TeleTrusT Deutschland e.V.
Der IT-Sicherheitsverband.

SICCT
Secure Interoperable ChipCard Terminal

Version: 1.6
Date: 15.12.2009

VERSIONSHISTORIE

Datum	Version	Release
15.02.2008	1.0	Working Draft
21.02.2008	1.1	Working Draft
13.03.2008	1.2	Working Draft
14.03.2008	1.3	SICCT-WG: confirmed Release
16.07.2008	1.4	New Release Candidate to be confirmed by SICCT-WG:
13.08.2008	1.5	Minorfix : New Release on gematik Request
14.09.2009	1.6.	Tags for TLS 1.1 added
01.12.009		[CMD DO]
15.12.2009		SICCT MODIFY VERIFICATION DATA

Errata Beschreibung

Dieses Dokument beschreibt bekannte und von der SICCT-WG bearbeitete Errata-Korrekturen zu der Spezifikation “Secure Interoperable Chipcard Terminal“ [SICCT_120] der Version V1.20 vom 19.11.2007.

Geänderte Inhalte zur [SICCT-120] wurden im Text gelb markiert.

Data Length Lc und Expected Response Length Le - 5.3.1

Korrektur (13.03.2008): 5.3.1 Genereller Zusatz für alle SICCT Kommandos

Für die Darstellung von Lc sowie Le soll es in allen SICCT-Kommandos ebenso zulässig sein, die erweiterte Längendarstellung nach den Regeln aus ISO 7816-4 (s. 5.1 SICCT Command Structure) für Lc und Le durchgängig zu verwenden, auch wenn diese Form in den Beschreibungen zu den SICCT-Kommandos nicht explizit erscheint.

Betriebsmodus 'SICCT' und Command Set - 5.5.7

Korrektur (18.02.2008 / 13.03.2008): Korrektur 5.5.7

CardTerminal Basic Command	CLA Code (hex)	INS Code (hex)	P1	P2	Lc	Cmd Data	Le	Brief Description	
SICCT RESET CT / ICC	80	11	FU	CQ	cond	cond	opt	man	Perform Cold / Warm Reset and optional PPS. Reset of the ▪ cardterminal device ▪ RF antenna (option) ▪ Chipcards
SICCT REQUEST ICC	80	12	FU	CQ	cond	cond	opt	man	Request for chipcard presentation and monitoring for time period.
SICCT GET STATUS	80	13	FU	CQ	cond	cond	man	man	Request parameter for the ▪ Cardterminal ▪ functional units ▪ ChipCard
SICCT EJECT ICC	80	15	FU	CQ	cond	cond	absent	man	Disable chipcard logically and / or electrically. Optionallly: mechanical operation.
SICCT INPUT	80	16	FU	CQ	cond	cond	opt	man	Query input data by the user interface functions of the cardterminal ▪ Keypad ▪ (Biometrical) Sensors
SICCT OUTPUT	80	17	FU	CQ	man	man	absent	Man	Send output data to the Cardterminal or a functional unit of the cardterminal. ▪ Display Message ▪ Printer Data / Message
SICCT PERFORM VERIFICATION	80	18	FU	CQ	man	man	opt	Man	Process Card Holder Verification. Perform a password / PIN entry operation, build a chipcard command and perform verification by an addressed chipcard.
SICCT MODIFY VERIFICATION DATA	80	19	FU	CQ	man	man	opt	man	Perform modify operation of Card Holder Verification Data ▪ Password / PIN

CardTerminal Basic Command	CLA Code (hex)	INS Code (hex)	P1	P2	Lc	Cmd Data	Le	Brief Description	
SICCT SELECT CT MODE	80	20	FU	CQ	cond	opt	opt	man	Select Operation / Command Set Mode ▪ BCS Mode ▪ SICCT Mode
SICCT COMFORT_ AUTHENTICATION	80	21	FU	CQ	opt	opt	opt	opt	Support command for authentication. Learns and stores an authentication dataset with ▪ authentization data ▪ and Serialnumber (ICCSN).
SICCT COMFORT_ ENROLL	80	22	FU	CQ	opt	opt	opt	opt	Support command for authentication. Learns and stores an authentication dataset with ▪ authentization data and ▪ Serialnumber (ICCSN).
SICCT SET STATUS	80	23	FU	CQ	man	man	absent	man	Set parameter (Data Object) for the ▪ cardterminal ▪ functional units. ▪ chipcards.
SICCT DOWNLOAD INIT	80	24	FU	CQ	cond	cond	man	man	Start of FW download
SICCT DOWNLOAD DATA	80	25	FU	CQ	man	man	man	man	Data transportation during FW download
SICCT DOWNLOAD FINISH	80	26	FU	CQ	cond	cond	man	man	Manifestation and completion of a FW download
SICCT CONTROLCOMMAND	80	27	FU	CQ	man	man	absent	man	Abort or termination of SICCT command.
SICCT INIT CT SESSION	80	28	FU	CQ	man	man	man	man	Init and open a Cardterminal .
SICCT CLOSE CT SSESSION	80	29	FU	CQ	man	man	absent	man	Close a Cardterminal Session.
FU = Functional Unit									
CQ = Command Qualifier									
cond = conditional									
opt = optional									
man = mandatory									

Tabelle : Overview of the SICCT Command Set

CardTerminal Manufacturer Data Object – 5.5.10.6

Korrektur (15.02.2008): 5.5.10.6 - *DD - Discretionary Data (112 Bytes)*

CardTerminalManufacturer Data Object (CTM DO)				
TAG	'46'	One byte tag according MCT-Specifications: CardTerminalManufacturer Data Object		
		Tag coding according ASN.1 BER see 5.5.10.3		
		BER-Coding : Application context, primitive, Tag-Number = 82 ('52')		
LEN	LEN coding see 5.5.10.3			
	one byte coding - LEN in the range of : 0 <= LEN <= 127			
	'0F' ... '7F'	15 <= LEN <= 127	One byte coding	
VALUE	Cardterminal pre-issuing data			
	CTM	CTT	CTSV	[Discretionary Data]
	man	man	Man	opt
	5 Byte	5 Byte	5 Byte	0 =< LEN <= 112 Bytes
	Cardterminal Manufacturer	SICCT Version	Cardterminal Software Version	Discretionary Data
	RID provided	SICCT specification provided	Vendor provided	Vendor provided

Data		Len		Description				
CTM	Cardterminal Manufacturer	5	man	5 Byte ASCII String- padded with Space ('20')				
				Unique Manufacturer Coding value according the RID German National Registration Authority				
				2 byte Country Code according ISO 3166		3 byte Manufacturer-Acronym.		
				Germany				
				'44'	'45'	'20'	'20'	'20'
CTT	SICCT Cardterminal Version	5	man	5 Byte ASCII String- padded with Space ('20')				
				SICCT Specification Version				
				SICCT Major Number	SICCT Major Number	SICCT Minor Number	SICCT Minor Number	Release Number / Character or Padding
				'30'	'31'	'32'	'30'	'20'
CTSV	Cardterminal Software Version	5	man	5 Byte ASCII String- padded with Space ('20')				
				Major Number	Major Number	Minor Number	Minor Number	Release Number or Character
				'30'	'31'	'30'	'30'	'20'
DD	Discretionary Data	0 ... 112	opt	vendor proprietary or domain specific format				

Functional Unit Name Data Object - 5.5.10.11

Korrektur (15.02.2008): 5.5.10.11 - *Längenangaben der Datenobjekte*
Motivation: An empty DO shall clear the Friendly Name in any case.

<table>
<tr><th colspan="5">Functional Unit Name Data Object (FU NAME DO)</th></tr>
<tr><td rowspan="3">TAG</td><td rowspan="3">'A1'</td><td colspan="3">One byte tag according SICCT-Specifications: Functional Unit Name Data Object</td></tr>
<tr><td colspan="3">Tag coding according ASN.1 BER see 5.5.10.3</td></tr>
<tr><td colspan="3">BER-Coding : Context specific, constructed,, Tag-Number = '01'</td></tr>
<tr><td rowspan="3">LEN</td><td colspan="4">LEN coding see 5.5.10.3</td></tr>
<tr><td colspan="4">One byte coding - LEN in the range of : 0 <= LEN <= 34</td></tr>
<tr><td>'00' ... '22'</td><td colspan="2">0 <= LEN <= 34</td><td>One byte coding</td></tr>
<tr><td rowspan="4">VALUE</td><td colspan="4">Friendly Name</td></tr>
<tr><td rowspan="3">'13'</td><td>'00' <= L <= '20'</td><td>Printable String, ASN.1 Coding</td></tr>
<tr><td rowspan="2">0 < = L < = 32</td><td>Friendly Name : Up to 32 characters</td></tr>
<tr><td>See 5.5.9.2</td></tr>
<tr><td colspan="5">Note: LEN == '00' or '02' means an empty Friendly Name (with Tag == '13' and L='00') in order to delete / erase a Friendly Name.</td></tr>
</table>

SICCT Message-To-Be-Displayed Data Object - 5.5.10.21

Korrektur (15.02.2008): 5.5.10.21 – Message coded as OCTETSTRING

<table>
<tr><th colspan="6">SICCT Message-To-Be-Displayed Data Object (SMTBD DO)</th></tr>
<tr><td rowspan="3">TAG</td><td rowspan="3">'A0'</td><td colspan="4">One byte tag according SICCT-Specifications: SICCT Message-To-Be-Displayed</td></tr>
<tr><td colspan="4">Tag coding according ASN.1 BER see 5.5.10.3</td></tr>
<tr><td colspan="4">BER-Coding : Context specific, constructed, Tag-Number = 0 ('00')</td></tr>
<tr><td rowspan="4">LEN</td><td colspan="5">LEN coding see 5.5.10.3</td></tr>
<tr><td colspan="5">one or two byte coding - LEN in the range of : 0 <= LEN <= 255</td></tr>
<tr><td colspan="2">'00' ... '7F'</td><td colspan="2">0 <= LEN <= 127</td><td>One byte coding</td></tr>
<tr><td>'81'</td><td>'80' ...'FF'</td><td colspan="2">128 <= LEN <= 255</td><td>Two byte coding</td></tr>
<tr><td rowspan="6">VALUE</td><td colspan="5">One Character Set DO and corresponding Message (OCTETSTRING DO)</td></tr>
<tr><td colspan="3">Character Set Data Object</td><td colspan="2">see 5.5.10.20</td></tr>
<tr><td rowspan="4">'04'</td><td colspan="4">The actual supported length depends on the capabilities of the selected FU of type 'display' . At minimum 32 ('20') characters according a two line display with 16 characters each.</td></tr>
<tr><td rowspan="3">'00' <= L <= '7F'</td><td colspan="3">ASN.1 coded OCTETSTRING (Universal 4)</td></tr>
<tr><td colspan="3">0 <= L <= 127</td></tr>
<tr><td colspan="3">Byte Sequence formatted according the selected character set
giving the message to be displayed.</td></tr>
</table>

Reduced / Card Terminal Status Data Object - 5.5.10.13

Korrektur (16.07.2008) – 5.5.10.13 Replaced INTEGER (Universal 2) Data Object(s) by OCTETSTRING (Universal 4)

<table>
<tr><td colspan="10">Reduced / Card Terminal Status Data Object (CTS DO)</td></tr>
<tr><td rowspan="3">TAG</td><td rowspan="3">'63'</td><td colspan="8">One byte tag according SICCT-Specifications:</td></tr>
<tr><td colspan="8">Tag coding according ASN.1 BER see 5.5.10.3.</td></tr>
<tr><td colspan="8">BER-Coding : Application context, constructed, Tag-Number = 3 ('03')</td></tr>
<tr><td rowspan="6">LEN</td><td colspan="9">LEN coding see 5.5.10.3.</td></tr>
<tr><td colspan="9">one or two bytes coding - LEN in the range of : 0 <= LEN <= 255</td></tr>
<tr><td colspan="5">'00' ... '7F'</td><td colspan="2">0 <= LEN <= 127</td><td colspan="2">One byte coding</td></tr>
<tr><td>'81'</td><td colspan="4">'80' ...'FF'</td><td colspan="2">128 <= LEN <= 255</td><td colspan="2">Two byte coding</td></tr>
<tr><td rowspan="2">’82’</td><td>'01'</td><td colspan="3">'00' ...'FF'</td><td colspan="2" rowspan="2">256 <= LEN <= 512</td><td colspan="2" rowspan="2">Two byte coding</td></tr>
<tr><td>’02’</td><td colspan="3">’00’</td></tr>
<tr><td colspan="10"></td></tr>
<tr><td rowspan="10">VALUE</td><td colspan="9">Cardterminal Status Information</td></tr>
<tr><td>Contained in complete DO</td><td>Contained in Reduced DO</td><td colspan="7"></td></tr>
<tr><td>✔</td><td>-</td><td colspan="6">Functional Unit Data Object</td><td>See 5.5.10.8.</td></tr>
<tr><td>✔</td><td>✔</td><td colspan="6">ICC Status Data Object</td><td>See 5.5.10.7.</td></tr>
<tr><td>[✔]</td><td>-</td><td colspan="6">optional - if present: RFID Antenna Status Data Object</td><td>See 5.5.10.14.</td></tr>
<tr><td>[✔]</td><td>[✔]</td><td colspan="6">optional - if present: RFID Token Status Data Object</td><td>See 5.5.10.12.</td></tr>
<tr><td rowspan="3">✔</td><td rowspan="3">[✔]</td><td colspan="7">Maximum Length of SICCT Commands – and Response APDUs[1]</td></tr>
<tr><td rowspan="2">'04'</td><td>'01'</td><td>'xx'</td><td colspan="3" rowspan="2">ASN.1 BER Coding OCTETSTRING (UNIVERSAL 4): <HB> <LB></td></tr>
<tr><td>'02'</td><td>'yyxx'</td></tr>
</table>

Command-To-Perform Data Object - 5.5.10.23

Korrektur (26.11.2008) – 5.5.10.23 Added Control Byte – Options for SICCT- MODIFY VERIFICATION DATA - In case b4..b3 code ‘01’ then b8..b5 code the (minimal) length of the new (2nd) PIN. [2]

<table>
<tr><td colspan="8">Command-To-Perform Data Object (CMD DO)</td></tr>
<tr><td rowspan="3">TAG</td><td rowspan="3">'52'</td><td colspan="6">One byte tag according MCT-Specifications: Command To Perform</td></tr>
<tr><td colspan="6">Tag coding according ASN.1 BER see</td></tr>
<tr><td colspan="6">BER-Coding : Application context, primitive, Tag-Number = 18 ('12')</td></tr>
<tr><td rowspan="4">LEN</td><td colspan="8">LEN coding see</td></tr>
<tr><td colspan="8">one or two byte coding - LEN in the range of : 0 <= LEN <= 255</td></tr>
<tr><td colspan="3">'00' ... '7F'</td><td colspan="2">0 <= LEN <= 127</td><td colspan="2">One byte coding</td></tr>
<tr><td>'81'</td><td colspan="2">'01' ...'FF'</td><td colspan="2">128 <= LEN <= 255</td><td colspan="2">Two byte coding</td></tr>
<tr><td rowspan="8">VALUE</td><td colspan="8">Command-to-perform</td></tr>
<tr><td colspan="8">Command-to-perform is a byte string containing the concatenation of
control byte || insertion position(s) || CC APDU</td></tr>
<tr><td rowspan="5">Control Byte</td><td colspan="7">Control Byte for user authentication</td></tr>
<tr><td>‘x0’</td><td colspan="6">BCD coded PIN / password with <x> digits or characters</td></tr>
<tr><td>‘x1</td><td colspan="6">ASCII coded PIN / password with <x> digits or characters</td></tr>
<tr><td>‘x2’</td><td colspan="6">Format-2 PIN –Block coded PIN / password with <x> digits or characters</td></tr>
<tr><td></td><td colspan="4">SICCT PERFORM VERIFICATION</td><td colspan="2">Note: This command shall ignore b4..b3 within the Control Byte.</td></tr>
</table>

[1] The maximum size is vendor sprecific.

[2] This extension meets an enhancement suggested by [gemSpec_KT].

<table>
<tr><td colspan="6">Command-To-Perform Data Object (CMD DO)</td></tr>
<tr><td rowspan="11"></td><td rowspan="6"></td><td></td><td colspan="2">SICCT MODIFY VERIFICATION DATA</td><td>Note: This command resumes from b4..b3 that the Control Byte specifies the settings for the 2nd PIN. In this case the 1st PIN's settings are of same PIN-type but with variable length.</td></tr>
<tr><td>'x4'</td><td colspan="3">BCD coded PIN / password with minimum <x> digits or characters for the new (2nd) PIN.</td></tr>
<tr><td>'x5'</td><td colspan="3">ASCII coded PIN / password with minimum <x> digits or characters for the new (2nd) PIN.</td></tr>
<tr><td>'x6'</td><td colspan="3">Format-2 PIN –Block coded PIN / password with minimum <x> digits or characters for the new (2nd) PIN.</td></tr>
<tr><td>'FF'</td><td colspan="3">In case of biometric identification</td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td rowspan="5">1st Insertion Position Byte</td><td rowspan="5">'06' ... 'FF'</td><td colspan="3">Mandatory Field - Insertion Position for the (1st) PIN</td></tr>
<tr><td>SICCT PERFORM VERIFICATION</td><td>Mandatory Field - Insertion position for the PIN</td></tr>
<tr><td>SICCT MODIFY VERIFICATION DATA</td><td>Mandatory Field - Insertion position for the 1st PIN</td></tr>
<tr><td colspan="2">The insertion position for the first PIN digit / character within the CC APDU</td></tr>
<tr><td colspan="2">The insertion position counts from one starting at 'CLA'. Typically the 1st insertion position is 'typically equal or greater than 06' (after a five byte APDU: CLA, Len, P1, P2, Lc).</td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td rowspan="6">[2nd Insertion Position Byte]</td><td rowspan="6">'06' ... 'FF'</td><td colspan="3">Conditional Field - Insertion Position for the 2nd PIN</td></tr>
<tr><td>SICCT PERFORM VERIFICATION</td><td>Note: This field must not be transmitted. for this command.</td></tr>
<tr><td rowspan="2">SICCT MODIFY VERIFICATION DATA</td><td>Conditional Field - Insertion position for the 2nd PIN</td></tr>
<tr><td>Note: This field has to be transmitted. for this command.</td></tr>
<tr><td colspan="2">The insertion position for the first PIN digit / character within the CC APDU</td></tr>
<tr><td colspan="2">The insertion position counts from one starting at 'CLA'. Typically the 2nd insertion position is greater than the 1st insertion position (after a five byte APDU: CLA, Len, P1, P2, Lc).</td></tr>
<tr><td rowspan="20">Chipcard APDU</td><td colspan="5">APDU to be sent to the Chipcard</td></tr>
<tr><td>CLA</td><td>INS</td><td>P1</td><td>P2</td><td>Lc</td><td>'x' bytes PIN / Password</td></tr>
<tr><td colspan="6">Valid INS-Bytes</td></tr>
<tr><td>CLA</td><td>INS</td><td colspan="4">Other INS Bytes rejected by the SICCT terminal</td></tr>
<tr><td rowspan="16"></td><td rowspan="5">'20'</td><td colspan="4">VERIFY</td></tr>
<tr><td colspan="4">Verification data reference acc. to ISO 7816-4, table 65 [STD8]</td></tr>
<tr><td colspan="4">VERIFY CHV</td></tr>
<tr><td colspan="4">Verification data reference acc. to GSM 11.11</td></tr>
<tr><td colspan="4">Verification data reference acc. to prEN 726-3</td></tr>
<tr><td rowspan="5">'24'</td><td colspan="4">CHANGE REF. DATA</td></tr>
<tr><td colspan="4">Change reference data acc. to ISO 7816-4, table 65 [STD8]</td></tr>
<tr><td colspan="4">CHANGE CHV</td></tr>
<tr><td colspan="4">Change Cardholder Verification according GSM 11.11</td></tr>
<tr><td colspan="4">Change Cardholder Verification according prEN 726-3</td></tr>
<tr><td rowspan="4">'26'</td><td colspan="4">DISABLE CHV</td></tr>
<tr><td colspan="4">Disable Cardholder Verification according ISO 7816-8</td></tr>
<tr><td colspan="4">Disable Cardholder Verification according GSM 11.11</td></tr>
<tr><td colspan="4">Disable Cardholder Verification according prEN 726-3</td></tr>
<tr><td rowspan="2">'28'</td><td colspan="4">ENABLE CHV</td></tr>
<tr><td colspan="4">Enable Cardholder Verification according ISO 7816-8</td></tr>
</table>

Command-To-Perform Data Object (CMD DO)						
				Enable Cardholder Verification according GSM 11.11		
				Enable Cardholder Verification according prEN 726-3		
			'2A'	**PERFORM SECURITY OPERATION**		
				P1	P2	according ISO 7816-8, 5.9. table 13
				'82'	'80'	PSO (Encipher) operation according ISO 7816-8 in order to support VERSA-concept (VERSA : "distributed signature workplaces").
				'84'		
				'86'		
			'2C'	**RESET RETRY COUNTER**		
				RESET RETRY COUNTER data acc. to ISO 7816-4, table 65 [STD8]		
				UNBLOCK CHV		
				Verification data reference acc. to GSM 11.11		
				Verification data reference acc. to prEN 726-3		

Control Byte Coding for user authentication					
Control Byte	Coding for PIN / Password				
	b8…b5	Length of PIN to be presented.			
		0000		'0'	Variable length PIN / password
					If length = 0 (value for variable length), then pressing of validation key is required.
		0001 ... 1100		'1' … '12'	Number of PIN digits or characters
					Minimal 1 digit / character
					Maximal 12 digits / characters
	b4..b3	0	0	'0'	default
		0	1	'1'	SICCT PERFORM VERIFICATION This command shall ignore b4..b3 within the Control Byte.
					SICCT MODIFY VERIFICATION DATA: In this case b8…b5 code the minimal length of the new (2nd) PIN.
		1	0	'2' ... '3'	RFU
		1	1		
	b2 .. b1	0	0	BCD coded PIN	
		0	1	T.50 coding according International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) - Information technology - 7-bit coded character set for information interchange, see table below	
				characters according to T.50 according T.50 with b8=0 (i.e. digit 0 is coded '30', digit 1 is coded '31' etc.)	
		1	0	Format 2 PIN Block according to ISO 9564-1, see table below	
		1	1	RFU	
	Coding for Biometric identification				
	b8 .. b1	11111111		'FF'	In case of biometric identification

[4] Suppress internal ('Abort') message.

Sequence Number Data Object - 5.5.10.24

Korrektur (18.02.2008) – 5.5.10.24 - SICCT CONTROL COMMAND
Korrektur (16.07.2008) – 5.5.10.24 Replaced INTEGER (Universal 2) Data Object by OCTETSTRING (Universal 4)

<table>
<tr><th colspan="9">Sequence Number Data Object (SEQNO DO)</th></tr>
<tr><td rowspan="3">TAG</td><td colspan="2" rowspan="3">'68'</td><td colspan="6">One byte tag according SICCT-Specifications:</td></tr>
<tr><td colspan="6">Tag coding according ASN.1 BER see 5.5.10.3.</td></tr>
<tr><td colspan="6">BER-Coding : Application context, constructed, Tag-Number = 8 ('08')</td></tr>
<tr><td rowspan="15">LEN</td><td colspan="8">LEN coding 5.5.10.3.</td></tr>
<tr><td colspan="8">one byte coding - LEN in the range of : 4 <= LEN <= 8</td></tr>
<tr><td colspan="3" rowspan="3">'04' <= LEN <= '08'</td><td colspan="2" rowspan="3">LEN = 4 .. 8</td><td colspan="3">One byte coding</td></tr>
<tr><td colspan="3">DO in Request: 4 Bytes</td></tr>
<tr><td colspan="3">DO in Response: 8 Bytes</td></tr>
<tr><td colspan="5">Command Sequence Number</td><td colspan="3">A distinct two byte value</td></tr>
<tr><td rowspan="2">'04'</td><td rowspan="2">'L = '02'</td><td><HB></td><td><LB></td><td colspan="3">0000' <= Sequence Number <= 'FCFF'</td><td rowspan="11">ASN.1
Universal
4
Coding</td></tr>
<tr><td>'00' ... 'FF'</td><td>'00' ... 'FF'</td><td colspan="3">Note:
'FD00' <= Sequence Number <= 'FFFF'
signal Events sent by the SICCT to the host entity.</td></tr>
<tr><td colspan="4" rowspan="2">[Command Sequence Status Word]</td><td colspan="3">Presence – Conditional</td></tr>
<tr><td colspan="3">For requests
not. present.</td></tr>
<tr><td rowspan="6">['04']</td><td rowspan="6">['00' <= L <= '02']</td><td>[<HB>]</td><td>[<LB>]</td><td colspan="3">For responses:
A distinct two byte value set by the CT for the response APDU.</td></tr>
<tr><td>'90'</td><td>'00'</td><td colspan="3">Sequence Number found:
Command queued and not in processing state</td></tr>
<tr><td>'62'</td><td>'0x'</td><td colspan="3">Sequence Number found:
command in processing state '0x'</td></tr>
<tr><td>'64'</td><td>'0x'</td><td colspan="3">Sequence Number found:
processing state found at stage '0x' - state cannot be changed.</td></tr>
<tr><td>'6F'</td><td>'00'</td><td colspan="3">Sequence Number not found:
no information given on processing state</td></tr>
</table>

Use Cases for Sequence Number Data Object		
SICCT Command	Description	Reference
SICCT CONTROL COMMAND	Query command execution state for given Sequence No DO	see 5.9
	Terminate command execution for given Sequence No DO	

Download Parameter Data Object - 5.5.10.25

Korrektur (18.02.2008) – 5.5.10.25 Korrektur Beschreibung Waiting Time and LEN
Korrektur (16.07.2008) – 5.5.10.25 Replaced INTEGER (Universal 2) Data Object by OCTETSTRING (Universal 4)

<table>
<tr><th colspan="8">Download Parameter Data Object (DLPARAM DO)</th></tr>
<tr><td rowspan="3">TAG</td><td colspan="2" rowspan="3">'73'</td><td colspan="5">One byte tag according ISO 7816-6: Discretionary Data Objects</td></tr>
<tr><td colspan="5">Tag coding according ASN.1 BER see 5.5.10.3</td></tr>
<tr><td colspan="5">BER-Coding : Application context, constructed, Tag-Number = 19 ('13')</td></tr>
<tr><td rowspan="3">LEN</td><td colspan="7">LEN coding see 5.5.10.3</td></tr>
<tr><td colspan="7">one byte coding - LEN in the range of : 6 <= LEN <= 8</td></tr>
<tr><td colspan="2">'06' ... '08'</td><td colspan="3">6 <= LEN <= 8</td><td colspan="2">One byte coding</td></tr>
<tr><td rowspan="6">VALUE</td><td colspan="7">Download Parameter</td></tr>
<tr><td colspan="7">Sequence of TLV-Objects</td></tr>
<tr><td rowspan="2">'04'</td><td>'01'</td><td>'xx'</td><td><LB></td><td rowspan="4">ASN.1 BER Coding OCTETSTRING (UNIVERSAL 4)</td><td colspan="2" rowspan="2">Timeout - Waiting Time
Waiting time in seconds how long the device needs to process the last or next download data object.</td></tr>
<tr><td>'02'</td><td>'yyxx'</td><td><HB> <LB></td></tr>
<tr><td rowspan="2">'04'</td><td>'01'</td><td>'xx'</td><td><LB></td><td colspan="2" rowspan="2">Maximum Length of Download Data Object as number of bytes.</td></tr>
<tr><td>'02'</td><td>'yyxx'</td><td><HB> <LB></td></tr>
</table>

Download Termination Data Object - 5.5.10.27

Korrektur (13.03.2008 / 14.03.2008) – 5.5.10.27 Ergänzungen – Timeout und Finalisation Condition
Korrektur (16.07.2008) – 5.5.10.27 Replaced INTEGER (Universal 2) Data Object by OCTETSTRING (Universal 4)

Das Download Termination Data Object (DLTERM DO) enthält einzelne Parameter zum Abschluss des Downloads. Das Datenobjekt gibt an, wieviel Zeit vom Terminal zum Abschluss des Downloads (ggf. Für die interne Verarbeitung) benötigt wird, und unter welchen Bedingungen die Download Operation abgeschlossen wird.

<table>
<tr><td colspan="10">Download Termination Data Object (DLTERM DO)</td></tr>
<tr><td rowspan="3">TAG</td><td colspan="2" rowspan="3">'73'</td><td colspan="7">One byte tag according ISO 7816-6: Discretionary Data Objects</td></tr>
<tr><td colspan="7">Tag coding according ASN.1 BER see 5.5.10.3</td></tr>
<tr><td colspan="7">BER-Coding : Application context, constructed, Tag-Number = 19 ('13')</td></tr>
<tr><td rowspan="3">LEN</td><td colspan="9">LEN coding see 5.5.10.3</td></tr>
<tr><td colspan="9">one byte coding - LEN in the range of : Len = 5 … 8</td></tr>
<tr><td colspan="2">‘05’ … '08’</td><td colspan="3">5 <= LEN <= 8</td><td colspan="4">One byte coding</td></tr>
<tr><td rowspan="6">VALUE</td><td colspan="9">Timeout</td></tr>
<tr><td rowspan="3">'04'</td><td>‘00’</td><td colspan="2">Empty DO</td><td colspan="4">No time indication mandatory in case of Finalisation Condition b3=1 or b4=1</td></tr>
<tr><td>'01'</td><td>‘xx’</td><td colspan="2" rowspan="2">Timeout coded as ASN.1 BER Coding OCTETSTRING (UNIVERSAL 4): [<HB>] <LB></td><td colspan="4" rowspan="2">Extended Timeout
Timeout in seconds how long the device needs to process last download data object or finish the download process.</td></tr>
<tr><td>'02'</td><td>'yyxx'</td></tr>
<tr><td colspan="9">Finalisation Condition</td></tr>
<tr><td rowspan="6">'04'</td><td rowspan="3">'01'</td><td rowspan="3">‘xx’</td><td colspan="6">At least one condition or (bit)combination shall be indicated by the terminal.</td></tr>
<tr><td colspan="6">Coded as ASN.1 BER Coding OCTETSTRING (UNIVERSAL 4): [<HB>] <LB></td></tr>
<tr><td>b1 = ‘1’</td><td colspan="5">A SICCT CLOSE CT SESSION (disconnection) is needed / expected by the terminal to end the download operation after the timeout period.</td></tr>
<tr><td>b2 = ‘1’</td><td colspan="5">The terminal needs a reboot / restart in order to end the download operation. Therefore is SICCT RESET CT necessary after the timeout period.</td></tr>
<tr><td rowspan="4">'02'</td><td rowspan="4">'xxyy'</td><td>b3 = ‘1’</td><td colspan="5">Terminal performs disconnection, reboot / restart automatically at the end of processing SICCT DOWNLOAD FINISH in order to end the download operation.
Note: Do not set this b3 in combination with b1 and/or b2.
Note: A new LAN connection must be etablished, if needed.</td></tr>
<tr><td>b4 = ‘1’</td><td colspan="5">He terminal needs manual assistance in order to end the download operation or to reboot / restart.
Note: A new LAN connection must be etablished, if needed.</td></tr>
<tr><td>‘00’</td><td colspan="5">Regular operation after Response</td></tr>
<tr><td>‘xy’</td><td colspan="5">All other values RFU</td></tr>
</table>

Standard-PIN-Prompt / Max. PIN-Prompt - Länge- 5.6.1

5.6.1 Handling von Display Messages im SICCT-Mode

Korrektur (13.08.2008): Die max. Länge des darzustellenden PIN-Prompts ist 10 Zeichen.
Motivation: Das Trennzeichen '0x0F' zählt nicht zur PIN-Prompt-Länge.

Der 8. Aufzählpunkt unter 5.6.1 soll nunmehr lauten:

- " Der Aufbau von Display-Nachrichten in den Datenobjekten (APPL DO bzw. SMTB DO) für PIN-Eingaben erfolgt für das Value-Feld nach folgendem Schema. Eine übergebene Text-Nachrichtenstruktur für PIN-Eingabe darf maximal 50 Zeichen (inkl. Trennzeichen) umfassen und unterteilt sich in
  - **<Message** (max. 40 Zeichen)**> <Trennzeichen '0F'> <PIN-Prompt** (max. 10 Zeichen)**>**"

Korrektur (15.02.2008): Ergänzung einer Definition des Standard-PIN-Prompts
Motivation: Die Definition des Standard-PIN-Prompts fehlt in [SICCT_120].

Der 11. Aufzählpunkt unter 5.6.1 soll nunmehr lauten:

- "Erfolgt für einen <PIN-Prompt> in einer Nachricht keine Definition, so wird der Standard-PIN-Prompt, bestehend aus dem Trennzeichen '0F', dem String "INPUT:" und eines abschliessenden Space-Zeichens, verwendet. Standdard-PIN-Prompt: <Trennzeichen '0F'> <"INPUT"> <":"><space>"

Korrektur (13.08.2008): Die max. Länge des darzustellenden PIN-Prompts ist 10 Zeichen.
Motivation: Das Trennzeichen '0x0F' zählt nicht zur PIN-Prompt-Länge.

Der 12. Aufzählpunkt unter 5.6.1 soll nunmehr lauten:

- "Für die Ausgabe von Display-Nachrichten sollen folgende minimal zu unterstützende Länge gelten
  - von 48 Zeichen für SICCT OUTPUT - Nachrichten.
  - von 50 (40 +10 Zeichen) für PIN-Eingabe-Nachrichten (inklusive 10 Zeichen PINPrompt exklusive des Trennzeichens '0F')"

Handling von Tastatureingaben (Keypad-Entries) im SICCT-Mode - 5.7

Korrektur (13.03.2008): 5.7 - Ergänzung – Secure PIN Entry

- Secure PIN Entry - Während der Ausführung der SICCT-Kommandos SICCT PERFORM VERIFICATION und SICCT MODIFY VERIFICATION DATA werden die Zeichen einer PIN-Eingabe am Display mit jeweils einem Ersatzzeichen (üblicherweise Sternchen) pro eingegebener Ziffer angezeigt. Zusätzlich wird dem Benutzer der sichere Eingabe-Modus ("Secure PIN Entry Mode") signalisiert. Es ist nicht möglich, die PIN-Eingabezeichen als Klartext im (optionalen) Terminal-Display darzustellen.

Command SICCT INIT CT SESSION - 5.10

COMMAND SICCT INIT CT SESSION

Korrektur (15.02.2008) - 5.10 - *Rechtschreibfehler*

Je nachdem ob die Login-Informationen eine Benutzerkennung und Authentifizierungsdaten (Password-Phrase) enthält, differenziert das SICCT Terminal den Zugriff durch

- Eine Administrator-Rolle (CT ADMIN Session)
- Eine (möglw. anonyme) Control-Rolle (CT CONTROL Session).

ANWENDUNGSBEDINGUNGEN

Korrektur (15.02.2008): 5.10.2 - *Der Aufruf von SICCT INIT CT SESSION kann auch für eine ADMIN Session erfolgen.*

SICCT INIT CT SESSION							
CT Mode		Conditions					
		CT ADMIN Session	CT CONTROL Session	Abortable by SICCT CONTROL COMMAND			
					Stage		
BCS	SICCT				1	2	3
no	✓	✓	✓	No	-	-	-

Status-Codes
Ergänzung (15.02.2008): 5.10.6

SW1-SW2	Addressed Functional Unit P1	Specification	Meaning
'6400'	CT	Error - Opening CT Session was not successful	Error
			Invalid Username
'6403'			Invalid Password
			Invalid Session-ID. DO Session ID has to be empty.
'6700'		Wrong (command) length	Wrong Lc: Inconsistent command body or no Command Data field supported.
'6900'		Command not allowed.	Open CT Session found.
'6A00'		Wrong parameters P1, P2	▪ P1 addresses invalid Functional Unit. ▪ Invalid FUI DO referenced by P1 (command data) ▪ P2 specifies not supported value
'6A80'		Invalid Data Object	▪ Invalid CT SESS DO
		Incorrect parameters in the command data field	▪ Invalid FUI DO
'6C00'		Wrong Length Le	Wrong Le:
'9000'		Opening CT Session was successful	The specified CT session has been opened.

Command SICCT CLOSE CT SESSION - 5.11

Korrektur (15.02.2008):

FUNKTION

Korrektur (15.02.2008) - 5.11.1 - *Rechtschreibfehler*

Fehlerfreier Betrieb
Der Aufrufer übermittelt mit dem SICCT CLOSE CT SESSION Kommando ein Datenobjekt CT Session Data Object.

Korrektur (15.02.2008) – Ergänzung

Nach der erfolgreichen Kommandoausführung sind alle Functional Units im Reset-Zustand bzw. deaktiviert, und das Terminal unterhält keine offene CT Session.

ANWENDUNGSBEDINGUNGEN

Korrektur (15.02.2008) – 5.11.2 - *Ergänzung*

Normalfall - Beenden einer CT-Session (ohne Administratorberechtigung)
Im Fall eines User-Zugriffs muss die Session-ID im CT SESS DO korrekt zum Wert der offenen CT Session angegeben sein. Im CT SESS DO können optional auch Username und Passwort-Phrase angegeben sein. Sofern diese angegeben wurden, muss das Terminals neben der Session-ID die Zugangsberechtigung prüfen, und bei fehlender Übereinstimmung bzw. Berechtigung die Ausführung des Kommandos abbrechen.

COMMAND STRUCTURE

Korrektur (15.02.2008) – 5.11.3 - *Tabelle Data - Die Übergabe eines CT SESS DOs mit Angabe von Username und Passwort soll immer möglich sein.*

Motivation: Ergänzung - Ermöglichung des Schliessens einer CT Session für den Admin-Zugriff, ggf. ohne Übergabe der Session-Id. Für User- oder Admin-Zugriff können neben der Session-ID Username und Passwort übergeben werden.

<table>
<tr><td rowspan="8">Data</td><td colspan="7">Command Data</td></tr>
<tr><td colspan="7">In case of Direct Coding of 'P1' (mandatory)</td></tr>
<tr><td rowspan="6">CT SESS DO</td><td colspan="6">Cardterminal Session Data Object</td></tr>
<tr><td>'69'</td><td>L</td><td colspan="4">Value</td></tr>
<tr><td rowspan="4"></td><td>'13'</td><td>Len</td><td><0 ... 12 Byte></td><td>Username</td></tr>
<tr><td>'13'</td><td>Len</td><td><0 ... 12 Byte></td><td>Password</td></tr>
<tr><td rowspan="2">'13'</td><td>Len</td><td><0 ... 12 Byte></td><td>Session ID</td></tr>
<tr><td>‘00’</td><td>Absent</td><td>Admin: Close all sessions.</td></tr>
<tr><td colspan="7">In case of Referenced Coding of 'P1'</td></tr>
</table>

	FUI DO	'84020000'	Functional Unit Index Data Object referencing the cardterminal.
	CT SESS DO	Cardterminal Session Data Object	
		Coding see above : Direct Coding.	

STATUS-CODES SW1-SW2

Ergänzung (15.02.2008): 5.11.6

SW1-SW2	Addressed Functional Unit	Specification	Meaning
	P1		
'6400	CT	Error - Closing CT Session was not successful	Error
			Invalid Username
			Invalid Password
'6403'			Invalid Session-ID
'6700'		Wrong (command) length	Wrong Lc: Inconsistent command body or no Command Data field supported.
'6900'		Command not allowed.	No open CT Session found.
'6A00'		Wrong parameters P1, P2	▪ P1 addresses invalid Functional Unit. ▪ Invalid FUI DO referenced by P1 (command data) ▪ P2 specifies not supported value
'6C00'		Wrong Length Le	Wrong Le:
'9000'		Closing CT Session was successful	The specified CT session has been closed.

Command SICCT RESET CT / ICC - 5.12.2

Korrektur (21.02.2008) – 5.12.2 – Editorischer Fehler beseitigt.

SICCT RESET CT							
CT Mode		Conditions					
		CT ADMIN Session	CT CONTROL Session	Abortable by SICCT CONTROL COMMAND			
BCS	SICCT				Stage		
					1	2	3
No	✓	✓	✓	no	-	-	-

Command SICCT REQUEST ICC -5.13.2

Korrektur (21.02.2008) – 5.13.2 – Editorischer Fehler beseitigt.

SICCT REQUEST ICC							
CT Mode		Conditions					
		CT ADMIN Session	CT CONTROL Session	Abortable by SICCT CONTROL COMMAND			
BCS	SICCT				Stage		
					1	2	3
no	✓	✓	✓	✓	✓	no	no

Command SICCT EJECT ICC - 5.14.2

Korrektur (21.02.2008) – 5.14.2 – Editorischer Fehler beseitigt.

SICCT EJECT ICC							
CT Mode		Conditions					
		CT ADMIN Session	CT CONTROL Session	Abortable by SICCT CONTROL COMMAND			
BCS	SICCT				Stage		
					1	2	3
no	✓	✓	✓	✓	no	no	✓

Command SICCT GET STATUS - 5.15

Korrektur (18.02.2008) – 5.15 – Fall Lc empty entfernt und extended Lc ergänzt
Korrektur (21.02.2008) – 5.15.2 – Editorischer Fehler beseitigt.
Korrektur (13.03.2008) – P2 – Textkorrektur/ Ergänzung FU KeyPad

P2	Command Qualifier: indicates requested Data Object		
	bit8 .. bit1	Referenced Coding	
		'FF'	Escape : Signal Referenced Coding of 'P2': Requested Data Object contained within Command Data Field: An empty Data Object (Tag and L=0) is given within the Command Data Field e.g. 'A1' '00' for FU NAME DO.
	bit8 .. bit1	Direct Coding	
		Data Objects served by all Functional Units	
		'A1'	Functional Unit Name Data Object
		In case P1 addresses the Cardterminal (CT):	
		'46'	CardTerminal Manufacturer Data Object
		'63'	CardTerminal Status Data Object
		'80'	ICC Status Data Object (all ICC Interfaces)
		'81'	Functional Unit Data Object
		In case P1 addresses an ICC , RFID-Slot	
		'80'	ICC Status Data Object (ICC Interface as addressed by 'P1')
		'66'	Interface Capabilities Data Object
		In case P1 addresses an RFID-Slot	
		'83'	RFID Token Status Data Object
		'66'	Interface Capabilities Data Object
		In case P1 addresses a Display FU	
		'85'	Character Set data Object
		'67'	Display Capabilities Data Object
		In case P1 addresses a RFID Antenna Unit	
		'64'	RFID Antenna Status Data Object
		In case P1 addresses a KeyPad FU	
		'6A'	Keypad Capabilities Data Object

Lc	Length of Command Data Nc		
	variable length	Length of Command Data Nc (no. of bytes contained in Data field)	
		Lc short '01' <= Lc <= 'FF	1 <= Nc <= 255
		Lc extended 3 Byte Coding'000000' <= Lc <= '00FFFF'	0 <= Nc <= 65535

SICCT GET STATUS							
CT Mode		Conditions					
		CT ADMIN Session	CT CONTROL Session	Abortable by SICCT CONTROL COMMAND			
BCS	SICCT				Stage		
					1	2	3
no	✓	✓	✓	No	no	no	no

Command SICCT INPUT - 5.17.2

Korrektur (21.02.2008) – 5.17.2 – Editorischer Fehler beseitigt.

SICCT INPUT							
CT Mode		Conditions					
		CT ADMIN Session	CT CONTROL Session	Abortable by SICCT CONTROL COMMAND			
BCS	SICCT				Stage		
					1	2	3
no	✓	✓	✓		✓	no	no

Command SICCT OUTPUT - 5.18.2

Korrektur (21.02.2008) – 5.18.2 – Editorischer Fehler beseitigt.
Korrektur (13.03.2008) – P2 – Textkorrektur: P2 == '70'

SICCT OUTPUT							
CT Mode		Conditions					
		CT ADMIN Session	CT CONTROL Session	Abortable by SICCT CONTROL COMMAND			
BCS	SICCT				Stage		
					1	2	3
no	✓	✓	✓		✓	no	no

P2	Command Qualifier:		
	bit8 .. bit1	'00'	Default value = do not care
		In case P1 addresses a FU other than Display type.	
		'xx'	other values RFU
		In case P1 addresses a Display FU	
		'01'	Display the cardterminals' Idle Message
		'70'	Suppress internal display messages during command execution[4]
		'xx'	other values RFU

Command SICCT PERFORM VERIFICATION - 5.19.2

Korrektur (21.02.2008) – 5.19.2 – Editorischer Fehler beseitigt.

SICCT PERFORM VERIFICATION							
CT Mode		Conditions					
		CT ADMIN Session	CT CONTROL Session	Abortable by SICCT CONTROL COMMAND			
BCS	SICCT				Stage		
					1	2	3
no	✓	✓	✓		✓	no	No

Command SICCT MODIFY VERIFICATION DATA - 5.20.2

Korrektur (21.02.2008) – 5.20.2 – Editorischer Fehler beseitigt.
Ergänzung (15.12.2009) – Ergänzungen zur Interpretation der PIN-Längenangabe im CMD DO

SICCT MODIFY VERIFICATION DATA							
CT Mode		Conditions					
		CT ADMIN Session	CT CONTROL Session	Abortable by SICCT CONTROL COMMAND			
BCS	SICCT				Stage		
					1	2	3
no	✓	✓	✓		✓	no	no

Die Anwahl des PIN-Formats, eine APDU-Bytesequenz, die PIN-Länge sowie eine Einfügeposition (Insertion Position), werden dem Terminal durch ein übergebenes Command-To-Perform Data Object (CMD DO) vorgegeben. Zusätzlich bestimmt das CMD DO über das Control-Byte die Länge der einzugebenden PINs.

Wenn in den Bits b4...b3 des Control Bytes des CMD DO (s. 5.5.10.23) der Wert '0' (b4=0, b3=0) codiert ist, so wird in den Bits b8...b5 die exakte Länge der einzugebenden alten und neuen PIN vorgegeben. Dabei wird eine Länge von 0 als variable Eingabelänge interpretiert.

[4] Suppress internal (‘Abort’) message.

Wenn in den Bits b4...b3 des Control Bytes des CMD DO der Wert '1' (b4=0, b3=1) codiert ist, so wird in den Bits b8...b5 die Mindestlänge der einzugebenden neuen PIN vorgegeben. In diesem Fall gilt für die alte PIN eine variable Eingabelänge.

Das Terminal soll auch bei Format2PIN Block formatierten PINs die vom Control Byte vorgegebenen Längenangaben nutzen und keine zusätzlichen Beschränkungen bzgl. einer Mindestlänge (vgl. [SICCT_120#Seite 68] vornehmen.

Command SICCT CT DOWNLOAD INIT - 5.23.4

COMMAND STRUCTURE

Korrektur (18.02.2008) – 5.23.4 - Added missing case 'extended Le'
Korrektur (20.02.2008) – 5.23.4 – Absent Le' not allowed, Case1 and Case 2 eliminated.

SICCT Kommando	Kodierung C-APDU						
	CLA	INS	P1	P2	[Lc]	[Data]	Le
SICCT DOWNLOAD INIT	'80'	'24'	Functional Unit	Command Qualifier	[Length Command Data]	[Command Data]	Length Requested Data
	▪ CLA = Class ▪ INS = Instruction ▪ P1, P2 = Parameter 1 and 2 ▪ Lc = Length of command data field ▪ Le = Length of expected ▪ SW1, SW2 = Status Bytes				Case 2 (no cmd data, rsp data): no Lc, Le=1-256 Bytes		
					Case 4 (cmd data, rsp data): Lc=1-255 Bytes or extended Lc Le=1-256 Bytes or extended Le		

Le	Length of Requested Data Ne Return up to Ne bytes of requested information		
	variable length	Condition: Lc short Le short '01 <= Le <= 'FF'	1 <= Ne <= 255
		Condition: Lc short Le short Le = '00'	Ne = 256
		Condition: Lc absent Le extended '000001' <= Le <= '00FFFF'	1 <= Ne <= 65535
		Condition: Lc absent Le extended Le = '000000'	Ne = 65536
		Condition: Lc extended Le extended '0001' <= Le <= 'FFFF'	1 <= Ne <= 65535
		Condition: Lc extended Le extended Le = '0000'	Ne = 65536

Status-Codes SW1-SW2

Korrektur (20.02.2008) – 5.23.7 – Added cases / case descriptions

SW1-SW2	Addressed Functional Unit (FU) P1	Specification	Meaning
'6200'	CT	Warning - Download Session already started.	Download Session already started.
'6400'		Error	Command execution error: Error at Reset of Terminal / FUs.
'6501'		Memory Failure	Terminal internal error: Flash-Memory or memory capacity error
'6700'		Wrong (command) length parameter	Wrong Lc: Inconsistent command body or Command Data field length error.
'6900'		Command not allowed	▪ No open CT Session ▪ Access Rights not fulfilled (no Admin CT Session) ▪ Cardterminal busy, Download Session cannot start.
'6A00'		Wrong parameters P1, P2	▪ P1 addresses invalid Functional Unit. ▪ P2 specifies not supported value
'6C00'		Wrong (information) length parameter	Wrong Le: Le absent – not allowed.
'6F00'		Communication with CT not possible.	In case ▪ the terminal detected general protocol errors or ▪ the terminal detected errors within the CT Session or TLS connection.
'9000'		Command successful	Download Initialisation was successful. Cardterminal and all functional units successfully set to reset state.

Command SICCT CT DOWNLOAD DATA - 5.24.3

COMMAND STRUCTURE

Korrektur (18.02.2008) – 5.24.3 - *Added missing case 'extended Le'*
Korrektur (20.02.2008) – 5.24.3 – *Absent Le' not allowed, Case 3 has been eliminated.*

SICCT Kommando	Kodierung C-APDU						
	CLA	INS	P1	P2	Lc	Data	Le
SICCT DOWNLOAD DATA	'80'	'25'	Functional Unit	Command Qualifier	Length Command Data	Command Data	Length Requested Data
	▪ CLA = Class ▪ INS = Instruction ▪ P1, P2 = Parameter 1 and 2 ▪ Lc = Length of command data field ▪ Le = Length of expected ▪ SW1, SW2 = Status Bytes				Case 4 (cmd data, rsp data): Lc=1-255 Bytes or extended Lc Le=1-256 Bytes or extended Le		

Le	Length of Requested Data Ne Return up to Ne bytes of requested information		
	variable length	Condition: Lc short Le short '01 <= Le <= 'FF'	1 <= Ne <= 255
		Condition: Lc short Le short Le = '00'	Ne = 256
		Condition: Lc extended Le extended '0001' <= Le <= 'FFFF'	1 <= Ne <= 65535
		Condition: Lc extended Le Extended Le = '0000'	Ne = 65536

Status-Codes SW1-SW2

Korrektur (20.02.2008) – 5.24.6 – Added cases / case descriptions

SW1-SW2	Addressed Functional Unit (FU) P1	Specification	Meaning
'6400'	CT	Error	Command execution error.
'6501'		Memory Failure	Terminal internal error: Flash-Memory or memory capacity error
'6700'		Wrong (command) length parameter	Wrong Lc: Inconsistent command body or Command Data field length error.
'6900'		Command not allowed	▪ No pending Download Session.
'6A00'		Wrong parameters P1, P2	▪ P1 addresses invalid Functional Unit. ▪ P2 specifies not supported value
'6C00'		Wrong (information) length parameter	Wrong Le: Le absent – not allowed.

SW1-SW2	Addressed Functional Unit (FU) P1	Specification	Meaning
'6F00'		Communication with CT not possible.	In case ▪ the terminal detected general protocol errors or the terminal detected errors within the CT Session or TLS connection.
'9000'		Command successful	Transmission of Download Data Object was successful.

Command SICCT CT DOWNLOAD FINISH - 5.25.3

COMMAND STRUCTURE

Korrektur (18.02.2008) – 5.25.3 - Added missing case 'Lc'
Korrektur (20.02.2008) – 5.25.3 – Absent Le' not allowed, Case 1 and Case 3 have been eliminated.

SICCT Kommando	Kodierung C-APDU						
	CLA	INS	P1	P2	[Lc]	[Data]	Le
SICCT DOWNLOAD FINISH	'80'	'26'	Functional Unit	Command Qualifier	[Length Command Data]	[Length Command Data]	Length Requested Data
	▪ CLA = Class ▪ INS = Instruction ▪ P1, P2 = Parameter 1 and 2 ▪ Lc = Length of command data field ▪ Le = Length of expected ▪ SW1, SW2 = Status Bytes				Case 2 (no cmd data, rsp data): no Lc, Le=1-256 Bytes		
					Case 4 (cmd data, rsp data): Lc=1-255 Bytes or extended Lc Le=1-256 Bytes or extended Le		

Lc	Length of Command Data Nc		
	Empty	Lc absent	no Command Data provided; Nc = 0
	Length of Command Data Nc		
	variable length	Length of Command Data Nc (no. of bytes contained in Data field)	
		Lc short '01' <= Lc <= 'FF	1 <= Nc <= 255
		Lc extended 3 Byte Coding'000000' <= Lc <= '00FFFF'	0 <= Nc <= 65535

Le	Length of Requested Data Ne Return up to Ne bytes of requested information		
	variable length	Condition: Lc short Le short '01 <= Le <= 'FF'	1 <= Ne <= 255
		Condition: Lc short Le short Le = '00'	Ne = 256
		Condition: Lc extended Le extended '0001' <= Le <= 'FFFF'	1 <= Ne <= 65535
		Condition: Lc extended Le Extended Le = '0000'	Ne = 65536

Status-Codes SW1-SW2

SW1-SW2	Addressed Functional Unit (FU) P1	Specification	Meaning
'6400'	CT	Error	
'6501'		Memory Failure	
'6700'		Wrong (command) length parameter	Message too long.
'6900'		Command not allowed	No pending Downlaod Session.
'6A00'		Wrong parameters P1, P2	▪ P1 addresses invalid Functional Unit. ▪ P2 specifies not supported value
'6C00'		Wrong (information) length parameter	Wrong Le.
'6F00'		Communication with CT not possible.	
'9000'		Command successful	Download Termination was successful.

Ergänzungen / Änderungen des Anhangs C (Status Codes)

Entfallene Status Code (SW1Sw2)

Complete SICCT Status Code Overview		
SW1 SW2	Meaning	
Warning		
~~'6200'~~	~~SICCT INIT CT SESSION~~	~~Warning - CT Session already set.~~
~~'6200'~~	~~SICCT CLOSE CT SESSION~~	~~Warning - No pending / open CT Session found.~~

Geänderte / aktuelle SICCT Status Code Vergleichstabelle

Korrektur (15.07.2008) – Edit - Added missing status codes.

Complete SICCT Status Code Overview		
SW1 SW2	Meaning	
Warning		
'6200'	SICCT SELECT CT MODE	Warning - Specified Mode already set.
'6200'	SICCT TERMINATE COMMAND	Warning - Specified command not found
'6200'	SICCT REQUEST ICC	Warning: No card presented in time
'6200'	SICCT CONTROL COMMAND	Warning – Specified command not found The specified command could not be found.
'6200'	SICCT EJECT ICC	Card not removed within specified time
'6201'	SICCT REQUEST ICC	Warning: Reset successfu, ICC alrady inserted and activated.
'620x'	Sequence Number Data Object Command Sequence Status Word	Sequence Number found: command in processing state '0x'
'63Cx'	SICCT PERFORM VERIFICATION	Verification unsuccessful. x = number of possible retries
General Execution Errors		
'6400'	SICCT TERMINATE COMMAND	Not terminated at preprocessing phase
'6400'	SICCT INIT CT SESSION	Error - Opening CT Session was not successful
'6400'	SICCT CLOSE CT SESSION	Error - Closing CT Session was not successful
'6400'	SICCT RESET CT / CC	Reset not successful
'6400'	SICCT REQUEST ICC	Reset not successful
'6400'	SICCT GET STATUS	Execution Error
'6400'	SICCT SET STATUS	Execution Error

Complete SICCT Status Code Overview		
SW1 SW2	Meaning	
'6400'	SICCT INPUT	Nor or incomplete input in time
'6400'	SICCT PERFORM VERIFICATION	Nor or incomplete input in time
'6400'	SICCT MODIFY VERIFICATION DATA	Nor or incomplete input in time
'6400'	SICCT CT Download INIT	Error
'6400'	SICCT CT Download DATA	Error
'6400'	SICCT CT Download FINISH	Error
'6401'	SICCT CONTROL COMMAND	Not terminated; command currently at stage 1
'6401'	SICCT REQUEST ICC	Process aborted by pressing of CANCEL key
'6401'	SICCT INPUT	Process aborted by pressing of CANCEL key
'6401'	SICCT PERFORM VERIFICATION	Process aborted by pressing of cancel key
'6401'	SICCT MODIFY VERIFICATION DATA	Process aborted by pressing of cancel key
'6402'	SICCT CONTROL COMMAND	Not terminated; command currently at stage 2
'6402'	SICCT MODIFY VERIFICATION DATA	Process unsuccessful, new PIN not identical
'6403'	SICCT INIT CT SESSION	Error - Opening CT Session was not successful DO Session ID has to be empty.
'6403'	SICCT CLOSE CT SESSION	Error - Closing CT Session was not successful Invalid Session ID. .
'6403	SICCT CONTROL COMMAND	Not terminated; command currently at stage 3
'640x'	SICCT CONTROL COMMAND	The ct could not terminate the specified command.
'640x'	Sequence Number Data Object Command Sequence Status Word	Sequence Number found: processing state found at stage '0x' - state cannot be changed.
'64A1'	SICCT RESET CT / CC	No Card present
'64A1'	SICCT GET STATUS	No Card present
'64A1'	SICCT PERFORM VERIFICATION	No Card present
'64A1'	SICCT MODIFY VERIFICATION DATA	No Card present
'64A2'	SICCT PERFORM VERIFICATION	Card not activated
'64A2'	SICCT MODIFY VERIFICATION DATA	Card not activated
'6501'	SICCT CT Download INIT	Memory Failure
'6501'	SICCT CT Download DATA	Memory Failure
'6501'	SICCT CT Download FINISH	Memory Failure
General Checking Errors		
'6700'	ALL SICCT Commands	Wrong (Command Length) length
		Too less / many Data (Objetcs) given within command.

Complete SICCT Status Code Overview		
SW1 SW2	Meaning	
'6900'	SICCT INIT CT SESSION	Command not allowed. Open CT Session found.
'6900'	SICCT CLOSE CT SESSION	Command not allowed. No open CT Session
'6900'	SICCT GET STATUS	Command not allowed ▪ Cardterminal Session: Admin Access Rights required. ▪ No open CT Session
'6900'	SICCT SET STATUS	Command not allowed ▪ Cardterminal Session: Admin Access Rights required. No open CT Session
'6900'	SICCT CT Download INIT	Command not allowed ▪ No open CT Session ▪ Cardterminal busy, Downlaod Session cannot start.
'6900'	SICCT CT Download DATA	Command not allowed ▪ No pending Download Session.
'6900'	SICCT CT Download FINISH	Command not allowed ▪ No pending Download Session.
'6930'	SICCT REQUEST ICC	Command with timer not supported. ▪ Terminal does not support the timer option.
'6930'	SICCT EJECT ICC	Command with timer not supported. Terminal does not support the timer option.
'6930'	SICCT INPUT	Command with timer not supported. Terminal does not support the timer option.
'6930'	SICCT OUTPUT	Command with timer not supported. Terminal does not support the timer option.
'6930'	SICCT PERFORM VERIFICATION	Command with timer not supported. Terminal does not support the timer option.
'6930'	SICCT MODIFY VERIFICATION DATA	Command with timer not supported. Terminal does not support the timer option.
'6940'	SICCT REQUEST ICC	Command with Display not supported.
'6940'	SICCT EJECT ICC	Command with Display not supported.
'6940'	SICCT INPUT	Command with Display not supported.
'6940'	SICCT OUTPUT	Command with Display not supported.

Complete SICCT Status Code Overview		
SW1 SW2	Meaning	
'6940'	SICCT PERFORM VERIFICATION	Command with Display not supported.
'6940'	SICCT MODIFY VERIFICATION DATA	Command with Display not supported.
'6941'	SICCT REQUEST ICC	Functional Unit (Display, Slot, Keypad) busy / not available. ▪ The addressed FU is busy and at the moment not available.
'6941'	SICCT INPUT	Functional Unit (Display, Slot, Keypad) busy / not available. ▪ The addressed FU is busy and at the moment not available.
'6941'	SICCT OUTPUT	Functional Unit (Display, Slot, Keypad) busy / not available. ▪ The addressed FU is busy and at the moment not available.
'6941'	SICCT PERFORM VERIFICATION	Functional Unit (Display, Slot, Keypad) busy / not available. ▪ The addressed FU is busy and at the moment not available.
'6941'	SICCT MODIFY VERIFICATION DATA	Functional Unit (Display, Slot, Keypad) busy / not available. ▪ The addressed FU is busy and at the moment not available.
'6942'	SICCT REQUEST ICC	Selected Character Set not supported. ▪ The addressed display does not support the selected character set.
'6942'	SICCT EJECT ICC	Selected Character Set not supported. ▪ The addressed display does not support the selected character set.
'6942'	SICCT INPUT	Selected Character Set not supported. ▪ The addressed display does not support the selected character set.
'6942'	SICCT OUTPUT	Selected Character Set not supported. ▪ The addressed display does not support the selected character set.
'6942'	SICCT PERFORM VERIFICATION	Selected Character Set not supported. ▪ The addressed display does not support the selected character set.
'6942'	SICCT MODIFY VERIFICATION DATA	Selected Character Set not supported. The addressed display does not support the selected character set.
'6A00'	ALL SICCT Commands	Wrong parameters P1, P2 ▪ P1 addresses invalid Functional Unit. ▪ Invalid FUI DO referenced by P1 (command data) P2 specifies not supported value
'6A80'	SICCT GET STATUS	Invalid Data Object ▪ Incorrect parameters (data object) in the command data field
'6A80'	SICCT SET STATUS	Invalid Data Object ▪ Incorrect parameters (data object) in the command data field
'6A88'	SICCT GET STATUS	Missing Data Object
		Referenced data or reference data not found
'6A88'	SICCT SET STATUS	Missing Data Object

Complete SICCT Status Code Overview		
SW1 SW2	Meaning	
		Referenced data or reference data not found
'6C00'	ALL SICCT Commands	Wrong length Le
'6D00'	ALL SICCT Commands	Wrong instruction
'6E00'	ALL SICCT Commands	Class not supported
'6F00'	Sequence Number Data Object Command Sequence Status Word	Sequence Number not found: no information given on processing state
'6F00'	SICCT REQUEST ICC	Communication with ICC not possible
'6F00'	SICCT RESET CT / CC	Communication with ICC not possible
'6F00'	SICCT CT Download INIT	Communication with CT not possible.
'6F00'	SICCT CT Download DATA	Communication with CT not possible.
'6F00'	SICCT CT Download FINISH	Communication with CT not possible.
Normal Processing		
'9000'	Sequence Number Data Object Command Sequence Status Word	Sequence Number found: Command queued and not in processing state
'9000'	SICCT SELECT CT MODE	Mode Selection was successful ▪ The specified CT mode has been selected. In order to activate the mode the cardterminal has to be reset.
'90xx'	SICCT TERMINATE COMMAND	Command successful ▪ The specified command with the given sequence number has been terminated at stage 'xx'
'9000'	SICCT CONTROL COMMAND	Command successful ▪ Command terminated before execution.
'9000'	SICCT INIT CT SESSION	Opening CT Session was successful ▪ The specified CT session has been opened.
'9000'	SICCT CLOSE CT SESSION	Closing CT Session was successful ▪ The specified CT session has been closed.
'9000'	SICCT RESET CT / ICC	Reset successful ▪ Cardterminal and all functional units successfully set to reset state. All chipcards deactivated.

Complete SICCT Status Code Overview		
SW1 SW2	Meaning	
'9000'	SICCT RESET CT / ICC	Reset successful, synchronous ICC ▪ Synchronous chipcard detected, activated and successfully set to demanded reset state.
'9000'	SICCT RESET CT / ICC	Reset successful ▪ Cardterminal and all functional units successfully set to reset state. All chipcards deactivated.
'9000'	SICCT RESET CT / ICC	Reset successful, synchronous ICC ▪ Synchronous chipcard detected, activated and successfully set to demanded reset state.
'9000'	SICCT EJECT ICC	Command successful ▪ Chipcard deactivated but not removed.
'9000'	SICCT GET STATUS	Command successful ▪ Data Object query successful.
'9000'	SICCT SET STATUS	Command successful ▪ Data Object adjusted: Value set.
'9000'	SICCT INPUT	Command successful ▪ Captured Input data returned within body of command response.
'9000'	SICCT OUTPUT	Command successful ▪ Output data processed by addressed FU
'9000'	SICCT PERFORM VERIFICATION	Command successful ▪ Note: Chipcard generated status word in case the PIN verification was successful.
'9000'	SICCT MODIFY VERIFICATION DATA	Command successful ▪ Note: Chipcard generated status word in case the PIN verification was successful.
'9000'	SICCT CT Download INIT	Command successful ▪ Download Initialisation was successful.
'9000'	SICCT CT Download DATA	Command successful ▪ Transmission of Download Data Object was successful.
'9000'	SICCT CT Download FINISH	Command successful ▪ Download Termination was successful.
'9001'	SICCT CONTROL COMMAND	Command terminated at preprocessing phase
'9001'	SICCT RESET CT / ICC	Reset successful, asynchronous ICC ▪ Asynchronous chipcard detected, activated and successfully set to demanded reset state.
'9001'	SICCT REQUEST CT / ICC	Reset successful, asynchronous ICC Asynchronous chipcard detected, activated and successfully set to demanded reset state.
'9001'	SICCT EJECT ICC	Command successful Chipcard deactivated and removed.
'9002'	SICCT CONTROL COMMAND	Command successful Command terminated at processing phase

Complete SICCT Status Code Overview		
SW1 SW2	Meaning	
'9003'	SICCT CONTROL COMMAND	Command successful Command terminated at postprocessing phase
'900F'	SICCT CONTROL COMMAND	Command successful Command abortion forced.
'90FF'	SICCT CONTROL COMMAND	Command status unknown - or command terminated at unknown stage

Dienstanfrage (Service Discovery) - 6.1.3.1

Korrektur (14.09.2008) – 6.1.3.1 - Ergänzung für TLS 1.1 in der Tabelle

Sicherheitsprotokolle:					
Protokoll	**TAG (hex.)**	**Datenlänge (Bytes)**	**Daten**	**Wert (hex.)**	**Beschreibung**
TLS	´8A´	1	Unterstützte Protokollversion (1 Byte)	´10´	TLS 1.0 [RFC2246]
				´11´	TLS 1.0 [RFC2246] **+** AES TLS Erweiterungen [RFC3268]
				’20’	TLS 1.1 [RFC4346]
...	...	...	...	...	...

TLS - 6.3.1.1

Korrektur (14.09.2008) – 6.3.1.1 - Ergänzung für TLS 1.1 in der Tabelle

Für die Verschlüsselung der Kommunikation mittels TLS (Transport Layer Security) gilt die Protokollversion 1.0 [RFC2246] sowie die Erweiterungen um AES basierte Cipher Suites [RFC 3268] oder TLS 1.1 [RFC4346].

Zeigt das Terminal im Dienstbeschreibungspaket TLS 1.0 Unterstützung an, so sind nur Ciphers Suites aus dem TLS 1.0 Standard relevant. Wird AES Unterstützung angezeigt, so sind auch Cipher Suites aus der erweiterten Liste zulässig. Bei der Anzeige von TLS 1.1, so sind die Ciphers Suites aus dem TLS1.1 zu verwenden. Welche Cipher Suites konkret durch ein Terminal angeboten werden, ergibt sich aus dessen Konfiguration zur Erfüllung fachspezifischer Sicherheitsvorgaben (Protection Profile, Policy). Wird TLS implementiert und gibt es keine fachspezifischen Vorgaben bezüglich der zu unterstützenden Cipher Suiten, so muss aber zumindest die Cipher Suite TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA implementiert sein, um die Mindestanforderungen des TLS 1.0 Standards zu erfüllen (siehe RFC 2246, Kapitel 9: „Mandatory Cipher Suites“). Die Aushandlung der konkret zu verwendenden Cipher Suite und ihrer Parameter erfolgt im Rahmen des im TLS Standard definierten Handshakeverfahrens.