eHealth Terminal ST-1506

Kurzanleitung für Benutzer

64410078-05, DE, © Mar 2023 (ST-1506)

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.

Das **eHealth Terminal ST-1506** wurde für die Verwendung in der Telematikinfrastruktur (TI) entwickelt. Es zeichnet sich besonders durch folgende Eigenschaften aus:

- gematik zugelassen
- Gute Lesbarkeit und intuitive Bedienung durch hochauflösendes Farbdisplay
- Leicht desinfizierbare Glasoberfläche für optimale Hygiene
- Praktischer Betrieb des Terminals ohne Netzteil via Power over Ethernet (PoE)
- Vorbereitet für künftige Anwendungen durch Kontaktlos-/NFC-Schnittstelle

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/eHealth**.

Wir wünschen Ihnen viel Vergnügen mit Ihrem **ST-1506**.

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.

Für neuere Firmwareversionen kann der Inhalt abweichen. Die aktuellste Version der Kurzanleitung finden Sie unter **https://www.cherry.de/ehealth/downloads/st-1506**.

Sofern nicht anders angegeben, beziehen sich die Begriffe "Terminal" bzw. "Kartenterminal" immer auf das **eHealth Terminal ST-1506**.

Handbuch für Administratoren

Ein ausführliches **Handbuch für Administratoren** (Artikel-Nr. 64410079) finden Sie unter **https://www.cherry.de/eHealth/downloads/st-1506**.

Lieferumfang

Der Lieferumfang des eHealth Terminals **ST-1506** enthält:

- Terminal ST-1506
- Netzteil (24 V, 0,5 A)
- Netzwerkkabel
- USB-Kabel
- 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**)

SICHERHEIT

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

1 Sichere PIN-Eingabe

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 14 "Sicherer 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.
- 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.

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

HINWEIS: Verdacht auf Manipulation, falls am Ende der Eigendiagnose "Fehlerhafter Code" erscheint

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

3 Benutzerprofile und Authentisierung

Folgende Benutzerprofile sind implementiert:

- "Benutzer"
- "Administrator"
- "Reset-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:
  - Anzeige- und Akustikeinstellungen vornehmen
  - Eigendiagnosefunktionen ausführen
  - Aktuelle Terminal-Konfiguration anzeigen (Verbindungsstatus, Firmwareversion, Hardware Version, Firmware Gruppe, Hersteller-ID, Produktkürzel, Produktversion, Produkttyp, Produkttypversion, Gerätename, Seriennummer, MAC Adresse)

"Administrator"
Durch Eingabe der PIN kann im Hauptmenü das Admin-Menü aufgerufen werden. Die Freigabe bleibt erhalten, bis das Menü wieder verlassen wird (manuell oder automatisch nach 5 Minuten).

- Der Administrator überprüft vor der ersten Inbetriebnahme die Integrität des Terminals.
- Bei der ersten Inbetriebnahme des Terminals muss der Administrator eine persönliche PIN festlegen (siehe 9 "Administrator-PIN").
- 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
- Trust-Service Status Liste (TSL) für Konnektoren aktualisieren

"Reset-Administrator"
Mit diesem Benutzerprofil kann das Kartenterminal wieder in den Auslieferungszustand zurückversetzt werden (Werksreset). Hierfür wird der Support von CHERRY benötigt (siehe "Handbuch für Administratoren").

INBETRIEBNAHME

Das eHealth-Kartenterminal kann ausschließlich in Verbindung mit einem Konnektor in einem Netzwerk betrieben werden.

Diese Anleitung bezieht sich nicht auf die erstmalige Installation des Kartenterminals.

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

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.

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 4 "Einsatzumgebung").

2 Überzeugen Sie sich von der Unversehrtheit des Geräts. Überprüfen Sie insbesondere das Gehäuse, die Anschlusskabel und die Siegel gemäß der Beschreibung (siehe 6 "Versiegelung prüfen"). Wenden Sie sich bei Verdacht auf Manipulationen an Ihren Administrator.

3 Schließen Sie das Gerät an (siehe 8 "Terminal anschließen").

4 Einsatzumgebung

Das **ST-1506** ist für den stationären Einsatz in einer kontrollierten Umgebung konzipiert. Es ist zur Anbindung an die Telematikinfrastruktur 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 das Terminal gerichtet sind
- Bei Verdacht auf Manipulationen am Gerät wenden Sie sich an Ihren Administrator.

5 Typenschild prüfen

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

HINWEIS: 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 Administrator.

6 Versiegelung prüfen

HINWEIS: Verdacht auf Manipulation

Bei verletztem, getauschtem oder fehlendem Siegel 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 6.4 "Slotsiegel für gSMC-KT und ggf. SMC-B Karte prüfen".
- Kontaktieren Sie bei zerstörtem oder nicht vorhandenem Siegel Ihren Administrator.

6.1 Gehäuseversiegelung prüfen

Zusätzlich zum aktiven physikalischen Manipulationsschutz verfügt das Terminal über Gehäusesiegel, an denen ein Öffnen des Gehäuses erkannt werden kann.

1 Notieren Sie sich zur Identifizierung der Siegel deren Seriennummern, um einen Geräte- oder Siegelaustausch feststellen zu können.

2 Prüfen Sie vor jedem Neustart, ob die Siegel verletzt oder ausgetauscht wurden.

3 Prüfen Sie auch die Slotsiegel (gSMC-KT und ggf. der SMC-B Karte), siehe 6.4 "Slotsiegel für gSMC-KT und ggf. SMC-B Karte prüfen".

6.2 Positionen der Gehäusesiegel

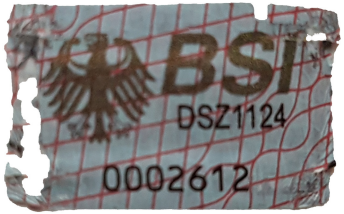
6.3 Beschreibung des Gehäusesiegels

Unbeschädigtes Siegel

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

Siegel nach Ablöseversuch

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



6.4 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 linken Seite des Terminals), siehe 10 "Karten einstecken".

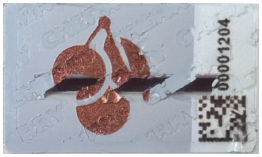
1 Notieren Sie sich zur Identifizierung der Siegel deren Seriennummer.

2 Prüfen Sie vor jedem Neustart des Terminals, ob die Siegel verletzt oder ausgetauscht wurden.

Position Slotsiegel

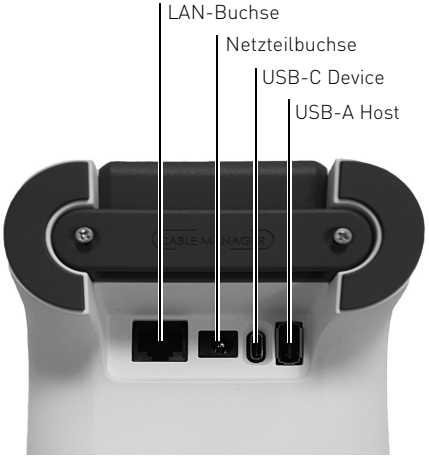
Unbeschädigtes Slotsiegel

Slotsiegel nach Ablöseversuch



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

7 Anschlüsse



LAN-Buchse

- Verbinden Sie das Terminal mit einem Netzwerkkabel mit Ihrem Netzwerk. Die LAN-Buchse unterstützt Power over Ethernet (PoE).

Netzteilbuchse

- Stecken Sie ausschließlich das mitgelieferte Netzteil mit 24 V und 0,5 A an der Netzteilbuchse an, um die Stromversorgung des Terminals zu gewährleisten.

USB-C Device

- Über diese Schnittstelle kann das Terminal mit einem Host-PC verbunden werden.

- Diese Verbindung ist optional und kann verwendet werden, wenn keine Netzwerkdose zur Verfügung steht.

USB-A Host

- An dieser Schnittstelle kann das CHERRY PIN-Pad PP - 1516 betrieben werden.

Verwenden Sie nur von CHERRY freigegebenes Zubehör.

8 Terminal anschließen

8.1 Terminal mit Strom versorgen

Je nach Anschlussart kann das Terminal über 3 Wege mit Strom versorgt werden. Diese 3 Wege sind aufsteigend priorisiert: Wenn ein Weg mit höherer Priorität angeschlossen wird, wird automatisch ein Neustart des Terminals ausgelöst und die Stromversorgung über die höhere Priorität verwendet.

TIPP: Mangelnde Stromversorgung aufgrund falscher Anschlussreihenfolge

Wenn Sie von einer höheren Priorität auf eine niedrigere wechseln und nur das höher priorisierte Kabel entfernen, kann ein fehlerfreier Betrieb des Terminals nicht gewährleistet werden.

- Entfernen Sie alle Kabel und schließen Sie sie von unten nach oben an (erst USB, dann PoE).

Priorität 1: 24 Volt-Netzteil

- Die Stromversorgung mit der höchsten Priorität geschieht über das Netzteil. Verwenden Sie ausschließlich das mitgelieferte Netzteil mit 24 V und 0,5 A.

Priorität 2: Power over Ethernet (PoE)

- Die im Terminal befindliche LAN-Buchse ist PoE-fähig. Sollte die Infrastruktur vorhanden sein, kann das Terminal über die LAN-Buchse mit Strom versorgt werden.

Priorität 3: USB

- Wird das USB-Kabel für den Betrieb des Terminals verwendet, so kann das Terminal auch über USB mit Strom versorgt werden.

HINWEIS: Überlastung des USB-Anschlusses

Bei Verwendung des mitgelieferten USB-Kabels kann der USB-A Anschluss des PCs durch den Betrieb des Terminals überlastet und beschädigt werden.

- Nutzen Sie möglichst einen USB-C Anschluss an Ihrem PC. Hierfür ist ein separates aktives USB-C Kabel nötig (nicht im Lieferumfang enthalten).

Falls Sie das Terminal nur an einem USB 2.0 Anschluss betreiben können:

- Vergewissern Sie sich, dass am USB-Anschluss des PCs mindestens 1000 mA zur Verfügung stehen.
- Falls dies nicht der Fall ist, verwenden Sie das im Lieferumfang enthaltene Netzteil.

8.2 Terminal ein- und ausschalten

Das Terminal besitzt keinen Schalter. Wenn eine gSMC-KT Karte installiert ist und es mit Strom versorgt wird, ist es automatisch eingeschaltet. Um das Terminal auszuschalten, trennen Sie es von der Stromversorgung.

8.3 Terminal direkt mit dem Netzwerk verbinden

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

- Verbinden Sie das Terminal mit einer Netzwerkdose.

8.4 Terminal über den PC mit dem Netzwerk verbinden

Sollten Sie keine freie Netzwerkdose zur Verfügung haben, so kann das Terminal auch optional über einen PC betrieben werden. Hierbei nutzt das Terminal die Netzwerkschnittstelle des PCs. Schließen Sie hierfür das Terminal über das mitgelieferte USB-Kabel an dem PC an.

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

2 Stecken Sie das Termial direkt am USB-Anschluss des PCs an, verwenden Sie keinen USB-Hub.

  Das Terminal meldet sich am PC als USB-Netzwerkadapter an. Es werden die beiden USB-Protokolle **RNDIS** und **CDC-ECM** unterstützt.

3 Erstellen Sie anhand der folgenden Schritte eine Netzwerkbrücke zwischen dem USB-Netzwerkadapter des Terminals und dem Netzwerkadapter des PCs, der mit dem Netzwerk verbunden ist:
   - Öffnen Sie in der **Windows Systemsteuerung** das **Netzwerk und Freigabecenter > Adaptereinstellungen**.
   - Markieren Sie den Netzwerkadapter des PC-Systems und den Netzwerkadapter (RNDIS oder CDC-ECM) des Terminals.
   - Klicken Sie mit der rechten Maustaste auf den Netzwerkadapter (RNDIS oder CDC-ECM) des Terminals.
     Das Kontextmenü öffnet sich
   - Wählen Sie **Verbindung überbrücken**.
   - Warten Sie kurz, bis die Netzwerkbrücke von Windows eingerichtet und das Netzwerk identifiziert wurde.
4 Wenn die Netzwerkbrücke erstellt ist, kann das Terminal im selben Netzwerk des PCs als eigenständiges Netzwerkgerät betrieben werden. Dem Terminal kann eine eigene IP-Adresse zugewiesen werden.
5 Für Informationen zum Anschluss des Terminals unter weiteren Betriebssystemen, besuchen Sie unsere Homepage:
https://www.cherry.de/eHealth

9 Administrator-PIN

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 der Administrator-PIN

Das Festlegen der Administrator-PIN darf ausschließlich durch den Administrator erfolgen.

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

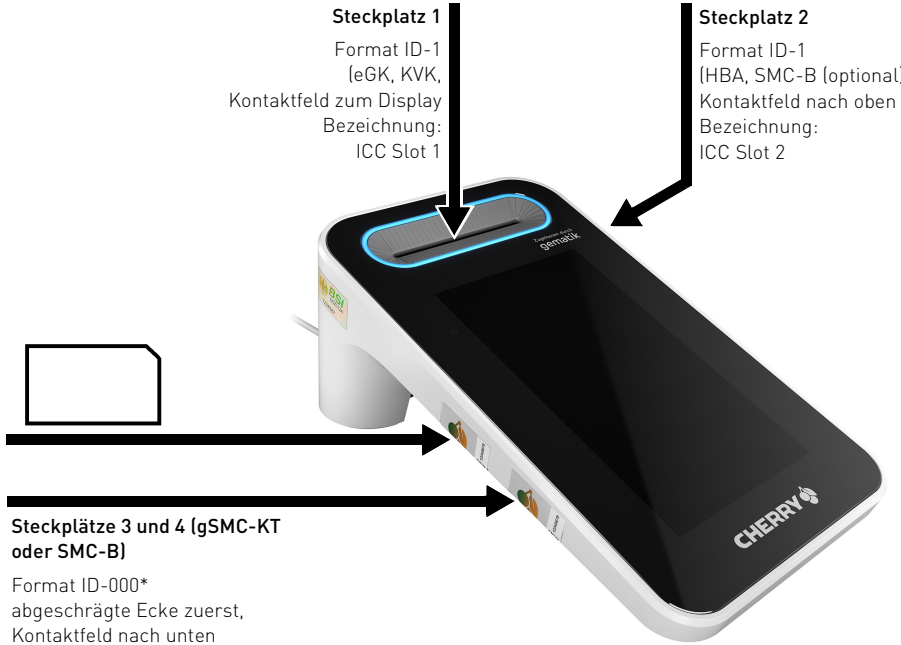
BEDIENUNG

10 Karten einstecken

Nur die gSMC-KT Karte muss in einen der beiden ID-000 Slots 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.

HINWEIS: Manipulation am Gerät

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



Bei gesteckter Karte mit Slotsiegel versiegelt:

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

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

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

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

Steckplätze 3 und 4 für Format ID-000 Karten (gSMC-KT oder SMC-B)

- Diese Kontaktiereinheiten sind für die gSMC-KT- oder die SMC-B-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 sein, siehe 6.4 "Slotsiegel für gSMC-KT und ggf. SMC-B Karte prüfen".
- Entfernen Sie die Karte nur im stromlosen Zustand des Terminals.

11 Navigation

11.1 Betriebsarten

Das Terminal stellt 3 verschiedene Betriebsarten zur Verfügung.

Menü-Modus

1 Um in den Menü-Modus zu kommen, drücken Sie den entsprechenden Button auf dem Display.
2 Um den Menü-Modus zu verlassen, drücken Sie den Zurück-Button auf dem Display.

Sicherer PIN-Eingabe-Modus

- Dieser Modus wird aktiviert, wenn eine PIN-Eingabe angefordert wird.

SICCT-Modus

- Dieser Modus wird aktiviert, wenn für die Bearbeitung eines empfangenen SICCT-Befehls eine Nutzereingabe benötigt wird.

12 Statusanzeige LEDs

LED	Status
LED oben links am Display leuchtet rot	Sichere PIN-Eingabe aktiv.
Ring um senkrechten Kartensteckplatz leuchtet	Karte aktiv (mit Strom versorgt)
Ring um senkrechten Kartensteckplatz blinkt	Bitte Karte stecken

13 Displaysymbole

Symbole für Kartensteckplätze

Die Symbole und Statusfarben gelten für alle Steckplätze. Die Ziffer und die entsprechende Position auf dem Display bezeichnen den Steckplatz.

Symbol	Farbe: Status
	Grau: Inaktiv, keine Karte gesteckt
	Blau: Karte gesteckt
	Grün: Karte aktiviert
	Grün und blinkend: Auf Karte wird aktuell zugegriffen
	Rot: Sichere PIN Eingabe für aktuelle Karte

Symbole für Kommunikationsverbindung über Netzwerk

Symbol	Farbe: Status
	Grau: Inaktiv, keine Verbindung
	Blau: Aktive Verbindung vorhanden
	Grün: Sichere Verbindung zum Konnektor

Symbole für Kommunikationsverbindung über USB

Symbol	Farbe: Status
	Grau: Inaktiv, keine Verbindung
	Blau: Aktive Verbindung vorhanden
	Grün: Sichere Verbindung zum Konnektor

Symbole für Kommunikationsverbindung über VPN

Symbol	Farbe: Status
VPN	Grau: Inaktiv, keine Verbindung
VPN	Blau: Aktive Verbindung vorhanden
VPN	Grün: Sichere Verbindung zum Konnektor

Symbole für Kommunikationsverbindung mit CHERRY PIN-Pad PP-1516

Symbol	Farbe: Status
	Grau: Inaktiv, kein PIN-Pad angeschlossen
	Blau: Aktive Verbindung vorhanden
	Grün: Sichere Verbindung zum PIN-Pad

14 Sicherer PIN-Eingabe-Modus

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

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

Im sicheren PIN-Eingabe-Modus wird das Kartensymbol in der obersten Displayzeile rot eingefärbt. Anhand des roten Kartensymbols des entsprechenden Kartensteckplatzes ist erkennbar, für welche Karte die PIN-Eingabe angefordert wird.

Für die PIN-Eingabe gibt es zwei Sicherheitsstufen, zwischen denen im Menü gewechselt werden kann. Im Auslieferungszustand oder nach einem Werksreset befindet sich das Terminal in der höchsten Sicherheitsstufe. In dieser Stufe wird das Tastenfeld verwürfelt. Das heißt, zu Beginn einer PIN-Eingabe wird die Position der Zahlen auf dem Tastenfeld zufällig angeordnet, welches eine zusätzliche Schutzmaßnahme darstellt. Ist die höchste Sicherheitsstufe aktiv, wird dies durch eine rote LED oben links neben dem Display angezeigt.

Wird die Sicherheitsstufe gewechselt, dann wird das Tastenfeld der PIN-Eingabe nicht verwürfelt und die rote LED ist nicht aktiv.

Die sichere PIN-Eingabe wird durch Entnahme der Karte, Ablauf der Eingabezeit oder Betätigung der Abbruchtaste abgebrochen.

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 sichere PIN-Eingabe-Modus aktiv ist und eine sichere Verbindung zum Konnektor besteht (grünes Netzwerk- oder USB-Symbol wird angezeigt).
- In Ihrer Anwendung muss dabei erkennbar eine PIN angefordert worden sein.

HINWEIS: Sicherer zertifizierter Betriebszustand

- Nur in der höchsten Sicherheitsstufe mit aktivierter roter LED befindet sich das Gerät im sicheren zertifizierten Betriebszustand.

14.1 Remote-PIN-Konnektor

Der Konnektor stellt ein Remote-PIN-Verfahren zur Verfügung. Hierbei wird die am Terminal eingegebene Karten-PIN mithilfe der gesteckten gSMC-KT Karte verschlüsselt und an eine Karte in einem anderen Terminal des eigenen Netzwerks übertragen. Die beiden verwendeten Terminals müssen im Konnektor entsprechend konfiguriert werden.

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

15 Eigendiagnose

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

- Buzzer
- Kartenslots
- Integrität
- Batteriestatus

Siehe 16 "Mögliche Einstellungen im Menü".

Wenn Sie die Firmwaregruppenliste (**Einstellungen > Status > Firmware Gruppe**) aufrufen, erfolgt vor der Anzeige eine automatische Integritätsprüfung der Daten.

KONFIGURATION

16 Mögliche Einstellungen im Menü

- Um in das Hauptmenü zu gelangen, drücken Sie auf die Taste **Menü**.

Fett = Werkseinstellungen

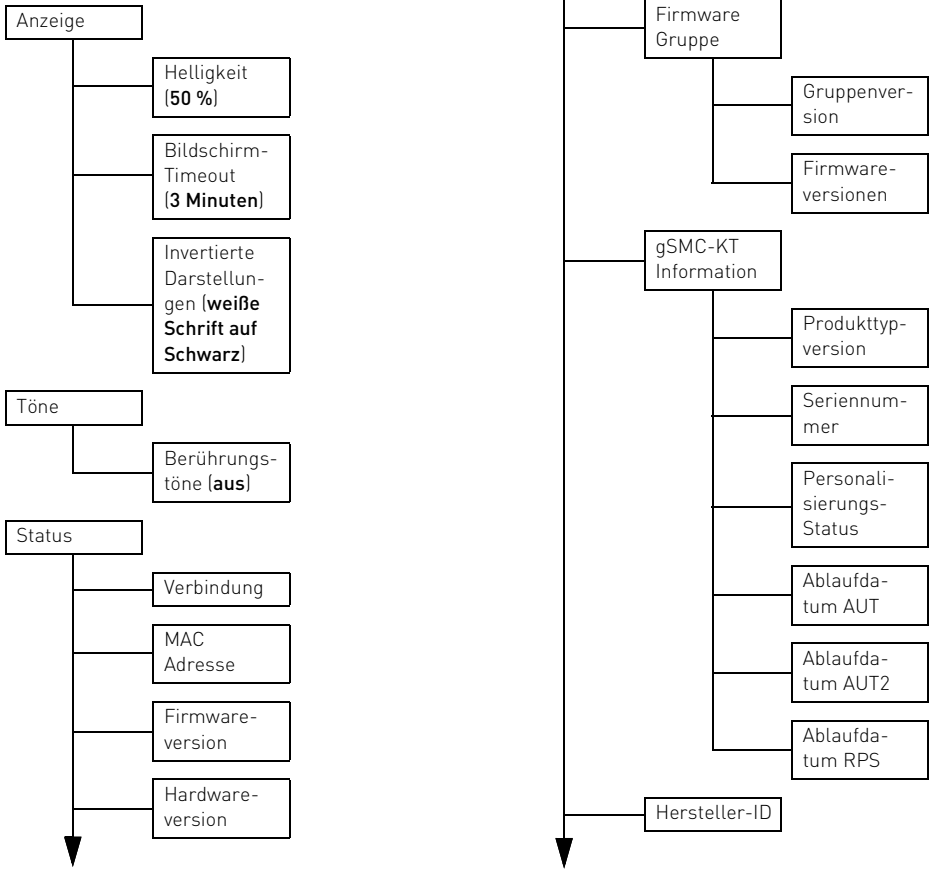
Sie können die auf den folgenden Seiten dargestellten Einstellungen vornehmen:

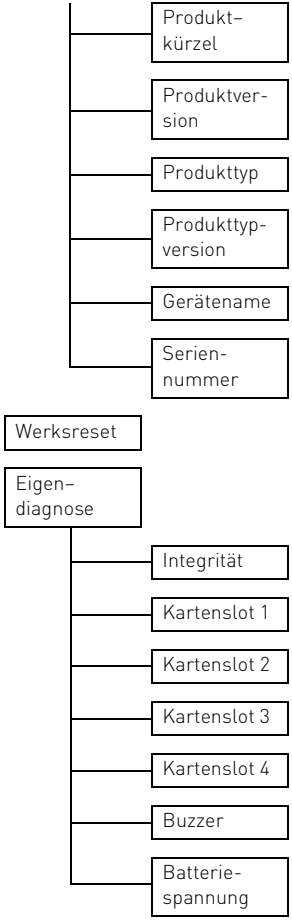
Einstellungen

Gerät neu starten

Das Admin-Menü ist nur für Administratoren zugänglich.

16.1 Menü "Einstellungen" (Benutzer)





AUSSER-BETRIEBNAHME

HINWEIS: Weitergabe von Pairing-Informationen

- Stellen Sie sicher, dass bei einer Außerbetriebnahme des Terminals alle Pairing-Informationen gelöscht werden. Kontaktieren Sie dazu Ihren Administrator.

17 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.

18 Batterie

Das Gerät enthält eine fest eingebaute Batterie mit einer durchschnittlichen Kapazität von 220 mAh.

Im Fall einer entladenen Batterie während der Nutzungsphase des Geräts wird der Manipulationsschutz aktiviert und Sie erhalten die Fehlermeldung "System angehalten", zusätzlich wird die Information "Manipulationsschutz ausgelöst! Code: xx" angezeigt. Wenden Sie sich an Ihren Administrator.

19 Geräte entsorgen

- Entsorgen Sie Geräte mit diesem Symbol nicht mit dem Hausmüll.
- Entsorgen Sie die Geräte, entsprechend den gesetzlichen Vorschriften, bei Ihrem Händler oder den kommunalen Sammelstellen.

ALLGEMEINES

20 Terminal reinigen

Schmierstreifen sehen Sie am besten auf dem ausgeschalteten Display.

1 Verwenden Sie zur Reinigung des Touchscreens ein fusselfreies Tuch. Mikrofasertücher und Reinigungstücher für Brillengläser haben sich bewährt.

2 Bei normaler Verschmutzung genügt es, wenn Sie mit leicht kreisenden Bewegungen und ohne Druck über den Touchscreen streichen.

3 Wenn Sie mit ein wenig Flüssigkeit nachhelfen möchten, genügt es, das Tuch mit sauberem Wasser leicht zu befeuchten. Außerdem gibt es spezielle Reinigungstücher und Bildschirmreiniger für Touchscreens.

HINWEIS: Beschädigung des Touchscreens durch Druck, aggressive Reinigungsmittel oder Flüssigkeit im Gerät

- Üben Sie keinen Druck auf die Glasoberfläche des Touchscreens aus.
- 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.

21 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
- Verwendeter Konnektor (Hersteller Version)

Cherry Digital Health GmbH
Einsteinstraße 174
81677 München

Internet: https://www.cherry.de

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

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

22 Technische Daten

Bezeichnung	Wert
Systemvoraussetzungen	USB Anschluss oder RJ45 Anschluss, gSMC-KT, Konnektor
Display	Graphisches Display (5,0 Zoll (= 12,7cm) IPS 720 x 1280 Pixel)
Anschlüsse	USB-C, USB-A, RJ45, **Buchse** für externes Netzteil
Software-Schnittstellen	SICCT, RNDIS, CDC-ECM, IPsec
Internet-Protokolle	IPv4
Kartenschnittstellen	**Smartcard Terminal:** 1 ID-1 Slot Absenkleser (oben), 1 ID-1 Slot Absenkleser (seitlich), 2 ID-000 Schleifleser Plug-Ins für SMCs (seitlich)
Kompatible (Chip-) kartentypen	**Smartcard Terminal:** ISO 7816 Karten, eGK, KVK, HBA, SMC-B und gSMC-KT **RF/NFC Terminal:** ISO 14443A /B, ISO 15693 Karten und Tags
Übertragungsgeschwindigkeit	Zur Karte: 820 kBit/s, zum System: bis 12 MBit/s
Steckzyklen	eGK/HBA ca. 400.000 Betätigungen (~10 Jahre Betrieb bei über 100 Steckzyklen pro Tag)
Stromversorgung	Netzteil (24 V, 0,5 A), PoE (48 V), USB-C (5 V)

Bezeichnung	Wert
Stromaufnahme	**Terminal (Standalone Betrieb)** 24 V-Netzteil: max. 250 mA 48 V PoE, IEEE 802.3af, 802.3at: max. 125 mA 5 V USB-C: max. 1000 mA **Terminal (mit PIN-Pad)** 24 V-Netzteil: max. 500 mA 48 V PoE, IEEE 802.3af, 802.3at: max. 250 mA 5 V USB-C: max. 2000 mA
Lagertemperatur	-20 °C bis +65 °C
Betriebs-temperatur	0 °C bis +50 °C

23 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
CDC-ECM	**C**ommunications **D**evice **C**lass – **E**thernet **C**ontrol **M**odule (USB-Protokoll, um das Terminal mit dem Netzwerk zu verbinden)
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
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
RNDIS	**R**emote **N**etwork **D**river **I**nterface **S**pecification (USB-Protokoll, um das Terminal mit dem Netzwerk zu verbinden)
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.

Abkürzung/ Begriff	Bedeutung
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
VPN	**V**irtual **P**rivate **N**etwork

24 Lieferweg prüfen

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

25 Lizenzinformationen

Die Firmware dieses Produkts beinhaltet Bestandteile von Open-Source-Software.

Informationen zu den jeweiligen Lizenzen finden Sie auf unserer Webseite unter **https://www.cherry.de/eHealth/downloads/st-1506**.

Cherry Digital Health GmbH, Einsteinstraße 174, 81677 München, Germany – **https://www.cherry.de**