UBI
APPLICAZIONE PRIVATIVA

Versione:	1.1
Data Rilascio:	06/11/2014
Autore:	Donato Petraccone
Approvato da:	

INDICE DEL DOCUMENTO

1 Revisioni del documento

Versione	Data	Descrizione
1.0	06/11/2014	Versione iniziale
1.1	06/11/2014	Aggiunti i comandi di lettura e scrittura

2 Riferimenti

Indice	Descrizione

3 Scopo del documento

Scopo di questo documento è quello di definire le specifiche d'interazione con il chip fornito da Oberthur Technologies – Chrysalis Fly V3.0.

4 Introduzione

Il presente documento illustra la proposta tecnica Oberthur per l'implementazione di un'applicazione proprietaria crittograficamente sicura ed adeguata alle esigenze del cliente.

5 Smart card di supporto

La piattaforma Smart Card utilizzata per l'implementazione dell'applicazione di controllo accessi è la piattaforma nativa Oberthur Technologies Chrysalis Fly 3.0.
L'applicazione Proprietaria si appoggia alle funzionalità esposte dall'applicazione di "Data Storage" e sui dati memorizzati negli oggetti creati in un file a record specifico.

L'ATR a contatto della carta di test è: 3B6500002063CBAD20
L'ATR contactless della carta di test è: 3B8580012063CBAD20

L'ATR a contatto della carta di produzione è: 3B6500002063CBAD20
L'ATR contactless della carta di produzione è: 3B8580012063CBAD2001

Chiave TDES di test:

6 Struttura dati

Lo schema seguente esemplifica la struttura dati implementata sull'applicazione di Data Storage nella parte riguardante il riconoscimento dello studente.

Il file system è così strutturato:

- Master File Data Storage
  a. File 1
     i. Record 1
     ii. Record 2
     iii. Record 3
  b. File 2
     i. Record 1
  c. File 3
     i. Record 1

La chiave TDES per External Authentication è l'oggetto deputato alla gestione dell'autenticazione dei terminali presso la carta per concedere autorizzazioni di lettura e scrittura sull'EF 0003.
L'autenticazione dinamica avviene secondo l'algoritmo TDES-ECB con chiave a lunghezza doppia (16 byte).

La chiave TDES non è modificabile in fase d'uso.

La struttura dei dati è descritta in Figura 1.

```
A700 (Master File Data Storage)
|
+------- 0001 (EF)
|         |
|         +------- 0001 [Lettura Libera/No Scrittura] [VAR. MAX 127 byte]
|         |
|         +------- 0002 [Lettura Libera/No Scrittura] [VAR. MAX 127 byte]
|         |
|         +------- 0003 [Lettura Libera/No Scrittura] [MAX 127 byte]
|         |
+------- 0002 (EF)
|         |
|         +------- 0001 [Lettura/Scrittura Vincolata] [MAX 127 byte]
|         |
+------- 0003 (EF)
          |
          +------- 0001 [Lettura/Scrittura Vincolata] [MAX 127 byte]
```

Figura 1

7 Data Storage

Prima d'iniziare qualsiasi operazione di lettura o scrittura (se possibile) è necessario selezionare il Data Storage.
Questa operazione va eseguita una sola volta.
L'accesso viene implementato tramite le seguenti APDU (eseguibili sia in modalità a contatto che contactless):

```
T->C 00 A4 04 00 07 53 54 4F 52 41 47 45 (Select Data Storage)
C->T 9000
```

8 File 1 - record 1

Questo record è disponibile in sola lettura.
L'accesso viene implementato tramite le seguenti APDU (eseguibili sia in modalità a contatto che contactless):

```
T->C 00 B2 01 0C 1B (Lettura Dato F1R1)
C->T 9000
```

9 File 1 - record 2

Questo record è disponibile in sola lettura.
L'accesso viene implementato tramite le seguenti APDU (eseguibili sia in modalità a contatto che contactless):

```
T->C 00 B2 02 0C 10 (Lettura Dato F1R2)
C->T 9000
```

10 File 1 - record 3

Questo record è disponibile in sola lettura.
L'accesso viene implementato tramite le seguenti APDU (eseguibili sia in modalità a contatto che contactless):

```
T->C 00 B2 03 0C 05 (Lettura Dato F1R3)
C->T 9000
```

11 Autenticazione per Lettura e Scrittura File 0002 e 0003

I File 2 e 3 (record 1) possono essere letti e scritti previa autenticazione.
Lo schema seguente esemplifica la sequenza operativa di autenticazione. Il terminale si autentica per mezzo di un crittogramma basato su un random di 8 byte e poi accede al record contenente i dati proprietari.
Tutte le operazioni si svolgono nell'applicazione "Data Storage".

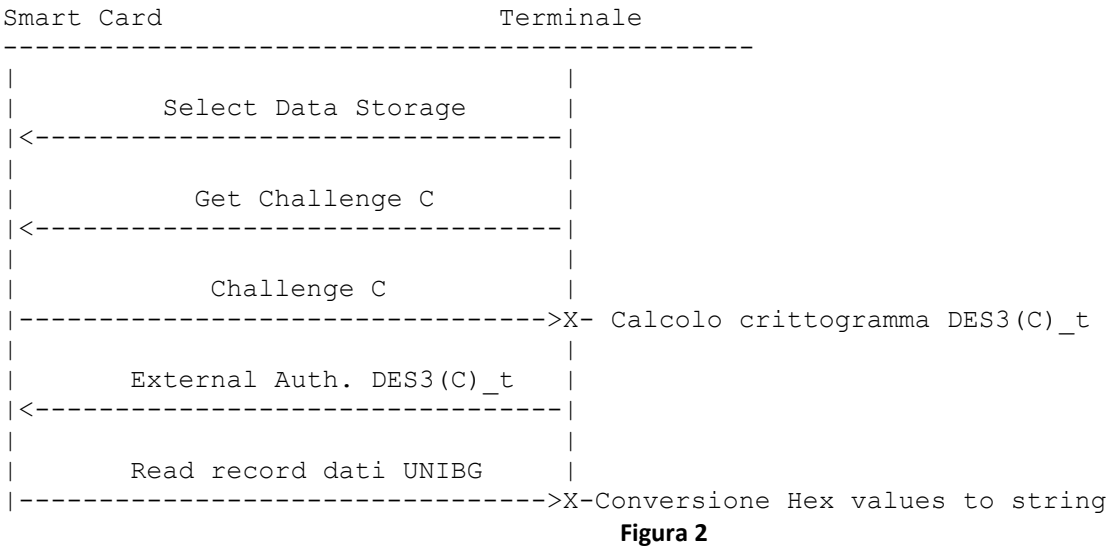

Figura 2

La transazione precedente viene implementata tramite le seguenti APDU (eseguibili sia in modalità a contatto che contactless):

```
T->C 00 A4 04 00 07 53 54 4F 52 41 47 45 (Select Data Storage)
C->T 9000

T->C 00 84 00 00 08 (Get 8 bytes random challenge C)
C->T C 9000

Calcolo DES3(C, UDK(V_UDK))_t
T->C 00 82 00 00 08 DES3(C, UDK(V_UDK))_t (External Auth DES3(C, UDK(V_UDK))_t)
C->T 9000
```

11.1File 2 - record 1

Questo record è disponibile in lettura e scrittura.

```
T->C 00 B2 01 14 7F (LETTURA EF 0002 RECORD 1)
C->T SC (9000)

T->C 00 DC 01 04 7F [XXXX](SCRITTURA EF 0002 RECORD 1 con i dati [XXXX])
C->T SC (9000)
```

11.2File 2 - record 1

Questo record è disponibile in lettura e scrittura.

```
T->C 00 B2 01 1C 7F (LETTURA EF 0003 RECORD 1)
C->T SC (9000)

T->C 00 DC 01 04 7F [XXXX](SCRITTURA EF 0003 RECORD 1 con i dati [XXXX])
C->T SC (9000)
```

Come indicato nei paragrafi 11.1 e 11.2, se richiesto, il comando di scrittura/update deve/può essere eseguito solo dopo aver lanciato un comando di Read Record per il File/Record Interessato:
Ad esempio:

```
(SCRITTURA EF 0002/0003 RECORD 1 – Es. 127 byte di '30')
T->C 00 DC 01 04 7F
303030303030303030303030303030303030303030303030303030303030303030303030303030
303030303030303030303030303030303030303030303030303030303030303030303030303030
303030303030303030303030303030303030303030303030303030303030303030303030303030
30303030303030
C->T SC (9000)
```

12 Esempio Transazione

I seguenti passi esemplificano i comandi indicati nei precedenti capitoli.

```
(Select Data Storage)
Command: 00 A4 04 00 07
Input Data: 53 54 4F 52 41 47 45
Output Data: 6F 19 84 07 53 54 4F 52 41 47 45 A5 0E 50 0C 44 61 74 61 20 53 74 6F
72 61 67 65
Status: 90 00

(LETTURA EF 0001 RECORD 3)
Command: 00 B2 03 0C 05
Output Data: 31 32 33 34 35
Status: 90 00

(Get 8 bytes random challenge C) -> 00 84 00 00 08 (9000)
Command: 00 84 00 00 08
Output Data: CB 66 8E 38 88 79 D4 D4
Status: 90 00

.SET_DATA   R           (R contiene il risultato della random challenge)
.SET_KEY    %MKEY       (Impostazione della chiave TDES)
.DES3       K 00        (Cifratura di R con la chiave TDES, il risultato è posto in
                        K)

K = 71 F3 81 9C 62 F2 48 BF

(External Auth DES3(C, UDK(V_UDK))_t) -> 00 82 00 00 08 K (9000)
Command: 00 82 00 00 08
Input Data: 71 F3 81 9C 62 F2 48 BF
Output Data: none
Status: 90 00
```

(LETTURA EF 0002 RECORD 1) -> 00 B2 01 14 7F (9000)
Command: 00 B2 01 14 7F
Output Data:
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30
Status: 90 00

(SCRITTURA EF 0002 RECORD 1)
Command: 00 DC 01 04 7F
Input Data:
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30
Output Data: none
Status: 90 00

(LETTURA EF 0003 RECORD 1) -> 00 B2 01 1C 7F (9000)
Command: 00 B2 01 1C 7F
Output Data:
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30
Status: 90 00

(SCRITTURA EF 0003 RECORD 1)
Command: 00 DC 01 04 7F
Input Data:
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
30 30 30 30 30 30 30 30 30 30 30 30 30 30
Output Data: none
Status: 90 00