Schlumberger Multiflex 3K/8K and (limited) Cryptoflex

March 25, 2008

Contents

1 Preface

I wrote this document, because there is (Update: was) nearly no detailed technical documentation available about chipcards.

The sources for this documentation are the Smartcard Developer Kit (Can't say, that it is worth it's money. "Handbuch der Chipkarten" (or in English probably "Handbook of Chipcards") from Rankl and Effing is a much better and at least in Germany much cheaper book.), the data files of EZFormatter, the "technical highlights" from Schlumberger (This is the "manual" which you can order there for US$5. Not that interesting, that it would justify that much money.), usenet newsgroups and from experimenting with the card.

You can order Schlumberger cards (Multiflex 3K, Multiflex 8K, Cryptoflex (if in the USA or Canada), Cyberflex (Java card), Payflex, etc.) in quantities of 5 at their eshop at https://www.cyberflex.slb.com/.

2 Commands

2.1 Change PIN

Description

Replaces the 8-byte PIN in the currently selected PIN file with a new 8-byte value.

C-APDU

CLA	INS	P1	P2	Lc
F0	24	00	01	10

Data1: Current PIN (8 Byte filled up with FF)

Data2: New PIN (8 Byte filled up with FF)

R-APDU

SW1	SW2

2.2 Check ROM

Description

Tests integrity of ROM code.

C-APDU

CLA	INS	P1	P2	Lc
??	CC	??	??	??

R-APDU

??	SW1	SW2

2.3 Create File

Description

Creates a new file in the current directory. The new file becomes the current file.

C-APDU

CLA	INS	P1	P2	Lc
F0	E0	P1	P2	Lc

P1: Initialization flag (00: Initialize, FF: Do not initialize)

P2: Number of records for (fixed-length?) record files

Data1: File description

Data2: First 6 bytes of cryptogram when required by access conditions.

R-APDU

SW1	SW2

2.4 Create Record

Description

Creates a new record at the end of the current record file and optionally write data to it. The filesize can still not be more than allocated at creation time.

C-APDU

CLA	INS	P1	P2	Lc
C0	E2	00	00	Lc

Data1: Data to be written to new record.

Data2: First 6 bytes of cryptogram when required by access conditions.

Table 1: File description for creation of file

Byte	Value	Meaning
1-2	FFFF	Unused
3-4	-	Size (also for DF)
5-6	-	FID
7		File type
	01	Transparent file
	02	Record file with fixed-length records
	04	Record file with variable-length records
	06	Cyclic file
	38	Directory file
8	-	Update access conditions (see below)
9-11		Access conditions (see below)
9 High		DF: Directory (Only Multiflex 8K and Cryptoflex) EF: Read, Seek
9 Low		DF: - EF: Update, Decrease, Decrease Stamped
10 High		DF: Delete File EF: Increase, Increase Stamped
10 Low		DF: Create File EF: Create Record
11 High		DF/EF: Rehabilitate
11 Low		DF/EF: Invalitate
12		Status
	00	blocked
	01	unblocked
13	-	Number of following bytes
n - n+2	-	Access keys for access conditions (Nibble is cryptographic key number)
m	-	Record length (only for record files)

Table 2: Elementary file update access conditions

Bit 8	Bit 7	Allowed Operations	Disallowed Operations
0	0	Update	Increase, Decrease
0	1	Update, Increase	Decrease
1	0	Update, Decrease	Increase
1	1	Decrease, Increase	Update

R-APDU

SW1	SW2

Table 3: Identities or authentications for access conditions

Key knowledge needed	Value of access condition nibble
Always possible	0
PIN	1
Protected	3
Authenticated	4
PIN and protected	6
PIN and authenticated	8
Never possible	F

2.5 Decrease

Description

The oldest (that is, previous) record in a cyclic file is overwritten with the newest (that is, current) record, minus the amount given in the command. This new record then becomes the current record.

C-APDU

CLA	INS	P1	P2	Lc
F0	30	00	00	Lc

Data1: 3 Byte value to be subtracted

Data2: First 6 bytes of cryptogram when required by access conditions.

R-APDU

SW1	SW2

Data may be available.

2.6 Decrease Stamped (Only Multiflex 8K)

Description

The oldest (that is, previous) record in a cyclic file is overwritten with the newest (that is, current) record, minus the amount given in the command. This new record then becomes the current record. Give Challenge must preceede this command.

C-APDU

CLA	INS	P1	P2	Lc
F0	34	00	00	Lc

Data1: 3 Byte value to be subtracted

Data2: First 6 bytes of cryptogram when required by access conditions.

R-APDU

SW1	SW2

Stamped data may be available.

Table 4: Stamped data

Byte	Description
1 - 3	New value
4 - 6	Ammount subtracted
7 - 12 (14?)	Cryptogram

2.7 Delete File

Description

Deletes the named file.

It appears, that files in a DF can only be deleted in same order as creation. Luckily whole DFs can be deleted.

C-APDU

CLA	INS	P1	P2	Lc
F0	E4	00	00	Lc

Data1: 2 Byte file identifier

Data2: First 6 bytes of cryptogram when required by access conditions.

R-APDU

SW1	SW2

2.8 Directory (Only Multiflex 8K and Cryptoflex)

Description

C-APDU

CLA	INS	P1	P2	Le
F0	A8	00	00	00

R-APDU

SW1	SW2

Directory data my be available.

Table 5: Directory data for each file

Byte	Value	Meaning
1-2	-	DF: Free bytes available (?) EF: Size
3-4	-	FID
5	-	File type
6	-	Status
7	-	Record length
8	-	Number of records

2.9 External Authentication

Description

The terminal wishes to gain external authentication access to the card without sending a key to it using Verify Key. It got a challenge from the card using Get Challenge and is now going to return its encryption of this challenge to prove it knows the key.

C-APDU

CLA	INS	P1	P2	Lc
C0	82	00	00	07

Data1: Key number (00-0F)

Data2: First 6 bytes of DES encrypted challenge

R-APDU

SW1	SW2

2.10 Get Challenge

Description

The card is requested to send back an 8-byte challenge.

C-APDU

CLA	INS	P1	P2	Le
C0	84	00	00	08

R-APDU

Challenge	SW1	SW2

Challenge: 8 Byte random challenge to be used with External Authentication

2.11 Get Response

Description

C-APDU

CLA	INS	P1	P2	Le
C0	C0	00	00	Le

R-APDU

Data	SW1	SW2

Data: Le Bytes of available data

2.12 Give Challenge (Only Multiflex 8K)

Description

Sends a 8-byte challenge to the card.

C-APDU

CLA	INS	P1	P2	Lc
F0	86	00	00	08

Data: 8 Byte random challenge

R-APDU

SW1	SW2

2.13 Increase

Description

The oldest (i.e., previous) record in a cyclic file is overwritten with the newest (i.e., current) record, plus the amount given in the command. This new record then becomes the current record.

C-APDU

CLA	INS	P1	P2	Lc
F0	32	00	00	Lc

Data1: 3 Byte numeric value to be added

Data2: First 6 bytes of cryptogram when required by access conditions.

R-APDU

SW1	SW2

Data may be available.

2.14 Increase Stamped (Only Multiflex 8K)

Description

The oldest (i.e., previous) record in a cyclic file is overwritten with the newest (i.e., current) record, plus the amount given in the command. This new record then becomes the current record. Give Challenge must preceede this command.

C-APDU

CLA	INS	P1	P2	Lc
F0	36	00	00	Lc

Data1: 3 Byte numeric value to be added

Data2: First 6 bytes of cryptogram when required by access conditions.

R-APDU

SW1	SW2

Stamped data may be available.

Table 6: Stamped data

Byte	Description
1 - 3	New value
4 - 6	Ammount subtracted
7 - 12 (14?)	Cryptogram

2.15 Internal Authentication

Description

The terminal wishes to authenticate the card to ensure it is a valid card, so it sends the card a challenge that the card must encrypt using a specified key in the internal authorization file (0001) for the current directory. A following Get Response command returns the first 6 bytes of the DES encryption of the challenge using the indicated key.

C-APDU

CLA	INS	P1	P2	Lc
C0	88	00	P2	08

P2: Key number (00-0F)

Data: 8 Byte challenge

R-APDU

SW1	SW2

Data may be available.

2.16 Internal RSA Authentication (Only Cryptoflex)

Description

”Signs a message given by the external world using RSA.”

C-APDU

CLA	INS	P1	P2	Lc
94	42	00	KeyNum	80

KeyNum: RSA key number

Data: Data

R-APDU

SW1	SW2

2.17 Invalidate

Description

The currently selected elementary file is invalidated and will subsequently only respond successfully to the Selected File and Rehabilitate commands.

C-APDU

CLA	INS	P1	P2	Lc
F0	04	00	00	Lc

Data: First 6 bytes of cryptogram when required by access conditions.

R-APDU

SW1	SW2

2.18 Key Generation (Only Cryptoflex)

Description

Generates 1024bit RSA key.

C-APDU

CLA	INS	P1	P2	Lc
F0	14	00	KeyNum	00

KeyNum: RSA key number

R-APDU

SW1	SW2

2.19 Load Certificate (Only Cryptoflex)

Description

”Loads a certificate signed by a certificate authority and extracts the application’s RSA public key from it.”

C-APDU

CLA	INS	P1	P2	Lc
F0	84	00	KeyNum	80

KeyNum: RSA key number

Data: RSA public key

R-APDU

SW1	SW2

2.20 Load EXE

Description

Loads executable code into EEPROM to add new functions.

C-APDU

CLA	INS	P1	P2	Lc
F0	F4	??	??	??

Arguments: FID, Data

R-APDU

??	SW1	SW2

2.21 Read Binary

Description

Reads a sequence of bytes from the currently selected transparent file.

C-APDU

CLA	INS	P1	P2	Le
C0	B0	P1	P2	Le

P1: High byte of the 2-byte offset

P2: Low byte of the 2-byte offset

Le: Number of bytes to read starting at the offset byte

R-APDU

Data	SW1	SW2

Data: Le Bytes of data from file

2.22 Read Header (Only Multiflex 8K and Cryptoflex)

Description

Retrives detailed information on current file descriptor.

C-APDU

CLA	INS	P1	P2	Lc
??	??	??	??	??

R-APDU

??	SW1	SW2

2.23 Read EEPROM

Description

Reads EEPROM test zone.

C-APDU

CLA	INS	P1	P2	Le
??	BA	??	??	??

R-APDU

??	SW1	SW2

2.24 Read Record

Description

Reads one record from the currently selected record file.

C-APDU

CLA	INS	P1	P2	Le
C0	B2	P1	P2	Le

P1: Index of record to be read (00: current record)

P2: Selection of the record to be read (00: first record, 01: last record, 02: next record, 03: previous record, 04: current record if index is 00, else index record)

Le: Bytes to read (Must be equal record length)

R-APDU

Data	SW1	SW2

Data: Le Bytes of data from record

2.25 Read Status (Only Multiflex 8K and Cryptoflex)

Description

Lists status and context variables.

C-APDU

CLA	INS	P1	P2	Lc
??	??	??	??	??

R-APDU

??	SW1	SW2

2.26 Rehabilitate

Description

The currently selected elementary file is rehabilitated (that is, removed from invalidated status).

C-APDU

CLA	INS	P1	P2	Lc
F0	44	00	00	Lc

Data: First 6 bytes of cryptogram when required by access conditions.

R-APDU

SW1	SW2

2.27 Seek

Description

Locate a record in a linear record file by matching a pattern of characters to the characters in each record starting at a given offset from the beginning of the record

C-APDU

CLA	INS	P1	P2	Lc
F0	A2	P1	P2	Lc

P1: Offset

P2: Search mode (00: from first record, 02: from next record)

Data: Character string to be matched

R-APDU

SW1	SW2

2.28 Select File

Description

The file whose file ID is given in the data field of the command becomes the currently selected file. It must be a file in the currently selected directory. If the named file is a directory, then it becomes the currently selected directory. If the file identifier is 0x3F00 it is always the master files selected. If the file identifier is the directory file directly above the current file it becomes the current file.

C-APDU

CLA	INS	P1	P2	Lc
C0	A4	00	00	02

Data: 2-Byte file identifier

R-APDU

SW1	SW2

File description data my be available.

2.29 Unblock PIN

Description

The selected PIN file has become blocked because the number of presentations of an incorrect PIN has exceeded the number of allowed tries. This command will unblock the PIN file and reset the PIN to a new value.

C-APDU

CLA	INS	P1	P2	Lc
F0	2C	00	01	10

Data1: 8-Byte unblocking PIN for current PIN file

Data2: 8-Byte new PIN

R-APDU

SW1	SW2

2.30 Update Binary

Description

A sequence of bytes is written into thee currently selcted transparent elementary file.

Table 7: File description for selection of file

Byte	Value	Meaning
1-2	-	Unused
3-4	-	DF: Free bytes available EF: Size
5-6	-	FID
7		File type
	01	Transparent file
	02	Record file with fixed-length records
	04	Record file with variable-length records
	06	Cyclic file
	38	Directory file
8	-	Update access conditions (see Create File) Unused of directory files
9-11		Access conditions (see Create File)
9 High		DF: Directory EF: Read, Seek
9 Low		DF: - EF: Update, Decrease, Decrease Stamped
10 High		DF: Delete File EF: Increase, Increase Stamped
10 Low		DF: Create File EF: Create Record
11 High		DF/EF: Rehabilitate
11 Low		DF/EF: Invalitate
12		Status
	00	blocked
	01	unblocked
		Directory files:
13	05	Number of following bytes
14	-	Unused
15	-	Number of subdirectories in this directory
16	-	Number of elementary files in this directory
17	-	Number of secret codes in this directory
18	-	Unused
19	-	Status of the PIN for this directory
20	-	Status of the PIN unblocking key
		Elementary files:
13	01	Number of following bytes
14	-	Unused
15	-	Length of record in fixed-length record files (00 for non-record files)

C-APDU

CLA	INS	P1	P2	Lc
C0	D6	P1	P2	Lc

P1: High byte of the 2-byte offset

P2: Low byte of the 2-byte offset

Lc: Number of bytes to be written into the file starting at the offset byte; +6 if cryptogram is provided

Data1: Data to be written starting at he offset byte

Data2: First 6 bytes of cryptogram when required by access conditions.

R-APDU

SW1	SW2

2.31 Update Key Enciphered (Only Cryptoflex)

Description

"Receives enciphered data by means of the DES algorithm."
(Is this Update Binary with cryptogram?)

C-APDU

CLA	INS	P1	P2	Le
C0	DE	P1	P2	Le

P1: High offset

P2: Low offset

Data: Data

R-APDU

SW1	SW2

2.32 Update Record

Description

One record in the currently slected record file is overwritten with new data.

C-APDU

CLA	INS	P1	P2	Lc
C0	DC	P1	P2	Lc

P1: Index of record to be overwritten (00: current record)

P2: Selection of the record to be overwritten (00: first record, 01: last record, 02: next record, 03: previous record, 04: current record if index is 00, else index record)

Le: Bytes to be written (Must be equal record length); +6 if cryptogram is provided

Data1: Data to be written

Data2: First 6 bytes of cryptogram when required by access conditions.

R-APDU

SW1	SW2

2.33 Verify Data (Only Cryptoflex)

Description

"Authenticates data signed and sent by the application. The length of the applied RSA is 1024 bits."

C-APDU

CLA	INS	P1	P2	Lc
F0	82	00	KeyNum(?)	80

KeyNum: RSA key number

Data: Data

R-APDU

SW1	SW2

2.34 Verify Key

Description

Match a byte sequence with a key in the external authorization file (0011) for the current directory. If the match is exact, external authorization access priviledges are granted.

C-APDU

CLA	INS	P1	P2	Lc
F0	2A	00	P2	Lc

P2: Key number (00-0F)

Data: Key

R-APDU

SW1	SW2

2.35 Verify PIN

Description

Attempt to match the 8 bytes in the command with the 8-byte PIN in the PIN file for the current directory. If the match is exact the PIN access priviledges are granted.

C-APDU

CLA	INS	P1	P2	Lc
C0	20	00	01	08

Data: 8-Byte PIN

R-APDU

SW1	SW2

2.36 Verify Pub Key (Only Cryptoflex)

Description

"Receives the public key of the application Kp_App in plain text and in full length for verification with a previously extracted public key (see Load Certificate)."

C-APDU

CLA	INS	P1	P2	Lc
F0	86	00	KeyNum(?)	80

KeyNum: RSA key number

Data: Data

R-APDU

SW1	SW2

2.37 Write EEPROM

Description

Writes to EEPROM test zone.

C-APDU

CLA	INS	P1	P2	Lc
??	B8	??	??	??

R-APDU

??	SW1	SW2

3 File Structures

3.1 Important files

FID	File Name	Contents	Max. Num.
			of Keys
0000	PIN file	PIN code	1
0001	Internal authentication file	Internal cryptographic keys	16
0002	Serial number file	Serial number, customer ID, etc.	
0011	External authentication file	External cryptographic keys	16
3F00	Master File		

3.2 Record file sizes

File type	Maximum Record Size	Maximum Number of Records
Record file with fixed-length records	255 Bytes	255
Record file with variable-length records	255 Bytes	255
Cyclic file	255 Bytes	255

3.3 Serial number file

Bytes	Description
1 - 4	Series number
5	Customer identification code
6 - 7	Schlumberger manufacturing site
8	Usage

3.4 PIN file

Bytes	Description
1	Activation byte (00: PIN blocked, FF: unblocked)
2 - 3	RFU
4 - 11	PIN code (FF: Byte is ignored)
12	Attempts allowed
13	Attempts remaining
14 - 21	Unblocking PIN code (FF: Byte is ignored)
22	Unblocking attempts allowed
23	Unblocking attempts remaining

3.5 Authentication key files

Bytes	Description
1	Unused
2	Length of key 0 (Normally 8, because of DES)
3	Algorithm for key 0 (0: DES)
4 - 11	Key 0 (when 8 bytes long)
12	Maximum attempts for key 0
13	Remaining attempts for key 0
14 -	For next keys repeate bytes 2 - 13

Default external authentication key file in MF contains keys 0, 1 and 2. Key 1 is set to 47h 46h 58h 49h 32h 56h 78h 40h. You have three tries to present the correct key. This is valid for the cards which come with the SCDK and the cards ordered at the web site mentioned in the preface.

4 Misc

4.1 Validity of PINs and cryptographics keys

PINs and cryptographics keys are valid in the directory of the key files and all subdirectories where no appropriate key file is.

The cryptogram ist the first 6 bytes of a DES-encrypted challenge. (SCDK varies between 6 and 8 bytes, but most of the time it is 6 bytes.)

4.2 Cryptogram

The normal command excluding the CLA byte is filled up with 0xFF up to a multiple of 8 bytes. The maximum data size is 24 bytes. This data is encrypted with DES-CBC with a previously fetched challenge as an initial vector. The first 6 bytes of the last encrypted block is the cryptogram.

To use this cryptogram send everything of the above data starting at the length byte including the filling bytes up to the cryptogram as the data of the instruction and adjust the Lc byte of the real header accordingly.

4.3 ATR

Card	ATR
Multiflex 3K - G1	3B 02 14 50
Multiflex 3K - G1	3B 32 15 00 06 80
Multiflex 8K	3B 32 15 00 06 80
Cryptoflex	3B 63 00 00 36 41 80

4.4 Status words

Status word	Description
61 XX	Command executed successfully; XX bytes available
62 81	Data my be corrupted
62 83	Current directory/file is invalidated
63 00	Invalid PIN/cryptogram
65 00	Too much data for protected-mode
65 81	Memory problem
65 81	Update impossible
67 XX	Incorrect P3; expected XX
69 81	No PIN or key defined
69 82	Access condition not fulfilled
69 83	(Unblocking) PIN/Key currently blocked
69 85	No Get Challenge immediately preceding command
69 86	Currently selected file is not a cyclic file
69 86	No file selected
6A 80	Pattern not found
6A 80	File ID already in use in this directory
6A 80	Record length value is too large
6A 80	Type of current file is inconsistent with command
6A 82	File ID not found
6A 83	Record index out of range
6A 84	Insufficient memory space available
6B 00	Incorrect P1 or P2
6B 00	Offset out of range
6D 00	Unknown INS
6E 00	Unknown CLA
6F 00	Internal problem
90 00	Command executed successfully
98 50	Decrease cannot be performed; new value would be less than minimum