libSIAEcard

Specifiche libreria e ambiente di collaudo

Document Version 1.0.3

Document Revision History

Version	Date	Subject	Issued by	Authorized by
1.0.0 (Draft)	Mag. 13, 2002	Edizione	L.Consiglio	A.Scognamiglio
1.0.1 (Draft)	Mag. 27, 2002	Revisione	L.Consiglio	A.Scognamiglio
1.0.2	Giu. 11, 2002	Revisione	L.Consiglio	A.Scognamiglio
1.0.3	Giu. 13, 2002	Revisione	L.Consiglio	A.Scognamiglio

INDICE

Premessa

Piattaforma di riferimento e di collaudo

Le caratteristiche della piattaforma sulla quale la libreria "*libSIAEcard*" è stata sviluppata e testata sono le seguenti:

Sistema Operativo	*Linux* *(Distribuzione RedHat 7.2)*	http://www.redhat.com
Sistema di sviluppo	*GNU GCC 2.96*	http://www.gnu.org
PC/SC Toolkit	*M.U.S.C.L.E.* *(Movement for Use of Smart Card Environmet over Linux Environment)* *PC/SC Lite v1.0.1*	http://www.linuxnet.com
Lettore di Smart Card	*Incard miniLector*	http://www.incard.it
Smart Card	*Incrypto 34*	JDC ST-Incard
File System	*S.I.A.E. Card v 1.0*	

Acronimi

AC	Access Conditions
AID	Application Identifier
APDU	Application Protocol Data Unit
ASN	Abstract Syntax Notation
ATR	Answer-To-Reset
BER	Basic Encoding Rules
BS	Base Security
BSO	Base Security Object
CC	Common Criteria Version 2.1
CGA	Certification Generation Application

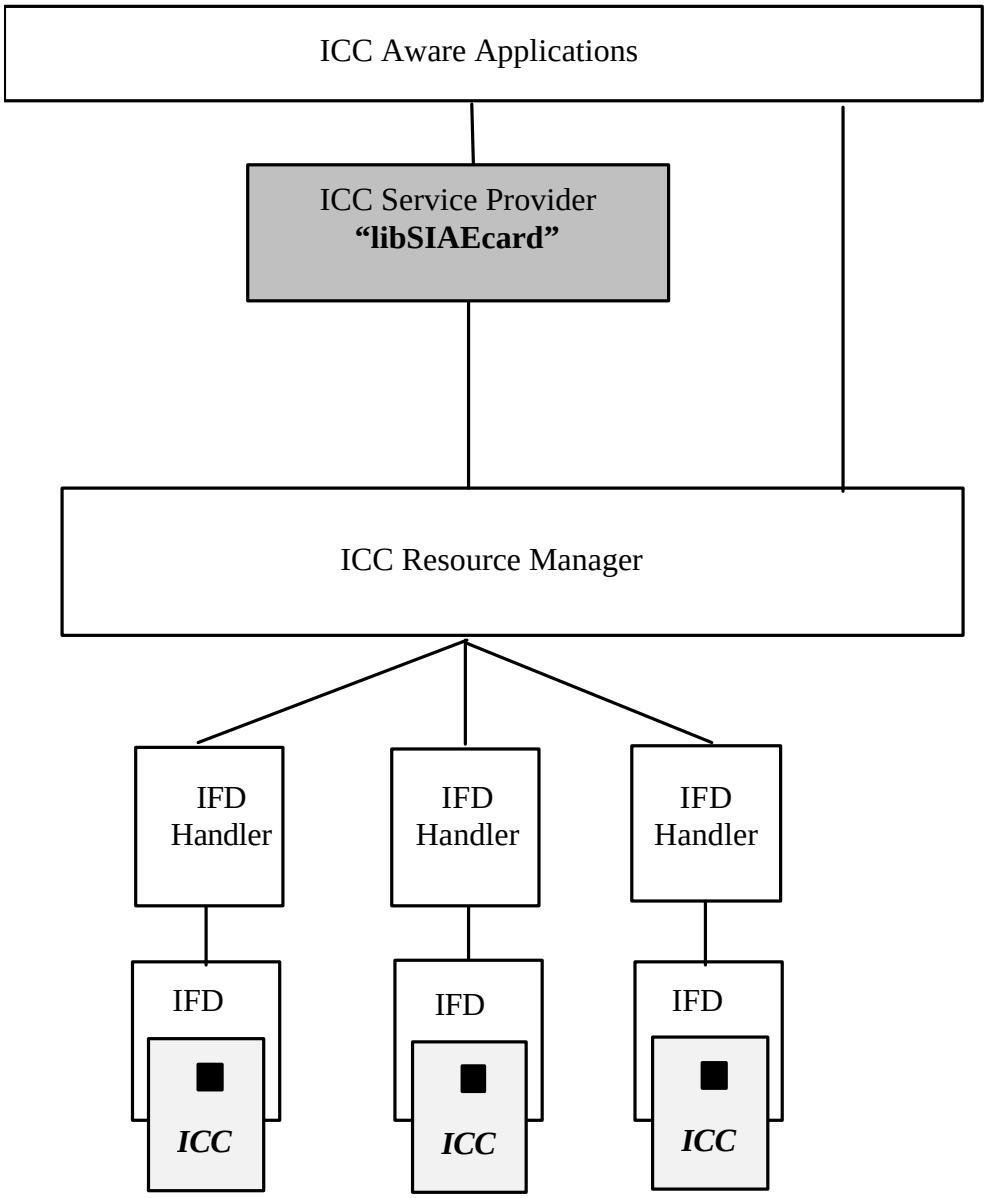
CSE	Current Security Environment
DES	Data Encryption Standard
DF	Directory File
DIR	Directory
DS	Digital Signature
EAL	Evaluation Assurance Level
EF	Elementary File
ETU	Elementary Time Unit
FCI	File Control Information
FID	File ID
HI	Human Interface
HW	Hardware
ICC	Integrated Circuit Card
ID Card	Identity Card
I/O	Input/Output
IT	Information Technology
lsb	Last Significant Bit (b0)
LSB	Last Significant Byte
MAC	Message Authentication Code
MF	Master File
msb	Most Significant Bit (b7)
MSB	Most Significant Byte
MSE	Manage Security Environment (command)
MTSC	Manufacturer Transport Secure Code
OS	Operating System
OCI	Object Control Information
PDA	Personal Digital Assistant
PDC	Patient Data Card
PIN	Personal Identification Number
PP	Protection Profile
PPSC	Pre Personalization Secure Code
PSO	Perform Security Operation (command)
RFU	Reserved for Future Use
RSA	Rivest, Shamir, Adleman
SCA	Signature-Creation Application
SCD	Signature-Creation Data
SD	Signatory's data
SDO	Signed Data Object

SE	Security Environment
SECI	Security Environment Control Information
SEO	Security Environment Object
SF	Security Function
SFI	Short File Identifier
SHA	Secure Hash Algorithm
SFP	Security Function Policy
SM	Secure Messaging
SOF	Strength of Function
SSCD	Secure Signature-Creation Device
ST	Security Target
SVD	Signature-Verification Data
TLV	Tag Length Value
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

Introduzione

Architettura PC/SC

"*libSIAEcard*" è stata implementata tenendo conto dello standard PC/SC (rif. http://www.pcscworkgroup.com).
In tale ottica, la libreria costituisce uno strato middleware che consente ad applicazioni con un livello di astrazione più alto, di comunicare, in maniera del tutto trasparente con la smart card, ovvero un ICC Service Provider (come è possibile evincere dallo schema dell'architettura PC/SC riportato di seguito).
La scelta dell'architettura standard PC/SC è giustificata dal fatto che, essa rappresenta, di fatto, uno standard di riferimento per lo sviluppo di applicazioni su smart card in tutti gli ambienti software al momento più diffusi.



Descrizione delle API implementate

API per la gestione del collegamento con la smart card.

Initialize

La funzione *Initialize* crea ed inizializza il collegamento con la smart card presente in un lettore.

Prototipo:

int Initialize(int Slot)

Argomenti:
Slot indica il numero dello slot nel quale è inserita la carta con la quale si vuole stabilire il collegamento PC/SC.

N.B.: la funzione Initialize deve essere sempre chiamata prima di ogni altra funzione della libreria.

Descrizione codici di ritorno:
C_OK
Operazione conclusa con successo.
C_CONTEXT_ERROR
Questo errore si verifica quando la libreria non riesce a stabilire un contesto PC/SC dell'applicazione.
Attenzione! E' un errore estremamente grave e non recuperabile dal programmatore.
Il modulo PC/SC potrebbe non essere stato installato correttamente. Verificare la corretta installazione del software e/o contattare l'amministratore di sistema.
C_ READER_UNKNOWN
Il valore Slot passato alla libreria non è riconosciuto come valido.
Una possibile causa di ciò potrebbe essere una cattiva installazione dei driver del lettore di smart card. Contattare l'amministratore di sistema per una verifica della corretta installazione dei driver.
C_NO_CARD
Non è presente nessuna carta nel lettore.
C_UNKNOWN_CARD
La carta presente nel lettore non è una S.I.A.E. card o c'è qualche problema sul file system.
C _ALREADY_INITIALIZED
La libreria è già stata inizializzata.
C_GENERIC_ERROR
Si è verificato un errore durante l'operazione.

Finalize

Conclude la comunicazione con la carta.

Prototipo:

int Finalize()

Descrizione codici di ritorno:
C_OK:
Operazione conclusa con successo.
C_NOT_INITIALIZED:
Non è stato inizializzato alcun canale di comunicazione.

Esempio di utilizzo delle funzioni di gestione della comunicazione con le smart card:

```
…
/* Dichiarazioni ed inizializzazioni varie */
int rc=C_OK;
…
/*      Inizializzazione comunicazione con la carta
        presente nel primo lettore (0)                  */
rc=Initialize(0) ;
…
// Operazioni sulla carta
…
rc=Finalize() ;
…
```

API per la gestione dei file.

La “S.I.A.E. Card” è inizializzata in modo tale da consentire la gestione di un numero massimo di 256 file compatibilmente con la quantità di memoria disponibile.
I file possono essere di diverse tipologie:
EF binary: cioè file che vengono visti, all’interfaccia, come sequenze di byte ai quali si può accedere in maniera causale.
File a record: tali file possono essere visti come sequenze di record identificabili individualmente. A loro volta, i file a record possono essere di diverso tipo:

> **EF Linear Fixed**: sono sequenze di record aventi tutti la stessa dimensione;
> **EF Linear Variable**: le dimensioni dei singoli record sono variabili;
> **EF Cyclic**: sono file con record di lunghezza fissa nei quali l’accesso avviene in maniera circolare, ovvero, dopo aver letto l’ultimo record, si ricomincia a leggere il primo.

Select

La funzione Select, selezione un file sulla carta, preparando la stessa, nel caso in cui il file sia di tipo elementare, ad una operazione di lettura.

Prototipo:

int Select(int fid)

Parametri:
fid è l’indice del file da selezionare.

Descrizione codici di ritorno:
C_OK:
Operazione conclusa con successo.
C_NOT_INITIALIZED:
Non è stato inizializzato alcun canale di comunicazione.
C_FILE_NOT_FOUND:
Il file che si sta cercando di leggere non è presente sulla smart card.

ReadBinary

La funzione ReadBinary consente la lettura del contenuto di un file di tipo binario.

Prototipo:

int ReadBinary(WORD Offset, BYTE* Buffer, int *Len)

Parametri:
Offset è il byte del file a partire dal quale si vuole cominciare la lettura.
Buffer è il puntatore alla zona di memoria destinata a contenere il risultato.

Len è il numero di byte che si desidera leggere. Qualora tale valore sia superiore ai byte effettivamente presenti nel file, all'uscita della funzione,in Len sarà contenuto il numero di byte effettivamente letti.

Descrizione codici di ritorno:
C_OK:
Operazione conclusa con successo.
C_NOT_INITIALIZED:
Non è stato inizializzato alcun canale di comunicazione.
C_FILE_NOT_FOUND:
Il file che si sta cercando di leggere non è presente sulla smart card.
C_NOT_AUTHORIZED:
Non è stato possibile leggere dal file richiesto in quanto non si possiedono i diritti per questa operazione sul file.
C_WRONG_TYPE:
Il file scelto è incompatibile con la funzione ReadBinary; è possibile, ad esempio che si stia cercando di effettuare una lettura di tipo binario su di un file con struttura a record.
C_WRONG_LENGTH:
Non è stato possibile leggere tutti i dati richiesti. Il numero di byte effettivamente letti è contenuto il Len.

Esempio:
Il seguente esempio mostra come leggere dal file "5F0A", 20 byte a partire dal 30°.

```
…
BYTE Buff[20];
int rc=C_OK;
int Len=20;
rc=Select(0x5F0A);
rc=ReadBinary(30, Buff, &Len);
…
```

ReadRecord

La funzione ReadRecord estrae un record da un file avente una struttura a record.

Prototipo:

int ReadRecord(int nRec, BYTE* Buffer, int *Len)

Parametri:
nRec è l'indice del record che si vuole estrarre.
Buffer è il puntatore alla zona di memoria nella quale deve essere estratto il record.
Len è la lunghezza del record che si vuole estrarre. Qualora la lunghezza del record da estrarre non fosse nota a priori, è possibile ricavarla effettuando la ReadRecord in due passi come indicato nell'esempio che segue.

Esempio:

```
…
int rc=C_OK;
int Len;
rc=Select(0x3F00);
rc=Select(0x0000);
rc=Select(0x1111);
rc=Select(0x5F02);
/*      Passando NULL come terzo parametro la funzione
        ReadRecord ricava la lunghezza del record selezionato
        e la restituisce in Len                                  */
rc=ReadRecord(1, NULL, &Len);
BYTE *Buff;
Buff=(BYTE)malloc(Len);
rc= ReadRecord (1, Buff, Len);
…
```

Descrizione codici di ritorno:

C_OK:

Operazione conclusa con successo.

C_NOT_INITIALIZED:

Non è stato inizializzato alcun canale di comunicazione.

C_NOT_AUTHORIZED:

Non è stato possibile estrarre il record richiesto in quanto non sono soddisfatte le condizioni di accesso per tale operazione.

C_WRONG_TYPE:

Il file scelto è incompatibile con la funzione ReadRecord; è possibile, ad esempio che si stia cercando di estrarre un record da un file che non presenta una struttura a record.

C_RECORD_NOT_FOUND:

Il record che si vuole estrarre non è presente nel file.

Funzioni per la gestione dei PIN

VerifyPIN

La funzione VerifyPIN verifica in PIN consente di effettuare una verifica del PIN sulla smart card.
La carta riceve in ingresso il valore del pin, lo confronta con il corrispettivo valore in essa memorizzato e, nel caso in cui tali valori coincidessero, abilita tutte le operazioni del caso.
Attenzione! Dopo 3 volte che la verifica di un PIN fallisce, tale PIN risulta bloccato.

Prototipo:

int VerifyPIN(int nPIN, char *pin)

Parametri:
nPIN è il numero del PIN da verificare.
pin è una stringa NULL terminated contenente il valore da verificare.

Descrizione codici di ritorno:
C_OK:
Operazione conclusa con successo.
C_NOT_INITIALIZED:
Non è stato inizializzato alcun canale di comunicazione.
C_PIN_BLOCKED:
Il PIN che si sta cercando di verificare è bloccato.
0x63Cx:
La verifica del PIN non è andata a buon fine, restano ancora x tentativi.

ChangePIN

La funzione ChangePIN consente di cambiare il valore di un PIN.

Prototipo:

int ChangePIN(int nPIN, char *Oldpin, char *Newpin)

Parametri:
nPIN è il numero del PIN da verificare.
Oldpin è una stringa NULL terminated contenente il vecchio valore del PIN.
Newpin è una stringa NULL terminated contenente il nuovo valore del PIN.

Descrizione codici di ritorno:
C_OK:
Operazione conclusa con successo.
C_NOT_INITIALIZED:
Non è stato inizializzato alcun canale di comunicazione.
C_PIN_BLOCKED:
Il PIN che si sta cercando di cambiare è bloccato.
0x63Cx:
La verifica del vecchio PIN non è andata a buon fine, restano ancora x tentativi.

UnblockPIN

La funzione UnblockPIN consente di sbloccare il valore di un PIN previa verifica del PUK ad esso associato.

Prototipo:

int UnblockPIN(int nPIN, char *Puk, char *Newpin)

Parametri:
nPIN è il numero del PIN da sbloccare.
Puk è una stringa NULL terminated contenente il PUK da verificare.
Newpin è una stringa NULL terminated contenente il valore da assegnare al PIN una volta sbloccato.

Descrizione codici di ritorno:
C_OK:
Operazione conclusa con successo.
C_NOT_INITIALIZED:
Non è stato inizializzato alcun canale di comunicazione.
0x63Cx:
La verifica del PUK non è andata a buon fine, restano ancora x tentativi.

Funzioni per la gestione del contatore di emissioni

ReadCounter

Legge il valore corrente del contatore di emissioni (EF_CNT).

Prototipo:

int ReadCounter(DWORD *value)

Parametri:
value è il puntatore alla zona di memoria destinata a contenere il valore attuale del contatore.

Descrizione codici di ritorno:
C_OK:
Operazione conclusa con successo.
C_NOT_INITIALIZED:
Non è stato inizializzato alcun canale di comunicazione.
C_NOT_AUTHORIZED:
Condizioni di accesso non soddisfatte per questa operazione.

ReadBalance

Legge il valore corrente del contatore di bilancio (EF_CNT_BALANCE).

Prototipo:

int ReadBalance(DWORD *value)

Parametri:
value è il puntatore alla zona di memoria destinata a contenere il valore attuale del "Balance Counter".

Descrizione codici di ritorno:
C_OK:
Operazione conclusa con successo.
C_NOT_INITIALIZED:
Non è stato inizializzato alcun canale di comunicazione.
C_NOT_AUTHORIZED:
Condizioni di accesso non soddisfatte per questa operazione.

ComputeSigillo

Incrementa il valore del contatore di emissioni di una unità e ne restituisce il MAC calcolato in base al nuovo valore del contatore, della data e dell'ora dell'incremento, del prezzo del biglietto emesso e del numero di serie del biglietto.

Prototipo:

int ComputeSigillo(BYTE *Data_Ora,DWORD Prezzo,BYTE *SN, BYTE *mac,DWORD *cnt)

Parametri:
Data_Ora è una sequenza di 8 byte che contiene l'ora del conteggio.
Prezzo è il prezzo del biglietto emesso.
SN è una sequenza di byte contenente il numero di serie del biglietto.
mac è il puntatore alla zona di memoria nella quale la funzione restituisce il MAC calcolato sull'attuale valore di conteggio. Il MAC è costituito da 8 byte.
cnt è il valore attuale di conteggio.

Descrizione codici di ritorno:
C_OK:
Operazione conclusa con successo.
C_NOT_INITIALIZED:
Non è stato inizializzato alcun canale di comunicazione.
C_NOT_AUTHORIZED:
Condizioni di accesso non soddisfatte per questa operazione.

Funzioni Crittografiche

Sign

La funzione Sign effettua la firma di un blocco di byte (la cui dimensione deve essere di 128 byte).

Prototipo:

int Sign(int kx,BYTE *toSign, int Len, BYTE *Signed)

Parametri:
kx è l'indice della chiave privata da utilizzare per la firma.
toSign è il puntatore al buffer da firmare.
Len è la dimensione del buffer da firmare.
Len è il puntatore ad un buffer dalle dimensioni di 128 byte (precedentemente allocato) destinato a contenere il risultato della firma.

Descrizione codici di ritorno:
C_OK:
Operazione conclusa con successo.
C_NOT_INITIALIZED:
Non è stato inizializzato alcun canale di comunicazione.
C_NOT_AUTHORIZED:
Condizioni di accesso non soddisfatte per questa operazione.

Hash

Prototipo:

int Hash(int mec,BYTE *toHash, int Len, BYTE *Signed)

Parametri:
mec è il meccanismo che si vuole utilizzare per effettuare l'hash (vd. Appendice A).
toHash è il puntatore al buffer del quale si desidera calcolare l'hash.
Len è la dimensione del buffer del quale si desidera calcolare l'hash.
Hashed è il puntatore ad un buffer destinato a contenere l'hash del buffer toHash (le dimensioni di tale buffer sono di 20 byte nel caso di hash SHA1 e 16 nel caso di MD5).

Descrizione codici di ritorno:
C_OK:
Operazione conclusa con successo.
C_GENERIC_ERROR:
Si è verificato un errore durante l'operazione.

Padding

Prototipo:

int Padding(BYTE *toPad, int Len, BYTE *Padded)

Parametri:
toPad è il puntatore al buffer del quale si desidera ottenere il Padding.
Len è la dimensione del buffer del quale si desidera ottenere il Padding.
Padded è il puntatore ad un buffer destinato a contenere il padding del buffer toPad (le dimensioni di tale buffer sono di 128 byte).

Descrizione codici di ritorno:
C_OK:
Operazione conclusa con successo.
C_GENERIC_ERROR:
Si è verificato un errore durante l'operazione.

Appendice A: Costanti definite nella libreria

ACCESS CONDITIONS	
AC_NEVER	00
AC_PIN1	01
AC_PIN2	02
…	…
AC_ALWAYS	15
FILE TYPE	
EF_BINARY	01
EF_LINEAR_FIXED	02
EF_LINEAR_FIXED_TLV	03
EF_LINEAR_VARIABLE	04
EF_LINEAR_VARIABLE_TLV	05
EF_CYCLIC	06
EF_CYCLIC_TLV	07
HASHING MECHANISMS	
HASH_SHA1	01
HASH_MD5	02

Appendice B: Tipi definiti nella libreria

La libreria definisce ed utilizza i seguenti tipi:

DWORD: *unsigned long;*

WORD: *unsigned short;*

BYTE: *unsigned char;*

AccessConditions:

```
typedef struct {
        int  ACRead;
        int  ACUpdate;
        int ACAppend;
        int ACDelete;
        int ACAdmin;
        int ACIncrease;
        int ACDecrease;
} AccessConditions;
```

Tali definizioni si trovano all'interno del file "libSIAEcard.h"

Appendice C: Definizione e descrizione degli errori

Tutte le funzioni implementate ritornano il valore C_OK se concluse con successo. In caso di errore, fare riferimento alla seguente tabella.

Risposta	Valore (hex)
C_OK	0000
C_CONTEXT_ERROR	0001
C_NOT_INITIALIZED	0002
C_ALREADY_INITIALIZED	0003
C_NO_CARD	0004
C_UNKNOWN_CARD	0005
C_COUNTER_ALREADY_INITIALIZED	0010
C_WRONG_LENGTH	6282
	63Cx
C_WRONG_TYPE	6981
C_NOT_AUTHORIZED	6982
C_PIN_BLOCKED	6983
C_WRONG_DATA	6A80
C_FILE_NOT_FOUND	6A82
C_RECORD_NOT_FOUND	6A83
C_WRONG_LEN	6A85
C_ALREADY_EXISTS	6A89
C_GENERIC_ERROR	FFFF