Part 6

IC cards
with synchronous transmission

Part 2: Transmission protocols

Draft

20.07.95

DIN NI-17.4

Contents

1. Scope

This part of the specification for IC cards with synchronous transmission defines transmission protocols. The various protocol types are provided with an unambiguous identifier S. The protocol types from S = 0 to S = 7 are reserved for ISO.
The following types are specified in this part:

- S = 10 (2 Wire Bus Protocol 2WBP, half-duplex)
- S = 11 to S = 14 (reserved).

Note: The protocol types S = 8 and S = 9 denote the Serial Data Access Protocol SDAP and 3 Wire Bus Protocol 3WBP, both manufacturer specified transmission protocols.

2. Normative references

DIN NI-17: 1995
Integrated circuit(s) cards with synchronous transmission
Part 1: ATR and data sections

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
(The WD October 1994 in which AM 1 and AM 2 are intergrated is used)

3. Abbreviations

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

4. S=10: Half-duplex ´2 Wire Bus Protocol´

4.1 Overview

The protocol S = 10 is used for communication with IC cards, which indicate this protocol in the ATR. Due to the fact that two contacts (clock and I/O) are used for the communication after ATR, the protocol was simply named ´2 Wire Bus´ protocol or 2WBP.
The value 10 (= 2WBP) is coded in the most significant half-byte of H1 (see ICC with synchronous transmission, Part 1: ATR and data sections), so that an interface device (IFD) is able to set the correct protocol type for the communication with the card after the ATR has been received.

4.2 Data transmission

4.2.1 Conventions for data transmission

The bit b1 (least significant bit) of a byte is transmitted first. A logical 1 is depicted with level H (= high) on I/O, a logical 0 with level L (=low).

4.2.2 ATR

The reset of a card with the following ATR complies with the definitions of ISO/IEC 7816-3 and is illustrated in fig. 1, Annex A. Thus 32 clock pulses are needed to receive the 32 bit of the ATR. After the 32 clock pulses another clock pulse shall follow to set the I/O to H. Further following clock pulses do not change the state of the I/O any more.

4.2.3 Command mode

During data transmission from the IFD to the ICC each bit sequence (ICC command) starts with a START sequence and stops with a STOP sequence.

The START sequence is defined as follows:

Initial state: I/O = H, ICC in receptive state
IFD action: falling edge on the I/O, while clock is in state H

The bit transmission of a command is defined as follows:

Each bit is sent by

- applying the bit
- setting the clock to H
- setting the clock to L

as described in fig. 2 in annex A. After sending the last bit of a command from the IFD to the ICC the IFD must set the I/O to L.

The STOP sequence is defined as follows:

Initial state: I/O = L
IFD action: rising edge on the I/O, while the clock is in state H.

After transmission of a command to the ICC including the START and STOP sequences the card will be, depending on the command sent from the IFD, either in the 'data outgoing mode' or in the 'processing mode'. In these modes and also while sending the ATR the card ignores all START-/STOP-sequences.

4.2.4 Data outgoing mode

In the data outgoing mode the card reacts to the received command by sending data to the IFD. The first data bit on the I/O is transported with the first falling edge after the command mode is terminated. After the card has sent the last data bit another clock pulse must follow to set the I/O to state H. Then a new command, starting with the START sequence, can be received by the card.
Further following clock pulses do not change the state of the I/O any more.

4.2.5 Processing mode

In this mode the card reacts only internally to the received command. In order to process the command the card needs more pulses on CLK. In this mode the card sets the I/O to L after the pulse in which the STOP sequence occured. The IFD recognizes the end of this mode from the change of the I/O from L to H. Then a new command, starting with the START sequence, can be received by the card.
Further following clock pulses do not change the state of I/O any more.

4.3 Command structure and command overview

4.3.1 General command structure

The general format of a command consists of the three fields instruction code, address and data unit (see fig. 1).

Instruction Code	Address	Data Unit

Fig. 1: General command structure

The value field ´Instruction Code´ denotes the command and has a length of one byte.

The address field consists of one byte, if the memory has up to 256 data units, of two bytes when the memory has between 257 and 65536 data units and of three bytes, if the memory is larger than 65536 data units. If an address consists of more than one byte the most significant byte follows immediately after the instruction code. The memory size is indicated in the ATR in byte H2 (protocol parameter).

The data unit field consists of one data unit. The data unit size (e.g. one byte) is indicated in the ATR in byte H2 (protocol parameter).

4.3.2 Command overview

Tab. 1 and tab. 2 show all available commands with their instruction codes (INS) and the mode that the card adopts after the reception of the

command (D = data outgoing mode), P = processing mode).

INS	Meaning	Mode
´30´	READ MAIN MEMORY	D
´38´	UPDATE MAIN MEMORY	P
´34´	READ PROTECTION MEMORY	D
´3C´	WRITE PROTECTION MEMORY	P

Tab. 1: Commands for cards with write protection memory

INS	Meaning	Mode
´31´	READ SECURITY MEMORY	D
´39´	UPDATE SECURITY MEMORY	P
´33´	COMPARE VERIFICATION DATA	P

Tab. 2: Commands for cards with additional security memory

4.4 Memory types

4.4.1 Main memory

The general storage in the IC card with synchronous transmission is called main memory. The first data unit starts with the address '00'.

Note:
There is no separate memory for the ATR. The ATR is stored at the beginning of the main memory (see IC cards with synchronous transmission, Part 1: ATR and data sections).

4.4.2 Protection memory

The protection memory provided in cards supporting S = 10 is dimensioned according to the type of the chip, e.g. 4 byte (= 32 bit). It is a separate memory section outside the main memory. Each byte is assigned to a data unit, (bit 0 to data unit 0, bit 1 to data unit 1, etc.) and protects the respective data unit against update, if it is set to 0. Set once to 0, it cannot be reset to 1.

4.4.3 Security memory

The security memory, if present, is a separate memory. Its size is chip dependent, e.g. 4 byte. The first byte contains an error counter (address '00'), the following bytes starting at address '01' are used to store verification data. The error counter operates usually only with the bits b1-b3 so that the number of attempts is restricted to three. Before starting a verification procedure one bit must be set from 1 to 0. Then the verification data must be sent using the COMPARE VERIFICATION DATA command (see 4.5.7). After that the error counter can be reset (bits b3-b1=111) using the UPDATE SECURITY MEMORY command (see 4.5.6). The verification procedure is successful, when the error counter can be reset. This can be checked by reading the error counter using the command READ SECURITY MEMORY (see 4.5.5).

When the verification procedure has been successfully performed the following actions can be taken:

- Updating the main memory using the command UPDATE MAIN MEMORY
- Setting write protection bits from 1 to 0 in the write protection memory using the WRITE PROTECTION MEMORY command
- Changing the verification data in the security memory using the UPDATE SECURITY MEMORY command.

4.5 Commands

4.5.1 READ MAIN MEMORY

The READ MAIN MEMORY command is used to read data units and can be executed in one of two ways:

a) type 1: reading from a start address to the end of memory:

´30´	Start Address	(no effect)

Tab 3: Coding of the READ MAIN MEMORY-commands (type 1)

In the READ MAIN MEMORY command of type 1 the data unit field is present, but not evaluated. All bits of the data unit field shall therefore be set to '0' (= parameter not used).

b) type 2: reading a specified number of data units starting at the designated start address.

´30´	Start Address	Number

Tab. 4: Coding of the READ MAIN MEMORY commands (type 2)

The type of execution is indicated in bit b8 in byte H2 of the ATR.

4.5.2 UPDATE MAIN MEMORY

The UPDATE MAIN MEMORY command allows the update of the data unit specified in the address field, if the update conditions are given (chip types without security memory allow the updating of data units, which are not write protected, chip types with security memory require a prior successful verification procedure, see 4.4.3).

´38´	Address	Data Unit

Tab. 4: Coding of the UPDATE MAIN MEMORY command

4.5.3 READ PROTECTION MEMORY

The READ PROTECTION MEMORY command effects the reading of the complete write protection memory.

´34´	(no effect)	(no effect)

Tab. 5: Coding of the READ PROTECTION MEMORY command

Address field and data field shall be set to '0' (= parameter not used).

4.5.4 WRITE PROTECTION MEMORY

The WRITE PROTECTION MEMORY command allows the setting of the write protection bits for a data unit in the main memory (for assignment write protection bit to data unit see 4.4.2). The respective bit in the protection memory is only set when the data unit given in the command data field is identical with that in the main memory.

´3C´	Address	Data Unit

Tab. 6: Coding of the READ PROTECTION MEMORY command

4.5.5 READ SECURITY MEMORY

The READ SECURITY MEMORY command effects the reading of the security memory. As long as no successful verification procedure has taken place, the value of the error counter and a sequence of '00' (number depending on the size of the security memory) are returned.

´31´	(no effect)	(no effect)

Tab. 7: Coding of the READ PROTECTION MEMORY command

Address field and data field shall be set to '0' (= parameter not used).

4.5.6 UPDATE SECURITY MEMORY

The UPDATE SECURITY MEMORY command allows the update of the security memory, when the conditions herefor are met (see 4.4.3).

´39´	Address	Data Unit

Tab. 8: Coding of the UPDATE SECURITY MEMORY command

4.5.7 COMPARE VERIFICATION DATA

The COMPARE VERIFICATION DATA command compares the supplied data unit (in the command) with the data unit addressed in the security memory. The command must be sent as many times as data units for verification exists (e.g. 3 times, if 3 bytes have to be compared). Each command with the next data unit address and the corresponding data unit content. How to check successful processing is described in 4.4.3.

´33´	Address	Data Unit

Tab. 9: Coding of the COMPARE VERIFICATION DATA command

Annex A (normative)

Signal sequences for reset and data transmission

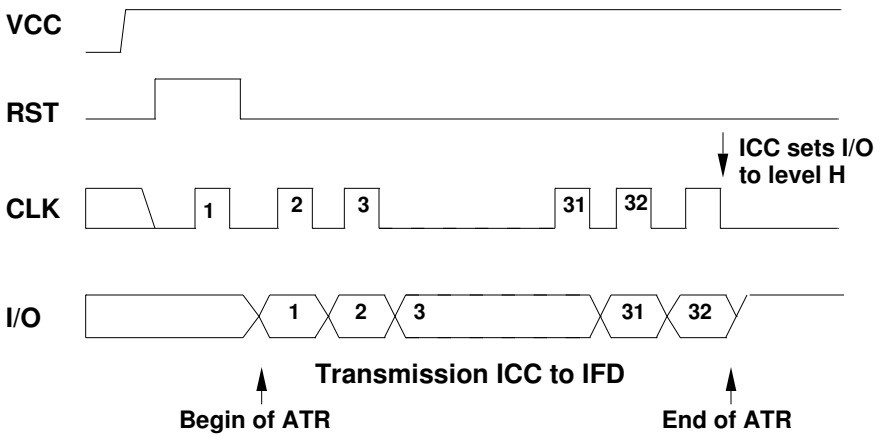

Fig. 1: Sequence of signals for reset

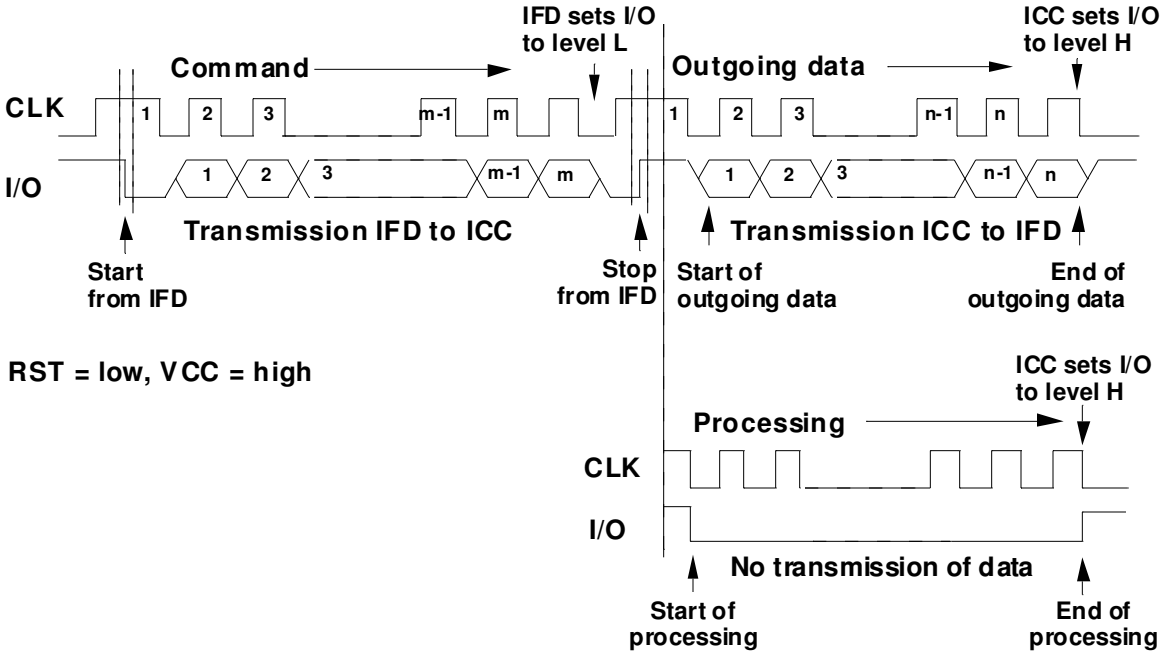

Fig. 2: Sequence of signals for data transmission