

Teil 7

**Chipkarten
mit synchroner Übertragung -
Anwendung von Interindustry
Commands**

MKT-Version 1.0

15.04.1999

Inhalt

| | | |
|-----|--|---|
| 1 | Zweck..... | 1 |
| 2 | Normative Verweisungen..... | 1 |
| 3 | Abkürzungen | 1 |
| 4 | Das Umsetzungsprinzip | 1 |
| 5 | Interindustry Commands für Grundfunktionen..... | 1 |
| 5.1 | SELECT FILE..... | 1 |
| 5.2 | READ BINARY | 2 |
| 5.3 | UPDATE BINARY..... | 2 |
| 6 | Interindustry Commands für Sicherheitsfunktionen | 4 |
| 6.1 | VERIFY | 4 |
| 6.2 | CHANGE REFERENCE DATA..... | 4 |

Anhang A (normativ)

| | | | | | | | | |
|-----------|-----|-----------|--------|-----|--------|-----------|------|---|
| Abbildung | der | Kommandos | VERIFY | und | CHANGE | REFERENCE | DATA | |
| | | | | | | | | 5 |

1 Zweck

Ziel dieses Teils der Spezifikation ist, die Verwendung von ISO/IEC 7816-4 Interindustry Commands für Chipkarten mit synchroner Übertragung zu beschreiben und ihre Umsetzung in Chip-spezifische Aktionen zu spezifizieren. Diese Spezifikation gilt nur für Chipkarten, deren Datenbereiche nach MKT-Teil 5: 'ATR und Datenbereiche' codiert sind. Die Verwendung von ISO/IEC 7816-4 Interindustry Commands an einem CardTerminal Application Programming Interface setzt neben der Einhaltung der Struktur des ATR und der Datenbereiche auch die Fähigkeit des Kartenterminals zur Umsetzung von Interindustry Commands in Chip-spezifische Aktionen voraus.

2 Normative Verweisungen

MKT-Teil 5: Chipkarten mit synchroner Übertragung - ATR und Datenbereiche

MKT-Teil 6: Chipkarten mit synchroner Übertragung - Übertragungsprotokolle

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

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

ISO/IEC 7816-10: 1998 (FDIS)
Identification cards - Integrated circuit(s) cards with contacts, Part 10 – Electronic signals and answer-to-reset for synchronous cards

3 Abkürzungen

| | |
|-----|----------------------------------|
| AID | = Application Identifier |
| ATR | = Answer-to-Reset |
| BCD | = Binary Coded Digits |
| CT | = CardTerminal |
| FID | = File Identifier |
| ICC | = Integrated Circuit(s) Card |
| PIN | = Personal Identification Number |
| RD | = Reference Data |
| TLV | = Tag, Length, Value |
| VD | = Verification Data |

4 Das Umsetzungsprinzip

Um die Ansteuerung von Chipkarten mit synchroner Übertragung einerseits so einfach wie möglich und andererseits weitgehend kompatibel mit der Ansteuerung von Prozessorchipkarten zu machen, werden bestimmte Interindustry Commands im Kartenterminal (bzw. in der zum Kartenterminal gehörenden Software) auf Interaktionen mit der entsprechenden synchronen Chipkarte abgebildet. Für alle Chipkarten sind folgende Kommandos zu unterstützen:

- SELECT FILE
- READ BINARY und
- UPDATE BINARY.

Für Chipkarten mit Verification Data sind zusätzlich die Kommandos

- VERIFY und
- CHANGE REFERENCE DATA

zu unterstützen. Das Setzen von Protection Flags (falls der Chip mit einem Protection Memory ausgestattet ist) wird in der Regel bei der Personalisierung vorgenommen und ist nicht im Leistungsumfang der nachfolgend beschriebenen Kommandos enthalten.

5 Interindustry Commands für Grundfunktionen

5.1 SELECT FILE

5.1.1 Funktion

a) Selektieren einer Anwendung

Zum Selektieren einer Anwendung wird das ISO/IEC 7816-4 SELECT FILE-Kommando verwendet. Hierbei wird der Application Identifier (AID) im Datenfeld übergeben. Das Kartenterminal liest den DIR-Datenbereich und prüft, ob die AID dort zu finden ist (Strukturen des DIR-Datenbereichs entsprechend MKT-Teil 5). Wenn ja, wird die Anwendung und damit der Anwendungsdatenbereich selektiert und als Return-Code '9000' zurückgegeben. Der Anwendungsdatenbereich beginnt bei Mono-Application Cards direkt hinter dem DIR-Datenbereich, in Multi-Application Cards wird der Anfang des Anwendungsdatenbereichs im Path-Element des entsprechenden Application Templates angezeigt.

b) Selektieren von Datenbereichen

Ein Datenbereich in einer synchronen Karte ist wie ein File in einer Mikroprozessorchipkarte über File-Identifizier (FIDs) bzw. über den File-Name mit dem SELECT FILE-Kommando selektierbar:

- der ATR-Datenbereich hat wie der ATR-File als FID '2F01' und beginnt nach dem ATR auf Byte-Adresse '04'
- der DIR-Datenbereich hat wie der DIR-File als FID '2F00' und beginnt auf der Byte-Adresse, die in Byte H4 (siehe MKT-Teil 5) angegeben ist
- der Anwendungs-Datenbereich hat als Kennung den Application Identifier und wird daher mit dem SELECT FILE-Kommando mit Angabe der AID selektiert, wie in a) beschrieben. Hierbei wird der Pointer auf das erste Byte des Anwendungs-Datenbereichs eingestellt.

Um auch den gesamten Datenspeicher bei Bedarf selektieren zu können, wird er als eine Sequenz von Datenbereichen bzw. Files gesehen, die im Master-File enthalten bzw. diesem untergeordnet sind; daher wird als FID für den gesamten Datenspeicher die MF-FID '3F00' verwendet (Adresse des ersten Bytes: '00').

5.1.2 Kommando-Struktur

| | |
|------------|---|
| 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, if P1 = '00' - FID, if P1 = '04': '3F00' = MF (total memory) '2F00' = DIR data section '2F01' = ATR data section |
| Le field | Empty |

Tab. 1: SELECT FILE-Kommando

Anmerkung: Das Kommando ist hier nur mit den benötigten Parameter-Codierungen dargestellt.

5.1.3 Antwort-Struktur

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

Tab. 2: SELECT FILE-Response

5.1.4 Status Bytes

- '9000' = Command successful
- '6A82' = File not found
- '6A82' = File not found (no file selected)

5.2 READ BINARY

5.2.1 Funktion

Mit dem ISO/IEC 7816-4 READ BINARY-Kommando können Daten aus dem zuvor selektierten Datenbereich gelesen werden. Das erste Byte des Datenbereichs hat die logische Adresse '0000'. Die Länge des Datenbereichs ergibt sich aus der Länge des ersten DOs (siehe MKT-Teil 5).

5.2.2 Anwendungsbedingungen

Der zu lesende Datenbereich muß zuvor selektiert worden sein.

5.2.3 Kommando-Struktur

| | |
|------------|---|
| 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-Kommando

Anmerkung: Das Kommando ist hier nur mit den benötigten Parameter-Codierungen dargestellt.

5.2.4 Antwort-Struktur

| | |
|---------|-----------------|
| Data | Data to be read |
| SW1-SW2 | 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
- '6A82' = File not found (no file selected)

5.3 UPDATE BINARY

5.3.1 Funktion

Mit dem ISO/IEC 7816-4 UPDATE BINARY-Kommando können Daten aus dem zuvor selektierten Datenbereich geändert werden. Das erste Byte des Datenbereichs hat die logische Adresse '0000'. Die Länge des Datenbereichs ergibt sich aus der Länge des ersten DOs (siehe MKT-Teil 5: 'ATR und Datenbereiche').

5.3.2 Anwendungsbedingungen

Der zu beschreibende Datenbereich muß zuvor selektiert worden sein. Bei Chipkarten, die eine Änderung des Datenspeichers (bzw. Teile davon) nur nach vorheriger erfolgreicher Präsentation des Sicherheitscodes erlauben, ist zuvor die entsprechende Authentisierung (siehe VERIFY command) durchzuführen. Bei Offset '0000' ist der komplette Inhalt des betreffenden Datenbereichs zurückzuschreiben und als Länge des Datenbereichs die entsprechende neue Länge einzutragen.

5.3.3 Kommando-Struktur

| | |
|------------|---|
| 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-Kommando

Anmerkung: Das Kommando ist hier nur mit den benötigten Parameter-Codierungen dargestellt.

5.3.4 Antwort-Struktur

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

Tab. 6: UPDATE BINARY-Response

5.3.5 Status Bytes

'9000' = Command successful

'6200' = Error

'6A82' = File not found (no file selected)

6 Interindustry Commands für Sicherheitsfunktionen

6.1 VERIFY

6.1.1 Funktion

Das ISO/IEC 7816-4 VERIFY-Kommando veranlaßt den Vergleich der Verification Data mit den in der Chipkarte gespeicherten Reference Data. Der Ablauf ist in Anhang A dargestellt. Verification Data sind BCD-codiert, wenn es sich um eine PIN handelt, ansonsten wird 'hexadecimal coding' verwendet.

6.1.2 Anwendungsbedingungen

Das Kommando ist nur bei Chipkarten mit entsprechender Sicherheitsfunktion zulässig.

6.1.3 Kommando-Struktur

| | |
|------------|--|
| CLA | '00' |
| INS | '20' (= VERIFY) |
| P1, P2 | '0000' |
| Lc field | '03' = Length of subsequent data field |
| Data field | Verification data (Bytes 1 - 3) Note: a PIN is BCD-coded and possibly padded with one or more 'F' |
| Le field | Empty |

Tab. 7: VERIFY-Kommando

Anmerkung: Das Kommando ist hier nur mit den benötigten Parameter-Codierungen dargestellt.

6.1.4 Antwort-Struktur

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

Tab. 8: VERIFY-Response

6.1.5 Status Bytes

'9000' = Command successful

'63Cx' = Verification unsuccessfull, x = number
of possible retries

'6983' = Verification method blocked

6.2 CHANGE REFERENCE DATA

6.2.1 Funktion

Mit dem ISO/IEC 7816-8 CHANGE REFERENCE DATA-Kommando können die in der Chipkarte gespeicherten Referenzdaten geändert werden.

Reference Data sind BCD-codiert, wenn es sich um eine PIN handelt, ansonsten wird 'hexadecimal coding' verwendet.

6.2.2 Anwendungsbedingungen

Das Kommando ist nur bei Chipkarten mit entsprechender Sicherheitsfunktion zulässig.

6.2.3 Kommando-Struktur

| | |
|------------|--|
| CLA | '00' |
| INS | '24' (= CHANGE REFERENCE DATA) |
| P1, P2 | '0000' |
| Lc field | '06' = Length of subsequent data field |
| Data field | Old reference data (Bytes 1 - 3), new reference data (Bytes 1 - 3) Note: PINs are BCD-coded and possibly padded with one or more 'F' |
| Le field | Empty |

Tab. 9: CHANGE REFERENCE DATA-Kommando

Anmerkung: Das Kommando ist hier nur mit den benötigten Parameter-Codierungen dargestellt.

6.2.4 Antwort-Struktur

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

Tab. 10: CHANGE REFERENCE DATA-Response

6.2.5 Status Bytes

'9000' = Command successful

'63Cx' = Verification unsuccessful, x =
number

of possible retries

'6983' = Verification method blocked

Anhang A (normativ)

Abbildung der Kommandos VERIFY und CHANGE REFERENCE DATA

Die folgenden Abbildung zeigen die Abbildung des ISO/IEC 7816-4 VERIFY-Kommandos und des ISO/IEC 7816-8 CHANGE REFERENCE DATA-Kommandos auf die Kommandofolge von Chipkarten mit 2WB-Protokoll (S = 10) und entsprechender Sicherheitsfunktion.

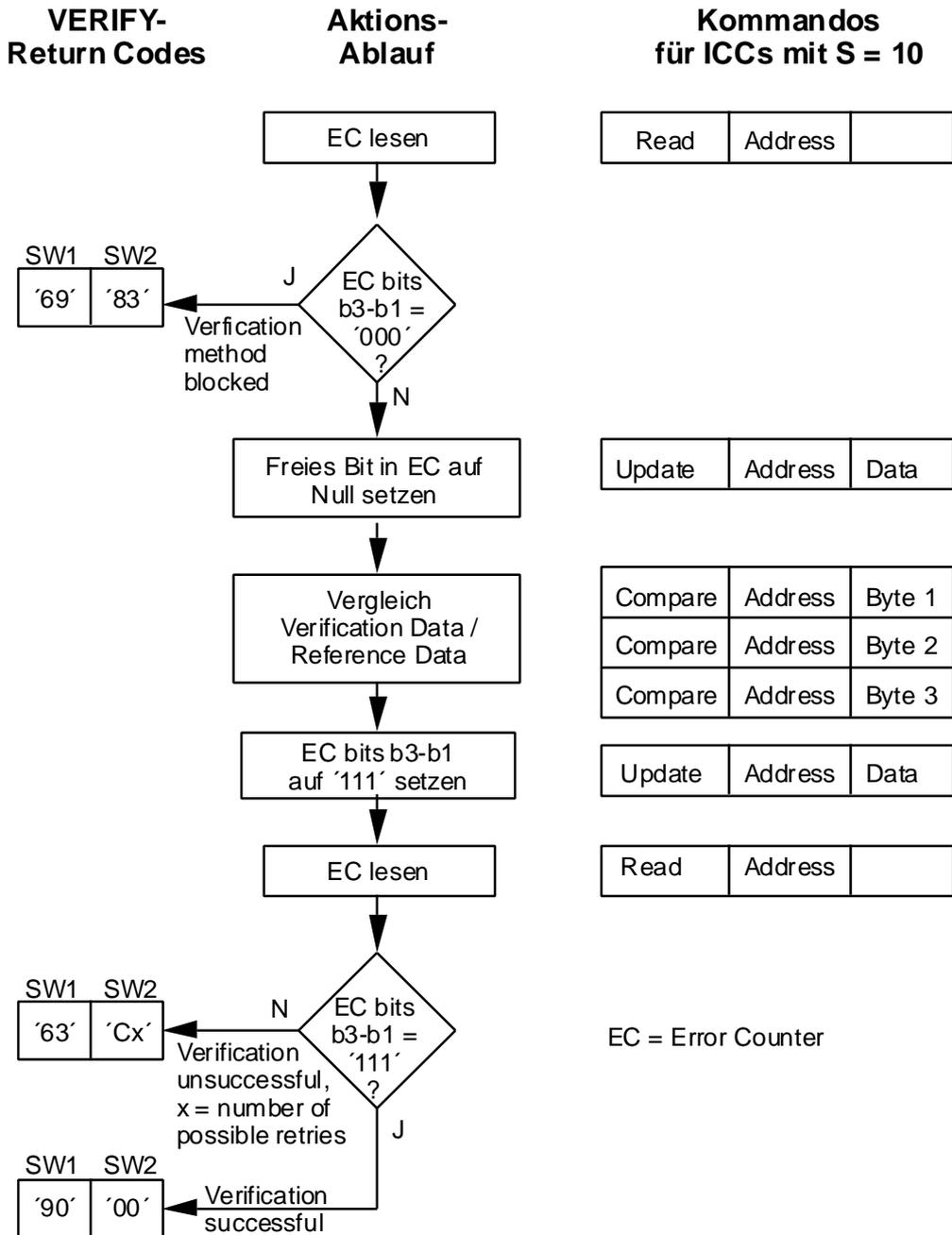


Abb. A.1: Flußdiagramm zum Ablauf des VERIFY-Kommandos

**CHANGE RD
Return Codes**

**Aktions-
Ablauf**

**Kommandos
für ICCs mit S = 10**

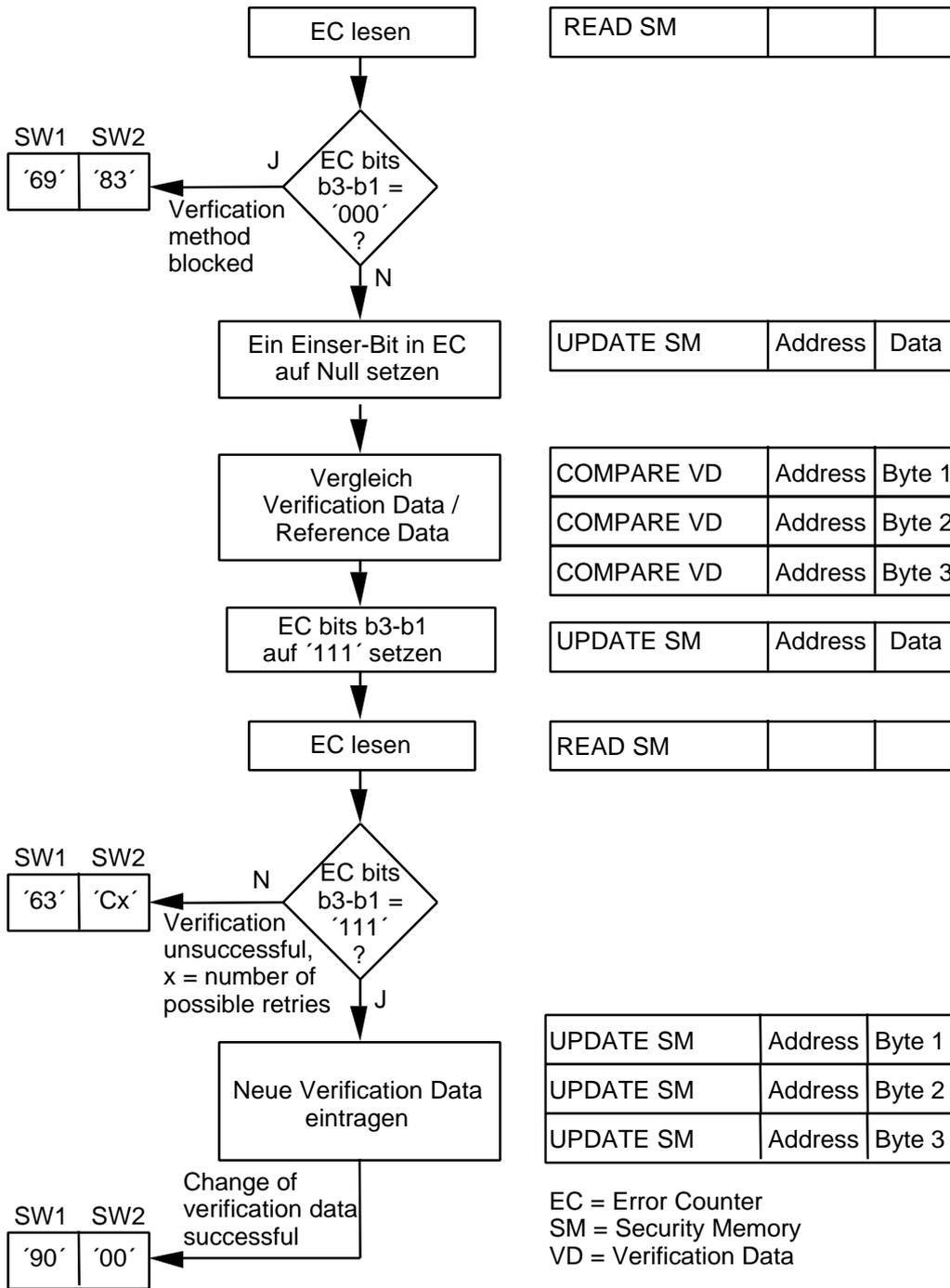


Abb. A.2: Flußdiagramm zum Ablauf des CHANGE REFERENCE DATA-Kommandos