



eGK Tastatur G87-1505

Kurzanleitung für Benutzer

Sicherheitsfunktionen	3
Inbetriebnahme	5
Bedienung.....	9
Konfiguration.....	13
Außerbetriebnahme	15
Allgemeines.....	16

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.

Ihre **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 der Tastatur ist weitgehend selbsterklärend durch die Navigation am Display des Geräts 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 dieser Kurzanleitung

Diese Kurzanleitung richtet sich an Beschäftigte im deutschen Gesundheitswesen, die in Betrieb befindliche Geräte bedienen. Sie enthält die für **Benutzer** notwendigen Handlungsabläufe und grundlegende Informationen zum sicheren Betrieb des Geräts.

Sie 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 Begriffe "Terminal" bzw. "Kartenterminal" immer auf das in der Tastatur integrierte Kartenterminal.

Handbuch für Administratoren

Ein ausführliches **Handbuch für Administratoren** (Artikel-Nr. 6440650-01) finden Sie unter <https://www.cherry.de>.

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 den Kartenterminals steht Ihnen unter <https://www.cherry.de> folgende Software inkl. 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.

SICHERHEITS- FUNKTIONEN

Damit ein sicherer Betrieb gewährleistet ist, verfügen die Geräte über folgende Sicherheitsfunktionen:

1 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 16.1 "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 16 "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.

2 Firmware auf Manipulation prüfen

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

- 1 Drücken Sie für 3 Sekunden die Taste unter dem Symbol  auf dem Display. Sie befinden sich nun im Menü-Modus. Bei aktivem Menü-Modus werden Tastatureingaben nicht mehr an den Rechner geleitet.
- 2 Wählen Sie im Menü **Eigendiagnose** den Punkt **Codeprüfung**.



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

- Führen Sie durch Ab- und Anstecken der Tastatur einen Neustart des Kartenterminals durch. Wird die Meldung weiterhin angezeigt, kann und darf es nicht weiter verwendet werden
- Wenden Sie sich zur Prüfung an Ihren Administrator.

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

3 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.
- 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 10 "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

INBETRIEBNAHME

4 Tastatur in Betrieb nehmen

Das integrierte eHealth-Kartenterminal kann ausschließlich in Verbindung mit einem Konnektor in einem Netzwerk betrieben werden. Dazu ist auch die Installation der CHERRY Software **eHealth USB-LAN Proxy** auf dem angeschlossenen Rechner (Host-PC) erforderlich (aktuelle Version unter <https://www.cherry.de>).

Diese Anleitung bezieht sich nicht auf die erstmalige Installation des Kartenterminals, sondern nur auf Situationen, in denen die Tastatur vom PC gelöst wurde (z. B. zur Reinigung oder beim Transport).

Kontaktieren Sie zur Erstinbetriebnahme Ihren Administrator. Er benötigt dafür das Handbuch für Administratoren, herunterzuladen unter <https://www.cherry.de>.

Die Tastaturfunktion ist erst nach dieser Erstinbetriebnahme betriebsbereit (Festlegung von Administrator-Kennwort und PUK des Kartenterminals).



ACHTUNG: Manipulation am Gerät

Das Gerät könnte auf dem Lieferweg manipuliert worden sein.

- Veranlassen Sie Ihren Administrator zu prüfen, ob das Gerät über einen sicheren Lieferweg zu Ihnen ausgeliefert wurde. Er benötigt dazu die Informationen auf der letzten Seite dieser Anleitung.



ACHTUNG: Inbetriebnahme nur durch einen Administrator

Die Inbetriebnahme darf aufgrund der Zulassungsbedingungen ausschließlich durch einen Administrator erfolgen.

- Es handelt sich dabei um eine besonders qualifizierte Person mit erweiterten Benutzerrechten.
- Der Administrator ist für Inbetriebnahme, Konfiguration und den sicheren Betrieb des Geräts verantwortlich.
- Bei Inbetriebnahme durch andere Personen erlischt die Zulassung!

Vorgehensweise zur Wiederinbetriebnahme (nicht: Erstinstallation!):

- 1 Beachten Sie die Hinweise zur Einsatzumgebung (siehe 5 "Einsatzumgebung").
- 2 Überzeugen Sie sich von der Unversehrtheit des Geräts. Überprüfen Sie insbesondere das Gehäuse, die Anschlusskabel und die Siegel gemäß der Beschreibung (siehe 7 "Versiegelung prüfen"). Wenden Sie sich bei Verdacht auf Manipulationen an Ihren Administrator.
- 3 Schließen Sie das Gerät an (siehe 9 "Tastatur anschließen").

5 Einsatzumgebung

Der Einsatz in Praxen, Apotheken und in Krankenhäusern 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 ausgeschlossen 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 Administrator.

6 Typenschild prüfen

Der Typenschild-Aufkleber befindet sich auf der Unterseite des Geräts. Dies ist der einzige Aufkleber, der auf dem Gerät angebracht 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 Rückseite 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 Administrator.

7 Versiegelung prüfen



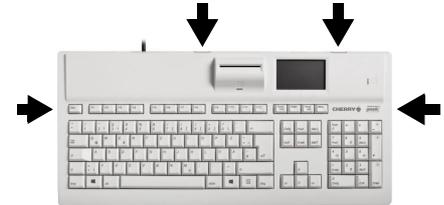
ACHTUNG: Manipulation am Gerät

Bei verletztem, getauschtem oder fehlendem Siegel(n) ist der Betrieb des Kartenterminals nicht mehr sicher.

- Prüfen Sie vor jedem Neustart des Terminals, ob ein Siegel verletzt oder ausgetauscht wurde.
- Prüfen Sie auch die Slotsiegel (gSMC-KT und ggf. der SMC-B Karte), siehe 7.2 "Slotsiegel für gSMC-KT und ggf. SMC-B Karte prüfen".
- Kontaktieren Sie bei zerstörtem oder nicht vorhandenem Siegel Ihren Administrator.

7.1 Gehäuseversiegelung prüfen

Zum Schutz vor Manipulation befinden sich an der Rückseite 2 und an den Seiten des Geräts je 1 Siegel. Die 4 Siegel sind auf der Gehäusenaht zwischen Ober- und Unterteil angebracht:



Der Bundesadler und die Buchstaben BSI wechseln je nach Blickwinkel ihre Farbe von Bronze über Grün nach Ocker.

Unbeschädigtes Siegel



Siegel nach Ablöseversuch

Das Siegel wurde manipuliert, wenn sich die graue Grundfarbe partiell in einen helleren Grauton aufspaltet:



- 1 Notieren Sie sich zur Identifizierung der Siegel deren Seriennummern, um einen Geräte- oder Siegelaustausch feststellen zu können.
- 2 Prüfen Sie vor jedem Neustart des Terminals, ob die Siegel verletzt oder ausgetauscht wurden.
- 3 Prüfen Sie auch die Slotsiegel (gSMC-KT und ggf. der SMC-B Karte), siehe 7.2 "Slotsiegel für gSMC-KT und ggf. SMC-B Karte prüfen".
- 4 Kontaktieren Sie bei zerstörtem oder nicht vorhandenem Siegel Ihren Administrator.

Weitere Informationen zum Siegel, sowie weitere Hinweise zum sicheren Einsatz des Terminals, finden Sie im Handbuch für Administratoren.

7.2 Slotsiegel für gSMC-KT und ggf. SMC-B Karte prüfen

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.

Die SMC-B Karte ist eine Security Module Card - Typ B für das Kartenterminal, die zur Authentifikation einer berechtigten Institution im Gesundheitswesen dient.

Die gSMC-KT Karte wird durch den Administrator eingesetzt und der Schlitz des Kartenlesers versiegelt (kleiner Leser auf der Rückseite der Tastatur über dem Display rechts), siehe 12 "Einstecken der Karten".

- 1 Notieren Sie sich zur Identifizierung der Siegel deren Seriennummer.
- 2 Prüfen Sie vor jedem Neustart des Terminals, 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.

8 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.

9 Tastatur anschließen

- 1 Stellen Sie sicher, dass die CHERRY Software **eHealth USB-LAN Proxy** (V 4.0.0.0 oder höher) durch den Administrator installiert wurde und der entsprechende Systemdienst aktiv ist (lt. Anleitung zur Software).
- 2 Stellen Sie sicher, dass Ihr PC mit Ihrem Netzwerk verbunden ist und nicht in den Sleep-Modus fährt.
- 3 Stecken Sie die Tastatur direkt am USB-Anschluss des PCs an, verwenden Sie keinen USB-Hub.

10 Administrator-Kennwort

Fordert Sie das Kartenterminal zur Eingabe eines Administrator-Kennworts auf, wurde es noch nicht initial in Betrieb genommen und konfiguriert. Kontaktieren Sie zur Erstinbetriebnahme Ihren Administrator.



ACHTUNG: Erstinbetriebnahme und Festlegung des Administratorkennworts

Das Festlegen des Administrator-Kennworts darf ausschließlich durch den Administrator erfolgen.

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

11 Reset-Administrator-PUK

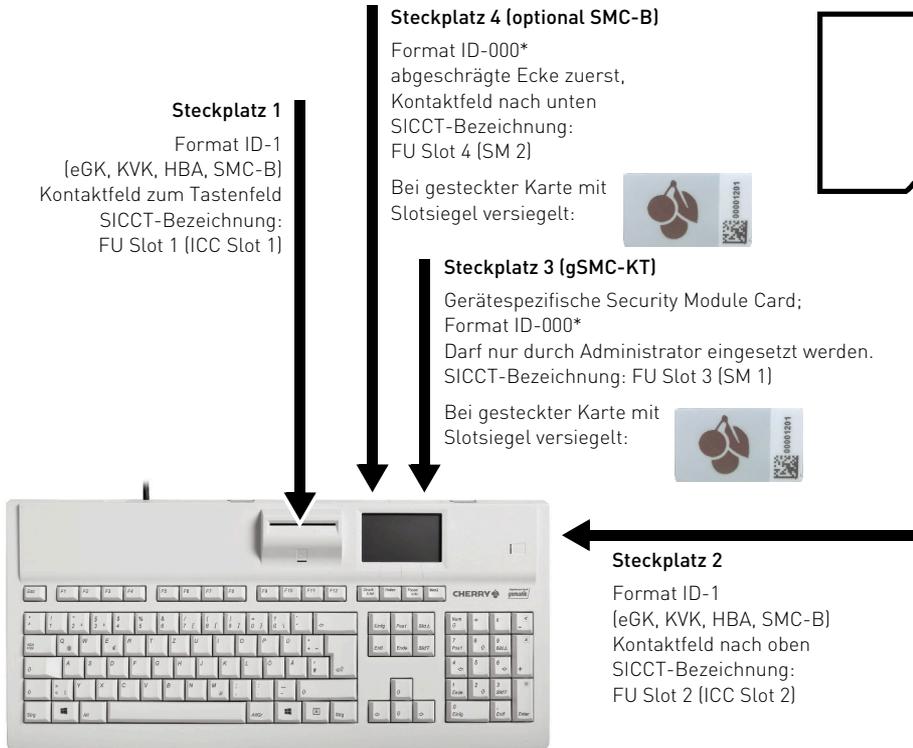
Der PUK ist das Kennwort des Reset-Administrators und dient bei Verlust des Administrator-Kennworts dazu, das Kartenterminal auf Werkseinstellungen zurückzusetzen.

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. Dies sollte nur durch den (Reset-) Administrator erfolgen.

BEDIENUNG

12 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).

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.
- Sie darf nur durch den Administrator eingesetzt werden. Der Slot muss versiegelt sein.

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

- Diese Kontaktiereinheit kann für die SMC-B Karte verwendet werden.
- Sie darf nur durch den Administrator eingesetzt werden. Falls dies geschehen ist, muss der Slot versiegelt sein.
- Bei freiem Slot und Verwendung anderer Karten, stecken Sie diese mit der abgeschrägten Ecke zuerst (Kontaktfeld nach unten) in die Kontaktiereinheit, bis sie einrastet. Erneutes Drücken entriegelt die Karte zum Entnehmen.

13 Navigation

13.1 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

- 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.
- 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.

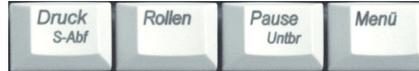
SICCT-Modus

- 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.

13.2 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.

13.3 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		

14 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

15 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)
	gSMC-KT Karte erkannt und aktiviert (mit Strom versorgt)

Symbol	Status
	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.

16 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:

- Bei der Durchführung einer elektronischen Signatur dürfen Sie nur die sichere PIN-Eingabe verwenden.
- 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.

16.1 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 .

- 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.
- Bestätigen Sie die eingegebene PIN mit der Taste mit dem Symbol  auf dem Nummernblock.

Die sichere PIN-Eingabe wird durch Entnahme der Karte, Ablauf der Eingabezeit oder Betätigung der Taste mit dem Symbol  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]".*

16.2 PIN-Eingabe über den Nummernblock

- Lehnen Sie ab, dass Sie die sichere PIN-Eingabe verwenden möchten.
- Geben Sie die PIN über den Nummernblock des Tastenfeldes ein.
Für jede eingegebene Stelle der PIN wird ein Sternchen (*) angezeigt.
- Bestätigen Sie die eingegebene PIN mit der Taste mit dem Symbol  auf dem Nummernblock.

Die PIN-Eingabe wird durch Entnahme der Karte, Ablauf der Eingabezeit oder Betätigung der Taste mit dem Symbol  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]".*

16.3 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.

KONFIGURATION

17 Terminal-Menü

- 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.

Die Navigation ist selbsterklärend. Weitere Informationen finden Sie unter 13 "Navigation".

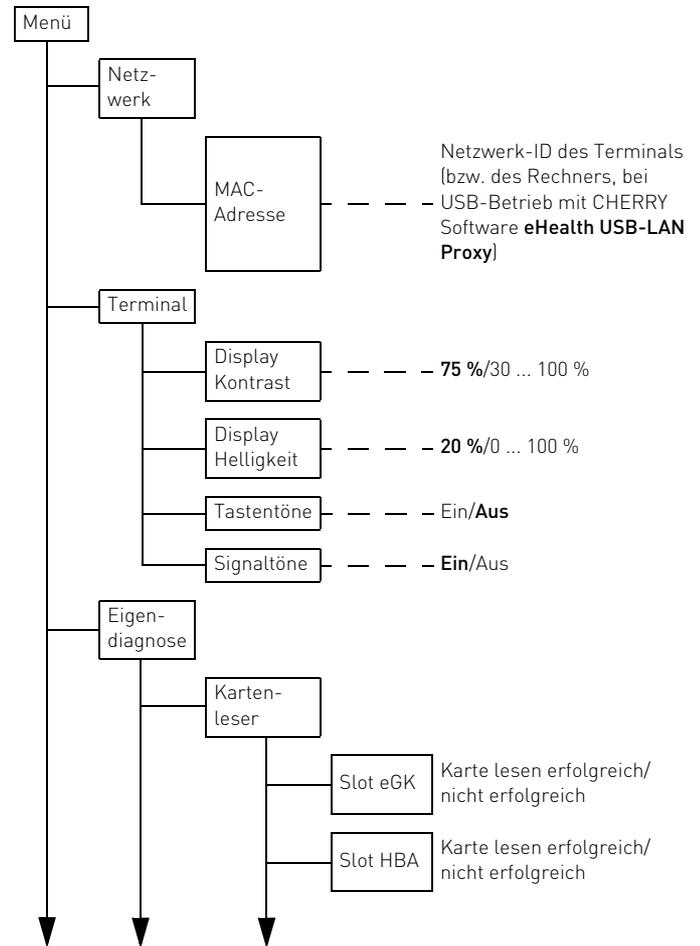


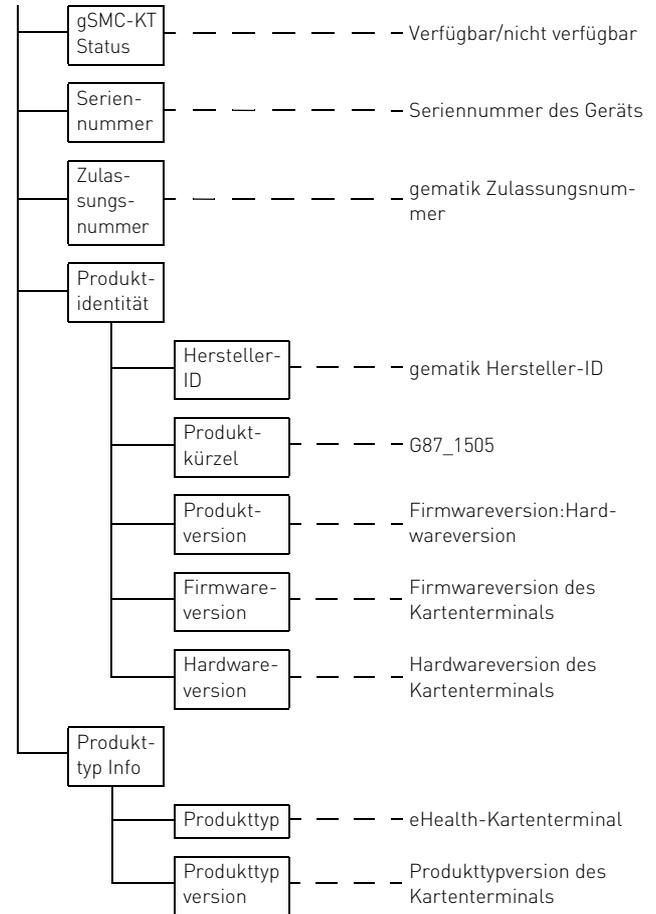
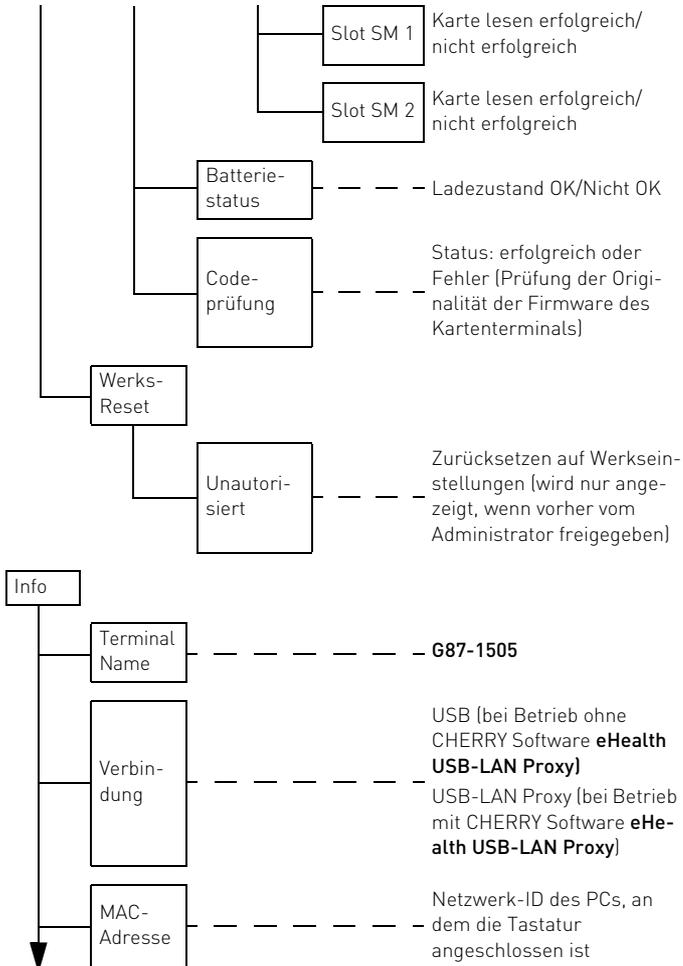
HINWEIS: Ausgeblendete Symbole "Menü" und "Info"

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.

Fett = Werkseinstellungen

Benutzer können folgende Informationen abrufen und Einstellungen vornehmen:





18 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.

- 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 zur fachkundigen Überprüfung des Geräts an Ihren Administrator.

AUSSER-BETRIEBNAHME



ACHTUNG: Weitergabe von Pairing-Informationen

- Stellen Sie sicher, dass bei einer Außerbetriebnahme der **G87-1505** alle Pairing-Informationen gelöscht werden. Kontaktieren Sie dazu Ihren Administrator.

19 Reparatur

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

20 Batterie

Das Gerät enthält eine fest eingebaute Lithium-Mangandioxid Batterie (Li-MnO₂/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 Administrator.

21 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.

ALLGEMEINES

22 Fehlermeldungen

Meldung	Bedeutung
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 Administrator.
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 Administrator.
Gehäuseüberwachung	Der Sicherheitsmechanismus wurde aktiviert. Mögliche Ursachen: Manipulation oder Öffnen des Gehäuses, Transport- oder Fallschaden, Gerätedefekt, Batterie entladen. Wenden Sie sich an Ihren Administrator.

Meldung	Bedeutung
gSMC-KT-Fehler	Es trat ein Fehler beim Lesen der gSMC-KT Karte auf.
Zum Neustarten Menü-Taste 5 Sek. lang drücken	Halten Sie die Menü-Taste gedrückt, bis zum Neustart des Terminals. Im wiederholten Fehlerfall wenden Sie sich an Ihren Administrator.
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 Administrator.
Ungültige Zeichen	Die Eingabe enthält keine oder ungültige Zeichen. Zulässig sind: A - Z, a - z, Leerzeichen, Komma, Punkt, Minus und 0 - 9.
Verbindungsfehler	Es trat ein Fehler in der (SICCT-) Verbindung zum Terminal auf.
Zum Neustarten Menü-Taste 5 Sek. lang drücken	Halten Sie die Menü-Taste gedrückt, bis zum Neustart des Terminals. Im wiederholten Fehlerfall wenden Sie sich an Ihren Administrator.

Meldung	Bedeutung
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.

23 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.

24 Reinigen der Tastatur



ACHTUNG: Beschädigung durch aggressive Reinigungsmittel oder Flüssigkeit in der Tastatur

- 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 die Tastatur gelangt.
- Entfernen Sie nicht die Tastkappen der Tastatur.

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

25 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.

26 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

27 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.

28 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.

29 Technische Daten

Bezeichnung	Wert
Systemvoraussetzungen	Für das Kartenterminal: 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)
Display	Graphisches Display (128 x 64 Pixel)
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
Karten-schnittstellen	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
Übertragungsgeschwindigkeit	Zur Karte: 820 kBit/s, zum System: bis 12 MBit/s

Bezeichnung	Wert
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

30 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
eGK	E lektronische G esundheits k arte

Abkürzung/ Begriff	Bedeutung
eHealth	Elektronisches Gesundheitswesen
eHealth-Terminal	Kartenlesegerät auf Basis SICCT zur Verwendung im deutschen Gesundheitswesen
FU-Name	F unctional U nit Name
gematik	Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (www.gematik.de)
gSMC-KT	G erätespezifische S ecurity M odule C ard für das K artenterminal
Heilberufsausweis (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 nformationssystem
KVK	K ranken v ersicherten k arte
LAN	L ocal A rea N etwork (lokales Netzwerk)

Abkürzung/ Begriff	Bedeutung
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
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

31 Lieferweg prüfen

Überprüfen Sie die sichere Auslieferung, indem Sie den Lieferweg über unsere Homepage nachverfolgen: <https://www.cherry.de/eHealth>.

Hinterlassen Sie uns einen Kommentar

#cherrykeyboards



social.cherry.de/fbm



social.cherry.de/youtube



social.cherry.de/twitter



social.cherry.de/insta



blog.cherry.de
