

SRQ-ID: 1206

Betrifft:

Themenkreis	Dezentrale Komponenten
Schlagwort	eHealth-BCS, MKT, SICCT
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemAnf_BCS], ersetzt SRQ_0764
Version	0.9.0
Bezug (Kap., Abschnitt, Tab., Abb.)	3.1, A5

Stichwort: eHealth-BCS

Frage:

Welche Vorgaben hat die gematik in Bezug auf die in der MKT-Spezifikation vorhandenen Unschärfen, auch in Hinblick auf den Schutz der PINs?

Betrifft:

Gültig ab	01.10.2011	Verbindlichkeit	normativ
Zulassungsrelevanz	SRQ ist gültig für Zulassungsanträge ab dem "Gültig ab"-Datum sowie Zulassungsanträge, deren Testobjekte nach dem "Gültig ab"-Datum bei der gematik eingereicht werden.		
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version		voraussichtl. Zeitpunkt	
Anmerkungen:			
Status	<input checked="" type="checkbox"/> erfasst <input checked="" type="checkbox"/> intern abgestimmt <input type="checkbox"/> extern abgestimmt <input type="checkbox"/> zurückgezogen <input checked="" type="checkbox"/> freigegeben <input type="checkbox"/> eingearbeitet in Folgeversion		

Antwort:

Alle Antworten beziehen sich auf das Kapitel Funktionale Anforderungen [gemAnf_BCS#3.1]

Die inhaltliche Änderung gegenüber der zurückgezogenen SRQ 0764 beschränkt sich auf 3.1.1.1.3 „Ergänzung zu eHealth-BCS INPUT“. Der Inhalt des korrespondierenden, ursprünglichen Abschnitts der SRQ 0764 (dort 1.1.3) wird vollständig ersetzt.

3.1 Funktionale Anforderungen

[...]

3.1.1 Kartenterminalkommandos

Alle eHealth-BCS-Kartenterminals **MÜSSEN** aus Gründen der Interoperabilität den gleichen Kommandosatz zur Ansteuerung unterstützen.

Die Kommandos des eHealth-BCS-Betriebsmodus gemäß Abschnitt 5.5.6 der SICCT-Spezifikation [SICCT] **MÜSSEN** verpflichtend implementiert werden.

Die Kommandos des eHealth-BCS-Betriebsmodus **MÜSSEN** zumindest für die V.24-Schnittstelle des Kartenterminals verpflichtend steckerkompatibel implementiert werden, sofern ein Kartenterminal über optionale V.24-Schnittstellen verfügt.

Wird ein Kartenterminal über eine nicht steckerkompatible Schnittstelle angesteuert, so **MUSS** hierzu eine Verbindung zwischen der CT-API und dem Kartenterminal aufgebaut werden.

Das Kartenterminal **SOLL** über einen 3 Kilobyte (KB) (3072 Byte) großen Kommandopuffer für APDUs verfügen.

3.1.1.1 Verbindlichkeit der unterstützten eHealth-BCS-Kommandos

Der in der SICCT-Spezifikation dargestellte Auszug aus dem Cardterminal Basis Command Set (CT-BCS) [SICCT #5.5.6] **MUSS** unterstützt werden. Spezielle Ausprägungen werden in den folgenden Punkten konkretisiert.

Bei den B1-Kommandos RESET und DEACTIVATE handelt es sich um optionale Kommandos.

Die in der SICCT-Spezifikation aufgeführten allgemeinen Statusworte [SICCT#5.4.1] **SOLLEN** verwendet werden. Analog gilt dies auch für die Prioritäten der Parameterüberprüfung [SICCT#5.4.2].

3.1.1.1.1 Ergänzung zu eHealth-BCS PERFORM VERIFICATION

Das Kartenterminal **SOLL** die mittels eHealth-BCS PERFORM VERIFICATION übergebenen Parameter der Display-Nachricht zur Anzeige bringen können. Hierbei **MUSS** mindestens die Länge von 32 Zeichen für die Display-Nachricht unterstützt werden.

Während der PIN-Eingabe **KÖNNEN** Teile der Display-Message ausgeblendet werden.

Es **MÜSSEN** mindestens PINs der Länge 4 bis 8 Zeichen unterstützt werden.

PINs der Länge bis 12 Zeichen **SOLLEN** unterstützt werden.

Wenn die Display-Nachricht nicht dargestellt werden kann, **MUSS** der Fehlercode 6410 ausgegeben werden.

Bevor der Text „Abbruch“ angezeigt wird, SOLL die Nachricht „Bitte Eingabe bestätigen“ angezeigt werden. (siehe [SICCT#5.17.1], [MKT#6.3.3] S. 15)

Eine Eingabe MUSS bestätigt werden.

3.1.1.1.2 Ergänzung zu eHealth-BCS MODIFY VERIFICATION DATA

Es gelten die oben genannten Festlegungen von eHealth-BCS PERFORM VERIFICATION.

Wird ein leeres Application Label Data Object (50-00) an das Terminal übergeben, so MUSS der entsprechende Standardtext vom Terminal ausgegeben werden.

Analog zu SICCT- MODIFY VERIFICATION DATA MUSS die erste Einfügeposition des CHANGE REFERENCE DATA wie folgt beachtet werden:

“Null-PIN-Support - Only for usage with SICCT MODIFY VERIFICATION DATA might this value be zero ('00') in order to instruct this SICCT command to skip the 1st PIN entry phase and process only the second PIN and conformance entry.“

3.1.1.1.3 Ergänzung zu eHealth-BCS INPUT

Das INPUT-Kommando DARF NICHT zur Nutzung angeboten werden. Ein Aufruf des Kommandos MUSS vom Kartenterminal mit dem Returnwert '6900' (=Command not allowed) beantwortet werden.

3.1.1.1.4 Ergänzung zu eHealth-BCS EJECT ICC

Status/Antwortcode bei EJECT:

- wird bei einem EJECT-ICC-Kommando das bit b3=1 (keep) übergeben, MUSS bei Vorhandensein eines WT DO der Returnwert 9000 / 9001 zurückgegeben werden.
- wird bei einem EJECT-ICC-Kommando das bit b3=0 (throwout) übergeben, SOLL ohne WT DO der Returnwert 6200 / 9001 zurückgegeben werden.
- steckt beim Empfang eines EJECT-Kommandos keine Karte, so SOLL 9001 zurückgegeben werden.

3.1.1.1.5 Ergänzung zu Kommandos mit extended Length

Bei Überschreiten der physikalischen Ressourcen des eHealth-BCS-Kartenterminals (z.B. Kommandopuffer für APDUs) SOLL das eHealth-BCS-Kartenterminal die Aktion mit den Returnwerten 61xx beenden [ISO7816-4#5.1.3]. Bei Überschreiten der physikalischen Ressourcen des eHealth-BCS-Kartenterminals MUSS zudem sichergestellt sein, dass kein undefinierter Zustand eintritt.

Dazu KANN folgendes Vorgehen gewählt werden:

- die Karte bleibt nach dem Abbruch unter Spannung
- wenn das Terminal den nächsten maximalen (T=1 Chaining) Block nicht mehr komplett empfangen kann, ist auf der Ebene T=1 mittels CHAINING ABORT ein Abbruch durchzuführen
- die bis zum Abbruch empfangenen Daten sind an das Primärsystem zurückzusenden

A5 – Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
ISO7816-4	ISO/IEC 7816-4: 2004 (2nd edition) Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange