Teil 5

Chipkarten
mit synchroner †bertragung

Teil 1: ATR und Datenbereiche

01.06.95

DIN NI-17

Inhalt

1. Zweck

Dieses Dokument beschreibt den Answer-to-Reset (ATR) sowie die Anordnung und den Aufbau der Datenbereiche im Datenspeicher von Chipkarten mit synchroner †bertragung (allgemein Ÿbliche Bezeichnung: «Speicherchipkarten«):

- ATR
- ATR-Datenbereich
- Directory-Datenbereich
- Anwendungs-Datenbereich.

Aufbau und Struktur von evtl. zusŠtzlich vorhandenen Speicherbereichen fŸr Schutzmechanismen beim Zugriff auf den Datenspeicher werden hier nicht betrachtet.

2. Normative Verweisungen

ISO 3166: 1994
Codes for the representation of names of countries

ISO/IEC 7816-3: 1988
Identification cards - Integrated circuit(s) cards with contacts, Part 3 - Electronic signals and transmission protocols

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

ISO/IEC 7816-5: 1994
Identification cards - Integrated circuit(s) cards with contacts, Part 5 - Numbering system and registration procedure for application identifiers

ISO/IEC 7816-6: 1995 (DIS)
Identification cards - Integrated circuit(s) cards with contacts, Part 6 - Inter-industry data elements

ISO 8825: 1990
Information technology - Open systems Interconnection - Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1)

3. Definitionen und AbkŸrzungen

3.1 Definitionen

3.1.1 Datenbereich (data section): logische Datenzone im Speicher, die einem File nach ISO/IEC 7816-4 entspricht

3.1.2 Dateneinheit (data unit): logische Gruppe von Bits, die bei einem Speicherzugriff als Einheit angesprochen wird (Ÿbliche Grš§e: 8 bits = 1 byte)

3.1.3 Datenobjekt (data object): Folge von logisch zusammengehšrenden Bytes. Ein BER-TLV-codiertes Datenobjekt besteht aus den drei Datenfeldern Tag, Length und Value.

3.1.4 Datenspeicher (data memory): physikalisches Medium mit sequentieller Anordnung von Dateneinheiten. Die Adresse der ersten Dateneinheit (Beginn des Datenspeichers) hat den Wert 0.

3.1.5 Tag: engl. Bezeichnung fŸr Datenobjekt-Kennzeichen fŸr BER-TLV-codierte Datenobjekte

3.1.6 Template: engl. Bezeichnung fŸr Datenobjekt-Rahmen fŸr eine logisch zusammengehšrende Menge BER-TLV-codierter Datenobjekte

3.2 AbkŸrzungen

AID = Application identifier
ANW = Anwendung
ASN.1=Abstract syntax notation one
ATR = Answer-to-Reset
BER = Basic encoding rules
DB = Datenbereich
DIR = Directory
DO = Data object
FID = File identifier
IC = Integrated circuit
ICC = Integrated circuit(s) card
ICCF= ICC fabricator
ICM = IC manufacturer
ICT = IC type
PIX = Proprietary apllication identifier extension
RFU = Reserved for future use
RID = Registered application provider identifier
TLV = Tag, length, value

3.3 Sonstige Konventionen

Bei allen Darstellungen werden die Bits innerhalb eines Bytes mit b1 bis b8 bezeichnet, wobei b1 das niederwertigste Bit (least significant bit) ist.
Logisch zusammengehšrende Bytes (z.B. Offset) werden mit B1 bis Bn bezeichnet, wobei B1 das niederwertigste Byte ist.
Dargestellt wird hier immer nur die logische Struktur der Daten, unabhŠngig von der tatsŠchlichen Abfolge der Bits bei der †bertragung.

4. Codierungstechnik

4.1 Datenobjekte

Als Codierungstechnik fŸr Datenobjekte werden die «Basic Encoding Rules (BER)« der ISO-Codierungskonvention «Abstract Syntax Notation One (ASN.1)« verwendet. Ein Datenobjekt besteht danach aus

- einem Datenobjekt-Kennzeichen («Tag«)
- einem LŠngenangabe («Length«) und
- einem Datenobjekt-Wert («Value«).

Abb. 1 zeigt den allgemeinen Aufbau eines BER-TLV-codierten Datenobjekts.

Abb.1: Allgemeiner Aufbau eines BER-TLV-codierten Datenobjektes

4.2 Datenbereiche

Mit Ausnahme des ATR enthalten alle Datenbereiche BER-TLV-codierte Datenobjekte. Jeder Datenbereich besteht entweder aus einem einfachen oder einem zusammengesetzten Datenobjekt, d.h. im LŠngenfeld dieses Datenobjekts ist die LŠnge des Datenbereichs codiert. Folgende Varianten sind zu unterscheiden:

- Der Datenbereich besteht nur aus einem einfachen Datenobjekt (Typ = «primitive«). Das durch seinen Tag identifizierbare Datenobjekt gehšrt zu der Menge der fŸr diesen Datenbereich zulŠssigen Datenobjekte.

- Der Datenbereich besteht aus einem zusammengesetzten Datenobjekt aus der Menge der fŸr diesen Datenbereich zulŠssigen Templates (Typ = «constructed«). Innerhalb des Templates sind dann BER-TLV-codierte, Template-spezifische Datenobjekte zu finden.

- Der Datenbereich beginnt mit dem zusammengesetzten Datenobjekt «Sequence« (standardisiertes Datenobjekt der Klasse «universal« mit der Codierung «30«) und enthŠlt eine Sequenz datenbereichsspezifischer Templates und/oder sonstiger datenbereichsspezifische Datenobjekte, die nicht in einem Template integriert sind.

Abb. 2 zeigt die verschiedenen Varianten der Struktur eines Datenbereichs.

Abb. 2: Struktur-Varianten eines Datenbereichs

4.3 Datenspeicher

Der Datenspeicher wird logisch als Sequenz von Bytes gesehen. Das erste Byte hat als Byte-Adresse den Wert 0. Die generelle Anordnung der Datenbereiche im Datenspeicher zeigt Abb. 3.

Abb.3: ATR u. Datenbereiche im Datenspeicher

5. ATR

Nach ISO/IEC 7816-3 besteht der SYN-ATR aus

- Byte H1: Protocol Type
- Byte H2: Protocol Parameter
- Bytes H3, H4: Historical Bytes.

Der ATR ist im Datenspeicher im Adressbereich «00« - «03« (Byte-Adressen) abgelegt.

5.1 H1 - Protocol Type

Das Byte H1 (in ISO/IEC 7816-3 nur funktionell festgelegt) gibt das †bertragungsprotokoll und die ATR-Struktur an.

Abb. 4: Protocol Type
Die ATR-Struktur kennzeichnet den Aufbau des ATR und ist in den Bits b3-b1 codiert. In den Bits b8-b5 ist die Kennung S des †bertragungsprotokolls angegeben.

5.2 H2 - Protocol Parameter

Das Byte H2 «Protocol Parameter« - in ISO/IEC 7816-3 nicht in seinem Aufbau beschrieben - beinhaltet weitere, fŸr die Fortsetzung der Kommunikation mit der Chipkarte wichtige Angaben:

- LŠnge der Dateneinheiten
- Gršße des Datenspeichers
- Optionsangabe zu den Lesebefehlen

Abb.5 zeigt den Aufbau des Bytes H2.

Abb. 5: Protocol Parameter

5.3 Historical Bytes

Die Bytes H3 und H4 enthalten nach ISO/IEC 7816-3 Informationen Šhnlich denen der «Historical Bytes« bei Chipkarten mit asynchroner †bertragung. Die «Historical Bytes« sind in ISO/IEC 7816-4 definiert.

5.3.1 H3 - Category indicator

Entsprechend ISO/IEC 7816-4 beginnen «Historical Bytes« mit dem «Category indicator«, der den Aufbau der Historical Bytes charakterisiert. Der fŸr Chipkarten mit synchroner †bertragung vorgesehene Wert (siehe Tabelle 78 in ISO/IEC 7816-4) ist «10«. Dieser Wert sagt aus, das als nŠchtes Byte eine «DIR data reference« folgt, deren Aufbau jedoch «outside the scope« von ISO/IEC 7816-4 ist.

Abb.6: «Category indicator« nach ISO/IEC 7816-4

5.3.2 H4 - DIR data reference

Das Byte H4 beinhaltet die «DIR data reference«, also einen Pointer (Byte-Adresse), der auf das erste Byte des Directory-Bereichs zeigt. Den genauen Aufbau dieses Bytes zeigt Abb.7.

Abb. 7: «DIR data reference« nach ISO/IEC 7816-4 mit vom DIN festgelegten Aufbau

6. ATR-Datenbereich

Der ATR-Datenbereich ist ein optionaler Datenbereich und ist dem ATR File bei Mikroprozessorkarten vergleichbar (siehe ISO/IEC 7816-4). Er enthŠlt, wenn vorhanden, ein Datenobjekt mit herstellerspezifischen Angaben. Er folgt im Speicher unmittelbar im Anschlu§ an den ATR. Der ATR-Datenbereich ist leer, wenn der Pointer «DIR data reference« den Wert «84« hat, was bedeutet, da§ der DIR-Datenbereich unmittelbar nach dem ATR-header kommt.

Abb. 8: Manufacturer data object

Die Angaben zu «IC type« in Verbindung mit «IC-manufacturer« kšnnen auf Anwendungsebene eine Rolle spielen, da sie funktionelle Unterschiede von Chips mit demselben †bertragungsprotokoll kennzeichnen.
Die Werte fŸr ICM und ICCF werden von einer Registration Authority vergeben (siehe Anhang B). Die Werte fŸr ICT werden von den Herstellern vergeben und von der Registration Authority in eine Liste eingetragen. Die Werte fŸr ICCSN werden vom Hersteller vergeben und nicht zentral registriert.

7. DIR-Datenbereich

Der DIR-Datenbereich soll immer vorhanden sein und enthŠlt entsprechend ISO/IEC 7816-5 Datenobjekte zur Anwendungsselektion. Folgende Varianten sind zu unterscheiden:

- Die Chipkarte ist eine Mono-Application Card und im DIR-Datenbereich ist nur das Datenobjekt «Application Identifier« (Tag «4F«) abgelegt.

- Die Chipkarte ist eine Mono-Application Card und im DIR-Datenbereich ist das Datenobjekt «Application Template« (Tag «61«) abgelegt, das neben dem «Application Identifier« (Tag «4F«) noch weitere Datenobjekte enthalten kann (z.B. «Application Label«, Tag «50«, oder «Discretionary Data«, Tag «53«).

- Die Chipkarte ist eine Multi-Application Card. In diesem Fall beginnt der DIR-Datenbereich mit dem Datenobjekt «Sequence« (Tag «30«). Im Value-Teil des Datenobjekts «Sequence« sind dann mindestens zwei «Application Templates« (Tag «61«) zu finden. Diese Application Templates mŸssen neben dem «Application Identifier« (Tag «4F«) auch das Datenobjekt «Path« (Tag «51«) enthalten. Das Datenobjekt «Path« kennzeichnet den Pfad zur zugehšrigen Anwendung (bei Mikroprozessorkarten enthŠlt «Path« im Value-Teil einen File Identifier oder eine FID-Sequenz) und beinhaltet im Value-Teil fŸr Chipkarten mit synchroner †bertragung den Pointer (phy-

sikalische Adresse) auf das erste Byte des zur betreffenden Anwendung gehšrenden Anwendungs-Datenbereichs.

Den allgemeinen Aufbau eines «Application Identifiers« der Kategorie «National Registration« zeigt Abb. 9.

Abb. 9: Aufbau eines ISO/IEC 7816-5-konformen «Application Identifiers« der Kategorie «National Registration«

Eine RID kann bei der RID German National Registration Authority (Adresse siehe Anhang B) beantragt werden.

8. Anwendungs-Datenbereich(e)

In Mono-Application Cards (siehe Anhang A, Abb. 1 und Anhang C) beginnt der Anwendungs-Datenbereich unmittelbar hinter dem DIR-Datenbereich. Dieser fŠngt entweder mit dem

- Tag «40« (= Kennzeichen des «primitive« Anwendungsdaten-Objekts), falls die Anwendungsdaten keine TLV-Struktur haben, andernfalls mit dem
- Tag «60« (= Kennzeichen des Anwendungsdaten-Templates) an.

Das LŠngenfeld des Anwendungsdaten-Objekts bzw. -Templates kennzeichnet die LŠnge des Anwendungs-Datenbereichs.
In Multi-Application Cards (siehe Anhang A, Abb. 2) wird die Byte-Adresse des ersten Bytes des jeweiligen Anwendungs-Datenbereichs im Datenobjekt «Path« des zur Anwendung gehšrenden «Application Templates« angegeben.

9. Extension Areas

An die Anwendungs-Datenbereiche kšnnen sich «Extension areas« anschlie§en. Der Default Wert der Bytes in den «Extension areas« ist der «logical erased state« des Chips (z.B. «FF«).

Anhang A (normativ)

Datenbereiche in Mono- und Multiapplication Cards

Abb. 1: Allgemeine Struktur einer Mono-Application Speicherkarte mit einfacher DIR-Struktur

Abb. 2: Allgemeine Struktur einer Multiapplication-Speicherkarte (Beispiel)

Hinweis: Ein Pointer (z.B. in H4 oder in einem Path-DO) enthŠlt eine Byte-Adresse, d.h. das n-te Byte im Datenspeicher hat als Byte-Adresse den Wert n-1, da die Adresswert-ZŠhlung mit 0 beginnt.

Anhang B (informativ)

Protocol Types und andere Identifier

Folgende Protocol Type Ids (Bits b8-b5 von H1) sind in Benutzung:

«8« = Serial Data Access Protocol (SDA Protocol)
«9« = 3-Wire Bus Protocol (3WB Protocol)
«A« = 2-Wire Bus Protocol (2WB Protocol)

FŸr folgende Identifier wird eine zentrale Registrierung vorgenommen:

- ICM (IC Manufacturer)
- ICCF (ICC Fabricator)
- ICT (IC Type)

Als Registrierungsinstanz fungiert - solange keine anderen Festlegungen getroffen werden - die RID German National Registration Authority. Die ICM-, ICT- und ICCF-Listen sind Ÿber World Wide Web (Internet-Informationsdienst) unter

http://www.darmstadt.gmd.de

abrufbar oder auf Anfrage bei der RID German National Registration Authority erhŠltlich.

Adresse der Registrierungsinstanz:

RID German National Registration Authority
c/o GMD
Bruno Struif
Rheinstr.75
64295 Darmstadt
Tel. 06151-869-206
Fax 06151-869-224

Anhang C (informativ)

Datenbereiche der Versichertenkarte

Abb. 1: Datenbereiche der Versichertenkarte (ohne Filler-Element nach Application data)