabella 2

SW1	SW2	Description
6A	81	Funzione non supportata
6A	82	File non trovato
6A	86	P1 o P2 incorrettp
6A	87	Lc inconsistente con P1 or P2

Tabella 3

Read Binary

Restituisce il contenuto di un file elementare di tipo binario.
Offset individua il byte a partire dal quale si vuole cominciare a leggere mentre Le indica il numero di byte che si desidera leggere.

CLA	0x00
INS	0xB0
P1	Offset_byte alto
P2	Offset_byte basso
P3	Le = numero di byte da leggere

Tabella 4

SW1	SW2	Description
90	00	Correct execution.
69	86	No current EF selected
69	81	Command incompatible with file structure (Current EF not transparent file)
6A	86	Wrong P1 (b7 != 0)
69	82	Access condition for this command not fulfilled
6B	00	Wrong parameter P1 – P2 (Offset outside the EF)
62	82	Read part of Le bytes (if ISO compliant)
67	00	Wrong length Le

Tabella 5

Read Record

Questo comando legge il contenuto di un record o parte di esso.
Il tentativo di utilizzo di tale comando è consentito esclusivamente sui file che presentano una struttura a record (semplice o TLV).
Nel caso in cui la struttura dei record sia di tipo TLV allora, è possibile individuare i record attraverso il loro identificativo (tag).

CLA	0x00
INS	0xB2
P1	Numero record o identificativo record (0x00 indicates the current record)
P2	Modalità di accesso ai record
Le	Numero di byte da leggere
Data Field	Vuoto

Tabella 6

Il byte P_1 contiene l'identificativo del record (il valore 0xFF non è consentito).

P_2 specifica la modalità di accesso al record secondo quanto riportato in Tabella 7.

P1	P2	Descrizione
00	04	Record corrente
00	00	Primo record
00	01	Ultimo record
00	02	Record successivo
00	03	Record precedente
>00	00	Prima occorrenza del record identificato con P1
>00	01	Ultima occorrenza del record identificato con P1
>00	02	Prossima occorrenza del record identificato con P1
>00	03	Occorrenza precedente del record identificato con P1
>00	04	Record identificato da P1
>00	05	Legge tutti i record partendo da P1 fino alla fine
>00	06	Legge tutti i record dall'inizio del file fino a P1

Tabella 7

I codici di risposta della carta al comando Read Record sono riassunti nella Tabella 8.

SW1	SW2	Description
0x90	0x00	Esecuzione corretta.
0x69	0x86	Nessun EF selezionato
0x69	0x81	Struttura file incompatibile con il comando
0x69	0x82	Condizioni di accsso non soddisfatte
0x6A	0x86	Parametro P2 incorretto
0x6A	0x83	Record non trovato
0x67	0x00	Lunghezza (Le) errata
0x62	0x82	E'stata letta solo una parte del record
0x6C	0xXX	Le = 0x00. XX indica la lunghezza esatta

Tabella 8

3 Comandi per la gestione di PIN e PUK

Verify

Verifica un PIN.

CLA	0x00
INS	0x20
P1	0x00
P2	0…….. PIN in MF 1…….. PIN with backtracking .xxxxxx ID of PIN

P3	PIN length or 8 (PUK)
Data Field	PIN

Tabella 9

NOTE sul valore di P2: Il bit più significativo di P2 indica se il PIN indicato deve essere è un BSO appartenente al Master File o se deve essere ricercato con il backtracking, ovvero, partendo dal DF corrente e procedendo a ritroso fino ad arrivare al MF.

SW1	SW2	Description
90	00	Esecuzione corretta.
63	00	Autenticazione fallita (ad es. il PIN inserito non è corretto)
63	Cx	x=numero di tentativi rimanenti
69	82	Condizioni di accesso non soddisfatte
69	83	PIN bloccato
69	86	Comando non consentito (stato della carta invalido)
6A	84	Memoria insufficiente
6A	86	P1 o P2 incorretti
6A	88	BSO non trovato

Tabella 10

NOTE: qualora l'autenticazione non vada a buon fine (status word 6300h) è possibile ottenere il numero di tentativi ancora disponibili prima che il PIN si blocchi inviando alla carta l'APDU con Lc=0 ed il data field vuoto.

SW1	SW2	Description
90	00	Esecuzione corretta.
67	00	Lunghezza errata Lc
69	82	Condizioni di accesso non soddisfatte
63	00	Autenticazione fallita (ad es. il PIN inserito non è corretto)
6A	86	P1 o P2 incorretti
6A	84	Memoria insufficiente
6A	88	BSO non trovato

Tabella 11

Change Reference Data

Consente di cambiare il valore di un BSO.

CLA	0x00
INS	0x24
P1	=00 per PIN(vecchio+nuovo) =XX per altri OCI vd. Tabella di seg.
P2	OCI ID da cambiare 0…….. OCI in MF

	1…….. OCI con backtracking .xxxxxxx ID dell'OCI
P3	Lc = lunghezza del data field
Data Field	Dati di verifica + presentazione nuovo valore

Tabella 12

P1 descrizione								
Bit Numero								**Descrizione**
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
0								Deve essere 0
	1	0	0	0	0	1		RSA KPRI EXP-CRYPT/DECRYPT
	1	0	0	0	0	0		RSA KPRI MOD-CRYPT/DECRYPT
	1	0	0	0	0	1		RSA KPRI EXP-SIGN
	1	0	0	0	0	0		RSA KPRI MOD-SIGN
	0	0	0	0	0	1		RSA KPUB EXP-EXT AUTH
	0	0	0	0	0	0		RSA KPUB MOD-EXT AUTH
	1	0	0	0	0	0		3DES/DES - CRYPT/DECRYPT
	0	1	0	0	0	0		3DES/DES – SM
	0	0	0	0	0	0		3DES/DES – EXT AUTH
	0	0	0	0	0	0		PIN
							0	Test implicito
							1	Test esplicito

Tabella 13

NOTA: se il bit0 è basso allora il data field è composto dal vecciho valore (che la carta verifica internamente) e la presentazione del nuovo valore da attribuire al BSO. Viceversa, se il bit0 è alto allora nel data field viene passato esclusivamente il nuovo valore da attribuire al BSO. Ovviamente, qualora le condizioni di accesso AC_CHANGE per il BSO non fossero soddisfatte, si avrebbe un codice di errore 6982h.

SW1	**SW2**	**Description**
90	00	Esecuzione corretta.
63	00	Autenticazione fallita (ad es. il PIN inserito non è corretto)
63	Cx	x=numero di tentativi rimanenti
69	82	Condizioni di accesso non soddisfatte
69	83	PIN bloccato
69	86	Comando non consentito (stato della carta invalido)
6A	84	Memoria insufficiente
6A	86	P1 o P2 incorretti
6A	88	BSO non trovato

Tabella 14

Reset Retry Counter

Riporta al valore originario il valore del contatore di errori di verifica di un BSO.

CLA	0x00
INS	0x2C
P1	=00 per PIN(vecchio+nuovo) =XX per altri OCI
P2	OCI ID da cambiare 0…….. OCI in MF 1…….. OCI con backtracking .xxxxxxx ID dell'OCI
P3	Lc = lunghezza del data field
Data field	Dati di verifica + presentazione nuovo valore

Tabella 15

P1 descrizione								
Bit Numero								**Descrizione**
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
0	0							
		1	0	0				RSA KPRI EXP-CRYPT/DECRYPT
		1	0	0				RSA KPRI MOD-CRYPT/DECRYPT
		1	0	0				RSA KPRI EXP-SIGN
		1	0	0				RSA KPRI MOD-SIGN
		0	0	0				RSA KPUB EXP-EXT AUTH
		0	0	0				RSA KPUB MOD-EXT AUTH
		1	0	0				3DES/DES - CRYPT/DECRYPT
		0	1	0				3DES/DES – SM
		0	0	0				3DES/DES – EXT AUTH
		0	0	0				PIN
					0	0	0	Il data field contiene sia i dati di verifica, sia la presentazione del nuovo valore. Questo caso è possibile solo se il BSO referenziato è un PIN.
					0	0	1	Il data field contiene solo i dati di verifica e ciò è valido solo se il BSO referenziato in P2 ha come condizione di accesso AC_UNBLOCK il riferimento ad un PIN.
					0	1	1	Il data field è vuoto

Tabella 16

SW1	**SW2**	**Description**
90	00	Esecuzione corretta.
63	00	Autenticazione fallita (ad es. il PIN inserito non è corretto)
63	Cx	x = numero di tentativi rimanenti
67	00	Lunghezza errata Lc

69	82	Condizioni di accesso non soddisfatte
69	83	Autenticazione bloccata
69	86	Comando non consentito (stato della carta invalido)
6A	83	Oggetto non trovato
6A	84	Memoria insufficiente
6A	86	P1 o P2 incorretti
6A	88	BSO non trovato

Tabella 17

4 Comandi crittografici

Manage Security Environment

Il comando Manage Security Environment è utilizzato per creare (modalità SET) o per richiamare (modalità RESTORE) un oggetto SE.

CLA	0x00
INS	0x22
P1	vd. Tabella 20
P2	vd. Tabella 20
P3	Lc = data field length
Data Field	Data to be used in the Current Security environment (CSE) in TLV format

Tabella 18

I codici di risposta del comando sono riportate nella Tabella 19.

SW1	SW2	Description
0x90	0x00	Esecuzione corretta
0x67	0x00	Lc errata
0x69	0x82	Condizioni di accesso non soddisfatte
0x6A	0x83	Oggetto non trovato
0x6A	0x85	Struttura TLV inconsistente
0x6A	0x86	P1 o P2 incorretto

Tabella 19

Le modalità del comando possono essere selezionate con i parametri P1 e P2, così come da Tabella 20.

MODE	P1	P2	Data Field
RESTORE	0xF3	Security Environment (SE) object ID	vuoto
SET	0xF1	0xB8/0xA4/0xB6 (dv. Tabella 21).	Tabella 21

Tabella 20

CSE	Command MSE SET				Related Commands
CSE Component	P2 (component TAG)	Data Field T	L	V	
Confidentiality component (CON)	0xB8	0x83/0x84	0x01	Object ID	PSO_DEC, PSO_ENC
Authentication component (TEST)	0xA4	0x83/0x84	0x01	Object ID	EXTERNAL AUTHENTICATION, VERIFY
Digital Signature component (DS)	0xB6	0x83/0x84	0x01	Object ID	PSO_CDS
Compute Checksum component (CC)	0xB4	0x83/0x84	0x01	Object ID	PSO_CCC, PSO_VERIFYCC
Hash component (HASH)	0xAA	0x83/0x84	0x01	Object ID	HASH

Tabella 21

Perform Security Operation: Hash (PSO_HASH)

Il comando restituisce l'hash dei dati.
L'algoritmo utilizzato è lo SHA1.

CLA	0x00
INS	0x2A
P1	0x90
P2	0xA0 in caso di hash intermedio 0x80 in caso di ultimo blocco
P3	Lc = length data to be hashed
Data field	Data = dati dsei quali si vuole calcolare l'hash
Le	Non presente se P2 = 0xA0; 0x20 se P1 = 0x80

Tabella 22

SW1	SW2	Description
0x90	0x.00	Esecuzione corretta
0x6A	0x87	Lc inconsistente con i valori di P1 e P2

Tabella 23

Attenzione:
I dati devono essere passati alla carta nel formato lsb-msb, ovvero con il byte meno significativo in test. Allo stesso modo, il risultato viene fornito in lsb-msb.

Nel caso in cui si effettui un hash multiplo, i comandi di hash intermedio devono essere consecutivi.

Perform Secutity Operation: Decrypt (PSO_DEC)

Questo applica l'algoritmo RSA ad un blocco di byte utilizzando un BSO chiave privata.

CLA	0x0x
INS	0x2A
P1	0x80
P2	0x86
P3	Lc = Lunghezza dei dati da decifrare + 1byte padding indicator
Data field	0x00 (padding indicator) || dati cifrati
Le	Lunghezza dei dati decifrati

Tabella 24

SW1	SW2	Description
0x90	0x.00	Esecuzione corretta
0x69	0x82	Condizioni di accesso non soddisfatte
0x69	0x84	Formato del BSO non corretto
0x69	0x85	Condizioni non soddisfatte (lunghezza della chiave errata)
0x6A	0x80	Data Field incorretto
0x6A	0x81	Funzione non supportata
0x6A	0x83	Ogetto non trovato
0x6A	0x86	Parametro P1o P2 invalido
0x6A	0x87	Lc inconsistente con P1 e P2

Tabella 25

5 Comandi per la gestione dei file contatore

Manage Counter

Legge, incrementa, decrementa il valore di un file contatore.

CLA	00h
INS	32h
P1	00h oppuer KID quando è richiesto il calcolo del MAC (BSO ID)
P2	Modalità vd. Tabella 27
Lc	Numero di byte nel data field. Valori possibili: 00h (Nessun Data Challenge in ingresso) 02h (Viene fornito solo l'incremento / decremento) N dove N è la lunghezza del Data Challenge. I valori accettati sono tutti quelli compresi tra 1 e 128

	2+ N dove N è la lunghezza del Data Challenge 04h (MANAGE COUNTER init mode)
Data Field	Vuoto 2-byte valore da sommare o sottrarre al contatore || N-Byte data Challenge per il calcolo del MAC (Opzionale) 4-bytes valore iniziale (init mode)
Le	Valore atteso per il risultato. Valori possibili sono: 04h (solo il valore di conteggio) 0Dh (valore di conteggio + 8 byte MAC)

Tabella 26

P2 mode byte description								
Bit Number								**Description**
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
-	-	-	-	0	0	0	1	Legge il contatore
-	-	-	-	0	0	1	0	Incrementa the contatore
-	-	-	-	0	1	0	0	Decrementa il contatore
-	-	-	-	1	0	0	0	Inizializza il contatore
-	-	-	-	x	x	x	x	RFU
-	-	-	0	-	-	-	-	Non calcola il MAC
-	-	-	1	-	-	-	-	Calcola il MAC
-	-	0	-	-	-	-	-	Valore ricevuto nei dati del comando
-	-	1	-	-	-	-	-	Valore fissato implicitamente.
0	0	-	-	-	-	-	-	Fixed to 0

Tabella 27