APDU-Test Card
Functional Requirements

Autor **Andreas Schwier**
Version **V1.1**
Datum **03. January 2012**

Content

Revisions

Datum	Bearbeiter	Änderungen	Version
18.11.2011	Andreas Schwier	Initial Version for Public Release	1.0
03.01.2012	Andreas Schwier	Removed requirement FX.CAS2.2 and FX.CAS4.2 to allow zero sized card objects	1.1

1 Overview

The APDU-Test Card implements four test APDUs, one for each case and each supporting short or extended APDUs. Each APDU implements a deterministic behaviour that allows testing the communication path between a test application and the test card.

2 Card Configuration

2.1 Answer to Reset (ATR)

During a reset the card answers with the ATR

3B FE 18 00 00 81 31 FE 45 80 31 81 54 48 53 4D 31 73 80 21 40 81 07 FA

which has the following meaning:

Element	Content	Meaning
TS	3B	Direct logic
TO	FE	TA1, TB1, TC1, TD1 present 14 Historical bytes
TA1	18	Clock conversion rate 372 Maximum frequency 5 MHz Bit rate conversion factor 12
TB1	00	Deprecated
TC1	00	Extra guard time
TD1	81	TD2 present T=1
TD2	31	TA3, TB3 present T=1
TA3	FE	Information field size 254
TB3	45	Character waiting time 43 etu Block waiting time 15371 etu
HB1	80	Category indicator
HB2-3	3181	Card service data byte - Application selection by full DF name - No EF.DIR / EF.ATR access service - Card without MF
HB4-8	5448534D31	Card issuer data - "HSM1"
HB9-12	73802140	Card capabilities - DF selection by full DF name - Proprietary write - Data unit 8 bit - Command chaining supported - Extended Lc und Le fields - No logical channel
HB13-14	8107	Life Cycle Operational State
TCK	FA	XOR of T0 to HB14

Table 1 - Answer to Reset

The card supports T=1 on the contact interface and T=CL on the contactless interface.

3 Commands

3.1.1 SELECT

The SELECT APDU allows the terminal to select the APDU-Test applet on the card. The application is identified by the application identifier:

E8 2B 06 01 04 01 81 C3 1F 02 02

The aid represents the object identifier

iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) CardContact(24991) iso7816(2) apdutest (2)

For selecting the application on the card, the following APDU shall be used:

CLA	'00'	
INS	'A4'	SELECT
P1	'04'	Select application DF
P2	'04'	Return File Control Parameter (FCP)
Lc	'0B'	
C-Data	AID	Application identifier as defined above
Le	'00'	
R-Data	FCP	File control parameter as defined below
SW1/2	'90 00'	Normal processing
	'6A 82'	Applet not found

Table 2 - SELECT APDU for the Applet

The following file control parameters are returned when selecting the application:

Tag	**Len**	**Value**
'62'		File Control Parameter
'82'	'01'	'78' – shareable DF
'85'	'02'	Major || Minor version number
'89'	'05'	The transmission parameter as defined in Table 4

Table 3 – File Control Parameter for SELECT application

In tag '89' the card transmits the current communication parameter:

Offset	**Length**	**Content**
0	1	Media interface and active protocol 0x – Contact interface 8x - Contactless Type A 7x – Contactless Type B 6x - USB x0 – T=0 x1 – T=1 or T=CL
1	2	Information Field Size for ICC (IFSC)
3	2	Information Field Size for Interface Device (IFSD)

Table 4 – Transmission parameter

/FR.SELA.1/ The system must select the application and return in R-Data the file control parameter and SW1/SW2 = '90 00' – Normal processing.

3.1.2 Case 1 Test

The Case 1 Test command expects the reader to transmit a Case 1 APDU as defined in [ISO7816-3]. The APDU only returns SW1/SW2, but no response data.

CLA	'80'	
INS	'F1'	Case 1 APDU Test
P1	'00'	
P2	'00'	
Lc	Absent	
C-Data	Absent	
Le	Absent	
R-Data	Absent	
SW1/2	'90 00'	Normal processing
	'67 00'	Wrong length
	'6A 86'	Incorrect parameters P1-P2

Table 5 – Case 1 Test APDU

/FR.CAS1.1/ The system must respond with empty R-Data and SW1/SW2 = '90 00' – Normal processing.

3.1.2.1 Exception Handling

/FX.CAS1.1/ If the C-Data field is present, then the system must respond with empty R-Data and SW1/SW2 = '67 00' - Wrong length.

/FX.CAS1.2/ If the P1 field does not contain '00' or the P2 field does not contain '00', then the system must respond with empty R-Data and SW1/SW2 = '6A 86' - Incorrect parameters P1-P2.

3.1.3 Case 2 Test

The Case 2 Test command transmits to the reader the number of bytes requested in Ne, based on a card object with the size defined by P1 and P2.

CLA	'80'	
INS	'F2'	Case 2 APDU Test
P1	Var	MSB of card object size
P2	Var	LSB of card object size
Lc	Absent	
C-Data	Absent	
Le	Var	Ne encoded in short or extended format
R-Data	Var	The requested number of bytes which is a repeating sequence of the bytes 'A55A0000FFFFCAFEBABE'
SW1/2	'90 00'	Normal processing
	'62 82'	End of file reached before reading Ne bytes.
	'67 00'	Wrong length

Table 6 – Case 2 Test APDU

/FR.CAS2.1/ The system must respond with the requested number of bytes build from the reference string in R-Data and SW1/SW2 = '90 00' – Normal processing.

/FR.CAS2.2/ If Ne is not 0 and requests more data than is actually available based on the definition in P1 and P2, then the system must respond with the available data in R-Data and SW1/SW2 = '62 82' – End of file reached before reading Ne bytes.

3.1.3.1 Exception Handling

/FX.CAS2.1/ If the C-Data field is present, then the system must respond with empty R-Data and SW1/SW2 = '67 00' - Wrong length.

3.1.4 Case 3 Test

The Case 3 Test command transmits arbitrary data to the card. The received data is silently discarded.

CLA	'80'	
INS	'F3'	Case 3 APDU Test
P1	'00'	
P2	'00'	
Lc	Var	Nc encoded in short or extended format
C-Data	Var	Arbitrary data with the length encoded in Nc
Le	Absent	
R-Data	Absent	
SW1/2	'90 00'	Normal processing
	'67 00'	Wrong length
	'6A 86'	Incorrect parameters P1-P2

Table 7 – Case 3 Test APDU

/FR.CAS3.1/ The system must accept arbitrary data in C-Data and respond with empty R-Data and SW1/SW2 = '90 00' – Normal processing.

3.1.4.1 Exception Handling

/FX.CAS3.1/ If the C-Data field is missing, then the system must respond with empty R-Data and SW1/SW2 = '67 00' - Wrong length.

/FX.CAS3.2/ If the P1 field does not contain '00' or the P2 field does not contain '00', then the system must respond with empty R-Data and SW1/SW2 = '6A 86' - Incorrect parameters P1-P2.

/FX.CAS3.3/ If the number of bytes transmitted in C-Data field does match Nc, then the system must respond with empty R-Data and SW1/SW2 = '6A 80' - Incorrect parameters in the command data field.

3.1.5 Case 4 Test

The Case 4 Test command transmits arbitrary data to the card and responds with the number of bytes requested in Ne. The received data is silently discarded and the transmitted data is as defined for the Case 2 Test.

CLA	'80'	
INS	'F4'	Case 4 APDU Test
P1	Var	MSB of card object size
P2	Var	LSB of card object size
Lc	Var	Nc encoded in short or extended format
C-Data	Var	Arbitrary data with the length encoded in Nc
Le	Var	Ne encoded in short or extended format
R-Data	Var	The requested number of bytes which is a repeating sequence of the bytes 'A55A0000FFFFCAFEBABE''
SW1/2	'90 00'	Normal processing
	'67 00'	Wrong length
	'6A 86'	Incorrect parameters P1-P2

Table 8 – Case 4 Test APDU

/FR.CAS4.1/ The system must accept arbitrary data in C-Data and respond with the requested number of bytes in R-Data and SW1/SW2 = '90 00' – Normal processing.

/FR.CAS4.2/ If Ne is not 0 and requests more data than is actually available based on the definition in P1 and P2, then the system must respond with the available data in R-Data and SW1/SW2 = '62 82' – End of file reached before reading Ne bytes.

3.1.5.1 Exception Handling

/FX.CAS4.1/ If the C-Data field is missing, then the system must respond with empty R-Data and SW1/SW2 = '67 00' - Wrong length.

/FX.CAS4.3/ If the number of bytes transmitted in C-Data field does match Nc, then the system must respond with empty R-Data and SW1/SW2 = '6A 80' - Incorrect parameters in the command data field.

3.1.6 GET INFO

The GET INFO command returns information about the last APDU processed.

CLA	'80'	
INS	'F0'	GET INFO
P1	'00'	
P2	'00'	
Lc	Absent	
C-Data	Absent	
Le	'00'	
R-Data	Var	A sequence of information bytes reflecting the processing of the last APDU as defined in Table 10
SW1/2	'90 00'	Normal processing
	'67 00'	Wrong length
	'6A 86'	Incorrect parameters P1-P2

Table 9 – GET INFO APDU

Offset	Length	Content
0	1	CLA
1	1	INS
2	1	P1
3	1	P2
4	2	Nc requested
6	2	Nc received
8	2	Ne requested
10	2	Ne transmitted

Table 10 – GET INFO R-Data

/FR.INFO.1/ The system must respond with the information about the last processed test APDU in R-Data and SW1/SW2 = '90 00' – Normal processing.

3.1.6.1 Exception Handling

/FX.INFO.1/ If the C-Data field is present, then the system must respond with empty R-Data and SW1/SW2 = '67 00' - Wrong length.

/FX.INFO.2/ If the Ne field does not encode 0 or 12, then the system must respond with empty R-Data and SW1/SW2 = '67 00' - Wrong length.

References

[ISO7816-3] Information Technology – Identification card – Integrated circuit(s) card with contacts – Part 3: Electronic signals and transmission protocols.