NETLINK – Specifiche PDC

NK/4/FNS/T/3/1.3

Reference:	NK/4/FNS/T/3/1.3
Date of last change:	22.12.06
Authors:	G. Meazzini
Stage:	Version 1.3

Contenuto

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 sanitarie dei pazienti (PDC).

Le specifiche PDC 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.

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

2.1 Variazioni rispetto alla precedente versione

- note aggiuntive su GDO ed NKCF

3 Abbreviazioni e notazioni

3.1 Abbreviazioni

AID = Application Identifier
ATR = Answer-to-Reset
AUT = Authentication
CH = Cardholder
CRT = Control Reference Template
DES-3 = Data Encryption Standard, triple DES
DO = Data Object
DF = Dedicated File
DI = Baud rate adjustment factor
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
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
MF = Master File
MII = Major Industry Identifier
P = Patient
PDC = Patient Data Card
PK = Public Key
PI = Padding Indicator
PIN = Personal Identification Number
PPS = Protocol Parameter Selection
RC = Retry Counter
RD = Reference Data
RND = Random Number
S = Server
SK = Secret Key (equiv. to private key)
SN = Serial Number
UID = User Identification
VD = Verification Data

3.2 Notazioni

Per le chiavi la seguente notazione semplificata di Backus-Naur si applica:

```
<object descriptor> ::= <key 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> | <health professional
      card> | <patient data card>

      <health professional> ::= HP
      <patient> ::= P
      <health professional card> ::= HPC
      <patient data card> ::= PDC

      <usage>::= <authentication>

      <authentication>::= AU
```

|| = Concatenazione di dati

4 Caratteristiche tecniche

Le PDC sono “smartcard" a contatto in grado di eseguire algoritmi simmetrici tipo DES-3 per le funzioni di sicurezza. Le caratteristiche fisiche sono conformi ad ISO/IEC 7816-1 e standard collegati.
Le dimensioni e la posizione dei contatti sono coerenti con ISO/IEC 7816-2. I dati sono trasmessi tramite ‘direct convention’. La tecnologia è 5V/3V class AB cards (preferenziale) o 5V class A cards.
Una PDC è una carta di dimensioni normali (ID-001 card).

5 Answer-to-Reset

La codifica raccomandata per gli Historical bytes dell’ATR è mostrata in seguito:

5.1 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 (3 bytes):
DD1 - ATR coding version
DD2 - Netlink card type: ‘x1’ dove x è il livello delle Master Keys (valori da ‘1’ a ‘9’ chiavi di produzione, valori ‘0’ e da ‘A’ a ‘E’ chiavi di test, valore ‘F’ RFU)
DD3 - Certification tag
TCP = ‘31’ come da ISO/IEC 7816-4
(1 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’

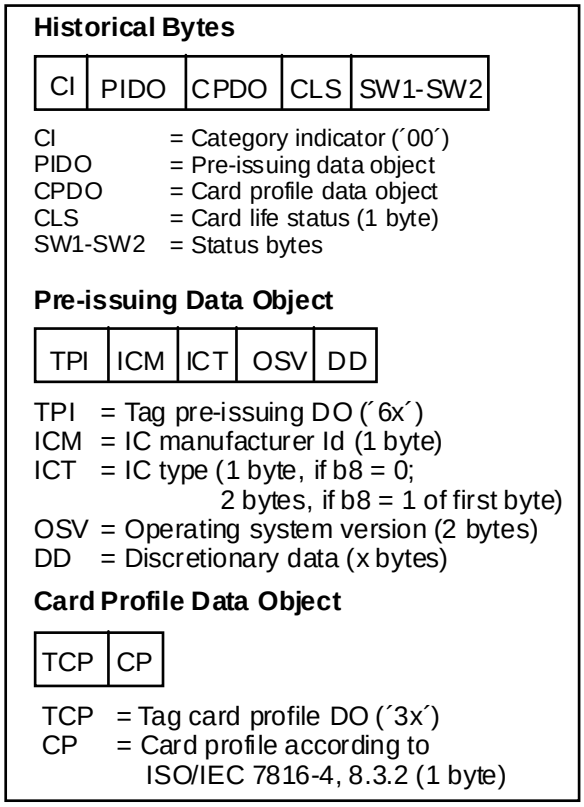

Fig. 1: Struttura degli Historical Bytes

Tab. 1 - Valori per ICM.

ICM	**IC Manufacturer** **according to 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: ICM coding

6 Protocol Parameter Selection

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

7 Protocolli di trasmissione

Il protocollo di trasmissione supportato, T=0 o T=1, sarà indicato nell'ATR.

L'implementazione sarà in accordo con ISO/IEC 7816-3. Nella descrizione dei comandi seguenti, nel caso T=0 il parametro P3 va usato, così come specificato in ISO/IEC 7816-4, al posto di Lc ed Le.

8 Diagramma di flusso

Il diagramma di flusso riportato in fig. 3 mostra le fasi relative all'uso della PDC.

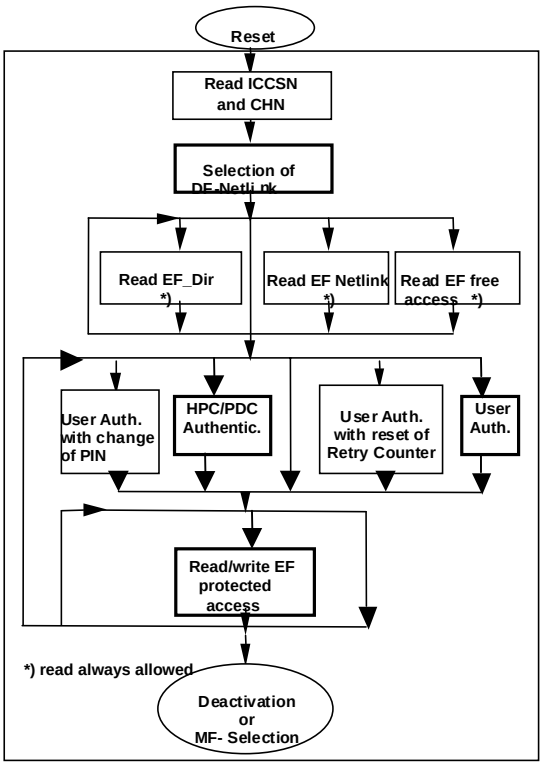

Fig. 2: Diagramma di flusso

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 sul fronte della carta) saranno letti.

Il successivo passo richiede la selezione della DF.Netlink attraverso la selezione applicazione tramite AID (riferimento "application independent card services" come definiti in ISO/IEC 7816-4).

Una volta selezionata l'applicazione, e ogni volta in seguito, sarà possibile l'accesso ai seguenti file:

- File EF.DIR contiene l'indirizzo di EF.NETLINK
- File EF.NETLINK contiene gli indirizzi degli EF con dati a codifica internazionale
- File EF.NETKITA contiene gli indirizzi degli EF con dati a codifica nazionale
- File EF.NKCF contiene i dati della carta a lettura libera
- Files EF.NKAF contiene i dati amministrativi a lettura libera
- File EF.NKEF contiene i dati di emergenza a lettura libera

Il prossimo passo richiede una procedura di autenticazione attraverso la presentazione del PIN e/o la mutua autenticazione HPC/PDC. L'accesso protetto (in lettura o in scrittura a seconda dei file) è soggetto a:

- Mutua autenticazione PDC/HPC. Il professionista sanità deve provare il suo diritto ad accedere un EF: la group key contenuta nella HPC sarà usata per derivare la PDC Individual key relativa all'EF/DF da accedere.

e/o

- La verifica del PIN, cioè il possessore della carta deve presentare il suo codice personale. Il PIN può essere cambiato in qualsiasi momento. Il contatore di tentativi (retry counter) bloccherà la carta dopo "n" tentativi falliti; per sbloccare il contatore e riposizionarlo a zero è necessario inserire il codice di reset.

Se un comando di lettura o scrittura è effettuato su un EF la PDC deve verificare il rispetto delle condizioni di accesso relative all'EF o alla DF relativa (vedi allegato_A).

9 Struttura e contenuto dei file

9.1 Struttura dei file e condizioni di accesso

L'organizzazione dei file nella PDC è in accordo con ISO/IEC 7816-4. La struttura dei file e le condizioni di accesso agli EF sono riportati in allegato_A.

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

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

Le condizioni di accesso (e le chiavi di autenticazione) definite a livello EF potranno essere diverse in lettura e in scrittura.

9.2 File a livello MF

9.2.1 EF.GDO

Il file EF.GDO contiene il DO ICC Serial Number (ICCSN, Tag ´5A´) (vedi Fig. 4), il DO Cardholder Name (CHN, Tag ´5F20´) con lo stesso contenuto della superficie di una carta ID-1 ed il DO Dati Discrezionali (Tag '53') con la stringa 'PDCxxxx' (xxxx versione file system) seguita da 5 coppie (2 byte FID, 2 byte lunghezza) per gli EF dei dati applicativi contenuti nella carta. Le lunghezze "minime" suggerite per le 5 coppie sono rispettivamente: "D10107D0", "D20109C4", "D30107D0", "D40109C4", "D50103E8". Per carte CNS, in caso di personalizzazione differita, cioè se la struttura Netlink viene inizializzata prima che sia definito il titolare e/o il serial number della carta, il file può essere impostato a '00'.

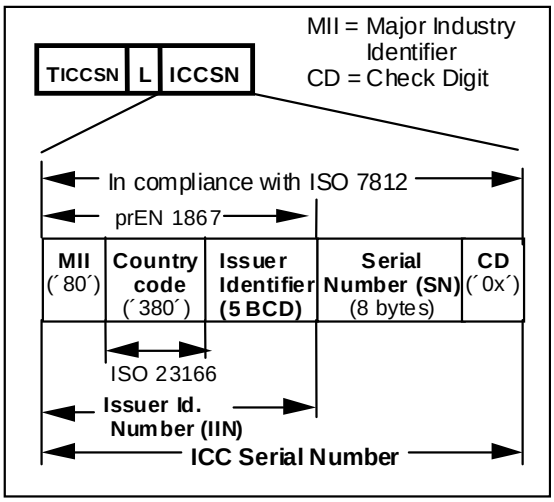

Fig. 3: ICC Serial No.

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 keys files

Le Secret Keys possono essere memorizzate in uno o più file chiavi in base alle caratteristiche del sistema operativo della carta utilizzata.
La PDC garantirà che le rispettive chiavi siano utilizzate soltanto per i servizi (e per gli EF/DF) a cui sono adibite.

9.3.1 EF.PIN

Nell'EF.PIN è memorizzato il personal identification number (PIN) (8 bytes con eventuale padding a "FF"). Il Resetting Code (RC) consiste di 8 cifre ASCII.

9.3.2 EF.IK.AU

Per ogni EF ad accesso protetto saranno selezionate automaticamente dal comando External Authenticate le Individual keys necessarie per l'accesso ai file. Le individual keys sono nella forma Ka e Kb per DES-3. La posizione per la lettura è "2", per la scrittura è "4".

9.4 File dati

9.4.1 EF.DIR

EF.DIR contiene il FID di EF.NETLINK.

9.4.2 EF.NETLINK

EF.NETLINK contiene gli ID's degli EF che contengono i dati previsti nel data set di interoperabilità internazionale (vedi Allegato B).

9.4.3 EF.NETKITA

EF.NETKITA contiene gli ID's degli EF che contengono i dati previsti nel data set di interoperabilità nazionale (vedi Allegato B).

9.4.4 EF.NKCF

EF.NKCF contiene i gruppi di dati che descrivono la carta secondo il dataset di interoperabilità. Tutti i gruppi sono incapsulati in un gruppo con Tag ´31´, cioè SET secondo ISO/IEC 8825. Per carte CNS, in caso di personalizzazione differita, cioè se la struttura Netlink viene inizializzata prima che sia definito l'ente emettitore e/o il serial number della carta, il file può essere impostato a '00'.

9.4.5 EF.NKAF

EF.NKAF contiene i gruppi di dati che descrivono i dati amministrativi secondo il dataset di interoperabilità. Tutti i gruppi sono incapsulati in un gruppo con Tag ´31´, cioè SET secondo ISO/IEC 8825.

9.4.6 EF.NKEF

EF.NKEF contiene i gruppi di dati che descrivono i dati di emergenza secondo il dataset di interoperabilità. Tutti i gruppi sono incapsulati in un gruppo con Tag ´31´, cioè SET secondo ISO/IEC 8825.

9.4.7 EF.NKAP

EF.NKAP contiene i gruppi di dati che descrivono i dati amministrativi protetti nazionali. Tutti i gruppi sono incapsulati in un gruppo con Tag ´31´, cioè SET secondo ISO/IEC 8825.

9.4.8 EF.NKEP

EF.NKCF contiene i gruppi di dati che descrivono i dati di emergenza secondo il dataset di interoperabilità. Tutti i gruppi sono incapsulati in un gruppo con Tag ´31´, cioè SET secondo ISO/IEC 8825.

9.4.9 EF.NKPP

EF.NKPP contiene i gruppi di dati (nazionali) che descrivono i puntatori agli eventi della storia clinica. Tutti i gruppi sono incapsulati in un gruppo con Tag ´31´, cioè SET secondo ISO/IEC 8825.

10 Apertura della PDC

10.1 Sequenza dei comandi

Dopo il reset 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/P3	'02' = Length of subsequent data field
Data field	FID of EF.GDO, see annex A
Le	Empty

Tab. 3: comando SELECT FILE per 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' or offset
Lc	Empty
Data field	Empty
Le/P3	Number of bytes to be read

Tab. 5: READ BINARY per lettura GDO

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

Tab. 6: risposta READ BINARY

11 Protocollo applicativo

L'applicazione Netlink consiste delle seguenti fasi:

- Apertura applicazione Netlink
- Accesso dati liberi
- Autenticazione del possessore carta e/o
- Autenticazione HPC/PDC
- Accesso dati protetti
- Manutenzione PDC

Nel seguito vengono descritti i comandi relativi a tali fasi.

12 Apertura applicazione Netlink

12.1 Selezione applicazione

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

CLA	'00'
INS	'A4' = SELECT FILE
P1	'04' = DF selection by AID
P2	'00'
Lc/P3	'05' = Length of subsequent data field
Data field	'A000000073'= AID of Netlink-application
Le	Empty

Tab. 7: comando SELECT FILE per "application selection with AID"

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

Tab. 8: risposta SELECT FILE

12.2 Lettura EF.Netlink

CLA	'00'
INS	'B0' = READ BINARY
P1,P2	'0000' or offset
Lc	Empty
Data field	Empty
Le/P3	'xx' = Length of data to be read

Tab. 9: READ BINARY di EF.Netlink

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

Tab. 10: risposta READ BINARY

13 Accesso dati liberi

I file ad accesso libero in lettura sono

- EF.NKAF (amministrativi)
- EF.NKEF (emergenza)
- EF.NKCF (carta)

CLA	'00'
INS	'A4' = SELECT FILE
P1	'00'
P2	'00'
Lc/P3	'02' = Length of subsequent data field
Data field	FID (see annex A) of - EF.NKAF - EF.NKEF - EF.NKCF
Le	Empty

Tab. 11: comando SELECT FILE

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

Tab. 12: risposta SELECT FILE

CLA	'00'
INS	'B0' = READ BINARY
P1,P2	'0000' or offset
Lc	Empty
Data field	Empty
Le/P3	'xx' = Length of data to be read

Tab. 13: READ BINARY per EF lettura libera

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

Tab. 14: risposta READ BINARY

14 Autenticazione possessore carta

Il possessore della carta deve inserire il proprio PIN per permettere l'accesso agli EF/DF protetti. Si utilizza il comando ISO/IEC 7816-4 VERIFY.

CLA	'00'
INS	'20' = VERIFY
P1	'00'
P2	'xx' = PIN qualifier
Lc/P3	'08' = PIN length
Data field	PIN
Le	Empty

Tab. 15: comando VERIFY

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

Tab. 16: 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).

15 Autenticazione HPC/PDC

Per permettere l'accesso agli EF/DF protetti, la sequenza di autenticazione deve essere verificata tra HPC e PDC.

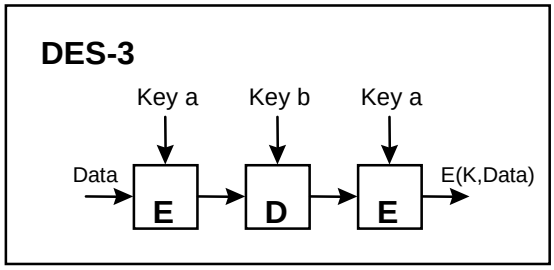

Fig. 4 Encryption with DES-3

La sequenza di comandi inviati alla PDC è mostrata in seguito:

CLA	'00'
INS	'88' = INTERNAL AUTHENTICATE
P1	'00' = Implicit alg. Selection (DES-3)
P2	KID
Lc/P3	'08' = Length of subsequent data field
Data field	RND.HPC (challenge, 8 bytes)
Le	'00'

table 1: INTERNAL AUTHENTICATE command for proving access rights to a PDC

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

table 2: INTERNAL AUTHENTICATE response

Il risultato è inviato alla HPC per verifica autenticazione. Nel caso in cui la PDC si autentichi al sistema attraverso un protocollo asimmetrico (RSA), il comando di Internal Authenticate può essere omesso.

CLA	'00'
INS	´84´ = GET CHALLENGE
P1, P2	´0000´
Lc	Empty
Data field	Empty
Le/P3	´08´

table 3: comando GET CHALLENGE per accesso a PDC

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

table 4: risposta GET CHALLENGE

CLA	'00'
INS	´82´ = EXTERNAL AUTHENTICATE
P1	'00' = Implicit alg. Selection (DES-3)
P2	KID
Lc/P3	´08´ = Length of subsequent data field
Data field	Enciphered challenge (8 bytes)
Le	Empty

table 5: comando EXT. AUTHENTICATE

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

table 6: risposta EXT. AUTHENTICATE

16 Accesso dati protetti

Dopo una corretta autenticazione possono essere acceduti EF/DF protetti. La PDC deve verificare che le condizioni di sicurezza per l'accesso a EF o DF sono verificate.

CLA	'00'
INS	'A4' = SELECT FILE
P1	'00'
P2	'00'
Lc	'02' = Length of subsequent data field
Data field	FID (see annex A) of - EF.NKAP - EF.NKEP - EF.NKPP

	- EF.NKAF - EF.NKEF
Le	Empty

Tab. 17: comando SELECT FILE

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

Tab. 18: risposta SELECT FILE

CLA	'00'
INS	'B0' = READ BINARY
P1,P2	'0000' or offset
Lc	Empty
Data field	Empty
Le/P3	'xx' = Length of data to be read

Tab. 19: comando READ BINARY per accesso protetto in lettura

Data field	Data read (Le bytes)
SW1-SW2	'9000' OK or '6982' security status not satisfied or other specific status bytes

Tab. 20: risposta READ BINARY

CLA	'00'
INS	'D6' = UPDATE BINARY
P1,P2	'0000' or offset
Lc/P3	Length of the subsequent data field
Data field	String of data units to be updated
Le	Empty

Tab. 21: comando UPDATE BINARY per scrittura protetta

Data field	Empty
SW1-SW2	'9000' OK or '6982' security status not satisfied or other specific status bytes

Tab. 22: risposta UPDATE BINARY

17 Manutenzione PDC

17.1 Cambiamento PIN

Il comando CHANGE RD può essere usato in qualsiasi momento.

CLA	´00´
INS	'24' = CHANGE REFERENCE DATA
P1	'00' = Exchange reference data
P2	'xx' = PIN qualifier
Lc/P3	'10' = Length of subsequent data field
Data Field	Old PIN followed by new PIN (ASCII coding)
Le	Empty

Tab. 23: comando CHANGE RD

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

Tab. 24: risposta CHANGE RD

17.2 Reset di RC

Con il comando RESET RETRY COUNTER di ISO/IEC 7816-8, RC è riportato al suo valore iniziale. Il Resetting Code avrà una lunghezza fissa di 8 byte (8 digits forniti come caratteri ASCII).

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. 25: comando RESET RETRY COUNTER

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

Tab. 26: 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 – PDC files

1 Struttura logica dei file

Una possibile struttura dei file della PDC è mostrata nella figura seguente :

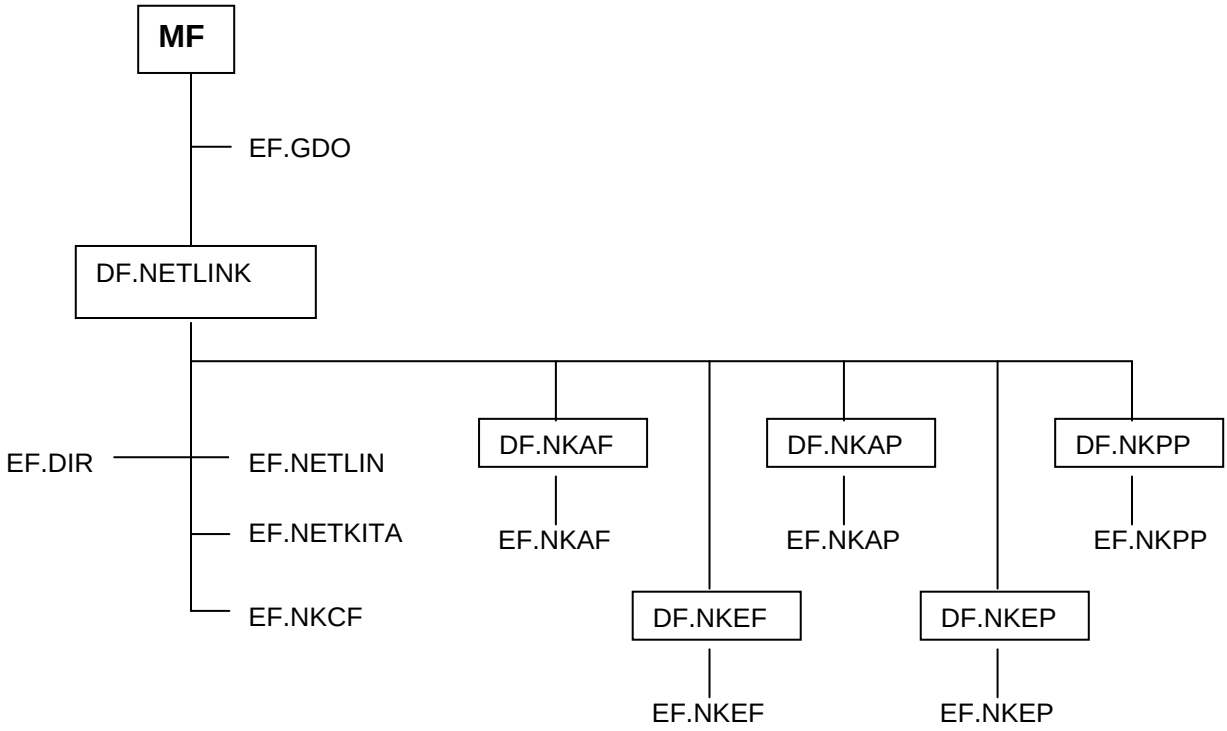

Fig. 5: struttura file della PDC

2 Caratteristiche di EF e DF

File	FID	File structure	Read access condition	Update access condition
EF.GDO	'2F02'	Transparent	Always	never
DF.NETLINK	***'D000'***			
EF.DIR	'2F00'	transparent	always	never
EF.NETLINK (Netlink pointers)	'D002'	transparent	always	never
EF.NETKITA (National pointers)	'D004'	transparent	always	never
EF.NKCF (Card free data)	'D003'	transparent	always	never
DF.NKAF	***'D100'***			
EF.NKAF (Administrative free data)	'D101'	transparent	always	AM or MB
DF.NKEF	***'D200'***			
EF.NKEF (Emergency free data)	'D201'	transparent	always	MB
DF.NKAP	***'D300'***			
EF.NKAP (Administrative protected data)	'D301'	transparent	AM or AL or MB or ME or PIN	AM or MB
DF.NKEP	***'D400'***			
EF.NKEP (Emergency protected data)	'D401'	transparent	MB or ME or PIN	MB and PIN
DF.NKPP	***'D500'***			
EF.NKPP (Pointers protected data)	'D501'	transparent	AM or AL or MB or ME or ER or PIN	AM or MB

Tab. A.1: Caratteristiche EF e DF

Legenda:

AM – carta HPC con autorizzazione alla lettura e scrittura dei dati amministrativi
AL – carta HPC con autorizzazione alla lettura dei dati amministrativi
MB – carta HPC con autorizzazione alla lettura e scrittura dei dati amministrativi e medici
ME – carta HPC con autorizzazione alla lettura dei dati amministrativi e medici
ER – carta HPC con autorizzazione alla lettura di solo alcuni dati amministrativi
PIN – PIN della PDC

Allegato B – Struttura file EF.NETLINK e EF.NETKITA

1 EF.NETLINK

(Tratto dal documento "Netlink - Requirements for Interoperability" NK/2/ZI/A/3/2.2.2)

The content of the EF.NETLINK is defined as the ID's and paths of the EF's containing the patient's data of the G7-interoperability-dataset:

```
NETLINK_DataSet_EFPath ::= SEQUENCE
{
CardFileIdentification              [0] IMPLICIT SEQUENCE OF FileIdentification OPTIONAL,
AdministrativeFileIdentification    [1] IMPLICIT SEQUENCE OF FileIdentification OPTIONAL,
ClinicalFileIdentification          [2] IMPLICIT SEQUENCE OF FileIdentification OPTIONAL,
AdministrativeFilePINprotected      [3] IMPLICIT SEQUENCE OF FileIdentificationPIN OPTIONAL,
ClinicalFilePINprotected            [4] IMPLICIT SEQUENCE OF FileIdentificationPIN OPTIONAL,
AdministrativeFileHPCprotected      [5] IMPLICIT SEQUENCE OF FileIdentificationHPC OPTIONAL,
ClinicalFileHPCprotected            [6] IMPLICIT SEQUENCE OF FileIdentificationHPC OPTIONAL
}

FileIdentification::= SET
{
dFName                              [0] IMPLICIT OCTET STRING OPTIONAL,
dFID                                [1] IMPLICIT OCTET STRING OPTIONAL,
eFID                                [2] IMPLICIT OCTET STRING,
dataFormat                          [3] IMPLICIT ENUMERATED {ASN(0), other(1)} OPTIONAL,
discretionary Data                  [4] IMPLICIT OCTET STRING (SIZE(16)) OPTIONAL
}

FileIdentificationPIN::= SET
{
dFName                              [0] IMPLICIT OCTET STRING OPTIONAL,
dFID                                [1] IMPLICIT OCTET STRING OPTIONAL,
eFID                                [2] IMPLICIT OCTET STRING,
dataFormat                          [3] IMPLICIT ENUMERATED {ASN(0), other(1)} OPTIONAL,
discretionary Data                  [4] IMPLICIT OCTET STRING (SIZE(16)) OPTIONAL,
pinType                             [5] IMPLICIT ENUMERATED {ISO(0), EMV(1)},
pinLength                           [6] IMPLICIT NUMERIC STRING (SIZE(1)),
pinID                               [7] IMPLICIT OCTET STRING (SIZE(1))
}

FileIdentificationHPC::= SET
{
dFName                              [0] IMPLICIT OCTET STRING OPTIONAL,
dFID                                [1] IMPLICIT OCTET STRING OPTIONAL,
eFID                                [2] IMPLICIT OCTET STRING,
dataFormat                          [3] IMPLICIT ENUMERATED {ASN(0), other(1)},
discretionary Data                  [4] IMPLICIT OCTET STRING (SIZE(16)) OPTIONAL,
authenticationType                  [5] IMPLICIT ENUMERATED {symmetric(0), asymmetric(1)}
}
```

Note: one of dFName and dFID is mandatory.
The coded tag value for NETLINK_DataSet_EFPath is '30'.

2 EF.NETKITA

La struttura del file EF.NETKITA è uguale a quella del file EF.NETLINK, ma riferita ai file dati nazionali (Amministrativi protetti e Puntatori Protetti).