eGK Tastatur G87-1505

Handbuch für Administratoren

6440650-04, DE, Feb 2018 (G87-1505 = Mod. G-1505)

Inhalt

Herzlichen Glückwunsch!

CHERRY entwickelt und produziert seit 1967 innovative Eingabe-Systeme für Computer. Den Unterschied in Qualität, Zuverlässigkeit und Design können Sie jetzt mit Ihrem neuen Gerät erleben.

Bestehen Sie immer auf Original CHERRY.

Die **G87-1505** wurde für die Verwendung mit der elektronischen Gesundheitskarte (eGK) und der Krankenversichertenkarte (KVK) entwickelt. Sie zeichnet sich besonders durch folgende Eigenschaften aus:

- gematik zugelassen
- Secure Interoperable ChipCard Terminal (SICCT)
- Sichere PIN-Eingabe
- Investitionssicher, da upgradefähig

Die Bedienung und Konfiguration des Geräts ist weitgehend selbsterklärend durch die Navigation am Display oder in der Software am PC.

Für Informationen zu weiteren Produkten, Downloads und vielem mehr, besuchen Sie bitte **https://www.cherry.de**.

Wir wünschen Ihnen viel Vergnügen mit Ihrer **G87-1505**.

Ihr CHERRY Team

Zu diesem Handbuch

Dieses Handbuch enthält Handlungsabläufe und Informationen für Administratoren zur Installation, Inbetriebnahme, Konfiguration und zum sicheren Betrieb der **G87-1505**.

Es wurde auf der Basis der Kartenterminal-Firmware in der Version 3.0.1 erstellt. Für neuere Firmware-Versionen kann der Inhalt abweichen.

Sofern nicht anders angegeben, beziehen sich die Begriffe "Terminal" bzw. "Kartenterminal" immer auf das in der Tastatur integrierte Kartenterminal.

Kurzanleitung

Für Benutzer des Kartenterminals liegt der Tastatur folgende Kurzanleitung bei:

- Kurzanleitung eGK Tastatur G87-1505 (Artikel-Nr. 6440649-02)

Sie beschreibt die Bedienung der in Betrieb befindlichen Tastatur für Beschäftigte im deutschen Gesundheitswesen.

Lieferumfang

Der Lieferumfang der **G87-1505** enthält:

- Tastatur G87-1505
- Kurzanleitung für Benutzer
- 4 Slotsiegel für gSMC-KT und SMC-B Steckplatz
- Optional: gSMC-KT (Bezugsquellen für eine gSMC-KT finden Sie auf **https://www.cherry.de/eHealth**)

Software

Zu dem Kartenterminal steht Ihnen unter **https://www.cherry.de** folgende Software inklusive Anleitung zur Verfügung:

- CHERRY **eHealth USB-LAN Proxy** (ab Version 2.1.0.8)
- CHERRY **eHealth Device Manager** (ab Version 2.1.0.6)

Verwenden Sie immer die aktuelle Version.

SICHERHEIT

1 Dokument prüfen

1 Berechnen Sie mit einem der öffentlich verfügbaren Programme die SHA-256 Prüfsumme der Datei dieses Handbuchs.

2 Vergleichen Sie die berechnete Prüfsumme mit der veröffentlichten SHA-256 Prüfsumme zur Authentizität dieses Handbuchs. Diese finden Sie auf **https://www.cherry.de** im Downloadbereich dieses Handbuchs.

Wenn die Prüfsummen nicht übereinstimmen, wurde die Datei auf dem Übertragungsweg verändert und darf nicht verwendet werden.

2 Bestellung und sichere Auslieferung

2.1 Sichere Lieferkette prüfen

Die **G87-1505** darf nur über die auf unserer Homepage **https://www.cherry.de/eHealth** gelisteten Vertriebspartner oder deren Unterauftragsnehmer bestellt werden. Auf der Webseite des jeweiligen Vertriebspartners können Sie weitere Informationen über die zur Verfügung stehenden Bezugsquellen einsehen.

Die Auslieferung muss immer unter Einhaltung der sicheren Lieferkette erfolgen, die im Rahmen der Zulassung zertifiziert wurde.

Alle Beteiligten am Lieferprozess müssen darüber Auskunft geben, von wem sie das Gerät erhalten und an wen sie das Gerät ausgeliefert haben. Somit kann der Weg des Geräts komplett nachvollzogen werden. Entweder vom Händler bis zum Hersteller oder umgekehrt.

Überprüfen Sie die Lieferkette wie folgt:

1 Prüfen Sie anhand der Lieferankündigung, wie und durch wen das Gerät angeliefert werden sollte und ob dies den Tatsachen entspricht. (Die Lieferankündigung kann in der Bestellbestätigung enthalten sein.)

ACHTUNG: Verdacht auf Manipulation

Sollten Sie keine Lieferankündigung erhalten haben und können Sie die Anlieferung nicht überprüfen, ist davon auszugehen, dass das Gerät manipuliert wurde.

- Nehmen Sie das Gerät auf keinen Fall in Betrieb.
- Wenden Sie sich an Ihren Gerätelieferanten und fordern ein Austauschgerät an.

2 Prüfen Sie vor dem Auspacken die Sicherheitsmerkmale der Verpackung (siehe 2.2 "Sicherheitsmerkmale der Verpackung prüfen").

3 Prüfen Sie die Echtheit des Geräts, indem Sie unter **https://www.cherry.de/eHealth** oder über die Supporthotline die Seriennummer der Sicherheitsversandtasche (siehe 2.2 "Sicherheitsmerkmale der Verpackung prüfen") sowie die Seriennummer und die MAC-Adresse der **G87-1505** (angebracht auf der Rückseite der Kurzanleitung) angeben. Sie erhalten als Rückmeldung, ob es sich um ein sicher ausgeliefertes Originalprodukt handelt.

4 Prüfen Sie, ob alle Beteiligten am Lieferprozess vertraglich in die Pflichten der sicheren Lieferkette eingebunden sind:

- Prüfung der direkten Vertragspartner (z. B. Liste der zugelassenen Vertriebspartner oder deren Unterauftragsnehmer auf unserer Homepage **https://www.cherry.de/eHealth**, Kontaktaufnahme zum Verkäufer oder PED)
- Kontaktieren Sie unsere Supporthotline, um weiterführende Informationen zur Lieferkette zu erhalten.

5 Bewahren Sie alle Dokumente zur Auslieferung auf, um später die Echtheit des Geräts belegen zu können. Außerdem ist dadurch ein möglicher Austausch des Geräts nachweisbar.

2.2 Sicherheitsmerkmale der Verpackung prüfen

ACHTUNG: Verdacht auf Manipulation bei unerfüllten Sicherheitsmerkmalen

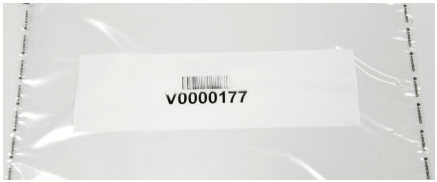
Ist der Produktkarton oder die Sicherheitsversandtasche beschädigt oder ist eines der unten beschriebenen Sicherheitsmerkmale nicht erfüllt, ist davon auszugehen, dass die Verpackung und/oder das Gerät manipuliert wurde.

- Packen Sie das Gerät nicht weiter aus.
- Nehmen Sie das Gerät auf keinen Fall in Betrieb.
- Wenden Sie sich an Ihren Gerätelieferanten und fordern ein Austauschgerät an.

Die eGK Tastatur **G87-1505** wird in einem bedruckten Produktkarton verpackt.

Dieser Karton ist von einer speziell für CHERRY hergestellten Sicherheitsversandtasche mit den folgenden Merkmalen umschlossen:

1 Die Sicherheitsversandtasche hat eine aufgedruckte Seriennummer und einen Barcode, siehe nachfolgende Abbildung:

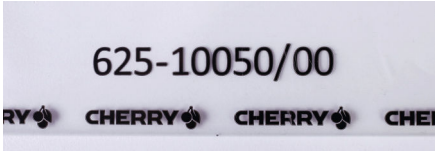


Diese Seriennummer wird zusammen mit der Seriennummer der **G87-1505** bei der Produktion gespeichert.
Prüfen Sie, ob die Seriennummer der Sicherheitsversandtasche nicht überklebt ist. Die Seriennummer der Sicherheitsversandtasche wird für die Überprüfung der Echtheit des Geräts benötigt (siehe 2.1 "Sichere Lieferkette prüfen").

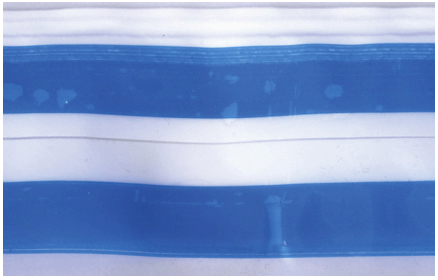
2 Die Sicherheitsversandtasche hat entlang der Außenkante einen durchgängigen CHERRY-Aufdruck.
Prüfen Sie, ob dieser Aufdruck ununterbrochen und unbeschädigt ist.

3 An den Längskanten der Sicherheitsversandtasche befindet sich jeweils eine Schweißnaht.
Prüfen Sie, ob diese Schweißnähte geschlossen sind und sich der CHERRY-Aufdruck außerhalb der Schweißnaht befindet:

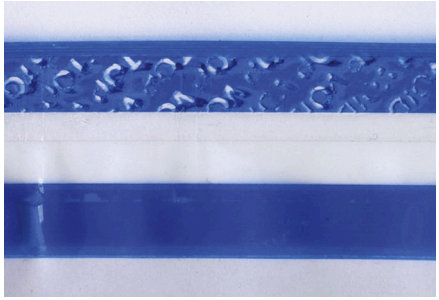
4 Die untere Kante der Tasche ist durchgängig und hat keine Schweißnaht.
Prüfen Sie, ob die Unterkante unbeschädigt und nicht verschweißt ist:



5 Die Öffnung an der oberen Kante der Sicherheitsversandtasche hat einen Sicherheitsverschluss.
Prüfen Sie, ob der Sicherheitsverschluss unbeschädigt ist:



Wurde der Sicherheitsverschluss geöffnet und wieder verschlossen, so ist der Schriftzug "VOID" zu erkennen:



3 IT-Sicherheit

Die in Kapitel 7 "Gerät identifizieren" genannten Varianten der Tastatur besitzen ein IT-Sicherheitszertifikat des Bundesamts für Sicherheit in der Informationstechnik (BSI) nach Common Criteria (CC) Standard, siehe 41 "Literatur", [1] mit der Verfahrens-ID BSI-DSZ-CC-0513-V2.

Um qualifizierte Signaturen zu erstellen, müssen Sie das Terminal mit einer zugelassenen Signaturkarte (HBA) sowie einer zugelassenen Signaturanwendungskomponente (Konnektor) betreiben (Liste der zugelassenen Komponenten siehe **www.gematik.de**).

4 Sicherheitsfunktionen

Damit ein sicherer Betrieb gewährleistet ist, verfügt das Gerät über folgende Sicherheitsfunktionen.

4.1 Meldung von Manipulation am Gehäuse

Das Gerät schützt sich aktiv vor Manipulation. Wird eine Manipulation im nicht sichtbaren Bereich des Gehäuses erkannt, löst dies eine elektronische Gerätesperre aus. Am Display erscheint die Meldung "Gehäuseüberwachung".

Ein gesperrtes Gerät besitzt keine Funktionalität mehr und kann nicht weiter verwendet werden. Wenden Sie sich an Ihren Gerätelieferanten.

4.2 Meldung von unautorisiertem Zurücksetzen

ACHTUNG: Verdacht auf Manipulation, falls im Display ▟ erscheint

- Verwenden Sie das Gerät nicht weiter.
- Wenden Sie sich an Ihren Gerätelieferanten.

Auch Fremde können das Terminal auf Werkseinstellungen zurücksetzen, wenn am Terminal das unautorisierte Zurücksetzen freigegeben ist, indem die Option **Werks-Reset > Unautorisiert** aktiviert wurde (siehe 27.3 "Werks-Reset ohne Authentisierung"). Wenn Sie den Verdacht oder die Gewissheit darüber haben, dass ein Werks-Reset durch eine unberechtigte Person ausgelöst wurde, darf das Terminal nicht weiter verwendet werden. Wenden Sie sich an Ihren Gerätelieferanten.

Folgende Indikatoren deuten darauf hin, dass ein Werks-Reset durch eine unberechtigte Person und nicht durch einen berechtigten Administrator durchgeführt wurde:

- Das Kartenterminal war mit einem Konnektor verbunden, dieser erkennt es nicht mehr (bzw. es ist für Anwendungsfälle nicht mehr nutzbar).
- Die Ihnen bekannte Administrator-PIN ist ungültig.
- Die Konfiguration des Terminals hat sich geändert.

Es wird ein Ausrufezeichen ▟ im oberen linken Bereich des Displays angezeigt. Nach erfolgreichem Pairing wird es wieder ausgeblendet.

4.3 Sichere PIN-Eingabe

ACHTUNG: Ausspähen der PIN möglich.

Bei der Eingabe der PIN über den Nummernblock kann diese ausgespäht werden.

- Verwenden Sie immer die sichere PIN-Eingabe über das Display (siehe 21.1 "Sichere PIN-Eingabe").
- Die PIN-Eingabe über den Nummernblock entspricht nicht dem zertifizierten Anwendungsfall.

Die sichere PIN-Eingabe ist ein Eingabeverfahren des PIN-Eingabe-Modus. Dieser wird immer

dann aktiviert, wenn eine Abfrage zu einer Karten-PIN angefordert wird.

Im PIN-Eingabe-Modus werden Eingaben am Kartenterminal direkt zur eingesteckten Karte (z. B. Heilberufsausweis) gesendet. Die PIN verlässt das Kartenterminal nie im Klartext.

Nähere Informationen zur PIN-Eingabe finden Sie unter 21 "PIN-Eingabe-Modus".

Beachten Sie folgende Sicherheitshinweise:

- Achten Sie darauf, dass Sie bei der Eingabe der PIN nicht beobachtet werden.
- Halten Sie Ihre PIN geheim.
- Geben Sie die PIN nur ein, wenn der PIN-Eingabe-Modus aktiv ist und eine sichere Verbindung zum Konnektor besteht (geschlossenes Schloss-Symbol wird angezeigt).
- In Ihrer Anwendung muss dabei erkennbar eine PIN angefordert worden sein.

4.4 Sicheres Firmware-Update

Das Terminal prüft die Integrität und Authentizität jeder neu zu installierenden Firmware. Es wird nur eine unveränderte, integere, korrekt und vollständig in das Kartenterminal übertragene Version von CHERRY aktiv geschaltet. Fehlerhafte oder nicht authentische Übertragungen werden abgewiesen.

Dieser Vorgang muss vom Administrator mit dem Kennwort der SICCT-Schnittstelle angestoßen werden. Nähere Informationen finden Sie unter 26 "Firmware aktualisieren".

4.5 Firmware auf Manipulation prüfen

Die Originalität der Firmware wird bei jedem Start des Kartenterminals geprüft. Sie können diese Prüfung auch manuell durchführen.

- Wählen Sie im Menü **Eigendiagnose** den Punkt **Codeprüfung**.

ACHTUNG: Verdacht auf Manipulation, falls am Ende der Codeprüfung "Fehlerhafter Code" erscheint

- Führen Sie einen Neustart des Kartenterminals durch. Wird die Meldung weiterhin angezeigt, kann und darf es nicht weiter verwendet werden

4.6 Benutzerprofile und Authentisierung

Folgende Benutzerprofile sind implementiert:

- "Benutzer"
- "Reset-Administrator"
- "Administrator"

Die Benutzerprofile verfügen über unterschiedliche Berechtigungen und sind voneinander getrennt. Der jeweilige Benutzer wird nicht explizit angezeigt.

"Benutzer":
Im Normalzustand wird das Benutzerprofil "Benutzer" ausgeführt. Hierfür ist keine Authentifizierung notwendig.

- Im Hauptmenü sind grundlegende Einstellungen einsehbar. Eine weitergehende Konfiguration ist nicht möglich, der Betriebszustand des Terminals somit nicht änderbar.
- Berechtigungen:
  - Aktuelle Terminal-Konfiguration anzeigen
  - Produkt Serien- und Versionsnummer, Terminalname und MAC-Adresse anzeigen
  - Anzeige- und Akustikeinstellungen vornehmen
  - Eigendiagnosefunktionen ausführen

"Reset-Administrator":
Mit diesem Benutzerprofil sind folgende Aktionen und Berechtigungen verknüpft:

- Bei der ersten Inbetriebnahme des Terminals muss der Reset-Administrator einen persönlichen Zugangscode, PUK (Personal Unblocking Key), festlegen (siehe 13 "PUK").
- Berechtigungen:
  - Kartenterminal in den Auslieferungszustand zurücksetzen (Werks-Reset), durch Eingabe der PUK nach Verlust des Administrator-Kennworts
  - PUK ändern

"Administrator":
Nach Eingabe des Kennworts ist das Benutzerprofil "Administrator" aktiv. Dieses bleibt erhalten, bis das Hauptmenü wieder verlassen wird (manuell oder automatisch nach 5 Minuten), oder eine SICCT Verbindung aufgebaut wird.

- Der Administrator überprüft vor der ersten Inbetriebnahme die Integrität des Terminals.
- Bei der ersten Inbetriebnahme des Terminals muss der Administrator ein persönliches

Kennwort festlegen (siehe 12 "Administrator-Kennwort").
- Zugang zu administrativen Einstellungen im Hauptmenü durch den Administrator.
- Höchste Rechte zur Konfiguration und Verwaltung des Geräts.
- Berechtigungen:
  - Anmeldung an allen Managementschnittstellen
  - Einstellungen zur Benutzerverwaltung und Netzwerkkonfiguration durchführen
  - Terminal- und Slot-Namen ändern
  - Pairing durchführen
  - Firmware-Updates einspielen
  - CA-Zertifikate für Konnektoren aktualisieren

4.7 Management-Schnittstellen

Der Zugang zum Kartenterminal erfolgt durch folgende, gesicherte Managementschnittstellen. Jede Managementschnittstelle besitzt ein eigenes, separates Kennwort. Darüber hinaus sind die Schnittstellen mit einer Zugriffspriorität versehen.

- **Priorität 1. SICCT-Schnittstelle:**
  Zugriff auf das Kartenterminal über den Konnektor oder Zugriff über die CHERRY Software **eHealth Device Manager**.
  Benutzername: admin
  Kennwort: Initial wird das lokal am Terminal vergebene Administrator-Kennwort verwendet. Ändern Sie es aus Sicherheitsgründen nach der Erstinbetriebnahme. Verwenden Sie für die SICCT-Schnittstelle ein anderes. Melden Sie sich dazu an der Web-Schnittstelle an.
- **Priorität 2. Direkte Managementschnittstelle:**

ACHTUNG: Ausspähen des Administrator-Kennworts möglich.

- Geben Sie das Administrator-Passwort nur in einer sicheren Umgebung an der direkten Managementschnittstelle ein.

  Lokaler Zugang, direkt am Kartenterminal.
  Die direkte Managementschnittstelle besteht aus dem Display, der Tastenmatrix und je einer LED an den Kontaktiereinheiten für die eGK/KVK und HBA, zur Statusanzeige. Die Sicherheitsfunktionen "Sichere PIN-Eingabe" und "Benutzerprofile und Authentifizierung" ermöglichen die Eingabe von Daten und die Ausgabe von Meldungen, Auswahlmöglichkeiten oder des Status.
- **Priorität 3. Web-Schnittstelle:**
  Zugriff auf das Kartenterminal mittels Internet-Browser.
  Benutzername: admin
  Kennwort: Initial wird das lokal am Terminal vergebene Administrator-Kennwort verwendet. Ändern Sie es aus Sicherheitsgründen nach der Erstinbetriebnahme. Verwenden Sie für die Web-Schnittstelle ein anderes.

Durch die Priorisierung der Zugänge wird die gleichzeitige, parallele Nutzung mehrerer Managementschnittstellen ausgeschlossen. Es kann immer nur eine Schnittstelle aktiv genutzt werden. Die Anmeldung an einer höher priorisierten Managementschnittstelle sperrt zugleich alle niedrigeren.

Beispiel: Der Administrator ist lokal am Terminal angemeldet (Direkte Managementschnittstelle = aktiv). Der Zugriff auf die Web-Schnittstelle ist nun nicht mehr möglich. Wird zusätzlich eine SICCT-Verbindung aufgebaut (SICCT-Schnittstelle = aktiv), erfolgt automatisch eine Abmeldung an der direkten Managementschnittstelle (der Nutzer "fliegt raus"). Die erneute Anmeldung an der direkten Managementschnittstelle ist gesperrt, die Web-Schnittstelle ist weiterhin nicht verfügbar.

ACHTUNG: Gesperrte Zugänge bei aktiver Konnektor-Verbindung

Bei aktiver Konnektor-Verbindung ist der Zugang über die CHERRY Software gesperrt.

- Beenden Sie am Konnektor die bestehende (SICCT-)Verbindung zum Terminal.

Folgende Funktionen sind nur lokal am Terminal zugänglich:

- Pairing mit einem Konnektor (siehe 15 "Pairing mit einem Konnektor")
- Aktivieren oder Deaktivieren administrativer SICCT-Kommandos (siehe 23.1 "Mögliche Einstellungen (Hauptmenü)")
- Aktivieren oder Deaktivieren der Web-Schnittstelle (siehe 24 "Konfiguration über Web-Schnittstelle")

Medizinische und personenbezogene Daten werden aufgrund der Zulassungsbedingungen nicht über Managementschnittstellen angezeigt oder übertragen.

HINWEIS: Deaktivierte Einstellungen

Folgende Einstellungen sind nach initialer Inbetriebnahme deaktiviert:

- Remote Zugang über Web-Schnittstelle
- Alle administrativen SICCT-Kommandos (z. B. Firmware oder CA-Zertifikate aktualisieren)
- Unautorisiertes Zurücksetzen auf Werkseinstellungen

4.8 Verschlüsselte Kommunikation

Das Kartenterminal kommuniziert ausschließlich über gesicherte, verschlüsselte Verbindungen (Ausnahme: Lokalisieren des Terminals im Netzwerk). Es nutzt die eingesetzte gSMC-KT Karte und die im Terminal vorhandenen CA-Zertifikate der Konnektoren.

Zum einen wird dadurch die Sicherung der Netzwerkkommunikation durch TLS 1.1 oder TLS 1.2 gewährleistet, zum anderen ermöglicht die verschlüsselte Kommunikation, zusammen mit einem sogenannten "Shared Secret", die sichere Identifikation und Authentifizierung des Kartenterminals durch den Konnektor.

Das Shared Secret wird während des Pairings mit einem Konnektor erzeugt und gesichert im Kartenterminal abgelegt.

Sicherheitsrelevante SICCT- bzw. eHealth-Kommandos werden ausschließlich im vertrauenswürdigen Zustand ausgeführt. Der vertrauenswürdige Zustand des Kartenterminals über die sichere, verschlüsselte Netzwerkverbindung mit einem gepairten Konnektor wird im oberen Displaybereich durch ein geschlossenes Schloss-Symbol angezeigt.

4.9 Vertrauenswürdiges Kartenterminal

Das Kartenterminal stellt den Schutz der Vertraulichkeit, Authentizität und Integrität der übertragenen Daten sicher, was u. a. durch die Zulassung bestätigt wurde.

Beispielsweise können Kennwörter nicht ausgelesen werden und verlassen das Gerät nie im Klartext. Falls mehrere Karten gleichzeitig im Terminal genutzt werden, wird jede Verbindung in einer eigenen Sicherheitsbeziehung geführt. Das Kartenterminal löscht eingegebene PINs und Kennwörter, kryptografische Schlüssel und alle Informationen aus gesteckten Karten und vom Konnektor, sobald diese nicht mehr benötigt werden (Ausnahme: die Pairinginformationen).

Im vertrauenswürdigen Zustand ist nach Stand der Technik keine Beeinflussung oder Informationsabschöpfung durch Komponenten (z. B. Software), welche nicht über eine Zulassung durch die gematik verfügen, möglich.

INBETRIEBNAHME

Sie benötigen:

- Lieferumfang
- gSMC-KT Karte
- Reset-Administrator
- PC mit Netzwerkverbindung

Vorgehensweise:

1 Prüfen Sie die Vollständigkeit des Packungsinhalts (siehe "Lieferumfang").

2 Prüfen Sie vor der Inbetriebnahme, ob das Gerät über den vorgeschriebenen sicheren Lieferweg zu Ihnen geliefert wurde. Folgen Sie hierzu den Anweisungen im Kapitel 2 "Bestellung und sichere Auslieferung" oder auf unserer Homepage unter: **https://www.cherry.de/eHealth**. Sollte die Prüfung negativ verlaufen, nehmen Sie das Gerät auf keinen Fall in Betrieb und wenden Sie sich an Ihren Gerätelieferanten.

3 Machen Sie sich mit den Sicherheitsfunktionen des Geräts vertraut (siehe 4 "Sicherheitsfunktionen").

4 Beachten Sie die allgemeinen Sicherheitshinweise (siehe 5 "Allgemeine Sicherheitshinweise").

5 Beachten Sie die Hinweise zur Einsatzumgebung (siehe 6 "Einsatzumgebung").

6 Identifizieren Sie das Produkt (siehe 7 "Gerät identifizieren").

7 Überzeugen Sie sich von der Unversehrtheit des Geräts. Überprüfen Sie insbesondere das Gehäuse, die Anschlusskabel und die Siegel gemäß der Beschreibung (siehe 9 "Versiegelung prüfen"). Wenden Sie sich bei Verdacht auf Manipulationen an Ihren Gerätelieferanten.

8 Installieren Sie das Gerät (siehe 11 "Tastatur anschließen").

9 Legen Sie das Administrator-Kennwort fest (siehe 12 "Administrator-Kennwort").

10 Lassen Sie den Reset-Administrator den PUK festlegen (siehe 13 "PUK").

11 Installieren Sie die gSMC-KT Karte (siehe 14 "gSMC-KT Karte installieren").

12 Beachten Sie die Benutzungsvorschriften (siehe 16 "Maßnahmen zur sicheren Benutzung").

13 Schalten Sie ggf. deaktive Einstellungen frei (siehe 23 "Lokale Konfiguration über direkte Managementschnittstelle" oder 24 "Konfiguration über Web-Schnittstelle" oder 25 "Konfiguration über CHERRY Software"). Folgende Einstellungen sind nach Erstinbetriebnahme deaktiviert:
   - Remote Zugang über Web-Schnittstelle
   - Alle administrativen SICCT-Kommandos (z. B. Firmware oder CA-Zertifikate aktualisieren)
   - Unautorisiertes Zurücksetzen auf Werkseinstellungen

14 Führen Sie das Pairing mit einem Konnektor durch (siehe 15 "Pairing mit einem Konnektor").

Falls Sie bei der Installation Unterstützung benötigen, kontaktieren Sie CHERRY.

5 Allgemeine Sicherheitshinweise

- Stellen Sie sicher, dass Ihr Netzwerk ausreichend abgesichert ist, damit kein unautorisierter Zugriff möglich ist.
- Stellen Sie sicher, dass der Benutzer (Heilberufler) die erforderlichen Unterlagen und die Benutzerdokumentation erhält.
- Betreiben Sie das Gerät nur mit einem zertifizierten Konnektor. Der Konnektor prüft periodisch den Pairingstatus und gibt ggf. eine Warnung aus.
- Verwenden Sie für den Betrieb des Geräts nur eine zertifizierte gSMC-KT Karte. Das Gerät verwendet den Zufallszahlengenerator der Karte z. B. zum Aufbau einer sicheren Verbindung.
- Verwenden Sie für automatische Updates aus dem lokalen Netzwerk nur einen Push Server. Der Push Server muss die Kennung der Kartenterminals, die Version der installierten Firmware sowie das Ergebnis des Updateprozesses dokumentieren. (Unter einem Push Server versteht man z. B. den Konnektor.) Stellen Sie sicher, dass im Push-Server das richtige Update-Paket für ein automatisches Update ausgewählt ist.
- Nachdem Sie eine Karte in einen der ID-000 Kartenslots (z. B. gSMC-KT) gesteckt haben, versiegeln Sie diesen mit einem der beiliegenden Slotsiegel.

6 Einsatzumgebung

Die **G87-1505** ist für den stationären Einsatz in einer kontrollierten Umgebung konzipiert. Sie ist zur Anbindung an die Telematik-Infrastruktur des deutschen Gesundheitswesens vorgesehen.

Das Gerät ist für den Einsatz in Praxen, Apotheken und in Krankenhäusern gedacht. Diese Einsatzumgebung wird als kontrollierte Einsatzumgebung angenommen. Für den sicheren Betrieb des Kartenterminals ist der Administrator zusammen mit dem Leistungserbringer verantwortlich.

- Das Kartenterminal muss hinreichend vor Manipulation geschützt werden. Betreiben Sie das Gerät so, dass ein Missbrauch auszuschließen ist.
- Sorgen Sie dafür, dass unbefugte Personen keinen unbeaufsichtigten Zugriff auf das Terminal haben.
- Das Gerät darf maximal 10 Minuten unbeaufsichtigt bleiben.
- Falls es länger unbeaufsichtigt ist, muss sichergestellt werden, dass das Gerät in einem geschützten Bereich aufbewahrt wird. In diesem Fall muss das Terminal durch seine Umgebung geschützt sein.
- Überprüfen Sie regelmäßig, vor der Nutzung und nach Abwesenheit, die Unversehrtheit des Geräts. Achten Sie dabei insbesondere auf das Gehäuse, die Anschlusskabel und die Versiegelungen (Seriennummer auf Gehäusesiegel und gSMC-KT Slotsiegel). Stellen Sie sicher, dass keine Siegel manipuliert wurden oder andere bauliche Änderungen einen Angriff verschleiern sollen.
- Achten Sie auf Manipulationen zum Ausspionieren der PIN-Eingabe, z. B.:
  - Miniatursender, die an den Karten-Steckplätzen angebracht sind
  - Abhörelektronik am Gerät oder in der Nähe (z. B. ein Richtmikrofon in bis zu 1 m Abstand)
  - Kameras, die auf die Tasten gerichtet sind
  - Ausgebohrte/manipulierte Tastenkappen
  - Verringerung des Tastenhubs des Nummernblocks
- Bei Verdacht auf Manipulationen am Gerät wenden Sie sich an Ihren Gerätelieferanten.

7 Gerät identifizieren

Prüfen Sie vor der Inbetriebnahme des Geräts, ob es sich um eine zertifizierte Gerätevariante handelt. Diese ist eindeutig über die Artikelnummer und die Firmware- und Hardwareversion definiert. Gehen Sie dazu folgendermaßen vor:

1 Prüfen Sie die Artikelnummer. Diese ist auf der Unterseite des Geräts auf dem Typenschild aufgedruckt.

2 Prüfen Sie die Firmware- und Hardwareversion. Diese werden im Menü **Info** angezeigt (siehe 23.2 "Menü Info").

3 Verwenden Sie das Gerät nur, wenn es sich um eine der folgenden Varianten handelt:

   - Artikelnummer: G87-1505LBZDE-2
     Firmwareversion: 3.0.1
     Hardwareversion: 1.1.1
   - Artikelnummer: G87-1505LBZDE-10
     Firmwareversion: 3.0.1
     Hardwareversion: 1.1.1

8 Typenschild prüfen

Der Typenschild-Aufkleber befindet sich auf der Unterseite des Geräts. Dies ist der einzige Aufkleber, der auf dem Gerät aufgebracht sein darf.

ACHTUNG: Verdacht auf Manipulation

Bei entferntem, verletztem oder falsch platziertem Typenschild ist das Gerät möglicherweise kompromittiert und nicht mehr sicher.

- Prüfen Sie, ob das Typenschild auf der Unterseite des Geräts unbeschädigt auf der dafür vorgesehenen Freifläche aufgeklebt ist.
- Prüfen Sie, dass sich keine weiteren Aufkleber auf dem Gerät befinden.
- Falls dies nicht der Fall ist: Verwenden Sie das Gerät nicht weiter.
- Wenden Sie sich an Ihren Gerätelieferanten.

9 Versiegelung prüfen

9.1 Gehäuseversiegelung prüfen

Anhand authentischer und fälschungssicherer Sicherheitssiegel, welche über die Trennkante zwischen Gehäuseunter- und -oberteil geklebt sind, können Sie die Manipulationsfreiheit der Hardware sicher erkennen. Ein Öffnen des Gehäuses beschädigt das Siegel.

Die Beschaffenheit (Zerstöreigenschaft) des Siegels gewährleistet, dass es nicht unbeschädigt entfernt und wieder aufgeklebt werden kann.

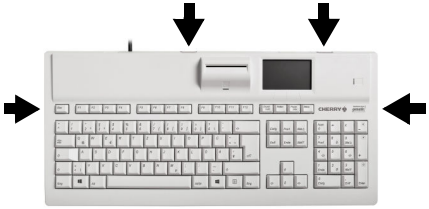
1 Notieren Sie sich zur Identifizierung der Siegel deren Seriennummern, um einen Geräte- oder Siegelaustausch feststellen zu können.
2 Prüfen Sie mindestens bei der Installation des Terminals und vor jedem Pairing, ob die Siegel verletzt oder ausgetauscht wurden.
3 Prüfen Sie auch die Slotsiegel (gSMC-KT und ggf. der SMC-B Karte), siehe 9.4 "Slot für gSMC-KT und ggf. SMC-B Karte versiegeln".

ACHTUNG: Verdacht auf Manipulation

Bei verletztem, getauschtem oder fehlendem Siegel(n) ist das Gerät möglicherweise kompromittiert und nicht mehr sicher.

- Verwenden Sie das Gerät nicht weiter.
- Wenden Sie sich an Ihren Gerätelieferanten.

9.2 Positionen der Gehäusesiegel



9.3 Beschreibung des Gehäusesiegels

Unbeschädigtes Siegel

Das graue, 20 mm lange und 12 mm breite Siegel ist mit einer 7-stelligen Seriennummer versehen, um die eindeutige Identifizierbarkeit zu gewährleisten.

Als Echtheitsmerkmal sind der Bundesadler und der Schriftzug BSI mit einem Farbkippeffekt versehen. Die Kippfarbe wechselt je nach Betrachtungswinkel und Lichteinfall seine Farbe von Bronze über Grün nach Ocker.

Als verdecktes Echtheitsmerkmal befindet sich ein UV-Druck auf dem Siegel. Unter UV-Licht wird bei 254nm und 365nm der Schriftzug "Security" sichtbar.

Das Siegel selbst ist als Zerstörsiegel ausgeführt, wodurch Manipulationen durch partielles Aufspalten der grauen Grundfarbe in einen helleren Grauton erkennbar werden.

Siegel nach Ablöseversuch

Beispiel eines Siegels nach Ablöseversuch. Es weist eindeutige Zerstörungsmuster auf:

9.4 Slot für gSMC-KT und ggf. SMC-B Karte versiegeln

Jedem Gerät liegen 4 Slotsiegel bei. Mit diesen müssen Sie gesteckte Karten in den Steckplätzen SM1 und SM2 versiegeln.

1 Verwenden Sie bei Erneuerung des Slotsiegels die dafür vorgesehene Klebefläche.
2 Entfernen Sie rückstandslos evtl. vorhandene Reste alter Siegel um den Kartenleser und stellen Sie sicher, dass die glatte Siegelfläche staub- und fettfrei ist.
3 Achten Sie darauf, dass die Siegel den Kartenschlitz vollständig bedecken.

4 Notieren Sie sich zur Identifizierung der Siegel deren Seriennummern.

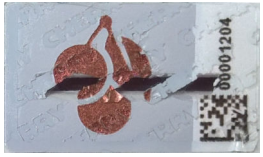
5 Verwahren Sie nicht benötigte Siegel an einem sicheren Ort.

6 Prüfen Sie vor jedem Pairing, ob die Siegel verletzt oder ausgetauscht wurden.

Position Slotsiegel

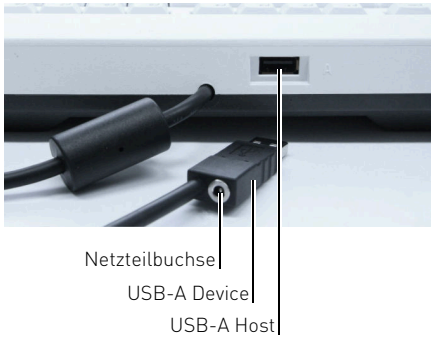
Unbeschädigtes Slotsiegel

Slotsiegel nach Ablöseversuch



Am Slotsiegel kann eine Manipulation erkannt werden. In diesem Fall ist der Betrieb des Kartenterminals nicht mehr sicher.

10 Anschlüsse



Netzteilbuchse

- Die Netzteilbuchse ist in den USB-Stecker des Anschlusskabels integriert. Sie können hier ein Netzteil zur zusätzlichen Stromversorgung der Tastatur anschließen. Eine zusätzliche Stromversorgung ist nur notwendig, wenn ein zusätzliches Gerät an der USB-A Host-Schnittstelle betrieben wird.

USB-A Device

- Stecken Sie das USB-Kabel der Tastatur in die USB- Schnittstelle des Host-PCs.

USB-A Host

- An dieser Schnittstelle können weitere Geräte, wie ein PIN-Pad, betrieben werden. Im Auslieferungszustand ist diese Schnittstelle nicht aktiv und muss durch ein Firmware-Update aktiviert werden.

Verwenden Sie nur von CHERRY freigegebenes Zubehör.

11 Tastatur anschließen

Das eHealthTerminal der Tastatur kann ausschließlich in Verbindung mit einem Konnektor in einem Netzwerk (LAN) betrieben werden.

Das Terminal besitzt keine explizite LAN-Buchse, es wird am USB-Anschluss eines PCs mit Netzwerkverbindung betrieben. Voraussetzung dafür ist die Installation der CHERRY Software **eHealth USB-LAN Proxy** am PC.

1 Stellen Sie sicher, dass Ihr PC mit Ihrem Netzwerk verbunden ist und nicht in den Sleep-Modus fährt.

2 Installieren Sie die CHERRY Software **eHealth USB-LAN Proxy** der Tastatur **G87-1505**. Die aktuelle Version inklusive Anleitung erhalten Sie unter **https://www.cherry.de**. Der eHealth USB-LAN Proxy ist ein Systemdienst, mit dem das – an USB betriebene – Kartenterminal die LAN-Verbindung des Rechners verwenden kann. Es kann nur ein CHERRY eHealth Gerät mittels Proxy an einem PC betrieben werden.

3 Stellen Sie sicher, dass der entsprechende Systemdienst aktiv ist (siehe Anleitung zur Software).

4 Stecken Sie die Tastatur direkt am USB-Anschluss des PCs an, verwenden Sie keinen USB-Hub.

12 Administrator-Kennwort

12.1 Kennwort erstmalig festlegen

Das Gerät funktioniert erst nach Festlegung des Kennworts.

Bei der Erstinbetriebnahme werden Sie aufgefordert, ein neues 8- bis 12-stelliges Administrator-Kennwort festzulegen.

ACHTUNG: Manipulation am Gerät

Erscheint bei der Erstinbetriebnahme, nach Erhalt des Geräts, **keine** Aufforderung ein neues Kennwort festzulegen:

- Nehmen Sie das Gerät nicht in Betrieb und kontaktieren Sie Ihren Gerätelieferanten.

1 Wählen Sie das Kennwort unter Vermeidung von Trivialpasswörtern, wie "Arztpraxis", Geburtsdaten oder gleichen Zahlenfolgen. Beachten Sie die "Regelung des Passwortgebrauchs" unter: **www.bsi.bund.de**
   - Das Kennwort muss mindestens eine Zahl enthalten. Verwenden Sie nur die Buchstaben A - Z, a - z und Zahlen 0 - 9. Unerlaubte Zeichen werden nicht angenommen.
2 Geben Sie das Kennwort ein. Achten Sie darauf, dass Sie bei der Eingabe nicht beobachtet werden.

   Für jede eingegebene Stelle des Kennworts wird ein Sternchen (*) angezeigt.
3 Bestätigen Sie mit der Taste unter dem Symbol [O] auf dem Display.
4 Geben Sie das Kennwort erneut ein.
5 Bestätigen Sie mit der Taste unter dem Symbol [O] auf dem Display.
6 Notieren Sie das Kennwort und bewahren Sie es unter Verschluss auf.

HINWEIS: Identische Kennwörter

Das Administrator-Kennwort wird initial für **alle** Zugänge gesetzt. Es ist also anfangs für alle drei Management-Schnittstellen gleich: **direkter Zugang** am Terminal, **Web-Schnittstelle** und **SICCT-Schnittstelle**. Jede Managementschnittstelle besitzt eine separate Kennwortverwaltung.

- Ändern Sie nach der Erstinbetriebnahme aus Sicherheitsgründen die Kennwörter für den Web- und SICCT-Zugang.
- Verwenden Sie unterschiedliche Kennwörter.

12.2 Kennwort ändern

Die Änderung des Kennworts betrifft immer nur die jeweils gewählte Managementschnittstelle.

Das Kennwort für den **direkten Zugang** ändern Sie lokal am Terminal: **Menü > Kennwort ändern**.

Das Kennwort für den **Web-Zugang** ändern Sie nach Login an der Web-Schnittstelle (siehe 24 "Konfiguration über Web-Schnittstelle"). Es muss bei erstem Login zwingend geändert werden.

Das Kennwort für den **SICCT-Zugang** ändern Sie nach Login an der Web-Schnittstelle. Die geänderten Zugangsdaten müssen folglich auch am Konnektor hinterlegt werden! Verbindungsversuche mit falschen Zugangsdaten führen sonst zur Sperrung der SICCT-Schnittstelle.

12.3 Kennwort falsch oder vergessen

Ab der 3. Fehleingabe des Kennworts wird die jeweilige Management-Schnittstelle zeitweise gesperrt (direkter Zugang, Web-Schnittstelle, SICCT-Schnittstelle). Jeder Zugang besitzt seinen eigenen, separaten Fehlerzähler.

Zahl ungültiger Eingaben	Sperrzeit
3 – 6	1 Minute
7 –10	10 Minuten
11 – 20	1 Stunde
ab 21	1 Tag

- Die Sperrung bleibt auch im spannungslosen Zustand des Geräts erhalten. Die Sperrzeit wird währenddessen nicht weiter verringert.
- Der Stand des Fehlerzählers am direkten Zugang wird bei einem Zugriffsversuch auf einen gesperrten Menübereich lokal am Terminal angezeigt.
- Der Stand der Fehlerzähler für SICCT- und Web-Schnittstelle ist nicht abfragbar.
- Der Fehlerzähler des jeweiligen Zugangs wird nach Eingabe des korrekten Kennworts zurückgesetzt.

Ein vergessenes Administrator-Kennwort kann nur durch Reset des Kartenterminals auf Werkseinstellungen zurückgesetzt werden. Dabei wird auch der Fehlerzähler für den direkten (lokalen) Zugang auf Null gesetzt. Siehe 27 "Zurücksetzen auf Werkseinstellungen".

13 PUK

13.1 PUK erstmalig festlegen

Der PUK ist das Kennwort des Reset-Administrators und dient bei Verlust des Administrator-Kennworts dazu, das Kartenterminal auf Werkseinstellungen zurückzusetzen.

Bei der Erstinbetriebnahme werden Sie, direkt nach der Festlegung des Administrator-Kennworts, aufgefordert, zusätzlich einen 8- bis 12-stelligen PUK (**P**ersonal **U**nblocking **K**ey) festzulegen.

1 Der PUK sollte sich vom Administrator-Kennwort unterscheiden. Wählen Sie den PUK unter Vermeidung von Trivialpasswörtern, wie "Arztpraxis", Geburtsdaten oder gleichen Zahlenfolgen. Beachten Sie die "Regelung des Passwortgebrauchs" unter: **www.bsi.bund.de**.

   Der PUK muss mindestens eine Zahl enthalten. Verwenden Sie nur die Buchstaben A - Z, a - z und Zahlen 0 - 9. Unerlaubte Zeichen werden nicht angenommen.

2 Geben Sie den PUK ein. Achten Sie darauf, dass Sie bei der Eingabe nicht beobachtet werden.

   Für jede eingegebene Stelle des PUKs wird ein Sternchen (*) angezeigt.

3 Bestätigen Sie mit der Taste unter dem Symbol [ ] auf dem Display.

4 Geben Sie den PUK erneut ein.

5 Bestätigen Sie mit der Taste unter dem Symbol [ ] auf dem Display.

6 Notieren Sie den PUK und bewahren Sie ihn unter Verschluss auf.

13.2 PUK ändern

Der PUK kann ausschließlich direkt am Terminal geändert werden: Menü **PUK ändern**.

13.3 PUK falsch oder vergessen

Ab der 3. Fehleingabe des PUKs wird dessen Eingabe zeitweise gesperrt.

Zahl ungültiger Eingaben	Sperrzeit
3 – 6	1 Minute
7 – 10	10 Minuten
11 – 20	1 Stunde
ab 21	1 Tag

- Die Sperrung bleibt auch im spannungslosen Zustand des Geräts erhalten. Die Sperrzeit wird währenddessen nicht weiter verringert.
- Die PUK-Sperrzeit beeinflusst nicht die Eingabe des Administrator-Kennworts.
- Der Stand des PUK-Fehlerzählers am direkten Zugang wird bei einem Zugriffsversuch auf einen gesperrten Menübereich lokal am Terminal angezeigt.
- Der PUK-Fehlerzähler wird nach Eingabe des korrekten PUK oder Reset des Kartenterminals auf Werkseinstellungen zurückgesetzt.

14 gSMC-KT Karte installieren

Die gSMC-KT Karte ist eine gerätebezogene Security Module Card (ein Sicherheitsmodul im Format ID-000, d. h. in der Größe einer SIM-Karte). Sie implementiert die Identität des Kartenterminals und dient zur sicheren Kommunikation. Bezugsquellen für eine gSMC-KT finden Sie auf **https://www.cherry.de/eHealth**.

1 Notieren Sie sich die MAC-Adresse des CHERRY eHealthTerminals (**Info > MAC-Adresse**).

2 Verwahren Sie den Fingerprint des in der gSMC-KT Karte abgelegten X.509-Zertifikats sicher. Der Fingerprint befindet sich entweder auf dem ID-1-Anteil, aus dem die ID-000-Karte herausgebrochen wird, oder er wird in Papierform (z. B. in einem Begleitschreiben) übermittelt.

3 Stecken Sie die gSMC-KT Karte in den kleinen Leserschlitz mit der Beschriftung **1** (SM 1), (siehe 17 "Einstecken der Karten"). Verwenden Sie für die gSMC-KT Karte nur diesen Steckplatz!

4 Entfernen Sie rückstandslos eventuell vorhandene Reste alter Siegel um den Kartenleser und stellen Sie sicher, dass die glatte Siegelfläche staub- und fettfrei ist (siehe 33 "Reinigen der Tastatur").

5 Überkleben Sie den Schlitz des Kartenlesers mit einem neuen Siegel (siehe 9.4 "Slot für gSMC-KT und ggf. SMC-B Karte versiegeln").

6 Notieren Sie sich zusätzlich zu den vorhandenen Daten (MAC-Adresse, gSMC-KT Fingerprint) die Seriennummer des aufgeklebten Slotsiegels.

7 Eine PIN-Freischaltung der gSMC-KT Karte ist nicht notwendig.

ACHTUNG: Manipulation am Gerät

Bei zerstörtem Siegel ist der Betrieb des Kartenterminals nicht mehr sicher.

- Überprüfen Sie regelmäßig, ob das Siegel verletzt oder ausgetauscht wurde.
- Prüfen Sie bei zerstörtem Siegel die gSMC-KT Karte auf Manipulation oder Tausch (Fingerprint prüfen).
  Ist ein erneutes Pairing notwendig, wurde möglicherweise die gSMC-KT Karte ausgetauscht und es liegt eine Manipulation vor! Eine unbekannte gSMC-KT Karte darf nicht weiter verwendet werden!

15 Pairing mit einem Konnektor

Falls nötig, konfigurieren Sie das Terminal, bevor Sie das Pairing mit einem Konnektor durchführen. Bei aktiver Konnektor-Verbindung ist die Konfiguration des Terminals nicht möglich.

Durch das Pairing können sich Kartenterminal und Konnektor gegenseitig authentifizieren und eine Verbindung aufbauen. Jedes neu ins Netzwerk eingebrachte eHealthTerminal muss aufgrund der Zulassungsbedingungen einzeln in Betrieb genommen werden.

ACHTUNG: Zugang unautorisierter Dritter zum Kartenterminal oder Konnektor

- Stellen Sie sicher, dass das Kartenterminal während des Pairing-Prozesses in Ihrer organisatorischen Hoheit steht.
- Unautorisierte Dritte dürfen während des Pairings keinen Zugang zum Kartenterminal oder zum Konnektor erlangen.

Pairing bezeichnet das Verfahren, dem Kartenterminal eine vom Konnektor erzeugte digitale Kennung zu übergeben. Diese Kennung ist ein Shared Secret zwischen Konnektor und Kartenterminal.

Das Pairing dient grundsätzlich als Sicherung gegen den unbemerkten Austausch von eHealthTerminals oder deren Identitäten. Dazu wird die gSMC-KT Karte über den Konnektor logisch an das Kartenterminal gebunden.

Ein Konnektor dient zur sicheren Anbindung der Systeme in Praxen, Apotheken, Krankenhäusern usw. an die Telematikinfrastruktur. Beispielsweise verwaltet er die Clientsysteme und Kartenterminals (und deren Relationen zueinander) und führt eine Liste aller Ereignisse und Operationen der verwendeten Karten.

Für das Pairing benötigen Sie:

- Eine installierte gSMC-KT Karte (siehe 14 "gSMC-KT Karte installieren")

1 Wählen Sie an der Kartenterminalverwaltung des Konnektors das CHERRY Terminal aus.

  Der Fingerprint der gSMC-KT Karte (Komponentenzertifikat) wird angezeigt.

2 Überprüfen Sie, ob der am Konnektor angezeigte Fingerprint mit dem notierten gSMC-KT Fingerprint übereinstimmt und bestätigen Sie dies.

  Das Kartenterminal zeigt eine konnektorspezifische Display-Meldung an.

3 Bestätigen Sie das Pairing mit der Taste **0** am Nummernblock der Tastatur.

  Der öffentliche Schlüssel (Public Key) des Konnektorzertifikats wird im Terminal gespeichert, sofern ein freier Pairing-Block vorhanden und das Konnektorzertifikat gültig ist.

Um die Verwaltung zu vereinfachen, kann der Terminalname bei der Inbetriebnahme des Kartenterminals verändert werden (**Menü > Terminal > Terminal Name**). Er wird zum Konnektor übertragen und kann in der Kartenterminalverwaltung des Konnektors im Sinne eines Friendly Name verwendet werden.

Das Kartenterminal besitzt 3 Pairingblöcke. Jeder Pairingblock kann mit bis zu 3 Konnektoren bekannt gemacht werden und die jeweiligen öffentlichen Schlüssel (Public Keys) und das Shared Secret verwalten. Zeitgleiche Verbindungen mit verschiedenen Konnektoren sind nicht möglich. Pairinginformationen können im Menü eingesehen werden (siehe 23.1 "Mögliche Einstellungen (Hauptmenü)").

15.1 CA-Zertifikate aktualisieren

Das Kartenterminal prüft bei jedem Verbindungsaufbau, ob es sich um einen betriebszugelassenen, d. h. vertrauenswürdigen, Konnektor handelt. Dazu enthält das Kartenterminal eine Trust-Service Status Liste verfügbarer CA-Zertifikate für zugelassene Konnektoren. Diese können Sie mit einer Zertifikatsliste gleicher oder höherer Version aktualisieren.

HINWEIS: Authentifizierung des Konnektors

Falls der bei Ihnen eingesetzte Konnektor nicht authentifiziert werden kann:

- Aktualisieren Sie die Zertifikate (Trust-Service Status Liste).
- Verwenden Sie die CHERRY Software **eHealth Device Manager** (siehe 25 "Konfiguration über CHERRY Software"). Sie erhalten die Software, zusammen mit der aktuellen Trust-Service Status Liste, auf unserer Homepage unter **https://www.cherry.de**.

BEDIENUNG

16 Maßnahmen zur sicheren Benutzung

Ein sicherer Betrieb des Geräts setzt die Umsetzung und kontinuierliche Einhaltung folgender Sicherheitsmaßnahmen voraus:

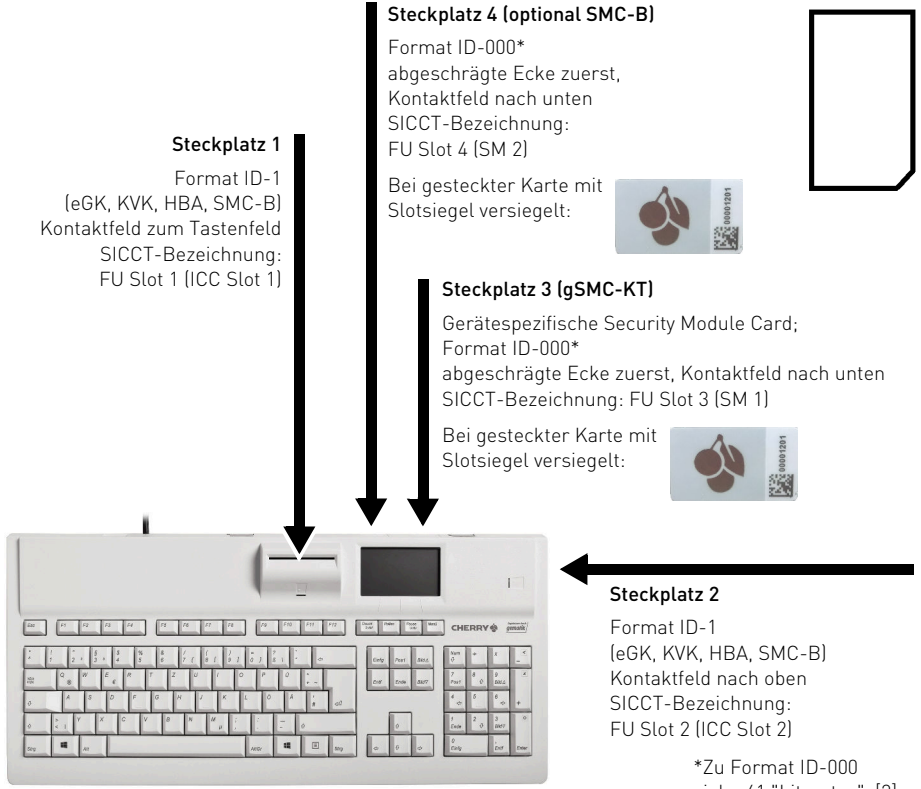
1 Lesen Sie sich dieses Handbuch genau durch.
2 Halten Sie Ihr Administrator-Kennwort geheim und geben Sie es nicht weiter.
3 Achten Sie darauf, dass Sie während der Eingabe des Kennworts nicht beobachtet werden.
4 Bringen Sie auf dem Kartenterminal keine Aufkleber oder Notizzettel an.
5 Sorgen Sie dafür, dass das Personal mit den Sicherheitsvorkehrungen, die zum Schutz des Terminals notwendig sind, vertraut gemacht wird.
6 Lassen Sie keine Flüssigkeit in das Innere des Geräts eindringen, da elektrische Schläge oder Kurzschlüsse die Folge sein können.
7 Entfernen Sie die gSMC-KT Karte nur im stromlosen Zustand des Terminals.

17 Einstecken der Karten

Nur die gSMC-KT Karte muss in SM1 gesteckt werden. Alle anderen Karten können in alle Slots gesteckt werden. Der Konnektor gibt entweder den Slot vor oder erkennt automatisch, welche Karte in welchen Slot gesteckt wurde.

ACHTUNG: Manipulation am Gerät

- Überprüfen Sie vor dem Einstecken einer Karte den Kartenschacht auf Manipulation (z. B. Elektronik oder Folien zum Abhören der Kartenkommunikation).



*Zu Format ID-000 siehe 41 "Literatur", [2].

Steckplatz 1 (senkrecht) für Format ID-1 Karten (eGK, KVK, HBA, SMC-B)

- Stecken Sie die Karte von oben in die Kontaktiereinheit, bis sie spürbar einrastet. Das Kontaktfeld muss für Sie sichtbar sein, also in Richtung Tastenfeld (zu Ihnen) zeigen.

Steckplatz 2 (waagrecht) für Format ID-1 Karten (eGK, KVK, HBA, SMC-B)

- Stecken Sie die Karte seitlich in die Kontaktiereinheit, bis sie spürbar einrastet. Das Kontaktfeld muss nach oben zeigen, sodass es für Sie sichtbar ist.

Steckplatz 3 für Format ID-000 Karten (gSMC-KT)

- Diese Kontaktiereinheit ist ausschließlich für die gSMC-KT Karte vorgesehen. Stecken Sie die Karte mit der abgeschrägten Ecke zuerst (Kontaktfeld nach unten) in die Kontaktiereinheit, bis sie einrastet. Erneutes Drücken entriegelt die Karte zum Entnehmen. Eine in diesen Slot gesteckte Karte muss mit dem beigelegten Slotsiegel versiegelt werden, siehe 9.4 "Slot für gSMC-KT und ggf. SMC-B Karte versiegeln".
- Entfernen Sie die gSMC-KT Karte nur im stromlosen Zustand des Terminals.

Steckplatz 4 für Format ID-000 Karten (optional SMC-B)

- Diese Kontaktiereinheit kann für die SMC-B Karte verwendet werden. Stecken Sie die Karte mit der abgeschrägten Ecke zuerst (Kontaktfeld nach unten) in die Kontaktiereinheit, bis sie einrastet. Erneutes Drücken entriegelt die Karte zum Entnehmen. Eine in diesen Slot gesteckte Karte muss mit dem beigelegten Slotsiegel versiegelt werden, siehe 9.4 "Slot für gSMC-KT und ggf. SMC-B Karte versiegeln".

18 Navigation

18.1 Betriebsarten

Die Tastatur stellt 4 verschiedene Betriebsarten zur Verfügung.

Tastatur-Modus

- Als Grundfunktionalität stehen Ihnen alle Funktionen einer Windows-kompatiblen Tastatur zur Verfügung. Es werden alle Tastatureingaben über USB an den PC übertragen.

Menü-Modus

1 Um in den Menü-Modus zu kommen, drücken Sie für 3 Sekunden die Taste unter dem Symbol [🔧] auf dem Display.

Bei aktivem Menü-Modus werden Tastatureingaben nicht mehr an den Rechner geleitet.

2 Um den Menü-Modus zu verlassen, drücken Sie die Taste unter dem Symbol [🔧→] auf dem Display.

Sicherer PIN-Eingabe-Modus

- Dieser Modus wird aktiviert, wenn eine PIN-Eingabe angefordert wird. Hier werden keine Tastatureingaben über USB an den PC übertragen.

SICCT-Modus

- Dieser Modus wird aktiviert, wenn für die Bearbeitung eines empfangenen SICCT-Befehls eine Nutzereingabe benötigt wird. Hierbei werden Tastatureingaben nicht an den PC weitergeleitet, sondern für die Bearbeitung des SICCT- Befehls verwendet.

18.2 Funktion der 4 Tasten unter dem Display

Im unteren Bereich des Displays wird im Normalbetrieb der jeweilige Status der Tasten **Num**, **Umschalt** und **Rollen** angezeigt. Zusätzlich sehen Sie rechts daneben das Symbol eines Schraubenschlüssels ([🔧]). Bei aktivem Menü-Modus erscheinen dort andere, bedienungsrelevante Symbole.

Benutzen Sie die darunterliegenden 4 Tasten, um durch das Menü zu navigieren oder entsprechende Menüpunkte auszuwählen:

Bei aktivem sicheren PIN-Eingabe-Modus werden diese Tasten zur PIN-Eingabe verwendet.

18.3 Funktion der Tasten im Nummernblock und Alphafeld

Die Tasten in der rechten Spalte des Nummernblocks zeigen zusätzliche, eingerahmte Symbole. Diese Tastenfunktion ist im Menü-Modus und im sicheren PIN-Eingabe-Modus aktiv. Sie können sie auch während der SICCT-Kommunikation zum Terminal anwenden.

Funktion	Taste Nummernblock	Taste Alphafeld
Vorgang abbrechen		
Letzte Eingabe löschen		
Bestätigen		

19 Statusanzeige LEDs

Die beiden LEDs zeigen den Status der jeweiligen Karte:

LED	Status
Rot blinkend	Sichere PIN-Eingabe (wird vom Konnektor aktiviert)
Grün	Karte aktiv (mit Strom versorgt)
Grün blinkend	Karte defekt

20 Display

Die Symbole im oberen Bereich des Displays haben folgende Bedeutung:

Symbol	Status
	Terminal über USB angeschlossen
	Vertrauenswürdiger Zustand und sichere, verschlüsselte Verbindung mit gepairtem Konnektor
	Sichere, verschlüsselte Verbindung über LAN
	Karte im Steckplatz 1 gesteckt
	Karte im Steckplatz 1 aktiviert
	Datenübertragung zur Karte
	Karte im Steckplatz 2 gesteckt
	Karte im Steckplatz 2 aktiviert
	Datenübertragung zur Karte
	Karte gesteckt (SM 1)

Symbol	Status
	gSMC-KT Karte erkannt und aktiviert (mit Strom versorgt)
	Karte gesteckt (SM 2)
	Karte gesteckt und aktiviert (SM 2)
	Datenübertragung zur Karte (SM 1 und SM 2)
	Kartenterminal unautorisiert auf Werkseinstellungen zurückgesetzt. Das Gerät befindet sich daher in einem unsicheren Zustand. Verdacht auf Manipulation am Gerät. Das Symbol wird nach erfolgreichem Pairing wieder ausgeblendet.

21 PIN-Eingabe-Modus

Der PIN-Eingabe-Modus wird immer dann aktiviert, wenn eine Abfrage zu einer Karten-PIN angefordert wird.

Im PIN-Eingabe-Modus werden Eingaben am Kartenterminal direkt zur eingesteckten Karte (z. B. Heilberufsausweis) gesendet. Die PIN verlässt das Kartenterminal nie im Klartext.

Dem senkrechten und dem seitlichen Kartenslot (Steckplatz 1 und 2) ist jeweils eine LED zugeordnet. Das rote Blinken der jeweiligen Kartenslot-LED zeigt den aktiven PIN-Eingabe-Modus für die gesteckte Karte an. Zusätzlich wird in der oberen Displayzeile ein Hinweistext auf das verwendete Eingabeverfahren eingeblendet.

Für die PIN-Eingabe gibt es zwei Verfahren, die sichere PIN-Eingabe und die PIN-Eingabe über den Nummernblock. Zu Beginn jeder PIN-Eingabe müssen Sie bestätigen, dass Sie die sichere PIN-Eingabe verwenden möchten. Lehnen Sie dies ab, können Sie auch die PIN-Eingabe über den Nummernblock verwenden.

Beachten Sie folgende Sicherheitshinweise:

- Verwenden Sie immer die sichere PIN-Eingabe über das Display.
- Die PIN-Eingabe über den Nummernblock entspricht nicht dem zertifizierten Anwendungsfall.
- Achten Sie darauf, dass Sie bei der Eingabe der PIN nicht beobachtet werden.
- Halten Sie Ihre PIN geheim.
- Geben Sie die PIN nur ein, wenn der PIN-Eingabe-Modus aktiv ist und eine sichere Verbindung zum Konnektor besteht (geschlossenes Schloss-Symbol wird angezeigt).
- In Ihrer Anwendung muss dabei erkennbar eine PIN angefordert worden sein.

21.1 Sichere PIN-Eingabe

Die sichere PIN-Eingabe zur Authentisierung gegenüber einer Chipkarte ist nur über die Auswahl der einzelnen PIN-Ziffern im Display möglich. Hierbei werden in der oberen Displayzeile die Ziffern 0 bis 9 angezeigt, von denen eine zufällig ausgewählt und markiert wird.

1 Bestätigen Sie, dass Sie die sichere PIN-Eingabe verwenden möchten.

2 Wählen Sie die gewünschte PIN-Ziffer über die Pfeil-Tasten (links, rechts) oder die Tasten unter den Displaysymbolen [←] und [→].

3 Bestätigen Sie die ausgewählte Ziffer mit den Pfeil-Tasten (oben, unten) oder der Taste unter den Displaysymbol [✓].

   Diese Ziffer wird an die aktuelle Stelle der PIN gesetzt. Für jede eingegebene Stelle der PIN wird ein Sternchen (*) angezeigt.

4 Bestätigen Sie die eingegebene PIN mit der Taste mit dem Symbol [O] auf dem Nummernblock.

Die sichere PIN-Eingabe wird durch Entnahme der Karte, Ablauf der Eingabezeit oder Betätigung der Taste mit dem Symbol [X] auf dem Nummernblock abgebrochen.

Steckplatz	Position	Hinweistext*
1 (ICC Slot 1)	Senkrecht	Sichere PIN Slot 1
2 (ICC Slot 2)	Seitlich	Sichere PIN Slot 2
3 (SM1)	Hinten	Sichere PIN SM 1
4 (SM2)	Hinten	Sichere PIN SM 2

** Wird der bei Auslieferung vorhandene FU-Name des Steckplatzes verändert und hat dann weniger als 9 Zeichen, lautet der Hinweistext "Sichere PIN [FU-Name]".*

21.2 PIN-Eingabe über den Nummernblock

1 Lehnen Sie ab, dass Sie die sichere PIN-Eingabe verwenden möchten.

2 Geben Sie die PIN über den Nummernblock des Tastenfeldes ein.

   Für jede eingegebene Stelle der PIN wird ein Sternchen (*) angezeigt.

3 Bestätigen Sie die eingegebene PIN mit der Taste mit dem Symbol [O] auf dem Nummernblock.

Die PIN-Eingabe wird durch Entnahme der Karte, Ablauf der Eingabezeit oder Betätigung der Taste mit dem Symbol [X] auf dem Nummernblock abgebrochen.

Steckplatz	Position	Hinweistext*
1 (ICC Slot 1)	Senkrecht	PIN unsicher Slot 1
2 (ICC Slot 2)	Seitlich	PIN unsicher Slot 2
3 (SM1)	Hinten	PIN unsicher SM 1
4 (SM2)	Hinten	PIN unsicher SM 2

** Wird der bei Auslieferung vorhandene FU-Name des Steckplatzes verändert und hat dann weniger als 9 Zeichen, lautet der Hinweistext "PIN unsicher [FU-Name]".*

21.3 Remote-PIN

Bei der Remote-PIN wird die eingegebene PIN mit Hilfe der gesteckten gSMC-KT Karte verschlüsselt und an eine Karte in einem anderen Terminal des eigenen Netzwerks übertragen.

Das Kartenterminal schaltet zur Remote-PIN Eingabe in den PIN-Eingabe-Modus.

Die Anzeige des aktiven PIN-Eingabe-Modus erfolgt hierbei ausschließlich durch den Hinweistext in der oberen Displayzeile für den Steckplatz der gSMC-KT Karte.

22 Eigendiagnose

Im Menü **Eigendiagnose** können Sie Folgendes prüfen:

- Funktion der Kartenleser
- Batteriestatus
- Originalität der Firmware

Siehe 23.1 "Mögliche Einstellungen (Hauptmenü)".

Wenn Sie die Firmwaregruppenliste (**Firmwaregruppe > Gruppen Version**) oder die CA-Zertifikate (**SICCT > CA-Zertifikate > Zertifikatsliste**) aufrufen, erfolgt vor der Anzeige eine automatische Integritätsprüfung der Daten.

KONFIGURATION

23 Lokale Konfiguration über direkte Managementschnittstelle

Folgende Funktionen sind nur lokal am Gerät zugänglich:

- Pairing mit einem Konnektor (siehe 15 "Pairing mit einem Konnektor")
- Aktivieren oder Deaktivieren administrativer SICCT-Kommandos (siehe 23.1 "Mögliche Einstellungen (Hauptmenü)")
- Aktivieren oder Deaktivieren der Web-Schnittstelle (siehe 24 "Konfiguration über Web-Schnittstelle")

23.1 Mögliche Einstellungen (Hauptmenü)

1 Drücken Sie für 3 Sekunden die Taste unter dem Symbol  auf dem Display.

Bei aktivem Menü-Modus werden Tastatureingaben nicht mehr an den Rechner geleitet.

2 Wählen Sie am Display des Kartenterminals im unteren Bereich **Menü**.

3 Um den Menü-Modus zu verlassen, drücken Sie die Taste unter dem Symbol  auf dem Display.

HINWEIS: Ausgeblendete Symbole "Menü" und "Info"

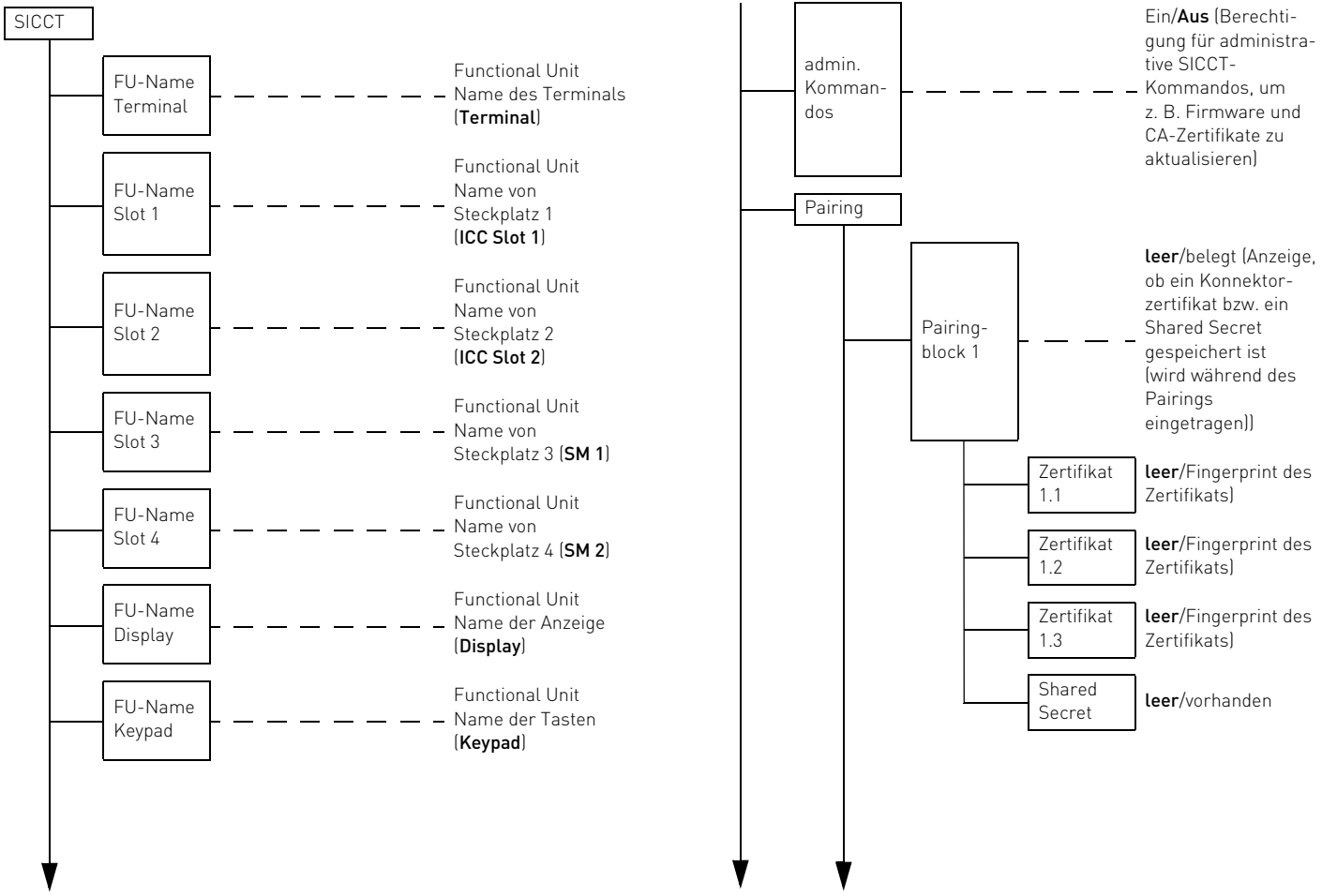
Bei aktiver SICCT-Verbindung, z. B. mit einem Konnektor, ist die Konfiguration des Terminals nicht möglich. Die Symbole "Menü" und "Info" werden in der Displayanzeige ausgeblendet.

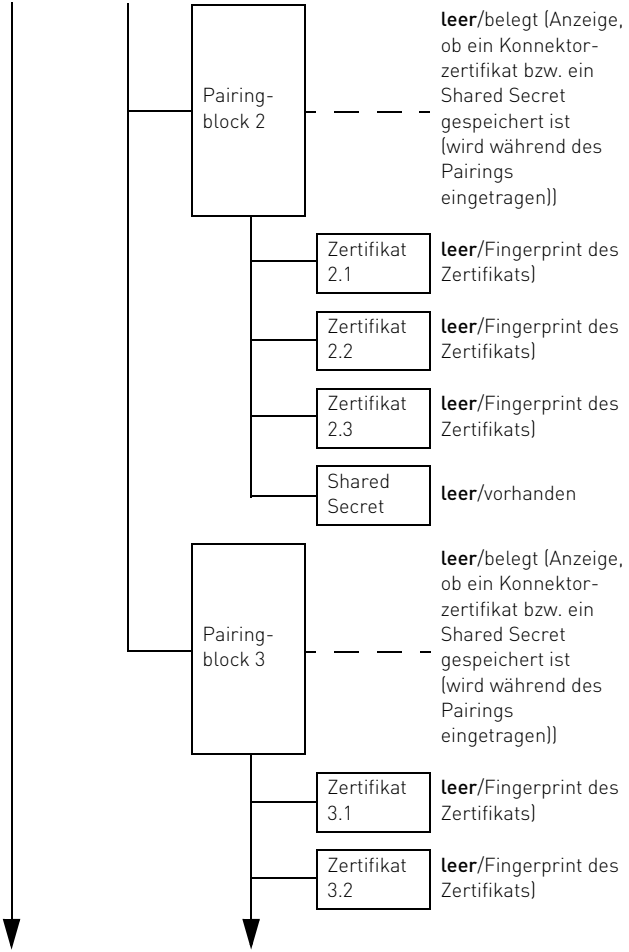
Blau und kursiv dargestellte Menüpunkte = Freier Zugriff durch Benutzer

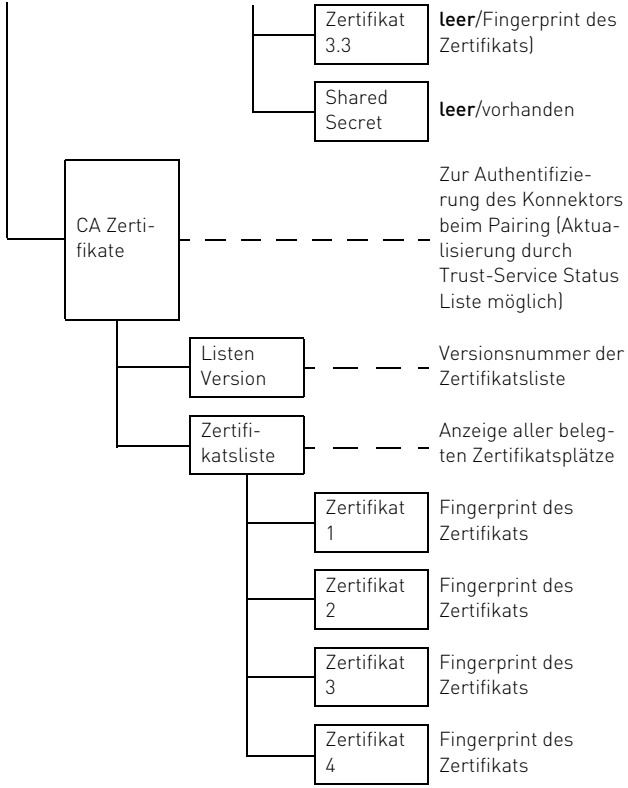
Schwarze Menüpunkte = Zugriff durch Administrator (Kennwort-Eingabe nötig)

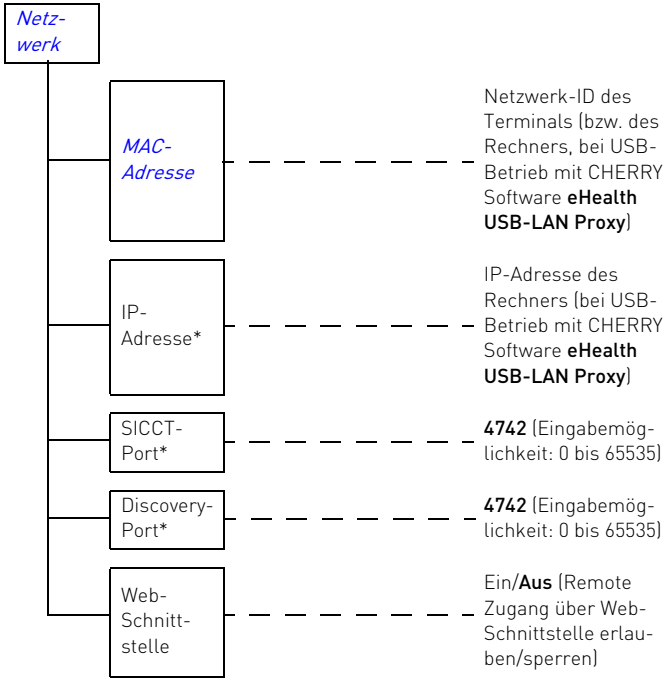
Fett = Werkseinstellungen

Sie können die auf den folgenden Seiten dargestellten Einstellungen vornehmen:

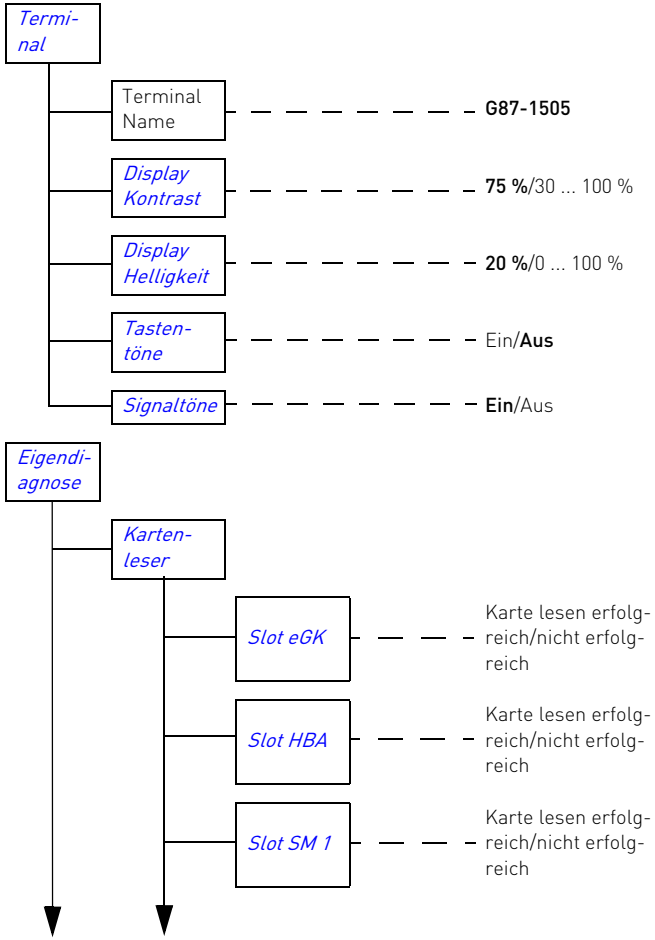

SICCT
FU-Name Terminal
Functional Unit Name des Terminals (**Terminal**)
FU-Name Slot 1
Functional Unit Name von Steckplatz 1 (**ICC Slot 1**)
FU-Name Slot 2
Functional Unit Name von Steckplatz 2 (**ICC Slot 2**)
FU-Name Slot 3
Functional Unit Name von Steckplatz 3 (**SM 1**)
FU-Name Slot 4
Functional Unit Name von Steckplatz 4 (**SM 2**)
FU-Name Display
Functional Unit Name der Anzeige (**Display**)
FU-Name Keypad
Functional Unit Name der Tasten (**Keypad**)
admin. Kommandos
Ein/**Aus** (Berechtigung für administrative SICCT-Kommandos, um z. B. Firmware und CA-Zertifikate zu aktualisieren)
Pairing
Pairing-block 1
leer/belegt (Anzeige, ob ein Konnektorzertifikat bzw. ein Shared Secret gespeichert ist (wird während des Pairings eingetragen))
Zertifikat 1.1
leer/Fingerprint des Zertifikats)
Zertifikat 1.2
leer/Fingerprint des Zertifikats)
Zertifikat 1.3
leer/Fingerprint des Zertifikats)
Shared Secret
leer/vorhanden

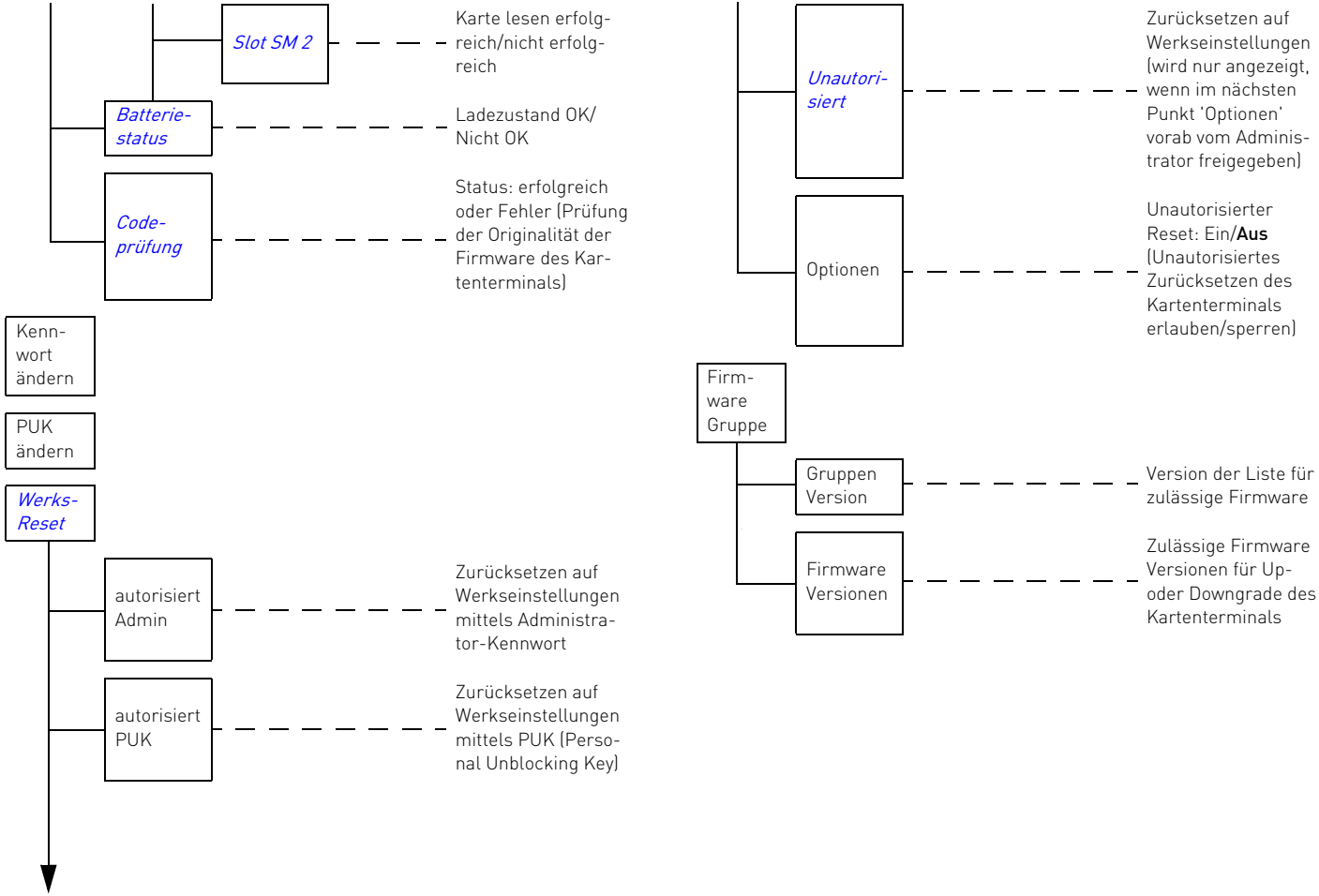

Pairing-block 2
leer/belegt (Anzeige, ob ein Konnektor-zertifikat bzw. ein Shared Secret gespeichert ist (wird während des Pairings eingetragen))
Zertifikat 2.1
leer/Fingerprint des Zertifikats)
Zertifikat 2.2
leer/Fingerprint des Zertifikats)
Zertifikat 2.3
leer/Fingerprint des Zertifikats)
Shared Secret
leer/vorhanden
Pairing-block 3
leer/belegt (Anzeige, ob ein Konnektor-zertifikat bzw. ein Shared Secret gespeichert ist (wird während des Pairings eingetragen))
Zertifikat 3.1
leer/Fingerprint des Zertifikats)
Zertifikat 3.2
leer/Fingerprint des Zertifikats)


Zertifikat 3.3
leer/Fingerprint des Zertifikats)
Shared Secret
leer/vorhanden
CA Zertifikate
Zur Authentifizierung des Konnektors beim Pairing (Aktualisierung durch Trust-Service Status Liste möglich)
Listen Version
Versionsnummer der Zertifikatsliste
Zertifikatsliste
Anzeige aller belegten Zertifikatsplätze
Zertifikat 1
Fingerprint des Zertifikats
Zertifikat 2
Fingerprint des Zertifikats
Zertifikat 3
Fingerprint des Zertifikats
Zertifikat 4
Fingerprint des Zertifikats



* Eine Änderung der IP-Adresse, des SICCT-Ports oder des Discovery-Ports wird erst nach einem Neustart übernommen.




Slot SM 2
Karte lesen erfolgreich/nicht erfolgreich
Batteriestatus
Ladezustand OK/ Nicht OK
Codeprüfung
Status: erfolgreich oder Fehler (Prüfung der Originalität der Firmware des Kartenterminals)
Kennwort ändern
PUK ändern
Werks-Reset
autorisiert Admin
Zurücksetzen auf Werkseinstellungen mittels Administrator-Kennwort
autorisiert PUK
Zurücksetzen auf Werkseinstellungen mittels PUK (Personal Unblocking Key)
Unautorisiert
Zurücksetzen auf Werkseinstellungen (wird nur angezeigt, wenn im nächsten Punkt 'Optionen' vorab vom Administrator freigegeben)
Optionen
Unautorisierter Reset: Ein/**Aus** (Unautorisiertes Zurücksetzen des Kartenterminals erlauben/sperren)
Firmware Gruppe
Gruppen Version
Version der Liste für zulässige Firmware
Firmware Versionen
Zulässige Firmware Versionen für Up- oder Downgrade des Kartenterminals

23.2 Menü Info

1 Drücken Sie für 3 Sekunden die Taste unter dem Symbol [⚿] auf dem Display.

Bei aktivem Menü-Modus werden Tastatureingaben nicht mehr an den Rechner geleitet.

2 Wählen Sie am Display des Kartenterminals im unteren Bereich **Info**.

3 Um den Menü-Modus zu verlassen, drücken Sie die Taste unter dem Symbol [⚿→⊓] auf dem Display.

HINWEIS: Ausgeblendete Symbole "Menü" und "Info"

Bei aktiver SICCT-Verbindung, z. B. mit einem Konnektor, ist die Konfiguration des Terminals nicht möglich. Die Symbole "Menü" und "Info" werden in der Displayanzeige ausgeblendet.

Blau und kursiv dargestellte Menüpunkte = Freier Zugriff durch Benutzer

Schwarze Menüpunkte = Zugriff durch Administrator (Kennwort-Eingabe nötig)

Die folgenden Informationen werden angezeigt:

- *Terminal Name* — **G87-1505**
- *Verbindung* — USB (bei Betrieb ohne CHERRY Software **eHealth USB-LAN Proxy)**
- *Verbindung* — USB-LAN Proxy (bei Betrieb mit CHERRY Software **eHealth USB-LAN Proxy**)
- *MAC-Adresse* — Netzwerk-ID des PCs, an dem die Tastatur angeschlossen ist
- *gSMC-KT Status* — Verfügbar/nicht verfügbar
- *Seriennummer* — Seriennummer des Geräts

- *Zulassungs-nummer* — gematik Zulassungsnummer
- *Produkt-identität*
  - *Hersteller-ID* — gematik Hersteller-ID
  - *Produktkürzel* — G87_1505
  - *Produktversion* — Firmwareversion:Hardwareversion
  - *Firmware-version* — Firmwareversion des Kartenterminals
  - *Hardware-version* — Hardwareversion des Kartenterminals
- *Produkttyp Info*
  - *Produkttyp* — eHealth-Kartenterminal
  - *Produkttyp-version* — Produkttypversion des Kartenterminals

24 Konfiguration über Web-Schnittstelle

Das Terminal enthält einen integrierten Webserver, der über eine https-Verbindung angesprochen werden kann. Dadurch kann die Konfiguration in einem Browser auf einer Webseite erfolgen.

Es stehen dabei nahezu die gleichen Informationen und Konfigurationsmöglichkeiten zur Verfügung, wie an der direkten Managementschnittstelle (lokaler Zugang).

Folgende Funktionen sind nur lokal am Terminal zugänglich:

- Pairing mit einem Konnektor (siehe 15 "Pairing mit einem Konnektor")
- Aktivieren oder Deaktivieren administrativer SICCT-Kommandos (siehe 23.1 "Mögliche Einstellungen (Hauptmenü)")
- Aktivieren oder Deaktivieren der Web-Schnittstelle (siehe 24 "Konfiguration über Web-Schnittstelle")

Derzeit wird ausschließlich der Mozilla Firefox Browser unterstützt. Browser anderer Hersteller wurden nicht getestet.

Für den Zugang über die Web-Schnittstelle müssen die folgenden Bedingungen erfüllt sein:

- Die gSMC-KT Karte steckt im Terminal (siehe 14 "gSMC-KT Karte installieren").
- Die Web-Schnittstelle wurde lokal am Terminal aktiviert (Standard = Aus). Umstellung unter **Menü > Netzwerk > Web-Schnittstelle > Ein**.
- Bei Verwendung einer Firewall, sind dort die Ports 4742 für UDP und TCP freigeschaltet. Falls dem Terminal andere Ports zugewiesen wurden, erhalten Sie diese am Terminal über **Menü > Netzwerk > SICCT-Port** bzw. **Discovery-Port**.
- Die IP-Adresse des Kartenterminals ist bekannt. Ab Werk ist DHCP aktiviert, d. h. die automatische Zuweisung einer freien IP-Adresse. Sie erhalten die IP-Adresse am Terminal über **Menü > Netzwerk > IP-Adresse** (oder über Ihren DHCP-Server).
- Ihr Browser unterstützt **TLS 1.1** oder **TLS 1.2** und diese Einstellung ist auch aktiviert (siehe 24.1 "Browser-Konfiguration auf TLS 1.1 oder TLS 1.2"). Empfehlung: Mozilla Firefox ab Version 33.

HINWEIS: Gesperrte Berechtigung bei aktiver Konnektor-Verbindung

Bei aktiver Konnektor-Verbindung ist der Zugang zur Web-Schnittstelle gesperrt.

- Beenden Sie am Konnektor die bestehende (SICCT-)Verbindung zum Terminal, um es zu konfigurieren.

1 Geben Sie im Browser die IP-Adresse des Terminals ein, z. B.: **https://192.168.1.199**.

- Beachten Sie dabei das **"s"** für die TLS-Verbindung.

  Die **Anmeldefläche des Kartenterminals** erscheint im Browser.

HINWEIS: Falls die Anmeldefläche nicht im Browser erscheint:

Für die sichere TLS-Verbindung zum Browser wird auch das Komponentenzertifikat der gSMC-KT verwendet. Da der Browser dieses Zertifikat nicht selbst überprüfen kann, wird die Meldung "Dieser Verbindung wird nicht vertraut" angezeigt.

- Überprüfen Sie das angezeigte Zertifikat der gSMC-KT anhand des Fingerprints (siehe 14 "gSMC-KT Karte installieren") und fügen dieses als Ausnahme im Browser hinzu.

Solange die gSMC-KT nicht ausgetauscht wird, erkennt dann der Browser das Zertifkat und leitet Sie zur Anmeldefläche weiter.

ACHTUNG: Ausspähen des Administrator-Kennworts möglich.

- Geben Sie das Administrator-Passwort nur in einer sicheren Umgebung ein.

2 Melden Sie sich an.
Benutzer: admin
Kennwort: Das Kennwort, welches Sie bei der Inbetriebnahme vergeben haben.
Siehe 12 "Administrator-Kennwort".

3 Folgen Sie den Anweisungen auf dem Bildschirm.

Der Aufbau des Menüs an der Webschnittstelle entspricht der direkten Benutzerschnittstelle (siehe 23 "Lokale Konfiguration über direkte Managementschnittstelle"). Informationen zur Parametrierung sind beim jeweiligen Menüpunkt hinterlegt.

24.1 Browser-Konfiguration auf TLS 1.1 oder TLS 1.2

Kann Ihr eingesetzter Browser keine Verbindung aufbauen, müssen Sie die Verwendung von TLS 1.1 oder TLS 1.2 wie folgt aktivieren:

Mozilla Firefox

1 Verwenden Sie Mozilla Firefox erst ab Version 23, da frühere Versionen TLS 1.1 nicht unterstützen.
2 Geben Sie in die Adresszeile **about:config** ein.
3 Suchen Sie den Parameter **security.tls.version.max**.
4 Falls der Wert auf **1** gesetzt ist, ändern Sie ihn auf **3**.

25 Konfiguration über CHERRY Software

Die Verwaltung des Kartenterminals kann auch mittels der CHERRY Software **eHealth Device Manager** erfolgen. Es handelt sich um ein 32-Bit Windows Programm, das sich ohne Installation ausführen lässt. Sie erhalten es unter **https://www.cherry.de**.

Im Download-Bereich wird zur Software eine SHA-256 Prüfsumme angegeben. Damit müssen Sie vor dem Einsatz deren Authentizität überprüfen. Entsprechende Tools, um diese Prüfung durchzuführen, sind im Internet frei verfügbar.

Der **eHealth Device Manager** baut eine Verbindung zum Kartenterminal auf (SICCT-Zugang) und bietet die folgenden Funktionen:

- Übersicht aller CHERRY eHealth Geräte innerhalb des Netzwerks
- Terminal- und Diagnoseinformationen auslesen
- Firmware aktualisieren
- Komponentenzertifikate für Konnektoren aktualisieren

Für den Einsatz der CHERRY Software **eHealth Device Manager** müssen die folgenden Bedingungen erfüllt sein:

- Die gSMC-KT Karte steckt im Terminal (siehe 14 "gSMC-KT Karte installieren").
- Es ist keine aktive SICCT-Verbindung vorhanden (die Verbindung mit dem Konnektor wurde beendet).
- Die administrativen SICCT-Kommandos wurden lokal am Terminal aktiviert (Standardeinstellung = Aus). Umstellung unter **Menü > SICCT > admin. Kommandos > Ein**.
- Bei Verwendung einer Firewall, sind dort die Ports 4742 für UDP und TCP freigeschaltet. Falls dem Terminal andere Ports zugewiesen wurden, erhalten Sie diese am Terminal über **Menü > Netzwerk > SICCT-Port** bzw. **Discovery-Port**.

HINWEIS: Gesperrte Berechtigung bei aktiver Konnektor-Verbindung

Bei aktiver Konnektor-Verbindung ist der Zugang über die CHERRY Software gesperrt.

- Beenden Sie am Konnektor die bestehende (SICCT-)Verbindung zum Terminal

26 Firmware aktualisieren

Halten Sie die Firmware des Kartenterminals sowie die zugehörige CHERRY Software **eHealth Device Manager** und **eHealth USB-LAN Proxy** stets aktuell. Prüfen Sie dazu regelmäßig unsere Homepage unter **https://www.cherry.de**.

Neben der Hardware ist die Firmware ein sicherheitssensibles Element. Verwenden Sie aus diesem Grund nur zertifizierte und bestätigte Firmware-Versionen.

Es besteht die Möglichkeit, auch ältere Firmware einzuspielen. Welche Versionen in das Terminal geladen werden können, ist in der Liste

unter Firmware-Gruppe ersichtlich: **Menü > Firmware-Gruppe > Firmware-Versionen**.

Eine sich nicht in dieser Liste befindliche alte Firmware-Version kann nicht eingespielt werden. Die Liste wird jeweils durch die eingespielte Firmware aktualisiert.

HINWEIS: Risiko durch Einspielen älterer Firmware

Möglicherweise sind darin bestimmte Konfigurationen und Funktionen nicht oder nur noch teilweise vorhanden.

Informationen zu den jeweiligen Firmwareständen und den in der Firmware-Gruppe erlaubten Versionen erhalten Sie unter **https://www.cherry.de**.

1 Prüfen Sie, ob die administrativen SICCT-Kommandos aktiviert sind (Standard-einstellung = Aus): **Menü > SICCT > admin. Kommandos > Ein**.
2 Verwenden Sie zur Aktualisierung entweder den Konfigurationsdienst des verbundenen Konnektors oder die CHERRY Software **eHealth Device Manager**.
3 Bei Verwendung der CHERRY Software **eHealth Device Manager**:
Laden Sie das aktuelle Update Paket von unserer Homepage unter **https://www.cherry.de** auf einen gesicherten Rechner innerhalb Ihres Netzwerks herunter. Prüfen Sie, ob die Version der heruntergeladenen Datei mit der gewünschten übereinstimmt und führen Sie sofort den Updatevorgang aus.
4 Folgen Sie den Anweisungen der Software bzw. der beiliegenden Anleitung.

HINWEIS: Die Eingabe des Administrator-Kennworts im eHealth Device Manager ist risikobehaftet!

Stellen Sie Folgendes sicher:

- Es wird eine authentische Software verwendet (Empfehlung: Download direkt von der CHERRY Website und Vergleich der angegebenen Prüfsumme).
- Die Daten zwischen Software und Kartenterminal werden nicht abgefangen (es wird eine TLS-Verbindung zum Terminal aufgebaut).
- Das richtige Terminal wird angesprochen (Achten Sie auf die angezeigten IP-/MAC-Adressen. Verwenden Sie ggf. eindeutige Terminal-Namen).

5 Geben Sie im **eHealth Device Manager** das Administrator-Kennwort der SICCT-Schnittstelle ein.

Die Konfiguration des Kartenterminals bleibt beim Update erhalten (z. B. Terminal-Name, IP-Adresse oder Pairing-Informationen).
6 Prüfen Sie nach dem Update, ob sich tatsächlich die gewünschte Firmware-Version im Gerät befindet. Sollte dies nicht der Fall sein, prüfen Sie, ob Sie die originale Firmware von unserer Homepage **https://www.cherry.de** verwendet haben.

27 Zurücksetzen auf Werkseinstellungen

Es wird der Auslieferungszustand des Geräts wieder hergestellt (mit Ausnahme der Firmware und der Firmwaregruppe). Die Inbetriebnahme ist damit erneut durchzuführen.

Im Folgenden werden 3 Möglichkeiten beschrieben, das Gerät auf die Werkseinstellungen zurückzusetzen. Falls Sie diese nicht nutzen können, wenden Sie sich an Ihren Gerätelieferanten.

27.1 Werks-Reset durch den Administrator

- Wählen Sie im **Menü > Werks-Reset > autorisiert Admin > (Administrator-Kennwort eingeben) > Werkseinstellungen wiederherstellen (Taste 0)**.

27.2 Werks-Reset durch PUK-Eingabe

Falls Sie das Administrator-Kennwort vergessen haben, kann der Reset-Administrator das Kartenterminal durch Eingabe des PUKs (**P**ersonal **U**nblocking **K**ey) auf Werkseinstellungen zurücksetzen.

- Wählen Sie im **Menü > Werks-Reset > autorisiert PUK > (PUK eingeben) > Werkseinstellungen wiederherstellen (Taste 0)**.

27.3 Werks-Reset ohne Authentisierung

Das unautorisierte Zurücksetzen auf Werkseinstellungen darf ausschließlich durch den (Reset-) Administrator erfolgen.

Der folgende Menüpunkt wird nur angezeigt, wenn die Möglichkeit des unautorisierten Werks-Resets vorab durch den Administrator aktiviert wurde (**Menü > Werks-Reset > Optionen > Ein**).

- Wählen Sie im **Menü > Werks-Reset > Unautorisiert > Werkseinstellungen wiederherstellen**.

Ein Ausrufezeichen im oberen linken Bereich des Displays zeigt an, dass das Kartenterminal unautorisiert auf Werkseinstellungen zurückgesetzt worden ist. Das Gerät befindet sich in einem unsicheren Zustand. Nach erfolgreichem Pairing wird das Ausrufezeichen wieder ausgeblendet.

ACHTUNG: Verdacht auf Manipulation, falls im Display erscheint

Das Terminal war bereits mit einem Konnektor verbunden und kann darüber nicht mehr angesprochen werden bzw. die Pairing-Informationen sind nicht mehr vorhanden.

Das Terminal wurde nicht durch den (Reset-) Administrator auf Werkseinstellungen zurückgesetzt.

- Verwenden Sie das Gerät nicht weiter.
- Wenden Sie sich an Ihren Gerätelieferanten.

AUSSER-BETRIEBNAHME

28 Löschen der Pairing-Informationen

ACHTUNG: Weitergabe von Pairing-Informationen

- Stellen Sie sicher, dass bei einer Außerbetriebnahme des Geräts alle Pairing-Informationen gelöscht werden.

1 Wählen Sie im Menü des Kartenterminals **SICCT > Pairing > Pairingblock 1 ... 3**.

Bei Anwahl eines belegten Pairingblocks wird eine Löschoption angezeigt.

2 Löschen Sie alle belegten Pairingblöcke (beinhaltet die Public Keys und das Shared Secret).

29 Reparatur

Das Öffnen des Geräts aktiviert den Manipulationsschutzmechanismus und löst eine elektronische Sperre aus. Ein gesperrtes Gerät besitzt keine Funktionalität mehr. Wenden Sie sich an Ihren Gerätelieferanten.

30 Batterie

Das Gerät enthält eine fest eingebaute Lithium-Mangandioxid Batterie (Li-MnO_2/organische Elektrolyte) mit einer durchschnittlichen Kapazität von 950 mAh.

Im Fall einer entladenen Batterie während der Nutzungsphase des Geräts wird der Manipulationsschutz aktiviert und Sie erhalten die Fehlermeldung "Gehäuseüberwachung". Wenden Sie sich an Ihren Gerätelieferanten.

31 Entsorgung

Wenn sich die Batterie am Ende ihrer Lebensdauer nicht mehr laden lässt, entsorgen Sie sie nicht im Hausmüll. Batterien enthalten möglicherweise Schadstoffe, die Umwelt und Gesundheit schaden können. Bitte geben Sie die Batterie gemeinsam mit dem Gerät im Handel oder bei den Recyclinghöfen der Kommunen ab. Die Rückgabe ist gesetzlich vorgeschrieben und unentgeltlich.

Alle Batterien und Akkus werden wiederverwertet. So lassen sich wertvolle Rohstoffe, wie Eisen, Zink oder Nickel, zurückgewinnen. Batterierecycling ist der leichteste Beitrag zum Umweltschutz.

Vielen Dank für's Mitmachen.

32 Fehlermeldungen

32.1 Direkte (lokale) Schnittstelle

Meldung	Bedeutung
Abbruch nach Fehler	Während des Firmware-Updates trat ein Fehler auf, der zum Abbruch führte. Trennen Sie das Kartenterminal kurz von der Stromversorgung und starten Sie es danach neu. Im wiederholten Fehlerfall wenden Sie sich an Ihren Gerätelieferanten.
Abbruch nach Timeout	Verbindungsabbruch zum Terminal während des Aktualisierens der Firmware oder notwendige Benutzerinteraktionen wurden über längere Zeit nicht ausgeführt (Timeout). Starten Sie den Vorgang neu. Halten Sie die Verbindung zum Rechner aufrecht und führen Sie Benutzerinteraktionen zügig durch.
Die Version dieser Firmware ist nicht zulässig	Das Einspielen der vorliegenden Firmware ist nicht zulässig. Prüfen Sie die zugelassenen Firmware-Versionen im **Menü > Firmware-Gruppe > Firmware-Versionen**. Verwenden Sie eine passende Version und versuchen Sie es erneut.
Eingaben nicht gleich	Die Wiederholung des Kennworts bzw. der PUK war abweichend zur ersten Eingabe. Versuchen Sie es erneut.
Fehler beim Lesen der Konfiguration	Die Terminalkonfiguration konnte nicht gelesen werden. Trennen Sie das Kartenterminal kurz von der Stromversorgung und starten Sie es danach neu. Im wiederholten Fehlerfall wenden Sie sich an Ihren Gerätelieferanten.
Fehler beim Speichern der Konfiguration	Die Terminalkonfiguration konnte nicht gespeichert werden. Versuchen Sie es mit einem anderen Wert erneut. Im wiederholten Fehlerfall wenden Sie sich an Ihren Gerätelieferanten.
Fehlerhafter Code	Möglicherweise ist die Firmware fehlerhaft. Eine Prüfung erfolgt automatisch bei Neustart des Geräts oder manuell nach Auswahl im Hauptmenü. Wenden Sie sich an Ihren Gerätelieferanten.
Gehäuseüberwachung	Der Sicherheitsmechanismus wurde aktiviert. Mögliche Ursachen: Manipulation oder Öffnen des Gehäuses, Transport- oder Fallschaden, Gerätedefekt, Batterie entladen. Wenden Sie sich an Ihren Gerätelieferanten.

Meldung	Bedeutung
gSMC-KT-Fehler Zum Neustarten Menü-Taste 5 Sek. lang drücken	Es trat ein Fehler beim Lesen der gSMC-KT Karte auf. Halten Sie die Menü-Taste gedrückt, bis zum Neustart des Terminals. Im wiederholten Fehlerfall wenden Sie sich an Ihren Gerätelieferanten.
Keine freien Pairing-Blöcke verfügbar	Das initiale Pairing mit einem Konnektor ist gescheitert, weil die maximale Anzahl an Pairing-Blöcken erreicht ist. Löschen Sie mindestens einen Pairing-Block und starten Sie das Pairing erneut.
Kennwort enthält Benutzernamen	Das Kennwort darf den Benutzernamen nicht enthalten. Vergeben Sie ein anderes Kennwort.
Kennwort falsch	Geben Sie das korrekte Administrator-Kennwort ein.
Kennwort ist unzulässig	Das Kennwort muss mindestens eine Zahl enthalten. Verwenden Sie nur die Buchstaben A - Z, a - z und Zahlen 0 - 9. Vergeben Sie ein anderes Kennwort.

Meldung	Bedeutung
Länge des Kennwortes ungültig	Das Kennwort muss mindestens 8 und darf maximal 12 Zeichen lang sein.
Länge des PUKs ungültig	Der Personal Unblocking Key (PUK) muss mindestens 8 und darf maximal 12 Zeichen lang sein.
PUK falsch	Geben Sie den korrekten Personal Unblocking Key (PUK) ein.
PUK ist unzulässig	Der Personal Unblocking Key (PUK) muss mindestens eine Zahl enthalten. Verwenden Sie nur die Buchstaben A - Z, a - z und Zahlen 0 - 9. Vergeben Sie einen anderen PUK.
Signatur fehlerhaft	Das Firmware-Update wurde abgebrochen. Verwenden Sie nur von CHERRY freigegebene Firmware.

Meldung	Bedeutung
Unerwarteter Fehler	Ein Fehler ohne verfügbare Beschreibung ist aufgetreten. Trennen Sie das Kartenterminal kurz von der Stromversorgung und starten Sie es danach neu. Im wiederholten Fehlerfall wenden Sie sich an Ihren Gerätelieferanten.
Ungültige Eingabe	Die Eingabe ist ungültig. Das Format oder der Wertebereich sind nicht zulässig. Versuchen Sie es mit einem passenden Wert erneut.
Ungültige Zeichen	Die Eingabe enthält keine oder ungültige Zeichen. Zulässig sind: A - Z, a - z, Leerzeichen, Komma, Punkt, Minus und 0 - 9.
Ungültiger Wert	Die Eingabe ist ungültig. Versuchen Sie es mit einem passenden Wert erneut.

Meldung	Bedeutung
Verbindungs-fehler Zum Neustarten Menü-Taste 5 Sek. lang drücken	Es trat ein Fehler in der (SICCT-) Verbindung zum Terminal auf. Halten Sie die Menü-Taste gedrückt, bis zum Neustart des Terminals. Im wiederholten Fehlerfall wenden Sie sich an Ihren Gerätelieferanten.
Zugang zur Zeit gesperrt	Kennwort oder PUK wurde zu oft falsch eingegeben. Das Kartenterminal ist zeitabhängig gesperrt. Die Anzahl der Falscheingaben und die verbleibende Sperrzeit werden angezeigt. Warten Sie, bis die Sperrzeit abgelaufen ist und versuchen Sie es dann erneut.

32.2 Web-Schnittstelle

Meldung	Bedeutung
Das eingegebene Kennwort war erneut falsch.	Bei der Kennwortänderung wurde das bisherige Web-Schnittstellen-Kennwort wiederholt falsch eingegeben. Aus Sicherheitsgründen ist eine erneute Anmeldung an der Web-Schnittstelle erforderlich.
Das Kennwort darf den Benutzernamen nicht enthalten.	Wählen Sie ein anderes Kennwort und versuchen Sie es erneut.
Das Kennwort ist unzulässig.	Das Kennwort entspricht nicht den Sicherheitsvorgaben. Es enthält unzulässige Zeichen oder keine Zahlen. Verwenden Sie nur die Buchstaben A - Z, a - z und Zahlen 0 - 9. Es muss mindestens eine Zahl enthalten sein.

Meldung	Bedeutung
Die Codeprüfung kann nicht durchgeführt werden. Das Ausführen der Codeprüfung ist nur möglich, wenn keine SICCT-Verbindung aktiv ist und das Konfigurationsmenü lokal am Terminal verlassen wurde.	Beenden Sie die Verbindung mit dem Terminal und verlassen Sie ggf. das Konfigurationsmenü am Terminal. Wiederholen Sie dann die Codeprüfung. Im wiederholten Fehlerfall wenden Sie sich an Ihren Gerätelieferanten.
Die eingegebenen Kennwörter stimmen nicht überein.	Das neue Kennwort wurde bei der Bestätigung nicht korrekt wiederholt. Versuchen Sie es erneut.
Die Einstellungen können nicht gespeichert werden. Das Speichern der Einstellungen während einer aktiven SICCT-Verbindung ist nicht möglich.	Beenden Sie die SICCT-Verbindung mit dem Terminal und versuchen Sie es erneut.

Meldung	Bedeutung
Die Konfiguration kann nicht geöffnet werden. Es besteht ein aktiver Zugriff am Terminal. Ein paralleler Zugriff auf die Konfiguration, von mehreren Managementschnittstellen aus, ist nicht erlaubt. Verlassen Sie zuerst das Konfigurationsmenü am anderen Zugang. Versuchen Sie es dann erneut.	Das Öffnen der Terminalkonfiguration ist fehlgeschlagen, da der Menü- oder Info-Button am Terminal gedrückt wurde bzw. die entsprechende Funktion aktiv ist. Melden Sie sich am Terminal ab, indem Sie den Menü-Modus verlassen.
Die Länge des Kennwortes ist ungültig.	Das Kennwort muss zwischen 8 und 12 Zeichen lang sein. Überprüfen Sie die Kennwortlänge und versuchen Sie es erneut.
Die markierten Parameter wurden nicht geändert, da die eingegebenen Werte nicht zulässig waren.	Bisherige Werte werden angezeigt und sind weiterhin gültig. Andere Parameter, sofern geändert, wurden erfolgreich übernommen.

Meldung	Bedeutung
Die markierten Parameter wurden nicht geändert, die übrigen Änderungen wurden erfolgreich übernommen. Bitte starten Sie das Terminal neu, damit die geänderten Parameter wirksam werden.	Die markierten Werte sind weiterhin gültig. Aufgrund der übrigen Änderungen ist ein Neustart des Terminals erforderlich.
Es ist ein unerwarteter Fehler aufgetreten. Bitte starten Sie das Terminal neu.	Im wiederholten Fehlerfall wenden Sie sich an Ihren Geräteliferanten.
Falsches Kennwort.	Geben Sie das gültige Kennwort für die Web-Schnittstelle ein.
Fehler beim Erstellen der Tabelle der CA-Zertifikate.	Das Kartenterminal enthält eine sog. Trust-Service Status Liste verfügbarer CA-Zertifikate für zugelassene Konnektoren. Beim Anzeigen dieser Liste ist ein Fehler aufgetreten. Im wiederholten Fehlerfall wenden Sie sich an Ihren Geräteliferanten.

Meldung	Bedeutung
Fehler beim Erstellen der Tabelle der Pairing-Informationen.	Beim Anzeigen der Pairing-Informationen ist ein Fehler aufgetreten. Versuchen Sie es erneut. Im wiederholten Fehlerfall wenden Sie sich an Ihren Geräteliferanten.
Fehlerhafter oder korrupter Firmware Code!	Trennen Sie das Kartenterminal kurz von der Stromversorgung und starten Sie es danach neu. Im wiederholten Fehlerfall wenden Sie sich an Ihren Geräteliferanten.
HTTP/1.0 401 Unauthorized Zugriff verweigert. Zugriff zur eHealth Terminal Konfiguration verweigert. Bitte versuchen Sie es in ... noch einmal.	Die gewünschte Seite erfordert eine Authentisierung. Der Zugang via Web-schnittstelle ist nach mehr als zwei Fehlversuchen für die angegebene Zeit gesperrt.

Meldung	Bedeutung
HTTP/1.0 401 Unauthorized Zugriff verweigert. Zugriff zur eHealth Terminal Konfiguration verweigert. Melden Sie sich als Administrator an.	Die gewünschte Seite erfordert eine Authentisierung als Administrator.
HTTP/1.0 403 Forbidden Verboten Zugriff zum eHealth Terminal verweigert. Der angemeldete Benutzer hat nicht die nötigen Rechte, um auf diese Seite zuzugreifen. Sofern Benutzername oder Passwort falsch eingegeben wurden, bitte ausloggen und erneut einloggen.	Das aufgerufene Verzeichnis existiert, es ist aber nur der komplette Pfad erlaubt. Beispiel: Verzeichnis "[...]/Status" wurde aufgerufen, anstatt des kompletten Pfads "[...]/Status/ReadOnly".
HTTP/1.0 404 Not Found Webseite nicht gefunden Die angeforderte Webadresse (URL) existiert am eHealth Terminal nicht.	Überprüfen Sie die Schreibweise.

Meldung	Bedeutung
HTTP/1.0 501 Not implemented Fehler beim Laden des Formats der Webadresse (URL) Kodierungstyp wird nicht unterstützt.	Standardmeldung für unbestimmte Fehlerbedingungen.
WEB-Schnittstelle gesperrt. Der Zugang über die Web-Schnittstelle ist am Terminal gesperrt. Aktivieren Sie die Web-Schnittstelle lokal, direkt am Kartenterminal.	Meldung erscheint nach einem Anmeldeversuch bei deaktivierter Web-Schnittstelle.

33 Reinigen der Tastatur

ACHTUNG: Beschädigung durch aggressive Reinigungsmittel oder Flüssigkeit im Gerät

- Verwenden Sie zur Reinigung keine Lösungsmittel wie Benzin oder Alkohol und keine Scheuermittel oder Scheuerschwämme.
- Verhindern Sie, dass Reinigungsmittel in Kontakt mit den Siegeln geraten.
- Verhindern Sie, dass Flüssigkeit in das Gerät gelangt.
- Entfernen Sie nicht die Tastkappen.

1 Schalten Sie den PC aus.
2 Reinigen Sie das Gerät mit einem leicht feuchten Tuch und etwas mildem Reinigungsmittel (z. B.: Geschirrspülmittel).
3 Trocknen Sie das Gerät mit einem fusselfreien, weichen Tuch.

34 Zubehör

WetEx® – die Flexible Tastatur-Schutzfolie, schützt die **G87-1505** vor Flüssigkeiten, Staub und Fremdkörpern.

Bestellnummer: 615-5211

ACHTUNG: Manipulation am Gerät

Fremdkörper können zur Vertuschung oder Tarnung eines Angriffs genutzt werden.

- Aus sicherheitstechnischer Sicht sollten Sie das Gerät nicht bekleben oder abdecken.

35 RSI-Syndrom

"Repetitive Strain Injury" = "Verletzung durch wiederholte Beanspruchung". RSI entsteht durch kleine, sich ständig wiederholende Bewegungen.

Typische Symptome sind Beschwerden in den Fingern oder im Nacken.

- Richten Sie Ihren Arbeitsplatz ergonomisch ein.
- Positionieren Sie Tastatur und Maus so, dass sich Ihre Oberarme und Handgelenke seitlich vom Körper befinden und ausgestreckt sind.
- Machen Sie mehrere kleine Pausen, ggf. mit Dehnübungen.
- Ändern Sie oft Ihre Körperhaltung.

36 Kontakt

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

- Artikel- und Serien-Nr. des Produkts
- Bezeichnung und Hersteller Ihres Systems
- Betriebssystem und ggf. installierte Version eines Service Packs

Cherry GmbH
Cherrystraße
91275 Auerbach/OPf.

Internet: https://www.cherry.de

Telefon: +49 (0) 9643 2061-100*

*zum Ortstarif aus dem deutschen Festnetz, abweichende Preise für Anrufe aus Mobilfunknetzen möglich

37 Allgemeiner Anwenderhinweis

Technische Änderungen, die dem Fortschritt dienen, behalten wir uns vor. Unsachgemäße Behandlung und Lagerung können zu Störungen und Schäden am Produkt führen.

Die vorliegende Anleitung ist nur gültig für das mitgelieferte Produkt.

38 Gewährleistung

Es gilt die gesetzliche Gewährleistung. Bitte wenden Sie sich an Ihren Händler oder Vertragspartner.

Die Gewährleistung erlischt komplett, sofern unautorisierte Änderungen am Produkt durchgeführt worden sind. Führen Sie eigenmächtig keine Reparaturen durch und öffnen Sie das Produkt nicht.

39 Technische Daten

Bezeichnung	Wert
Systemvoraussetzungen (bei USB-Betrieb)	Installation der CHERRY Software **eHealth USB-LAN Proxy** auf entsprechendem Betriebssystem (siehe **https://www.cherry.de**) Nur Tastaturfunktion: USB-unterstützendes Betriebssystem (Windows, Linux oder Apple Mac OS)
Systemvoraussetzungen für CHERRY Software **eHealth Device Manager**	Unterstütztes Windows Betriebssystem (siehe **https://www.cherry.de**)
Display	Graphisches Display (128 x 64 Pixel)

Bezeichnung	Wert
Terminal-schnittstellen	**USB-A Host Buchse:** USB 2.0 Full Speed, für den Anschluss weiterer Geräte, z. B. PIN-Pad (vorbereitet, nicht aktiviert) **Netzteilbuchse:** für externes Netzteil 5,2 V DC, 1000 mA
Internet-Protokolle	IPv4
Kartenschnitt-stellen	ISO 7816 Typ A, B, C, 2 ID-1 Slots landende Kontakte, 2 ID-000 Plug-Ins
Protokolle	T=0, T=1, S=8, S=9, S=10
Übertragungsge-schwindigkeit	Zur Karte: 820 kBit/s, zum System: bis 12 MBit/s
Steckzyklen	> 300.000
Lebensdauer Einzeltaste	> 20.000.000 Betätigungen
Stromversorgung	Über USB
Stromaufnahme	Max. 500 mA
Lagertemperatur	–20 °C bis +60 °C
Betriebs-temperatur	0 °C bis +40 °C

40 Abkürzungen und Begriffserklärungen

Abkürzung/ Begriff	Bedeutung
Administrator (bzw. Admin)	Verwalter des Systems. Er nimmt das System oder Teile davon in Betrieb und betreut es während der Produktlebensdauer.
Benutzer	Endanwender bzw. Nutzer des Geräts, mit eingeschränkten Rechten zur Systemverwaltung
BSI	**B**undesamt für **S**icherheit in der **I**nformationstechnik
CA-Zertifikat	Von einer Zertifizierungsstelle (**C**ertificate **A**uthority, CA) bereitgestellter, digitaler Datensatz
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol (dient zur automatischen Einbindung in ein Netzwerk)
EAL	**E**valuation **A**ssurance **L**evel
eGK	**E**lektronische **G**esundheits**k**arte
eHealth	Elektronisches Gesundheitswesen
eHealth-Terminal	Kartenlesegerät auf Basis SICCT zur Verwendung im deutschen Gesundheitswesen
FU-Name	**F**unctional **U**nit Name

Abkürzung/ Begriff	Bedeutung
gematik	Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (**www.gematik.de**)
gSMC-KT	**G**erätespezifische **S**ecurity **M**odule **C**ard für das **K**arten**t**erminal
Heilberufs-ausweis (HBA)	Personenbezogener Ausweis im Gesundheitswesen. Er beinhaltet die Dienste Authentifizierung, Verschlüsselung sowie elektronische Signatur und ermöglicht den Zugriff auf Daten der eGK.
Konnektor	Bindeglied zwischen der Leistungserbringerseite und der Telematikinfrastruktur. Der Konnektor koordiniert und verschlüsselt die Kommunikation.
KIS	**K**rankenhaus**i**nformations**s**ystem
KVK	**K**ranken**v**ersicherten**k**arte
LAN	**L**ocal **A**rea **N**etwork (lokales Netzwerk)
Leistungs-erbringer	Alle Personengruppen, die im deutschen Gesundheitssystem Leistungen für die Versicherten der Krankenkassen erbringen.
PIN	**P**ersonal **I**dentification **N**umber (persönliche Geheimzahl)
PVS	**P**raxis**v**erwaltungs**s**ystem

Abkürzung/ Begriff	Bedeutung
SHA-265 Prüfsumme	**S**ecure **H**ash **A**lgorithm: Dient zur Erstellung einer Prüfsumme für digitale Daten. Mit einer frei verfügbaren Software bildet der Sender der Datei eine Prüfsumme und teilt diese dem Empfänger mit. Der Empfänger bildet anhand der erhaltenen Datei ebenfalls eine Prüfsumme. Wenn die Prüfsummen nicht übereinstimmen, wurde die Datei auf dem Übertragungsweg verändert.
SICCT	**S**ecure **I**nteroperable **C**hip **C**ard **T**erminal: Eine Spezifikation für ein universell einsetzbares Chipkartenterminal. In der Online-Phase werden eHealth-Terminals der SICCT-Spezifikation (www.teletrust.de/projekte/sicct) entsprechend angesprochen.
SMC-B	**S**ecurity **M**odule **C**ard - Typ B für das Kartenterminal. Eine Chipkarte, die zur Authentifikation einer berechtigten Institution im Gesundheitswesen dient.
USB-A Device	USB Gerät mit Stecker Typ-A
USB-A Host	USB Host mit Buchse Typ-A

41 Literatur

[1]

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1, Revision 4, September 2012

Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

[2]

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 – Interindustry commands for interchange

Hinterlassen Sie uns einen Kommentar

#cherrykeyboards

 social.cherry.de/fbmx

 social.cherry.de/youtube

 social.cherry.de/twitter

 social.cherry.de/insta

 blog.cherry.de

Cherry GmbH, Cherrystraße, 91275 Auerbach/OPf., Germany – **https://www.cherry.de**