eHealth Terminal ST-1506

Handbuch für Administratoren

64410079-04, DE, © Apr 2022 (ST-1506)

Inhalt

Herzlichen Glückwunsch! 3
Zu diesem Handbuch 3
Kurzanleitung 3
Lieferumfang 3

SICHERHEIT 4
1 Dokument prüfen 4
2 Bestellung und sichere Auslieferung 4
2.1 Sichere Lieferkette prüfen 4
2.2 Sicherheitsmerkmale der Verpackung prüfen 5
3 IT-Sicherheit 5
4 Sicherheitsfunktionen 6
4.1 Meldung von Manipulation am Gehäuse 6
4.2 Sichere PIN-Eingabe 6
4.3 Sicheres Firmware-Update 6
4.4 Firmware auf Manipulation prüfen 6
4.5 Benutzerprofile und Authentisierung 6
4.6 Management-Schnittstellen 7
4.7 Verschlüsselte Kommunikation 8
4.8 Vertrauenswürdiges Kartenterminal 8

INBETRIEBNAHME 9
5 Allgemeine Sicherheitshinweise 9
6 Einsatzumgebung 10
7 Gerät identifizieren 10
8 Typenschild prüfen 10
9 Versiegelung prüfen 11
9.1 Gehäuseversiegelung prüfen 11
9.2 Positionen der Gehäusesiegel 11
9.3 Beschreibung des Gehäusesiegels 11
9.4 Slot für gSMC-KT und ggf. SMC-B Karte versiegeln 11
10 Anschlüsse 12
11 Terminal anschließen 13
11.1 Terminal mit Strom versorgen 13
11.2 Terminal ein- und ausschalten 13
11.3 Terminal direkt mit dem Netzwerk verbinden 13
11.4 Terminal über den PC mit dem Netzwerk verbinden 13
12 Administrator-PIN 14
12.1 PIN erstmalig festlegen 14
12.2 PIN ändern 14
12.3 PIN falsch oder vergessen 14
13 gSMC-KT Karte installieren 15
14 Pairing mit einem Konnektor 15

BEDIENUNG 17
15 Maßnahmen zur sicheren Benutzung 17
16 Karten einstecken 17
17 Navigation 18
17.1 Betriebsarten 18
18 Statusanzeige LEDs 18
19 Displaysymbole 18
20 Sicherer PIN-Eingabe-Modus 19
20.1 Remote-PIN-Konnektor 20
21 PIN-Eingabe über die Remote-Schnittstelle 20
22 Eigendiagnose 20

KONFIGURATION 21
23 Lokale Konfiguration über direkte Managementschnittstelle 21
23.1 Mögliche Einstellungen im Menü 21
23.2 Menü "Einstellungen" (Benutzer) 21
23.3 Admin-Menü 22
24 Konfiguration über Remote-Schnittstelle 24
25 Terminalname ändern 25
26 Virtual Private Network (VPN) 26
27 Firmware aktualisieren 26
27.1 Firmware über Konnektor aktualisieren 26
27.2 Firmware über Remote-Schnittstelle aktualisieren 26
28 Trust-Service Status Liste (TSL) aktualisieren 27
29 Auf Werkseinstellungen zurücksetzen 27

AUSSERBETRIEBNAHME 28
30 Pairing-Informationen löschen 28
31 Reparatur 28
32 Batterie 28
33 Geräte entsorgen 28

ALLGEMEINES 29
34 Fehlermeldungen 29
35 Terminal reinigen 30
36 Kontakt 30
37 Technische Daten 31
38 Abkürzungen und Begriffserklärungen 31
39 Literatur 33
40 Lizenzinformationen 33

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 diesem Handbuch

Dieses Handbuch enthält Handlungsabläufe und Informationen für Administratoren zur Installation, Inbetriebnahme, Konfiguration und zum sicheren Betrieb des **ST-1506**.

Es wurde auf der Basis der Kartenterminal-Firmware in der Version 3.0.0 erstellt. Für neuere Firmwareversionen kann der Inhalt abweichen. Die aktuellste Version des Handbuchs 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**.

Kurzanleitung

Für Benutzer des Kartenterminals liegt dem Terminal folgende Kurzanleitung bei:

- Kurzanleitung eHealth Terminal ST-1506 (Artikel-Nr. 64410078)

Sie beschreibt die Bedienung des in Betrieb befindlichen Terminals für Beschäftigte im deutschen Gesundheitswesen.

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

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/eHealth** 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

Das **ST-1506** 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.)

HINWEIS: 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.

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

2 Prüfen Sie die Echtheit des Geräts, indem Sie unter **https://www.cherry.de/eHealth** oder über die Supporthotline die Seriennummer der Versiegelung der Verpackung (siehe 2.2 "Sicherheitsmerkmale der Verpackung prüfen") sowie die Seriennummer und die MAC-Adresse vom Typenschild des **ST-1506** angeben. Sie erhalten als Rückmeldung, ob es sich um ein sicher ausgeliefertes Originalprodukt handelt.

3 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.

4 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 das Siegelband 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.

Das Terminal **ST-1506** wird in einem bedruckten Produktkarton verpackt.

Dieser Karton ist an den vier Seiten rundherum mit einem speziell für CHERRY hergestellten Siegelband mit den folgenden Merkmalen verschlossen:

1 Das Siegelband hat eine aufgedruckte Seriennummer und einen Barcode, siehe nachfolgende Abbildung:

Diese Seriennummer wird zusammen mit der Seriennummer des **ST-1506** bei der Produktion gespeichert.

2 Prüfen Sie, ob die Seriennummer des Siegelbandes nicht überklebt ist. Die Seriennummer des Siegelbandes wird für die Überprüfung der Echtheit des Geräts benötigt (siehe 2.1 "Sichere Lieferkette prüfen").

3 Prüfen Sie, ob das Siegelband unbeschädigt ist.

Wurde das Siegelband abgelöst und wieder angebracht, so ist der Schriftzug "GEÖFFNET" zu erkennen:

3 IT-Sicherheit

Die in Kapitel 7 "Gerät identifizieren" genannten Varianten des Terminals besitzen ein IT-Sicherheitszertifikat des Bundesamts für Sicherheit in der Informationstechnik (BSI) nach Common Criteria (CC) Standard, siehe 39 "Literatur", [1] mit der Verfahrens-ID BSI-DSZ-CC-1124.

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 "System angehalten", zusätzlich wird die Information "Manipulationsschutz ausgelöst! Code: xx" angezeigt.

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

4.2 Sichere PIN-Eingabe

HINWEIS: Ausspähen der PIN möglich.

- Verwenden Sie immer die sichere PIN-Eingabe über das Display (siehe 20 "Sicherer PIN-Eingabe-Modus").

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 20 "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.

4.3 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 angestoßen werden. Nähere Informationen finden Sie unter 27 "Firmware aktualisieren".

4.4 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

4.5 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 12 "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 29 "Auf Werkseinstellungen zurücksetzen").

4.6 Management-Schnittstellen

Der Zugang zum Kartenterminal erfolgt durch folgende, gesicherte Managementschnittstellen. Jede Managementschnittstelle besitzt eine eigene, separate PIN.

- **SICCT-Schnittstelle**
  Zugriff auf das Kartenterminal über den Konnektor.
  Benutzername: admin
  Session Admin PIN: Initial wird die lokal am Terminal vergebene Administrator-PIN verwendet. Ändern Sie sie aus Sicherheitsgründen nach der Erstinbetriebnahme. Verwenden Sie für die SICCT-Schnittstelle eine andere. Melden Sie sich dazu an der direkten oder der Remote-Schnittstelle an.
- **Direkte Managementschnittstelle**

HINWEIS: Ausspähen der Administrator-PIN möglich.

- Geben Sie die Administrator-PIN nur in einer sicheren Umgebung an der direkten Managementschnittstelle ein.

Lokaler Zugang, direkt am Kartenterminal.
Die direkte Managementschnittstelle besteht aus dem Touchdisplay und der Status-LED am senkrechten Kartenslot 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.

- **Remote-Schnittstelle**
  Zugriff auf das Kartenterminal mittels JSON-Schnittstelle oder Internet-Browser.
  Benutzername: admin
  PIN: Initial wird die lokal am Terminal vergebene Administrator-PIN verwendet. Ändern Sie sie aus Sicherheitsgründen nach der Erstinbetriebnahme. Verwenden Sie für die Remote-Schnittstelle eine andere.

Folgende Funktionen sind nur lokal am Terminal zugänglich:

- Pairing mit einem Konnektor (siehe 14 "Pairing mit einem Konnektor")
- Aktivieren oder Deaktivieren der Admin Session für die SICCT-Schnittstelle (siehe 23.1 "Mögliche Einstellungen im Menü")
- Aktivieren oder Deaktivieren der Remote-Schnittstelle (siehe 24 "Konfiguration über Remote-Schnittstelle")

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

INFO: Deaktivierte Einstellungen

Folgende Einstellungen sind nach initialer Inbetriebnahme deaktiviert:

- Remote-Zugang über Remote-Schnittstelle
- Admin Session für die SICCT-Schnittstelle (z. B. Firmware oder TSL aktualisieren)

4.7 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 in der TSL hinterlegten CA-Zertifikate der Konnektoren.

Zum einen wird dadurch die Sicherung der Netzwerkkommunikation durch 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 das grüne Netzwerksymbol angezeigt.

4.8 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
- 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 die gSMC-KT Karte (siehe 13 "gSMC-KT Karte installieren").

9 Legen Sie die Administrator-PIN fest (siehe 12 "Administrator-PIN").

10 Installieren Sie das Gerät (siehe 11 "Terminal anschließen").

11 Beachten Sie die Benutzungsvorschriften (siehe 15 "Maßnahmen zur sicheren Benutzung").

12 Schalten Sie ggf. deaktive Einstellungen frei (siehe 23 "Lokale Konfiguration über direkte Managementschnittstelle" oder 24 "Konfiguration über Remote-Schnittstelle"). Folgende Einstellungen sind nach Erstinbetriebnahme deaktiviert:
   - Remote Zugang über Remote-Schnittstelle
   - Die Admin Session der SICCT-Schnittstelle (z. B. Firmware oder TSL aktualisieren)

13 Führen Sie das Pairing mit einem Konnektor durch (siehe 14 "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 zugelassenen Konnektor. Der Konnektor prüft periodisch den Pairingstatus und gibt ggf. eine Warnung aus.
- Verwenden Sie für den Betrieb des Geräts nur eine zugelassene gSMC-KT Karte.
- 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

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 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 **Einstellungen > Status** angezeigt (siehe 23.2 "Menü "Einstellungen" (Benutzer)").

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

- Artikelnummer: ST-1506 AFHZ
  Firmwareversion: 3.0.0
  Hardwareversion: 4.0.0
- Artikelnummer: ST-1506 AFEZ
  Firmwareversion: 3.0.0
  Hardwareversion: 4.0.0

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.

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 Gerätelieferanten.

9 Versiegelung prüfen

9.1 Gehäuseversiegelung prüfen

Zusätzlich zum aktiven physikalischen Manipulationsschutz (siehe 4.1 "Meldung von Manipulation am Gehäuse") 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 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".

HINWEIS: 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

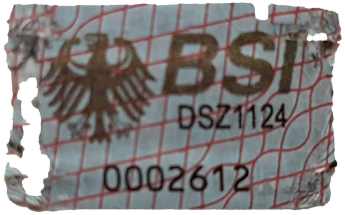
Das graue, 20 mm lange und 12 mm breite Siegel ist mit einer 7-stelligen Seriennummer versehen, um die eindeutige Identifizierbarkeit zu gewährleisten.

Als Echtheitsmerkmal sind der Bundesadler und der Schriftzug BSI mit einem Farbkippeffekt versehen. Die Kippfarbe wechselt je nach Betrachtungswinkel und Lichteinfall 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.

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 Slot 3 und Slot 4 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.

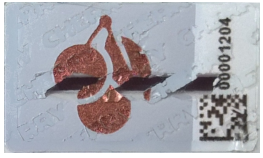
5 Verwahren Sie nicht benötigte Siegel an einem sicheren Ort.

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

Position Slotsiegel

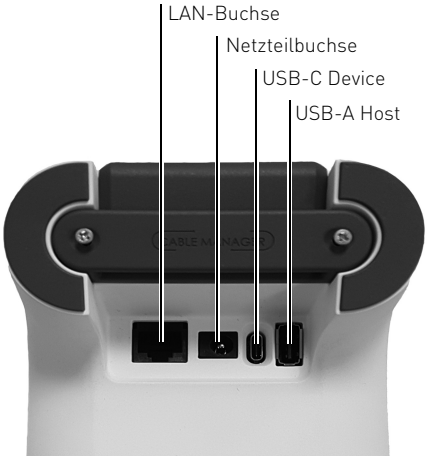
Unbeschädigtes Slotsiegel

Slotsiegel nach Ablöseversuch



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

10 Anschlüsse



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 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 Terminal anschließen

11.1 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.

11.2 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.

11.3 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.

11.4 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. Das verwendete Protokoll können Sie am Terminal unter **Admin-Menü > Verbindung > USB Ethernet** konfigurieren.
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**

12 Administrator-PIN

12.1 PIN erstmalig festlegen

Das Gerät funktioniert erst nach Festlegung der Administrator-PIN.

Bei der Erstinbetriebnahme werden Sie aufgefordert, eine neue 8- bis 12-stellige Administrator-PIN festzulegen.

HINWEIS: Manipulation am Gerät

Erscheint bei der Erstinbetriebnahme, nach Erhalt des Geräts, **keine** Aufforderung eine neue PIN festzulegen:

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

1 Wählen Sie die PIN unter Vermeidung von Geburtsdaten oder gleichen Zahlenfolgen. Beachten Sie die "Regelung des Passwortgebrauchs" unter: **www.bsi.bund.de**

2 Geben Sie die PIN ein. Achten Sie darauf, dass Sie bei der Eingabe nicht beobachtet werden.

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

3 Bestätigen Sie die Eingabe.

4 Geben Sie die PIN erneut ein.

5 Bestätigen Sie die Eingabe.

6 Notieren Sie die PIN und bewahren Sie sie unter Verschluss auf.

HINWEIS: Identische PINs

Die Administrator-PIN wird initial für **alle** Zugänge gesetzt. Sie ist also anfangs für alle drei Management-Schnittstellen gleich: **direkter Zugang** am Terminal, **Remote-Schnittstelle** und **SICCT-Schnittstelle**. Jede Managementschnittstelle besitzt eine separate PIN-Verwaltung.

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

12.2 PIN ändern

Die Änderung der PIN betrifft immer nur die jeweils gewählte Managementschnittstelle.

Die PIN für den **direkten Zugang** ändern Sie lokal am Terminal: **Admin-Menü > Gerät > Admin-PIN ändern**.

Die PIN für den **Remote-Zugang** ändern Sie direkt über die Remote-Schnittstelle.

Die PIN für den **SICCT-Zugang** ändern Sie lokal am Terminal: **Admin-Menü > Gerät > Session Admin-PIN** oder über die Remote-Schnittstelle. Die geänderten Zugangsdaten müssen folglich auch am Konnektor hinterlegt werden! Verbindungsversuche mit falschen Zugangsdaten führen sonst zur Sperrung der SICCT-Schnittstelle.

12.3 PIN falsch oder vergessen

Ab der 3. Fehleingabe der PIN wird die jeweilige Management-Schnittstelle zeitweise gesperrt (direkter Zugang, Remote-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 nach dem Einschalten des Terminals wieder auf den Ausgangswert zurückgesetzt.

- 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 Remote-Schnittstelle ist nicht abfragbar.
- Der Fehlerzähler des jeweiligen Zugangs wird nach Eingabe der korrekten PIN zurückgesetzt.

Eine vergessene Administrator-PIN kann nur durch Reset des Kartenterminals auf Werkseinstellungen zurückgesetzt werden. Dabei wird auch der Fehlerzähler für den direkten (lokalen) Zugang auf Null gesetzt. Siehe 29 "Auf Werkseinstellungen zurücksetzen".

13 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. Ohne gSMC-KT startet das Terminal nicht und hat somit auch keine Funktion. Bezugsquellen für eine gSMC-KT finden Sie auf **https://www.cherry.de/eHealth**.

1 Prüfen Sie, ob Ihre gSMC-KT Karte echt ist. Informationen zur Überprüfung finden Sie auf **https://www.cherry.de/eHealth**.
2 Notieren Sie sich die MAC-Adresse des CHERRY eHealthTerminals (**Verbindung > MAC-Adresse**).
3 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.
4 Stecken Sie die gSMC-KT Karte in einen der beiden kleinen Steckplätze auf der rechten Seite des Terminals (siehe 16 "Karten einstecken").
5 Entfernen Sie rückstandslos eventuell vorhandene Reste alter Siegel um den Kartenleser und stellen Sie sicher, dass die glatte Siegelfläche staub- und fettfrei ist (siehe 35 "Terminal reinigen").
6 Überkleben Sie den Schlitz des Kartenlesers mit einem neuen Siegel (siehe 9.4 "Slot für gSMC-KT und ggf. SMC-B Karte versiegeln").
7 Notieren Sie sich zusätzlich zu den vorhandenen Daten (MAC-Adresse, gSMC-KT Fingerprint) die Seriennummer des aufgeklebten Slotsiegels.
8 Eine PIN-Freischaltung der gSMC-KT Karte ist nicht notwendig.

HINWEIS: 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!

14 Pairing mit einem Konnektor

Falls nötig, konfigurieren Sie das Terminal, bevor Sie das Pairing mit einem Konnektor durchführen.

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.

HINWEIS: 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 13 "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 am Terminal.

  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 der Terminals im Konnektor zu vereinfachen, kann der Terminalname des Kartenterminals verändert werden (siehe 25 "Terminalname ändern"). 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 im Menü").

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 für zugelassene Konnektoren (siehe 28 "Trust-Service Status Liste (TSL) aktualisieren").

TIPP: Authentifizierung des Konnektors

Falls der bei Ihnen eingesetzte Konnektor nicht authentifiziert werden kann:

- Aktualisieren Sie die TSL (Trust-Service Status Liste). Die aktuelle TSL finden Sie auf **https://www.cherry.de/eHealth**.

BEDIENUNG

15 Maßnahmen zur sicheren Benutzung

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

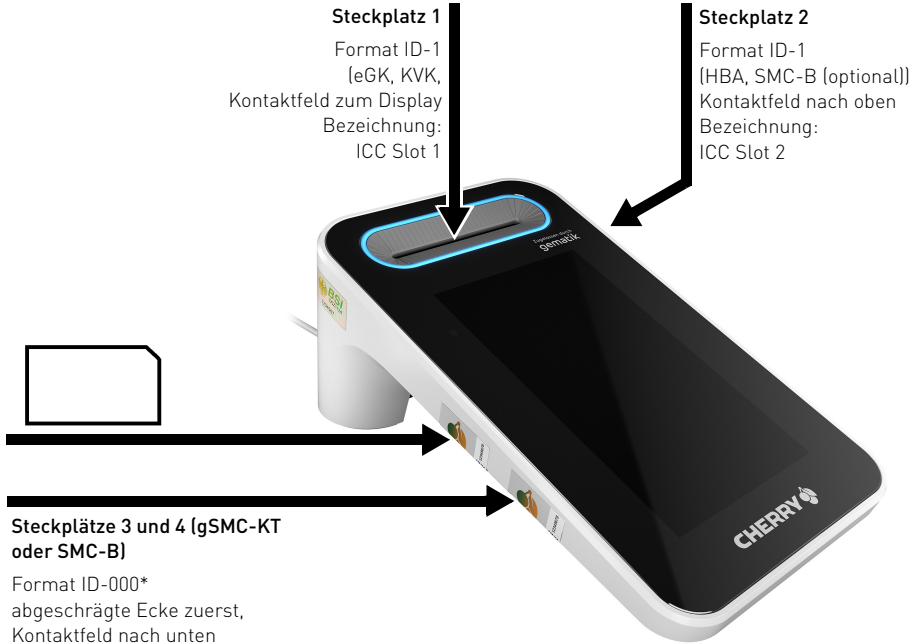
1 Lesen Sie sich dieses Handbuch genau durch.
2 Halten Sie Ihre Administrator-PIN geheim und geben Sie sie nicht weiter.
3 Achten Sie darauf, dass Sie während der Eingabe der PIN nicht beobachtet werden.
4 Bringen Sie auf dem Kartenterminal keine Aufkleber oder Notizzettel an.
5 Sorgen Sie dafür, dass 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.

16 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:

*Zu Format ID-000 siehe 39 "Literatur", [2].

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 werden, siehe 9.4 "Slot für gSMC-KT und ggf. SMC-B Karte versiegeln".
- Entfernen Sie die Karte nur im stromlosen Zustand des Terminals.

17 Navigation

17.1 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.

18 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

19 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

20 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 und zugelassener Betriebszustand

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

20.1 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.

21 PIN-Eingabe über die Remote-Schnittstelle

Zusätzlich zur lokalen sicheren PIN-Eingabe verfügt das Terminal über die Möglichkeit, die Karten-PIN auch über die Remote-Schnittstelle einzugeben. Hierfür müssen Sie unter **Admin-Menü > Gerät > Remote PIN-Eingabe** den gewünschten Kartenslot auf den Wert "Webservice" konfigurieren. Sie können alle Kartenslots zur PIN-Eingabe über die Remote-Schnittstelle verwenden. Achten Sie darauf, dass Sie nur den Kartenslot, in dem sich eine SMC-B befindet, für die PIN-Eingabe über die Remote-Schnittstelle konfigurieren.

HINWEIS: Sicherer zertifizierter und zugelassener Betriebszustand

- Nur bei der Verwendung der sicheren PIN-Eingabe befindet sich das Gerät im sicheren zertifizierten und zugelassenen Betriebszustand.

22 Eigendiagnose

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

- Buzzer
- Kartenslots
- Integrität
- Batteriestatus

Siehe 23.1 "Mögliche Einstellungen im Menü".

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

KONFIGURATION

HINWEIS: Neustart nach Konfiguration der Verbindung

- Damit die Änderung der Verbindungsart übernommen wird, müssen Sie das Gerät neu starten.

23 Lokale Konfiguration über direkte Managementschnittstelle

Folgende Funktionen sind nur lokal am Gerät zugänglich:

- Pairing mit einem Konnektor (siehe 14 "Pairing mit einem Konnektor")
- Aktivieren oder Deaktivieren der Admin Session der SICCT-Schnittstelle (siehe 23.1 "Mögliche Einstellungen im Menü")
- Aktivieren oder Deaktivieren der Remote-Schnittstelle (siehe 24 "Konfiguration über Remote-Schnittstelle")

23.1 Mögliche Einstellungen im Menü

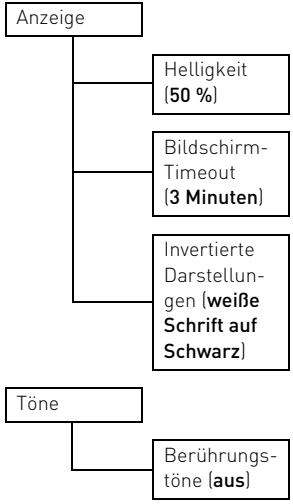
- Um in das Hauptmenü zu gelangen, drücken Sie auf die Taste **Menü**.

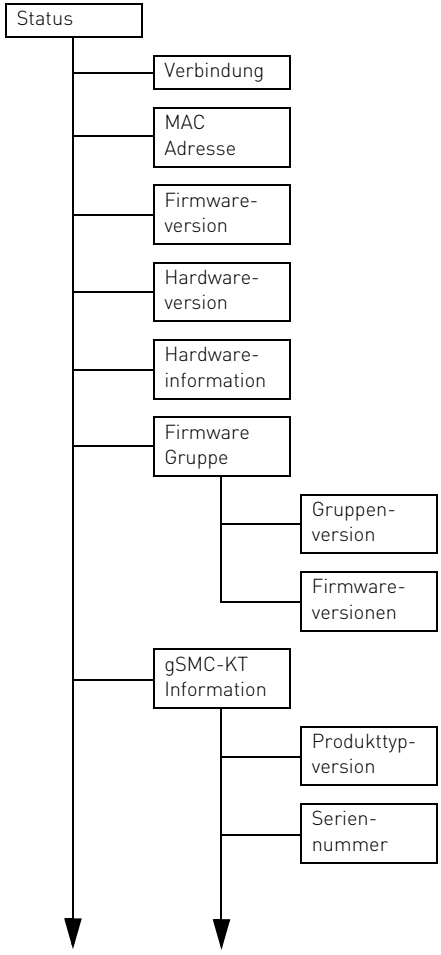
Fett = Werkseinstellungen

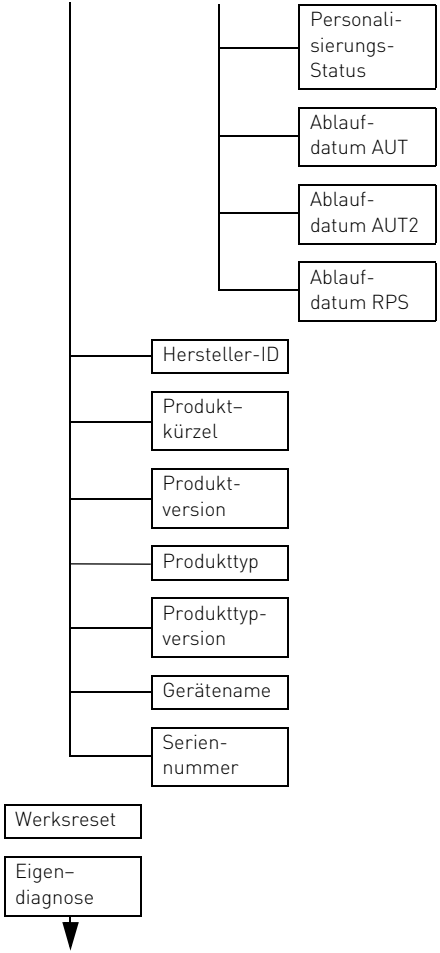
Sie können die auf den folgenden Seiten dargestellten Einstellungen vornehmen:

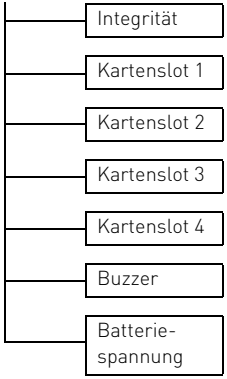
- Einstellungen
- Admin-Menü
- Gerät neu starten

23.2 Menü "Einstellungen" (Benutzer)

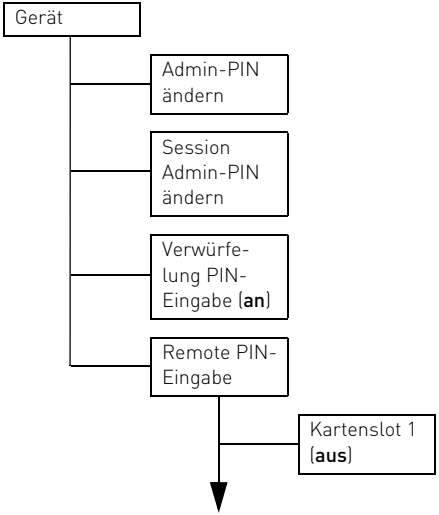


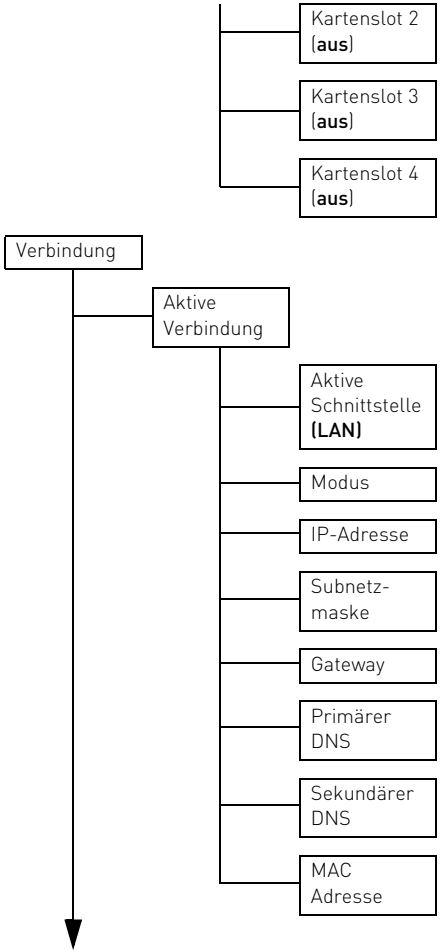


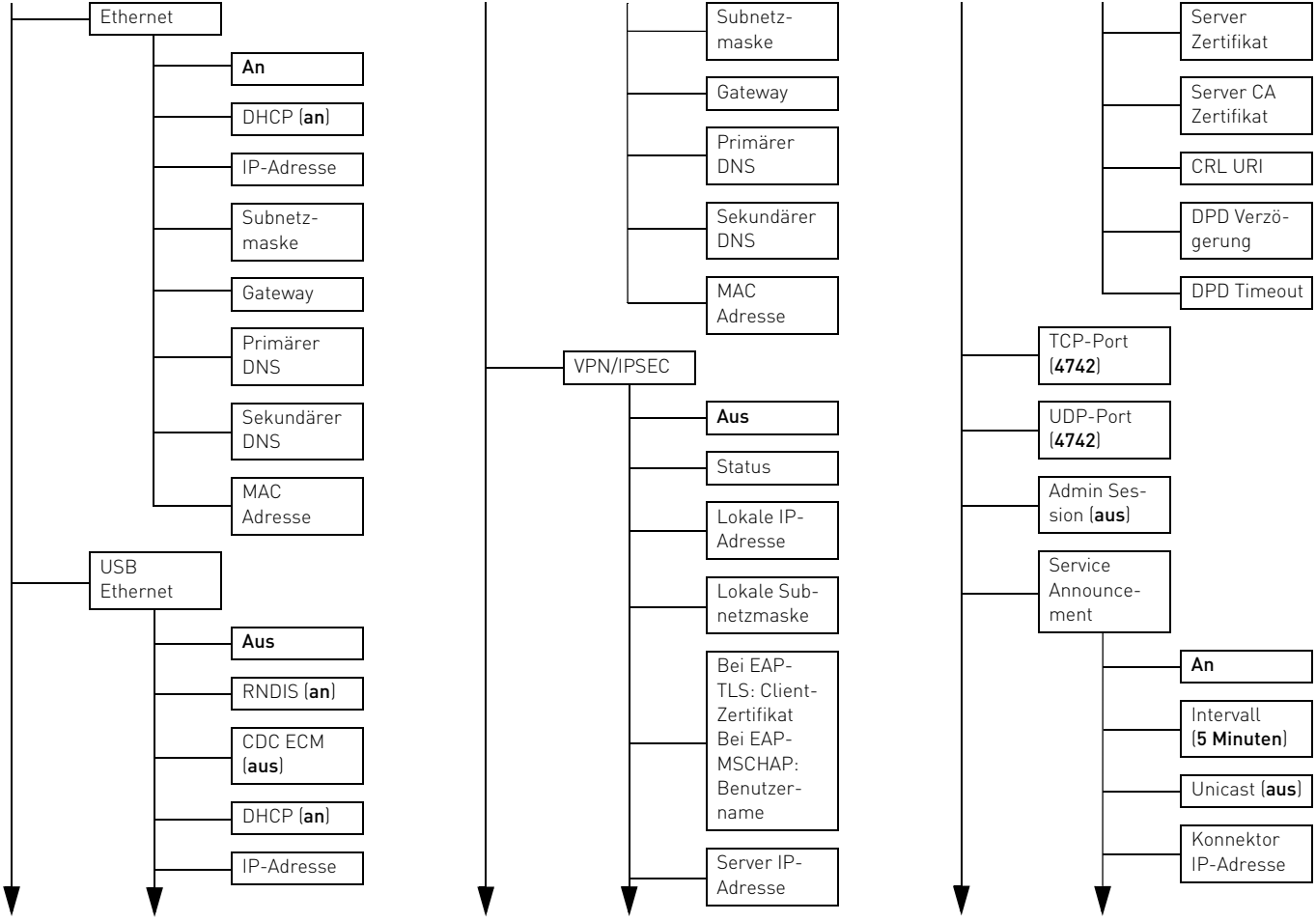


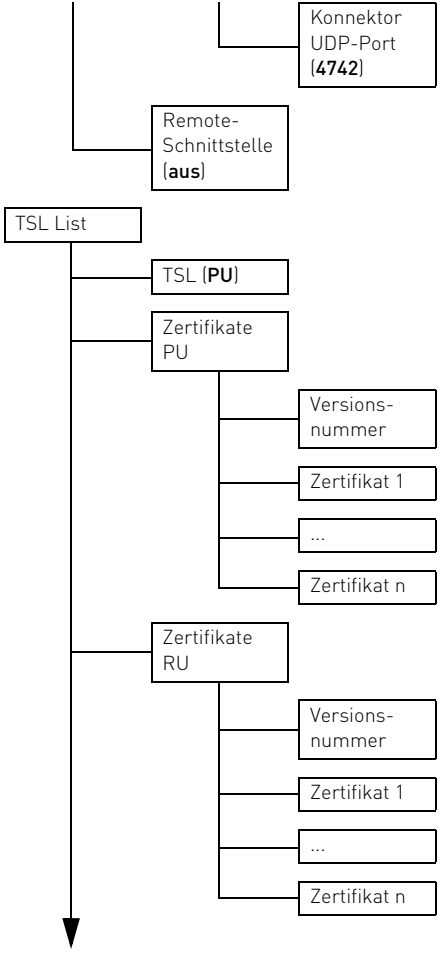


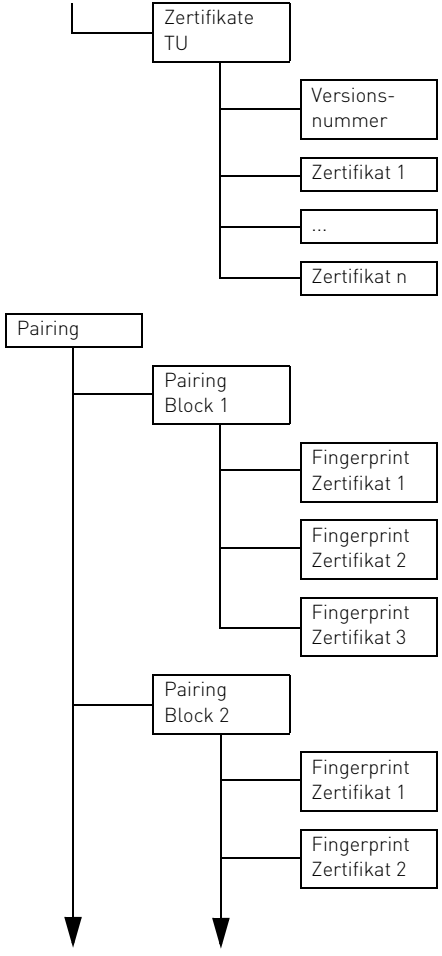
23.3 Admin-Menü

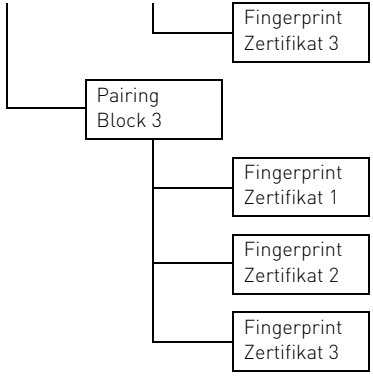





Ethernet
An
DHCP (an)
IP-Adresse
Subnetz-maske
Gateway
Primärer DNS
Sekundärer DNS
MAC Adresse
USB Ethernet
Aus
RNDIS (an)
CDC ECM (aus)
DHCP (an)
IP-Adresse
Subnetz-maske
Gateway
Primärer DNS
Sekundärer DNS
MAC Adresse
VPN/IPSEC
Aus
Status
Lokale IP-Adresse
Lokale Sub-netzmaske
Bei EAP-TLS: Client-Zertifikat Bei EAP-MSCHAP: Benutzer-name
Server IP-Adresse
Server Zertifikat
Server CA Zertifikat
CRL URI
DPD Verzö-gerung
DPD Timeout
TCP-Port (4742)
UDP-Port (4742)
Admin Ses-sion (aus)
Service Announce-ment
An
Intervall (5 Minuten)
Unicast (aus)
Konnektor IP-Adresse







Werksreset

24 Konfiguration über Remote-Schnittstelle

Das Terminal verfügt über eine Remote-Schnittstelle, die über das Netzwerk zur Fernverwaltung angesprochen werden kann. Sie können entweder direkt mit Nachrichten, die der JavaScript Object Notation (JSON) entsprechen, mit dieser Schnittstelle kommunizieren oder über einen Webbrowser.

Wenn Sie direkt mit der Remote-Schnittstelle kommunizieren möchten, erhalten Sie weitere Informationen auf unserer Webseite **https://www.cherry.de/eHealth**.

In diesem Kapitel wird die Verwendung der Remote-Schnittstelle über den Webbrowser beschrieben.

Über die Remote-Schnittstelle stehen 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 14 "Pairing mit einem Konnektor")
- Aktivieren oder Deaktivieren administrativer SICCT-Kommandos (siehe 23.1 "Mögliche Einstellungen im Menü")
- Aktivieren oder Deaktivieren der Remote-Schnittstelle

Für den Zugang zur Remote-Schnittstelle müssen die folgenden Bedingungen erfüllt sein:

- Die gSMC-KT Karte steckt im Terminal (siehe 13 "gSMC-KT Karte installieren").
- Die Remote-Schnittstelle wurde lokal am Terminal aktiviert (Standard = Aus). Umstellung unter **Admin-Menü > Verbindung > Remote-Schnittstelle > Ein**.
- 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 **Admin-Menü > Verbindung > Aktive Verbindung** (oder über Ihren DHCP-Server).

Bei der Verwendung eines Webbrowser müssen Sie Folgendes beachten:

- Ihr Browser unterstützt **TLS 1.2** und diese Einstellung ist auch aktiviert.

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.

TIPP: 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 13 "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.

HINWEIS: Ausspähen der Administrator-PINs möglich.

- Geben Sie die Administrator-PIN nur in einer sicheren Umgebung ein.

2 Melden Sie sich an.
Benutzer: admin
Kennwort: Die PIN, die Sie bei der Inbetriebnahme vergeben haben (siehe 12 "Administrator-PIN").

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.

25 Terminalname ändern

Um die Verwaltung zu vereinfachen, können Sie den Terminalnamen bei der Inbetriebnahme des Kartenterminals über die Remote-Schnittstelle verändern (siehe 24 "Konfiguration über Remote-Schnittstelle"). Er wird zum Konnektor übertragen und kann in der Kartenterminalverwaltung des Konnektors im Sinne eines Friendly Name verwendet werden.

Der Terminalname muss folgende Kriterien erfüllen:

- Der Terminalname besteht aus maximal 32 Zeichen.
- Jedes Zeichen ist entweder das Minuszeichen "-" oder einer der 26 Großbuchstaben "A" bis "Z" oder einer der 26 Kleinbuchstaben "a" bis "z" oder eine der zehn Ziffern "0" bis "9".
- Das Minuszeichen "-" ist als letztes Zeichen nicht zulässig.

HINWEIS: Konnektorprobleme

Entspricht der Terminalname nicht der vorgegebenen Konvention, kann es vorkommen, dass der Konnektor den Terminalnamen nicht richtig auflösen kann und somit das Terminal nicht findet bzw. anzeigt.

26 Virtual Private Network (VPN)

Das Terminal stellt einen VPN-Client zur Verfügung, um eine Verbindung zu einem Rechenzentrum (VPN-Gateway, z. B. Krankenhaus-IT) über eine IPsec VPN-Verbindung herstellen zu können. Es werden die beiden Authentifizierungsverfahren **EAP-MSCHAPv2** und **EAP-TLS** unterstützt. Die Konfiguration erfolgt ausschließlich über die Remote-Schnittstelle. Lokal an der direkten Managementschnittstelle kann die VPN-Option nur aktiviert, das entsprechende Authentifizierungsverfahren ausgewählt und die entsprechende Konfiguration eingesehen werden.

27 Firmware aktualisieren

Halten Sie die Firmware des Kartenterminals stets aktuell. Prüfen Sie dazu regelmäßig unsere Homepage unter **https://www.cherry.de/eHealth**.

Der Konnektor prüft automatisch in regelmäßigen Abständen, ob ein Update für die angeschlossenen Geräte in der TI vorliegt.

Neben der Hardware ist die Firmware ein sicherheitssensibles Element. Verwenden Sie aus diesem Grund nur zertifizierte und zugelassene Firmwareversionen.

Welche Versionen in das Terminal geladen werden können, ist in der Liste unter Firmware Gruppe ersichtlich:
Einstellungen > Status > Firmware Gruppe.

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

HINWEIS: Abbruch des Firmware-Updates

Nach dem Update wird das Terminal automatisch neu gestartet. Anschließend wird die Installation der Firmware geprüft. Dieser Vorgang dauert einige Minuten.

- Trennen Sie das Terminal nach der Installation für 5 Minuten nicht von der Stromversorgung. Andernfalls wird die Firmware wieder auf die ursprüngliche Version zurückgesetzt.
- Führen Sie innerhalb von 5 Minuten kein weiteres Firmware-Update durch.
- Prüfen Sie nach 5 Minuten am Terminal im Menü **Einstellungen > Status**, ob die gewünschte Firmwareversion angezeigt wird.

27.1 Firmware über Konnektor aktualisieren

1 Prüfen Sie, ob die Admin Session der SICCT Schnittstelle aktiviert ist (Standardeinstellung = Aus): **Admin-Menü > Verbindung > Admin Session > Ein**.

2 Verwenden Sie zur Aktualisierung den Konfigurationsdienst des verbundenen Konnektors.

Die Konfiguration des Kartenterminals bleibt beim Update erhalten (z. B. Terminal-Name, IP-Adresse oder Pairing-Informationen).

27.2 Firmware über Remote-Schnittstelle aktualisieren

Das Firmware-Update wird vom Hersteller in Form einer signierten Datei zum Download angeboten. Über die Remote-Schnittstelle werden zwei Möglichkeiten zur Firmware-Update angeboten:

Firmware-Aktualisierung über HTTP Server Download

1 Öffnen Sie in Ihrem Browser die Remote-Schnittstelle (siehe 24 "Konfiguration über Remote-Schnittstelle").

2 Wählen Sie **Konfiguration**.

3 Tragen Sie eine gültige Webadresse ein, die auf die Update-Datei verweist (http://*.bin).

4 Klicken Sie auf **Aktualisieren**.

Firmware-Aktualisierung über File Upload

1 Öffnen Sie in Ihrem Browser die Remote-Schnittstelle (siehe 24 "Konfiguration über Remote-Schnittstelle").
2 Wählen Sie **Konfiguration**.
3 Klicken Sie auf die Schaltfläche **Durchsuchen...** und wählen Sie die Firmware-Datei aus.
4 Klicken Sie auf **Aktualisieren**.

28 Trust-Service Status Liste (TSL) aktualisieren

Es kann notwendig sein, dass eine neue Trust-Service Status Liste (TSL) für einen der Vertrauensräume eingespielt werden muss. Diese Liste wird vom Hersteller in Form einer signierten Datei zum Download angeboten. Die aktuelle TSL finden Sie auf **https://www.cherry.de/eHealth**.

TSL-Aktualisierung über HTTP Server Download

1 Öffnen Sie in Ihrem Browser die Remote-Schnittstelle (siehe 24 "Konfiguration über Remote-Schnittstelle").
2 Wählen Sie **Konfiguration**.
3 Tragen Sie eine gültige Webadresse ein, die auf die Update-Datei verweist (http://*.bin).
4 Klicken Sie auf **Aktualisieren**.

TSL-Aktualisierung über File Upload

1 Öffnen Sie in Ihrem Browser die Remote-Schnittstelle (siehe 24 "Konfiguration über Remote-Schnittstelle").
2 Wählen Sie **Konfiguration**.
3 Klicken Sie auf die Schaltfläche **Durchsuchen...** und wählen Sie die Firmware-Datei aus.
4 Klicken Sie auf **Aktualisieren**.

TIPP: Authentifizierung des Konnektors

Falls der bei Ihnen eingesetzte Konnektor nicht authentifiziert werden kann:

Aktualisieren Sie die Trust-Service Status Liste (TSL). Die aktuelle TSL finden Sie auf **https://www.cherry.de/eHealth**.

29 Auf Werkseinstellungen zurücksetzen

Durch den Werksreset wird der Auslieferungszustand des Geräts wieder hergestellt (mit Ausnahme der Firmware und der Firmwaregruppe). Die Inbetriebnahme muss damit erneut durchgeführt werden.

Der Werksreset kann entweder durch den Administrator oder durch CHERRY erfolgen.

- Wählen Sie **Admin-Menü > Werksreset (Administrator-PIN eingeben)**.

Sollten Sie Ihr Admin-Passwort vergessen haben, kann der Werksreset auch von CHERRY durchgeführt werden. Wenden Sie sich an CHERRY, um die nötigen Informationen zu erhalten.

- Wählen Sie **Einstellungen > Werksreset**.

AUSSER-BETRIEBNAHME

30 Pairing-Informationen löschen

HINWEIS: Weitergabe von Pairing-Informationen

- Führen Sie vor der Außerbetriebnahme einen Werksreset durch (siehe 29 "Auf Werkseinstellungen zurücksetzen". Hierbei werden alle kritischen Informationen im Gerät gelöscht.

31 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.

32 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 Gerätelieferanten.

33 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

34 Fehlermeldungen

Meldung	Bedeutung
Eingabe fehlgeschlagen	Beim Ändern der Administrator-PIN wurde die falsche PIN eingeben.
Eingabe nicht erfolgreich! Fehlerzähler [n]	Die Eingabe der Administrator-PIN war inkorrekt und dadurch hat sich der Fehlerzähler auf den Wert [n] erhöht.
Firmware erfolgreich installiert	Das Update der Firmware oder der TSL-Liste wurde erfolgreich durchgeführt. Es erfolgt ein automatischer Neustart des Terminals.
Firmware ungültig: Downgrade unterbunden!	Die Version der Firmware ist nicht in der Firmware Gruppe enthalten, die Version der TSL-Liste ist gleich oder niedriger als die im Gerät enthaltene. Der Update-Vorgang wurde abgebrochen.
Firmware ungültig: Signaturprüfung fehlgeschlagen!	Die Signatur der Firmware oder der TSL-Datei ist ungültig. Der Update-Vorgang wurde abgebrochen.
Firmware-Update fehlgeschlagen!	Es ist ein Problem beim Update der Firmware oder der TSL-Liste aufgetreten. Der Update-Vorgang wurde abgebrochen.
Kein weiterer Versuch möglich	Die Eingabe beim Werksreset durch CHERRY ist gesperrt. Führen Sie den Prozess erneut aus.
Passwort gesperrt!	Die Eingabe der Administrator-PIN ist gesperrt, da zu viele Falscheingaben durchgeführt wurden.
Fehlerzähler [n]	Der Fehlerzähler hat den Wert [n].
Sperrzeit übrig: HH:MM:SS	Restliche Sperrzeit, die bis zur Freigabe gewartet werden muss
PINs stimmen nicht überein	Die Wiederholung der PIN war abweichend zur ersten Eingabe. Versuchen Sie es erneut.
Response falsch! Verbleibende Versuche: [n]	Die Eingabe beim Werksreset durch CHERRY ist ungültig. Versuchen Sie es erneut.
SICCT Download Firmware wird im Hintergrund geprüft und installiert. Dieser Vorgang dauert einige Minuten.	Der Download Vorgang wurde erfolgreich abgeschlossen. Die Update-Datei wird überprüft.
System angehalten Manipulationsschutz ausgelöst! Code: xx	Der Sicherheitsmechanismus wurde aktiviert. Mögliche Ursachen: Manipulation oder Öffnen des Gehäuses, Transport- oder Fallschaden, Gerätedefekt, Batterie entladen. Wenden Sie sich an Ihren Gerätelieferanten.
Ungültige IP-Adresse	Die Eingabe ist ungültig. Das Format oder der Wertebereich sind nicht zulässig. Versuchen Sie es mit einem passenden Wert erneut.
Ungültige Subnetzmaske	Die Eingabe ist ungültig. Das Format oder der Wertebereich sind nicht zulässig. Versuchen Sie es mit einem passenden Wert erneut.

Meldung	Bedeutung
Ungültiger Gateway	Die Eingabe ist ungültig. Das Format oder der Wertebereich sind nicht zulässig. Versuchen Sie es mit einem passenden Wert erneut.
Ungültiger Primärer DNS	Die Eingabe ist ungültig. Das Format oder der Wertebereich sind nicht zulässig. Versuchen Sie es mit einem passenden Wert erneut.
Ungültiger Sekundärer DNS	Die Eingabe ist ungültig. Das Format oder der Wertebereich sind nicht zulässig. Versuchen Sie es mit einem passenden Wert erneut.

35 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.

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
- 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

37 Technische Daten

Bezeichnung	Wert
Systemvoraus-setzungen	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-Schnitt-stellen	SICCT, RNDIS, CDC-ECM, IPsec
Internet-Protokolle	IPv4
Kartenschnitt-stellen	**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
Übertragungsge-schwindigkeit	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)
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

38 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)
CDC-ECM	**C**ommunications **D**evice **C**lass – **E**thernet **C**ontrol **M**odule (USB-Protokoll, um das Terminal mit dem Netzwerk zu verbinden)
EAL	**E**valuation **A**ssurance **L**evel
EAP-MSCHAPv2	**E**xtensible **A**uthentication **P**rotocol-**M**icro**s**oft **C**hallenge **H**andshake **A**uthentication **P**rotocol **V**ersion **2** (Authentifizierungsverfahren)

Abkürzung/ Begriff	Bedeutung
EAP-TLS	**E**xtensible **A**uthentication **P**rotocol-**T**ransport **L**ayer **S**ecurity (Authentifizierungsverfahren)
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
Heilberufsausweis (HBA)	Personenbezogener Ausweis im Gesundheitswesen. Er beinhaltet die Dienste Authentifizierung, Verschlüsselung sowie elektronische Signatur und ermöglicht den Zugriff auf Daten der eGK.
IPsec	**I**nternet **P**rotocol **sec**urity für VPN-Verbindung

Abkürzung/ Begriff	Bedeutung
JSON	Die **J**ava **S**cript **O**bject **N**otation ist ein kompaktes Datenformat in einer einfach lesbaren Textform zum Datenaustausch zwischen Anwendungen.
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)
Leistungserbringer	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)

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.
TSL	**T**rust-service **S**tatus **L**ist: Liste zur Prüfung der Zertifikate auf Vertrauenswürdigkeit.

Abkürzung/ Begriff	Bedeutung
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

39 Literatur

[1]

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1, Revision 5, 2017.

Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, 2017.

Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, 2017.

[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

40 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**