

Part 7

**IC cards
with synchronous transmission**

Part 3: Usage of inter-industry Commands

Draft

20.07.95

DIN NI-17.4

Contents

| | |
|---|---|
| 1. Scope | 3 |
| 2. Normative references | 3 |
| 3. Abbreviations | 3 |
| 4. Implementation | 3 |
| 5. Inter-industry commands for basic functions | 3 |
| 5.1 SELECT FILE | 3 |
| 5.2 READ BINARY | 4 |
| 5.3 UPDATE BINARY | 4 |
| 6. Inter-industry commands for security functions | 5 |
| 6.1 VERIFY | 5 |
| 6.2 CHANGE VERIFICATION DATA | 5 |
| Annex A (normative) Processing of the commands VERIFY und CHANGE VERIFICATION DATA | 7 |

1. Scope

The scope of this specification is to describe the use of ISO/IEC 7816-4 inter-industry commands for IC cards with synchronous transmission and to specify how they are mapped on chip specific actions. This specification is valid only for IC cards whose data sections are encoded according to the specification 'IC cards with synchronous transmission, Part 1: ATR and data sections'. It is a prerequisite for the use ISO/IEC 7816-4 inter-industry commands at a CardTerminal Application Interface that the IC card has the structure of the ATR and the data sections according to the specification mentioned above *and* that the CT is capable to map the related inter-industry commands on chip specific actions.

2. Normative references

DIN NI-17: 1995
IC cards with synchronous transmission
Part 1: ATR and Data Sections

DIN NI-17: 1995
IC cards with synchronous transmission
Part 2: Transmission protocols

ISO/IEC 7816-3: 1989
Identification cards - Integrated circuit(s) cards with contacts
Part 3 - Electronic Signals and transmission protocols
AM 1: Clause 9: Protocol T=1, asynchronous half duplex block transmission protocol
AM 2: Protocol type selection
(The WD October 1994 in which AM 1 and AM 2 are intergrated is used)

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

3. Abbreviations

AID = Application Identifier
ATR = Answer-to-Reset
BCD = Binary Coded Digits
CT = CardTerminal
CT-API =CT Application Programming Interface
FID = File Identifier
ICC = Integrated Circuit(s) Card

HTSI = Host Transport Service Interface
PIN = Personal Identification Number
TLV = Tag, Length, Value
VD = Verification Data

4. Implementation

To make access to IC cards with synchronous transmission on the one hand as easy as possible and on the other hand to make it as compatible as possible with access to processor IC cards certain inter-industry commands are mapped in the CardTerminal (or in software applied with the CT) to interactions with the corresponding synchronous IC card. The following commands shall be supported for all IC cards:

- SELECT FILE
- READ BINARY and
- UPDATE BINARY.

For IC cards with security code, the additional commands

- VERIFY and
- CHANGE VERIFICATION DATA

shall be supported. The setting of protection flags (if the chip is provided with a protection memory) is normally carried out during personalisation and is not within the scope of the description of the following commands.

5. Inter-industry commands for basic functions

5.1 SELECT FILE

5.1.1 Function

- a) Selection of an application

To select an application the ISO/IEC 7816-4 SELECT FILE command is used. The application identifier (AID) is hereby to be transmitted in the data field. The card terminal reads the DIR data section and checks whether the AID is present there (structures of the DIR data section acc. to part 1: 'ATR and Data Sections'). If so, the application and with it the application data section is selected and as status '9000' is returned. The application data section begins in mono-application cards directly after the DIR data section, in multi-application cards the beginning of the appli-

cation data section is indicated in the path element of the respective application template.

b) Selection of data sections

A data section in the synchronous card can be selected like a file in a microprocessor IC card by file identifiers (FIDs) or by the file name with the SELECT FILE command:

- the ATR data section, equivalent to the ATR file, has '2F01' as FID and begins after the ATR at byte address '04'
- the DIR data section, equivalent to the DIR file, has '2F00' as FID and begins at byte address cited in byte H4 (see part 1: 'ATR and data sections').
- the application data section has the application identifier as file name and is selected therefore with the SELECT FILE command giving the AID as described in a). The pointer is hereby set to the first byte of the application data section.

In order to be able to select the total data memory, the whole data storage is seen as a sequence of data sections or files that are contained in or subordinated to the master file. For this reason the MF-FID '3F00' is used as FID for the total data memory (address of first byte: '00').

5.1.2 Usage conditions

No restrictions.

5.1.3 Command structure

| | |
|------------|--|
| CLA | '00' |
| INS | 'A4' (= SELECT FILE) |
| P1 | Selection control '00' = FID in data field '04' = AID in data field |
| P2 | '00' |
| Lc field | Length of subsequent data field |
| Data field | AID or FID ('3F00' = MF (= total data memory), '2F00' = DIR data section, '2F01' = ATR data section) |
| Le field | Empty |

Tab. 1: SELECT FILE command

Note: The command is depicted here only with required parameter codings

5.1.4 Response structure

| | |
|-----------------|-----------------------|
| Data SW1-SW2 | Empty Status bytes |
|-----------------|-----------------------|

Tab. 2: SELECT FILE response

5.1.5 Status bytes

'9000' = Command successful
'6A82' = File not found

5.2 READ BINARY

5.2.1 Function

With the READ BINARY command data can be read from the previously selected data section. The first byte of data section has the logical address '0000'. The length of the data section results from the length of the first DO (see 'IC cards with synchronous transmission, Part 1: ATR and data sections').

5.2.2 Usage conditions

The data section to be read has to be selected before.

5.2.3 Command structure

| | |
|------------|--|
| CLA | '00' |
| INS | 'B0' (= READ BINARY) |
| P1, P2 | Offset ('0000' = Logical start address of the file) |
| Lc field | Empty |
| Data field | Empty |
| Le field | Length of data to be read or '00' (= read available data) |

Tab. 3: READ BINARY command

Note: The command is described here only with the supported parameter codings.

5.2.4 Response structure

| | |
|-----------------|---------------------------------|
| Data SW1-SW2 | Data to be read Status bytes |
|-----------------|---------------------------------|

Tab. 4: READ BINARY response

5.2.5 Status bytes

'9000' = Command successful
 '6281' = Data corrupted
 '6282' = Warning, end of file reached before
 reading Le bytes
 '6501' = Memory failure

5.3 UPDATE BINARY

5.3.1 Function

With the UPDATE BINARY command data can be updated in the selected data section. The first byte of the data section has the logical address '0000'. The length of the data section results from the length of the first DO (see 'IC cards with synchronous transmission, Part 1: ATR and data sections') and shall be observed.

5.3.2 Usage conditions

The data section to be updated has to be selected before. With IC cards which allow an alteration of the data memory (or parts thereof) only after successful presentation of the security code the appropriate authentication (see VERIFY command) has first to be carried out.

5.3.3 Command structure

| | |
|------------|---|
| CLA | '00' |
| INS | 'D6' (= UPDATE BINARY) |
| P1, P2 | Offset ('0000' = Logical start address of the file) |
| Lc field | Length of subsequent data field |
| Data field | Data to be written |
| Le field | Empty |

Tab. 5: UPDATE BINARY command

Note: The command is described here only with the supported parameter codings.

5.4.4 Response structure

| | |
|-----------------|-----------------------|
| Data SW1-SW2 | Empty Status bytes |
|-----------------|-----------------------|

Tab. 6: UPDATE BINARY response

5.5.5 Status bytes

'9000' = Command successful
 '6200' = Error

6. Inter-industry commands for security functions

6.1 VERIFY

6.1.1 Function

The VERIFY command initiates the comparison of the verification data with the stored reference data. The sequence is depicted in annex A. Verification data are BCD encoded, when a PIN is concerned, otherwise hexadecimal coding is used.

6.1.2 Usage conditions

The command is only applicable for IC cards with the appropriate security function.

6.1.3 Command structure

| | |
|------------|--|
| CLA | '00' |
| INS | '20' (= VERIFY) |
| P1 | '00' |
| P2 | '00' |
| Lc field | Length of subsequent data field |
| Data field | VERIFICATION DATA (Byte1, Byte 2, Byte 3) Note: a PIN is BCD-coded possibly padded with one or more 'F' |
| Le field | Empty |

Tab. 7: VERIFY command

Note: The command is described here only with the supported parameter codings..

6.1.4 Response structure

| | |
|-----------------|-----------------------|
| Data SW1-SW2 | Empty Status bytes |
|-----------------|-----------------------|

Tab. 8: VERIFY response

6.1.5 Status bytes

'9000' = Command successful
 '63Cx' = Verification unsuccessful,
 x = number of possible retries
 '6983' = Verification method blocked

Tab. 10: CHANGE VERIFICATION DATA response

6.2.5 Status bytes

'9000' = Command successful
 '63Cx' = Verification unsuccessful,
 x = number of possible retries
 '6983' = Verification method blocked

6.2 CHANGE VERIFICATION DATA

6.2.1 Function

With the CHANGE VERIFICATION DATA command verification data can be changed. Verification data are BCD encoded, when a PIN is concerned, otherwise hexadecimal coding is used.

6.2.2 Usage conditions

The command is only applicable for IC cards with the appropriate security function.

6.2.3 Command structure

| | |
|------------|---|
| CLA | '00' |
| INS | '24' (= CHANGE VD) |
| P1, P2 | '0000' |
| Lc field | Length of subsequent data |
| Data field | Old verification data (Byte1, Byte 2, Byte 3), new reference data (Byte1, Byte 2, Byte 3) Note: PINs are BCD-coded possibly padded with one or more 'F' |
| Le field | Empty |

Tab. 9: CHANGE VERIFICATION DATA command

Note: The command is described here only with the supported parameter codings.

6.2.4 Response structure

| | |
|---------|--------------|
| Data | Empty |
| SW1-SW2 | Status bytes |

Annex A (normative)

Processing of the commands VERIFY and CHANGE VERIFICATION DATA

The following figures show the configuration mapping of the ISO/IEC 7816-4 VERIFY command and the CHANGE VERIFICATION DATA command to the command sequence of IC cards with 2WB protocol and corresponding security function.

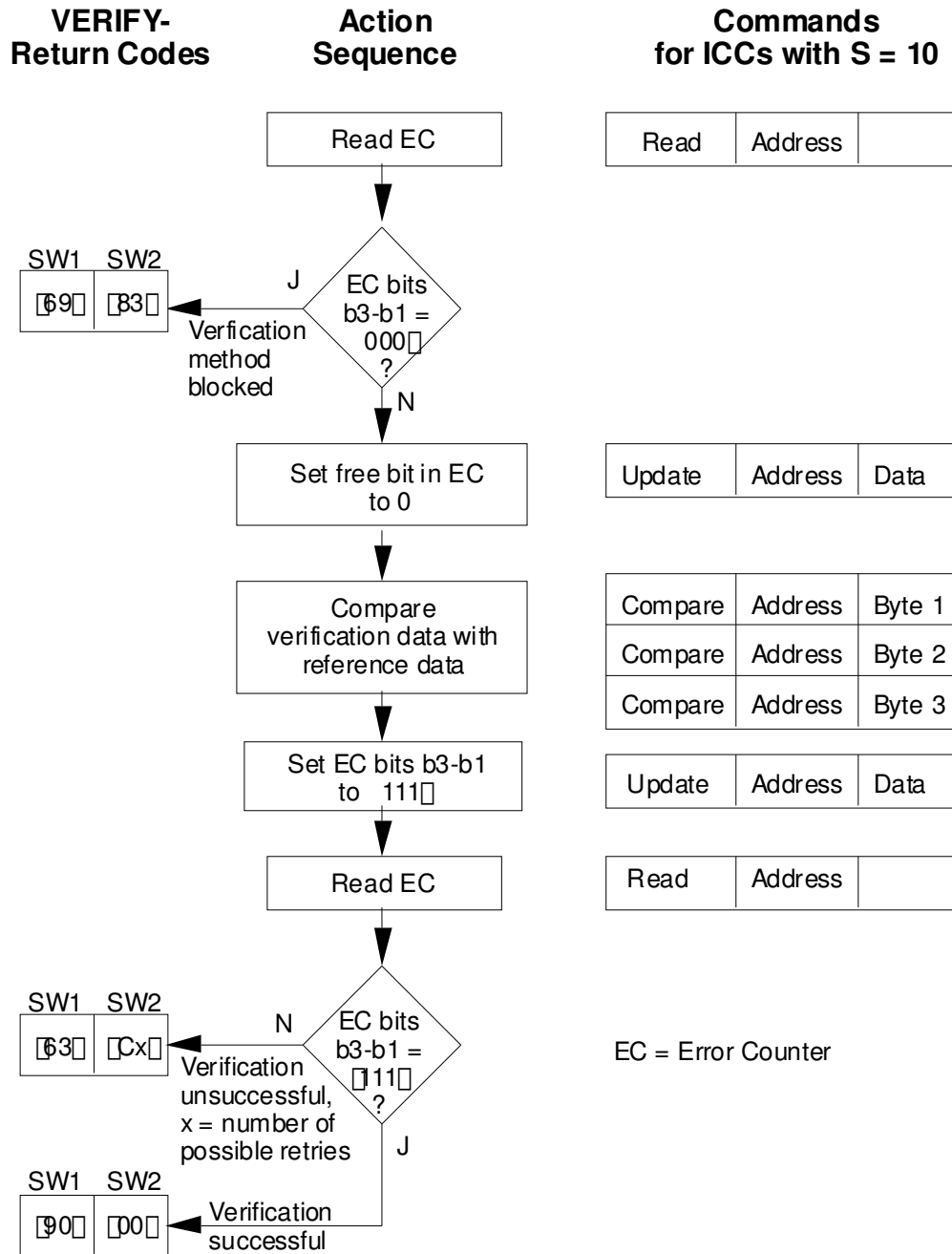


Fig. 1: Flow chart of the action sequence for processing of the VERIFY command

Fig. 2: Flow chart of the action sequence for processing of the CHANGE VD command