

SRQ-ID: 0857

**Betrifft (wird vom FLS (optional vom Erfasser) ausgefüllt):**

Themenkreis	Dezentrale Komponenten
Schlagwort	eHealth-BCS, MKT, SICCT
zu Dokument / Datei	[gemAnf_BCS]
Version	0.9.0
Bezug (Kap., Abschnitt, Tab., Abb.)	gesamt

**Stichwort: eHealth-BCS**

**Frage:**

Welche Änderungen haben sich am eHealth-lastenheft ergeben?

**Betrifft (wird vom PB ausgefüllt):**

Gültig ab Release	0.5.2	Verbindlichkeit	
zusätzlicher Download-Link zu Datei:			
Herstellerebefragung durchgeführt		am	
Wird behoben mit Version		voraussichtl. Zeitpunkt	
Anmerkungen:			
Status	<input type="checkbox"/> erfasst <input type="checkbox"/> intern abgestimmt <input type="checkbox"/> extern abgestimmt <input type="checkbox"/> zurückgezogen <input type="checkbox"/> freigegeben <input checked="" type="checkbox"/> eingearbeitet in Folgeversion		

**(wird von der bearbeitenden AG ausgefüllt):**

**Antwort:**

## 3 Anforderungen und Annahmen

eHealth-BCS-Kartenlesegeräte mit direktem Anschluss werden über eine USB- oder V24-Schnittstelle in Verbindung mit einer zugehörigen CT-API (aus Sicht der Primärsysteme) bzw. PCSC-API an die Primärsysteme angeschlossen.

[...]

Die elektrischen und physikalischen Tests, die im Rahmen einer MKT-Evaluierung vom TÜVIT durchgeführt wurden, können anerkannt werden und brauchen dann nicht erneut in Auftrag gegeben zu werden.

Für folgende Punkte sind Herstellererklärung ausreichend:

- - elektrisch-magnetische. Verträglichkeit / CE
- - Verwendung GS-Netzteil
- - Teile des Sicherheitsgutachtens
- - Bei Fremdprüfungen (Akkreditierung und gemäß den BCS Anforderungen)

## 3.1 Funktionale Anforderungen

In den folgenden Punkten sind die funktionalen Anforderungen zu den SICCT-, KVK- und eGK-Funktionalitäten aufgeführt. Für die Testung ist das gematik Testlabor zu beauftragen.

- [...]
- Der Basic Command Set (SICCT-Spezifikation Kapitel 5.5.6 [SICCT]) zur Ansteuerung des Kartenterminals, der Kartenslots, des Displays und der Tastatur sowie der Karten MUSS korrekt implementiert sein (APDUS konform zur ISO/IEC 7816-4).
- funktionale Tests mit eGK

### 3.2.1 Informationssicherheit

- ~~• Es MUSS wegen der Implementierung eines KVK-Moduls eine Sicherheitsüberprüfung durchgeführt werden. Die Prüfung erfolgt entweder durch eine ITSEC-Evaluierung, Stufe E2 / niedrige Mechanismenstärke oder durch eine kurze Sicherheitsbegutachtung, wie sie nach einer Revision der portablen Kartenleser ersatzweise eingeführt wurde.~~
- Die eHealth-BCS Kartenterminals MÜSSEN im Feld ohne Austausch der Geräte migrationsfähig sein. Dazu wird es notwendig sein, dass die eHealth-BCS Kartenterminals im Upgradeverfahren mit einer neuen Firmware aufgerüstet werden. Dieses Upgradeverfahren für eHealth-BCS Kartenterminals MUSS vom BSI gemäß EAL 3 hoch evaluiert werden und zertifizierungsfähig sein. Download/Upgrade-Fähigkeit MUSS beim eHealth-BCS-KT vorhanden sein. Daher MUSS, ähnlich wie beim KV-Modul (siehe unten), bei der CC Evaluierung des finalen eHealth-KTs begonnen werden. Eine doppelte Prüfung entfällt somit.
- Die Migrationsfähigkeit setzt eine Beantragung auf Zertifizierung der Bauart (HW) beim BSI auf Basis der aktuellen Protection Profile voraus.
- Die Hardwaresicherheit MUSS vom BSI evaluiert werden und zertifizierungsfähig sein.
- Ein Nachweis der QES-Fähigkeit des eHealth-BCS Kartenterminals ist NICHT für die erste Migrationsstufe im Basis-Rollout Voraussetzung. Für evtl. später zusätzlich anzuschließende Hardware (RFID, Fingerprint-Scanner, usw.)

MÜSSEN die HW-Schnittstellen vorhanden sein. Die Funktionalität dieser Schnittstellen wird nicht geprüft.

- Die Anforderungen des BSI zur Gehäuseverriegelung und zum Klappensiegel aus den Dokumenten:
  - TR-03120\_Anhang\_KTVersiegelung\_v102.pdf [BSI\_TR3120]
  - BSI-TL 03415\_Sicherheitsetiketten.pdf [BSI\_TL03415]
  - BSI-TL 03400\_7500\_November\_2007.pdf [BSI\_TL03400]

MÜSSEN erfüllt werden.

- Ein gematik Prüfzeichen MUSS gut erkennbar und in nicht unbeschadet ablösbarer Form auf dem Gehäuse aufgebracht sein d. h. ein Prüfzeichen darf nicht nach dem Entfernen auf ein anderes Gerät aufgebracht werden können. Es stehen zwei Varianten des Prüfzeichens zur Verfügung (siehe Abbildung 1). Das Prüfzeichen KANN auch in inverser Form (Weiß auf schwarzem Untergrund) aufgebracht werden. Das gematik Prüfzeichen MUSS folgende Mindestgröße haben: 8 mm Höhe und 27 mm Breite. Das in der EPS-Datei vorgegebene Seitenverhältnis MUSS beibehalten werden. Das Gehäuse MUSS Platz für ein gematik Prüfzeichen an einer während der PIN-Eingabe für den Benutzer gut sichtbaren Stelle bieten. Die Berechtigung und Verpflichtung zur Nutzung des Prüfzeichens durch den Hersteller erfolgt mit der Zulassung der Geräte durch die gematik. Im Rahmen des Zulassungsantrags werden den Herstellern die beiden Versionen des gematik Prüfzeichens im Encapsulated PostScript (EPS) Format zur Verfügung gestellt. Das Prüfzeichen bietet einen Wiedererkennungswert für zugelassene Kartenterminals, es sind keine Sicherheitsfunktionen damit verbunden.



Abbildung 1 gematik Prüfzeichen

Die Farbgebung des Prüfzeichens ist vierfarbig CMYK:

- für den Grün-Anteil: C40, M0, Y60, K0
  - für den Rot-Anteil: C0, M100, Y100, K0
  - für den Gelb-Anteil: C0, M20, Y100, K0
- Sicherheitsbegutachtung des KVK-Moduls (Schreibschutz, Übertragungsschutz, Datenplausibilität und Speicher-Aufbereitung als Auflage des Datenschützers).
- Die in der Sicherheitsbegutachtung erforderlichen Prüfungen der Entwicklungs- und Produktionsumgebung sowie der Gehäuseversiegelung und der

Auslieferung werden durch Referenzierung auf Prozesse der schon gestarteten CC Evaluierung des finalen eHealth KT's ersetzt.

### 3.2 Elektrische / physikalische Anforderungen

Die Anforderungen zur elektrischen / physikalischen Eignung gemäß ISO/IEC 7816-3 und eHealth Spezifikation [gemSpec KT] sind in den folgenden Abschnitten zusammengefasst: Für die Testung ist ein Prüflabor zu beauftragen.

#### 3.2.1 Basisfunktionalität

- ISO/IEC 7816-3 Test (Initialisierung, Reset, ATR, Chipkartenprotokolle, Bitübertragung, Befehlsübertragung und Response)
- Korrekte Funktion von Kommandos und Rückmeldungen von APDUs gemäß ISO/IEC 7816-4 (KVK, BCS)
- Speicherkartentests KVK
- Speicherkartenprotokolle
- Testung des KVK-Moduls  
Bei eHealth-KTs (SICCT) MUSS die Unterstützung kompletter Speicherkarteneinhalte gewährleistet sein, da der Konnektor die "alte" KVK als komplette Speicherkarte einliest.

#### 3.2.2 Basissicherheitstest

- Es MUSS wegen der Implementierung eines KVK-Moduls eine Sicherheitsüberprüfung durchgeführt werden. Die Prüfung erfolgt entweder durch eine ITSEC-Evaluierung, Stufe E2 / niedrige Mechanismenstärke oder durch eine kurze Sicherheitsbegutachtung, wie sie nach einer Revision der portablen Kartenleser ersatzweise eingeführt wurde.

#### 3.2.3 Physikalische Sicherheit - Klima

- Trockene Wärme (Dry Heat) nach IEC 68-2-2 Methode Bb (DIN/IEC 60068-2-2) wird für die Bedingungen als obere Lagertemperatur von 55°C und einer Beanspruchungsdauer von 16 h geprüft und die Funktionsfähigkeit MUSS bestätigt werden.

#### 3.2.4 Physikalische Sicherheit - Vibration

- Sinusförmige Schwingungstests (Vibration, sinusoidal) nach IEC 68-2-6 Methode Fc in drei senkrecht stehenden Achsen in einem Frequenzbereich von 2 Hz bis 200 Hz üblicherweise 1 h je Achse MÜSSEN erfolgreich nachgewiesen werden.

## A5 – Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI_TR3120]	BSI (04.04.2008): TR-03120_Anhang_KTVersiegelung_v102.pdf
[BSI_TL03415]	BSI (Sept. 2005): BSI-TL 03415_Sicherheitsetiketten.pdf
[BSI_TL03400]	BSI (Nov. 2007): BSI-TL 03400_7500_November_2007.pdf