Specifiche HPC

NK/4/FNS/T/2/1.2

Reference:	NK/4/FNS/T/2/1.2
Date of last change:	12.09.06
Authors:	G. Meazzini
Stage:	Version 1.2

Indice

1 Scopo

Il presente documento definisce:

- le caratteristiche tecniche
- le convenzioni per la trasmissione dei dati
- gli archivi e le strutture dei dati
- i meccanismi di sicurezza
- i comandi da utilizzare

per le carte dei professionisti della sanità (HPC).

Le specifiche HPC si basano principalmente su:

- il documento “Netlink Requirements for interoperability “
- gli standard ISO particolarmente rilevanti (nella fattispecie ISO / IEC 7816 Parti 4, 8 e 9)
- altro materiale (es. specifica HPC tedesca).

2 Riferimenti

ISO/IEC 7816-2: 1996 (2nd edition)
Information technology - Identification cards - Integrated circuit(s) cards with contacts -
Part 2: Dimensions and location of contacts

ISO/IEC 7816-3: 1997 (2nd edition)
Information technology - Identification cards - Integrated circuit(s) cards with contacts -
Part 3: Electronic signals and transmission protocols

ISO/IEC 7816-4: 1995
Information technology - Identification cards - Integrated circuit(s) cards with contacts -
Part 4: Interindustry commands for interchange

ISO/IEC 7816-5: 1995
Information technology - Identification cards - Integrated circuit(s) cards with contacts -
Part 5: Numbering system and registration procedure for application identifiers

ISO/IEC 7816-6: 1995
Information technology - Identification cards - Integrated circuit(s) cards with contacts -
Part 6: Interindustry data elements

ISO/IEC 7816-8: FDIS 1998
Information technology - Identification cards - Integrated circuit(s) cards with contacts -
Part 8: Security related interindustry commands

ISO/IEC 7816-9: CD2 1998
Information technology - Identification cards - Integrated circuit(s) cards with contacts -
Part 9: Additional interindustry commands and security attributes

2.1 Variazioni rispetto alla precedente versione

- GDO: Issuer identifier e commento
- Allegato C: correzione riferimento figura

3 Abbreviazioni e simboli utilizzati

3.1 Abbreviazioni

AID = Application Identifier
ATR = Answer-to-Reset
AUT = Autenticazione
C = Certificato
CA = Certification Authority
CAR = Certification Authority Reference
CBC = Cipher Block Chaining
CH = Cardholder
CRT = Control Reference Template
CV = Card Verifiable (Certificato)
DES-3 = Data Encryption Standard, triplo DES
DO = Data Object
DF = Dedicated File
DI = Baud rate adjustment factor
DS = Digital Signature
DSI = Digital Signature Input
EF = Elementary File
FCI = File Control Information
FI = Clock rate conversion factor
FID = File Identifier
GK = Group Key
HB = Historical Bytes
HP = Health Professional
HPC = Health Professional Card
HPD = Health Professional Data
ICC = Integrated Circuit(s) Card
ICCSN = ICC Serial Number
ID = Identifier
IFD = Interface Device
IFSC = Information Field Size Card
IFSD = Information Field Size Device
IIN = Issuer Identification Number
IK = Individual Key
KE = Key Encipherment
KEI = Key Encipherment Input
MF = Master File
MII = Major Industry Identifier
MSE = MANAGE SECURITY ENVIRONMENT
P = Paziente
PA = Personalization Authority
PDC = Patient Data Card
PK = Public Key
PI = Padding Indicator
PIN = Personal Identification Number
PPS = Protocol Parameter Selection
PSO = PERFORM SECURITY OPERATION
RC = Retry Counter
RCA = Root CA
RD = Reference Data
RND = Random Number
RSA = Algorithm of Rivest,Shamir,Adleman
S = Server
SSD = Security Service Descriptor
SK = Secret Key (equiv. to private key)
SN = Serial Number
UID = User Identification
VD = Verification Data

3.2 Simboli

Per le chiavi ed i certificati si utilizza la seguente notazione semplificata di Backus-Naur:

```
<object descriptor> ::= <key descriptor> |
<certificate descriptor>

<key descriptor>::=
<key>.<keyholder>.<usage>

      <key>::= <secret key> | <public key>
      | <group key> | <individual key>

      <secret key>::= SK (asym.)
      <public key>::= PK (asym.)
      <group key>::= GK (sym.)
      <individual key>::=IK (sym.)

      <keyholder>::= <health professional>
      | <patient> | <certification
      authority> | <health professional
      card> | <patient data card>

      <health professional> ::= HP
      <patient> ::= P
      <certification authority>::= CA | RCA
      <health professional card> ::= HPC
      <patient data card> ::= PDC


      <usage>::= <digital signature> | <key
      encipherment> | <authentication>

      <digital signature>::= DS
      <key encipherment >::= KE
      <authentication>::= AUT
```

Per le stringhe di dati successivi si utilizza la seguente notazione:

|| = Concatenazione di dati

4 Caratteristiche tecniche

Le HPC sono “smartcard" a contatto con “cryptocontroller” in grado di eseguire algoritmi a chiave pubblica e simmetrici. Le caratteristiche fisiche sono conformi ad ISO/IEC 7816-1 e standard collegati.
Le dimensioni e la posizione dei contatti è coerente con ISO/IEC 7816-2. I dati sono trasmessi tramite ‘direct convention’. La tecnologia alla base delle HPC è 5V/3V class AB cards (preferenziale) o 5V class A cards.
Una HPC è una carta di dimensioni normali (ID-001 card).

5 Answer-to-Reset

5.1 Global interface characters

Le caratteristiche sono:

- Direct convention
- Protocollo di trasmissione T=1.

5.2 Historical Bytes

Per la codifica degli Historical Bytes (obbligatori) si applicano le seguenti convenzioni in accordo con ISO/IEC 7816-4:

CI = ‘00’ come da ISO/IEC 7816-4

TPI = ‘6x’ come da ISO/IEC 7816-4
(x è la lunghezza di DO)

ICM = IC Manufacturer Id (vedi Tab. 1)

ICT = Manufacturer specific (1 byte)

OSV = Manufacturer specific (2 bytes)

DD = Discretionary data (7 bytes):
DD1 - ATR coding version
DD2 - Card type: ‘x2’ dove x è il livello del primo set di Master keys (valori da ‘1’ a ‘9’ per le chiavi di produzione, valori ‘0’ e da ‘A’ a ‘E’ per le chiavi di test, valore ‘F’ RFU)
DD3 – Livello del secondo set di Master Keys
DD4, DD5, DD6 – “HPC”
DD7 – RFU (1 byte)

TCP = ‘3x’ come da ISO/IEC 7816-4
(x è la lunghezza di DO)

CP = Come da ISO/IEC
7816-4 (cioè ‘80’ per ‘direct application selection’)

CLS = Card Life Cycle (default ‘00’)

SW1-SW2 = ‘9000’

Historical Bytes

CI	PIDO	CPDO	CLS	SW1-SW2

CI = Category indicator (´00´)
PIDO = Pre-issuing data object
CPDO = Card profile data object
CLS = Card life status (1 byte)
SW1-SW2 = Status bytes

Pre-issuing Data Object

TPI	ICM	ICT	OSV	DD

TPI = Tag pre-issuing DO (´6x´)
ICM = IC manufacturer Id (1 byte)
ICT = IC type (1 byte, if b8 = 0;
2 bytes, if b8 = 1 of first byte)
OSV = Operating system version (2 bytes)
DD = Discretionary data (x bytes)

Card Profile Data Object

TCP	CP

TCP = Tag card profile DO (´3x´)
CP = Card profile according to
ISO/IEC 7816-4, 8.3.2 (1 byte)

Fig. 1: Struttura degli Historical Bytes

La Tab. 1 mostra i valori per ICM.

ICM	IC Manufacturer Come da ISO/IEC 7816-6/AM 1
‘01’	Motorola
‘02’	STMicroelectronics
‘03’	Hitachi
‘04’	Philips Semiconductors
‘05’	Siemens
‘06’	Cylinc
‘07’	Texas Instruments
‘08’	Fujitsu
‘09’	Matsushita
‘0A’	NEC
‘0B’	Oki
‘0C’	Toshiba
‘0D’	Mitsubishi
‘0E’	Samsung
‘0F’	Hyundai
‘10’	LG

Tab. 1: codifica ICM

6 Protocol Parameter Selection

Il Protocol Parameter Selection (PPS) in accordo con ISO/IEC 7816-3 sarà supportato dalla HPC per la negoziazione dei valori FI/DI per velocità maggiori.

7 Protocolli di trasmissione

La HPC deve supportare il protocollo di trasmissione asincrono block half-duplex T=1.

L'implementazione di T=1 sarà in accordo con ISO/IEC 7816-3.

8 Diagramma di flusso

Dopo il reset il Master File è selezionato implicitamente. Nel primo passo, i Global data objects ICCSN (ICC Serial No.) e CHN (Cardholder Name come stampato sulla carta) saranno letti.

Il successivo passo richiede la selezione della applicazione HP. Può essere utilizzata la "direct application selection" per selezionare direttamente il file EF.HPD.

Una volta selezionata l'applicazione, e ogni volta in seguito, è possibile l'accesso al File EF.HPD con i dati del professionista della sanità (Health Professional Data).

Prima di poter accedere ai servizi di sicurezza, è richiesta l'autenticazione dell'HP, cioè il professionista deve far verificare i suoi dati (PIN).

Il PIN può essere modificato in qualunque momento ed il contatore di retry, che blocca l'utilizzo del servizio di sicurezza dopo "n" errori consecutivi nella presentazione dei dati di verifica, può essere azzerato se viene inserito dall'HP il codice di reset.

Dopo l'autenticazione dell'HP la HPC è pronta per fornire senza limitazioni i servizi di sicurezza, in particolare l'Interazione con le PDC.

Il PIN non deve essere ulteriormente richiesto fino all'eventuale reset della HPC.

9 Struttura e contenuto dei file

9.1 Struttura dei file e condizioni di accesso

L'organizzazione dei file nella HPC è in accordo con ISO/IEC 7816-4.

Gli identificatori dei file (FIDs) e le condizioni di accesso agli elementary files sono riportati in allegato_A.

Le condizioni di accesso supportate a livello EF/DF saranno, tra l'altro, le seguenti:

- PIN
- Mutua autenticazione
- Mutua autenticazione e PIN
- Mutua autenticazione o PIN

9.2 EF.GDO

Il file EF.GDO contiene il DO ICC Serial Number (ICCSN, Tag ´5A´) (vedi Fig. 5), il DO Cardholder Name (CHN, Tag ´5F20´) con lo stesso contenuto della superficie della carta e il DO Discretionary data (Tag '53') contenente la stringa: *HPCyyxxkzhw* con

yy: versione di HPC,
xx: tipo di professionista,
kz: PIN ID (hex) e lunghezza,
h: RFU,
w: schema chiavi contenute (bit "on" per chiave corrispondente attivata).

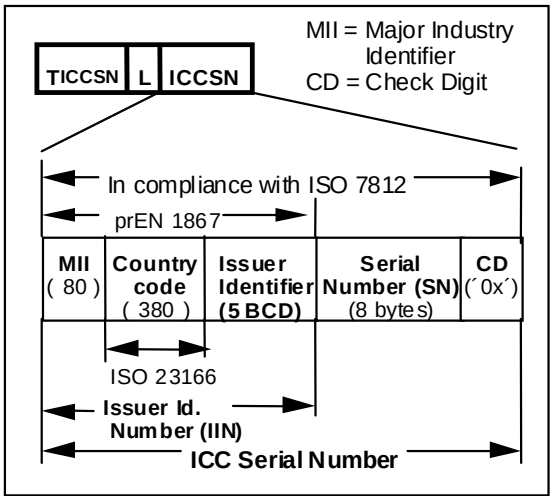


Fig. 2: ICC Serial No.

L'IIN da usare è mostrato in tab. 2.

MII for Health-care	Country Code Italy	Issuer Identifier assigned by registration authority
´80´	´380´	´xxxxx´

Tab. 2: Issuer Identification Number

9.3 Secret key files

Le Secret Keys possono essere memorizzate in uno o più key file in base alle caratteristiche del sistema operativo della carta utilizzata.
L'HPC garantirà che le rispettive chiavi siano utilizzate soltanto per i servizi a cui sono adibite

9.3.1 EF.PIN

Contiene il personal identification number (PIN) del professionista (8 bytes con padding a "FF"). Il Resetting Code (RC) consiste di 8 cifre ASCII.

9.3.2 EF.GK.HP.AU

File selezionato automaticamente dalla Internal Authenticate con le Group keys usate per l'accesso ai file della PDC. Le Group keys sono nella forma Ka e Kb per DES-3. Ogni posizione è riempita con la Group key relativa, o no, a seconda della tipologia di HPC. Il primo set comprende le chiavi da 1 a 8, il secondo le chiavi da 9 a 16.

9.4 Data files

9.4.1 EF.DIR

EF.DIR contiene il FID di EF.HPD

9.4.2 EF.HPD

L'EF.HPD contiene DO che danno una descrizione del professionista, incapsulati nel Cardholder Related Data Template (Tag ´65´, vedi ISO/IEC 7816-6, allegato A, tabella A.2) e della sua HPC (Tag '66'). Per una descrizione dei campi previsti vedi Allegato B.

10 Apertura della HPC

10.1 Sequenza dei comandi

Dopo il reset e la selezione dei file possono essere letti i Global data objects ICCSN e CHN.

10.2 Lettura dei Global data objects

Per leggere i Global data objects sono usati i comandi ISO/IEC 7816-4 SELECT FILE e READ BINARY.

CLA	'00'
INS	'A4' = SELECT FILE
P1	'00'
P2	'00'
Lc	'02' = Length of subsequent data field
Data field	FID of EF.GDO, vedi allegato A
Le	Empty

Tab. 3: comando SELECT FILE per selezionare il File GDO

Data field	Empty
SW1-SW2	'9000' or specific status bytes

Tab. 4: risposta SELECT FILE

CLA	'00'
INS	'B0' = READ BINARY
P1,P2	'0000'
Lc	Empty
Data field	Empty
Le	'xx' length od data to be read

Tab. 5: comando READ BINARY per leggere i global data objects

Data field	Global data objects
SW1-SW2	'9000' or specific status bytes

Tab. 6: risposta READ BINARY

11 Protocollo applicativo

L'applicazione HP consiste delle seguenti fasi:

- Apertura applicazione HP
- Autenticazione
- Manutenzione HPC

Nel seguito vengono descritti i comandi relativi a tali fasi.

12 Apertura applicazione HP

La sequenza di comandi per la fase di apertura dell'applicazione HP è mostrata nel seguito

12.1 Selezione applicazione

Il comando ISO/IEC 7816-4 per la 'Direct Application Selection' è mostrato in tab. 8 e 9.

CLA	'00'
INS	'A4' = SELECT FILE
P1	'04' = DF selection by AID
P2	'00'
Lc	'05' = Length of subsequent data field
Data field	'A000000073'= AID of HP-application
Le	Empty

Tab. 7: comando SELECT FILE con AID

Data field	Empty
SW1-SW2	'9000' or specific status bytes

Tab. 8: risposta SELECT FILE

12.2 Lettura dati professionista

Per la lettura degli Health Professional Data sono necessari i seguenti comandi:

CLA	'00'
INS	'A4' = SELECT FILE
P1	'00'
P2	'00'
Lc	'02' = Length of subsequent data field
Data field	FID of EF.HPD, vedi allegato A
Le	Empty

Tab. 9: comando SELECT FILE

Data field	Empty
SW1-SW2	'9000' or specific status bytes

Tab. 10: risposta SELECT FILE

CLA	'00'
INS	'B0' = READ BINARY
P1,P2	'0000' or offset
Lc	Empty
Data field	Empty
Le	'xx' = Length of data to be read

Tab. 11: comando READ BINARY

Data field	HP data
SW1-SW2	'9000' or specific status bytes

Tab. 12: risposta READ BINARY

13 Autenticazione

13.1 Autenticazione del professionista della sanità

Il professionista deve presentare un PIN (formattato a 'FF' se minore di 8 bytes) per provare di essere il legittimo possessore della HPC. A tal fine è usato il comando VERIFY di ISO/IEC 7816-4.

CLA	'00'
INS	'20' = VERIFY
P1	'00'
P2	'xx' = PIN qualifier
Lc	'08' = PIN length
Data field	PIN
Le	Empty

Tab. 13: comando VERIFY

Data field	Empty
SW1-SW2	'9000' or specific status bytes

Tab. 14: risposta VERIFY

Dopo la presentazione del corretto PIN o password, il retry counter è automaticamente impostato al suo valore iniziale.

I seguenti Status Bytes hanno particolare rilevanza:

- '6300': Warning - verification failed (no further information)
- '6983': Checking error: authentication method blocked (these status bytes shall be delivered, if the VERIFY command is sent and the RC is zero).

13.2 Autenticazione HPC/PDC

La fase di interazione tra HPC e PDC (mutual symmetric authentication) è descritta in Allegato C con riferimento al documento Netlink "Requirements for interoperability".

14 Manutenzione HPC

14.1 Cambiare PIN

Il comando CHANGE RD può essere usato in qualunque momento a scelta dell'HP per cambiare PIN.

CLA	´00´
INS	'24' = CHANGE REFERENCE DATA
P1	'00' = Exchange reference data
P2	'xx' = PIN qualifier
Lc	'10' = Length of subsequent data field
Data Field	Old PIN followed by new PIN (ASCII coding)
Le	Empty

Tab. 15: comando CHANGE RD

Data field	Empty
SW1-SW2	'9000' or specific status bytes

Tab. 16: risposta CHANGE RD

14.2 Reset di RC

Con il comando RESET RETRY COUNTER di ISO/IEC 7816-8, l'HP può attivare il reset dell'RC al suo valore iniziale. Il Resetting Code avrà una lunghezza fissa di 8 byte (8 digits forniti come caratteri ASCII).

Il supporto di tale comando è obbligatorio.

CLA	´00´
INS	'2C' = RESET RETRY COUNTER
P1	'00' = Reset retry counter and set new reference data
P2	'xx' = PIN qualifier
Lc/P3	'10' = Length of subsequent data field
Data Field	Resetting code (8 bytes) followed by new PIN
Le	Empty

Tab. 17: comando RESET RETRY COUNTER

Data field	Empty
SW1-SW2	'9000' or specific status bytes

Tab. 18: risposta RESET RETRY COUNTER

Dopo la presentazione del corretto Resetting Code, il retry counter viene automaticamente impostato al suo valore iniziale e anche il PIN viene cambiato.

Allegato A – File dati della HPC

Caratteristiche dei file dati della HPC

La seguente tabella mostra i file HPC con le loro caratteristiche

File	**FID**	**File structure**	**Access condition**
EF.GDO (Global Data Objects)	'2F02'	transparent	Read: always Update: never
DF.NETLINK	*'D000'*	*transparent*	
EF.DIR	'2F00'	transparent	Read: always Update: never
EF.HPD (HP Data)	'D001'	transparent	Read: always Update: never

Tab. A.1: caratteristiche dei file dati della HPC

Allegato B – File HPD

Caratteristiche del file dati della HPC

La seguente tabella mostra i campi del file HPD con le loro caratteristiche:

Tag	Length	Value	Status
´65´	***x***	***Cardholder related data***	***mandatory***
´5B´	x	Surname at birth	mandatory
´5F20´	x	Card holder name	mandatory
´5F2C´	3	Nationality (UNI EN ISO 3166-1)	mandatory
´5F2B´	8	Date of birth (YYYYMMDD)	mandatory
´5F30´	16	Service code, in this context used for National identification number	mandatory
´42´	5	Issuer authority	mandatory
´53´	x	Discretionary data, used for HP Regional number	mandatory
´66´	***x***	***Card related data***	***mandatory***
´59´	8	Card expiration date: YYYYMMDD	mandatory
´5F26´	8	Card effective date: YYYYMMDD	mandatory
´53´	2	Discretionary data, used for HPC type	mandatory
‘5F21’	Ans.76	Track 1	optional
‘5F22’	n.37	Track 2	optional
‘5F23’	n.104	Track 3	optional

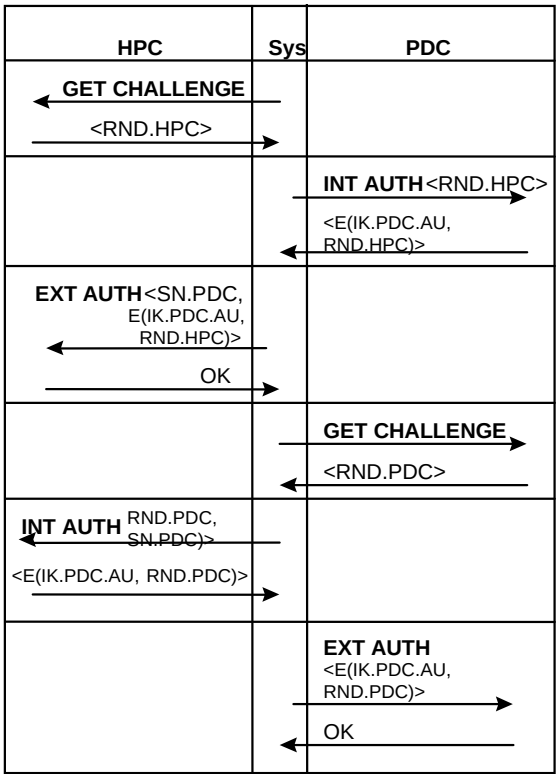
Tab. B.1: caratteristiche del file dati della HPC

Allegato C - Mutua autenticazione con algoritmo simmetrico

(tratto dal documento Netlink “Requirement for interoperability”)

Lo schema di mutua autenticazione è mostrato nel seguito

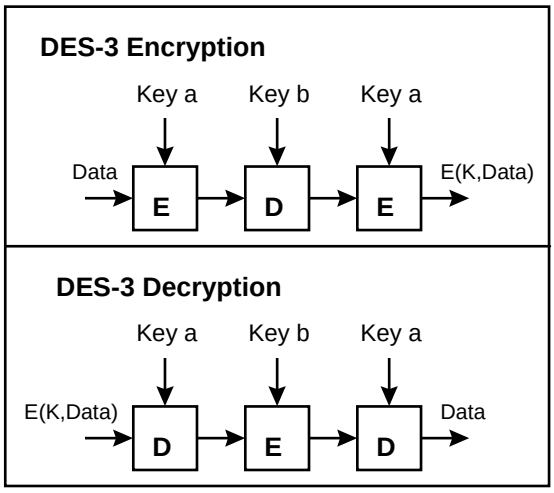
Fig. 3 Mutua autenticazione tra HPC e PDC



Se la carta PDC si autentica al sistema tramite protocolli asimmetrici (RSA), la prima parte dell’autenticazione descritta in Fig. 3 può essere omessa.

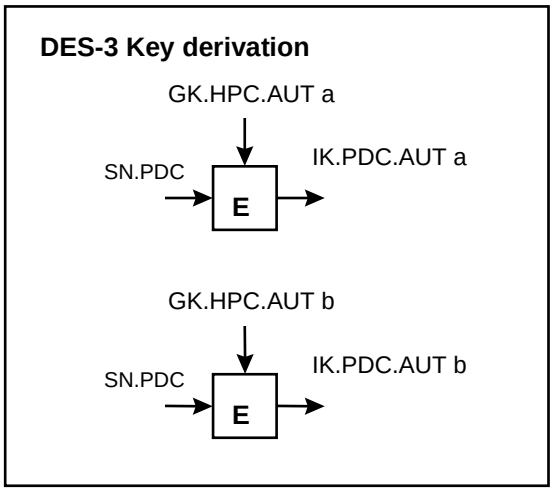
Per la encryption e decryption del challenge, è applicato il DES-3 come mostrato in Fig. 4.

Fig. 4 Encryption/Decryption with DES-3



La derivazione della individual key del PDC (IK.PDC.AUT-PHYS) con la group key del medico è mostrata in Fig. 5.

Fig. 5 Key derivation



Il primo comando da mandare all'HPC è il comando GET CHALLENGE.

TabellaC.1: comando GET CHALLENGE

CLA	'00'
INS	´84´ = GET CHALLENGE
P1, P2	´0000´
Lc	Empty
Data field	Empty
Le	´08´

tabella C.2: risposta GET CHALLENGE

Data field	RND.HPC (8 bytes)
SW1-SW2	´9000´ or specific status bytes

Dopo il GET CHALLENGE segue il comando EXTERNAL AUTHENTICATE. Nell'HPC deve essere calcolata la individual PDC-key, prima che il crttogramma possa essere decifrato e confrontato con il challenge.

tabella C.3: comando EXT. AUTHENTICATE

CLA	'00'
INS	´82´ = EXTERNAL AUTHENTICATE
P1	´00´
P2	´xx´ = KID
Lc	´10´ = Length of subsequent data field
Data field	Authentication related data (DES-3 Cryptogram): SN.PDC (8 bytes) || E (GK.PHYS.AUT, RND)
Le	Empty

tabella C.4: risposta EXT. AUTHENTICATE

Data field	Empty
SW1-SW2	´9000´ or specific status bytes

Infine il professionista deve provare che nell'HPC è presente la chiave richiesta.

tabella C.5: comando INTERNAL AUTHENTICATE per provare il diritto di accesso alla PDC

CLA	'00'
INS	'88' = INTERNAL AUTHENTICATE
P1	'00' = Implicit alg. selection (DES-3)
P2	'xx' = KID
Lc	'10' = Length of subsequent data field
Data field	SN.PDC (8 bytes, data item for deriving IK.PDC.AUT-PHYS) followed by a challenge (8 bytes)
Le	'00'

tabella C.6: risposta INTERNAL AUTHENTICATE

Data field	Enciphered challenge, 8 bytes: E(IK.PDC.AUT-PHYS, RND.PDC)
SW1-SW2	'9000' or specific status bytes

Il crittogramma calcolato viene poi inviato alla PDC per la verifica dell'autenticazione.