Teil 6

Chipkarten mit synchroner Übertragung

Teil 2: Übertragungsprotokolle

Entwurf

20.07.95

DIN NI-17.4

Inhalt

1. Zweck

Dieser Teil der Spezifikation zu Chipkarten mit synchroner Übertragung spezifiziert Übertragungsprotokolle. Die unterschiedlichen Protokoll-Typen werden mit einer eindeutigen Kennung S versehen. Der Protokoll-Typen-Bereich S = 0 bis S = 7 ist für ISO reserviert.
In diesem Teil werden spezifiziert

- S = 10 (2 Wire Bus Protocol 2WBP, halbduplex)
- S = 11 bis S = 14 (reserviert).

Hinweis: Die Protokoll-Typen S = 8 und S = 9 bezeichnen die von Herstellern spezifizierten Übertragungsprotokolle Serial Data Access Protocol SDAP bzw. 3 Wire Bus Protocol 3WBP.

2. Normative Verweisungen

DIN NI-17: 1995
Chipkarten mit synchroner Übertragung
Teil 1: ATR und Datenbereiche

ISO/IEC 7816-2: 1989
Identification cards - Integrated circuit(s) cards with contacts
Part 2 - Dimensions and location of contacts

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
(Verwendung findet der WD vom Oktober 1994, in dem AM 1 und AM 2 integriert sind)

3. Abkürzungen

ATR = Answer-to-Reset
CLK = Clock
CT = CardTerminal
H = Pegel ´high´
ICC = Integrated Circuit(s) Card
INS = Instruction Code
I/O = Input/Output
L = Pegel ´low´
IFD = Interface Device
RST = Reset
Vcc = Versorgungsspannung
2WBP = 2 Wire Bus Protocol

4. S = 10 : Halb-duplex ´2 Wire Bus´-Protokoll

4.1 Übersicht

Das Protokoll S = 10 dient zur Kommunikation mit Chipkarten, die dieses Protokoll im ATR anzeigen. Wesentliches Merkmal ist die Benutzung der Leitungen Clock (Kontakt C3, siehe ISO/IEC 7816-2) und I/O (Kontakt C7) für die Kommunikation mit der Karte (gilt nicht während der ATR-Sequenz, da dabei noch das Signal Reset an RST mitbenutzt wird). Aus diesem Grunde wird das Protokoll S =10 auch als ´2 Wire Bus´-Protokoll oder 2WBP genannt.
Eine Chipkarte mit diesem Übertragungsprotokoll soll im ATR-Byte ´Protocol Type´ S = 10 aufweisen (Wert 10 im oberen Halbbyte von H1, siehe Teil1 dieser Spezifikation), damit ein Interface Device (IFD) den richtigen Protokolltyp zur Kommunikation mit der Karte einstellen kann.

4.2 Datenübertragung

4.2.1 Bit-Übertragungskonventionen

Das Bit b1 (least significant bit) eines Bytes wird zuerst übertragen. Eine logische 1 wird auf der I/O-Leitung mit Pegel H (= high), eine logische 0 mit Pegel L (= low) dargestellt.

4.2.2 ATR

Der Reset der Karte mit nachfolgendem ATR entspricht den Vorgaben von ISO/IEC 7816-3 und ist im Anhang A in Abb. 1 dargestellt. Demnach werden 32 Clock-Impulse benötigt, um die 32 Bit des ATR zu erhalten. Nach den 32 Clock-Impulsen muß ein weiterer Clock-Impuls folgen, damit die I/O-Leitung den Zustand H annimmt. Weitere Clock-Impulse, die danach folgen, verändern den Zustand der I/O-Leitung nicht mehr.

4.2.3 Kommando-Modus

Bei der Datenübertragung vom IFD zur ICC wird jede Bit-Sequenz (Chipkarten-Kommando) mit einer START-Sequenz begonnen und mit einer STOP-Sequenz beendet.

Die START-Sequenz ist wie folgt definiert:

Ausgangszustand: I/O = H, ICC empfangsbereit
IFD-Aktion: Fallende Flanke auf der I/O-Leitung während die Clock-Leitung im Zustand H ist.

Die Bitübertragung eines Kommandos ist wie folgt definiert:

Jedes Bit wird gesendet durch

- Bit anlegen
- Clock auf H setzen
- Clock auf L setzen,

wie in Abb. 2 des Anhangs A dargestellt. Nach Senden des letzten Bits eines Kommandos vom IFD zur ICC muß die I/O-Leitung vom IFD auf L gesetzt werden.

Die STOP-Sequenz ist dann wie folgt definiert:

Ausgangszustand: I/O = L
IFD-Aktion: Steigende Flanke auf der I/O-Leitung während die Clock-Leitung im Zustand H ist.

Nach Übertragung eines Kommandos zur Karte inklusive START- und STOP-Sequenz geht die Karte in Abhängigkeit von dem vom IFD gesandten Kommando entweder in den Betriebszustand ´Datenantwort-Modus (Data outgoing mode)´ oder ´Verarbeitungs-Modus (Processing mode)´. In diesen Modi und auch beim Aussenden des ATR reagiert die Karte nicht auf START-/STOP-Sequenzen.

4.2.4 Datenantwort-Modus

Im Datenantwort-Modus reagiert die Karte auf das erhaltene Kommando mit Aussenden von Daten an das IFD. Das erste Datenbit auf der I/O-Leitung erscheint mit der ersten fallenden Flanke nach Beendigung des Kommando-Modus. Nachdem die Karte das letzte Datenbit gesendet hat, muß noch ein weiterer Clock-Impuls folgen, damit die I/O-Leitung den Zustand H annimmt. Danach ist die Karte wieder bereit, ein neues Kommando, beginnend mit der START-Sequenz, zu empfangen.

Weitere Clock-Impulse, die danach folgen, verändern den Zustand der I/O-Leitung nicht mehr.

4.2.5 Verarbeitungs-Modus

In diesem Modus reagiert die Karte intern auf das erhaltene Kommando. Damit die Karte das Kommando bearbeiten kann, benötigt sie weitere Impulse auf der Clock-Leitung. Die Karte setzt in diesem Modus I/O auf L als Folge des Takts, in dem die STOP-Sequenz auftrat. Das IFD erkennt das Ende dieses Modus daran, daß der Zustand auf der I/O-Leitung von L nach H wechselt. Danach ist die Karte wieder bereit, ein neues Kommando, beginnend mit der START-Sequenz, zu empfangen.
Weitere Clock-Impulse, die danach folgen, verändern den Zustand der I/O-Leitung nicht mehr.

4.3 Kommando-Aufbau und Kommando-Übersicht

4.3.1 Allgemeiner Kommando-Aufbau

Das generelle Format eines Kommandos besteht aus den drei Feldern Instruction Code, Address und Data Unit (siehe Abb. 1).

Instruction Code	Address	Data Unit

Abb. 1: Allgemeiner Kommando-Aufbau

Das Feld ´Instruction Code´ enthält den Befehlscode und hat eine Länge von 1 Byte.

Das Adreß-Feld besteht aus einem Byte bei einem Speicherausbau bis 256 Dateneinheiten, aus zwei Byte bei einem Speicherausbau zwischen 257 und 65536 Dateneinheiten und aus drei Byte bei mehr als 65536 Dateneinheiten. Bei einer Adresse von mehr als einem Byte folgt das höchstwertigste Byte direkt nach dem Instruction Code. Der Speicherausbau wird im ATR im Byte H2 (Protocol Parameter) angezeigt.

Das Data Unit-Feld enthält jeweils eine Dateneinheit. Die Größe einer Dateneinheit wird im ATR im Byte H2 (Protocol Parameter) angezeigt.

4.3.2 Kommando-Übersicht

Tab. 1 und Tab. 2 zeigen die Menge der verfügbaren Kommandos mit ihrem Instruction Code (INS) und den Betriebsmodus, den die Karte nach Empfang des Kommandos einnimmt (D = Datenantwort-Modus, V = Verarbeitungs-Modus).

INS	Bedeutung	Modus
´30´	READ MAIN MEMORY	D
´38´	UPDATE MAIN MEMORY	V
´34´	READ PROTECTION MEMORY	D
´3C´	WRITE PROTECTION MEMORY	V

Tab. 1: Kommandos für Karten mit Schreibschutz-Speicher

INS	Bedeutung	Modus
´31´	READ SECURITY MEMORY	D
´39´	UPDATE SECURITY MEMORY	V
´33´	COMPARE VERIFICATION DATA	V

Tab. 2: Kommandos für Karten mit zusätzlichem Sicherheits-Speicher

4.4 Speicherbereiche

4.4.1 Haupt-Speicher

Der Haupt-Speicher (´Main Memory´) ist der eigentliche Datenspeicher. Die erste Dateneinheit hat die Adresse ´00´.

Hinweis:
Für den ATR gibt es keinen separaten Speicherbereich, sondern er wird zu Beginn des Haupt-Speichers abgelegt (siehe Chipkarten mit synchroner Übertragung, Teil 1: ´ATR und Datenbereiche´)

4.4.2 Schreibschutz-Speicher

Der bei allen Karten vorhandene Schreibschutz-Speicher (´Protection Memory´) hat eine chiptyp-abhängige Größe, z.B. 4 Byte (= 32 Bit). Er ist ein separater Speicherbereich außerhalb des Haupt-Speichers. Jedes Bit ist einer Dateneinheit zugeordnet (Bit 0 der Dateneinheit 0, Bit 1 der Dateneinheit 1 usw.) und schützt die betreffende Dateneinheit gegen Update, falls es auf 0 gesetzt ist. Ist das betreffende Bit einmal auf 0 gesetzt, kann es nicht mehr auf 1 zurückgesetzt werden.

4.4.3 Sicherheits-Speicher

Der bei bestimmten Chiptypen zusätzlich vorhandene Sicherheits-Speicher (´Security Memory´) ist ein separater Speicherbereich und hat eine chiptyp-abhänige Größe, z.B. 4 Byte. Das erste Byte enthält einen Fehler-Zähler (´Error Counter´, Adresse ´00´), die folgenden Bytes beginnend mit der Adresse ´01´ sind für die Aufnahme von ´Verification Data´ bestimmt. Im Fehler-Zähler werden üblicherweise nur die Bits b3-b1 benutzt, womit die Anzahl der Fehlversuche auf drei begrenzt ist. Vor einer Verifikations-Prozedur muß ein Bit von 1 auf 0 gesetzt werden. Dann müssen die Verifkationsdaten unter Benutzung des COMPARE VERIFICATION DATA-Kommandos (siehe 4.5.7) gesendet werden. Danach kann der Fehler-Zähler mit dem UPDATE SECURITY MEMORY-Kommando (siehe 4.5.6) zurückgesetzt werden (bits b3-b1 = 111). Das Kriterium für eine erfolgreiche Verifikations-Prozedur ist, daß der Fehler-Zähler zurückgesetzt werden konnte, was durch Lesen des Fehler-Zählers mit dem Kommando READ SECURITY MEMORY (siehe 4.5.5) geprüft werden kann.

Wurde die Verifikations-Prozedur erfolgreich durchlaufen, dann können folgende Aktionen durchgeführt werden:

- Update im Haupt-Speicher mit dem Kommando UPDATE MAIN MEMORY
- Setzen von Schreibschutzbits von 1 auf 0 im Schreibschutz-Speicher durch das WRITE PROTECTION MEMORY-Kommando
- Ändern der Verifikationsdaten im Sicherheits-Speicher durch das UPDATE SECURITY MEMORY-Kommando.

4.5 Kommando-Beschreibungen

4.5.1 READ MAIN MEMORY

Das READ MAIN MEMORY-Kommando dient zum Lesen von Dateneinheiten und kann je nach Realisierungsform einen von zwei Ausführungstypen haben:

a) Typ 1: Lesen von einer Start-Adresse bis Speicherende

´30´	Start Address	(no effect)

Tab. 3: Codierung des READ MAIN MEMORY-Kommandos (Typ 1)

Das Data Unit-Feld wird bei diesem Ausführungstyp nicht ausgewertet. Alle Bits sind daher auf 0 (= Parameter not used) zu setzen.

b) Typ 2: Lesen einer spezifizierten Anzahl von Dateneinheiten ab der angegebenen Start-Adresse

´30´	Start Address	Number

Tab. 4: Codierung des READ MAIN MEMORY-Kommandos (Typ 2)

Der Ausführungstyp wird im Byte H2 (´Protocol Parameter´) im Bit b8 angezeigt (siehe Spezifikation Teil 1).

4.5.2 UPDATE MAIN MEMORY

Das UPDATE MAIN MEMORY-Kommando erlaubt das Überschreiben der im Adress-Feld spezifizierten Dateneinheit, falls die Update-Bedingungen hierfür gegeben sind (Chiptypen ohne Sicherheits-Speicher erlauben den Update nicht schreibgeschützter Dateneinheiten, Chiptypen mit Sicherheitsspeicher verlangen zuvor die erfolgreiche Abwicklung der Verifikations-Prozedur, siehe 4.4.3).

´38´	Address	Data Unit

Tab. 4: Codierung des UPDATE MAIN MEMORY-Kommandos

4.5.3 READ PROTECTION MEMORY

Das READ PROTECTION MEMORY-Kommando bewirkt das Lesen des gesamten Schreibschutz-Speichers.

´34´	(no effect)	(no effect)

Tab. 5: Codierung des READ PROTECTION MEMORY-Kommandos

Adreß- und Datenfeld sind auf 0 (= Parameter not used) zu setzen.

4.5.4 WRITE PROTECTION MEMORY

Das WRITE PROTECTION MEMORY-Kommando erlaubt das Setzen des Schreibschutz-Bits für eine Dateneinheit im Haupt-Speicher (bzgl. Zuordnung Schreibschutz-Bit zu Dateneinheit siehe 4.4.2). Das betreffende Bit im Schreibschutz-Speicher wird nur gesetzt, wenn die im Daten-Feld des Kommandos enthaltene Dateneinheit mit der im Haupt-Speicher abgelegten übereinstimmt.

´3C´	Address	Data Unit

Tab. 6: Codierung des READ PROTECTION MEMORY-Kommandos

4.5.5 READ SECURITY MEMORY

Das READ SECURITY MEMORY-Kommando bewirkt das Lesen des Sicherheits-Speichers. Zurückgeliefert werden - solange keine erfolgreiche Verifikationsprozedur durchlaufen wurde - der Wert des Fehler-Zählers und eine Sequenz von ´00´ (Anzahl von der Größe des Sicherheitsspeichers abhängig).

´31´	(no effect)	(no effect)

Tab. 7: Codierung des READ PROTECTION MEMORY-Kommandos

Adreß- und Datenfeld sind auf 0 (= Parameter not used) zu setzen.

4.5.6 UPDATE SECURITY MEMORY

Das UPDATE SECURITY MEMORY-Kommando erlaubt einen Update im Sicherheits-Speicher, wenn die Voraussetzungen hierfür gegeben sind (siehe 4.4.3).

´39´	Address	Data Unit

Tab. 8: Codierung des UPDATE SECURITY MEMORY-Kommandos

4.5.7 COMPARE VERIFICATION DATA

Das COMPARE VERIFICATION DATA-Kommando vergleicht die mitgelieferte Dateneinheit mit der im Sicherheits-Speicher adressierten Dateneinheit. Es ist entsprechend der Anzahl der Dateneinheiten, die die gesamten Verification Data bilden, mit jeweils fortgeschalteter Adresse und entsprechender Dateneinheit zu senden. Wie der erfolgreiche Ablauf geprüft werden kann, ist in Kapitel 4.4.3 beschrieben.

´33´	Address	Data Unit

Tab. 9: Codierung des COMPARE VERIFICATION DATA-Kommandos

Anhang A (normativ)

Signalablauf bei Reset und Datenübertragung

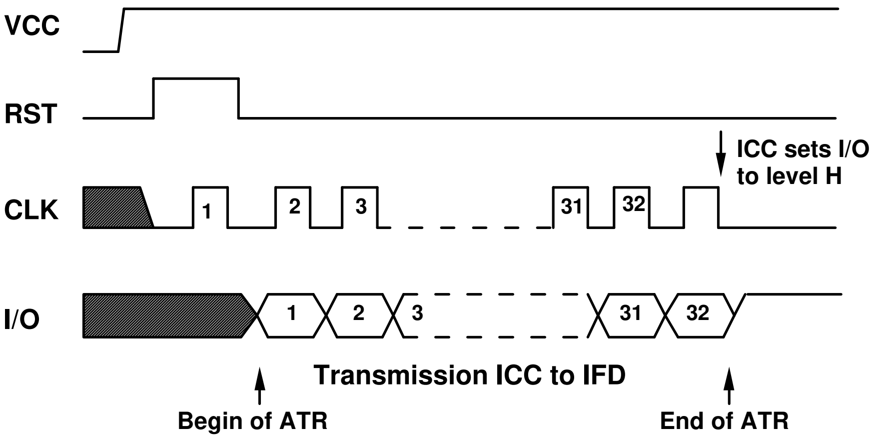

Abb. 1: Signalablauf bei Reset

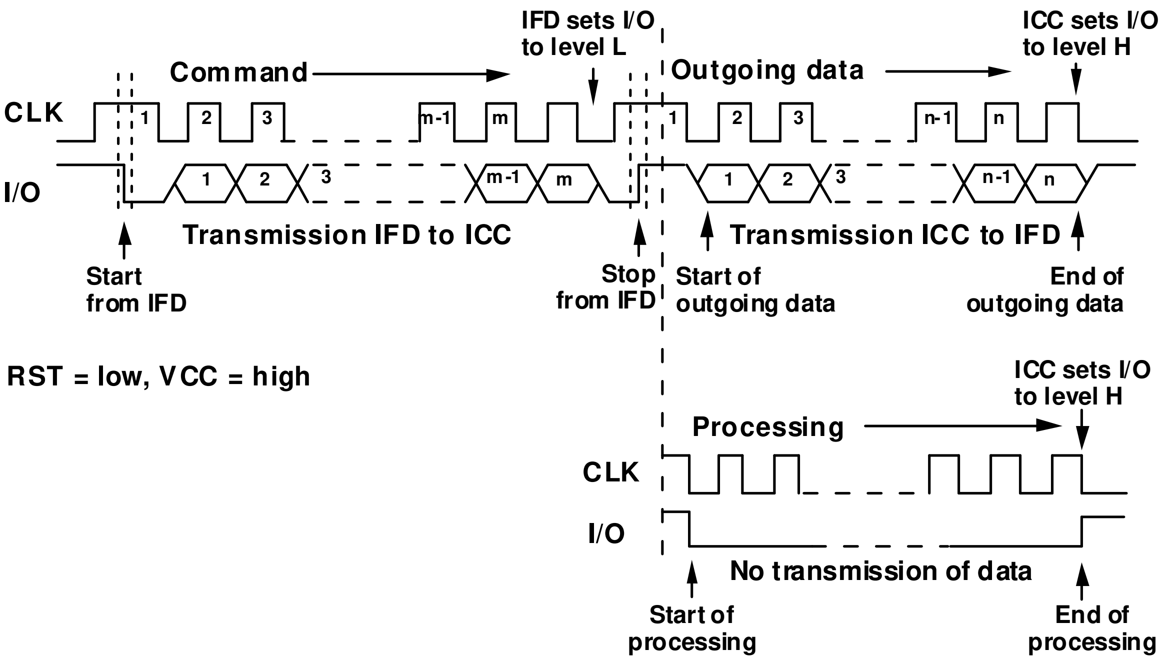

Abb. 2: Signalablauf bei Datenübertragung