eHealth PIN-Pad PP-1516

Handbuch

64410179-02, DE, © Nov 2023 (PP-1516)

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 PIN-Pad PP-1516** wurde für die Verwendung mit einem **CHERRY eHealth Terminal ST-1506** 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
- Klare Trennung von Patient und medizinischem Fachpersonal
- Praktischer Betrieb ohne Netzteil via USB
- (Vorbereitet) Lesen und Schreiben von kontaktlosen Karten durch 2 NFC-Schnittstellen (Rückseite und Display)
- (Vorbereitet) Kamerabasierter 5MP 2D-Barcodescanner zum Scannen von Datamatrix- und QR-Codes (z. B. eRezept)
- Flexible Geräteausrichtung: 1. liegend oder 2. stehend als Wandmontage bedienbar

HINWEIS: Achten Sie bei der Position der Wandmontage darauf, dass das PIN-Pad vor unbeabsichtigten Stößen geschützt ist.

Die Bedienung und Konfiguration des Geräts ist intuitiv 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 **PP-1516**.

Ihr CHERRY Team

Zu diesem Handbuch

Dieses Handbuch enthält Handlungsabläufe und Informationen für Beschäftigte im deutschen Gesundheitswesen und für Administratoren zur Installation, Inbetriebnahme, Konfiguration und zum sicheren Betrieb des **PP-1516**.

Für neuere Firmwareversionen kann der Inhalt abweichen. Die aktuellste Version des Handbuchs finden Sie unter **https://www.cherry.de/eHealth/downloads/pp-1516**.

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

Lieferumfang

Der Lieferumfang des **eHealth PIN-Pads PP-1516** enthält:

- PIN-Pad PP-1516
- USB-Kabel
- Handbuch

SICHERHEIT

1 Bestellung und sichere Auslieferung

1.1 Sichere Lieferkette prüfen

Das **PP-1516** 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.

2 Prüfen Sie vor dem Auspacken die Sicherheitsmerkmale der Verpackung (siehe 1.2 "Sicherheitsmerkmale der Verpackung prüfen").

3 Prüfen Sie die Echtheit des Geräts, indem Sie unter **https://www.cherry.de/eHealth** oder über die Supporthotline die Seriennummer der Versiegelung der Verpackung (siehe 1.2 "Sicherheitsmerkmale der Verpackung prüfen") sowie die Seriennummer und die MAC-Adresse vom Typenschild des **PP-1516** angeben. Sie erhalten als Rückmeldung, ob es sich um ein sicher ausgeliefertes Originalprodukt handelt.

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

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

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

1.2 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 PIN-Pad **PP-1516** 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 **PP-1516** 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 1.1 "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:

2 Sicherheitsfunktionen

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

2.1 Sicheres Firmware-Update

Das PIN-Pad prüft die Integrität und Authentizität jeder neu zu installierenden Firmware. Es wird nur eine unveränderte, integere, korrekt und vollständig in das PIN-Pad 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 21 "Firmware aktualisieren".

2.2 Firmware auf Manipulation prüfen

Die Originalität der Firmware wird bei jedem Start des PIN-Pads 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 PIN-Pads durch. Wird die Meldung weiterhin angezeigt, kann und darf es nicht weiter verwendet werden

2.3 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 PIN-Pads somit nicht änderbar.
- Berechtigungen:
  - Anzeige- und Akustikeinstellungen vornehmen
  - Eigendiagnosefunktionen ausführen
  - Aktuelle PIN-Pad-Konfiguration anzeigen (Verbindungsstatus, Firmwareversion, Hardware Version, Hersteller-ID, Produktkürzel, Produktversion, Produkttyp, 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 PIN-Pads.
- Bei der ersten Inbetriebnahme des PIN-Pads muss der Administrator eine persönliche PIN festlegen (siehe 10 "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
  - PIN-Pad-Namen ändern
  - Pairing durchführen
  - Firmware-Updates einspielen
  - Trust-Service Status Liste (TSL) für Terminal aktualisieren

"Reset-Administrator"
Mit diesem Benutzerprofil kann das PIN-Pad wieder in den Auslieferungszustand zurückversetzt werden (Werksreset). Hierfür wird der Support von CHERRY benötigt (siehe 23 "Auf Werkseinstellungen zurücksetzen").

2.4 Management-Schnittstellen

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

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 PIN-Pad.
Die direkte Managementschnittstelle besteht aus dem Touchdisplay. Die Sicherheitsfunktion "Benutzerprofile und Authentifizierung" ermöglicht die Eingabe von Daten und die Ausgabe von Meldungen, Auswahlmöglichkeiten oder des Status.

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

INFO: Deaktivierte Einstellungen
Die Remote-Schnittstelle ist nach initialer Inbetriebnahme deaktiviert.

Folgende Funktionen sind nur lokal am PIN-Pad zugänglich:

- Pairing mit einem Terminal (siehe 11 "Pairing mit einem CHERRY eHealth Terminal")
- Aktivieren oder Deaktivieren der Remote-Schnittstelle (siehe 18 "Konfiguration über Remote-Schnittstelle")

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

2.5 Verschlüsselte Kommunikation

Das PIN-Pad kommuniziert ausschließlich über gesicherte, verschlüsselte Verbindungen (Ausnahme: Lokalisieren des PIN-Pads im Netzwerk).

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 PIN-Pads durch das Terminal.

Das Shared Secret wird während des Pairings mit einem Terminal erzeugt und gesichert im PIN-Pad abgelegt.

Sicherheitsrelevante Kommandos werden ausschließlich im vertrauenswürdigen Zustand ausgeführt.

2.6 Vertrauenswürdiges PIN-Pad

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

Der vertrauenswürdige Zustand des PIN-Pads über die sichere, verschlüsselte Verbindung mit einem gepairten Termnal wird im oberen Displaybereich durch das grüne USB-Symbol angezeigt (siehe 14 "Displaysymbole").

Beispielsweise können Kennwörter nicht ausgelesen werden und verlassen das Gerät nie im Klartext. Das PIN-Pad löscht eingegebene PINs und Kennwörter, kryptografische Schlüssel und alle Informationen aus gesteckten Karten und vom Terminal, 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
- Reset-Administrator
- CHERRY eHealth Terminal

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 1 "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 2 "Sicherheitsfunktionen").

4 Beachten Sie die allgemeinen Sicherheitshinweise (siehe 3 "Allgemeine Sicherheitshinweise").

5 Beachten Sie die Hinweise zur Einsatzumgebung (siehe 4 "Einsatzumgebung").

6 Identifizieren Sie das Produkt (siehe 5 "Gerät identifizieren").

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

8 Legen Sie die Administrator-PIN fest (siehe 10 "Administrator-PIN").

9 Installieren Sie das Gerät (siehe 9 "PIN-Pad anschließen").

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

11 Schalten Sie ggf. deaktivierte Einstellungen frei (siehe 17 "Lokale Konfiguration über direkte Managementschnittstelle" oder 18 "Konfiguration über Remote-Schnittstelle"). Folgende Einstellung ist nach Erstinbetriebnahme deaktiviert:
   - Remote-Zugang über Remote-Schnittstelle

12 Führen Sie das Pairing mit einem Terminal durch (siehe 11 "Pairing mit einem CHERRY eHealth Terminal").

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

3 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 Terminal. Das Terminal prüft periodisch den Pairingstatus und gibt ggf. eine Warnung aus.

4 Einsatzumgebung

Das PIN-Pad **PP-1516** ist für den stationären Einsatz in einer kontrollierten Umgebung konzipiert. Es ist zur Anbindung an ein CHERRY eHealth Terminal 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 PIN-Pads ist der Administrator zusammen mit dem Leistungserbringer verantwortlich.

- Das PIN-Pad 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 PIN-Pad haben.

- Das Gerät darf niemals unbeaufsichtigt bleiben.
- Falls es unbeaufsichtigt ist, muss sichergestellt werden, dass das Gerät in einem geschützten Bereich aufbewahrt wird. In diesem Fall muss das PIN-Pad 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, das Anschlusskabel und die Versiegelungen (Seriennummer auf Gehäusesiegel). 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.:
  - Abhörelektronik am Gerät oder in der Nähe (z. B. ein Richtmikrofon in bis zu 1 m Abstand)
  - Kameras, die auf das PIN-Pad gerichtet sind
- Bei Verdacht auf Manipulationen am Gerät wenden Sie sich an Ihren Gerätelieferanten.

HINWEIS: Manipulation oder Diebstahl des PIN-Pads

Bei einem Manipulationsverdacht oder Diebstahl des PIN-Pads:

- Löschen Sie sofort das Pairing des PIN-Pads im Terminal.

5 Gerät identifizieren

Prüfen Sie vor der Inbetriebnahme des Geräts, ob es sich um eine zugelassene 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 17.2 "Menü "Einstellungen" (Benutzer)").

3 Verwenden Sie das Gerät nur, wenn es sich um die folgende Variante handelt:

- Artikelnummer: PP-1516 UHZ
  Hardwareversion: 1.0.0
  Firmwareversion: die offizielle Version finden Sie unter: https://www.cherry.de/eHealth/downloads/pp-1516

6 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.

7 Versiegelung prüfen

7.1 Gehäuseversiegelung prüfen

Das PIN-Pad verfügt 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 PIN-Pads und vor jedem Pairing, ob die Siegel verletzt oder ausgetauscht wurden.

HINWEIS: Verdacht auf Manipulation

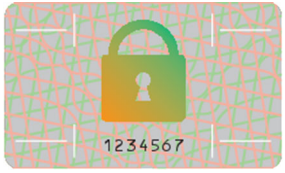
Bei verletztem, getauschtem oder fehlendem Siegel(n) ist das Gerät möglicherweise kompromittiert und nicht mehr sicher.

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

7.2 Positionen der Gehäusesiegel

7.3 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 ist ein Schlosssymbol 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 254 nm und 365 nm der Schriftzug "Security" sichtbar.

Siegel nach Ablöseversuch

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

8 Anschlüsse

USB-C Device

- Über diese Schnittstelle kann das PIN-Pad mit einem Terminal verbunden werden.
- Optional kann das PIN-Pad über diese Schnittstelle auch mit einem Host-PC verbunden werden.

9 PIN-Pad anschließen

9.1 PIN-Pad direkt mit dem CHERRY eHealth Terminal verbinden

Das PIN-Pad kann ausschließlich in Verbindung mit einem CHERRY eHealth Terminal betrieben werden.

1 Verbinden Sie das PIN-Pad mit der USB-A Host Schnittstelle des Terminals.
2 Aktivieren Sie die PIN-Pad Option im Terminal.

9.2 PIN-Pad ein- und ausschalten

Das PIN-Pad besitzt keinen Schalter. Wenn eine aktive USB-Verbindung vorhanden ist, ist es automatisch eingeschaltet. Um das PIN-Pad auszuschalten, trennen Sie die USB-Verbindung.

9.3 PIN-Pad über den PC mit dem CHERRY eHealth Terminal verbinden

Sollten Sie kein Terminal in der Nähe des PIN-Pads haben, so kann das PIN-Pad auch optional über einen PC betrieben werden. Hierbei nutzt das PIN-Pad die Netzwerkschnittstelle des PCs und es wird über das Netzwerk eine Verbindung zum Terminal aufgebaut. Schließen Sie hierfür das PIN-Pad 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 PIN-Pad direkt am USB-Anschluss des PCs an, verwenden Sie keinen USB-Hub.

   Das PIN-Pad 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 PIN-Pad unter **Admin-Menü > Verbindung > USB Ethernet** konfigurieren.

3 Erstellen Sie anhand der folgenden Schritte eine Netzwerkbrücke zwischen dem USB-Netzwerkadapter des PIN-Pads 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 PIN-Pads.
  - Klicken Sie mit der rechten Maustaste auf den Netzwerkadapter (RNDIS oder CDC-ECM) des PIN-Pads.
    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 PIN-Pad im selben Netzwerk des PCs als eigenständiges Netzwerkgerät betrieben werden. Dem PIN-Pad kann eine eigene IP-Adresse zugewiesen werden.
5 Für Informationen zum Anschluss des PIN-Pads unter weiteren Betriebssystemen, besuchen Sie unsere Homepage: **https://www.cherry.de/eHealth**.
6 Aktivieren Sie die PIN-Pad Option im Terminal.

10 Administrator-PIN

10.1 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 beide Managementschnittstellen gleich: **direkter Zugang** am PIN-Pad und **Remote-Schnittstelle**. Jede Managementschnittstelle besitzt eine separate PIN-Verwaltung.

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

10.2 PIN ändern

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

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

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

10.3 PIN falsch oder vergessen

Ab der 3. Fehleingabe der PIN wird die jeweilige Managementschnittstelle zeitweise gesperrt (direkter Zugang, Remote-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 PIN-Pads wieder auf den Ausgangswert zurückgesetzt.
- Der Stand des Fehlerzählers am direkten Zugang wird bei einem Zugriffsversuch auf einen gesperrten Menübereich lokal am PIN-Pad angezeigt.
- Der Stand der Fehlerzähler für die 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 PIN-Pads auf Werkseinstellungen zurückgesetzt werden. Dabei werden auch die Fehlerzähler aller Zugänge auf Null gesetzt. Siehe 23 "Auf Werkseinstellungen zurücksetzen".

11 Pairing mit einem CHERRY eHealth Terminal

Falls nötig, konfigurieren Sie das PIN-Pad, bevor Sie das Pairing mit einem Terminal durchführen.

Durch das Pairing können sich PIN-Pad und Terminal gegenseitig authentifizieren und eine Verbindung aufbauen.

HINWEIS: Zugang unautorisierter Dritter zum PIN-Pad oder Terminal

- Stellen Sie sicher, dass das PIN-Pad und das Terminal während des Pairing-Prozesses in Ihrer organisatorischen Hoheit stehen.
- Unautorisierte Dritte dürfen während des Pairings keinen Zugang zum PIN-Pad oder zum Terminal erlangen.

Pairing bezeichnet das Verfahren, dem PIN-Pad eine vom Terminal erzeugte digitale Kennung zu übergeben. Diese Kennung ist ein Shared Secret zwischen PIN-Pad und Terminal.

Das Pairing dient grundsätzlich als Sicherung gegen den unbemerkten Austausch von PIN-Pads. Dazu wird die Identität des PIN-Pads an das Terminal gebunden.

Um die Verwaltung der PIN-Pads im Terminal zu vereinfachen, können Sie den PIN-Pad Namen ändern (siehe 20 "PIN-Pad Name ändern"). Er wird zum Terminal übertragen und kann in der PIN-Pad Verwaltung des Terminals im Sinne eines Friendly Name verwendet werden.

Das PIN-Pad besitzt einen Pairingblock und kann somit nur mit einem Terminal bekannt gemacht werden. Zeitgleiche Verbindungen mit verschiedenen Terminals sind nicht möglich.

1 Wählen Sie in der PIN-Pad Verwaltung des Terminals das entsprechende PIN-Pad aus, mit dem Sie das Terminal pairen wollen, und starten Sie den Pairingvorgang.

   Das PIN-Pad zeigt eine Display-Meldung an.

2 Geben Sie zur Bestätigung des Pairings am PIN-Pad die Admin-PIN des PIN-Pads ein.

   Der öffentliche Schlüssel (Public Key) des Terminalzertifikats wird im PIN-Pad gespeichert.

Sobald das PIN-Pad mit einem Terminal gepairt ist, können die Pairinginformationen im PIN-Pad unter **Admin-Menü > Pairing** eingesehen werden.

Das PIN-Pad prüft bei jedem Verbindungsaufbau, ob es sich um ein betriebszugelassenes, d. h. vertrauenswürdiges Terminal handelt. Dazu enthält das PIN-Pad eine Trust-Service Status Liste für zugelassene PIN-Pads (siehe 22 "Trust-Service Status Liste (TSL) aktualisieren").

TIPP: Authentifizierung des Terminals

Falls das bei Ihnen eingesetzte Terminal nicht authentifiziert werden kann:

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

BEDIENUNG

12 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 PIN-Pad keine Aufkleber oder Notizzettel an.
5 Sorgen Sie dafür, dass das Personal mit den Sicherheitsvorkehrungen, die zum Schutz des PIN-Pads 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.

13 Navigation

13.1 Funktion der Displaybuttons

Funktion	Displaybutton
Aufruf des Menüs	Menü
zurück zur letzten Menü-seite	
Menü komplett verlas-sen	
Vorgang abbrechen	X
Vorgang bestätigen	OK
letzten Eingabe löschen	
Tastenfeld einblenden	
Tastenfeld ausblenden	

14 Displaysymbole

Symbole für Kommunikationsverbindung über USB

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

15 Duplizierte Terminalfunktionen

Im aktiven Zustand werden folgende Terminal-funktionen an das angeschlossene PIN-Pad zur Bearbeitung weitergeleitet:

- Ein- und Ausgaben
- Bestätigungsanforderungen
- PIN-Eingabe für entsprechend konfigurierte Kartenslots am Terminal

16 Eigendiagnose

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

- Integrität
- Buzzer

Siehe 17.1 "Mögliche Einstellungen im Menü".

Wenn Sie 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.

17 Lokale Konfiguration über direkte Managementschnittstelle

Folgende Funktionen sind nur lokal am Gerät zugänglich:

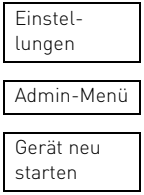
- Pairing mit einem Terminal (siehe 11 "Pairing mit einem CHERRY eHealth Terminal")
- Aktivieren oder Deaktivieren der Remote-Schnittstelle (siehe 18 "Konfiguration über Remote-Schnittstelle")

17.1 Mögliche Einstellungen im Menü

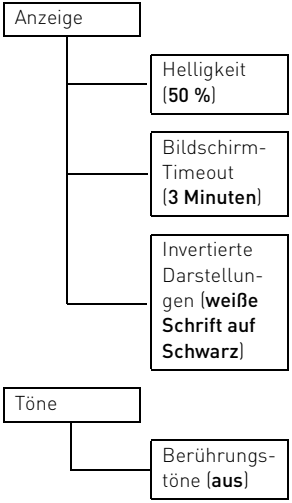
- Um in das Hauptmenü zu gelangen, drücken Sie auf die Taste **Menü**.

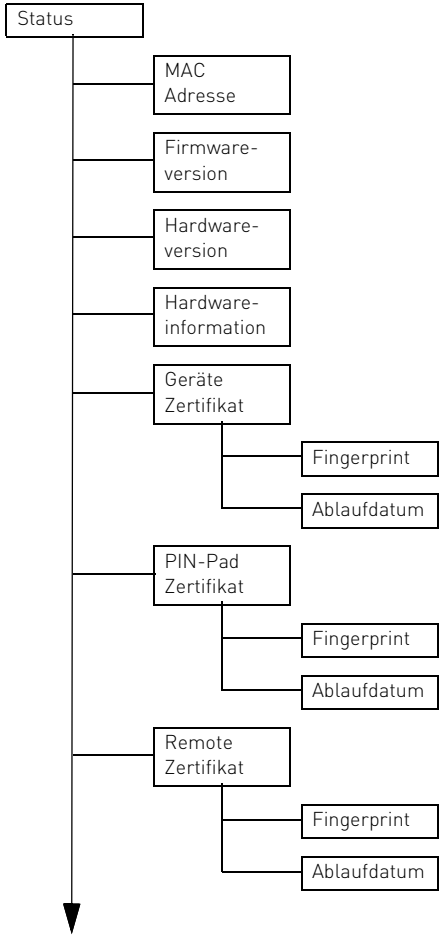
Fett = Werkseinstellungen

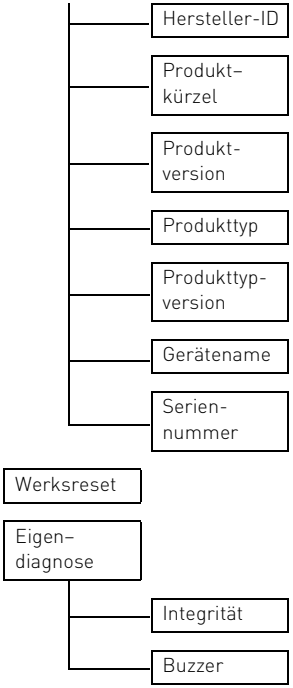
Sie können die auf den folgenden Seiten dargestellten Einstellungen vornehmen:



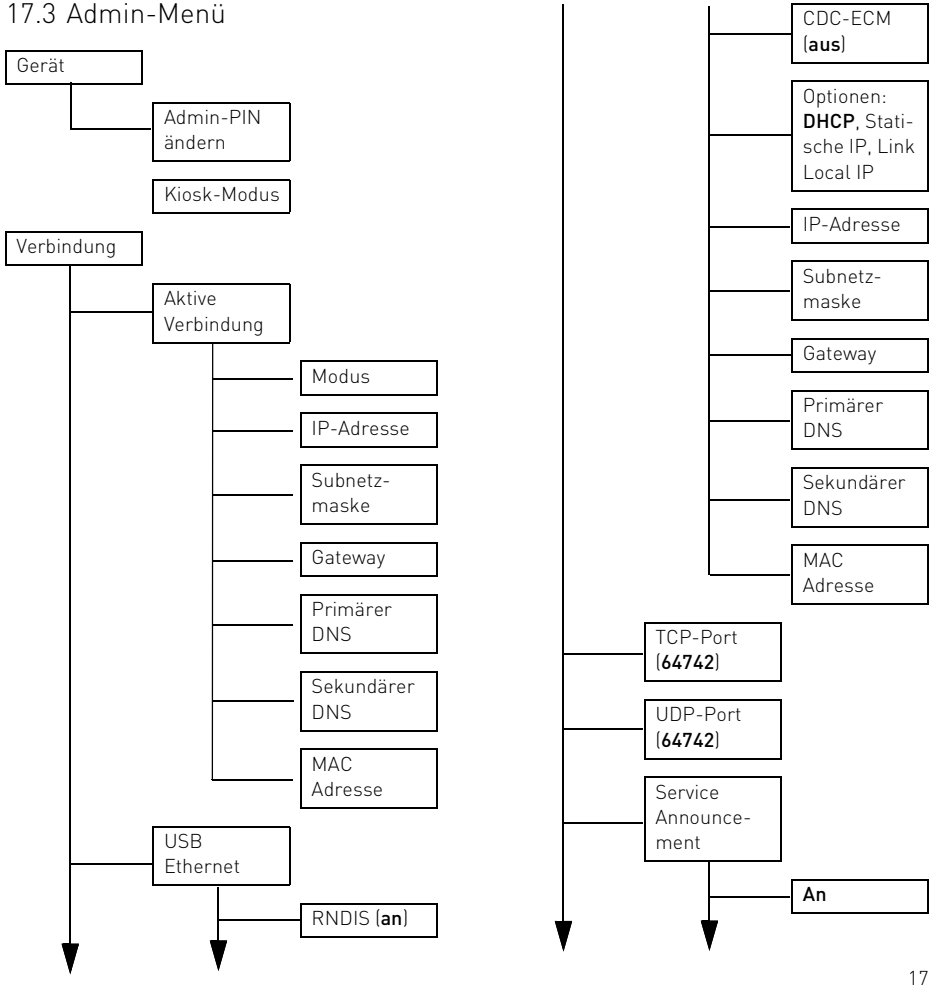
17.2 Menü "Einstellungen" (Benutzer)

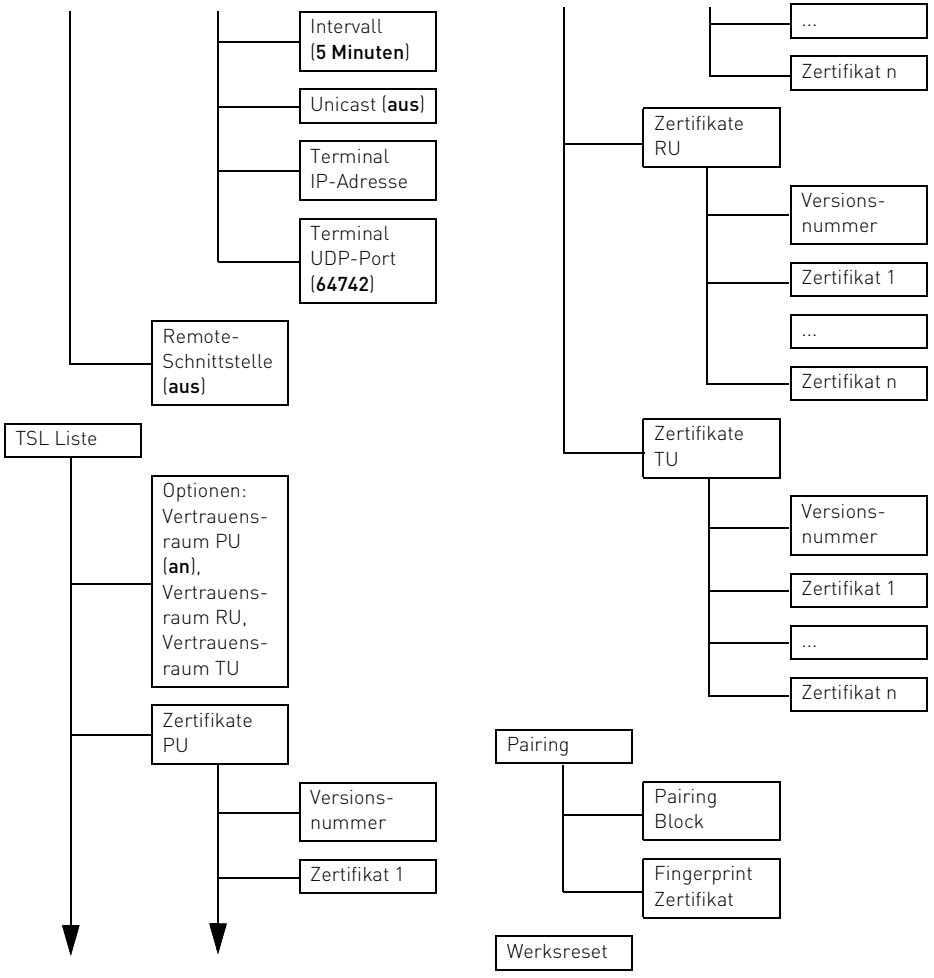






17.3 Admin-Menü





18 Konfiguration über Remote-Schnittstelle

Das PIN-Pad 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 Terminal (siehe 11 "Pairing mit einem CHERRY eHealth Terminal")
- Aktivieren oder Deaktivieren der Remote-Schnittstelle

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

- Die Remote-Schnittstelle wurde lokal am PIN-Pad aktiviert (Standard = Aus). Umstellung unter **Admin-Menü > Verbindung > Remote-Schnittstelle > Ein**.

- Wird das PIN-Pad direkt am eHealth Terminal betrieben, so muss für den Zugriff die IP-Adresse des Terminals mit Port 60443 verwendet werden, z. B.:
  https://192.168.1.199:60443.
- Wird das PIN-Pad an einem PC betrieben, so muss je nach Konfiguration die IP-Adresse des PCs oder des PIN-Pads mit Port 443 verwendet werden, z. B.:
  https://192.168.1.199:443.
- Ab Werk ist im PIN-Pad Link Local aktiviert, d. h. die automatische Zuweisung einer freien IP-Adresse. Sie erhalten die IP-Adresse am PIN-Pad 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 entsprechende IP-Adresse mit Port ein, z. B.:
https://192.168.1.199:443.

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

  Die **Anmeldefläche des PIN-Pads** erscheint im Browser.

TIPP: Falls die Anmeldefläche nicht im Browser erscheint:

Für die sichere TLS-Verbindung zum Browser wird das im PIN-Pad hinterlegte Herstellerzertifikat verwendet. Da der Browser dieses Zertifikat nicht selbst überprüfen kann, wird die Meldung "Dieser Verbindung wird nicht vertraut" angezeigt.

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 10 "Administrator-PIN").

3 Folgen Sie den Anweisungen auf dem Bildschirm.

Der Aufbau des Menüs an der Webschnittstelle entspricht der direkten Benutzerschnittstelle (siehe 17 "Lokale Konfiguration über direkte Managementschnittstelle"). Informationen zur Parametrierung sind beim jeweiligen Menüpunkt hinterlegt.

19 Kiosk-Modus

Bei aktivem Kiosk-Modus wird der Menü Button zum Aufruf des Menüs deaktiviert und ausgeblendet, so dass ein Aufruf des lokalen Menüs nicht mehr möglich ist.

Sollte dennoch ein Zugriff auf das lokale Admin Menü zur Konfiguration oder Deaktivierung des Kiosk-Modus nötig sein, kann dieses über einen Fallback-Mechanismus aufgerufen werden. Hierbei ist das Terminaldisplay in 4 gleiche Zonen aufgeteilt, Zone 1 oben links, Zone 2 unten links, Zone 3 oben rechts, Zone 4 unten rechts. Ist der Kiosk-Modus aktiviert und befindet sich das Terminal im Startbildschirm, kann das Admin-Menü aufgerufen werden, indem die Zonen in der folgenden Reihenfolge 1, 2, 3, 4 innerhalb eines Zeitraums vom 5 Sekunden gedrückt werden. Der Countdown beginnt mit dem Drücken der Zone 1. Nachdem alle vier Zonen in der richtigen Reihenfolge innerhalb der vorgegebenen Zeit gedrückt wurden, erscheint die Eingabeaufforderung der Admin-PIN, um in das Admin Menü zu gelangen.

20 PIN-Pad Name ändern

Um die Verwaltung zu vereinfachen, können Sie den PIN-Pad Namen bei der Inbetriebnahme des PIN-Pads über die Remote-Schnittstelle verändern (siehe 18 "Konfiguration über Remote-Schnittstelle"). Er wird zum Terminal übertragen und kann im Verwaltungsmenü des Terminals im Sinne eines Friendly Name verwendet werden.

Der PIN-Pad Name muss folgende Kriterien erfüllen:

- Der PIN-Pad Name 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: Probleme bei der Anzeige im Terminal

Entspricht der PIN-Pad Name nicht der vorgegebenen Konvention, kann es vorkommen, dass das Terminal den PIN-Pad Namen nicht richtig auflösen kann und somit das PIN-Pad nicht findet bzw. anzeigt.

21 Firmware aktualisieren

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

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

HINWEIS: Abbruch des Firmware-Updates

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

- Trennen Sie das PIN-Pad nach der Installation für 5 Minuten nicht von der Stromversorgung. Wird innerhalb dieser Zeit das Terminal dreimal neu gestartet, 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 PIN-Pad im Menü **Einstellungen > Status**, ob die gewünschte Firmwareversion angezeigt wird.

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

Firmware-Aktualisierung über File Upload

1. Öffnen Sie in Ihrem Browser die Remote-Schnittstelle (siehe 18 "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**.

Firmware-Aktualisierung über HTTP Server Download

1. Öffnen Sie in Ihrem Browser die Remote-Schnittstelle (siehe 18 "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**.

22 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 Listen werden vom Hersteller in Form einer signierten Datei zum Download angeboten.

Die aktuellen TSL finden Sie auf https://www.cherry.de/eHealth.

TSL-Aktualisierung über File Upload

1 Öffnen Sie in Ihrem Browser die Remote-Schnittstelle (siehe 18 "Konfiguration über Remote-Schnittstelle").
2 Wählen Sie **Konfiguration**.
3 Klicken Sie auf die Schaltfläche **Durchsuchen...** und wählen Sie die TSL-Update-Datei aus.
4 Klicken Sie auf **Aktualisieren**.

TSL-Aktualisierung über HTTP Server Download

1 Öffnen Sie in Ihrem Browser die Remote-Schnittstelle (siehe 18 "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**.

TIPP: Authentifizierung des Terminals

Falls das bei Ihnen eingesetzte Terminal nicht authentifiziert werden kann:

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

23 Auf Werkseinstellungen zurücksetzen

Durch den Werksreset wird der Auslieferungszustand des Geräts wieder hergestellt (mit Ausnahme der Firmware). 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

24 Pairing-Informationen löschen

HINWEIS: Weitergabe von Pairing-Informationen

- Führen Sie vor der Außerbetriebnahme einen Werksreset durch (siehe 23 "Auf Werkseinstellungen zurücksetzen". Hierbei werden alle kritischen Informationen im Gerät gelöscht.

25 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

26 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 PIN-Pads.
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.

Meldung	Bedeutung
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.
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.

27 PIN-Pad 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 Scheuermittel oder Scheuerschwämme und beachten Sie die Hinweise im Dokument "CHERRY eHealth Kartenterminal ST-1506 Desinfektionsmittel", unter **https://www.cherry.de/eHealth/downloads/st-1506**.
- Verhindern Sie, dass Reinigungsmittel in Kontakt mit den Siegeln geraten.
- Verhindern Sie, dass Flüssigkeit in das Gerät gelangt.

28 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
- Verwendetes Terminal (Hersteller, Firmwareversion, Hardwareversion)

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

29 Technische Daten

Bezeichnung	Wert
Systemvoraussetzungen	USB Anschluss, CHERRY eHealth Terminal
Display	Graphisches Display (5,0 Zoll (= 12,7cm) IPS 720 x 1280 Pixel)
Anschluss	USB-C
Software-Schnittstellen	RNDIS, CDC-ECM

Bezeichnung	Wert
Internet-Protokolle	IPv4
Stromversorgung	USB-C (5 V)
Stromaufnahme	5 V USB-C: max. 1000 mA
Lagertemperatur	–20 °C bis +65 °C
Betriebs-temperatur	0 °C bis +50 °C

30 Abkürzungen und Begriffserklärungen

Abkürzung/ Begriff	Bedeutung
Administrator (bzw. Admin)	Verwalter des Systems. Er nimmt das System oder Teile davon in Betrieb und betreut es während der Produktlebensdauer.
Benutzer	Endanwender bzw. Nutzer des Geräts, mit eingeschränkten Rechten zur Systemverwaltung
BSI	**B**undesamt für **S**icherheit in der **I**nformationstechnik
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)
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	gematik-zugelassenes Kartenlesegerät zur Verwendung im deutschen Gesundheitswesen
gematik	Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (**www.gematik.de**)
Heilberufsausweis (HBA)	Personenbezogener Ausweis im Gesundheitswesen. Er beinhaltet die Dienste Authentifizierung, Verschlüsselung sowie elektronische Signatur und ermöglicht den Zugriff auf Daten der eGK.
JSON	Die **J**ava**S**cript **O**bject **N**otation ist ein kompaktes Datenformat in einer einfach lesbaren Textform zum Datenaustausch zwischen Anwendungen.
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)
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-C Device	USB Gerät mit Stecker Typ-C
USB-C Host	USB Host mit Buchse oder Stecker Typ-C

31 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/pp-1516**.

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