ST-1530

MOBILES TERMINAL

HINWEISE ZUR DATENSICHERHEIT

6440574-01, DE, Apr 2012 (DS ST-1530)

Inhaltsverzeichnis

1 Allgemein

Das Chipkartenterminal **CHERRY ST-1530** ist für den Einsatz im deutschen Gesundheitswesen vorgesehen. Es erfüllt die Anforderungen der „Kassenärztlichen Bundesvereinigung" (KBV) zum Lesen der Krankenversicherungskarte (KVK) und die Anforderungen der „Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH" (gematik) zur Verarbeitung der neuen elektronischen Gesundheitskarte (eGK).

2 Sicherheitsmerkmale

Zu den Anforderungen gehört, dass der Benutzer des Gerätes sich mit dem Gebrauch vertraut macht und die einwandfreie Funktion und die Sicherheitsmerkmale regelmäßig überprüft.

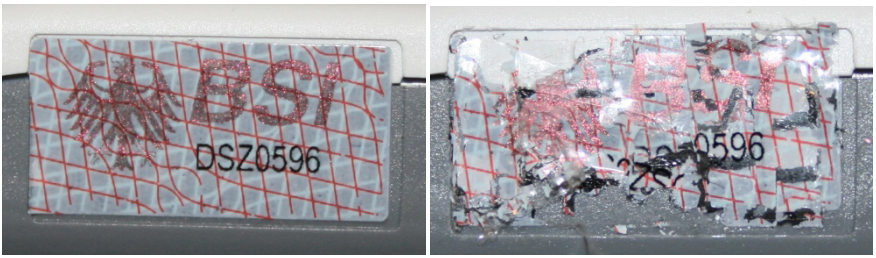
2.1 Siegel

2.1.1 Siegeleigenschaften

Mit einer „Kippfarbe" sind der Bundesadler und rechts davon das BSI Logo auf das Siegel gedruckt. Je nach Betrachtungswinkel erscheint die Farbe zwischen gold nach ocker zu grün. Unterhalb des BSI Logos ist die schwarz gedruckte, verkürzte BSI-Zulassungsnummer des Gerätes zu finden. Beim Cherry Mobilgerät ist dies: DSZ0596.

Unter einer speziellen Schwarzlichtlampe (UV) wird der Schriftzug „SECURITY" mehrzeilig über die ganze Siegelfläche sichtbar. Ein gefälschtes Siegel ist an den fehlenden Sicherheitsmerkmalen zu erkennen.

Bei einer Manipulation spalten sich die Schichten des Siegels und die sich lösende Schicht zerfällt in kleine Bruchstücke. Die Abbildung links zeigt das Siegel unversehrt, die rechte Abbildung zeigt das Siegel nach einer partiellen Ablösung und dem Versuch eines deckungsgleichen Wiederaufbringens.

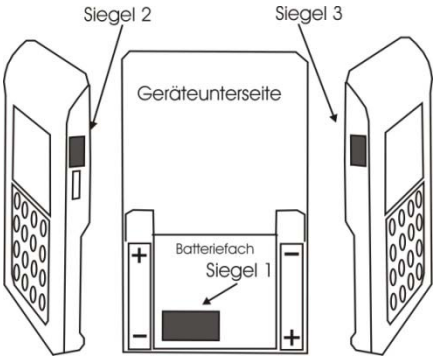


Wenden Sie sich an Ihren Lieferanten, wenn das Siegel beschädigt ist bzw. wenn Sie Zweifel an der Echtheit des Siegels haben.

2.1.2 Siegel prüfen

Um Manipulationen am Gerät zu erkennen, prüfen Sie vor der Inbetriebnahme und regelmäßig, insbesondere nach längeren Abwesenheiten, die Siegel auf Unversehrtheit und Echtheit. Die Lage der Siegel ist in den Skizzen dargestellt. Eines befindet sich unter dem Batteriefachdeckel auf der Geräteunterseite, jeweils ein weiteres an der linken und rechten Seite in Displayhöhe.

Hinweis: Berühren Sie beim Umgang mit dem Gerät möglichst nicht die Siegel bzw. behandeln Sie diese mit Vorsicht, um sie nicht zu beschädigen.



2.2 Geräteversion

Die Zertifizierung erfolgt nach CC = Common Criteria. Die vollständige BSI-Zertifizierungsnummer ist: BSI-DSZ-CC-0596. Auf den Gerätesiegeln finden Sie die verkürzte Nummer: DSZ0596.

Welche Geräteversion zertifiziert ist, finden Sie unter anderem im Internet auf den Seiten des BSI (Bundesamt für Sicherheit in der Informationstechnik): http://www.bsi.bund.de

Vergleichen Sie die Angaben auf den BSI-Seiten mit der Version der Gerätesoftware, die im Statusmenü (Menü\F2\ 33) des Gerätes angezeigt wird.

2.2.1 Integritätsprüfung

Das Gerät wird bei jedem Einschalten einer Softwareprüfung unterzogen. Das Ergebnis wird mit einem Vorgabewert verglichen. Ist das Ergebnis korrekt, geht das Gerät in Betrieb. Bei einem Fehler gibt es einen langen Dauerton und im Display steht: „ERROR" „Integrität". Nach etwa 5 Sekunden schaltet sich das Gerät aus. Tritt der Fehler bei erneutem Einschalten nochmals auf, ist das Gerät einzuschicken, die Software ist defekt und eine einwandfreie Funktion unter Umständen nicht mehr gegeben. Die Integritätsprüfung ist auch einer der Tests, die Sie im Menü: Service\Test... aufrufen können. Wird hierbei ein Fehler angezeigt, wird das Gerät mit dem nächsten Einschalten nicht mehr in den Betriebsmodus gehen.

2.3 Typenschild

Auf dem Typenschild steht unter anderem der Herstellername „Ingenico Healthcare", der Gerätename „ST-1530" die Information, welchen Hardware-Code (HC) das Gerät hat und die einmalige Seriennummer (SN) des Geräts.

3 Sicherheit bei der Inbetriebnahme

3.1 Aufstellungshinweise

Aus Gründen der Datensicherheit möchten wir darauf hinweisen, dass das Kartenterminal bei der Verwendung nur in einer sicheren Einsatzumgebung betrieben werden darf, in welcher es nie unbeaufsichtigt ist. Nach Dienstschluss ist das Gerät in einem verschlossenen Raum zu verwahren. Es ist sicherzustellen, dass unbefugte Personen keinen Zugang zum Gerät und angeschlossenen Systemeinheiten haben. Das Gerät darf nur von geschultem Personal bedient bzw. nur unter Aufsicht des geschulten Personals betrieben werden.

3.2 Admin-PIN-Eingabe bei der ersten Inbetriebnahme

Bei der ersten Inbetriebnahme muss als erstes eine aus acht Ziffern bestehende Administrator-PIN (Admin-PIN) vergeben werden. Die Admin-PIN ist die gesicherte Zugangsberechtigung zu den Einstellungen Ihres Gerätes und zu den gespeicherten Daten.

Die sichere Admin-PIN-Eingabe wird durch acht Schlosssymbole im Display dargestellt. Vermeiden Sie bei Ihrer Wahl konstante oder auf-/absteigende Ziffernfolgen (00000000, 12345678 etc.), die leicht zu „erraten" sind.

Notieren Sie die Admin-PIN und bewahren Sie sie unter Verschluss auf. Geben Sie Ihre PIN niemals bekannt. Bitte achten Sie darauf, dass Sie bei der Eingabe einer PIN nicht beobachtet werden. Stellen Sie sicher, dass das Gerät jederzeit vor unbefugtem Zugriff geschützt ist!

Werden Sie bei der ersten Inbetriebnahme nicht zur Eingabe aufgefordert, nehmen Sie das Gerät nicht in Betrieb und kontaktieren Sie Ihren Gerätelieferanten!

3.3 PIN-Trennung

Sind der Administrator Ihres Systems (Ihres Gerätes) und der Benutzer (User) Ihrer gespeicherten Daten nicht dieselbe Person, sollte die Zugriffsberechtigung aufgeteilt werden. Wählen Sie dazu in der PIN-Verwaltung des Gerätes den Menüpunkt „getrennte PINs", und schalten Sie ihn ein. Die Administrator-PIN behält den Zugriff auf die Geräteeinstellungen, hat aber nach der ersten User-PIN-Eingabe keinen Zugang mehr zu den gespeicherten Daten. Die zusätzliche User-PIN erlaubt nur den Zugriff auf

die Datenverwaltung und die Änderung der User-PIN. Auch der User sollte seine PIN notieren und unter sicherem Verschluss verwahren.

3.4 PIN-Zeitsperre

Nach drei fehlerhaften Eingaben wird die PIN-Eingabe für 1 Minute gesperrt! Weitere Fehleingaben verlängern die Sperrzeit bis zu 24 Stunden. Sollten Sie Ihre Admin-PIN vergessen haben, können Sie ab SW 3.20 eine neue PIN vom Gerätehersteller anfordern. Hierfür ist ein sicheres Vergabeverfahren notwendig. Bitte setzen Sie sich hierfür mit der Service-Hotline des Geräteherstellers in Verbindung.

4 Verwendung als Signaturanwendungs-komponente

4.1 Eingabe einer Karten-PIN nach Aufforderung

Nach dem Stecken einer Karte können Sie zum Aktivieren/Freischalten der Karte oder zur Durchführung bestimmter sicherheitsrelevanter Funktionen zwecks Berechtigungsprüfung zu einer Karten-PIN-Eingabe aufgefordert werden. Die Karten-PIN hat nichts mit der „Administrator"-PIN des Gerätes zu tun. Sie dient der Authentisierung gegenüber der Karte. Bitte achten Sie darauf, dass Sie, aber auch andere Benutzer, Ihre Karten-PIN geheim halten und bei der Eingabe der PIN nicht beobachtet werden. Die PIN-Eingabe erfolgt auf der Kartenlesertastatur. In dem Hinweis zur sicheren PIN-Eingabe (nächste Seite) wird der Ablauf genau beschrieben.

4.2 Ablauf einer Karten-PIN-Eingabe

Die Aktivierung dieser sicheren Betriebsart wird dadurch angezeigt, dass die einzugebenden PIN-Ziffern durch blinkende Schlosssymbole im Display dargestellt werden. Nur wenn diese Symbole erscheinen, ist sichergestellt, dass die eingegebene PIN ausschließlich zur gesteckten Karte übertragen wird. Die Durchführung der Signatur im Kartenterminal beginnt normalerweise mit der Ausgabe des Anzeigetextes:

„Bitte Geheimzahl eingeben"

und in der Zeile darunter:  für die Eingabe einer z. B. 6stelligen PIN.

4.2.1 Fehlerfreier Ablauf

Geben Sie die Signatur-PIN über die Tastatur nur ein, wenn die Schlosssymbole dargestellt werden. Die abgefragte PIN (üblicherweise min. 6, max. 8 Ziffern) wird im Display nach der Eingabe mit einem Sternchen pro eingegebener Ziffer angezeigt. Bestätigen Sie abschließend mit **OK**. Anschließend wird das PIN-Kontrollkommando zur Chipkarte übertragen. Bei erfolgreicher Eingabe der korrekten PIN wird im Display der Anzeigetext**: „Aktion erfolgreich"** ausgegeben.

4.2.2 Ablauf bei inkorrekter PIN-Eingabe

Der Ablauf ist derselbe wie bei der Eingabe der korrekten PIN, doch wird der Anzeigetext: „**Geheimzahl falsch / gesperrt"** ausgegeben.

4.2.3 Ablauf bei Abbruch der PIN-Eingabe durch den Benutzer

Drückt der Benutzer vor Abschluss der PIN-Eingabe die Taste **STOP**, wird kein Kommando zur Chipkarte geschickt und im Display wird der

Anzeigetext: **„Abbruch"** ausgegeben.

4.2.4 Ablauf im Fall von Zeitüberschreitung bei der PIN-Eingabe

Erfolgt nach der Eingabeaufforderung nicht innerhalb von 15 Sek. die Eingabe der ersten Ziffer oder verstreicht mehr Zeit als 5 Sek. bis zur Eingabe der jeweils nächsten Ziffer, dann wird im Display der Anzeigetext: **„Abbruch"** ausgegeben. Hat der Benutzer nur das Drücken der Taste **OK** vergessen, dann fordert das Kartenterminal den Benutzer mit dem Anzeigetext: **„Bitte Eingabe bestätigen"** zur Bestätigung der eingegebenen Geheimzahl auf.

5 Regeln zur Betriebssicherheit

Neben den Sicherheitsregeln bei der Inbetriebnahme müssen Sie eine Reihe von Maßnahmen treffen, um die Sicherheit Ihres Systems und der Patientendaten dauerhaft zu gewährleisten. Nehmen Sie das Gerät nicht in Betrieb, wenn Sie Zweifel an der Sicherheit haben.

- Es dürfen nur Personen mit dem Gerät arbeiten, die die Bedienungsanleitungen gelesen haben und geübt sind im Umgang mit technischem Gerät. Der Bediener sollte die gleiche Sorgfalt im Umgang mit dem Gerät anwenden wie im Umgang mit gespeicherten Daten.
- Vor jeder Benutzung sollten Sie das Gerät auf Manipulationen hin untersuchen. Prüfen Sie, ob das Gerät Veränderungen wie zum Beispiel Bohrungen aufweist, die unter Umständen mit Aufklebern verdeckt sind. Achten Sie auf Veränderungen am Karteneinführungsschlitz, dem Tastenfeld und im Batteriefach. Prüfen Sie die Siegel wie bei der ersten Inbetriebnahme. Prüfen Sie die angezeigte Uhrzeit und das Datum. Prüfen Sie anhand der oben angegebenen BSI-Webadresse, ob die Version der Gerätesoftware (Menü\F2\ 33) und der Hardware-Code (HC) auf dem Typenschild und die Zertifizierungsnummer auf den Siegeln mit dem zugelassenen Stand übereinstimmen.
- Wird das Gerät an Ihren PC angeschlossen, überzeugen Sie sich davon, dass die Verkabelung im Originalzustand ist und keine zusätzlichen Teile angebracht sind. Schließen Sie das Gerät nicht an „fremde" PCs an.
- Während der Benutzung darf das Gerät niemals unbeaufsichtigt sein.
- Übergeben Sie das Gerät niemals im aufgeschlossenen Zustand an andere. Verschließen Sie den Zugang, indem Sie vom Ruhezustand aus einmal die Taste **F2** drücken.
- Achten Sie darauf, dass Sie bei der PIN-Eingabe nicht beobachtet werden und angezeigte Patientendaten nicht von Dritten eingesehen werden können.
- Entfernen Sie nach der Benutzung alle eventuell noch steckenden Karten. Nach Gebrauch soll das Gerät unter Verschluss sicher verwahrt werden. Vergewissern Sie sich, dass keine Manipulation an der sicheren Verschlussmöglichkeit stattgefunden hat.
- Vergewissern Sie sich, dass das Gerät nach dem Gebrauch ausschaltet, bevor Sie es wegschließen.

- Notieren Sie sich die „persönlichen" Kennzeichen Ihres Gerätes als Identifizierungshilfe bei Ihren späteren Überprüfungen.

Gerät (Typ): _____

Hersteller: ZF Friedrichshafen AG, Electronic Systems

Seriennummer (SN): _____

Hardware-Code /HC): _____

BSI-Zertifizierungsnummer: BSI-DSZ-CC-0596

Software Version: _____

Software Datum: _____

Loader Version: _____

- Falls das Gerät nicht ordnungsgemäß funktioniert (z. B. Tastendruck wird nicht mehr angenommen), wenden Sie sich bitte an den Service des Herstellers oder Händlers.

6 EG-Konformitätserklärung

EG - KONFORMITÄTSERKLÄRUNG
DECLARATION OF EG - CONFORMITY

Wir / *We*

Ingenico Healthcare GmbH
(Name des Anbieters / supplier's name)
Konrad-Zuse-Ring 1, D - 24220 Flintbek
(Anschrift / address)

erklären in alleiniger Verantwortung, dass das Produkt,
declare under our sole responsibility that the product,

Chipkartenterminal Serie ORGA 900
(Bezeichnung, Typ oder Modell / name, type or model)

Ser. XX1X0000000001
(Los-, Chargen oder Seriennummer, möglichst Herkunft und Stückzahl)
(lot, batch or serial number, possibly sources and numbers of items)

auf das sich diese Erklärung bezieht, mit der/den folgenden Norm(en) oder normativen Dokument(en) übereinstimmt
to which this declaration relates is in conformity with the following standard(s) or other normative document(s)

EN 61000-6-3 Störemission (08.02)
EN 55022 Kl.B (09.03)
EN 61000-6-2 Störfestigkeit (08.02)
EN 61000-4-2 (12.01), -3 (03.03)

Titel und/oder Nummer sowie Ausgabedatum der Norm(en) oder der anderen normativen Dokumente
Title and/or number and date of issue of the standard(s) or other normative document(s)

(falls zutreffend) gemäß den Bestimmungen der Richtlinie
(if applicable) following the provisions of directive

73 / 23 / EWG
89 / 336 / EWG

veröffentlicht im / *published in* Amtsblatt der EG Nr. L 139 S.19

(K. Erichsen)

Flintbek, den 27.01.2012 ppa.

Ort, Datum der Ausstellung
place and date of issue

Namen und Unterschriften
oder gleichwertige Kennzeichnung der Befugten
names and signatures or equivalent marking of authorized persons

ZF Friedrichshafen AG
Electronic Systems
Cherrystraße
91275 Auerbach

www.cherry.de

E-Mail: info@cherry.de

Telefon:

Vertrieb: +49 (0) 180 5 243779* (0180 5 CHERRY*)
Technischer Support: +49 (0) 180 5 919108*
(*14 Cent/Min. aus dem deutschen Festnetz, abweichende Preise für Anrufe aus Mobilfunknetzen möglich.)

Bitte halten Sie bei Anfragen an den Technischen Support folgende Informationen bereit:

- Artikel- und Serien-Nr. des Produkts
- Bezeichnung und Hersteller Ihres PCs/Notebooks oder Motherboards
- Betriebssystem und ggf. installierte Version eines Service Packs