

Herstellereklärung

Die

Gemalto SA

6 Rue de la Verrerie

92190 Meudon

erklärt hiermit gemäß § 17 Abs. 4 Satz 2 SigG¹
in Verbindung mit § 15 Abs. 5 Satz 1 SigV²,
dass ihr Produkt

e-Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14

als Teil einer Signaturanwendungskomponente die nachstehend genannten Anforderungen des SigG
und der SigV an eine Signaturanwendungskomponente erfüllt.

Meudon, den 21.06.2011



Jacques SENECA – Executive Vice-President Security Business Unit.

Diese Herstellereklärung in Version F mit der Dokumentennummer DPC120090 besteht aus 11
Seiten.

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 die Verordnung vom 15. November 2010 (BGBl. I S. 1542)

Dokumentenhistorie

Version	Datum	Autor	Bemerkung
A	18.03.2011	D. Bonnardel	Initiale Version
B	7.04.2011	D. Bonnardel	Überarbeitung
C	05.05.2011	D. Bonnardel	Überarbeitung
D	16.05.2011	D. Bonnardel	Überarbeitung
E	25.05.2011	D. Bonnardel	Überarbeitung
F	21.06.2011	D. Bonnardel	Überarbeitung : Firmwareveränderung (V1.14)

1. Handelsbezeichnung

Die Handelsbezeichnung lautet: e-Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14
Auslieferung: Bereitstellung im Paket (e-Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14, USB-Kabel, Stromkabel, Installations-CD, Kurzinstallationsanleitung)
Hersteller: Gemalto SA.
Handelsregisterauszug: 562 113 530 R.C.S. Nanterre

2. Lieferumfang und Versionsinformationen

Nachfolgend ist der Lieferumfang, einschließlich der Versionsinformationen, aufgezählt:

Produktart	Bezeichnung	Version	Übergabeform
Hardware mit Firmware	e-Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 P/N: HWP116542 bestehend aus:	K	- In Einzelverpackung
	- e-Health Card Terminal GCR5500-D Hardware: P/N: HWP116760	H	
	- Firmware e-Health BCS v1.14: P/N: SWF117482	J	
Hardware	USB-Kabel, Stromkabel		- In Einzelverpackung
Software	Installations-CD P/N: SWP117063	K	- In Einzelverpackung
Dokumentation	Kurzinstallationsanleitung P/N: DOC117649	C	- Gedrucktes Dokument als Bestandteil der Einzelverpackung - PDF-Datei auf Installations-CD, - Internetdownload
Dokumentation	Installationsanleitung P/N: DPC117113	F	- PDF-Datei auf Installations-CD
Dokumentation	Benutzerhandbuch P/N: DPC116770	G	- PDF-Datei auf Installations-CD
Dokumentation	Administratorhandbuch P/N: DPC117780	F	- PDF-Datei auf Installations-CD

Tabelle 1: Lieferumfang und Versionsinformationen

Das Produkt -Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 nutzt keine nach SigG bestätigten Produkte, die nicht Bestandteil dieser Erklärung sind.

Das Produkt -Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 nutzt keine weiteren Produkte, die ebenfalls nicht Bestandteil dieser Erklärung sind, für die eine Herstellererklärung veröffentlicht wurde.

3. Funktionsbeschreibung

Das Produkt e-Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 ist ein Smartcard-Terminal, das die Anforderungen zur Verwendung mit der deutschen elektronischen Gesundheitskarte und der deutschen Health Professional Card erfüllt. Das Produkt erfüllt die nachstehend genannten Anforderungen des SigG und der SigV an Teile einer Signaturanwendungskomponente. Es unterstützt Smartcard-Übertragungsprotokolle gemäß ISO 7816 (T=0, T=1) und Übertragungsprotokolle für Speicherkarten.

Das Produkt e-Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 bietet:

- ein Tastaturfeld und einen LCD-Bildschirm zur sicheren PIN-Eingabe und Verwaltung der Terminalkonfiguration,
- zwei vollformatige Karteneinzugsschlitze (ID-1) (der erste befindet sich auf der Oberseite des Terminals für die Patientenkarte, der zweite rechts am Terminal für die Arztkarte),
- zwei USB-Master-Anschlüsse, die verwendet werden, um Firmwareaktualisierungen herunterzuladen, die auf einem USB-Stift gespeichert sind,
- Ein USB-Slave-Anschluss, der mit einem USB-Kabel an einen Host-PC angeschlossen werden kann. Dieser USB-Anschluss kann eine serielle Verbindung emulieren. So kann das Terminal über ein serielles Kabel mit einem Host-PC verbunden werden.

Für zukünftige Produktversionen wird ein Ethernet-Stecker bereitgestellt, der jedoch mit Firmware e-Health BCS v1.14 nicht funktionsfähig ist.

Der LCD-Bildschirm kann sowohl alphanumerische Zeichen (vier Zeilen à 16 Zeichen) als auch dedizierte Symbole anzeigen. Das Tastaturfeld weist die numerischen Tasten "0" bis "9" sowie funktionale Tasten auf:

- "Bestätigung" (grün), "Abbrechen" (rot), "Löschen" (gelb),
- "Menü" (Zugriff auf die Verwaltung der Terminalkonfiguration),
- "Aufwärtspfeil" und "Abwärtspfeil",
- Netzschalter "Ein/Aus".

Das Produkt -Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 verfügt über eine CT-API-kompatible serielle oder USB-Schnittstelle (USB-Slave-Anschluss) und kann mit allen Hostsystemen (für gewöhnlich in Form eines PC) verbunden werden, die eine USB-Schnittstelle aufweisen. Auf Hostseite bildet eine Anwendungssoftware (nicht vom Hersteller bereitgestellt) die Schnittstelle. Diese Anwendungssoftware verwaltet den Datenaustausch mit dem Produkt mit Unterstützung einer CT-API-Anwendung und eines vom Hersteller bereitgestellten Treibers.

Das Produkt e-Health Card Terminal GCR5500-D mit Firmware BCS v1.14 erkennt vom Host gesendete Kommandos zur PIN-Eingabe.

Das Produkt kann ID-Daten (PIN) erfassen und an ein sichere Signaturerstellungseinheiten (SSEE) übertragen. Hierzu wird eine Smartcard in einen dedizierten Einzugsschlitz des Produkts eingesteckt. Die PIN verlässt nie das Card Terminal GCR5500-D mit Firmware BCS v1.14 in Richtung Host und wird im Card Terminal nicht gespeichert.

Anschließend überträgt das Produkt einen von der Hostanwendungssoftware empfangenen Hash-Wert an die Signaturkarte. Daraufhin sendet das Produkt die vom SSEE generierte Signatur zurück an das Hostsystem. Somit bildet das Produkt -Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 eine an der Erzeugung elektronischer Signaturen beteiligte Komponente gemäß SigG und SigV.

Sicherer Authentifizierungsprozess für die Benutzer-PIN:

Die Signatur-Smartcard wird vom Benutzer in einen der beiden Karteneinzugsschlitze eingesetzt.

Die auf dem Host-PC ausgeführte Anwendungssoftware sendet einen Befehl ans Terminal, von dem die PIN-Eingabe über den USB-Slave-Anschluss angefordert wird (serielle oder USB-Verbindung).

Der Benutzer wird gebeten, die PIN einzugeben. Der zu verwendende Karteneinzugsschlitz wird dem Benutzer mit hierfür reservierten Symbolen angezeigt.

Der Benutzer gibt anschließend in einem sicheren Modus, der durch ein blinkendes Schlüsselsymbol angezeigt wird, die PIN ein. Jedes eingegebene Zeichen wird von einem Sternchen dargestellt. Die Eingabe muss anschließend überprüft werden.

Die vom Benutzer über die Tastatur des Produkts eingegebenen PIN-Daten werden an den entsprechenden Stellen des dedizierten Befehls eingefügt, der an die Smartcard gesendet wird. Das Terminal unterstützt nur die folgenden von der Hostanwendungssoftware gesendeten Befehle:

- 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

Nicht unterstützte Befehle werden mit einer Fehlermeldung abgelehnt.

Wenn die Authentifizierung erfolgreich ist, wird im LCD-Bildschirm eine Meldung angezeigt und ein Statuscode für „erfolgreich“ zum Host-PC zurückgesendet.

Die Konfigurationsmenüfunktion kann gestartet werden, wenn keine serielle oder USB-Verbindung (unter Verwendung des USB-Slave-Anschlusses) aktiviert ist. Der Benutzer kann einige Parameter (Kontrast und Hintergrundbeleuchtung des LCD-Bildschirms, Signaltöne der Tastatur) des Terminals festlegen und die aktuellen Firmware-Versionen anzeigen, ohne dass hierzu eine Authentifizierung erforderlich ist.

Eine vom Terminal verwaltete Administrator PIN schützt den Zugang zu den Administrationsfunktionen.

Die Administrator-PIN muss bei der Erstverwendung des Terminals wie in dem im Lieferumfang des Produkts enthaltenen Administratorhandbuch beschrieben initialisiert werden. Die Verwendung des Terminals ist erst möglich, nachdem die Administrator-PIN erfolgreich initialisiert wurde.

Der Benutzer muss die Administrator-PIN mit einem achtstelligen Wert festlegen.

Nach einer erfolgreichen Authentifizierung mit der Administrator-PIN kann der Benutzer folgende Aktionen durchführen:

- Sperrung der Administrator-PIN aufheben und Administrator-PIN ändern.
- Upgrade der Firmware des Terminals ausführen.
- Standardmäßige Einstellungsparameter des Terminals wiederherstellen, Terminal automatisch testen.

Die Firmware des Produkts -Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 kann nach einer erfolgreichen Authentifizierung der Administrator-PIN durch eine neue Firmware aktualisiert werden. Die Firmware-Aktualisierung muss auf einem USB-Stift gespeichert sein, der mit einem der beiden USB-Master-Anschlüsse verbunden ist.

Die neue Firmware-Version muss der aktuellen entsprechen oder neuer als diese sein. Vor der Installation prüft das Produkt die Authentizität der heruntergeladenen Firmware, indem es SHA-256-Hash-Funktions- und RSA2048-Signaturprüfalgorithmen verwendet. Durch diese Funktionalität werden unberechtigte Manipulationen des Produkts verhindert. Diese Herstellererklärung für die Firmware v1.14 verliert die Gültigkeit, sobald eine andere Firmwareversion geladen wird.

Das Produkt -Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 eignet sich für die Nutzung im privaten und im Bürobereich. Die Betriebsumgebung muss so gestaltet sein, dass ein angemessenes Sicherheitsniveau zum Schutz gegen physische Zugriffe unauthorisierter Personen erreicht wird.

4. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

Das Produkt -Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 erfüllt die nachfolgend aufgeführten Anforderungen der Verordnung zur elektronischen Signatur (SigV):

Referenz	Gesetzestext	Beschreibung
§15 Abs. 2 Nr. 1a SigV	<p>Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass</p> <p>1. bei der Erzeugung einer qualifizierten elektronischen Signatur</p> <p>a) die Identifikationsdaten</p>	<p>Die Anforderungen werden von den Sicherheitsfunktionen SF.PIN_USER, SF.INFO_DISPLAY und SF.Terminal_Management folgendermaßen erfüllt:</p> <p>SF.PIN_USER : Diese Funktion ermöglicht die Benutzer-PIN-Erfassung und die Übertragung der PIN an die Karte in einem dedizierten Einzugsschlitz über eine serielle oder USB-Verbindung (unter Verwendung des USB-Slave-Anschlusses), wie vom Host-PC erfordert. Gemäß dem vom Host-PC empfangenen Befehl wird das</p>

<p>nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden.</p>		<p>Terminal in den Modus zur sicheren PIN-Eingabe umgeschaltet.</p> <p>Das Terminal unterstützt nur die folgenden Befehle:</p> <ul style="list-style-type: none"> - 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 - Das Terminal erzeugt eine Fehlermeldung für nicht unterstützte Befehle. <p>Das Terminal warnt den Benutzer, indem es ein entsprechendes Symbol und den zu verwendenden Karteneinzugsschlitz anzeigt (siehe SF.INFO_DISPLAY).</p> <p>Der Benutzer gibt die PIN-Daten über das Tastaturfeld ein. Die über die numerischen Tasten vorgenommenen Eingaben werden nicht angezeigt und auch nicht an den Host gesendet. Das Terminal zeigt den Fortschritt der PIN-Eingabe durch Sternchen (*) an.</p> <p>Sobald der Benutzer die Eingabe bestätigt, werden die PIN-Daten in den Befehl eingefügt und an die Smartcard (sichere Signaturerstellungseinheit – SSEE) gesendet. Das Ergebnis wird zurück an den Host gesendet und angezeigt.</p> <p>Der Speicherbereich der PIN-Daten wird nach der Übertragung auf die Smartcard oder unter bestimmten Bedingungen (Abbruch durch den Benutzer oder durch den Host, Zeitüberschreitung während der PIN-Eingabe, Entnahme der Karte) sicher gelöscht.</p> <p>SF.INFO_DISPLAY : Die Sicherheitsfunktion zeigt auf dem Bildschirm der Terminals Sicherheitsinformationen an. Hierzu werden zwei Mechanismen verwendet:</p> <ul style="list-style-type: none"> - Anzeige einer Meldung in einem dedizierten Bereich des LCD-Bildschirms. - Anzeige dedizierter Symbole entsprechend der folgenden Tabelle 2. <p>Dem Benutzer werden der aktuelle Modus und mögliche Aktionen angezeigt:</p> <ul style="list-style-type: none"> - Wird eine Karte in den oberen (bzw. rechten) Karteneinzugsschlitz eingesetzt, zeigt der LCD-Bildschirm Symbol ID 1 (bzw. 3) an, - Wenn der Host-PC einen Befehl sendet, von dem eine PIN für die Karte angefordert wird, die in den oberen (bzw. rechten) Karteneinzugsschlitz eingesteckt wurde, wird Symbol ID 2 (bzw. 4) angezeigt. Ein Schlüsselsymbol (ID 5) blinkt während des gesamten Vorgangs der PIN-Eingabe, - Wenn der Benutzer als Administrator authentifiziert ist, wird ein Schraubenschlüssel-Symbol (ID 6) angezeigt, - Wenn ein USB-Stift in einen der beiden USB-Master-Anschlüsse eingesetzt wird, wird das USB-Symbol (ID 7) angezeigt, - Wenn das Terminal startet, wird das Symbol ID 8 angezeigt,
--	--	--

		<p>Die oben genannten Sicherungsfunktionen können nicht umgangen werden. Die Verarbeitung der PIN kann weder unterbrochen, noch von einem Angreifer beeinflusst werden. Dies stellt sicher, dass PIN-Daten nicht preis gegeben oder außerhalb der SSEE gespeichert werden.</p>
<p>§15 Abs. 4 SigV</p>	<p>Sicherheitstechnische Veränderungen an den Produkten für qualifizierte elektronische Signaturen nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.</p>	<p>Die Anforderungen werden von der Sicherheitsfunktion SF.START_UP und der passiven Sicherheitsfunktion SF.Tamper_Protection folgendermaßen erfüllt:</p> <p>SF.START_UP : Diese Sicherheitsfunktion führt Sicherheitsvorgänge während des TOE-Starts aus. Sie prüft die Integrität der im Produkt integrierten Firmware. Wenn die Integrität gegeben ist, startet SF.START_UP die unterschiedlichen Aufgaben, die für den Terminalbetrieb notwendig sind, und initialisiert Terminalsicherheitsattribute. Wenn die Integrität der Firmware während des Startvorgangs als fehlerhaft erkannt wird, wird das Produkt blockiert und kann nicht verwendet werden.</p> <p>SF.Terminal_Management : Diese Sicherheitsfunktion steuert die Befehlsausführung des Terminals im Menümodus.</p> <ul style="list-style-type: none"> - Sie behält die Administrator- und Benutzerrollen bei. - Sie prüft die Zugriffsbedingungen für die eingehenden Befehle, die vom Administrator/Benutzer über die Tastatur eingegeben wurden. - Sie stellt sicher, dass der Benutzer sich erfolgreich authentifiziert hat, bevor sie Aktionen entsprechend den Zugriffssteuerungsregeln autorisiert. <p>SF.Tamper_Protection : Diese Sicherheitsmaßnahme ermöglicht es dem Benutzer, zu erkennen, ob das Produkt geöffnet wurde oder ob ein Angreifer versucht hat, auf die internen Produktfunktionen zuzugreifen.</p> <p>Im Folgenden die passiven Sicherheitsfunktionen:</p> <ul style="list-style-type: none"> - Vorhandensein von Sicherheitssiegeln an Karteneinzugsschlitzten und an den Seiten des Gehäuses. Das Vorhandensein und die Integrität der drei Siegel müssen vom Benutzer kontrolliert werden: <ul style="list-style-type: none"> o Siegel 1: am oberen und unteren Gehäuseerand o Siegel 2: am oberen und unteren Gehäuseerand o Siegel 3: am oberen Gehäuseerand, am Display und auf der Tastatur Jeder Versuch, ein Sicherheitssiegel zu entfernen, führt zu einer unumkehrbaren physikalischen Modifizierung, durch die jede erneute Verwendung unmöglich wird. - Vorhandensein des Gehäuses, um einen direkten Zugriff auf interne Terminalfunktionen zu verhindern. Anhand einer visuellen Überprüfung des Produkts kann der Benutzer feststellen, ob ein Angriff stattgefunden hat

		<p>(die visuelle Überprüfung wird in den Benutzerhandbüchern beschrieben).</p> <p>Die PIN-Daten werden zwischen dem Produkt und der Smartcard des Benutzers ausgetauscht. Dieser Austausch findet im Innern des Produkts statt.</p> <p>Die oben beschriebenen Sicherheitsfunktionen SF.START_UP, SF.Terminal_Management und SF.Tamper_Protection stellen sicher, dass sicherheitstechnische Veränderungen am Produkt erkannt werden können.</p>
--	--	---

Tabelle 2: Erfüllung der Anforderungen


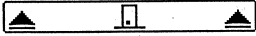

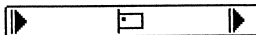



ID.	Symbol	Bedeutung
1		Eine Smartcard wird in den Patienteneinzugsschlitz eingesteckt.
2		Der über die Tastatur eingegebene PIN-Wert wird zum oberen Karteneinzugsschlitz (Patientenkartenschlitz) gesendet.
3		Eine Smartcard wird in den Arzteinzugsschlitz eingesteckt.
4		Der über die Tastatur eingegebene PIN-Wert wird zum rechten Kartenschlitz (Arztkartenschlitz) gesendet.
5		Blinkendes Schlüsselsymbol. Wenn dieses Symbol angezeigt wird, befindet sich das Terminal im Modus zur sicheren PIN-Eingabe.
6		Das Terminal befindet sich im Administratormodus (zur Verwaltung der Terminalkonfiguration)
7	USB	Ein USB-Stift (Massenspeichermedien) wird in einem der USB-Master-Steckplätze erkannt (z. B. Firmware-Aktualisierung)
8		Blinkendes Aktivitätssymbol. Wird im Rahmen einiger Aktivitätsphasen verwendet (z. B. bei der Startsequenz).

Tabelle 3: Bedeutung der angezeigten Symbole

Anforderungen an das Produkt bzgl. schwach werdender Algorithmen und qualifizierter Zeitstempel

Diese Anforderungen sind für das Produkt -Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 nicht relevant, da das Produkt die Überprüfung qualifizierter elektronische Signaturen und die Generierung qualifizierter Zeitstempel nicht unterstützt.

5. Maßnahmen in der Einsatzumgebung

5.1 Einrichtung der IT-Komponenten

Um sicherzustellen, dass das Produkt -Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 zur PIN-Erfassung und Weiterleitung der PIN an die SSEE verwendet wird, sind die folgenden zugeordneten Komponenten erforderlich:

- Eine sichere Signaturerstellungseinheit (SSEE) in Form einer Smartcard.
- Ein mit dem Produkt -Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 über eine serielle oder USB-Verbindung (unter Verwendung des Slave-Anschlusses) verbundener Host-PC.
- Eine dedizierte Anwendungssoftware, die auf dem Host-PC ausgeführt wird.

Die folgenden Sicherheitsmaßnahmen müssen bei der Einrichtung von IT-Komponenten strikt eingehalten werden:

- Der Benutzer muss die Integrität der seriellen oder USB-Verbindung überprüfen.
- Auf dem Host-PC muss eine aktuelle Virenschutzsoftware installiert sein.
- Der Benutzer muss die Konfigurationsschnittstelle des Produkts e-Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 durch Einrichten eines Administratorpassworts schützen.

5.2 Anbindung an ein Netzwerk

Dieses Kapitel entfällt, da in dem Produkt e-Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 kein direkter Anschluss an ein Netzwerk vorgesehen ist.

5.3 Auslieferung und Installation

Die beschriebenen Vorgänge zur Auslieferung und Installation müssen befolgt werden:

- Das Produkt -Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 wird vom Hersteller gemeinsam mit einer CD-ROM und einer Kurzeinstallationsanleitung in einer Verpackung geliefert. Software, Anleitungen und Handbücher können auch aus dem Internet heruntergeladen werden (Integrität und Authentizität der Firmware-Aktualisierungen werden von einer RSA2048-Signatur garantiert). Diese Herstellererklärung für die Firmware e-Health BCS v1.14 verliert die Gültigkeit, sobald eine andere Firmwareversion geladen wird.
- Das Terminal muss von autorisierten und geschulten Personen installiert und konfiguriert werden.
- Das Terminal darf nur in einer sicheren und zugelassenen Umgebung von identifizierten und autorisierten Personen verwendet werden (unbeaufsichtigter Zugriff nicht autorisierter Personen auf das Terminal ist untersagt).
- Der Administrator muss die Firmware- und Terminalversionen durch Ausführen des Befehls "Version" vom Konfigurationsmenü aus und durch Prüfung des Etiketts an der Rückseite des Terminals überprüfen. Der Administrator muss diese Versionen mit der Version gemäß Herstellererklärung vergleichen.
- Der Administrator muss die standardmäßige Administrator-PIN durch eine neue, individuelle PIN ersetzen.

5.4 Auflagen für den Betrieb des Produkts

Die folgenden Anforderungen müssen erfüllt sein, um einen ordnungsgemäßen Betrieb sicherzustellen:

- Das Terminal darf nur in einer sicheren und zugelassenen Umgebung von identifizierten und autorisierten Personen verwendet werden (unbeaufsichtigter Zugriff nicht autorisierter Personen auf das Terminal ist untersagt).
- Die Benutzer des Produkts -Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 müssen geschult sein und die im Benutzer- und Administratorhandbuch beschriebenen Sicherheitsempfehlungen befolgen.

- Die Benutzer müssen das Produkt-Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 visuell prüfen, um mögliche Änderungen durch einen Angreifer zu erkennen. Die Benutzer müssen insbesondere die Integrität und visuelle Konformität der drei Siegel prüfen (Siegel 1: am oberen und unteren Gehäuserand, Siegel 2: am oberen und unteren Gehäuserand, Siegel 3: am oberen Gehäuserand, am Display und auf der Tastatur). Jeder Versuch, ein Sicherheitssiegel zu entfernen, führt zu einer unumkehrbaren physikalischen Modifizierung, durch die jede erneute Verwendung unmöglich wird.
- Vor jeder Verwendung müssen die Benutzer sich vom Vorhandensein und von der Integrität der drei Siegel überzeugen sowie davon, dass keine sicherheitstechnischen Veränderungen am Kartenterminal vorgenommen worden sind.
- Während der sicheren PIN-Eingabe müssen die Benutzer sicherstellen, dass ein blinkendes Schlüsselsymbol auf dem Bildschirm angezeigt wird und dass ein Pfeil anzeigt, wo die Karte eingesteckt wurde.
- Auf dem mit dem Produkt e-Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 verbundenen Hostcomputer muss eine dedizierte Software installiert sein, die sicherstellt, dass keine Viren oder Trojaner vorhanden sind.

Mit Auslieferung des Produkts e-Health Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14 ist der Benutzer auf die Einhaltung der oben genannten Anforderungen hinzuweisen.

6. Algorithmen und zugehörige Parameter

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

Das Produkt Health Card Terminal GCR5500-D verwendet für den Firmware-Aktualisierungsmechanismus SHA-256-Hash-Funktions- und RSA2048-Signaturprüfalgorithmen. Die Qualifikation gemäß Anhang 1, Abs. I, Nr. 2 der Verordnung zur elektronischen Signatur für diese angewendeten kryptografischen Algorithmen wird entsprechend den von der Bundesaufsichtsbehörde erhaltenen Informationen (siehe) wie folgt klassifiziert:

Algorithmus	Prüflänge	Gültig bis:
SHA-256	256 Bits	31.12.2017
RSA2048	2048 Bits	31.12.2017

* Algorithmenreferenzliste: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 20.05.2011, veröffentlicht am 07. Juni 2011 im Bundesanzeiger Nr.85, Seite 2034.

7. Gültigkeit der Herstellererklärung

Diese Erklärung ist bis zu ihrem Widerruf, längstens jedoch bis zum 31.12.2017 gültig (aufgrund der Gültigkeit der verwendeten Algorithmen).

Die Gültigkeit der Erklärung wird darüber hinaus von der Gültigkeit der Algorithmen eingeschränkt, wie in Kapitel 6 festgelegt. Der Zeitraum der Gültigkeit kann verkürzt werden, wenn beispielsweise neue relevante Verordnungen zur Sicherheit des Produkts oder zur Eignung der Algorithmen von der Bundesnetzagentur veröffentlicht werden.

Der aktuelle Status der Gültigkeit der Erklärung ist bei der zuständigen Behörde (Bundesnetzagentur, Referat Qualifizierte Elektronische Signatur – Technischer Betrieb) zu erfragen.

8. Zusatzdokumentation

Folgende Bestandteile der Herstellererklärung wurden aus dem Veröffentlichungstext ausgegliedert und bei der zuständigen Behörde hinterlegt:

Titel	Referenz	Version	Datum	Anz. Seiten
Health Card Terminal GCR5500-D Security Target	DPC116718	2.8	06.2011	55
Health Card Terminal GCR5500-D Benutzerhandbuch	DPC116770	G	06.2011	19
Health Card Terminal GCR5500-D Administratorhandbuch	DPC117780	F	06.2011	14
Health Card Terminal GCR5500-D Installationsanleitung	DPC117113	F	06.2011	21
Health Card Terminal GCR5500-D Test Documentation	VTR117835	5.1	21.06.11	92
Health Card Terminal GCR5500-D Test Coverage	DPC116734	1.4	25.05.11	12

Ende der Herstellererklärung

