TeleTrusT – Bundesverband IT-Sicherheit e.V.
Der IT-Sicherheitsverband.

SICCT
Secure Interoperable ChipCard Terminal

ERRATA zu [SICCT_121]

Datei: [SICCT_121_Errata_1_0_1]
Version: 1.0.1
Datum: 12.09.2014
Editoren: Frank Osthoff / M.Bukow

Hinweise zum Dokumentenstand und Haftungsausschluss befinden sich in Kapitel 2.

Autoren

Jürgen Atrott	TÜV Informationstechnik GmbH
Maximilian Bukow	gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
Volker Czmok	CCV Deutschland GmbH
Andreas Kilger	ZF Electronics GmbH
Dr. Klaus Leistner	CCV Deutschland GmbH
Lothar Mawick	Verifone
Torsten Maykranz	Identive
Dr. Holger Mühlbauer	TeleTrusT – Bundesverband IT-Sicherheit e.V.
Frank Osthoff	Ingenico Healthcare GmbH
Uwe Schnabel	HID Global

Vorwort
Dieses Dokument wurde von der Arbeitsgruppe "SICCT" des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) erarbeitet.

1 Anwendungsbereich

Das Dokument beschreibt bekannte und von der SICCT-WG bearbeitete Errata-Korrekturen zu der Spezifikation “Secure Interoperable Chipcard Terminal“ [SICCT_121] der Version V1.21 vom 19.10.2010.

Geänderte Inhalte zur [SICCT_121] werden in diesem Dokument auszugsweise dargestellt und wurden im Text gelb markiert.

2 Anmerkungen zum Dokumentenstand

2.1 Dokumentenstand und Haftungsausschluss

Die veröffentlichte Version 1.21 der SICCT-Spezifikation [SICCT_121] gibt den momentanen Stand der Arbeiten wieder, aus dem Zielsetzung und Lösungsansätze ersichtlich sind. Das Dokument [SICCT_121] in der jetzigen Form kann als Basis für andere Spezifizierungsarbeiten oder technische Entwicklungen dienen.

Für die Richtigkeit, Vollständigkeit und Aktualität der Inhalte können die Autoren keine Gewähr übernehmen.

Die folgenden Angaben fokussieren einige wichtige Punkte, die zum Zeitpunkt der Erstellung als bekannt galten. Die Gesamtheit der Korrekturen erhebt keinerlei Anspruch auf Vollständigkeit mit der Konsequenz, dass das Dokument an jeder Stelle grundlegend oder im Detail noch späteren Erweiterungen unterworfen sein kann.

2.2 Errata-Beschreibung

Das vorliegende Dokument beinhaltet die SICCT-Basisspezifikation sowie alle bis zum Ausgabedatum bekannten und von der TeleTrusT-AG "SICCT" bearbeiteten Errata-Korrekturen zu der Spezifikation "Secure Interoperable Chipcard Terminal" [SICCT_121] in der Version V1.21 vom 19.10.2010. Zukünftige ERRATA-Dokumente erhalten einen eigenen Versionsbezug (Version X_Y_Z) sowie eine Versionsreferenz zur SICCT-Basisspezifikation (z.B. [SICCT_121_Errata_X_Y_Z_YYYYMMDD]) im Dateinamen.

3 Änderungen und Korrekturen

5.5.9.3 Direct Coding

Korrektur (15.10.2013): Tabelle 2: Functional Units - Direct Coding Representation – Seite 39: [1_21_gem_001]

Functional Units (Referenced Coding Representation)					
Functional Unit	**Meaning**	**Refer-enced Coding** (2 Byte)	**Mode** **SICCT**		**Description**
Address the Cardterminal (whole device)					
✓	CT-Kernel	**'0000'**	✓	man	Address the Cardterminal device with all attached / controlled resources / function-al units.
Address contact bound ChipCard Interface					
✓	ICC-Interface n	'00xx'	✓		Address single ICC Interface.
ICC1	ICC-Interface 1	**'0001'**		man	1st contact bound ChipCard Interface Unit
:	:	**:**		opt	:
ICC255	ICC-Interface 255	**'00FF'**		opt	255th ChipCard Interface Unit
Address RFID / Contactless ChipCard Interface					
RFID	RFID Antenna Unit	**'1000'**	✓	opt	Address RFID Antenna Unit with all rec-ognized RFID Tokens.
RFIDn	RFID Token n	**'100x'**	✓	opt	Address single RFID Token.
RFID1	RFID Token 1	**'1001'**		opt	1st RFID Token at Antenna Unit
:	:	**:**		opt	:
RFID14	RFID Token 14	**'100E'**		opt	14th RFID Token at Antenna Unit
Address Human Interface Device Unit					
CT-Display (0)	Standard Display	**'4000'**	✓	opt	1st Cardterminal controlled Display (0) (Standard Display)
CT-Display 1	Display1	**'4001'**	✓	opt	Additional Cardterminal controlled Display 1
:	:	**:**		opt	
CT-Display 14	Display 14	**'400E'**		opt	Additional Cardterminal controlled Display 14
CT-KeyPad	Standard Keypad	**'5000'**	✓	opt	1st Cardterminal controlled KeyPad
CT KeyPad 1	Keypad 1	**'5001'**		opt	Additional Cardterminal controlled Key-Pad 1
:	:	**:**		opt	
CT KeyPad 14	KeyPad 14	**'500E'**		opt	Additional Cardterminal controlled Key-Pad 14
CT-Printer	Printer port	**'6000'**	✓	opt	Cardterminal controlled Printer port
Address Human Interface Device Unit of Type 'Biometric Sensor'					
Biometrical Unit		'700x'	✓	opt	2nd nibble codes the unit type.
CT-FP	Finger Print Sensor Unit	**'7000'**		opt	Cardterminal controlled Finger Print Sensor
CT-VP	Voiceprint Unit	**'7001'**		opt	Cardterminal controlled Voiceprint Sensor
CT-DSV	Dynamic Signature Verification Unit	**'7002'**		opt	Cardterminal controlled Dynamic Signa-ture Verification Sensor / System
CT-FR	Face Recognition Unit	**'7003'**		opt	Cardterminal Face Recognition Sensor / System
CT-I	Iris Unit	**'7004'**		opt	Cardterminal Iris Unit Sensor / System
other Biometrical Units		'7005' - '70FF'	✓	opt	RFU
SICCT specific FUs		'8000' - '90FF'	✓	opt	RFU
Vendor specific FUs		'A000' - 'F0FE'	✓	opt	Vendor defined Functional Unit

Tabelle 2: Functional Units - Referenced Coding Representation

5.5.10.26 Download Data Object

Korrektur (15.10.2013): 5.5.10.26 Download Data Object (DLDATA DO)- Feld ‚02' in Zeile ‚Three Bytes Coding' entfernt – Seite 71: [1_21_gem_002]

Das Download Data Object (DLDATA DO) enthält jeweils ein Download-Datenpaket.

<table>
<tr><td colspan="6">Download Data Object (DLDATA DO)</td></tr>
<tr><td rowspan="3">TAG</td><td colspan="2" rowspan="3">'73'</td><td colspan="3">One byte tag according ISO 7816-6: Discretionary Data Objects</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 : Application context, constructed, Tag-Number = 19 ('13')</td></tr>
<tr><td rowspan="5">LEN</td><td colspan="5">LEN coding see 5.5.10.3</td></tr>
<tr><td colspan="5">one byte coding - LEN in the range of : 0 <= LEN <= 65535</td></tr>
<tr><td colspan="2">'00' ... '7F'</td><td>0 <= LEN <= 127</td><td>One byte coding</td></tr>
<tr><td>'81'</td><td colspan="2">'80' ...'FF'</td><td>128 <= LEN <= 255</td><td>Two byte coding</td></tr>
<tr><td>'82'</td><td>'01' .. 'FF'</td><td>'00' .. 'FB'</td><td>256 <= LEN <= 65531</td><td>Three byte coding[1]</td></tr>
<tr><td rowspan="2">VALUE</td><td colspan="5">Download Data Package</td></tr>
<tr><td colspan="5">Vendor specific Data Objects or Format</td></tr>
</table>

5.6.1 Handling von Display Messages im SICCT-Mode

Korrektur (15.13.2013): 5.6.1 Handling von Display Messages im SICCT-Mode - 8. Bulletpoint: SMTB DO ersetzt durch SMTBD DO – Seite 74: [1_21_gem_003]

Sofern ein Terminal ein (optionales) Display anbietet kann ein Text (Display-Nachricht) explizit per Kommandoparameter in Form auf den aktuellen Befehlskontext bezogener Standard-Texte oder explizit über Daten Objekte zur Anzeige gebracht werden. Für die Handhabung von Display-Nachrichten gelten die folgenden allgemeinen Vorgaben.

- Ein (optional vorhandenes) Terminal-Display unterstützt mindestens den 7-bit- Zeichensatz ISO646DE. In der Beschreibung zum Application Label Data Object (APPL DO) 5.5.10.19 sind die minimal zu unterstützenden Zeichen angegeben.
- :
- :
- Der Aufbau von Display-Nachrichten in den Datenobjekten (APPL DO bzw. SMTBD 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)>
- :
- :

[1] Siehe SICCT DOWNLOAD DATA : Max. Nc = 65536, d.h. max Länge für DLDATA DO = (65536-5) = 65531

5.5.10.27 Download Termination Data Object

Korrektur (09.09.2014): 5.5.10.27 Download Termination Data Object – Tabelle DLTERM DO: Entfall der 2-Byte – langen Darstellung 'xxyy' *der 'Finalisation Condition', da alle definierten Werte in einem Byte darstellbar sind.*

<table>
<tr><td colspan="8">Download Termination Data Object (DLTERM DO)</td></tr>
<tr><td rowspan="3">TAG</td><td colspan="3" rowspan="3">'73'</td><td colspan="4">One byte tag according ISO 7816-6: Discretionary Data Objects</td></tr>
<tr><td colspan="4">Tag coding according ASN.1 BER see Fehler! Verweisquelle konnte nicht gefunden werden.</td></tr>
<tr><td colspan="4">BER-Coding : Application context, constructed, Tag-Number = 19 ('13')</td></tr>
<tr><td rowspan="3">LEN</td><td colspan="7">LEN coding see Fehler! Verweisquelle konnte nicht gefunden werden.</td></tr>
<tr><td colspan="7">one byte coding - LEN in the range of : Len = 5 … 7</td></tr>
<tr><td colspan="3">'05' … '07'</td><td colspan="2">5 <= LEN <= 7</td><td colspan="2">One byte coding</td></tr>
<tr><td rowspan="6">VALUE</td><td colspan="7">Timeout</td></tr>
<tr><td rowspan="3">'04'</td><td>'00'</td><td colspan="2">Empty DO</td><td colspan="2">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="2" 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="7">Finalisation Condition</td></tr>
<tr><td colspan="7">
<table>
<tr><td rowspan="9">'04'</td><td rowspan="9">'01'</td><td rowspan="9">'xy'</td><td colspan="3">At least one condition or (bit)combination shall be indicated by the terminal.</td></tr>
<tr><td colspan="3">Coded as ASN.1 BER Coding OCTETSTRING (UNIVERSAL 4):
[<HB>] <LB></td></tr>
<tr><td>b1 = '1'</td><td colspan="2">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="2">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>b3 = '1'</td><td colspan="2">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="2">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="2">Regular operation after Response</td></tr>
<tr><td>'xy'</td><td colspan="2">All other values RFU</td></tr>
</table>
</td></tr>
</table>

5.17 Command SICCT INPUT

Korrektur (15.10.2013):5.17.3 Command Structure SICCT INPUT – „'000001' <= Lc <= '00FFFF'“ und „1 <= Nc <= 65535“ – Seite 122: *[1_21_gem_004]*

5.17.3 Command Structure

SICCT Kommando	Kodierung C-APDU						
	CLA	INS	P1	P2	[Lc]	[Data]	[Le]
SICCT INPUT	'80'	'16'	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 1 (no cmd data, no rsp data) : no Lc, no Le		
					Case 2 (no cmd data, rsp data): no Lc, Le=1-256 Bytes or extended Le		
					Case 3 (cmd data, no rsp data) : Lc=1-255 Bytes or extended Lc no Le		
					Case 4 (cmd data, rsp data): [2] 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
	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 '000001' <= Lc <= '00FFFF'	1 <= Nc <= 65535

:
:

[2] According ISO 7816-4 [STD8] either both Le and Lc are short or extended.

5.18 Command SICCT OUTPUT

Korrektur (15.10.2013):5.18.3 Command Structure SICCT OUTPUT – „„'000001' <= Lc <= '00FFFF'“ und „1 <= Nc <= 65535 / Case 1 (no cmd data, no rsp data) :no Lc, no Le / -Seite 126: *[1_21_gem_006]*

5.18.2 Anwendungsbedingungen

:
:

5.18.3 Command Structure

SICCT Kommando	Kodierung C-APDU						
	CLA	INS	P1	P2	Lc	Data	[Le]
SICCT OUTPUT	'80'	'17'	Functional Unit	Command Qualifier	Length Command Data	Command Data	absent
	▪ 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 1 (no cmd data, no rsp data) : no Lc, no Le		
					Case 3 (cmd data, no rsp data:) Lc=1-255 Bytes or extended Lc no Le		

:
:

Lc	Length of Command Data Nc		
	Empty	Lc absent [3]	no Command Data provided; Nc = 0
	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 '000001' <= Lc <= '00FFFF'	1 <= Nc <= 65535

:
:

[3] Der Fall / Use Case – “Lc darf ‚absent“ sein, z.B. wenn via P2 nur die Idle-Message dargestellt werden soll.

6.1.3.1 Dienstanfrage (Service Discovery)

Korrektur (15.10.2013):6.1.3.1 Ergänzung der Tabelle Sicherheitsprotkolle um TLS V1.2

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]
				'30'	TLS 1.2 [RFC5246]
...	...	...	...	...	...

6.1.4 Kommandotransport und Namensvergabe

Korrektur (15.10.2013):5.18.3 Falsche Referenzen „5.5.6.2“ und „5.5.10.21“ durch „5.5.9.2“ bzw. „5.5.10.24“ ersetzt – Seiten 172, 174, 175:[1_21_gem_007]

6.1.4.1 Adressierung

:
:
Die Adressierung und Benennung der FU eines Terminals erfolgt über das im Kapitel 5.5.9.2 Ressourcentabelle definierte Schema.
:
:

6.1.4.2 Envelope

:
:
Die Felder des Envelope:

- :
- wSrcOrDesAddr:
  Das Feld wSrcOrDesAddr spezifiziert die Absender- bzw Empfänger-FU des jeweiligen Kommandos; die Kodierung erfolgt über das in der "Ressourcentabelle" im Kapitel 5.5.9.2 definierte Schema. Die Adresse wird in network-byte-order übertragen werden.
- wSeq:
  Die Sequenznummer wSeq wird vom Client aus dem in Kapitel 5.5.10.24 beschriebenen Wertebereichschema für jede abgesandte Nachricht vergeben:
  :
- :
  :

6.1.4.3 Kommandoabarbeitung

:

- :
- :

Sessions sind nicht kaskadierbar, d.h. das in einer Kommandointerpreterverbindung zu einer Zeit immer maximal eine Session aktiv sein darf. Um z.B. von einer User Session in eine Administrator Session zu wechseln, muss zuerst die User Session mittels SICCT CT CLOSE SESSION geschlossen werden, um danach die Administrator Session mittels SICCT CT INIT SESSION zu öffnen.

6.1.4.4 Ereignisbenachrichtigung

:
:
Ein SICCT konformes Terminal muss alle Protokoll-, sowie FU- und Kartenereignisnachrichten aus Tabelle 12 Ereignisbenachrichtigung“ unterstützen. Die kommandospezifischen Ereignisse sind je nach Unterstützung der jeweiligen Kommandos und Terminalausprägung zu unterstützen. Die Kodierung der FU Nummern erfolgt über das in der Ressourcentabelle im Kapitel 5.5.9.2 definierte Schema.
:
:

Änderungsnachweise des Errata-Dokuments

Errata-Version	Release-Datum	Editor	
V1.0.0	24.07.2014	F. Osthoff	Initialversion zur Abstimmung mit gematik
V1.0.1	12.09.2014	F. Osthoff	Korrekturen nach Rückmeldungen der gematik aus 07 und 08 / 2014. Annahme / Freigabe der SICCT-AG am 12.09.2014.