

SICCT Secure Interoperable ChipCard Terminal

ERRATA zu [SICCT_121]

Datei: [SICCT_121_Errata_1_0_2]
Version: 1.0.2
Datum: 28.10.2015
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 |

© 2005 - 2014, TeleTrusT

All product names are trademarks, registered trademarks, or service marks of their respective owners.

| | |
|---|----------|
| Vorwort | 5 |
| 1 Anwendungsbereich | 5 |
| 2 Anmerkungen zum Dokumentenstand | 5 |
| 2.1 DOKUMENTENSTAND UND HAFTUNGSAUSSCHLUSS | 5 |
| 2.2 ERRATA-BESCHREIBUNG..... | 5 |
| 3 Änderungen und Korrekturen | 6 |
| 5.5.9.3 DIRECT CODING..... | 6 |
| 5.5.10.16 ICC INTERFACE CAPABILITIES DATA OBJECT..... | 7 |
| 5.5.10.23 COMMAND-TO-PERFORM DATA OBJECT | 9 |
| 5.5.10.26 DOWNLOAD DATA OBJECT..... | 10 |
| 5.6.1 HANDLING VON DISPLAY MESSAGES IM SICCT-MODE | 10 |
| 5.5.10.27 DOWNLOAD TERMINATION DATA OBJECT..... | 11 |
| 5.14 COMMAND SICCT EJECT ICC | 12 |
| 5.14.6 Status-Codes SW1-SW2..... | 12 |
| 5.17 COMMAND SICCT INPUT..... | 13 |
| 5.17.3 Command Structure..... | 13 |
| 5.18 COMMAND SICCT OUTPUT..... | 14 |
| 5.18.2 Anwendungsbedingungen..... | 14 |
| 5.18.3 Command Structure..... | 14 |
| 5.20 COMMAND SICCT MODIFY VERIFICATION DATA..... | 15 |
| 5.20.2 Anwendungsbedingungen..... | 15 |
| 5.20.6 Status-Codes SW1-SW2..... | 15 |
| 6.1.3.1 DIENSTANFRAGE (SERVICE DISCOVERY) | 17 |
| 6.1.4 KOMMANDOTRANSPORT UND NAMENSVERGABE | 18 |
| ÄNDERUNGSNACHWEISE DES ERRATA-DOKUMENTS | 19 |

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.

Durch die vorliegende Version des Errata geänderte Inhalte gegenüber [SICCT_121] werden auszugsweise dargestellt; die konkreten Änderungen werden im Text **grün** 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-Basispezifikation 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-Basispezifikation (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 | Referenced Coding (2 Byte) | Mode | | Description |
| | | | SICCT | | |
| Address the Cardterminal (whole device) | | | | | |
| ✓ | CT-Kernel | '0000' | ✓ | man | Address the Cardterminal device with all attached / controlled resources / functional units. |
| Address contact bound ChipCard Interface | | | | | |
| ✓ | ICC-Interface n | '00xx' | ✓ | | Address single ICC Interface. |
| ICC1 | ICC-Interface 1 | '0001' | | man | 1 st contact bound ChipCard Interface Unit |
| : | : | : | | opt | : |
| ICC255 | ICC-Interface 255 | '00FF' | | opt | 255 th ChipCard Interface Unit |
| Address RFID / Contactless ChipCard Interface | | | | | |
| RFID | RFID Antenna Unit | '1000' | ✓ | opt | Address RFID Antenna Unit with all recognized RFID Tokens. |
| RFIDn | RFID Token n | '100x' | ✓ | opt | Address single RFID Token. |
| RFID1 | RFID Token 1 | '1001' | | opt | 1 st RFID Token at Antenna Unit |
| : | : | : | | opt | : |
| RFID14 | RFID Token 14 | '100E' | | opt | 14 th 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 | 1 st 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 | 2 nd 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 Signature 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 |
| SICCT specific FUs | | '8000' - '90FF' | ✓ | opt | RFU |
| Vendor specific FUs | | 'A000' - 'F0FE' | ✓ | opt | Vendor defined Functional Unit |

Tabelle 2: Functional Units - Referenced Coding Representation

5.5.10.16 ICC Interface Capabilities Data Object

Korrektur und Ergänzung Fließtext (28.10.2015): Tabelle ICC Interface Capabilities Data Object (INTFC DO) – Seite 50-51:

| ICC Interface Capabilities Data Object (INTFC DO) | | | | | |
|---|---|--|---|------------------------------------|---|
| TAG | '66' | One byte tag according SICCT-Specifications: | | | |
| | | Tag coding according ASN.1 BER see 5.5.10.3 | | | |
| | | BER-Coding : Application context, constructed, Tag-Number = 6 ('06') | | | |
| LEN | LEN coding see 5.5.10.3 | | | | |
| | one or two bytes coding - LEN in the range of : 0 <= LEN <= 255 | | | | |
| | '00' ... '7F' | 0 <= LEN <= 127 | One byte coding | | |
| | '81' ... 'FF' | 128 <= LEN <= 255 | Two byte coding | | |
| VA- LUE | Interface Device Protocol Options | | | | |
| | Tag | LEN | | | |
| | '80' | '01' | Supported Card Size | | |
| | | | b1 | 1 | ID-000 |
| | | | b2 | 1 | ID-1 |
| | | | b3...b8 | | RFU |
| | | | '00' | | unknown / contactless |
| | '81' | '01' | Supported / available Mechanical Attributes | | |
| | | | b1 | 1 | swallowing mechanism |
| | | | b2 | 1 | ejection mechanism |
| | | | b3 | 1 | capture mechanism |
| | | | b4 | 1 | internal slot |
| | | | b5 | 1 | qualifier- mechanic / automatic feature |
| | | | b6 ..b8 | | RFU |
| | '00' | | no special characteristics | | |
| | '82' | '01' | Supported / available Card Contacts | | |
| | | | bn | 1 | C<n> present / available |
| | | | '00' | | unknown / contactless |
| | '83' | '01' | Supported Card Types | | |
| | | | b1 | 1 | ISO 7816-Asynchr. |
| | | | b2 | 1 | ISO 7816-Synchr (Type1) |
| | | | b3 | 1 | ISO 7816-Synchr (Type2) |
| | | | b4 | 1 | ISO 14443-A |
| | | | b5 | 1 | ISO 14443-B |
| | | | b6 | 1 | ISO 15693 |
| | | | b7 | 1 | ISO 7816-12 |
| | | | b8 | 1 | EMV Level 1 |
| | '00' | | unknown | | |
| | '84' | '01' | Supported Asynchr. Protocols | | |
| | | | b1 | 1 | T=0 |
| | | | b2 | 1 | T=1 |
| | | | b3..b6 | | RFU |
| | | | b7 | 1 | qualifier - ISO 7816 Compatible |
| b8 | | | 1 | qualifier - EMV Level 1 Compatible | |
| '00' | | unknown / none | | | |

| | | | | | |
|------|------|---|---|---|---|
| '85' | '01' | Supported Synchr. ISO 7816-10 Protocols | | | |
| | | b1 | 1 | S=8 | SDAP (IIC Bus), one Byte Address |
| | | b2 | 1 | | SDAP (IIC Bus), two Byte Address |
| | | b3 | 1 | S=9 | 3 WB (Type 1) |
| | | b4 | 1 | S=10 | 2 WB (Type 1) |
| | | b5 | 1 | S=11 | FCB (Type2) |
| | | b6 | | | RFU |
| | | b7 | 1 | | qualifier - ISO 7816 Compatible |
| | | b8 | 1 | | qualifier – supported in EMV Level 1 Mode |
| | | '00' | | | unknown / none |
| '86' | '01' | Supported Wireless ISO 14443-Protocols | | | |
| | | b1 | 1 | Type A | |
| | | b2 | 1 | Type B | |
| | | b3 | 1 | supported according ISO 14443-1 | |
| | | b4 | 1 | supported according ISO 14443-2 | |
| | | b5 | 1 | supported according ISO 14443-3 | |
| | | b6 | 1 | supported according ISO 14443-4 (T=CL) | |
| | | b7 | 1 | qualifier – supported in ISO 7816 Mode | |
| | | b8 | 1 | qualifier – supported in EMV Level 1 Mode | |
| | | '00' | | | unknown / none |
| '87' | '02' | Extended Length Indication | | | |
| | | '20' .. 'FFF5' | | 32 .. 65525 Bytes (Maximum value: maximum value of CTS DO - 10 Byte for SICCT-Envelope) | |

Für einen Client ergibt sich der Maximalwert einer längstmöglichen APDU (ohne den 10 Byte langen SICCT-Envelope) zu einer konkreten ICC/PICC aus dem kleineren Wert aus INTFC DO Tag '87' und CTS DO (Maximum Length of SICCT Commands – and Response APDUs). Diese Werte sind insofern statisch, als dass sie sich nicht über eine Gerätekonfiguration am Kartenterminal sondern nur über eine neue Firmwareversion anpassen lassen. Für einen Client bedeutet dies, dass diese Kartenterminal-individuellen Parameter nicht vor jeder Kartenkommunikation abgefragt werden müssen.

Für die Kommunikation zu einer konkreten gesteckten Karte sind für einen Client neben den Kartenterminal-individuellen Parametern insbesondere auch die Parameter der Karte zu berücksichtigen.

5.5.10.23 Command-To-Perform Data Object

Korrektur (28.10.2015): Festlegung zur zulässigen Mindestlänge von PINs auf 4 Zeichen in Tabelle Control Byte Coding for user authentication und Streichung des Satzes "Für andere PIN-Darstellungen sollen Eingaben im Bereich 1 bis max. 12 Zeichen zulässig sein".

...

| Control Byte Coding for user authentication | | | | | |
|---|-------------------------------------|--------------------------------|---------|---|---|
| Control Byte | Coding for PIN / Password | | | | |
| | b8...b5 | Length of PIN to be presented. | | | Variable length PIN / password |
| | | 0000 | '0' | | If length = 0 (value for variable length), then pressing of validation key is required. |
| | | 0100 | '4' ... | | Number of PIN digits or characters |
| | | ... 1100 | '12' | | Minimal 4 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. |
| | | 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 | |
| | | 1 | 0 | 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 | 1 | Format 2 PIN Block according to ISO 9564-1, see table below | |
| | Coding for Biometric identification | | | | |
| | b8 .. b1 | 11111111 | 'FF' | In case of biometric identification | |

...

Die Bedingungen, wie Informationen vom Kartenterminal einzufügen sind, hängt vom entsprechenden Kartenkommando (APDU) und von dem PIN-Format ab. Eine PIN nach ISO 9564-1 hat minimal 4 und maximal 12 Zeichen (digits).

[Streichung des Satzes: Für andere PIN-Darstellungen sollen Eingaben im Bereich 1 bis max. 12 Zeichen zulässig sein.]

Für die Ergänzung von PIN-Eingaben am Terminal in den Kommandos

SICCT PERFORM VERIFICATION

SICCT MODIFY VERIFICATION DATA

sind folgende Formen des APDU möglich

Command Header (CLA, INS, P1 P2 = 4 Bytes),

falls im Datenfeld des ICC-Kommandos nur der PIN ohne Padding eingetragen wird

Command Header mit Längelfeld Lc und mit Paddingbytes vorformatiertem Datenfeld.

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.

| Download Data Object (DLDATA DO) | | | | | |
|----------------------------------|---|---------------|---|---------------------|--------------------------------|
| TAG | '73' | | One byte tag according ISO 7816-6: Discretionary Data Objects | | |
| | | | Tag coding according ASN.1 BER see 5.5.10.3 | | |
| | | | BER-Coding : Application context, constructed, Tag-Number = 19 ('13') | | |
| LEN | LEN coding see 5.5.10.3 | | | | |
| | one byte coding - LEN in the range of : 0 <= LEN <= 65535 | | | | |
| | '00' ... '7F' | | 0 <= LEN <= 127 | One byte coding | |
| | '81' | '80' ... 'FF' | 128 <= LEN <= 255 | Two byte coding | |
| | '82' | '01' .. 'FF' | '00' .. 'FB' | 256 <= LEN <= 65531 | Three byte coding ¹ |
| VALUE | Download Data Package | | | | |
| | Vendor specific Data Objects or Format | | | | |

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.

| Download Termination Data Object (DLTERM DO) | | | | | | |
|--|---|---------------|---|--|--|--|
| TAG | '73' | | One byte tag according ISO 7816-6: Discretionary Data Objects | | | |
| | | | Tag coding according ASN.1 BER see 5.5.10.3 | | | |
| | | | BER-Coding : Application context, constructed, Tag-Number = 19 ('13') | | | |
| LEN | LEN coding see 5.5.10.13 | | | | | |
| | one byte coding - LEN in the range of : Len = 5 ... 7 | | | | | |
| | '05' ... '07' | 5 <= LEN <= 7 | | One byte coding | | |
| VALUE | Timeout | | | | | |
| | '04' | '00' | Empty DO | | No time indication mandatory in case of Finalisation Condition b3=1 or b4=1 | |
| | | '01' | 'xx' | Timeout coded as ASN.1 BER Coding OCTETSTRING (UNIVERSAL 4): [<HB>] <LB> | Extended Timeout Timeout in seconds how long the device needs to process last download data object or finish the download process. | |
| | | '02' | 'yyxx' | | | |
| | Finalisation Condition | | | | | |
| | '04' | '01' | 'xy' | At least one condition or (bit)combination shall be indicated by the terminal. | | |
| | | | | Coded as ASN.1 BER Coding OCTETSTRING (UNIVERSAL 4): [<HB>] <LB> | | |
| | | | | b1 = '1' | A SICCT CLOSE CT SESSION (disconnection) is needed / expected by the terminal to end the download operation after the timeout period. | |
| | | | | b2 = '1' | The terminal needs a reboot / restart in order to end the download operation. Therefore is SICCT RESET CT necessary after the timeout period. | |
| | | | | b3 = '1' | 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 established, if needed. | |
| b4 = '1' | | | | He terminal needs manual assistance in order to end the download operation or to reboot / restart. Note: A new LAN connection must be established, if needed. | | |
| '00' | | | | Regular operation after Response | | |
| 'xy' | All other values RFU | | | | | |

5.14 Command SICCT EJECT ICC

Korrektur (28.10.2015): Klarstellung zu den erwarteten Status-Codes bei SICCT EJECT ICC.

5.14.6 Status-Codes SW1-SW2

Nach erfolgreicher Ausführung des SICCT EJECT ICC Kommandos enthält das erste Byte des Statusworts SW1 den Wert '90'. Bei Anweisung „No Mechanical Throw out - Keep chipcard“ (P2 bit2=1) ist immer, auch unabhängig von der Art der Kartenkontaktiereinheit (auch bei Kontaktiereinheiten mit Auswurfmechanik), von einer erfolgreichen Ausführung des Kommandos auszugehen. SW1 enthält daher bei „No Mechanical Throw out - Keep chipcard“ immer den Wert '90'. Auch bei Anweisung „Mechanical Throw out“ (P2 bit2=0) enthält SW1 den Wert '90', wenn die Karte gezogen/ausgeworfen wurde.

Nur bei Anweisung „Mechanical Throw out“ (P2 bit2=0) enthält SW1 den Wert '62' (Warning), wenn die Karte gesteckt bleibt.

Das Statusbyte SW2 qualifiziert bei erfolgreicher Ausführung weitere Umstände in Abhängigkeit zu Kommandoparametern.

Dieser Wert SW2 lässt eine Statuserkennung der Chipkartenfunktionseinheit nach dem Deaktivieren zu:

- '01' Command Successful, card removed

| SW1-SW2 | Addressed Functional Unit | | Specification | Meaning |
|---------|---------------------------|---------|--|---|
| | P1 | | | |
| | Of Type | | | |
| '6200' | ICC<n> | RFID<n> | Warning: Card not removed within specified time | Chipcard deactivated but not removed (within specified time). |
| '6700' | | | Wrong (command) length parameter | Wrong Lc: Inconsistent command body or no Command Data field supported. |
| '6930' | | | Command with timer not supported. | Terminal does not support the timer option. |
| '6940' | | | Command with Display not supported. | Command with Display not supported. |
| '6941' | | | Functional Unit (FU) busy / not available. | The addressed FU (display, slot, ..) is busy at the moment or not available. |
| '6942' | | | Selected Character Set not supported. | The addressed display does not support the selected character set. |
| '6A00' | | | Wrong parameters P1, P2 | P1 addresses invalid Functional Unit. P2 specifies not supported value |
| '6C00' | | | Wrong (information) length parameter | Wrong Le. |
| '9000' | | | Command successful | Chipcard deactivated but no information if card has been removed (within specified time). |
| '9001' | | | Command successful | Chipcard deactivated and removed (within specified time). |

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 |
| | <ul style="list-style-type: none"> ▪ 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] |
| | '80' | '17' | Functional Unit | Command Qualifier | Length Command Data | Command Data | absent |
| SICCT OUTPUT | <ul style="list-style-type: none"> ▪ 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 |
| 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.

5.20 Command SICCT MODIFY VERIFICATION DATA

Korrektur (28.10.2015): Festlegung zur zulässigen Mindestlänge von PINs auf 4 Zeichen und Ergänzung des Status-Codes 6A80 analog zu SICCT PERFORM VERIFICATION.

5.20.2 Anwendungsbedingungen

...

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, **solange die vorgegebene Länge im zulässigen Bereich von 4-12 Zeichen liegt.**

Sonderfall Null-PIN-Verfahren:

Zur Initiierung einer sog. NULL-PIN-Abfrage soll das CMD DO in allen Datenobjekten vollständig besetzt übergeben werden. Die erste 'Insert Position' enthält als Indikator den Wert Null ('00'), nicht benötigte Display-Nachrichten werden als notwendige Platzhalter in Form von 'leeren' Datenobjekten, bestehend aus Tag und Value, übergeben. Die Kommandoausführung übergeht die erste PIN-Eingabe und beschränkt sich dann auf die Eingabe und Bestätigung der (zweiten) PIN, die an die Position der '2 nd INSERTION Position' in das Karten-APDU eingetragen wird. Der (Null)-Inhalt, bzw. der Wert, der ersten PIN ist im Karten-APDU vom Aufrufer im CMD DO zu übergeben.

...

5.20.6 Status-Codes SW1-SW2

Nach erfolgreicher Ausführung des SICCT MODIFY VERIFICATION DATA - Kommandos enthält das erste Byte des Statusworts SW1 den Wert '90'.

Das Statusbyte SW2 qualifiziert weitere Umstände in Abhängigkeit zu Kommandoparametern.

| SW1-SW2 | Addressed Functional Unit | | Specification | Meaning |
|---------|---------------------------|---------|--|---|
| | P1 | | | |
| | Of Type | | | |
| '6400' | ICC<n> | RFID<n> | Nor or incomplete input time | |
| '6401' | | | Process aborted by pressing of cancel key | |
| '6402' | | | Process unsuccessful, new PIN not identical | |
| '6700' | | | Wrong (command) length parameter | Message too long. |
| '6930' | | | Command with timer not supported. | Terminal does not support the timer option. |
| '6940' | | | Warning Command with Display not supported. | Command with Display not supported. |
| '6941' | | | Functional Unit (FU) busy / not available. | The addressed FU (display, slot, ..) is busy at the moment or not available. |
| '6942' | | | Selected Character Set not supported. | The addressed display does not support the selected character set. |
| '6A00' | | | Wrong parameters P1, P2 | <ul style="list-style-type: none"> ▪ P1 addresses invalid Functional Unit. ▪ P2 specifies not supported value |
| '6A80' | | | Incorrect parameters in the command data field | <ul style="list-style-type: none"> ▪ General data error ▪ In case of CMD DO e.g. non-allowed 'INS' code |
| '64A1' | | | No card present | <ul style="list-style-type: none"> ▪ Verification not performed, because no card present |
| '64A2' | | | Card not activated | <ul style="list-style-type: none"> ▪ Verification not performed, because card not activated. |
| '6C00' | | | Wrong (information) length parameter | Wrong Le |
| '9000' | | | Command successful | Change of Verification Data successful |
| | | | | |

6.1.3.1 Dienstanfrage (Service Discovery)

Korrektur (15.10.2013):6.1.3.1 Ergänzung der Tabelle Sicherheitsprotokolle 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 Kartenergebnisnachrichten 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. |
| V1.0.2 | 28.10.2015 | F. Osthoff | Initialvorschlag zur Abstimmung in der SICCT-AG: <ul style="list-style-type: none"> - Anpassung zu <i>INTFC DO</i> Tag 87 gemäß Beschluss der SICCT-AG vom 25.09.2015, - Ergänzung zu SICCT EJECT ICC, - Festlegung zur PIN-Mindestlänge. |