gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Prüfvorgaben / Anforderungen

eHealth-BCS-Kartenterminal

Version:	0.9.0
Stand:	29.02.2008
Status:	freigegeben

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich um eine Erstveröffentlichung.

Referenzierung

Die Referenzierung in weiteren Dokumenten der gematik erfolgt unter:

[gemAnf_BCS] gematik (29.02.2008): Einführung der Gesundheitskarte - Prüfvorgaben/Anforderungen eHealth-BCS-Kartenterminal Version 0.9.0

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.0.5	27.02.08		Ersterstellung	ZUL
0.0.6	28.02.08		Überarbeitung nach Kommentierung	ZUL
0.9.0	29.02.08		freigegeben	gematik

Inhaltsverzeichnis

1 Zusammenfassung

Für die weitergehenden Testmaßnahmen und der Einführung der eGK und der damit im Vorfeld verbundenen Infrastrukturmaßnahmen, sind in der Regel die Ausstattung der Praxen der Leistungserbringer mit entsprechenden Infrastrukturkomponenten (Kartenlesegräte, Konnektoren) sowie die Anpassung der installierten Primärsysteme (Verwaltungssysteme für die Praxen bzw. teilnehmenden Institutionen) hinsichtlich der Nutzung und Verarbeitung der neuen eGK, eine grundlegende Voraussetzung.

Abhängig von den funktionalen Anforderungen hinsichtlich der Einführung der eGK ergeben sich unterschiedliche Anforderungen an die dezentralen Infrastrukturkomponenten, insbesondere für die Ausstattung mit Kartenlesegeräten. Dabei wird nach folgenden Typen unterschieden:

- Kartenlesegeräte (MKT) mit direktem Anschluss an die Primärsysteme
- Migrationsfähige Kartenlesegeräte (ehealth-BCS-Kartenterminal) mit direktem Anschluss an die Primärsysteme
- Kartenlesegeräten (eHealth Kartenterminal) mit indirektem Anschluss (LAN) über einen Konnektor an die Primärsysteme

Um allen Anforderungen gerecht zu werden, wird die gematik bis auf weiteres alle zuvor genannten Typen von Kartenlesegeräten zulassen. Die mit der Zulassung verbundenen Prüfvorgaben und Anforderungen, werden im Folgenden kurz erläutert.

Aus den zuvor genannten Aspekten ergeben sich zusätzliche Anforderungen an ein eHealth-BCS-Kartenterminal, die über die eHealth Spezifikation [gemSpec KT] hinausgehen. Die hier formulierten Anforderungen referenzieren auf, erweitern oder konkretisieren die eHealth Spezifikation [gemSpec KT], so dass ein Höchstmaß an Interoperabilität sichergestellt wird. Hervorzuheben ist, dass die Kernfunktionalität der Kartenterminals, unabhängig vom jeweiligen Einsatzgebiet, immer gleich bleibt: eine performante, fehlerfreie Kommunikation zur Chipkarte MUSS ermöglicht werden und die notwendigen Sicherheitsfunktionalitäten MÜSSEN abgebildet sein. Darüber hinaus bleibt den verschiedenen Herstellern die Möglichkeit mit zusätzlichen Komfortcharakteristiken differenzierende Faktoren zu schaffen.

Das vorliegende Dokument beschreibt die Prüfvorgaben und Anforderungen an ein eHealth-BCS-Kartenterminal. Es ersetzt in diesem Fall eine eigene Spezifikation. In den hier aufgeführten Prüfvorgaben und Anforderungen wird jeweils auf die zugrunde liegenden Spezifikationen und mit geltenden Dokumente (z. B. technische Richtlinien) Bezug genommen. Darüber hinausgehende besondere und/oder zusätzliche Vereinbarungen bzw. Festlegungen werden gesondert dargestellt.

2 Einführung

2.1 Zielsetzung und Einordnung des Dokumentes

Um die Interoperabilität zwischen den verschiedenen Komponenten innerhalb der Telematikinfrastruktur im Gesundheitswesen sicherzustellen und alle funktionalen und nicht-funktionalen Anforderungen abzubilden, beschreibt dieses Dokument die Prüfvorgaben und Anforderungen für die im Gesundheitswesen - in Verbindung mit der elektronischen Gesundheitskarte – für den Einsatzbereich einzusetzenden eHealth-BCS-Kartenterminals.

Als Grundlage dieses Dokuments gilt die eHealth Spezifikation [gemSpec KT] sowie die dazugehörende SICCT-Spezifikation (Secure Interoperable Chip-Card Terminal) [SICCT] der TeleTrusT. Darauf aufbauend werden die speziellen und abweichenden Anforderungen beschrieben.

2.2 Zielgruppe

Das Dokument wendet sich an die Hersteller von Kartenterminals für den Einsatz im Deutschen Gesundheitswesen, an die Hersteller von eHealth-Konnektoren und an die zuständigen Prüf- und Zulassungsstellen, sowie an die Leistungserbringer mit ihren Administratoren und die Primärsystemhersteller mit ihren Servicekräften.

2.3 Geltungsbereich

Die hier getroffenen Festlegungen sind für den Einsatzbereich des eHealth-BCS Kartenterminals im Rahmen des geplanten Basis Roll-Outs sowie angrenzender Systeme, welche über die hier definierten Schnittstellen mit dem Kartenterminal interagieren, in der Telematikinfrastruktur des deutschen Gesundheitswesens verbindlich.

2.4 Arbeitsgrundlagen

Grundlage dieses Dokuments sind die §§ 291 und 291a des SGB V, SigG und SigV sowie die Rechtsverordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte.

Das Kartenterminal basiert auf der eHealth Spezifikation [gemSpec KT], welche durch additive und subtraktive Vorgaben in diesem Kontext für den Betrieb als eHealth-BCS-Kartenterminal in diesem Dokument eingeschränkt wird. eHealth-BCS Kartenterminals für den Einsatzbereich in der Telematikinfrastruktur des deutschen Gesundheitswesens MÜSSEN sich konform zu diesem Dokument und den durch dieses Dokument referenzierten Spezifikationen verhalten.

2.5 Abgrenzung des Dokumentes

Für globale Anforderungen an multifunktionale Kartenterminals wird auf die eHealth Spezifikation [gemSpec KT] verwiesen. Für spezielle Anforderungen gilt dieses Dokument.

Die eHealth Spezifikation [gemSpec KT] dient dabei als Basisdokument und

- orientiert sich an frei verfügbaren internationalen Standards,
- beschreibt technische Spezifikationen der Kommunikationsebene(n) und
- beschreibt grundlegende Sicherheitsanforderungen.

Dieses Zusatzdokument

- beschreibt besondere funktionelle Anforderungen an ein eHealth-BCS Kartenterminal,
- gibt besondere sicherheitstechnische Anforderungen vor und
- beschreibt technisch notwendige Maßnahmen für eine gleichzeitige Nutzung von bestehenden Systemen basierend auf der Krankenversichertenkarte (KVK) und neuen Diensten der Telematikinfrastruktur für das Gesundheitswesen auf Basis der eGK während einer befristeten Übergangszeit (Migration).

2.6 Notationen

Für die genauere Unterscheidung zwischen normativen und informativen Inhalten werden die dem RFC 2119 [RFC2119] entsprechenden in Großbuchstaben geschriebenen, deutschen Schlüsselworte verwendet:

- **MUSS** bedeutet, dass es sich um eine absolutgültige und normative Festlegung bzw. Anforderung handelt.
- **DARF NICHT** bezeichnet den absolutgültigen und normativen Ausschluss einer Eigenschaft.
- **SOLL** beschreibt eine Empfehlung. Abweichungen zu diesen Festlegungen sind in begründeten Fällen möglich.
- **SOLL NICHT** kennzeichnet die Empfehlung, eine Eigenschaft auszuschließen. Abweichungen sind in begründeten Fällen möglich.
- **KANN** bedeutet, dass die Eigenschaften fakultativ oder optional sind. Diese Festlegungen haben keinen Normierungs- und keinen allgemeingültigen Empfehlungscharakter.

3 Anforderungen und Annahmen (eHealth-BCS-KT)

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. Funktional soll durch solche Geräte ausschließlich das Auslesen der Versichertendaten (VSD) von der eGK durch Primärsysteme und Kartenlesegeräte unterstützt werden.

Neben der eGK-Funktionalität muss weiterhin das Lesen der Krankenversichertenkarte (KVK) sichergestellt sein. Dazu muss ein, den Sicherheitsanforderungen entsprechendes, KV-Modul Bestandteil der Kartenlesegeräte bzw. der zugehörigen API sein und unterstützt werden.

Aus diesen Gesichtpunkten lassen sich drei Gruppen von Anforderungen herausarbeiten:

- Funktionale Anforderungen
- IT-Sicherheitstechnische Anforderungen
- Elektrische / physikalische Anforderungen

3.1 Funktionale Anforderungen

In den folgenden Punkten sind die funktionalen Anforderungen zu den SICCT-, KVK- und eGK-Funktionalitäten aufgeführt:

- eHealth-BCS-Kartenterminals MÜSSEN migrationsfähige Kartenlesegeräte sein. Migrationsfähig sind in diesem Kontext solche Kartenlesegeräte, die den technischen Anforderungen der gültigen eHealth Spezifikation [gemSpec_KT] genügen, darüber hinaus zusätzlich eine USB- bzw. V24-Schnittstelle unterstützen sowie mit einem Upgrade ohne Austausch der Geräte zu einem vollwertigen LAN-fähigen "eHealth KT" aufgerüstet werden können (eHealth Spezifikation [gemSpec_KT]). Dieses setzt eine Zertifizierungsfähigkeit (z.B. durch Antrag auf Zertifizierung beim BSI oder eine Bestätigung durch das BSI) voraus.

  Kartenlesegeräte auf dieser Basis MÜSSEN an der V.24- und/oder USB-Schnittstelle mindestens den „Basis Command Set (BCS)“ unterstützen und werden in diesem Kontext als „ehealth-BCS-Kartenterminal“ bezeichnet.

- Gleichzeitig MUSS das Kartenterminal bzw. die zughörige API eine komplette Implementierung des KVK-Moduls zum Handling der Versichertendatenobjekte besitzen.

- Der Basic Command Set 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).

- Die anwendungsbezogene Interoperabilität (KVK-Anwendung und eGK-Anwendung) MUSS in einem Funktionstest bestätigt werden, der von der gematik durchgeführt wird. Hier werden die APDUS bzw. der BCS in anwendungsspezifischem Kontext genutzt.

3.2 IT-Sicherheitstechnische Anforderungen

Die Anforderungen zur IT-Sicherheit sind in dem folgenden Kapitel zusammengefasst:

3.2.1 Informationssicherheit

- Es MUSS wegen der Implementierung eines KVK-Moduls eine Sicherheits-überprüfung 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 Verfahren mit einer neuen Firmware aufgerüstet werden. Dieses Upgradeverfahren für eHealth-BCS Kartenterminals MUSS vom BSI evaluiert werden und zertifizierungsfähig sein.
- Die Migrationsfähigkeit setzt eine Beantragung auf Zertifizierung der Bauart (HW) beim BSI auf Basis der aktuellen Protection Profile voraus.
- Ein Nachweis der QES-Fähigkeit des eHealth-BCS Kartenterminals ist NICHT für die erste Migrationsstufe im Basis-RollOut Voraussetzung.

3.3 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:

3.3.1 Schnittstelle zur Chipkarte

- Die elektrischen Eigenschaften und die Ansteuerung von Prozessorkarten (T=1) MUSS konform zur ISO/IEC 7816-3 sein.
- Chipkarten MÜSSEN mit synchroner Übertragung zum Betrieb einer Versichertenkarte (KVK) unterstützt werden.

3.3.2 Schnittstelle zum Host

- Eine steckerkompatible V.24-Lösung oder eine USB-Anbindung über einen CT-API-Treiber MUSS vorhanden sein. Hierzu werden Konformitätsprüfungen (V.24, T=1 oder CT-API) durchgeführt (siehe www.ct-api.de). Der BCS MUSS an einer dieser Schnittstellen unterstützt werden.
- Eine LAN-Schnittstelle MUSS zum Anschluss an den Konnektor vorhanden sein.

3.3.3 Physikalische Sicherheit - GS

- In Arztpraxen MUSS als Schutz für Leib und Leben nachgewiesen werden, dass kein gefährlicher Zustand eintreten kann. Beim Betrieb von Niedervoltanlagen reicht eine Nutzung eines GS-geprüften Steckernetzteils aus. Die Verwendung ist vom Hersteller nachzuweisen.

3.3.4 Physikalische Sicherheit - EMV/CE

- Die Geräte DÜRFEN gemäß EMV-Gesetz vom 18.09.1998 keine Störstrahlung aussenden, bzw. DÜRFEN NICHT störempfindlich sein. Ein analoger Nachweis nach EMVG ist statthaft. Dieses ist Teil der CE-Konformitätsverfahren, die in diesem Fall durch eine Dokumentation der durchgeführten Prüfungen vom Hersteller nachzuweisen ist.

3.3.5 Physikalische Sicherheit - Klima

Als normaler Einsatzort für das eHealth KT wird hier ein Büroraum / ein Behandlungsraum spezifiziert. Davon abweichende Einsatzorte, insbesondere im Außenbereich, MÜSSEN die Funktionsfähigkeit unter strengeren Umweltbedingungen gewährleisten. In diesen Fällen sind gegebenenfalls von den nachfolgend aufgeführten Anforderungen abweichende Umweltbedingungen gesondert zu vereinbaren.

- Trockene Wärme (Dry Heat) nach IEC 68-2-2 Methode Bb wird für die Bedingungen als obere Lagertemperatur von 55°C und einer Beanspruchungsdauer von 16 h geprüft und die Funktionsfähigkeit MUSS bestätigt werden.
- Kälte (Cold) nach IEC 68-2-1 Methode Ab wird für die Bedingungen als untere Lagertemperatur von -10°C und einer Beanspruchungsdauer von 16 h geprüft und die Funktionsfähigkeit MUSS bestätigt werden.
- Nach den beiden oben genannten Belastungen durch extreme Lagertemperaturen und der Nachbehandlungsdauer von 1 h MUSS die Funktionsfähigkeit des Kartenterminals gewährleistet sein, was durch Funktionsprüfungen nachzuweisen ist.
- Die Funktionsfähigkeit im Betrieb MUSS bei einer oberen Temperatur von 40°C über eine Dauer von 2 h gewährleistet sein. Dies wird für das

Kartenterminal durch Prüfung nach IEC 68-2-2 Methode Bb bei gleichzeitigen Funktionsprüfungen nachgewiesen.

3.3.6 Physikalische Sicherheit - Vibration

Die durch Vibrationen und mechanische Schockbelastungen auftretenden Belastungen MÜSSEN vom Kartenterminal schadensfrei gemäß IEC 68-2 Methode nach den folgenden Anforderungen absolviert, geprüft und nachgewiesen werden:

- 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 8 h je Achse MÜSSEN erfolgreich nachgewiesen werden. Bis zu einer Frequenz von 9 Hz wird dabei mit einer konstanten Amplitude von 1,5 mm belastet, darüber bis zur oberen Frequenz wird mit einer konstanten Beschleunigung von 5 m/s^2 (0,5 g) belastet.
- Optional MÜSSEN mechanische Schockprüfungen (Shock) nach IEC 68-2-27 Methode Ea in drei senkrecht stehenden Achsen (sechs Richtungen) erfolgreich nachgewiesen werden. Es wird dabei für jede Achse mit 3 positiven und 3 negativen Schocks mit 150 m/s^2 (15 g) Amplitude und einer Dauer von 11 ms belastet.
- Dauerschocktests (Bump) nach IEC 68-2-29 Methode Eb in drei senkrecht stehenden Achsen mit halbsinusförmigen Schocks MÜSSEN erfolgreich nachgewiesen werden. Es wird dabei für jede Achse mit 1000 positiven und 1000 negativen Schocks mit 100 m/s^2 (10 g) Amplitude und einer Dauer von 16 ms belastet.

Anhang A

A1 - Abkürzungen

Tabelle 1 - Abkürzungen

Kürzel	Erläuterung
API	Application Programming Interface
BCS	Basic Command Set
BSI	Bundesamt für Sicherheit in der Informationstechnik
CE	Durch das CE-Zeichen wird von Seiten des Herstellers erklärt, dass grundlegende Sicherheitsanforderungen und alle anzuwendenden Richtlinien bei der Konstruktion von Maschinen nach dem EG-Konformitätsverfahren eingehalten wurden. Das CE-Zeichen ist kein Prüfzeichen, sondern nur eine Aussage des Herstellers im oben genannten Sinne.
ISO	International Standard Organisation
KVK	Krankenversichertenkarte
LAN	Local Area Network
MKT	Multifunktionales Kartenterminal
PP	Protection Profile
SICCT	Secure Interoperable ChipCard Terminal

A2 - Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

A4 - Tabellenverzeichnis

A5 - Referenzierte Dokumente

Tabelle 2 - Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[CC]	BSI (29.09.2006): Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria) http://www.bsi.de/cc/ (zuletzt geprüft am 13.12.2006)
[gemSpec_KT]	gematik (15.02.2008): Einführung der Gesundheitskarte – Spezifikation eHealth-Kartenterminal, Version 2.5.0, www.gematik.de
[ITSEC]	Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), GMBl vom 8. August 1992, S. 545
[RVO2006]	„Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte“ in der Fassung der Bekanntmachung vom 5. Oktober 2006 (Bundesgesetzblatt I (2006) vom 10.10.2006, Seite 2199 ff.).
[SGB V]	BGBl. I S.2477 (20.12.1988): Sozialgesetzbuch, Fünftes Buch
[SigG01]	Bundesgesetzblatt I (2001), S.876: Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz - SigG)
[SigV01]	Bundesgesetzblatt I (2001), S. 3074: Verordnung zur elektronischen Signatur – SigV
[SICCT]	TeleTrust (19.11.2007): SICCT Secure Interoperable ChipCard Terminal, Version 1.2.0

A6 – Mitgeltende Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[MKT]	TeleTrusT MKT Spezifikation 1.0