Herstellererklärung

Die
german telematics GmbH
Rankestrasse 26
D-10789 Berlin

erklärt hiermit gemäß § 17 Abs. 4 Satz 2 SigG[1]
in Verbindung mit § 15 Abs. 5 Satz 1 SigV[2],
dass ihr Produkt:

Chipkartenterminal eHealth GT900 BCS mit der
Firmwareversion: 1.0.10 und der
Hardwareversion: 2.0 / **2.0 SI** / **2.0 SW**

die nachstehend genannten Anforderungen des Signaturgesetzes
und der Signaturverordnung an eine Signaturanwendungskomponente
als Teil-Signaturanwendungskomponente erfüllt. Das Produkt unterstützt somit die Erstellung von qualifizierten elektronischen Signaturen mit Hilfe von Signaturerstellungseinheiten in Form von Signaturkarten und einer Signaturanwendungskomponente.

Berlin, den 07.07.2010

Sandeep S. Jolly, Geschäftsführer

Diese Herstellererklärung in Version 1.3 besteht aus 21 Seiten. Es wird derzeit ein Evaluierungsverfahren gemäß Common Criteria EAL3+ durchgeführt (BSI-DSZ-00594); der Abschluss der Zertifizierung und die Bestätigung gemäß SigG / SigV stehen jedoch noch aus. Um diesen Zeitraum zu überbrücken, wurde diese Herstellererklärung erstellt. Das Produkt Chipkartenterminal eHealth GT900 BCS hat bereits mit dem Datum vom 29.05.2009 eine Zulassung durch die gematik GmbH erhalten.

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 17. Dezember 2009 (BGBl. I S. 3932)

Dokumentenhistorie

Version	Datum	Beschreibung	Autor
1.0	23.12.2009	initiale Version	Jan Mihalyovics
1.1	17.02.2010	Datumsänderungen des Evaluierungszeitraumes nach Rücksprache mit der ausführenden Prüfstelle	Jan Mihalyovics
1.2	24.06.2010	Überarbeitung gemäß Prüfbericht: BNetzA-Prüfbericht-Auszug-german-telematics-eHealth-GT900-BCS-v0.1.pdf	Jan Mihalyovics
1.3	05.07.2010	Überarbeitung gemäß Prüfbericht: BNetzA-Prüfbericht-Auszug-german-telematics-eHealth-GT900-BCS-v0.2.pdf	Jan Mihalyovics

Inhaltsverzeichnis

Diese Seite wurde absichtlich leer gelassen

1 Handelsbezeichnungen

Die Handelsbezeichnung lautet: Chipkartenterminal eHealth GT900 BCS

Auslieferung:	Hardware in den Versionen 2.0 , 2.0 SI oder 2.0 SW mit der darauf installierten Firmware in der Version 1.0.10
Auslieferungsverfahren:	Versand in versiegelter Verpackung
Hersteller:	german telematics GmbH, Berlin
Handelsregisterauszug:	HRB 78255, Amtsgericht Berlin-Charlottenburg

2 Lieferumfang und Versionsinformationen

Produktart	Bezeichnung	Version	Datum	Übergabeform
Hardware	Chipkartenterminal eHealth GT900 BCS	HW V.2.0 HW V.2.0 SI (silber) HW V.2.0 SW (schwarz)	25.06.2009	In versiegelter Verpackung (Hardware mit geladener Firmware)
Zubehör	• USB - Anschlusskabel[3] • Netzteil[3]	-	25.06.2009	In versiegelter Verpackung
Software	Firmware des Chipkartenterminals eHealth GT900 BCS	FW 1.0.10	06.04.2010	In Hardware (s.o.) enthalten
Dokumentation	Benutzerhandbuch zum Chipkartenterminal eHealth GT900 BCS	1.6	14.07.2009	Gedruckt (Auslieferung) sowie als PDF im Internet zum Download und auf Treiber-CD
Software	Treiber-CD zum Chipkartenterminal eHealth GT900 BCS[3]	1.0	25.06.2009	In Verpackung

Tabelle 1: Lieferumfang und Versionsinformationen

[3] Kein Bestandteil des Evaluierungsgegenstandes

Zur Erstellung qualifizierter elektronischer Signaturen werden zusätzlich zu dem in Tabelle 1 genannten Lieferumfang die im Folgenden näher bezeichneten sicheren Signaturerstellungseinheiten, Signaturanwendungskomponenten und Hauptkomponenten benötigt:

- eine durch die Bundesnetzagentur sicherheitsbestätigte Signaturkarte/Signaturerstellungseinheit (bspw.: Signaturerstellungseinheit STARCOS 3.4 Health QES C1 / Registrierungsnummer: BSI.02120.TE.05.2009)
- eine durch die Bundesnetzagentur sicherheitsbestätigte Signaturanwendungskomponente in Form eines sogenannten Anwenderprogrammes (bspw.: Signaturanwenderkomponente SecSigner® Version 2.0.0 / Registrierungsnummer: BSI.02024.TE.03.2002)
- eine sogenannte Hauptkomponente im Folgenden auch als Primärsystem oder Hostsystem bezeichnet, auf welchem die sicherheitsbestätigte Signaturanwendungskomponente als Anwenderprogramm läuft, und an welches das Chipkartenterminal eHealth GT900 BCS physikalisch (z.B. über USB-Kabel) angeschlossen ist (bspw.: Personal Computer mit Betriebssystem Windows XP SP 3). Die Hauptkomponente muss die standardisierte CT-API / MKT Schnittstelle unterstützen.

Eine Auflistung von sicherheitsbestätigten Signaturkarten findet sich auf der Internetpräsenz der Bundesnetzagentur unter:

http://www.bundesnetzagentur.de/cln_1932/DE/Sachgebiete/QES/Produkte/Bestaetigungen/SicherSignaturErstellEinheit_Basepage.html

Eine Auflistung von sicherheitsbestätigten Signaturanwendungskomponenten (Anwenderprogramme) findet sich auf der Internetpräsenz der Bundesnetzagentur unter:

http://www.bundesnetzagentur.de/cln_1932/DE/Sachgebiete/QES/Produkte/Bestaetigungen/Signaturanwendungskomponente_Basepage.html

3 Funktionsbeschreibung

Der Chipkartenleser eHealth GT900 BCS ist ein Chipkartenlesegerät mit einer updatefähigen Firmware, welches Prozessorchipkarten nach ISO/IEC 7816 über eine Applikationsschnittstelle (CT-API) verarbeiten kann. Es ist konform zu den von der gematik GmbH herausgegebenen Richtlinien zum Aufbau einer Telematik -Infrastruktur für das Gesundheitswesen und unterliegt den darin beschriebenen Spezifikationen für eHealth-Kartenterminals **[1]** als dezentrale Komponente. Der EVG ist jedoch aufgrund der Applikationsschnittstelle und des unterstützten BCS-Kommando-Sets in vielen Marktsegmenten einsetzbar. In diesem Zusammenhang ist das Gerät technisch derart ausgelegt, dass ein angeschlossenes Primärsystem mittels einer im Chipkartenterminal gesteckten Signaturkarte (bspw. einem HBA) und einer auf dem Primärsystem installierten Signaturanwendungskomponente eine qualifizierte elektronische Signatur erzeugen kann.

Im Einsatzbereich des eHealth-Kartenterminals im Rahmen der Telematik-Infrastruktur des Deutschen Gesundheitswesens verfügt das Gerät über USB-Schnittstellen vom Typ A und Typ B, über eine RS232/V.24-Schnittstelle, eine Ethernet-LAN-Schnittstelle, zwei SIM-Slots für die SMC-B[4] und die SM-KT (ID-001) sowie über einen Kartensteckplatz für die Patientenkarte (KVK und eGK) und einen Kartensteckplatz für den Heilberufsausweis (HBA / ID000). Es werden alle gängigen Krankenversichertenkarten nach den technischen Spezifikationen **[2]** sowie alle elektronischen Gesundheitskarten (eGK) nach den Spezifikationen **[3]**, **[4]**, **[5]** unterstützt. Zudem unterstützt das Gerät an den zur Verfügung gestellten Schnittstellen den in **[6]** (Abschnitt 5.5.6) definierten Basis Command Set (BCS) für die geplante Einführung der eGK.

Das migrationsfähige Chipkartenterminal unterstützt gängige Betriebssysteme welche die standardisierte CT-API / MKT Schnittstelle unterstützen (z.B. Microsoft Windows ab Win98). Das Chipkartenterminal kann mit allen Host-Systemen betrieben werden, welche eine serielle RS232/V.24 und/oder eine USB-Schnittstelle zur Verfügung stellen. Die RS232/V.24-Schnittstelle ist steckerkompatibel zum B1 Standard **[7]** der Deutschen Telekom AG.

Das zu evaluierende Chipkartenterminal GT900 ist konform zu der vom Bundesministerium für Sicherheit und Informationstechnik (BSI) herausgegebenen Technischen Richtlinie **[9]** sowie dem zugehörigen Anhang **[10]**.

Das zu evaluierende Chipkartenterminal bietet zusammenfassend folgende Hauptfunktionen:

- Zugang zu einem Chipkartenslot jeweils für den HBA und die eGK (ID-000),
- zwei SIM-Slots für die SMC-B und die SM-KT (ID-001),
- sichere PIN-Eingabe,
- Benutzerauthentifizierung und
- die Durchführung eines Fimwareupdates.
- Erstellen qualifizierter elektronischer Signaturen

3.1 EVG-Beschreibung

Das migrationsfähige Kartenlesegerät eHealth GT900 BCS mit RS232/V.24- sowie USB-Schnittstelle (im folgenden EVG genannt) stellt ein Kartenlesegerät dar, welches Patientenkarten (KVK/eGK) und Heilberufsausweise (HBA) nach den Spezifikationen **[2]**, **[3]**, **[4]** und **[5]** in zwei dafür vorgesehenen Chipkartenslots verarbeiten kann. Das Gerät arbeitet mit allen in diesen Spezifikationen geforderten

[4] Die Institutionsidentität ist eine durch eine SMC-B repräsentierte Identität der Institution des Leistungserbringers bzw. einer Organisationseinheit in einer solchen Institution. Beispiele für solche Organisationseinheiten sind einzelne Arztpraxen innerhalb einer Praxisgemeinschaft. Die Institutionskarte entspricht technisch weitgehend der Health Professional Card (HBA), ist jedoch institutionsbezogen und wird lediglich bei Systemstart mit einer PIN freigeschaltet. In diesem Fall wird sie auch als Security Module Card (SMC) bezeichnet. Die Institutionskarte funktioniert nur in Verbindung mit einem HBA.

Datenübertragungsprotokollen. Das Chipkartenlesegerät unterstützt die anwendungsbezogene Interoperabilität, die durch die Spezifikation **[11]** definiert wurde.

Eine durch einen Benutzer eingegebene PIN verlässt den Chipkartenleser nie in Richtung Host. Der EVG kann an allen Hostsystemen (Hosts) verwendet werden, die eine serielle RS232/V.24- bzw. eine USB-Schnittstelle besitzen. Als Hostsysteme werden auch solche Systeme angesehen, die nach **[1]** und **[11]** als Primärsysteme bezeichnet werden. Das Chipkartenterminal wird im Release 0 als Zubehör im PC-Umfeld eingesetzt. Auf der Hostseite werden vom Kartenlesegerät die Applikationsschnittstellen CT-API **[12]** zur Verfügung gestellt, die für alle o.g. Chipkartenarten genutzt werden können. Alle Funktionalitäten an den Schnittstellen werden für CT-API gemäß **[12]** abgebildet. Der EVG besitzt keine Funktionalität - außer der Updatefunktion im Administrator-Modus, die ohne Anschluss an einen Host arbeitet. Er muss generell an einem Host betrieben werden. Der EVG endet an der seriellen RS232/V.24- bzw. USB-Schnittstelle zum Host-Rechner. Der EVG ist in dieser Release-Phase für einen Einsatz im deutschen Gesundheitswesen konzipiert und dabei bereits insbesondere für einen Einsatz als eHealth Terminal nach **[1]**. Der Funktionsumfang für die Release-Phase 0 wird durch die Spezifikation **[11]** gegeben und erfüllt. Um den Betrieb des EVG zu unterstützen, werden in Release-Phase 0 folgende Hard- bzw. Software benötigt.

- Netzteil (5V ⎓ 1300mA) – im Lieferumfang enthalten
- Treiber zur Installation auf dem Hostsystem – im Lieferumfang enthalten
- Software auf dem Hostsystem zur spezifikationsgemäßen Kommunikation mit dem Chipkartenterminal
- Anschlusskabel zum Anschluss des Chipkartenterminals an das Hostsystem (USB oder RS232) – im Lieferumfang enthalten

Das Gerät verfügt über eine sichtgeschützte Folientastatur. Diese besitzt die numerischen Tasten „0“ bis „9“ sowie die Tasten „Korrektur“ (gelb), „Info“ (blau), „Bestätigung“ (grün) und „Abbruch“ (rot), eine Stern-Taste („*“), eine Raute-Taste („#“) und vier Funktionstasten („F1“ bis „F4“). Desweiteren verfügt das Gerät über ein graphisches LC-Display. Die Stromversorgung erfolgt über einen separaten Anschluss auf der Rückseite des Gerätes.

Der Chipkartenleser wird durch Standardtreiber diverser Betriebssysteme (z.B. Microsoft Windows ab Win98) unterstützt, insofern diese die standardisierte CT-API / MKT Schnittstelle unterstützen. Die Treiber sind jedoch nicht Bestandteil des EVG. Da der Chipkartenleser als Teil der geplanten Telematik-Infrastruktur im deutschen Gesundheitswesen auch in der Lage ist, Identifikationsdaten (PIN) zu erfassen und an sichere Signaturerstellungseinheiten (Signatur-Chipkarten) nach §2 Nummer 10 SigG auf sicherem Weg zu übermitteln, kann er auch für Applikationen gemäß Signaturgesetz und Signaturverordnung eingesetzt werden. Das Chipkartenterminal ermöglicht außerdem die Übertragung des Hash - Wertes einer Signaturanwendung über den Chipkartenleser zur Signaturkarte und die Übertragung der Signatur von der Karte über den Chipkartenleser zurück zur Signaturanwendung auf den Host. Er stellt somit eine Teilkomponente für Signaturanwendungskomponenten dar, die eine Sicherheitsbestätigung benötigen, um für qualifizierte elektronische Signaturen nach §2 Nummer 3 SigG eingesetzt werden zu können. Zur Verwendung des EVG gemäß SigG/SigV sind sowohl Applikationen (Signaturanwendungen) als auch Chipkarten, die im SigG-Kontext evaluiert und bestätigt wurden, einzusetzen. Der EVG ist dabei nur in der Lage, Einzelsignaturen zu erzeugen.
Der EVG erfüllt die speziellen Anforderungen nach §15 Absatz 2 Nr.1a (keine Preisgabe oder Speicherung der Identifikationsdaten außerhalb der sicheren Signatur-Erstellungseinheit) und Absatz 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV. Nachfolgende Liste der zur sicheren PIN-Eingabe unterstützten Instruction-Bytes ist von den Applikationen zu verwenden und von den Chipkarten spezifikationsgemäß zu unterstützen bzw. bei Nicht-Unterstützung mit einer geeigneten Fehlermeldung abzulehnen:

VERIFY (ISO/IEC 7816-4): INS=0x20
CHANGE REFERENCE DATA (ISO/IEC 7816-8): INS=0x24
ENABLE VERIFICATION REQUIR EMENT (ISO/IEC 7816-8): INS=0x28
DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-8): INS=0x26
RESET RETRY COUNTER (ISO/IEC 7816-8): INS=0x2C

Die sichere Generierung und Verwaltung des für die Erzeugung eines verschlüsselten HASH-Wertes notwendigen Schlüssels zum Schutz eines Firmwareupdates werden durch den Hersteller GT German Telematics GmbH gewährleistet. Wird eine neue, unbestätigte Firmware in den EVG eingespielt, so verliert die Bestätigung nach Signaturgesetz und der Signaturverordnung ihre Gültigkeit. Eine möglicherweise eingereichte Herstellererklärung verliert in diesem Fall auch Ihre Gültigkeit. Eine neue Firmware muss einem neuen Bestätigungs- und Zertifizierungsverfahren unterzogen werden.

Die aktuell bestätigten und zertifizierten Versionen der Firmware und der Hardware des EVG sind auf den Webseiten der Bundesnetzagentur (BNetzA) unter http://www.bundesnetzagentur.de sowie auf den Webseiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unter http://www.bsi.bund.de sowie bei der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) unter http://www.gematik.de abrufbar. Es obliegt der Verantwortung des Benutzers, sich hier vor der Installation einer neuen Firmware davon zu überzeugen, ob eine neu zu installierende Firmware Version nach **[1]**, **[11]** bestätigt und gegebenenfalls nach Common Criteria zertifiziert ist. Die entsprechenden Downloads stellt der Hersteller GT German Telematics GmbH auf seinen Webseiten unter http://www.germantelematics.com bereit. Den Benutzern wird empfohlen, diese Webseiten regelmäßig zu besuchen, um sich über Aktualisierungen zu informieren.

Über einen Administrator-Modus kann die aktuell im EVG befindliche Firmware-Version ausgelesen und wenn nötig, ein Update eingeleitet werden; die Hardware-Version ist auf dem Typenschild des EVG aufgebracht.

Das Gehäuse ist mittels einer fälschungssicheren, durch das BSI zertifizierten Versiegelung verschlossen. Die Versiegelung zerstört sich bei einer Entfernung und ist damit nur einmal verwendbar. Diese Versiegelung ist konform zu **[9]** und **[10]** und besitzt pro Siegel eine Mindestfläche von 10x20 mm. Zudem ist das Gerät durch technische Maßnahmen vor Angriffen geschützt, welche auf einen physikalischen Kontakt mit der Platine des EVG abzielen ohne die Versiegelung des EVG zu beschädigen.

Das Chipkartenterminal unterscheidet verschiedene Benutzerrollen (siehe Abschnitt 3.4) und ist in der Lage insbesondere einen Administrator über eine PIN-basierte Abfrage zu identifizieren und zu authentifizieren. Der Kartenleser zeigt verschiedene Betriebsmodi für unterschiedliche Benutzerrollen mittels eines eingebauten Displays an. Diese sind:

Normal-Modus
In diesem Modus ist das Gerät als Chipkartenleser nach den Vorgaben der gematik GmbH **[1]** nutzbar.

Administrator-Modus
Dieser Betriebsmodus ist durch die Eingabe einer Administratoren-PIN vor unbefugter Benutzung geschützt. Diese PIN ist grundsätzlich geheim und nur dem autorisierten Benutzer – einem Administrator – bekannt. In diesem Modus kann von einem dazu berechtigten Administrator die aktuelle Firmware des EVG angezeigt und aktualisiert werden. Bei einer Aktualisierung der Firmware wird die neu einzuspielende Firmware durch das EVG einer Prüfung unterzogen. Eine Aktualisierung findet nur nach Verifikation der Signatur der neuen Firmware statt. In diesem Modus können zusätzlich alle notwendigen Netzwerkeinstellungen am Chipkartengerät vorgenommen und verändert werden. Über den Administratormodus werden des Weiteren alle relevanten Sicherheitsfunktionen des EVG verwaltet.

Tabelle 2 zeigt eine Auflistung aller durch das Chipkartenlesegerät zur Verfügung gestellten Schnittstellen. Das Chipkartenlesegerät befindet sich gemäß Abschnitt 5.4.5 in einem geschützten Einsatzbereich, folglich werden die in Tabelle 2 benannten Schnittstellen auch nur in diesem geschützten Einsatzbereich genutzt.

Schnittstelle	Beschreibung	Absicherung
USB Typ A	Zum Anschluss eines Massenspeichergerätes, um ein Firmware-Update durchzuführen	• Funktionslos im Normal-Modus. Nur autorisierte Benutzer (Administratoren) können die Schnittstelle verwenden um ausschließlich Firmware-Updates durchzuführen.
Ethernet LAN	Zum Anschluss des EVG an ein Netzwerk	• Schnittstelle ist für den hier betrachteten EVG mit der Firmwareversion 1.0.10 funktionslos[5].
2 SIM Slots	Zum Einlegen von sogenannten Sicherheitsmodulkarten (SMC)	• Schnittstelle ist für den hier betrachteten EVG mit der Firmwareversion 1.0.10 funktionslos[5].
Kartensteckplatz für eine Patientenkarte	Kontaktiereinheit für eine Chipkarte im Format ID-000	• Kommandoüberprüfung sowie spezifikationsgemäße Kommunikation
Kartensteckplatz für einen Heilberufsausweis	Kontaktiereinheit für eine Chipkarte im Format ID-000	• Kommandoüberprüfung sowie spezifikationsgemäße Kommunikation
RS232 Schnittstelle	Serielle Schnittstelle zum Host	• Es werden ausschließlich BCS-Kommandos verarbeitet
USB Typ B	USB Schnittstelle zum Host	• Es werden ausschließlich BCS-Kommandos verarbeitet
LC-Display	Monochromes Grafikdisplay	• Keine Bidirektionale Kommunikation mit dem Benutzer des EVG möglich • Art der Implementierung und Steuerung von angezeigten Informationen
Applikations-schnittstelle (CT-API)		• spezifikationsgemäße Kommunikation

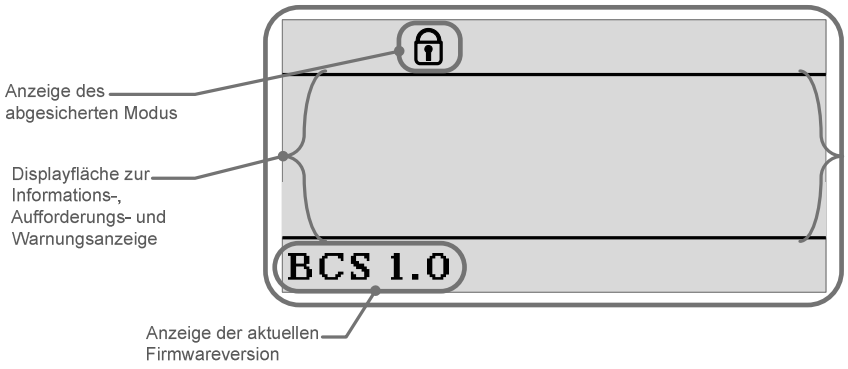
Tabelle 2: Schnittstellen des EVG

[5] Die Bezeichnung „funktionslos“ bezieht sich hier auf die Tatsache, dass die Schnittstelle physikalisch vorhanden, durch die Firmware des EVG jedoch nicht genutzt wird. Funktionslose Schnittstellen sichern die Migrationsfähigkeit des Chipkartenlesegerätes GT900 BCS zu einem vollwertigen eHealth-Terminal, so wie es durch die gematik GmbH spezifiziert wurde. Demnach werden diese Schnittstellen durch ein zukünftiges Firmwareupdate freigeschaltet und dann auch durch die neu eingespielte Firmware genutzt.

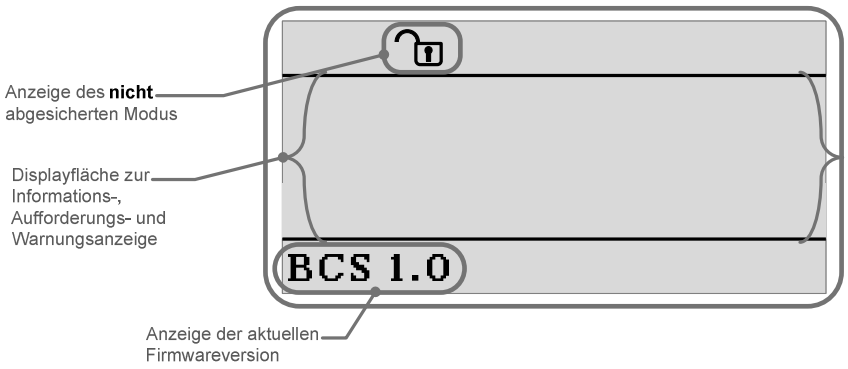
Der Chipkartenleser demonstriert verschiedene Betriebszustände mittels seines Displays wie folgt:

EVG befindet sich in einem abgesicherten Betriebszustand und ermöglicht somit:

Die Sichere Eingabe der PIN



EVG befindet sich in einem **nicht** abgesicherten Betriebszustand



Durch die Anzeige des geschlossenen Schlosssymbols im Display des EVG ist dem Anwender bewusst, dass sich der EVG nun in einem abgesicherten Betriebszustand befindet und somit eine sichere Eingabe einer PIN als Bestandteil der Durchführung einer qualifizierten elektronischen Signatur möglich ist.

3.2 Physikalischer Umfang des EVG

Der EVG ist ein freistehendes Kartenterminal und besteht aus:

- der Hardware und dem versiegeltem Gehäuse des Chipkartenterminals eHealth GT900 BCS hergestellt von der GT German Telematics GmbH,
- den bereitgestellten Schnittstellen eGK, HBA, SMC-B, SM-KT (ID-000), USB, RS232, Display, Folientastatur,
- der Firmware des Chipkartenterminals in der Version 1.0.10

sowie den Benutzerdokumentationen des Gerätes.

3.3 Logischer Umfang des EVG

Der logische Umfang des EVG wird durch seine Sicherheitsfunktionen repräsentiert:

- Zugang zu mehreren Chipkartenslots für Smart Cards,
- sichere PIN-Eingabefunktionalität,
- Benutzeridentifikation und -authentifizierung,
- Durchführung einer sicheren Firmware-Aktualisierung,
- Passiver physikalischer Schutz.

3.4 Rollentrennung

Der EVG unterscheidet folgende Rollen (Endanwender):

Benutzer:

Für einen normalen Benutzer des EVG wird keine gesonderte Identifikation oder Autorisierung vorgenommen. Nach dem Einschalten steht der EVG daher im Normal-Modus für jeden Benutzer zur Verfügung. In diesem Modus ist das Gerät als Chipkartenleser nutzbar. Benutzer können beispielsweise medizinisches Personal oder Patienten im Rahmen der Nutzung des Gerätes innerhalb der Telematikinfrastruktur im deutschen Gesundheitswesen sein.

Administrator:

Ein Benutzer kann sich durch das Drücken der F1-Taste im Normal-Modus als Administrator identifizieren, indem er aufgefordert wird eine Admin-PIN in das Gerät einzugeben (Autorisierung) und daraufhin in den Administrator-Modus verzweigt wird. Bei Administratoren handelt es sich um geschultes IT-Personal, das berechtigt ist Änderungen an den Einstellungen des Chipkartenterminals vorzunehmen.

Alle von diesen Rollen abweichenden Nutzer werden im Folgenden auch als nicht autorisierte Personen bezeichnet. Nicht autorisierte Personen besitzen ein Angriffspotential gegenüber dem Chipkartenlesegerät.

4 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

Das Chipkartenterminal GT 900 BCS stellt einen Teil der Signatur-Anwendungs-Komponente gemäß §2 SigG **[14]** dar:

- „Im Sinne dieses Gesetzes sind [...] 11. ‚Signaturanwendungskomponenten' Software- und Hardwareprodukte, die dazu bestimmt sind, a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder b) [...]"

und entspricht den Anforderungen des §15 SigV **[15]**:

- Abs. 2: „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass 1. bei der Erzeugung einer qualifizierten elektronischen Signatur a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden [...]" Diese Anforderung wird durch folgende Sicherheitsfunktionen abgedeckt:
  SF.CLRMEM
  SF.PINCMD

- Abs. 2: „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass 1. bei der Erzeugung einer qualifizierten elektronischen Signatur b) eine Signatur nur durch die berechtigt signierende Person erfolgt [...]" Diese Anforderung wird durch folgende Sicherheitsmaßnahmen abgedeckt:
  Die Authentifizierung gegenüber der sicheren Signaturerstellungseinheit kann nur durch die PIN(Identifikationsdaten)-Eingabe des Signaturschlüsselinhabers direkt über die Tastatur des Kartenlesegerätes erfolgen. Eine Eingabe der PIN über bspw. die Computertastatur des Hostsystems ist nicht möglich.
  Eine Weitergabe des PIN an andere Personen als an den Signaturschlüsselinhaber ist nicht zulässig. Durch die im Folgenden definierten Einsatzbedingungen/ -umgebung haben nur berechtigte Personen Zugang zu der Teilsignaturanwendungskomponente. Aufgrund dessen können auch nur berechtigte Personen die Erzeugung von Signaturen veranlassen.

- Abs. 2: „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass 1. bei der Erzeugung einer qualifizierten elektronischen Signatur c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird [...]" Diese Anforderung wird durch folgende Sicherheitsfunktionen abgedeckt:
  SF.PINCMD (durch Steuerung der Anzeige des abgesicherten Betriebszustandes)

- Abs. 4: „Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden." Diese Anforderung wird durch folgende Sicherheitsfunktionen abgedeckt:
  SF.SEAL
  SF.DRILLSEC
  SF.SECDOWN

Das Chipkartenterminal GT 900 BCS erfüllt des Weiteren die Anforderungen des Signaturgesetzes nach § 17 Abs. 2 Satz 1:

- „Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen […]"

durch die Tatsache, dass dem Benutzer vor der Eingabe seiner PIN zum Durchführen einer qualifizierten elektronischen Signatur ein sicherer Betriebszustand des EVG durch ein Schlosssymbol im Display des Chipkartenlesers angezeigt wird.

4.1 Erläuterung der Sicherheitsfunktionen

4.1.1 SF.PINCMD

Die Firmware im Lesegerät prüft die Kommandos an den Chipkartenleser anhand ihrer Kommandostruktur gemäß CT-BCS **[12]**. Das Einschalten des sicheren PIN-Eingabemodus wird durch ein explizites CT-Kommando nach **[12]** durchgeführt. Dieses CT-Kommando enthält die PIN-Handling-Vereinbarungen und das Chipkartenkommando, in welches die PIN an die spezifizierte Stelle integriert wird. Anhand des Instruction-Bytes des Chipkartenkommandos wird überprüft, ob es sich um ein PIN-Kommando handelt (siehe Tabelle), welches explizit eine PIN-Eingabe erwartet. Im PIN-Eingabemodus wird die Eingabe der persönlichen Identifikationsdaten im RAM zwischengespeichert, um sie nach erfolgreicher Beendigung der Eingabe direkt mit dem PIN-Kommando zur Chipkarte zu senden. Die RS232/V.24-, die USB- und die LAN-Schnittstellenanbindung des EVG unterscheiden sich lediglich im Protokoll-Anbindungs-Modul an den Host, so dass bei allendrei Host-Interface-Varianten ein identischer Datenstrom durch die Sicherheitsfunktion bearbeitet wird, wodurch nur zugelassene Kommandos an die Chipkarte weitergeleitet werden. Das LC-Display des Chipkartenterminals zeigt den Modus der „Sicheren PIN-Eingabe“ durch ein Schlosssymbol an, indem sichergestellt ist, dass die PIN den EVG nicht verlässt. Ein offenes Schlosssymbol bedeutet „keine sichere PIN-Eingabe“, ein geschlossenes Schlosssymbol bedeutet „sichere PIN-Eingabe“. Die PIN selbst wird am Display nicht angezeigt Die PIN wird vom Benutzer über die Tastatur eingegeben und an die Chipkarte exportiert. Dem Benutzer wird dabei im LC-Display angezeigt, an welche Chipkarte die PIN exportiert wird.

INS- Byte:	Bezeichnung:	Bedeutung:	Norm:
20h	VERIFY	PIN-Eingabe	ISO/IEC 7816-4
24h	CHANGE REFERENCE DATA	PIN ändern	ISO/IEC 7816-8
26h	DISABLE VERIFICATION REQUIREMENT	PIN aktivieren	ISO/IEC 7816-8
28h	ENABLE VERIFICATION REQUIREMENT	PIN deaktivieren	ISO/IEC 7816-8
2A	PERFORM SECURITY OPERATION		ISO/IEC 7816-8
2Ch	RESET RETRY COUNTER	PIN entsperren	ISO/IEC 7816-8

Das Vorhandensein einer Chipkarte im Slot 1 oder im Slot 2 des EVG wird dem Benutzer eindeutig im Display angezeigt. Der Zugriff auf eine Chipkarte im Slot 1 oder im Slot 2 des EVG wird dem Benutzer eindeutig im Display angezeigt.

4.1.2 SF.CLRMEM

Speicherbereiche, die zur PIN-Speicherung verwendet wurden, werden durch Überschreiben mit 0x0000 wiederaufbereitet, sobald die PIN nicht mehr benötigt wird. Dies sind insbesondere:

- Einschalten,
- Weiterleiten eines PIN-Kommandos,
- Ziehen der Chipkarte und
- Abbruch der PIN Eingabe

4.1.3 SF.SECDOWN

Eine neue Firmware kann von einem dazu berechtigten Administrator im Administrator-Modus in den EVG eingespielt werden. Die zu einem neuen Firmwarestand gehörenden Dateien umfassen:

- Firmwaredatei
- Signaturdatei

Die Firmwaredatei ist mit einer Signatur des Herstellers versehen. Diese Signatur stellt die Integrität (über die Hash -Funktion) und Authentizität (über den verwendeten Schlüssel) sicher.
Ein abgebrochenes Firmwareupdate wird vom EVG erkannt, welcher daraufhin eine Fehlermeldung ausgibt. Nach einer erfolgreichen Benutzerautorisierung wird der Updatevorgang erneut angestoßen. Ein Abbruch des Updatevorganges durch den Benutzer ist an dieser Stelle nicht mehr möglich. Auch dann nicht, wenn das Einspielen eines neuen Firmwarestandes mehrfach nicht erfolgreich war. Die Verifikation der Integrität und Authentizität erfolgt im EVG durch Vergleich des ermittelten Hash-Wertes und des Hash-Wertes als Bestandteil der entschlüsselten Signatur. Der öffentliche Schlüssel für die Entschlüsselung der Signaturdatei wurde werksseitig im EVG gespeichert.

4.1.4 SF.DRILLSEC

Die SF.DRILLSEC misst die physikalischen Eigenschaften von Sensoren, welche im EVG verbaut sind, vergleicht diese mit Sollwerten bzw. prüft auf diskrete Fehlerzustände. Diese Sicherheitsfunktion ist während des Betriebes des EVG aktiv und überwacht den EVG permanent.

4.1.5 SF.SEAL

Das Gehäuse des EVG ist durch eine Versiegelung so verschlossen, dass es ohne eine Beschädigung der Versiegelung nicht geöffnet werden kann. Die Versiegelung ist so beschaffen, dass eine Ablösung vom Untergrund (also vom Gehäuse) nicht ohne erkennbare Beschädigung der Versiegelung möglich ist. Die Siegel sind durch das BSI evaluiert. Der Benutzer wird in der Benutzerdokumentation darüber belehrt, die Unversehrtheit der Versiegelung vor jeder PIN-Eingabe zu kontrollieren und das Gerät im Falle einer beschädigten Versiegelung nicht weiter zu benutzen.

Durch organisatorische und vertragliche Maßnahmen ist sichergestellt, dass die Siegel nur im Rahmen der regulären Produktion von german telematics Chipkartenterminals eingesetzt werden und Dritten nicht zur Verfügung stehen.

Die Sicherheitsfunktion SF.SECDOWN beruht auf kryptographischen Wahrscheinlichkeits-Mechanismen. SF.SEAL basiert auf einem Mechanismus der mechanischen Versiegelung, die hohem Angriffspotential widersteht.

5 Maßnahmen an die Einsatzumgebung

5.1 Einrichtung der IT-Komponenten

Um mit Hilfe des EVG qualifizierte elektronische Signaturen durchführen zu können, muss dieser an einem Hostsystem betrieben werden, auf welchem eine Signaturanwendungskomponente in Form eines Anwenderprogrammes installiert ist. Das Hostsystem muss zudem die standardisierte CT-API / MKT-Schnittstelle unterstützen. Des Weiteren muss eine Signaturerstellungseinheit in Form einer Signaturkarte im Format ID-000 in einer der beiden Chipkartenkontaktiereinheiten gesteckt sein (siehe auch Abschnitt 2).

Das Chipkartenterminal GT900 BCS darf ausschließlich innerhalb der in Abschnitt 2 beschriebenen Hard- und Softwareausstattung zum Einsatz kommen.

5.2 Anbindung an ein Netzwerk

Ein direkter Anschluss des EVG an ein Netzwerk ist nicht vorgesehen. Dennoch können Anforderungen an die Netzwerkumgebung aus Anforderungen des Pimärsystems, der Signaturanwendungskomponente (Anwendersoftware) oder der Signaturerstellungseinheit resultieren. Diese sind dann umzusetzen.

5.3 Auslieferung und Installation

Die Auslieferung erfolgt durch „Versand“ oder „Download“. Bei der Auslieferungsart „Versand“ ist die Treibersoftware auf dem Hostsystem zu installieren. Im Auslieferungsweg „Download“ ist die heruntergeladene Firmware in den EVG einzuspielen.

Die Auslieferung des eHealth GT900 Chipkartenterminals geschieht auf zwei Wegen: durch die Auslieferungsart „Versand“ mit einer darin enthaltenen Firmware, die bei der Produktion eingebracht wird, und der Möglichkeit zum Update der Firmware durch ein gesichertes Software-Update, um für zukünftige Anforderungen vorbereitet zu sein. Das Softwareupdate kann auch durch die Auslieferungsart „Download“ bezogen werden.

Zum Lieferumfang des Produktes eHealth GT900 Chipkartenterminal gehören im Auslieferungsweg „Versand“ neben dem Chipkartenterminal mit vorinstallierter Firmware noch eine gedruckte Benutzeranleitung sowie eine Treiber-CD und Anschlusszubehör. In dem Auslieferungsweg „Download“ besteht der Lieferumfang aus der Firmware und einer Ergänzung zur Benutzerdokumentation mit Hinweisen für die korrekte Installation einer aktualisierten Firmware..

Durch die Verifikation der Signatur der Firmware wird die Integrität und Authentizität der Firmware beim Laden der Firmware in den Chipkartenleser garantiert. Die Signatur der neu zu installierenden Firmware ist mit dem asymmetrischen RSA-Kryptosystem, verschlüsselt und kann mit Hilfe eines im EVG abgelegten PublicKey decodiert werden. Nach einer erfolgreichen Signatur-Überprüfung der neuen Firmware kann diese installiert werden. Die Signatur-Prüfung wird dabei innerhalb des EVG von dessen aktueller Firmware durchgeführt. Nur nach erfolgreicher Signatur-Prüfung wird die neue Firmware aktiviert, andernfalls wird sie abgewiesen. Bei einer fehlerhaften oder nicht authentischen Übertragung der Firmware wird der Updatevorgang abgewiesen und keinerlei Veränderungen an der zertifizierten Softwareversion vorgenommen. Der Hersteller GT german telematics GmbH stellt eine Anleitung bereit, welche die Übertragung einer neuen Firmware an den EVG beschreibt, so dass er von Administratoren selbstständig vorgenommen werden kann.

Ausführliche Informationen zur Installation sowie zum Einspielen einer neuen Firmware in das Gerät finden sich im Benutzerhandbuch des eHealth GT900 Chipkartenterminals. Zusätzlich werden auf der Homepage des Herstellers unter www.germantelematics.de/ehealth-gt900 ausführliche Informationen sowie eine Erweiterung zum Benutzerhandbuch zur Verfügung gestellt, in welcher die Durchführung von qualifizierten elektronischen Signaturen mit dem Chipkartenterminal eHealth GT900 BCS beschrieben wird.

5.4 Auflagen für den Betrieb des Produktes

5.4.1 OE.USER.RESP1:
Die Regeln zur sicheren Handhabung und Nichtweitergabe der PIN müssen dem Benutzer vom Herausgeber der Signaturchipkarte (Signaturerstellungseinheit) mitgeteilt werden, insbesondere die unbeobachtete Eingabe der PIN.

5.4.2 OE.USER.RESP2:
Während der PIN-Eingabe über die Tastatur des Chipkartenlesegerätes muss der Benutzer die Anzeige im LC-Display dahingehend überprüfen, dass der Modus der sicheren PIN-Eingabe aktiv ist (Schlosssymbol im Display).

5.4.3 OE.USER.RESP3:
Zertifizierte bzw. bestätigte Firmware, die von der german telematics GmbH zum Download angeboten wird, muss durch Angabe der Zertifizierungs- bzw. Bestätigungs-IDs gekennzeichnet sein. Der Administrator muss sich vor der Installation einer neuen Firmware davon überzeugen, dass diese nach SigG/SigV bestätigt und nach Common Criteria zertifiziert ist.

5.4.4 OE.USER.RESP4:
Der Benutzer muss die Geräteversiegelung vor jeder PIN-Eingabe auf Unversehrtheit hin überprüfen.

5.4.5 OE.USER.RESP5:
Der EVG darf ausschließlich in einem geschütztem Einsatzbereich, wie zum Beispiel einer Arztpraxis oder vergleichbaren Räumlichkeiten betrieben werden, in welchen er einer ständigen Aufsicht unterliegt, d.h. das Terminal nie länger als 30 Minuten unbeaufsichtigt ist (d.h. sich nie länger als 30 Minuten . in einem ungeschützten Einsatzbereich befindet). Die Definition der hier benannten Einsatzbereiche findet sich in **[16]**. Es ist sicherzustellen, dass unbefugte Personen keinen Zugang zu dem Chipkartenterminal und daran angeschlossenen Systemeinheiten haben. Insbesondere bedeutet dies, dass sich das Gerät bei längerer Abwesenheit (auch nachts) in einem geschützten Bereich befindet, in welchem das Terminal durch seine Umgebung geschützt wird.

5.4.6 OE.USER.RESP6:
Für die qualifizierte Signatur ist der EVG nur in Verbindung mit Signatur-Chipkarten (Sichere Signatur-Erstellungseinheit, SSEE) zu verwenden, die den Anforderungen des SigG/SigV entsprechen.

5.4.7 OE.USER.RESP7:
Für die qualifizierte Signatur ist der EVG nur in Verbindung mit Signatur-Anwendungskomponenten zu verwenden, die den Anforderungen des SigG/SigV entsprechen.

Das Produkt eHealth GT900 BCS darf erst dann verwendet werden, wenn die soeben aufgeführten Auflagen für den Betrieb des Produktes umgesetzt wurden.

6 Algorithmen und zugehörige Parameter
Der EVG selbst erstellt oder verarbeitet keine Signaturen im Sinne des SigG/SigV, dies geschieht nur in Verbindung mit einer SSEE (Signaturkarte). Der EVG unterstützt alle Signaturkarten und Anwenderprogramme (Signaturanwendungskomponenten) welche Algorithmen gemäß **[17]** verwenden.

7 Gültigkeit der Herstellererklärung

Diese Herstellererklärung ist befristet. Sie wird ersetzt durch die Bestätigungsurkunde des BSI. Die Herstellererklärung verliert ihre Gültigkeit wenn:

- die Firmwareversion oder die Hardwareversion des Produktes geändert werden oder
- die Herstellererklärung durch die zuständige Behörde (BNetzA) oder den Hersteller selbst wiederrufen wird.

8 Zusatzdokumentation

Name	Version	Datum	Seitenzahl
Sicherheitskonzept	1.4	26.05.2009	28 mit Anhang
Endbericht zu den eHealth BCS Zulassungsprüfungen	1.1	27.05.2009	16
Bescheinigung für die Phase 1 der Evaluierung (BSI)	-	29.05.2009	2
Bescheinigung über die Komponentenzulassung ZLS_BCS_gtG_000102 (gematik)	-	29.05.2009	2
Security Target	1.4	19.02.2009	59
Benutzerhandbuch	1.6	14.07.2009	32
Erweiterung zum Benutzerhandbuch v.1.6	1.0	30.06.2010	10
Dokumentation des Produktlebenszyklus	1.6	21.10.2009	135 mit Anhang
Dokumentation der Entwicklung – Teilaspekt ADV_FSP.4	1.6	28.05.2009	35
Dokumentation der Entwicklung – Teilaspekt ADV_TDS.3	1.7	29.05.2009	57
Dokumentation der Entwicklung – Teilaspekt ADV_IMP.1	1.3	23.03.2010	101
Dokumentation der Entwicklung – Teilaspekt ADV_ARC.1	1.2	26.05.2009	21
Test-Dokumentation	1.3	14.04.2010	52 mit Anhang
Produktionstest GT900 Teil 1: Hauptplatine	1.1	25.08.2009	10
Produktionstest GT900 Teil 2: Selbsttest	1.0	25.08.2009	9
Produktionstest GT900 Teil 3: Endtest	1.0	25.08.2009	10
Testprotokolle	1.0	06.08.2009	36
Impact Analysis Report	1.1	06.04.2010	27

9 Abkürzungsverzeichnis

Abkürzung	Erklärung
AES	Advanced Encryption Standard
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
eHC	Electronic Health Card
EVG	Evaluationsgegenstand (siehe auch TOE)
HBA	Heilberufsausweis
HPC	Health Professional Card
LAN	Local Area Network
PP	Protection Profile
QES	qualifizierte elektronische Signatur
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
SMC	Security Module Card
SM-KT	Sicherheits Modul Karten Terminal
TOE	Target of Evaluation
TSF	TOE Security Function
TSP-K	Trust-Service Provider that issues connector certificates
VAM	Value-added module
PDF	Portable Document Format

10 Literaturverzeichnis

Ref.Kurzzeichen	Referenz	Beschreibung
[1]	[gemSpec_KT]	gematik GmbH ***Einführung der Gesundheitskarte – Spezifikation eHealth-Kartenterminal,*** Stand: 15.09.2009 Version: 2.8.0, www.gematik.de
[2]		Spitzenverbände der Krankenkasse; Kassenärtztliche Bundesvereinigung; Kassenzahnärtztliche Bundesvereinigung ***Technische Spezifikation der Versichertenkarte,*** Stand: 30.10.2006, gültig ab: 30.10.2006 Version: 2.07
[3]	[gemSpec_eGK_P1]	gematik GmbH ***Einführung der Gesundheitskarte – Spezifikation elektronische Gesundheitskarte; Teil 1 – Spezifikation der elektrischen Schnittstelle,*** Stand: 20.03.2008 Version: 2.2.0, www.gematik.de
[4]	[gemSpec_eGK_P2]	gematik GmbH ***Einführung der Gesundheitskarte – Spezifikation elektronische Gesundheitskarte; Teil 2 - Grundlegende Applikationen,*** Stand: 25.03.2008 Version: 2.2.0, www.gematik.de
[5]	[gemSpec_eGK_P3]	gematik GmbH ***Einführung der Gesundheitskarte – Spezifikation elektronische Gesundheitskarte; Teil 3 – Äußere Gestaltung,*** Stand: 20.12.2007 Version: 2.1.0, www.gematik.de
[6]	[SICCT]	TeleTrusT ***SICCT Secure Interoperable ChipCard Terminal,*** Stand: 19.11.2007 Version 1.20
[7]	B0/B1	PZ Telesec der Deutschen Telekom AG, Netphen ***HTSI Programmierhandbuch, Programmierhandbuch zum Host Transport Service Interface*** Version: 1.0
[8]	[CCID]	USB Implementors Forum, Inc.; Device Working Group (DWG). ***Universal Serial Bus Device Class Specification for USB Chip/Smart Card Interface Devices,*** Stand: 20.03.2001 Version: 1.0, http://www.usb.org
[9]	BSI-TR-03120	Bundesamt für Sicherheit in der Informationstechnik ***Technische Richtlinie BSI TR-03120, Sichere Kartenterminalidentität (Betriebskonzept), eHealth Kartenterminals,*** Stand: 25.10.2007 Version: 1.0, www.bsi.de

Ref.Kurzzeichen	Referenz	Beschreibung
[10]	BSI-TR-03120 Appendix	Bundesamt für Sicherheit in der Informationstechnik ***Anhang zur Technischen Richtlinie BSI TR-03120, Kartenterminalversiegelung, eHealth Kartenterminals,*** Stand: 04.04.2008 Version: 1.0.2, www.bsi.de
[11]	[gemAnf_BCS]	gematik GmbH ***Einführung der Gesundheitskarte – Prüfvorgaben/Anforderungen eHealth-BCS-Kartenterminal,*** Stand: 29.02.2008 Version: 0.9.0, www.gematik.de
[13]	[CT-API]	Deutsche Telekom AG (PZ Telesec), GMD Darmstadt, TÜV Informationstechnik GmbH, TeleTrusT Deutschland e.V. ***Anwendungsunabhängiges CardTerminal Application Programming Interface (CT-API) für Chipkartenanwendungen,*** Stand: 14.10.1998 Version 1.1, Publiziert in MKT Spezifikation [2, Teil 3].
[14]	Signaturgesetz	Gesetz über die Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz – SigG) vom 16. 05. 2001 BGBl. I, S. 876ff, 21. 05. 2001. zuletzt geändert durch Art. 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091).
[15]	Signaturverordnung	Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. 11. 2001 BGBl. I, S. 3074ff, 21. 11. 2001. zuletzt geändert durch Art. 1 ÄndVO vom 17. Dezember 2009 (BGBl. I S. 3932).
[16]		Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen ***Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten – Arbeitsgrundlage für Entwickler/Hersteller und Prüf-/Bestätigungsstellen,*** Stand: 19.07.2005 Version 1.4
[17]		Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen ***Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)*** Stand: 06.01.2010 Veröffentlicht am 04. Februar 2010 im Bundesanzeiger Nr. 19, Seite 426

Ende der Herstellererklärung