

Herstellereklärung

Die

HID Global GmbH

Am Klingenweg 6a

65396 Walluf

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

eHealth-BCS-Kartenterminal OMNIKEY eHealth 8751 LAN Version 2.06, Firmware 1.32

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

gez. Holger Thomas
Prokura

gez. Gerd Hacker
Prokura

Walluf, den 29.07.2011

Diese Herstellereklärung in Version 1.3 mit der Dokumentennummer eHealth8751LAN-QES-HE 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)
Herstellereklärung zu OMNIKEY eHealth 8751 LAN, Version 1.3

Dokumenthistorie

Version	Datum	Autor	Bemerkung
1.0	08.05.2011	Jacqueline Maatuq	Initialversion
1.1	06.06.2011	Jacqueline Maatuq	Änderungen auf Grund des Observation Reports Version 1.0
1.2	04.07.2011	Jacqueline Maatuq	Änderungen auf Grund des Observation Reports Version 2.0
1.3	29.07.2011	Jacqueline Maatuq	Änderungen auf Grund des Observation Reports Version 3.0

1 Handelsbezeichnung

Die Handelsbezeichnung lautet:

Auslieferung:

Hersteller:

Handelsregisterauszug:

OMNIKEY eHealth 8751 LAN

Version 2.06, Firmware 1.32

Gerät mit installierter Firmware

HID Global GmbH

HRB 20928, Amtsgericht Wiesbaden

2 Lieferumfang und Versionsinformationen

Produktart	Bezeichnung	Version	Übergabeart
Hardware	OMNIKEY eHealth 8751 LAN	2.06	In der Verpackung enthalten
Hardware	Netzwerkkabel (8-adrig, CAT 5 UTP LAN Patch Kabel RJ-45)		In der Verpackung enthalten.
Hardware	Externes AC/DC Steckernetzteil (Input 100-240 V, 0.3A , 50-60 Hz, Output +5V, 2A max.)		In der Verpackung enthalten.
Hardware	Serielles Anschlusskabel für BCS Funktion (4-adrig, 9-Pol. SUB Stecker auf RJ-11m)		In der Verpackung enthalten.
Hardware	USB-RS232 Konverterkabel für BCS Funktion		In der Verpackung enthalten.
Hardware	Grüner Schutzstecker für die Netzwerkbuchse (LAN) am Gerät		In der Verpackung enthalten.
Software	Firmware	1.32	In der Hardware enthalten.
Software	CT-API und Gerätetreiber		Auf der Produkt-CD in der Verpackung bzw. im Internet per Download.
Dokumentation	Bedienungsanleitung		Gedruckt bzw. auf der Produkt-CD als PDF enthalten.
Dokumentation	Lizenzheft		Gedruckt bzw. auf der Produkt-CD als PDF enthalten.
Dokumentation	Ergänzung zum Handbuch - Qualifizierte elektronische Signatur		Gedruckt in der Verpackung

Tabelle 1: Lieferumfang und Versionsinformationen

Das Produkt nutzt bzw. enthält keine weiteren nach SigG bestätigten Produkte.

Das Produkt nutzt keine weiteren Produkte, die ebenfalls nicht Bestandteil dieser Erklärung sind für die eine Herstellererklärung veröffentlicht wurde.

2.1 Reseller

Auf Wunsch wird durch HID Global GmbH das Logo von Vertriebspartnern aufgedruckt, z.B. für die Firma „3M“. Diese Geräte unterscheiden sich lediglich durch das aufgebrachte Logo und sind somit sicherheitstechnisch identisch zum Produkt OMNIKEY eHealth 8751 LAN.

Die Herstellererklärung gilt ebenfalls für diese Terminals.

3 Funktionsbeschreibung

Das eHealth-BCS-Kartenterminal OMNIKEY eHealth 8751 LAN Version 2.06 mit der Firmware 1.32 ist ein Chipkartenleser, der für den Einsatz im Bereich des Gesundheitswesens entwickelt wurde. In diesem Szenario wird der Chipkartenleser an einen Host, in der Regel ein PC, angeschlossen (die Anschlussmöglichkeiten werden weiter unten aufgeführt). Auf dem Host ist eine Anwendungskomponente (z.B. eine Arztsoftware) installiert, die standardisierte Befehle an den Chipkartenleser sendet. Die Firmware des Chipkartenlesers empfängt und interpretiert diese Befehle. Dabei unterscheidet sie zwischen zwei Kommandoarten:

- ✓ Terminalkommandos (z.B. Ausgabe eines Signaltons)
- ✓ Chipkartenkommandos (z.B. Auslesen der Patientendaten einer Krankenversicherungskarte)

Im Gesundheitswesen gibt es bisher zwei Sammlungen standardisierter Terminalbefehle:

- ✓ BCS – Basis Kommando Satz
- ✓ SICCT – Eine umfangreiche Erweiterung des BCS

Die vorliegende Firmware des Chipkartenlesers verarbeitet Befehle des BCS. Durch ein sicheres Upgrade der Firmware wird dann auch der vollständige SICCT-Befehlssatz durch den Chipkartenleser zur Verfügung stehen. Dies stellt keine Einschränkung dar, denn SICCT wird erst in der sogenannten „Online-Phase“ der neuen elektronischen Gesundheitskarte zur Anwendung kommen. HID Global GmbH wird den Download der durch die Gematik zugelassenen Versionen der Firmware auf ihrer Internetseite ermöglichen.

Der Chipkartenleser wird ausgeliefert mit

- ✓ bereits vollständig installierter Firmware

Die aktuelle Zulassungsnummer für den Chipkartenleser ist gematik_BCS_2010_0121_0016.

Der Chipkartenleser bietet Schnittstellen zur Kommunikation mit dem Anwender:

- ✓ Display zur Bedienung – 2 x 20 Zeichen
- ✓ Tastatur zur PIN-Eingabe, Änderung der Geräteeinstellungen – 4 x 5 Tasten
- ✓ LED zur Anzeige einer sicheren Netzwerkverbindung
- ✓ LED's zur Darstellung des sicheren Zustandes während der PIN-Eingabe
- ✓ „Buzzer“ zur Ausgabe von Signaltönen

Der Chipkartenleser kennt, gemäß SICCT, zwei verschiedene Benutzerrollen:

- ✓ Terminal-Benutzer
 - Kann nur Geräteeinstellungen einsehen (z.B. Firmwareversion, Gerätenetzwerkadresse (IP-Adresse))
- ✓ Terminal-Administrator
 - Besitzt die Berechtigungen eines Terminal-Benutzers
 - Muss sich durch die Eingabe der „Geräte-PIN“ (auch Administrator-PIN) am Gerät authentifizieren
 - Kann nach Autorisierung durch das Terminal Änderungen an den Geräteeinstellungen vornehmen oder ein Firmwareupgrade durchführen

Die Geräteeinstellungen des Chipkartenlesers können eingesehen oder geändert werden durch das:

- ✓ Terminalmenü
 - Wird durch Drücken der Menü-Taste am Terminal aufgerufen.
- ✓ Web-Interface
 - Dazu muss das Gerät über die LAN-Schnittstelle an den Host angeschlossen werden. Danach muss die Terminalnetzwerkadresse (IP-Adresse) durch das Terminalmenü ermittelt werden. Anschließend muss die IP-Adresse in ein Browserfenster des Host eingegeben und das Web-Interface aufgerufen werden.

Der Chipkartenleser wird geschützt durch:

- ✓ 2 Sicherheitssiegel
 - Die Siegel sind fälschungssicher und so beschaffen, dass eine Zerstörung oder Ablösung für den Benutzer erkennbar wird

- Der Benutzer muss die Siegel vor der Benutzung des Chipkartenlesers auf Unversehrtheit prüfen
- ✓ Geräte-PIN
 - Sie muss bei Inbetriebnahme vom Administrator geändert werden
 - Sie dient dem Schutz vor unautorisierter Veränderung der Terminaleinstellungen und eines unautorisierten Upgrades der Firmware
- ✓ Aktiver Gehäuseschutz
 - Erkennung einer Manipulation auf der Unterseite des Gerätes, in dem sich die empfindliche Elektronik befindet
 - Eine mögliche Manipulation wird dem Benutzer auf dem Terminal-Display angezeigt
- ✓ Sicherer Firmwareupgrade
 - Um die Echtheit und Korrektheit der zum Download bereitstehenden Firmware zu gewährleisten, wird diese mit einer digitalen Signatur durch die HID Global GmbH versehen. Nach dem Download kann die Firmware von Terminal-Administrator in das Terminal über das Web-Interface des Chipkartenlesers in den Chipkartenleser geladen werden. Der Chipkartenleser prüft die Signatur und die Version der neuen Firmware und lädt sie nach positiver Prüfung in den Speicher. Bei negativem Prüfergebnis jedoch, verweigert der Chipkartenleser die Annahme der Firmware und setzt den Terminal-Administrator davon durch eine Meldung am Terminal-Display in Kenntnis.

Die neue Firmware ist nicht Bestandteil dieser Herstellererklärung.

Auf Grund der oben aufgeführten Sicherheitsfunktionen und Sicherheitsmaßnahmen erfüllt der Chipkartenleser

- ✓ §15 Abs. 4 SigV - Sicherheitstechnische Veränderungen an Produkten für qualifizierte elektronische Signaturen nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden

Der Chipkartenleser kann über folgende Schnittstellen mit dem Host verbunden werden:

- ✓ COM (RS232 bzw. V.24) – mit Hilfe des mitgelieferten Kabels
- ✓ USB – mit Hilfe des mitgelieferten USB-RS232-Konverterkabels und des „COM“-Kabels
- ✓ LAN – mit Hilfe des mitgelieferten Kabels

Die Stromversorgung des Chipkartenlesers erfolgt über ein

- ✓ mitgeliefertes Steckernetzteil

Damit Anwendungskomponenten des Hosts mit dem Chipkartenleser kommunizieren können, benötigen diese, in den meisten Fällen, eine Schnittstellensoftware (CT-API). Hierzu muss der Administrator die

- ✓ mitgelieferte CT-API Software installieren.

Der Chipkartenleser verarbeitet folgende Chipkartentypen:

- ✓ kontaktbehafte Chipkarten (Prozessorchipkarten), die den Spezifikationen [ISO7816] bzw. [EMV2000] genügen und die Übertragungsprotokolle T=0 und T=1 unterstützen (z.B. HBA, eGK,...)
- ✓ kontaktbehafte Speicherkarten, welche die Übertragungsprotokolle 2-Wire, 3-Wire oder I2C unterstützen (z.B. KVK)
- ✓ kontaktlose Chipkarten, die der Spezifikation [ISO 14443] (Typ A und Typ B) genügen (z.B. Karten für die spätere Komfortsignatur im SICCT-Betrieb)

Dazu bietet der Chipkartenleser folgende Schnittstellen:

- ✓ 2 Kartenslots ID-000 (SIM-Karten-Format)
- ✓ 2 Kartenslots ID-1 (Kreditkarten-Format)
- ✓ 1 Feld für kontaktlose Chipkarten (nur SICCT-Betrieb)

Im Parallelbetrieb unterstützt der Chipkartenleser somit bis zu 5 Smartcards. Zur Unterscheidung, auf welchen Kartenslot sich die sichere PIN-Eingabe bezieht, verfügt jeder Slot über eine eigene LED.

Der Chipkartenleser kann eingesetzt werden um Kommandos einer Anwendungssoftware (SAK gemäß § 2 Abs. 11 b) SigG), die eine Eingabe der PIN erforderlich machen, auszuführen. Der Chipkartenleser prüft vor der Ausführung des Kommandos, ob ein gültiges Chipkartenkommando

vorliegt. Erst dann schaltet der Chipkartenleser in den sicheren Modus und zeigt dies dem Anwender durch das Blinken der dem Kartenslot zugeordneten LED an. Der Anwender kann nun seine Chipkarten-PIN auf der Terminal-Tastatur eingeben. Die Rückmeldung an den Anwender erfolgt durch die Darstellung eines Sternchens [*] auf dem Terminal-Display für jede vom Benutzer gedrückte Zifferntaste. Die PIN-Eingabe ist allerdings nur zulässig und sicher, solange die LED des Chipkartenslots blinkt und die Eingabe der PIN unbeobachtet erfolgt. Nach Abschluss der Eingabe fügt der Chipkartenleser die PIN in das übergebene Chipkartenkommando ein und leitet es, an die im Smartcardslot eingesteckte kontaktbehaftete Prozessorchipkarte (SSEE gemäß §2 Abs. 10 SigG), weiter und löscht die PIN vollständig aus seinem Speicher. Die PIN wird niemals über eine der äußeren Schnittstellen des Chipkartenlesers (RS232 / USB oder LAN) übertragen.

Der Chipkartenleser ist somit eine Teil-SAK im Sinne des SigG

- ✓ § 2 Abs. 11 a) - Daten dem Prozess der Erzeugung oder der Prüfung qualifizierter elektronischer Signaturen zuzuführen

Der Chipkartenleser erfüllt somit

- ✓ §15 Abs. 2 Ziffer 1 a) SigV - 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.

Zur Erstellung einer qualifizierten elektronischen Signatur sind ausschließlich kontaktbehaftete Prozessorchipkarten (SSEE gemäß §2 Abs. 10 SigG) zu verwenden.

Alle bisher aufgeführten Funktionen und Hinweise sind ausführlich in folgenden Dokumenten beschrieben :

- ✓ dem mitgelieferten Handbuch
- ✓ der auf CD befindlichen Dokumentation

Der Chipkartenleser darf ohne zusätzliche organisatorische Maßnahmen nur in einer kontrollierten oder geschützten Einsatzumgebung verwendet werden (z.B. Büro, Privatbereich,...).

Der Chipkartenleser wird an Hand folgender Angaben eindeutig identifiziert:

- ✓ Produktname
 - Der Produktname, OMNIKEY eHealth 8751 LAN, ist auf dem Etikett, das sich auf der Geräteunterseite befindet, aufgedruckt.
- ✓ Hardwareversion
 - Die Hardwareversion, 2.06, ist ebenfalls auf dem Etikett, das sich auf der Geräteunterseite befindet, aufgedruckt. Sie beginnt mit einem vorangestelltem großen "V" gefolgt von 3 Ziffern, die nach der 1. Stelle durch einen Punkt "." getrennt sind. Im vorliegenden Fall V2.06.
- ✓ Firmwareversion
 - Die Firmwareversion können Sie mit Hilfe des Terminalmenüs ermitteln.

4 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

Das Produkt OMNIKEY eHealth 8751 LAN Version 2.06 mit der Firmware 1.32 erfüllt die nachfolgend aufgeführten Anforderungen der SigV:

Referenz	Verordnungstext	Beschreibung
§15 Abs. 2	Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass <ol style="list-style-type: none"> 1. bei der Erzeugung einer qualifizierten elektronischen Signatur <ol style="list-style-type: none"> a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden, 	Der Chipkartenleser erfüllt die Anforderungen wie folgt: Die PIN wird, außer zum Zeitpunkt der Verarbeitung, vom Chipkartenleser nicht gespeichert (SF.1). Dem Anwender wird durch den Chipkartenleser die PIN-Eingabe durch Blinken der roten LED des zugehörigen Kartenslots eindeutig angezeigt (SF.1). Der Chipkartenleser stellt sicher, dass die PIN nur zur Chipkarte übertragen wird und niemals über eine der externen Schnittstellen des Chipkartenlesers an den Host übermittelt wird. (SF.2). Der Chipkartenleser stellt sicher, dass die PIN nur

		über PIN-Kommandos mit zulässigen Instruction Bytes an die Chipkarte weitergeleitet wird (SF.2). Während der PIN Eingabe muss der Anwender den Status der LED's dahingehend überprüfen, dass der Modus der sicheren PIN Eingabe aktiv ist und sich der Chipkartenleser im sicheren Zustand befindet. Der Anwender wird im Handbuch auf diese Kontrollpflicht und darüber hinaus auf die Annahmen für die Einsatzumgebung hingewiesen.
§15 Abs. 4	Sicherheitstechnische Veränderungen an Produkten für qualifizierte elektronische Signaturen nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden	Der Chipkartenleser erfüllt die Anforderungen wie folgt: Anhand authentischer und fälschungssicherer Sicherheitssiegel, welche über die Trennkante zwischen Gehäuseunter- und oberteil geklebt werden, kann die Unversehrtheit (Manipulationsfreiheit) der Hardware sicher erkannt werden (SM.SEAL, SF.4). Das Sicherheitssiegel muss regelmäßig vor Benutzung des Chipkartenlesers auf Unversehrtheit überprüft werden. Der Anwender wird im Handbuch auf diese Kontrollpflicht und darüber hinaus auf die Annahmen für die geschützte Einsatzumgebung hingewiesen. Die Integrität und Authentizität wird durch die Signierung der Firmware durch den Hersteller und der Prüfung der Signatur beim Einspielen der Firmware (SF.3) sichergestellt. Der Administrator wird im Handbuch über alle notwendigen Schritte des Upgrades und der Prüfung zur Konformität der Firmware gemäß den Anforderungen SigG / SigV informiert.

4.1 Sicherheitsfunktionen

4.1.1 SF.1 - Speicherwiederaufbereitung

Nach dem Einschalten, dem Weiterleiten eines PIN-Kommandos beziehungsweise dem Ziehen der Chipkarte oder dem Abbruch wird der PIN-Speicherbereich wiederaufbereitet und die LED zur Anzeige der sicheren PIN-Eingabe ausgeschaltet.

4.1.2 SF.2 - Schutz der PIN

Das Umschalten des Kartenterminals in den sicheren PIN-Eingabemodus wird durch ein explizites BCS-Kommando erreicht, welches die Signaturkomponente an das Terminal sendet. Dieses BCS-Kommando enthält die PIN-Handling-Vereinbarungen und das Chipkarten-Kommando, 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, welches explizit eine PIN-Eingabe erwartet. Im PIN-Eingabemodus wird die Eingabe der persönlichen Identifikationsdaten im RAM zwischengespeichert, um sie nach Beendigung der Eingabe direkt mit dem PIN-Kommando zur Chipkarte zu senden.

Der PIN-Eingabemodus wird optisch durch ein rotes Blinken der dem Slot zugeordneten SPE-LED angezeigt, bis die Vollständigkeit der PIN erreicht ist, beziehungsweise der Vorgang abgebrochen wird. Zum Abbruch des Vorgangs zählen das Ziehen der Karte, das Betätigen der Abbruchtaste und das Überschreiten der vorgegebenen Eingabezeit. Der Eingabefortschritt wird im Display mit Sternchen [*] dargestellt.

Zur Weiterleitung bestimmte Chipkartenkommandos sind:

Instruction-Byte	Bezeichnung	Bedeutung	Norm
------------------	-------------	-----------	------

20h	Verify	PIN-Eingabe	ISO 7816-4
24h	Change reference data	PIN ändern	ISO 7816-8
26h	Disable verification requirement	PIN aktivieren	ISO 7816-8
28h	Enable verification requirement	PIN deaktivieren	ISO 7816-8
2Ah	Perform security operation	PIN verschlüsseln	ISO 7816-8
2Ch	Reset retry counter	PIN entsperren	ISO 7816-8

Bei allen anderen Chipkartenkommandos beendet der Chipkartenleser die Ausführung des BCS-Kommandos und sendet einen BCS-Fehlercode an den Host.

4.1.3 SF.3 Firmware Download

Der Chipkartenleser unterstützt den nachträglichen Download von Firmware.

Die Firmware ist digital signiert, entsprechend der Technischen Richtlinie [BSI TR03116] des BSI. Die verwendeten Algorithmen (SHA 512 und RSA 2048) genügen auch der Vorgaben der BNetzA [BNetzA_Algo_2011]. Der Signaturschlüssel ist nur im Besitz des Herstellers und wird dort durch eine Smartcard mit PIN geschützt und sicher verwahrt.

Das Nachladen von Firmware ist nur durch Personal gestattet, dessen Berechtigung hierzu vorab geprüft wird (SF.5).

Für einen erfolgreichen Download ist es erforderlich, dass:

- ✓ die Version der zu ladenden Firmware höher ist als die der bereits geladenen Firmware
- ✓ die Signatur erfolgreich geprüft wurde

4.1.4 SF.4– Aktiver Gehäuseschutz

Der Chipkartenleser verfügt über einen aktiven Gehäuseschutz, der die komplette Unterseite inklusive der Verschraubung abdeckt. Eine Manipulation des Chipkartenlesers von der Unterseite wird durch die Firmware erkannt, auch wenn der Chipkartenleser über einen längeren Zeitraum ausgeschaltet war. Erkennt die Firmware einen Verdacht auf Manipulation, kann der Chipkartenleser erst nach erfolgreicher PIN Authentisierung der Geräte-PIN wieder in Betrieb genommen werden

4.1.5 SF.5 – Nutzerverwaltung (Geräte-PIN / Administrator-PIN)

Beim ersten Start des Chipkartenlesers muss der Administrator die Transport-PIN in eine mindestens 6- bis maximal 20-stellige individuelle Geräte-PIN ändern. Im Handbuch ist dieser Vorgang ausführlich beschrieben.

Nur ein Administrator kann Firmware downloaden oder Einstellungen am Gerät verändern.

Sicherheitsrelevante Einstellungen (SF.3 und SF.4) können durch das Menüsystem des Chipkartenlesers durchgeführt werden. Dazu muss sich der Administrator mit einem numerischen Passwort am Chipkartenleser selbst authentisieren.

4.2 Sicherheitsmaßnahmen

4.2.1 SM.SEAL - Sicherheitssiegel

Anhand authentischer und fälschungssicherer Sicherheitssiegel, welche über die Trennkante zwischen Gehäuseunter- und Oberteil geklebt werden, kann die Manipulationsfreiheit der Hardware sicher erkannt werden. Dies wird dadurch sichergestellt, dass ein Öffnen nicht ohne Beschädigung des Siegels möglich ist. Die Beschaffenheit (Zerstöreeigenschaften) des Siegels gewährleistet, dass es nicht unbeschädigt entfernt und wieder aufgeklebt werden kann.

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

Trifft für dieses Produkt nicht zu.

Diese Anforderungen sind für das Produkt OMNIKEY eHealth 8751 LAN nicht relevant, da das Produkt die Überprüfung qualifizierter elektronischer Signaturen und die Generierung qualifizierter Zeitstempel nicht unterstützt.

5 Maßnahmen in der Einsatzumgebung

5.1 Einrichtung der IT-Komponenten

Dieses Kapitel entfällt, da keine Vorgaben bzgl. der IT Komponenten gemacht werden müssen, um die Sicherheitsfunktionen zu erfüllen.

5.2 Anbindung an ein Netzwerk

Die Sicherheitsfunktionalität des Chipkartenlesers ist unabhängig von der ansteuernden SAK.

Die Signaturkomponente auf dem Hostsystem muss gegenüber folgenden potentiellen Bedrohungen geschützt werden:

- Potentiellen Angriffen aus dem Internet
- Potentiellen Angriffen aus einem angeschlossenes Intranet
- Manuellem Zugriff Unbefugter
- Dem Datenaustausch per Datenträger

Der Administrator hat durch technische Mittel (z.B. Firewalls, aktuelle Anti-Virensoftware) und organisatorische Maßnahmen (z.B. Zutritts- und Zugriffsbeschränkungen) für die Einhaltung der oben genannten Punkte Sorge zu tragen.

5.3 Auslieferung und Installation

Das Produkt OMNIKEY eHealth 8751 LAN Version 2.06, Firmware 1.32 wird bereits vorkonfiguriert und mit den in Tabelle 1 beschriebenen Komponenten ausgeliefert.

Der Administrator muss sich von der Echtheit und Unversehrtheit des Gerätes überzeugen.

Des Weiteren muss der Administrator vor der ersten Inbetriebnahme die Geräte-PIN des Gerätes ändern.

Diese Punkte sind ausführlich im Handbuch beschrieben.

5.4 Auflagen für den Betrieb des Produktes

Um einen sachgemäßen Einsatz des Geräts zu gewährleisten sind folgende Bedingungen einzuhalten:

- ✓ Der Anwender muss mit seiner PIN sorgsam umgehen und sie geheim halten.
- ✓ Der Anwender muss seine PIN unbeobachtet auf der Terminal-Tastatur eingeben.
- ✓ Der Anwender muss während der Eingabe der PIN darauf achten, dass die LED des Chipkartenslots durch Blinken den Modus der sicheren PIN-Eingabe signalisiert.
- ✓ Zur sicheren PIN-Eingabe müssen ausschließlich sichere SSEE (Prozessorkarten) und sichere SAKs (Anwendungssoftware) eingesetzt werden, die den Anforderungen des SigG / SigV und den Spezifikationen ISO 7816 oder EMV 2000 genügen.
- ✓ Der Anwender muss sich vor der Benutzung des Gerätes von der Unversehrtheit der Sicherheitssiegel und des Gerätes überzeugen.
- ✓ Der unautorisierte Zugang zum Chipkartenleser ist zu unterbinden.
- ✓ Der Chipkartenleser darf ohne zusätzliche organisatorische Maßnahmen nur in einer kontrollierten oder geschützten Einsatzumgebung verwendet werden (z.B. Büro, Privatbereich,...).

6 Algorithmen und zugehörige Parameter

Trifft für dieses Produkt nicht zu.

Dieser Abschnitt entfällt, da der Chipkartenleser 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, aufgrund der zum Firmwareupdate verwendeten Algorithmen (SHA 512 und RSA 2048) bis zum 31.12.2017 gültig.

Diese Herstellererklärung kann durch die Bundesnetzagentur oder den Hersteller selbst widerrufen werden.

8 Zusatzdokumentation

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

Name	ID	Version	Datum	Seitenanzahl
Bedienungsanleitung	8751-901	A.126	5.4.2011	43
Ergänzung zur Bedienungsanleitung - Qualifizierte elektronische Signatur	eHealth8751LAN_QES_AGD.doc	1.1	19.5.2011	8
Sicherheitsvorgaben	eHealth8751LAN_QES_ASE.doc	1.10	5.7.2011	22
Testdokument	eHealth8751LAN_QES_ATE.doc	1.20	29.7.2011	37

9 Anhang

Abkürzungen

BCS	Basic Command Set
BNetzA	Bundesnetzagentur
CT	Card Terminal
CT-API	CT-Application Programming Interface
Gematik	Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
HBA	Heilberufsausweis
PC	Personal Computer
SAK	Signaturanwendungskomponente
SEE	Signaturerstellungseinheit
SICCT	Secure Interoperable Chip Card Terminal
SPE	Secure Pin Entry (Sichere PIN Eingabe)
SSEE	Sichere SEE

9.1 Literaturverzeichnis

[BNetzA_Algo_2011]	Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), vom 20. Mai 2011, veröffentlicht am 07. Juni 2011 im Bundesanzeiger Nr. 85, Seite 2034
[BNetzA_Einsatzbed]	Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten, Version 1.4, Stand: 19.07.2005
[BSI TR03116]	BSI TR - 03116, Technische Richtlinie für die eCard-Projekte der Bundesregierung, Version 1.0 vom 23.03.2007
[EMV2000]	EMV 2000 Book 1 - Application independent ICC to Terminal Interface requirements, Version 4.0, December 2000
[ISO7816]	DIN ISO 7816 - 1 Identification cards - Integrated circuit(s) cards with contacts – Physical Characteristics DIN ISO 7816 - 2 Identification cards - Integrated circuit(s) cards with contacts - Dimensions and locations of the contacts DIN ISO 7816 - 3 Identification cards - Integrated circuit(s) cards with contacts - electrical characteristics and transmission protocols DIN ISO 7816 - 4 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Inter - industry commands for interchange DIN ISO 7816 – 8 Identification cards – Integrated circuit(s) cards with contacts – Security related interindustry commands
[ISO14443]	ISO14443 - 1 Physical characteristics (2008, Erstausgabe 2000) ISO14443 – 2 Radio frequency power and signal interface (2008, Erstausgabe 2001)

	ISO14443 – 3 Initialization and anticollision (2008, Erstausgabe 2001) ISO14443 – 4 Transmission protocol (2008, Erstausgabe 2001)
[TR3120Anhg]	Technische Richtlinie BSI TR-03120 - Anhang 1: Kartenterminalversiegelung -, Version 1.0.2 vom 04.04.2008

Ende der Herstellererklärung zum Produkt OMNIKEY eHealth 8751 LAN Version 2.06