HERSTELLERERKLÄRUNG

Der Hersteller

Hypercom GmbH
Konrad – Zuse - Str. 19 – 21
D-36251 Bad Hersfeld

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

Chipkartenterminal
medCompact eHealth Card Terminal BCS
Version 02.00

die nachstehend genannten Anforderungen des Signaturgesetzes und der Signaturverordnung an eine Signaturanwendungs-komponente als Teil-Signaturanwendungskomponente erfüllt.

Das Produkt medCompact eHealth Card Terminal BCS Version 02.00 befindet sich aktuell in CC Zertifizierung (BSI-DSZ-00514) und Bestätigung gemäß Signaturgesetz (BSI.02105.TE.xx.200x). Das Produkt medCompact eHealth Card Terminal BCS Version 02.00 hat bereits mit Datum vom 19.09.2008 eine gematik Zulassung für die Version eHealth BCS V02.00 erhalten.

Bad Hersfeld, den 19.03.2010

_____	_____
P. Vesco, Geschäftsführer	B. Rach, COO

Diese Herstellererklärung in Version 1.2 mit der Dokumentennummer GE003160 besteht aus 8 Seiten.

---

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) in der Fassung vom 16. 05.2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17.07 2009 (BGBl. I S. 2091)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) vom 16.11.2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 17.12.2009 (BGBl. I S. 3932)

Dokumentenhistorie

Version	Datum	Autor	Bemerkung
1.0	27.11.2009	Mawick	Initiale Version
1.1	03.03.2010	Mawick	Anmerkungen aus OR TüViT
1.2	19.03.2010	Braun	Anmerkungen aus 2. OR TüViT

1. Handelsbezeichnung

Die Handelsbezeichnung lautet:	Chipkartenterminal medCompact eHealth Card Terminal BCS Version 02.00 (Varianten mit 1 bzw. 2 Slots)
Auslieferung:	Hardware mit installierter Firmware BCS V02.00
Hersteller:	Hypercom GmbH, Bad Hersfeld
Handelsregisterauszug:	HRB 604, Amtsgericht Bad Hersfeld

2. Lieferumfang und Versionsinformationen

Nachfolgend ist der Lieferumfang, einschließlich der Versionsinformationen, aufgezählt:

Produktart	Bezeichnung	Version	Datum	Übergabeform
Hardware	Chipkartenterminal medCompact eHealth Card Terminal BCS Version 02.00			In Verpackung (Hardware mit geladener Firmware)
	1 Slot	P210-3050 F11	19.03.2009	
	2 Slots	3150 F11	22.09.2008	
Software	BCS Firmware	V02.00	22.09.2008	In der Hardware enthalten
Dokumentation	Kurzbedienungs-anleitung	Version 02	26.02.2010	Gedruckt (Auslieferung), auf CD sowie als PDF (Internet Download)
	Bedienungsanleitung	Version 03	01.03.2010	
Software	medCompact CD (Treiber, Bedie-nungsanleitung) *)		März 2010	In Verpackung

Tabelle 1: Lieferumfang und Versionsinformationen

*) Kein Bestandteil des Evaluierungsgegenstands

3. Funktionsbeschreibung

Die Hypercom Chipkartenterminals medCompact eHealth Card Terminal BCS Version 02.00 mit Firmware BCS V02.00 (Varianten mit 1 bzw. 2 Slot; im folgenden EVG genannt) stellen ein universelles Chipkartenterminal dar, das Prozessor- und Speicherkarten nach ISO/IEC 7816 über eine Applikationsschnittstelle (CT-API) verarbeiten kann.
Die Terminals arbeiten mit Chipkarten-Übertragungsprotokoll T=1 gemäß ISO/IEC 7816, die Übertragungsprotokolle für Speicherchipkarten (I2C-, 2-Wire und 3-Wire-Protokoll) werden ebenfalls unterstützt. Die Geräte verfügen über eine Tastatur mit großen Tasten und ein grafisches LC-Display (9 Zeilen zu je 22 Zeichen), um eine sichere PIN - Eingabe zu ermöglichen. Das Terminal besitzt zusätzlich eine rote LED zur Signalisierung des sicheren PIN- Eingabemodus.
Die Tastatur stellt die numerischen Tasten „0“ bis „9“ sowie die Tasten „Eingabe/OK“ (grün) „Korrektur/Lösch“ (gelb), „Abbruch“ (rot), „Menü“ sowie die Funktionstasten „F1“, „F2“ und „F3“ zur Verfügung.

Im Online Betrieb ist der EVG über USB bzw. RS232 an den PC angeschlossen und erkennt die von der Host-Software übermittelten BCS Kommandos zur PIN - Eingabe nach CCID und fügt die vom Benutzer über die Tastatur eingegebenen Ziffern als PIN in die entsprechenden Stellen des Chipkartenkommandos ein. In keinem Fall wird die Eingabe des Benutzers (insbesondere die PIN) an den Host übertragen. Der sichere PIN - Eingabemodus wird dem Benutzer optisch durch ein entsprechendes Symbol am LC-Display angezeigt und zusätzlich durch eine rote LED signalisiert. Im PIN – Eingabemodus werden die eingegebenen Ziffern nicht im Klartext, sondern maskiert als Sternchen (*) am LC-Display des EVG angezeigt.

Die Leser können an allen Hostsystemen verwendet werden, die über eine USB oder RS232 Schnittstelle verfügen. Für die Anbindung des EVG an einen Host wird durch den Hersteller eine geeignete Applikationsschnittstelle (CT-API) zur Verfügung gestellt.
Die Treiber des Chipkartenlesers sind nicht Bestandteil des EVG, da sie die Daten nur weiterleiten und selbst keinerlei Sicherheitsfunktionen implementieren. Sie unterstützen die wichtigsten Betriebssysteme. Sie werden auf einer CD mit dem Terminal ausgeliefert und müssen auf dem Host - PC installiert werden.

Der EVG ist aufgrund der Applikationsschnittstelle und des unterstützten BCS Kommando - Sets in vielen Marktsegmenten einsetzbar (z.B. im Gesundheitswesen zum Lesen der KVK bzw. der neuen eGK / HBA). Da der EVG einen Chipkartenleser der Klasse 3 darstellt und somit die Eingabe von Identifikationsdaten des Benutzers (PIN) ermöglicht und auf sicherem Weg direkt an eine sichere Signaturerstellungseinheit (Signatur - Chipkarte) nach §2 Nummer 10 SigG übermittelt, können diese Produkte auch für Applikationen gemäß Signaturgesetz und Signaturverordnung eingesetzt werden. Sie ermöglichen 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. Die Chipkartenleser stellen somit eine Teilkomponente einer Signaturanwendungskomponente dar, die eine entsprechende Sicherheitsbestätigung benötigen, um für qualifizierte elektronische Signaturen nach §2 Nummer 3 SigG eingesetzt werden zu können. Für eine entsprechende Nutzung des EVG (Chipkartenlesers) gemäß SigG / SigV sind nur Host – Applikationen (Signaturanwendungen) als auch Signaturkarten, die im SigG – Kontext evaluiert und bestätigt wurden, einzusetzen.

Synchrone Speicherchipkarten werden zwar vom EVG unterstützt, können aber nicht als Signaturerstellungskomponente eingesetzt werden und sind somit für die Herstellererklärung nicht relevant.

Der EVG erfüllt die spezifischen Anforderungen nach §15 Absatz 2, Nummer 1a (keine Preisgabe oder Speicherung der Identifikationsdaten außerhalb der sicheren Signaturerstellungseinheit) und Absatz 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) der Signaturverordnung.
Nachfolgend sind die Instruction – Bytes, die im EVG für eine sichere PIN – Eingabe implementiert sind, aufgelistet. Diese Instruction – Bytes sind von der Signaturanwendung auf dem Host und von den Signaturkarten spezifikationsgemäß zu unterstützen bzw. mit einer entsprechenden Fehlermeldung abzulehnen, falls sie nicht unterstützt werden:

VERIFY (ISO/IEC 7816-4)	INS = 0x20
CHANGE REFERENCE DATA (ISO/IEC 7816-4)	INS = 0x24
ENABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-4)	INS = 0x28
DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-4)	INS = 0x26
RESET RETRY COUNTER (ISO/IEC 7816-4)	INS = 0x2C
PERFORM SECURITY OPERATION (ISO/IEC 7816-8)	INS = 0x2A

Die Auslieferung der Chipkartenterminals medCompact eHealth Card Terminal BCS Version 02.00 erfolgt mit der im Gerät geladenen BCS Applikation in der Version 02.00, diese wird in der sicheren Produktionsumgebung eingebracht. Es besteht die Möglichkeit eines sicheren Softwaredownloads, damit ist das Terminal für zukünftige Anforderungen vorbereitet. Der sichere Softwaredownload gewährleistet die Integrität und Authentizität der Firmware und ist bereits Bestandteil einer Sicherheitsbestätigung des BSI.
Zum Lieferumfang des Hypercom medCompact eHealth Card Terminal BCS Version 02.00 gehört bei der Auslieferung an den Kunden neben dem Chipkartenterminal mit installierter Firmware (Teil des EVG) eine gedruckte Kurzbedienungsanleitung (Teil des EVG) und eine CD-ROM (kein Teil des EVG) mit Treibern, Software und der Benutzerdokumentation (Teil des EVG) in elektronischer Form. Für den Fall eines Updates des Terminals über den sicheren Download besteht der Lieferumfang aus der signierten Firmware (Teil des EVG), optional einer erweiterten Benutzerdokumentation (Teil des EVG) und einem Update – Tool (kein Teil des EVG). Die auf der CD-ROM enthaltenen Treiber, Dokumentation und Software (kein Teil des EVG) können auch über einen Download bezogen werden.
Die für den Auslieferweg „Download“ bereitgestellte Firmware wird durch den Hersteller Hypercom in der sicheren Produktionsumgebung digital signiert. Für diese Signatur wird der RSA Algorithmus mit einer Schlüssellänge von 2048 Bit und der Hash Algorithmus SHA-256 angewendet. Als Signaturerstellungseinheit wird eine nach SigG bestätigte Signaturkarte eingesetzt. Diese sowie die zugehörige PIN werden in der sicheren Produktionsumgebung des Herstellers aufbewahrt. Die Verifikation dieser Signatur garantiert die Integrität und Authentizität der Firmware bei einem Update des Chipkartenlesers. Die Prüfung der Signatur erfolgt dabei innerhalb der Firmware des EVG. Nur nach einer erfolgreichen Signatur- und Versionsprüfung (es kann nur die gleiche oder eine neuere Version der Software verwendet werden) wird die Firmware installiert und aktiviert, andernfalls wird sie abgewiesen. Der Hersteller Hypercom stellt ein Update – Tool zur Verfügung, das die Übertragung der Firmware in den EVG vornimmt, dieses Tool ist nicht Bestandteil des EVG, da es keine Sicherheitsfunktionen implementiert hat. Es dient lediglich der Übertragung der digital signierten Firmware vom Host in das Kartenterminal.
Hypercom garantiert, dass jede neue Version des EVG eine neue Versionsnummer erhält und somit eindeutig identifizierbar ist. Wird eine neue, unbestätigte Firmware eingespielt, so verliert die Bestätigung ihre Gültigkeit. Eine neue Firmware muss einem erneuten Bestätigungsverfahren unterzogen werden.
Das Produkt medCompact eHealth Card Terminal BCS Version 02.00 befindet sich aktuell in CC Zertifizierung (BSI-DSZ-00514) und Bestätigung gemäß Signaturgesetz (BSI.02105.TE.xx.200x). Das Produkt medCompact hat bereits eine vorläufige Sicherheitsbestätigung für die Version BCS V02.00 im Rahmen einer gematik Zulassung durch das BSI erhalten. Die Bestätigung umfasst die Bereiche sichere PIN Eingabe, Software Download, Versiegelung und Manipulationsschutz.

Die aktuell bestätigten Versionen der Firmware und der Hardware des EVG sind auf den Webseiten der Bundesnetzagentur (BNetzA) unter http://www.bundesnetzagentur.de für den Benutzer abrufbar, die zertifizierten Versionen beim Bundesamt für Sicherheit in der Informationstechnik (BSI) unter http://www.bsi.bund.de. Es liegt in der Verantwortung des Benutzers des Chipkartenterminals, sich hier vor der Installation einer neuen Firmware davon zu überzeugen, dass eine neu zu installierende Version der Firmware nach SigG / SigV bestätigt und nach Common Criteria zertifiziert ist. Die entsprechenden Hersteller Downloads stellt Hypercom auf seinen Webseiten unter http://www.medline.hypercom.com zur Verfügung. Den Benutzern wird daher empfohlen, diese Webseiten regelmäßig zu besuchen, um sich über Aktualisierungen zu informieren.
Die Version der aktuell im EVG befindlichen Firmware kann jederzeit am LC-Display des Terminals angezeigt werden, die Version der Hardware ist auf dem Typenschild des EVG angegeben.
Die Authentizität des EVG wird durch ein fälschungssicheres, durch das BSI zertifiziertes Siegel sichergestellt, dass sich bei einer Entfernung zerstört und damit nur einmal verwendbar ist. Eine Manipulation des Gerätes wird mittels einer aktiven Sicherheitsüberwachung des Gehäuses sicher verhindert. Der EVG besitzt eine entsprechende Sicherheitsbestätigung des BSI.

Der EVG ist für einen Einsatz im privaten oder zutrittsgeschützten Bereich (z.B. Praxis eines Leistungserbringers) konzipiert.

4. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

Das Produkt medCompact eHealth Card Terminal BCS Version 02.00 erfüllt die nachfolgend aufgeführten Anforderungen des SigV:

Anforderung	**Erfüllung**
§15 Absatz 2 SigV: *Signaturanwendungskomponenten nach § 17 Absatz 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,	SF1 Secure PIN entry SF5 Protection of the TSF
§15 Absatz 4 SigV:	
Sicherheitstechnische Veränderungen an technischen Komponenten... müssen für den Nutzer erkennbar werden."	SF1 Secure PIN entry SF5 Protection of the TSF SM1 Sealing SM2 Mesh board SM3 Cage switches SM4 Active security controller.

SF1 Secure PIN Entry:
Die Firmware im Lesegerät prüft die Kommandos anhand ihrer Kommandostruktur gemäß CCID. Wird ein Kommando zum Verifizieren bzw. Modifizieren einer PIN erkannt und ist ein an die Chipkarte weiterzuleitendes Kommando mit einem der folgenden Instruction -Bytes enthalten:

VERIFY (ISO/IEC 7816-4)	INS = 0x20
CHANGE REFERENCE DATA (ISO/IEC 7816-4)	INS = 0x24
ENABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-4)	INS = 0x28
DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-4)	INS = 0x26
RESET RETRY COUNTER (ISO/IEC 7816-4)	INS = 0x2C
PERFORM SECURITY OPERATION (ISO/IEC 7816-8)	INS = 0x2A

wird in den Modus zur sicheren Erfassung der PIN über die Tastatur des medCompact eHealth Card Terminal BCS Version 02.00 geschaltet.
Die Sicherheitsfunktion SF1 erkennt die von der Host-Software übermittelten Kommandos zur PIN - Eingabe und fügt die über die Tastatur eingegebenen Ziffern als PIN an die entsprechenden Stellen des Kommandos an die Chipkarte ein. Es findet keinerlei Rückmeldung über die eingegebene PIN an den Host statt. Die Eingabe einer Ziffer wird durch ein Sternchen (*) am LC-Display des EVG angezeigt. Der Benutzer kann die Eingabe der PIN mit der (roten) Abbruchtaste jederzeit abbrechen, wodurch die Übertragung der PIN zur Chipkarte verhindert wird. Der Benutzer muss die Eingabe der PIN mit der (grünen)

Bestätigungstaste abschließen.
Der sichere PIN – Eingabemodus wird dem Benutzer durch eine rote LED und ein entsprechendes Symbol im LC-Display signalisiert.

SF5 Protection of the TSF:
Nachdem eine eingegebene PIN an eine Chipkarte gesendet wurde, wird der entsprechende Speicherbereich im Terminal aktiv gelöscht (das SDRAM wird mit binären Nullen überschrieben).
Außerdem wird der Alarmzustand des EVG ständig überprüft. Im Falle eines Alarms wird dieser angezeigt und das Terminal ist nicht mehr nutzbar.

SM1 Sealing
Das Gehäuse des EVG ist durch Siegel geeignet versiegelt. Das eingesetzte Siegel besitzt eine laufende Nummer und ist durch das BSI zertifiziert.
Der Benutzer wird in der Benutzerdokumentation belehrt, die Unversehrtheit der Versiegelung vor einer Benutzung des EVG zu kontrollieren und das Gerät im Falle eines beschädigten Siegels nicht weiter zu benutzen.

SM2 Mesh board / SM3 Cage switches / SM4 Active security controller.
Die oben aufgeführten Sicherheitsmaßnahmen stellen eine aktive Überprüfung von Sicherheitseinrichtungen des EVG dar (Gehäuseschalter, Leiterplatten mit Sicherheitsleiterzügen), die eine Manipulation des Terminals überwachen und bei einem eventuellen Angriffsversuch dem Benutzer einen Alarm signalisieren.

5. Maßnahmen in der Einsatzumgebung

5.1 Einrichtung der IT-Komponenten

Dieser Abschnitt entfällt, da keine Vorgaben bzgl. der IT-Komponenten gemacht werden müssen, um die Sicherheitsfunktionen des EVG zu erfüllen.

5.2 Anbindung an ein Netzwerk

Dieser Abschnitt entfällt, da kein direkter Anschluss des EVG an ein Netzwerk vorgesehen ist.

5.3 Auslieferung und Installation

Das Chipkartenterminal medCompact eHealth Card Terminal BCS Version 02.00 wird als fertig konfiguriertes Terminal (versiegeltes Gehäuse, geladene Firmware Version 2.00) mit der zugehörigen Kurzbedienungsanleitung und CD in Transportverpackung ausgeliefert. Bei einer Inbetriebnahme ist die Unversehrtheit des Siegels zu prüfen, das initiale Admin Passwort zu vergeben und die Treibersoftware auf dem Host zu installieren.
Im Auslieferungsweg „Download“ ist die durch den Hersteller bereitgestellte Firmware zu installieren.

5.4 Auflagen für den Betrieb des Produktes

Die folgenden Auflagen werden gemacht:

OE.ENV
Das Terminal darf nur in kontrollierten Umgebung eingesetzt werden.

Der Benutzer muß vor der Verwendung des Terminals die Unversehrtheit der Siegel überprüfen.
Der Benutzer muss die Regeln zur sicheren Handhabung und Nichtweitergabe der PIN beachten.

Während der Eingabe einer PIN muss der Benutzer prüfen, dass sich das Terminal im sicheren PIN Eingabemodus befindet (rote LED und Symbol im LC – Display).

Für die qualifizierte Signatur ist der EVG nur in Verbindung mit Signatur Chipkarten (SSEE, Sichere Signaturerstellungseinheit) zu verwenden, die den Anforderungen des SigG / SigV entsprechen.

Für die qualifizierte Signatur ist der EVG nur in Verbindung mit Signaturanwendungskomponenten zu verwenden, die den Anforderungen des SigG / SigV entsprechen.

OE.ADMIN

Der Administrator muss vor einer Inbetriebnahme die korrekte Versiegelung des EVG überprüfen und ein initiales Admin – Passwort vergeben.
Der Administrator muss die Regeln zur sicheren Handhabung und Nichtweitergabe der PIN und des Administrator Passwortes beachten.

6. Algorithmen und zugehörige Parameter

Dieser Abschnitt entfällt, da der EVG selbst keine Signaturen im Sinne des SigG / SigV erstellt oder verarbeitet, sondern nur in Verbindung mit einer SSEE (Signaturkarte).

7. Gültigkeit der Herstellererklärung

Diese Herstellererklärung ist befristet bis 30.09.2011. Sie wird ersetzt durch die bis (spätestens) dann erstellte Bestätigungsurkunde des BSI.

8. Zusatzdokumentation

Folgende Dokumente werden vom Hersteller bereitgestellt:

- Security Target, Version 0.96 vom 19.03.2010
- Testdokumentation, Version 1.1 vom 09.03.2010
- Benutzerdokumentation, Version 03 vom 01.03.2010

Ende der Herstellererklärung