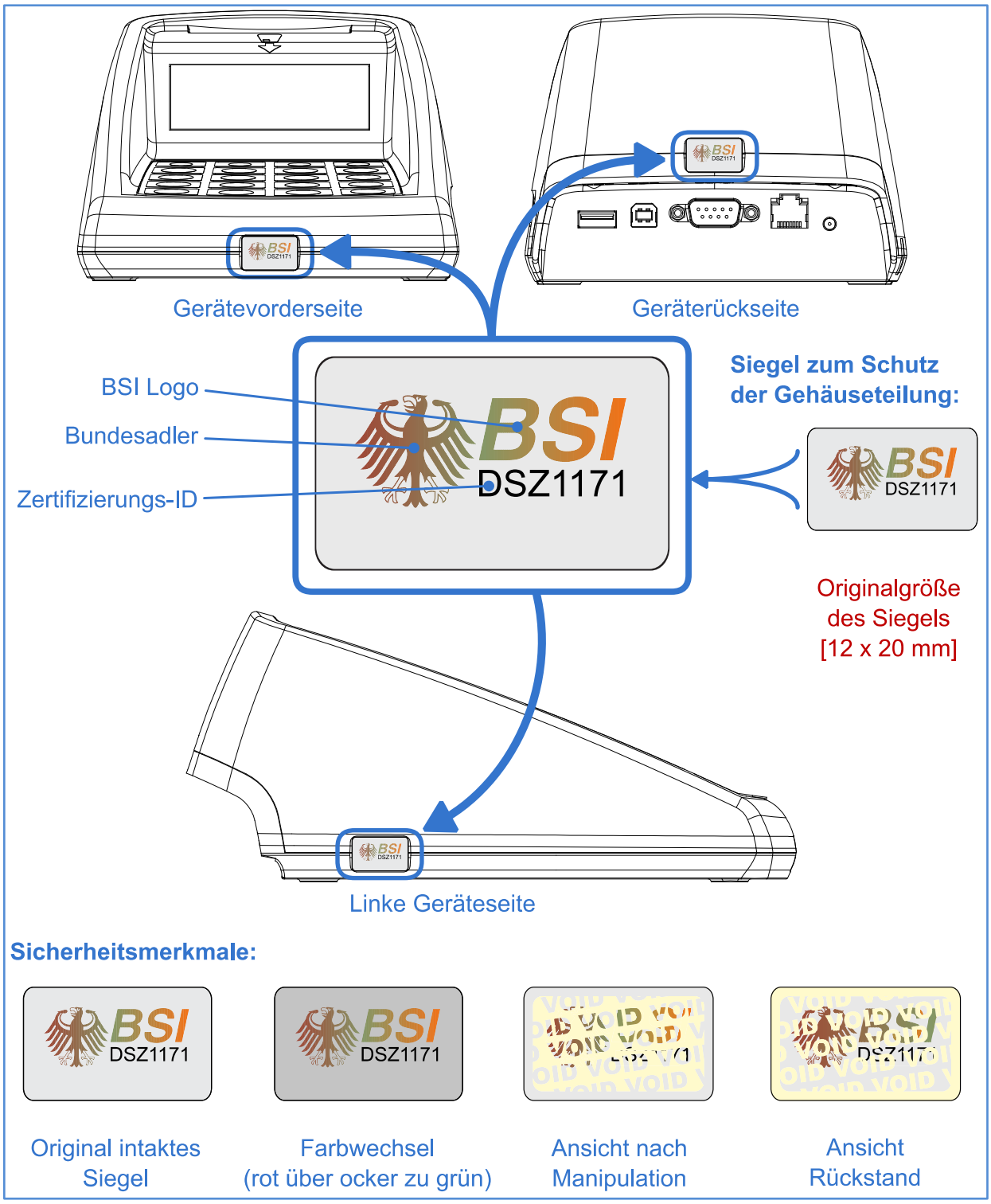
GT German Telematics GmbH

Kartenterminal eHealth GT900 –Benutzerhandbuch–

Version 2.1.4 / Deutsch



Bitte führen Sie vor jeder Nutzung des Kartenterminals eine Sichtprüfung des Gehäuses, der Siegel und des Netzteils auf Unversehrtheit durch! Das Gehäuse ist derart aufgebaut, dass die Siegel beim Öffnen zerstört werden. Dadurch können Eingriffe und Manipulationen am Gerät leichter erkannt werden. Lesen Sie hierzu auch die Hinweise in Kapitel 1.3 „Sicherheitskonzept des Terminals“.

Das vorliegende Benutzerhandbuch gilt für alle Kartenterminals eHealth GT900 mit der Firmware-Version 2.0.1. Angaben zur Firmware-Version finden Sie über die Menüsteuerung des Terminals (siehe vorliegendes Handbuch Kapitel 4.11.1) sowie für die Hardware auf dem Typenschild an der Unterseite des Gerätes.

Der Hersteller des Chipkarten-terminals erklärt hiermit die Konformität des Gerätes mit den von der "Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH" (gematik) vorgegebenen Richtlinien zum Aufbau einer Telematikinfrastruktur für das deutsche Gesundheitswesen. Das Kartenterminal eHealth GT900 wurde speziell für die elektronische Gesundheitskarte entwickelt und erfüllt alle Anforderungen für den sicheren Umgang mit schutzwürdigen Daten. Es wird Sie als Nutzer zuverlässig beim Umgang mit den für die Telematikinfrastruktur vorgesehenen Chipkarten (KVK, eGK, HBA, SMC-B, gSMC-KT, Standardsignaturkarten) unterstützen. Das Ihnen vorliegende Gerät ist von der gematik GmbH bis auf Widerruf* für die Benutzung innerhalb der Telematikinfrastruktur für das deutsche Gesundheitswesen zugelassen.

Benutzerhandbuch Identifikation:

Titel:

Kartenterminal
eHealth GT900
Benutzerhandbuch

Handbuchversion:

2.1.4

Ausgabedatum:

21.11.2022

Hersteller:

gt german telematics gesellschaft
für telematikdienste
Libellenstraße 9
14129 Berlin

*Widerruf - In ihrer Funktion als Zulassungsstelle kann die gematik Zulassungen widerrufen, wenn die Zulassung auf nicht mehr gegebenen Voraussetzungen (Geräteeigenschaften, Rahmenbedingungen) beruht, neue sicherheitstechnische Erkenntnisse vorliegen oder gravierende Änderungen an den Prüfspezifikationen notwendig waren. Im Fall des Widerrufs einer Zulassung einer Komponente informiert die gematik den Antragsteller unter Angabe von Gründen und verpflichtet ihn, die Zulassungsurkunde an die gematik zurückzugeben. Die Eintragung der betroffenen Komponente in der Liste erfolgter Zulassungen wird von der gematik gelöscht.

Inhaltsverzeichnis

Rollenzuordnung

Im Folgenden wird eine Rollenzuordnung der einzelnen Kapitel dieses Handbuchs vorgenommen. Weitere Informationen zu den Rollen finden Sie in Kapitel 1.6 „Betriebsmodi“.

Administrator

Alle Kapitel dieses Handbuchs sind für Geräteadministratoren relevant.

Benutzer

Die folgenden Kapitel sind für normale Benutzer (Leistungserbringer bzw. berechtigte Personen) des Gerätes bestimmt:

- Kapitel 1 „Sicherheitshinweise und allgemeine Informationen” (S. 8)
- Kapitel 1.3 „Sicherheitskonzept des Terminals“ (S. 13)
- Kapitel 1.8 „Ein- und Ausschalten des Kartenterminals“ (S. 26)
- Kapitel 1.9 „Reinigen und Desinfizieren des Gerätes“ (S. 26)
- Das gesamte Kapitel 2 „Bedienelemente“ (S. 28)
- Kapitel 3.2 „Eingabe einer Karten-PIN“ (S. 42)
- Das gesamte Kapitel 7 „Qualifizierte elektronische Signaturen“ (S. 99)
- Das gesamte Kapitel 8 „Problembehebung“ (S. 100)

Reset-Administrator

Die folgenden Kapitel sind für einen Reset-Administrator (Person mit Kenntnis der PUK oder des Resetcodes zur Durchführung eines Werksresets) relevant:

- Kapitel 1 „Sicherheitshinweise und allgemeine Informationen” (S. 8)
- Kapitel 1.7.2 „Setzen des PUK“ (S. 23)
- Kapitel 5 „Gerät zurücksetzen“ (S. 84) und hier insbesondere Kapitel 5.2 „Zurücksetzen ohne Kenntnis der Admin PIN“ (S. 86)

1 Sicherheitshinweise und allgemeine Informationen

Lesen, beachten und befolgen Sie bitte alle Sicherheitshinweise, die in dieser Bedienungsanleitung genannt werden! Bewahren Sie die Sicherheitshinweise auf. Beachten Sie zudem bitte alle Warnungen, die sich auf dem Gerät befinden und in der Bedienungsanleitung enthalten sind. Um einen sicheren Betrieb Ihres Kartenterminals zu gewährleisten, beachten Sie unbedingt die folgenden Vorgaben:

- Lesen Sie vor Inbetriebnahme des Gerätes die Bedienungsanleitung sorgfältig durch.
- Bevor Sie mit der Installation und Inbetriebnahme des Gerätes und der erforderlichen Komponenten beginnen, versichern Sie sich der Unversehrtheit des Gerätes. Lesen Sie auch das Kapitel 1.1 „Sichere Lieferkette“ sorgfältig durch.
- Überprüfen Sie regelmäßig vor der Nutzung und nach Abwesenheit die Unversehrtheit des Gerätes (Prüfen der Sicherheitsmerkmale, insbesondere der Siegel). Beachten Sie dazu das Kapitel 1.3 „Sicherheitskonzept des Terminals“.
- Das Kartenterminal muss hinreichend vor Manipulation geschützt werden. Betreiben Sie das Gerät so, dass ein Missbrauch auszuschließen ist. Das Gerät unterstützt Sie dabei, indem es (nicht erkennbare) physische Manipulationen für einen Zeitraum von mindestens 10 Minuten verhindert.
- Das Kartenterminal eHealth GT900 führt alle sicherheitsrelevanten Aktionen ausschließlich in einem vertrauenswürdigen Zustand aus. Im vertrauenswürdigen Zustand befindet sich das eHealth-Kartenterminal in einem Modus, bei dem keine Beeinflussung und keine Informationsabschöpfung durch Komponenten (dazu zählt auch Software), welche nicht über eine Zulassung durch die gematik verfügen, möglich ist.

- Verschließen Sie das Gerät bei längerer Nichtnutzung (z.B. über Nacht) stets sicher vor dem Zugriff Unbefugter. Sorgen Sie dafür, dass ein Eindringen Unbefugter in die Einsatzumgebung erkannt wird!
- Schließen Sie das Produkt so an, wie es in der Bedienungsanleitung vorgegeben ist.
- Verwenden Sie für das Kartenterminal nur das mitgelieferte Netzteil und die beiliegenden Anschlusskabel.
- Halten Sie die Firmware des Kartenterminals sowie die zugehörigen Administrationsprogramme stets aktuell. Prüfen Sie dazu regelmäßig unsere Homepage unter https://www.germantelematics.de.
- Um qualifizierte Signaturen (QES) zu erstellen, müssen Sie das Gerät mit einem QES-fähigen Konnektor sowie einer vom Konnektor unterstützten Signaturkarte (eHBA) betreiben.
- PINs müssen stets unbeobachtet eingegeben werden. Die Eingabe einer PIN darf nur dann erfolgen, wenn das geschlossene Schlosssymbol anzeigt, dass eine PIN-Eingabe erwartet wird. Die PIN wird dann sicher an die Karte übertragen. Eine unverschlüsselte Übertragung der PIN an ein anderes Gerät findet so unter keinen Umständen statt.
- Lassen Sie das Gerät nicht fallen und setzen Sie das Gerät keinen heftigen Erschütterungen aus.
- Bedienen Sie die Tastatur nie mit spitzen oder scharfen Gegenständen wie beispielsweise einem Kugelschreiber oder Ähnlichem.
- Bringen Sie keine Magnete in unmittelbare Nähe des Gerätes.
- Achten Sie darauf, dass kein Staub, keine Gegenstände oder Flüssigkeiten in das Innere des Gerätes gelangen. Es besteht die Gefahr eines elektrischen Schlages beziehungsweise eines Kurzschlusses.
- Das Gerät ist nicht wasserfest. Tauchen Sie das Gerät nie in Wasser.

- Verwenden Sie für den Wiederversand und sonstigen Transport des Gerätes die Originalverpackung oder eine andere geeignete Verpackung, die Schutz gegen Stoß, Schlag, Feuchtigkeit und elektrostatische Entladung gewährt.
- Beachten Sie bei Außerbetriebnahme und Wiederversand des Gerätes das Kapitel 10 „Außerbetriebnahme, Rückversand und Entsorgung“.
- Bewahren Sie das Gerät außerhalb der Reichweite von Kindern auf.
- Angaben zur Version finden Sie für die Hardware auf dem Typenschild an der Unterseite des Gerätes sowie für die Firmware über die Menüsteuerung des Gerätes (s. Kapitel 4.11.1).
- Vergewissern Sie sich vor dem ersten Einlesen einer Versichertenkarte oder eHBA/SMC-B, dass diese Versionsangaben mit den Angaben zur Firmware- und Hardwareversion auf Seite 3 dieses Handbuches übereinstimmen.
- Neben der Hardware ist die Firmware ein sicherheitssensibles Element. Verwenden Sie aus diesem Grund nur zugelassene Firmware-Versionen. Spielen Sie eine neue Firmware ein, so kann der Vorgang nicht abgebrochen werden. Es ist nicht möglich, eine alte Vorgänger-Firmware-Version, die sich nicht in der Firmwaregruppe (Liste der zulässigen Firmware-Versionen) befindet, einzuspielen. Das Gerät prüft vor dem Anwenden der neuen Firmware, ob es sich um eine unveränderte, integere Version von german telematics handelt.
- Sorgen Sie für eine umweltgerechte Entsorgung des eHealth GT900 Kartenterminals, wenn dieses endgültig nicht mehr benutzt werden soll. Lesen Sie hierzu auch die Hinweise in Kapitel 10 „Außerbetriebnahme, Rückversand und Entsorgung“.

1.1 Sichere Lieferkette

Ihr Kartenterminal wird von german telematics auf einem sicheren Lieferweg an Sie ausgeliefert. Um die Unversehrtheit des Kartenterminals beim Erreichen des endgültigen Aufstellungsortes, bspw. einer Arztpraxis, sicherzustellen, muss vor der Inbetriebnahme eine Überprüfung der Sendung durch Sie durchgeführt werden.

Das eHealth GT900 wird in einem verschlossenen und versiegelten Gerätekarton unter Einhaltung der sicheren Lieferkette geliefert. Alle an der Auslieferung des eHealth GT900 beteiligten Akteure erfüllen die strengen Anforderungen, deren Einhaltung für das sichere Einbringen des Gerätes in die Einsatzumgebung notwendig ist.

Bei Empfang der Ware müssen Sie den Gerätekarton auf Unversehrtheit prüfen.

Um Ihnen die Möglichkeit zu geben, den lückenlosen Lieferweg von uns bis zu Ihnen nachzuvollziehen, und so Manipulationen auszuschließen, haben wir auf unserer Internetseite unter https://www.germantelematics.de/sichere-lieferkette die **Checkliste Sichere Lieferkette Version 1.3.0** mit weiteren Informationen und Anweisungen hinterlegt.

Mit dieser Checkliste ist es Ihnen dann auch möglich die Unversehrtheit und Echtheit des Gerätekartons genau zu prüfen.

Sollten Sie begründete Zweifel an der Unversehrtheit und Echtheit der Sendung haben, folgen Sie den Anweisungen der **Checkliste Sichere Lieferkette Version 1.3.0**. Verständigen Sie den Verkäufer des Gerätes. Das Kartenterminal darf bei Verdacht auf Manipulationen nicht in Betrieb genommen werden!

1.2 Lieferumfang

Im Lieferumfang Ihres Gerätes sind enthalten:

- ein eHealth GT900 Kartenterminal
- ein GS (Geprüfte Sicherheit) zertifiziertes Netzteil (5V / 1200 mA)
- ein Ethernet-Kabel (2m)
- eine Kurzanleitung
- 4 SIM-Slotsiegel zur Versiegelung der SMC SIM-Slots. Bitte verwahren Sie diese Siegel bis zu Ihrer Verwendung an einem sicheren Ort[1] auf!
- Optional: Eine gSMC-KT [2] (gerätespezifische Security Module Card Kartenterminal)

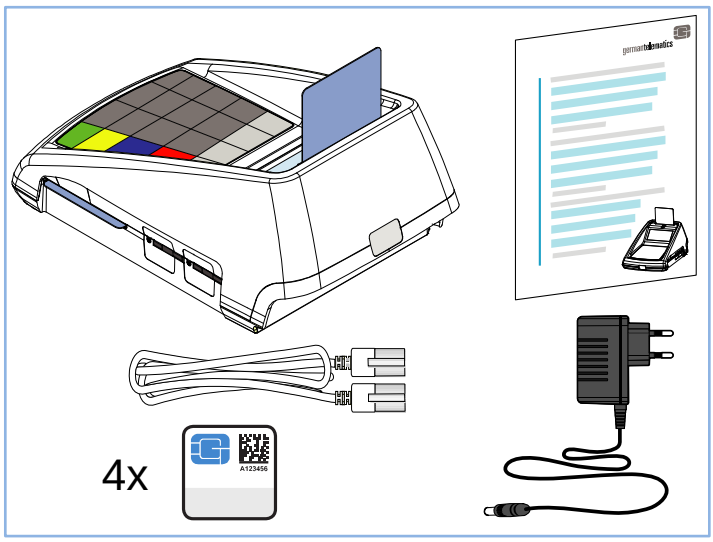


Abbildung 1: Lieferumfang

[1] Ein sicherer Ort ist dadurch gekennzeichnet, dass unbefugte Personen keinen Zugang dazu haben und das Eindringen unbefugter Personen erkannt wird. Dies kann beispielsweise ein verschließbares Schubfach oder ein Tresor sein.

[2] Eine gSMC-KT ist für den Betrieb Ihres Kartenterminals notwendig und bei Bedarf gesondert zu bestellen (wenn nicht bereits eine gültige gSMC-KT vorhanden ist).

1.3 Sicherheitskonzept des Terminals

Um Manipulationen am Gerät zu erkennen, prüfen Sie vor der Inbetriebnahme und danach regelmäßig, insbesondere nach längerer Abwesenheit (mehr als 10 Minuten) und bei jedem neuen Pairing-Prozess (s. Kapitel 3.1), das Gehäuse, alle Siegel und das Netzteil auf Unversehrtheit und Echtheit.

Sollten Sie begründete Zweifel an der Unversehrtheit und Echtheit des Gerätes haben, folgen Sie den Anweisungen der **Checkliste Sichere Lieferkette Version 1.3.0** (zu finden auf https://www.germantelematics.de/sichere-lieferkette). Verständigen Sie den Verkäufer des Gerätes. Das Kartenterminal darf bei Verdacht auf Manipulationen nicht in Betrieb genommen werden!

Das Terminal ist mit einem elektronischen Schutzmechanismus ausgestattet, um den Diebstahl geschützter Daten aus dem Terminal zu verhindern. Dieser Mechanismus ist mittels eingebauter Batterie auch dann aktiv, wenn das Terminal nicht an die Stromversorgung angeschlossen ist.

Um die eingebaute Batterie nicht unnötig zu belasten, sollten Sie das Terminal daher auch bei Nichtnutzung (beispielsweise über Nacht oder am Wochenende) nicht von der Stromversorgung trennen! Schalten Sie das Terminal immer gemäß Kapitel 1.8 „Ein- und Ausschalten des Kartenterminals“ aus und wieder ein.

1.3.1 Gehäuseprüfung

Das Gehäuse ist zweiteilig ausgeführt. Es besteht aus einer Ober- und einer Unterschale. Die Stoßkante der Gehäuseschalen befindet sich auf der Höhe der Siegel.

Vergewissern Sie sich, dass zwischen den Gehäusehälften der Ober- und Unterschale kein Spaltmaß vorhanden ist. Die Gehäusehälften sollen bündig aneinander liegen.

Prüfen Sie das Gehäuse auf sichtbare Manipulationen wie Bohrlöcher oder herausstehende Drähte. Entfernen Sie unbekannte Aufkleber, die eventuelle

Manipulationen verdecken! Kontrollieren Sie, dass das Gerätelabel auf der Geräteunterseite unversehrt ist und glattflächig auf der Klebefläche aufliegt.

Bei Manipulationsverdacht benachrichtigen Sie den Administrator, um die Angaben auf dem Aufkleber mit dem aufbewahrten Begleitdokument zu vergleichen.

1.3.2 Siegelprüfung

Um Ihr Kartenterminal vor elektrischer oder mechanischer Manipulation zu schützen, befindet sich jeweils auf der Vorder- und Rückseite sowie auf der linken Gehäuseseite ein Gehäusesiegel, welches ein Öffnen des Gerätes entlang der Gehäuseteilung sichtbar macht. Diese drei Siegel müssen vor jeder Benutzung des Gerätes durch eine Sichtprüfung auf Unversehrtheit kontrolliert werden. Die Echtheit der Siegel zum Schutz der Gehäuseteilung ist durch folgende Kennzeichen gegeben:

- Achten Sie auf irreversible Veränderungen an dem Siegel wie zum Beispiel:
  - Manipulationsbotschaft (siehe hierzu auch Umschlagsseite 2)
  - mechanische Beschädigung
- Achten Sie auf Farbveränderungen am Bundesadler und am BSI-Logo, durch Kippen kommt es zu einem Farbwechsel von Rot über Ocker zu Grün.

Sind bereits SIM-Karten im Terminal gesteckt, prüfen Sie auch das/die durch den Administrator aufgebrachte/n SIM-Slotsiegel an der Seite des Gerätes auf Unversehrtheit und lassen Sie bei Manipulationsverdacht die korrekte/n Siegelnummer/n durch den Administrator prüfen.

Ziehen Sie die Abbildung auf der Umschlagseite 2 (Gehäusesiegel) und auf Seite 35 (SIM-Slotsiegel) dieses Benutzerhandbuchs zu Rate, um die Lage, die Form und Größe sowie die Merkmale der Geräteversiegelung abzugleichen.

1.3.3 Netzteilprüfung

Abbildung 2: Detailansichten des Netzteils

Das GS (Geprüfte Sicherheit) zertifizierte Netzteil (5V / 1200 mA) besteht aus einem Steckergehäuse, einem Zuleitungskabel und einem gewinkelten Anschlussstecker.

Auf der Oberseite des Steckergehäuses ist das GT-Logo abgebildet. Durch einen Knickschutz ist das zweiadrige Zuleitungskabel ausgeführt und endet wiederum mit Knickschutz am gewinkelten Anschlussstecker.

Prüfen Sie anhand der Abbildung 2 die Merkmale des Netzteils insbesondere auf Veränderungen am Zuleitungskabel (z.B.: Beschädigungen, Verdickungen oder offene Leitungen), um Manipulationen und somit einen Angriffsversuch zu erkennen.

1.4 Aufstellungshinweise

Aus Gründen der Datensicherheit weisen wir darauf hin, dass das Kartenterminal nur in einem kontrollierten Bereich, wie zum Beispiel einer Arztpraxis oder vergleichbaren Räumlichkeiten, betrieben werden darf, sodass unbefugte Personen keine Manipulationen an dem Kartenterminal und daran angeschlossenen Systemeinheiten vornehmen können. Das Gerät muss darüber hinaus in einem Mindestabstand von 15 cm zu anderen Gegenständen (die von einem potentiellen Angreifer mit Abhörtechnik ausgestattet worden sein könnten) aufgestellt werden.

Das Gerät unterstützt Sie dabei, diese Sicherheitsrichtlinien umzusetzen, indem es (nicht erkennbare) physische Manipulationen für einen Zeitraum von mindestens 10 Minuten verhindert. Insbesondere bedeutet dies, dass sich das Gerät bei längerer Abwesenheit (auch nachts) in einem geschützten Bereich befinden muss, in welchem das Terminal durch seine Umgebung geschützt wird. Wenn aus irgendeinem Grund von diesen Vorschriften abgewichen wurde, ist das Terminal einer fachkundigen Prüfung durch den Administrator zu unterziehen (siehe Kapitel 1.3).

Stellen Sie das Gerät auf eine glatte Oberfläche. Achten Sie auf ein ordnungsgemäßes Anschließen aller benötigten Kabel (siehe Kapitel 1.5). Vergewissern Sie sich, dass das Gerät an seinem Aufstellungsort keiner übermäßigen Hitze (beispielsweise direkt unter einer Lampe) beziehungsweise Feuchtigkeit ausgesetzt ist.

Machen Sie sich bewusst, dass für regelmäßige Überprüfungen an den Siegeln ein leichter Zugang zum Gerät gewährleistet sein muss. Das Kartenterminal sollte zudem

Patienten zugänglich gemacht werden, wenn diese Eingaben an dem Gerät tätigen müssen.

1.5 Anschluss des Gerätes

Das eHealth GT900 Kartenterminal kann ausschließlich im Netzwerk in Verbindung mit einem Konnektor[3] genutzt werden. Das Gerät wird entweder über die Ethernet-LAN-Schnittstelle oder über USB an einem Windows PC mit dem Netzwerk verbunden werden.

Um das Gerät über eine **Ethernet-LAN-Schnittstelle** zu betreiben, stecken Sie das mitgelieferte Ethernet-Kabel in den dafür vorgesehenen Anschluss an ihrem Kartenterminal. In Abbildung 3 ist dieser Anschluss mit Position ④ gekennzeichnet. Das andere Ende stecken Sie in einen freien Ethernet-Anschluss an Ihrem Switch oder einer entsprechenden Netzwerkdose.

Um das Gerät über den **USB Typ B-Anschluss per RNDIS** mit einem Windows PC zu verbinden benötigen Sie ein USB-Gerätekabel (USB 2.0 Kabel A-Stecker, B-Stecker). Stecken den USB B-Stecker in den dafür vorgesehenen Anschluss an ihrem Kartenterminal. In Abbildung 3 ist dieser Anschluss mit Position ② gekennzeichnet. Das andere Ende stecken Sie in einen freien Anschluss an ihrem Windows PC. Bitte beachten Sie, dass die Netzwerkeinstellungen des Kartenterminals geändert werden müssen um das Gerät per RNDIS betreiben zu können. Welche Einstellungen Sie hierzu vornehmen müssen erfahren Sie in Kapitel 4.2 „Netzwerkkonfiguration“.

Bitte beachten Sie, dass sich sowohl der Konnektor als auch Ihr Kartenterminal im selben Netzwerk befinden oder bei verschiedenen Netzen diese über Routen einander erreichen können müssen. Das Kartenterminal kann zudem nur mit einer eingelegten

[3] Ein Konnektor sowie die notwendige Konfiguration des Konnektors gehören nicht zum Lieferumfang eines eHealth GT900 Kartenterminals.

gSMC-KT in einem der Geräte- SIM-Slots im Netzwerk kommunizieren. Das Einlegen einer gSMC-KT ist somit eine zwingende Voraussetzung zur erfolgreichen Inbetriebnahme Ihres Kartenterminals. Wie Sie eine gSMC-KT in einen der SIM-Slots des Gerätes einlegen, erfahren Sie in Kapitel 2.2.3 „SIM-Slots“.

Schließen Sie nun das mitgelieferte Netzteil an den dafür vorgesehenen Anschluss an Ihrem Kartenterminal an. Der Netzteil-Anschluss ist in Abbildung 3 mit der Position ⑤ gekennzeichnet. Stecken Sie abschließend das Netzteil in eine Steckdose (230V / 50 Hz)[4]. Ihr Gerät ist nun für die Erstinbetriebnahme bereit, beachten Sie daher die Hinweise in Kapitel 1.7 „Inbetriebnahme des Kartenterminals“. Der Anschluss mit der Position ③ (RS232) ist in dieser Firmware funktionslos.

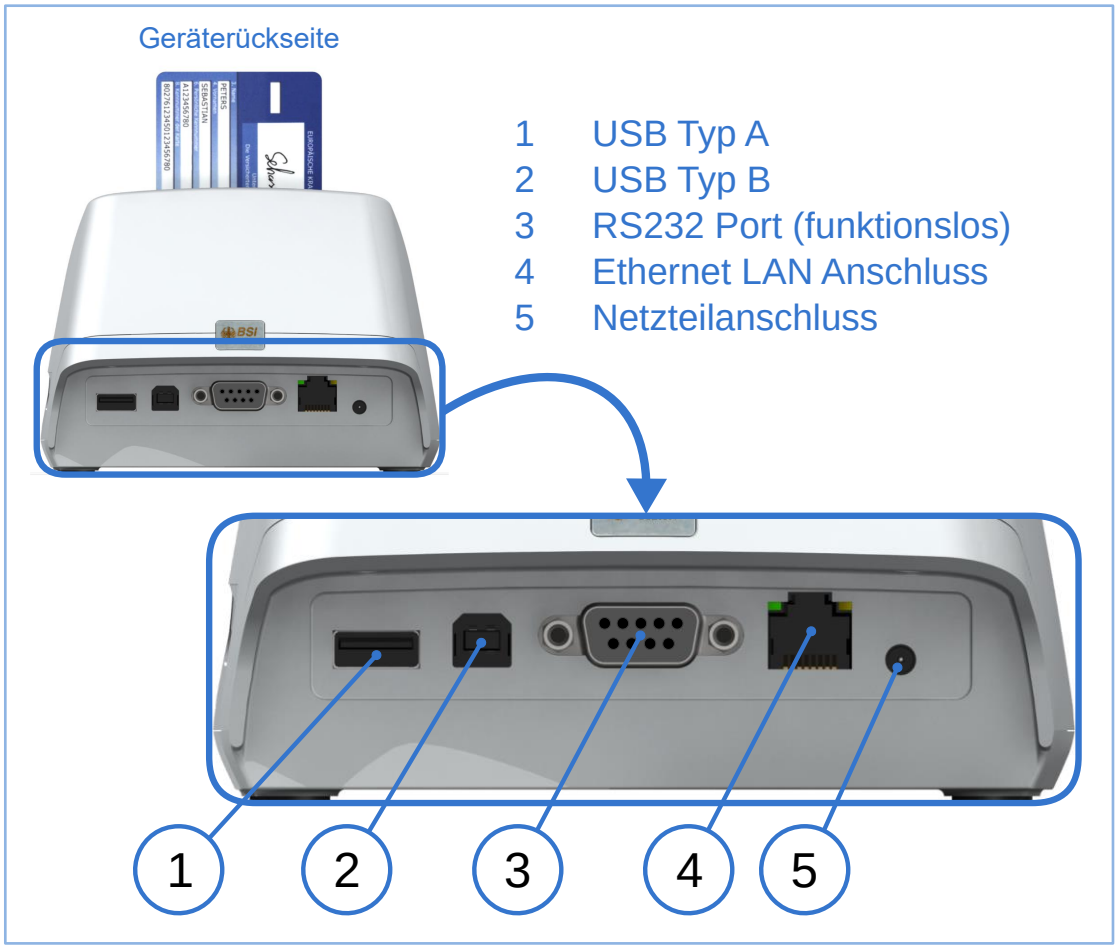


Abbildung 3: Belegung der Anschlüsse

[4] Das Gerät schaltet sich ein, sobald es mit Strom versorgt wird.

1.6 Betriebsmodi

1.6.1 Auslieferungs-Modus

In diesem Modus befindet sich das Kartenterminal in einem nicht konfigurierten Modus, dem sogenannten Auslieferungszustand. Sie erkennen diesen Zustand daran, dass das Kartenterminal beim Einschalten nach dem Selbsttest die Erstinbetriebnahme anzeigt und auffordert eine Admin PIN einzugeben (siehe Abbildung 4: PIN-Eingabe bei der Erstinbetriebnahme). Wenn Sie nicht der Administrator sind, trennen Sie das Kartenterminal wieder vom Strom oder übergeben die Aufgabe an den Administrator.

Um ein Kartenterminal wieder in den Auslieferungszustand zurückzusetzen, lesen Sie bitte Kapitel 5 „Gerät zurücksetzen“.

1.6.2 Benutzer-Modus

Dieser Modus ist der Normalzustand des Kartenterminals für die Rolle „Benutzer“. Hier können alle Funktionen, die keine weitere Authentifizierung durch eine PIN erfordern durchgeführt werden. In diesem Modus zeigt das Kartenterminal den Ruhebildschirm (siehe Abbildung 13: Displayaufbau des eHealth GT900 Kartenterminal).

1.6.3 Administrator-Modus

Eine Person der Rolle „Administrator“ darf die Erstinbetriebnahme des Kartenterminals durchführen und ist für die administrativen Einstellungen, sowie die Durchführung von Updates oder das Zurücksetzen des Gerätes in den Auslieferungszustand verantwortlich. Diese Funktionen können im Administrator-Menü direkt am Gerät oder teilweise über die Remote-Management Schnittstelle mit einem Browser durchgeführt werden.

Um in das Administrator-Menü zu gelangen, muss sich der Administrator mit Eingabe der Admin PIN am Kartenterminal authentifizieren (siehe Kapitel 4 „Geräteeinstellungen“). In der Weboberfläche der Remote-Management Schnittstelle muss sich der Administrator mit der Remote-Management PIN authentifizieren, sobald er Einstellungen vornimmt (siehe Kapitel 6 „Weboberfläche nutzen“).

1.6.4 Reset-Administrator-Modus

Eine Person der Rolle „Reset-Administrator“ kann das Kartenterminal in den Auslieferungszustand zurückversetzen. Dies ist nötig, wenn z.B. die Admin PIN oder die Remote-Management PIN verloren gegangen sein sollte. Der Reset-Administrator muss sich mit der PUK oder einem Resetcode authentifizieren, um die Rücksetzung durchführen zu können (siehe Kapitel 5.2 „Zurücksetzen ohne Kenntnis der Admin PIN“).

Wichtige Hinweise zur Inbetriebnahme des Gerätes:

Sollte sich im Gerät keine gSMC-KT-Karte in einem der Geräte-SIM-Slots befinden, so kann das Gerät zwar konfiguriert werden, aber es kann kein Pairing zu einem Konnektor erfolgen.

Wenn Sie keine gSMC-KT (Secure Module Card) in einen der SIM-Slots eingelegt haben, so ist eine Kommunikation des Kartenlesegerätes über das Netzwerk nicht möglich. Legen Sie daher bitte vor der Erstinbetriebnahme des Gerätes eine gSMC-KT in einen der SIM-Slots ein und versiegeln Sie diesen SIM-Slot, wie es in Kapitel 2.2.3 „SIM-Slots“ beschrieben ist.

Geräte mit eingelegter gSMC-KT und nicht versiegelten SIM-Slots dürfen nicht verwendet werden! Es ist zudem sicherzustellen, dass das lokale Netzwerk, in dem das Kartenterminal in Betrieb genommen wird, vor unbefugtem Zugriff abgesichert ist. Wenn Sie in Ihrem Netzwerk mehrere Geräte betreiben, so müssen Sie sicherstellen, dass jedes dieser Geräte individuelle Passwörter und PINs aufweist.

1.7 Inbetriebnahme des Kartenterminals

Die Inbetriebnahme des Kartenterminals ist durch einen Administrator vorzunehmen. Es ist zudem sicherzustellen, dass das lokale Netzwerk, in dem das Kartenterminal in Betrieb genommen wird, vor unbefugtem Zugriff abgesichert ist. Legen Sie vor der Inbetriebnahme alle notwendigen SMC in das Gerät ein (s. Kapitel 2.2.3). **Das Gerät schaltet sich durch den Anschluss der Stromversorgung selbst ein** (siehe Kapitel 1.5 „Anschluss des Gerätes“). Bei der Erstinbetriebnahme des Gerätes werden Sie nach

einem kurzen Systemtest gebeten, eine Admin PIN[5] zu vergeben. Nach dem Vergeben der Admin PIN müssen Sie zudem einen PUK vergeben, mit dem das Gerät beim Verlust der Admin PIN wieder in den Werkszustand zurückgesetzt werden kann.

1.7.1 Setzen der Admin PIN

Abbildung 4: PIN-Eingabe bei der Erstinbetriebnahme

Nach dem erstmaligen Einschalten des Kartenterminals werden Sie gebeten, eine Admin PIN zu vergeben.

Die PIN muss aus **mindestens 8 und höchstens 16 Ziffern** bestehen. Die Zeichen * und # können nicht verwendet werden. Bewahren Sie die PIN an einem sicheren Ort auf. Vermeiden Sie es, die Admin PIN in der Nähe des Gerätes aufzubewahren, insbesondere sollten Sie sie **nicht** auf dem Gerätegehäuse notieren. **Verwenden Sie zudem keine Trivial-PIN[6]**. Lesen Sie hierzu bitte auch die Hinweise zum Umgang mit der Admin PIN am Ende des Kapitels 4.1 „Admin-Menü“. Sie werden anschließend zu einer Wiederholung der PIN aufgefordert.

[5] Die Bezeichnung Admin PIN ist als Abkürzung des Begriffes Administrator PIN zu verstehen.

[6] Trivial-PINs und PUKs werden vom Gerät nicht angenommen und durch die Anzeige einer entsprechenden Fehlermeldung abgewiesen. Es werden alle Eingaben als Trivial-PIN bzw. -PUK abgelehnt, die nur aus einer Ziffer bestehen, wie z.B.11111111, sowie streng auf- oder absteigende Ziffernfolgen wie 01234567 oder 98765432.

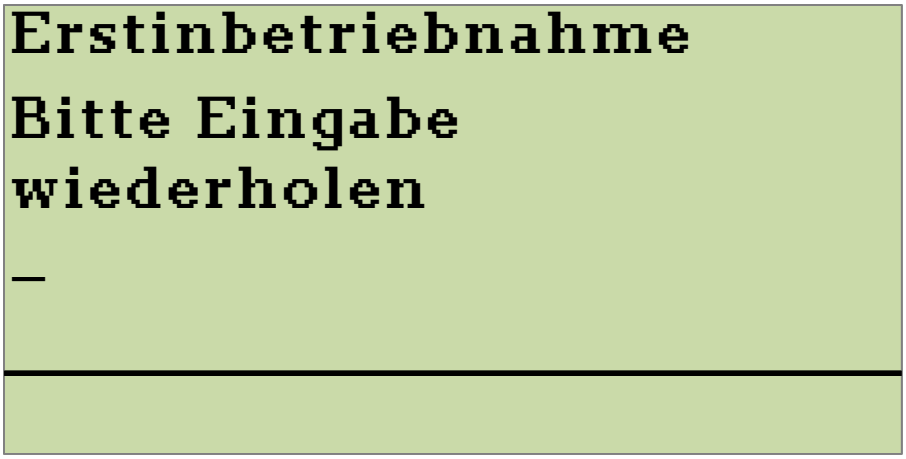


Abbildung 5: Bestätigung der PIN-Eingabe

Haben Sie die Admin PIN erfolgreich vergeben und Ihre Eingabe aus Sicherheitsgründen wiederholt bzw. bestätigt (siehe Abbildung 5), können Sie nach einer kurzen Bestätigungsanzeige, wie sie in Abbildung 6 dargestellt ist, mit der Vergabe eines PUK fortfahren. Sollten die von Ihnen eingegebenen PINs nicht identisch sein, werden Sie zur erneuten Eingabe aufgefordert.

Abbildung 6: Erfolgreiche Vergabe der Admin PIN

Die SICCT PIN für den administrativen Zugriff des Konnektors auf das Terminal und die Remote-Management PIN für die Weboberfläche zur Geräteadministrierung werden automatisch mit der Admin PIN vorbelegt. Diese lassen sich später jeweils einzeln

ändern. Siehe hierzu auch Kapitel 4.6 „Ändern der SICCT PIN“ sowie Kapitel 4.7 „Remote-Management Schnittstelle aus- oder einschalten“.

1.7.2 Setzen des PUK

Mit Hilfe des PUK können Sie das Kartenterminal später in den Auslieferungszustand zurücksetzen, sollte dies notwendig werden. Eine Person mit Kenntnis des PUK wird als Reset-Administrator bezeichnet. Wie Sie mittels PUK einen Werksreset auslösen, erfahren Sie in Kapitel 5.2.1 „Zurücksetzen mittels PUK“.

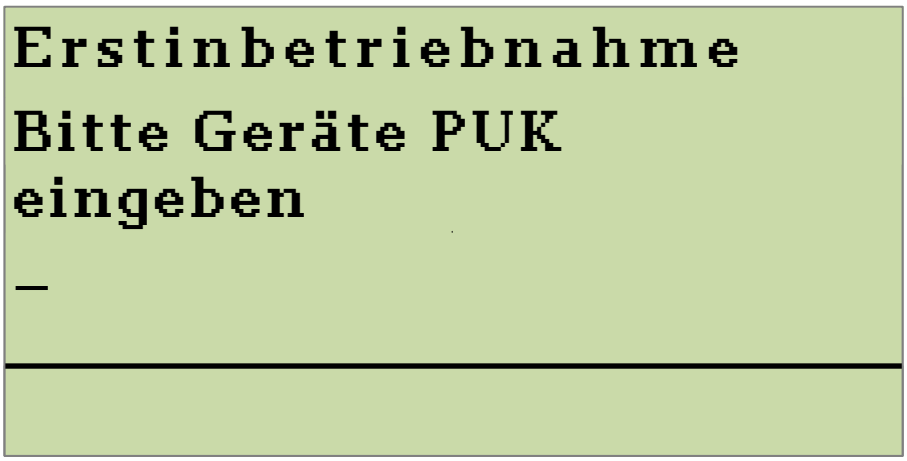


Abbildung 7: PUK-Eingabe bei der Erstinbetriebnahme

Der PUK muss aus **mindestens 8 und höchstens 16 Ziffern** bestehen. Die Zeichen * und # können nicht verwendet werden. Bewahren Sie den PUK an einem sicheren Ort auf. Vermeiden Sie es, den PUK in der Nähe des Gerätes aufzubewahren, insbesondere sollten Sie ihn **nicht** auf dem Gerätegehäuse notieren und sie nicht in der Nähe der Admin PIN aufbewahren. **Verwenden Sie zudem keinen Trivial-PUK**[6]. Lesen Sie hierzu bitte auch die Hinweise zum Umgang mit der Admin PIN und des PUK am Ende des Kapitels 4.1 „Admin-Menü“. Sie werden anschließend zu einer Wiederholung des soeben vergebenen PUK aufgefordert. Sollten die von Ihnen eingegebenen PUKs nicht identisch sein, werden Sie zur erneuten Eingabe aufgefordert.

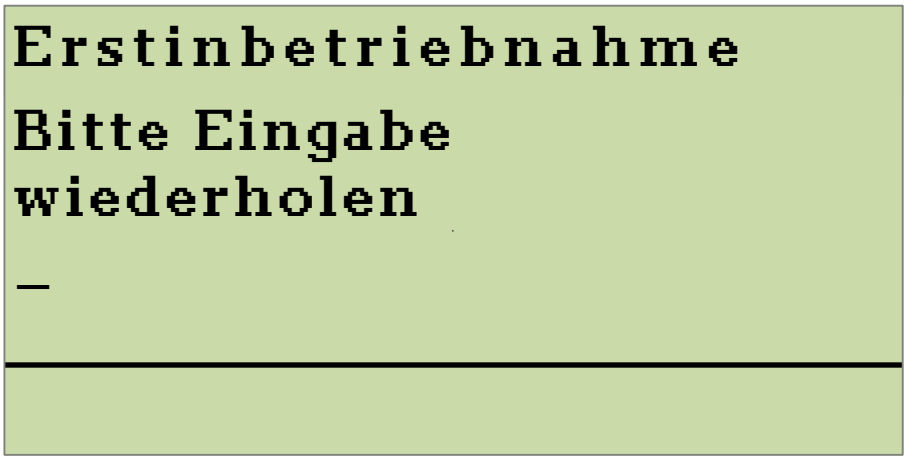


Abbildung 8: Bestätigung der PUK-Eingabe

Haben Sie den PUK erfolgreich vergeben und Ihre Eingabe wiederholt bzw. bestätigt (siehe Abbildung 8), ist nach einer kurzen Bestätigungsanzeige, wie sie in Abbildung 9 dargestellt ist, das Einrichten des eHealth GT900 abgeschlossen und das Gerät betriebsbereit.

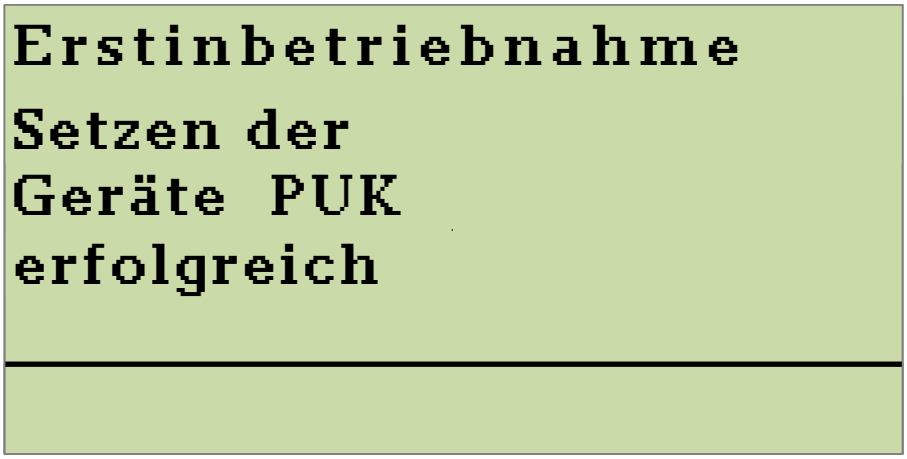


Abbildung 9: Erfolgreiche Vergabe des PUK

1.8 Ein- und Ausschalten des Kartenterminals

Schalten Sie das Gerät durch Drücken der  **-Taste ein**[7]**.** Nach einem kurzen Systemtest ist das Gerät einsatzbereit. Vergewissern Sie sich vor dem Ausschalten des Gerätes, dass die Kartenslots für KVK/eGK und eHBA/SMC-B leer sind. **Um das Gerät auszuschalten, betätigen Sie die**  **-Taste für mindestens 5 Sekunden.** Das Gerät bestätigt Ihnen den Ausschaltvorgang durch eine Anzeige im Display. Danach erlischt die Hintergrundbeleuchtung des Displays und das Gerät schaltet sich aus.

1.9 Reinigen und Desinfizieren des Gerätes

Bevor Sie das Kartenterminal feucht reinigen, trennen Sie das Gerät immer zuerst vom Stromnetz. Lassen Sie nach einer erfolgten Reinigung das Gerät trocknen. Für die Reinigung des Kartenterminals reicht ein feuchtes Tuch (feuchtes Desinfektionstuch), welches vorher gut ausgewrungen werden sollte, damit keine Nässe an empfindliche elektronische Bauteile gelangen kann. Achten Sie insbesondere darauf, dass keine Flüssigkeit durch die Öffnungen der Kartenslots in das Innere des Gerätes gelangt. Sollten Sie zur Reinigung eine spezielle Desinfektionsdispersion verwenden, benutzen Sie diese nie direkt auf dem Gerät, sondern benetzen Sie ein dafür geeignetes Tuch und benutzen Sie dieses. Feiner Sprühnebel beziehungsweise Tropfen könnten sonst an empfindliche Bauteile gelangen und dadurch Ihr Gerät zerstören beziehungsweise unbrauchbar machen. Achten Sie bei der Reinigung darauf, die Siegel auf dem Gerätegehäuse keiner erhöhten mechanischen sowie fluiden Belastung auszusetzen. Dies könnte die Siegel auf Ihrem Gerät unter Umständen beschädigen und dazu führen, dass eine sichere Benutzung nach den gesetzlichen Vorgaben nicht mehr gewährleistet

[7] Beachten Sie, dass sich das Gerät zunächst selbstständig einschaltet, sobald es mit Strom versorgt wird. Bleibt die Stromversorgung erhalten und das Gerät wird mit der X-Taste ausgeschaltet, kann es wie beschrieben wieder eingeschaltet werden.

ist. Sollten Sie sich nicht sicher sein, ob es eventuell zu einer Beschädigung eines Siegels gekommen ist, so lesen Sie bitte Kapitel 1.3.2 „Siegelprüfung“.

2 Bedienelemente

2.1 Tastatur

Das eHealth GT900 Kartenterminal verfügt über eine integrierte Folientastatur, die Ihnen eine sichere PIN-Eingabe garantiert. Die folgende Abbildung 10 (Gerätetastatur) und Tabelle 1 (Tastaturbelegung) sollen Sie mit den Funktionen der Tastatur vertraut machen.

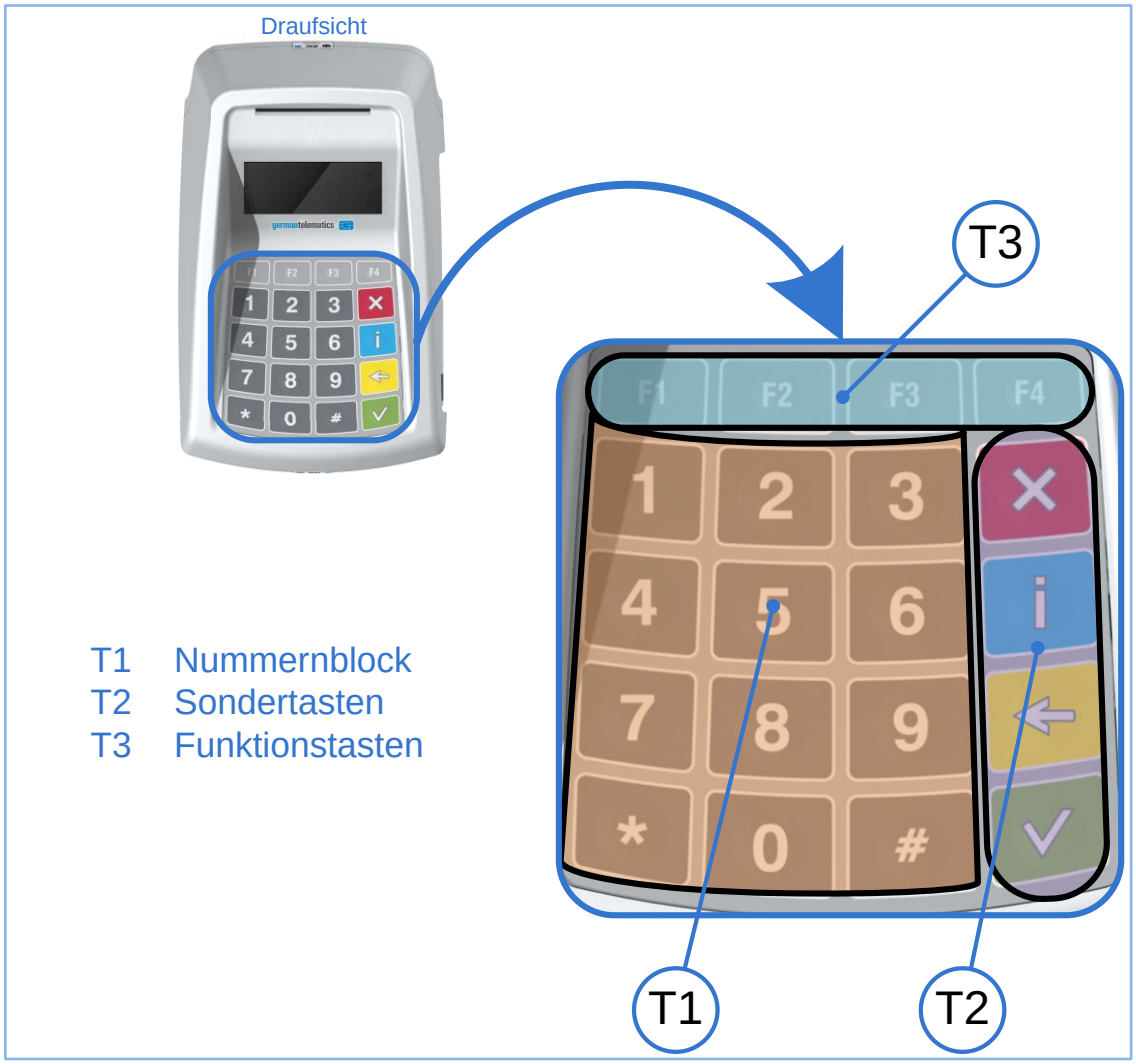


Abbildung 10: Tastatur des eHealth GT900 Kartenterminal

Tabelle 1: Tastaturbelegung des eHealth GT900 Kartenterminal

Symbol	In Abb.2	Funktion	Bemerkung
1	**T1**	Zifferntasten 0 bis 9	
F1	**T3**	Funktionstaste F1	**Halten Sie die F1 Taste länger gedrückt, um zum Admin-Modus zu gelangen.**
F2	**T3**	Funktionstaste F2	**Aufruf des Update-PIN cache (s. Kapitel 4.11.4) sowie Navigationstaste im Admin-Modus.**
F3	**T3**	Funktionstaste F3	**Navigationstaste im Admin-Modus.**
F4	**T3**	Funktionstaste F4	**Kurz drücken, um die Hintergrundbeleuchtung des Displays ein- oder auszuschalten.**
*	**T1**	derzeit funktionslos	
#	**T1**	derzeit funktionslos	
✗	**T2**	Abbruch / **Gerät ausschalten**	**Halten Sie die Taste min. 5 s gedrückt, um das Gerät auszuschalten.**
i	**T2**	Name des Terminals	**Drücken Sie die Taste, um den Namen des Terminals anzuzeigen.**
←	**T2**	Zurück / Löschen / Korrektur	
✓	**T2**	Bestätigen / **Gerät einschalten**	**Bei ausgeschaltetem Gerät kurz drücken, um das Gerät einzuschalten.**

Durch die Verwendung einer Folientastatur ist eine einfache und schnelle Reinigung und Desinfektion dieser häufig durch Patienten oder Personal berührten Fläche möglich. Hinweise zum Reinigen und gegebenenfalls Desinfizieren des Kartenterminals finden sich in Kapitel 1.9 „Reinigen und Desinfizieren des Gerätes“.

2.2 Kartenslots

Das eHealth GT900 Kartenterminal ist mit zwei Chipkarten-Kontakteinheiten ausgestattet, um die Verwendung der Krankenversichertenkarte (KVK), der elektronischen Gesundheitskarte (eGK) sowie des Heilberufsausweises (eHBA) und der Institutionenkarte (SMC-B) zu ermöglichen. Bestimmungsgemäß ist es nicht von Belang, in welcher Chipkarten-Kontakteinheit sich eine bestimmte Karte befindet. Das heißt insbesondere, dass jede der o.g. Karten in jeder Chipkarten-Kontakteinheit des Gerätes problemlos angenommen wird. Aus Gründen des einfacheren Umgangs mit dem Kartenterminal sei im Folgenden die Kontakteinheit 1 vornehmlich als eGK/KVK-Slot und die Kontakteinheit 2 vornehmlich als eHBA/SMC-B-Slot bezeichnet. Ziehen Sie für diese Zuweisung auch Abbildung 12 zu Rate.

Des Weiteren verfügt das Kartenterminal über 2 SIM-Slots für SMC-Karten (Secure Module Cards) auf der rechten Geräteseite. In die SIM-Slots des Kartenterminals können auch sogenannte gSMC-KT Karten eingelegt werden. Das Kartenterminal nutzt eine eingelegte gSMC-KT Karte, welche die kryptografische Identität des Kartenterminals in Form eines X.509 Zertifikates darstellt. Die kryptografischen Schlüssel der gSMC-KT Karte müssen eine hohe Güte aufweisen und der Prozess der Schlüssel- und Zertifikatgenerierung muss entsprechend abgesichert werden, um die Vertraulichkeit, Authentizität und Integrität der kryptografischen Schlüssel und Zertifikate zu gewährleisten. Aus diesem Grund bedarf die gSMC-KT gesonderter Sicherheitsmaßnahmen. Stellen Sie sicher, dass Ihre gSMC-KT durch die gematik zugelassen ist und über die entsprechenden Kennungen und Sicherheitsmerkmale verfügt. Beachten Sie bitte die Hinweise in Kapitel 2.2.3 „SIM-Slots“ und lesen Sie bitte auch die Info-Box „Wichtige Hinweise zum Umgang mit den SMC“ auf S. 35.

2.2.1 Kontakteinheit 1: Einstecken einer eGK/KVK

Eine eGK beziehungsweise KVK kann in der Chipkarten-Kontakteinheit 1 (eGK/KVK-Slot) des Gerätes bearbeitet werden. Die Karte wird von oben in die Kontakteinheit eingesteckt und nach unten gedrückt, bis sie leicht einrastet. Dazu muss das Kontaktfeld (Chip) auf der Karte für Sie sichtbar sein und nach unten zeigen (siehe nebenstehendes Piktogramm, das sich auch auf der Geräteoberschale befindet).

Das nebenstehende Symbol wird Ihnen in der oberen Statuszeile des Displays angezeigt (siehe Abbildung 13). Es repräsentiert den Chipkartenslot der Chipkarten-Kontakteinheit 1.

Wenn sich eine aktivierbare[8] Chipkarte in der Kontakteinheit 1 befindet, wird dieses Symbol ausgefüllt im Display dargestellt.

Bei einem Datenzugriff auf die Chipkarte in der Kontakteinheit 1 blinkt dieses Symbol für die Dauer des Zugriffs.

Das nebenstehende Symbol wird Ihnen angezeigt, sobald eine PIN an die betreffende Karteneinheit gesendet wird.

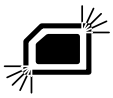
[8] Sobald eine Chipkarte in die Kontakteinheit gesteckt wird, wird diese durch das Kartenterminal kurzzeitig elektrisch aktiviert, um die Chipkarte auf grundsätzliche Funktion zu überprüfen. Haben Sie die Chipkarte korrekt gesteckt und das Kartensymbol wird nicht ausgefüllt dargestellt, so ist die Chipkarte defekt.

2.2.2 Kontakteinheit 2: Einstecken eines eHBA/einer SMC-B

Ein eHBA oder eine SMC-B kann vorzugsweise in der Chipkarten-Kontakteinheit 2 (eHBA/SMC-B-Slot), seitlich rechts am Gerät, zur Verwendung kommen. Die Karte wird mit nach unten und zum Gerät zeigenden Kontaktfeld von rechts in die Kontakteinheit bis zum Anschlag eingeführt.

Das nebenstehende Symbol wird Ihnen in der oberen Statuszeile des Displays angezeigt (siehe Abbildung 13). Es repräsentiert den Chipkartenslot der Chipkarten-Kontakteinheit 2.

Wenn sich eine aktivierbare[8] Chipkarte in der Kontakteinheit 2 befindet, wird dieses Symbol ausgefüllt im Display dargestellt.



Bei einem Datenzugriff auf die Chipkarte in der Kontakteinheit 2 blinkt dieses Symbol für die Dauer des Zugriffs.

Das nebenstehende Symbol wird Ihnen angezeigt, sobald eine PIN an die betreffende Karteneinheit gesendet wird.

2.2.3 SIM-Slots

Das Kartenterminal eHealth GT900 verfügt auf der rechten Geräteseite über 2 SIM-Slots. Die SIM-Slots werden werkseitig mit Chipkartenhaltern verschlossen. In diese SIM-Slots können sogenannte SMC (Secure Module Cards) eingelegt werden. Hierbei ist es Ihnen überlassen, in welchen Slot Sie eine SMC-B bzw. eine gSMC-KT einlegen. Beachten Sie jedoch, dass jeder Slot, in dem sich eine SMC befindet, mit einem SIM-Slotsiegel versehen sein muss.

Ein Entfernen der Chipkartenhalter führt, sofern das Gerät mit der Stromversorgung verbunden ist, zu einer Hinweismeldung im Display des Gerätes (s. Kapitel 8). Eine eventuell zum Konnektor bestehende Verbindung wird dabei beendet. Dabei ist es unerheblich, ob bereits eine Chipkarte eingelegt war oder der Chipkartenhalter leer ist. Um das Gerät weiter zu betreiben, müssen Sie einen Neustart ausführen. **Entfernen Sie diese Chipkartenhalter daher niemals leichtfertig.** Legen Sie die SMC Karte(n) nach Möglichkeit vor der Erstinbetriebnahme in das Gerät ein.

Um eine SMC in einen der SIM-Slots einzulegen, müssen Sie zunächst den Chipkartenhalter durch Drücken des Entriegelungsstifts aus dem Slot entfernen. Drücken Sie dazu den Entriegelungsstift (kleine Öffnung links neben jedem SIM-Slot) mit einem spitzen Gegenstand ohne Gewalt. Der Chipkartenhalter gleitet nun aus dem Gerät. Legen Sie Ihre SMC in den Chipkartenhalter ein und führen Sie den Chipkartenhalter mit der SMC wieder in das Gerät ein. **Der Chip zeigt dabei nach unten.** Schützen Sie die Chipkartenhalter vor Beschädigung oder Verlust. Das Gerät kann nur mit intakten eingesteckten Chipkartenhaltern betrieben werden. Sollten Sie Ersatz benötigen, wenden Sie sich bitte an den Verkäufer Ihres Gerätes.

Nachdem Sie eine SMC in einen der SIM-Slots des Gerätes geschoben haben, versiegeln Sie diesen SIM-Slot mit den im Lieferumfang enthaltenen SIM-Slotsiegeln. Der Administrator des Gerätes unterschreibt auf dem Siegel, bevor dieses auf dem Gerät angebracht wird in dem dafür vorgesehenen Feld (siehe Abbildung 11). Darüber

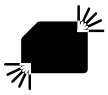
hinaus muss sich der Administrator die Siegel-Nr. notieren und diese Notiz an einem sicheren Ort verwahren[9].

Die SIM-Slotsiegel müssen beim Tausch einer SMC erneuert werden. Zu diesem Zweck ist im Lieferumfang des Kartenterminals eine entsprechende Anzahl an überzähligen SIM-Slotsiegeln vorhanden. Verwahren Sie die überzähligen Siegel ebenfalls an einem sicheren Ort, jedoch nicht zusammen mit Ihren Aufzeichnungen über die bereits verwendeten Siegel!

Das nebenstehende Symbol wird Ihnen in der oberen Statuszeile des Displays angezeigt (siehe Abbildung 13). Es repräsentiert jeweils einen der zur Verfügung stehenden SIM-Slots des Kartenterminals. Das obere der beiden SIM-Slot Symbole repräsentiert den hinteren SIM-Slot des Gerätes. Das untere der beiden SIM-Slot Symbole repräsentiert den vorderen SIM-Slot des Gerätes.

Wenn sich eine aktivierbare[8] SMC in einem der SIM-Slots befindet, so wird dieses Symbol teilweise ausgefüllt im Display dargestellt.

Wenn sich eine durch den Konnektor aktivierte SMC in einem der SIM-Slots befindet, so wird dieses Symbol vollständig ausgefüllt im Display dargestellt



Bei einem Datenzugriff des Konnektors auf eine aktivierte SMC in einem SIM-Slot blinkt dieses Symbol für die Dauer des Zugriffs.

Das nebenstehende Symbol wird Ihnen angezeigt, sobald eine PIN an die betreffende SMC in einem der SIM-Slots gesendet wird.

[9] Bevor Sie einen SIM-Slot versiegeln, sollten Sie die mit den eingelegten Karten in Verbindung stehenden Aufgaben durchführen. Dazu zählt z.B. das Pairing des Kartenterminals mit dem Konnektor für die eingelegte gSMC-KT, die Vergabe einer Echt-PIN für eine eventuell eingelegte SMC-B oder die Registrierung des Konnektors am VPN-Zugangsdienst mit einer eventuell eingelegten SMC-B.

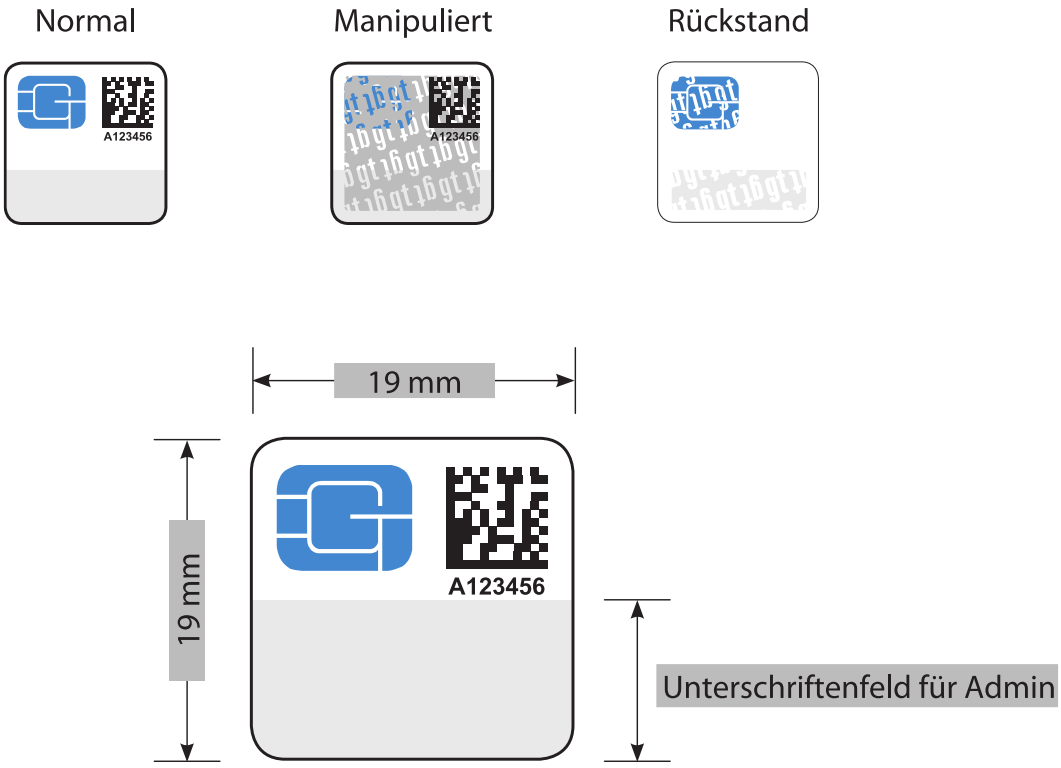


Abbildung 11:Sicherheitsmerkmale der SIM-Slotsiegel[10]

Wird das Anbringen eines neuen Siegels durch den Wechsel einer SMC nötig, entfernen Sie vorher die Klebereste des alten Siegels.

Wichtige Hinweise zum Umgang mit den SMC:

SMC SIM-Slots müssen versiegelt werden, wenn sich darin eine SMC befindet. Wenn Sie eine SMC in einen der SIM-Slots eingelegt haben, muss dieser SIM-Slot durch den berechtigten Administrator mit einem Siegel verschlossen werden. Darüber hinaus muss sich der Administrator die Siegel-Nr. notieren und diese Notiz verwahren. Haben Sie kein SIM-Slotsiegel mehr zur Verfügung, so wenden Sie sich bitte an Ihren zuständigen Systemdienstleister.

[10] Bitte verwahren Sie überzählige Siegel bis zu Ihrer Verwendung an einem sicheren Ort!

Geräte mit eingelegten SMC in unversiegelten SIM-Slots dürfen nicht verwendet werden! Überprüfen Sie auch die SIM-Slotsiegel regelmäßig auf mögliche Manipulationen! Bei Manipulationsverdacht muss der Administrator die Siegel-Nr. mit seinen Aufzeichnungen auf Übereinstimmung kontrollieren.

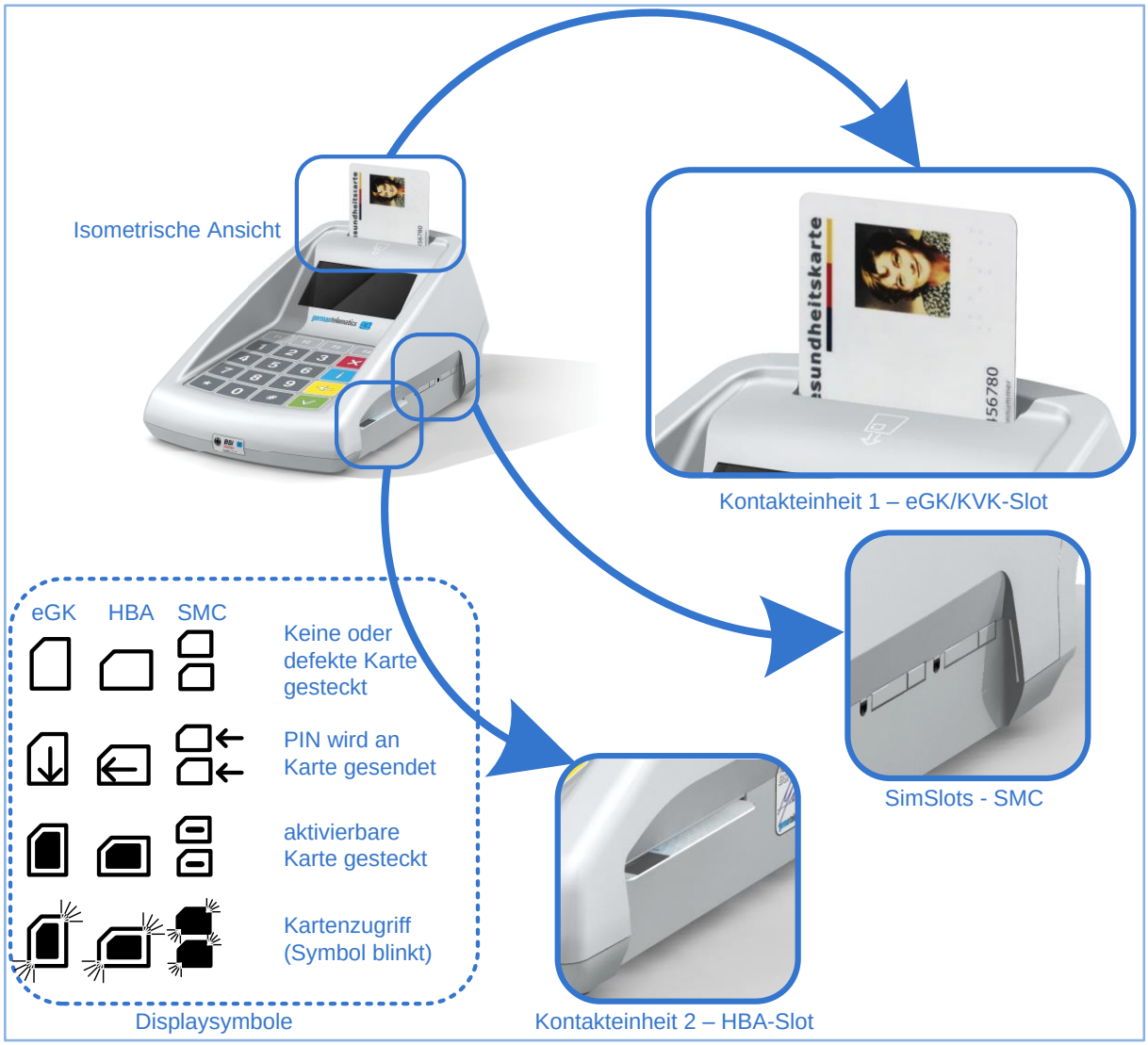


Abbildung 12: Anordnung und Benennung der Kartenslots

2.3 Aufbau der Displayanzeige

Auf dem Display des Gerätes werden Ihnen Informationen und Anweisungen angezeigt, die für die Arbeit mit dem Kartenterminal notwendig sind. Das Display gliedert sich, wie in Abbildung 13 dargestellt, in die obere Statusleiste, die Displaymitte und die untere Statusleiste. Das grafische Display hat eine monochromatische Anzeige (128 x 64 Bildpunkte) und verfügt über eine eigene Hintergrundbeleuchtung, so dass die Lesbarkeit des Displays auch in abgedunkelten Räumen und bei schwachem Umgebungslicht möglich ist.

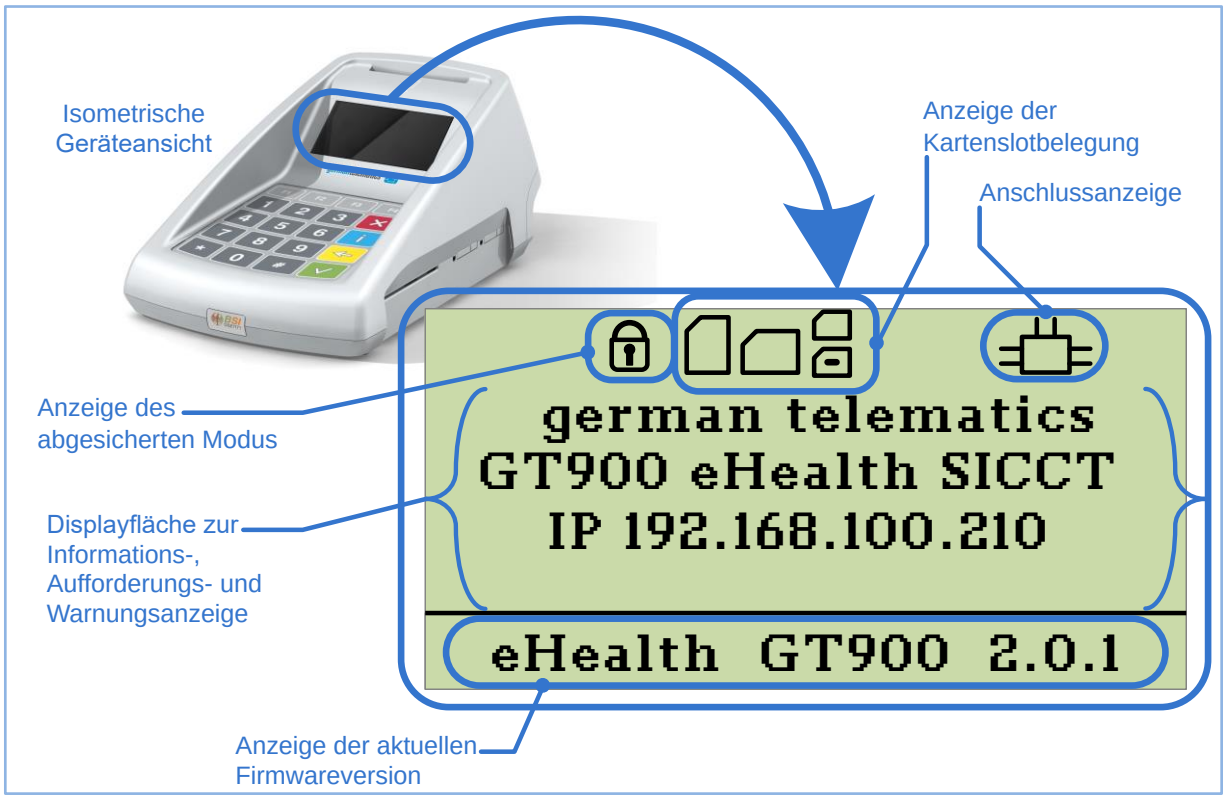
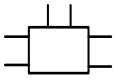
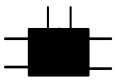


Abbildung 13: Displayaufbau des eHealth GT900 Kartenterminal

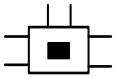
Der Anschluss des Kartenterminals an ein Netzwerk wird in der oberen Statusleiste rechts im Display angezeigt. Hierbei bedeutet:



Eine physikalische Ethernetverbindung ist vorhanden.



Eine SICCT-Session zu einem gepairten Konnektor ist über Ethernet aufgebaut.



Eine TLS-Verbindung zu einem Konnektor oder eine SICCT-Session zu einem nicht-gepairten Konnektor ist über Ethernet aufgebaut.

Eine physikalische USB-Verbindung ist vorhanden.

Eine SICCT-Session zu einem gepairten Konnektor ist über USB-RNDIS aufgebaut.

Eine TLS-Verbindung zu einem Konnektor oder eine SICCT-Session zu einem nicht-gepairten Konnektor ist über USB-RNDIS aufgebaut.

Die Anzeige des abgesicherten Modus[11] befindet sich in der oberen Statusleiste links im Display. In der Displaymitte werden Ihnen Informationen, Aufforderungen oder Warnungen angezeigt. Diese sind von der von Ihnen verwendeten Software (Praxisverwaltungssystem) abhängig. Daher kann an dieser Stelle nicht weiter auf sie eingegangen werden. Typischerweise sind diese angezeigten Informationen, Aufforderungen oder Warnungen selbsterklärend und bedürfen keiner weiteren Erläuterung. Eine mögliche Anzeige ist beispielhaft in Abbildung 14 dargestellt.

[11] Der abgesicherte Modus garantiert Ihnen eine sichere PIN-Eingabe für sämtliche Chipkarten-Geheimnummern (PIN) für eGK, HBA, SMC-B oder Standardsignaturkarten, zu deren Eingabe das Kartenterminal auffordert. Der sichere PIN-Modus besagt, dass PIN-Eingaben am Kartenterminal nicht in die unsichere Umgebung des Personalcomputers oder über offene Übertragungswege an den Client gelangen.

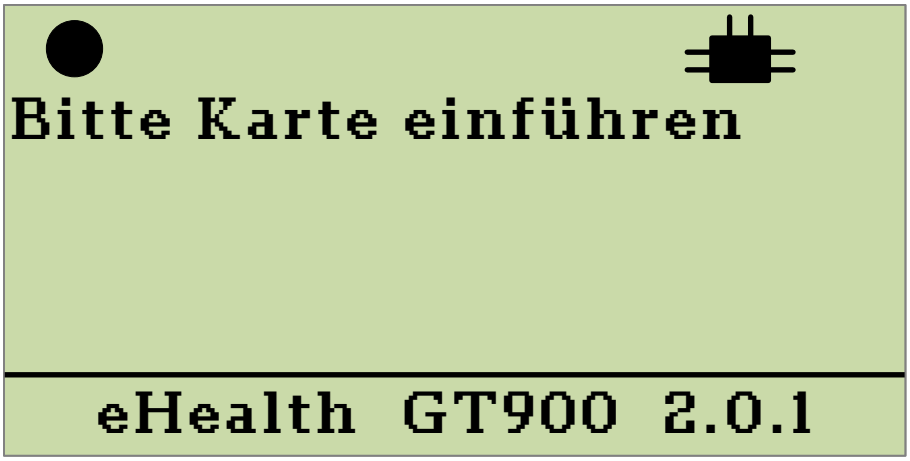


Abbildung 14: Beispielhafte Anzeige

In der oberen linken Ecke wird Ihnen, gesteuert durch den Konnektor und Ihre Software, eventuell zeitgleich mit einer Displaymeldung ein blinkender Punkt angezeigt. Dieser optische Hinweis dient dazu, Ihre Aufmerksamkeit auf die angezeigte Meldung zu lenken. In der unteren Statusleiste des Displays werden Sie über die aktuelle Firmware-Version informiert.

3 Betrieb als eHealth Kartenterminal am Konnektor

Als eHealth Kartenterminal wird das Kartenterminal in ein Netzwerk eingebunden. Das Kartenterminal wird entweder über die Ethernet-Schnittstelle oder über die USB B-Schnittstelle per RNDIS an einem Windows PC betrieben und muss mit einem Konnektor Verbindung aufnehmen, um die Funktionen eines eHealth Kartenterminals bereitzustellen. Das Gerät kann somit nur in Verbindung mit einem Konnektor bestimmungsgemäß betrieben werden.

Das Kartenterminal wird in einer LAN-Umgebung gemäß den Bestimmungen der gematik zum Aufbau einer IT-Infrastruktur für das deutsche Gesundheitswesen verwendet. Um sich innerhalb der eHealth Infrastruktur zu identifizieren, muss zudem eine von der gematik zugelassene gSMC-KT in das Gerät eingelegt sein. Lesen Sie hierzu auch Kapitel 2.2.3 „SIM-Slots“.

Der Konnektor, der sich, wie auch das Kartenterminal, innerhalb eines kontrollierten Bereiches befindet, muss durch die gematik zugelassen sein. Der Konnektor muss in der Lage sein, eine gesicherte Verbindung zum Kartenterminal aufzubauen und über geeignete Mittel verfügen, eine gegenseitige Authentifizierung sicherzustellen. Des Weiteren muss der Konnektor periodisch den Pairingstatus mit dem Kartenterminal überprüfen und den Administrator bei Unregelmäßigkeiten warnen. Lesen Sie vor Inbetriebnahme des Kartenterminals an einem Konnektor das Handbuch des Konnektors vollständig durch und befolgen Sie alle Sicherheitshinweise die im Handbuch des Konnektors genannt werden.

3.1 Pairing

Um Ihr Kartenterminal als eHealth Kartenterminal mit einem Konnektor zu koppeln, muss ein sogenannter Pairingprozess[12] eingeleitet werden. Der Pairingprozess wird durch den Administrator im Konnektor angestoßen. Im Handbuch des Konnektors ist beschrieben, wie dieser Pairingprozess in Gang gesetzt werden kann. Während des Pairingprozesses wird durch den Konnektor der Fingerprint (Hashwert des Komponentenzertifikats) der eingelegten gSMC-KT überprüft. Anschließend wird eine Bestätigungsanweisung im Display des Kartenterminals angezeigt. Diese Anweisung muss befolgt werden, um einen erfolgreichen Pairingprozess von Konnektor und Kartenterminal durchzuführen.

Das Kartenterminal verwaltet drei Pairingblöcke mit jeweils drei Zertifikaten. Das Pairing wird mittels eines Pairinggeheimnisses zwischen dem Konnektor und dem Kartenterminal aufrechterhalten. Bestandteil des Pairings ist eine 16 Byte lange Zufallszahl (Pairinggeheimnis) und der öffentliche Schlüssel des Konnektorzertifikates.

Wichtige Hinweise zum Pairing-Prozess:

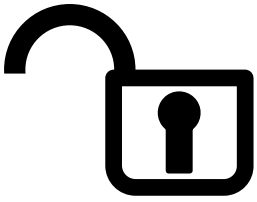
! **Stellen Sie als Administrator des Kartenterminals sicher, dass während des Pairing-Prozesses, d.h. während des Pairings des Kartenterminals mit einem Konnektor, keine unautorisierten Personen Zugang zum Kartenterminal oder zum Konnektor erlangen können. Um den initialen Pairing-Prozess zu autorisieren, müssen Sie die Pairing-Abfrage am Terminal bestätigen.**

[12] Als Pairing bezeichnet man die logische Verbindung zwischen Kartenterminal, der darin eingelegten gSMC-KT und dem Konnektor. Das Pairing verhindert somit, dass eine dieser Komponenten unberechtigter Weise ausgetauscht werden kann.

3.2 Eingabe einer Karten-PIN

Die sichere und vertrauliche Eingabe einer entsprechenden PIN (eGK, eHBA oder SMC-B) ist elementarer Bestandteil des Sicherheitskonzeptes dieses Kartenlesegerätes. Daher müssen PINs stets unbeobachtet eingegeben werden! Um die Sicherheit während der PIN-Eingabe zu gewährleisten, wird Ihnen im Display des Kartenterminals ein **Schlosssymbol** angezeigt. Dieses Symbol befindet sich während einer PIN-Eingabe **in der oberen Statusleiste links im Display.**

Die Eingabe einer PIN darf nur dann erfolgen, wenn das geschlossene Schlosssymbol anzeigt, dass eine PIN-Eingabe erwartet wird, keine Fehlermeldung des Konnektors vorliegt und die TLS-Verbindung zwischen Kartenterminal und Konnektor nicht unterbrochen ist. Die PIN wird dann sicher an die Karte übertragen. Eine Übertragung der PIN an ein anderes Gerät findet so unter keinen Umständen statt.

Das Kartenterminal befindet sich in einem abgesicherten Betriebszustand und ermöglicht somit: Die sichere Eingabe einer Karten-PIN	
Das Kartenterminal befindet sich in einem **nicht** abgesicherten Betriebszustand.	

Eine beispielhafte Aufforderung zur PIN-Eingabe ist in Abbildung 15 dargestellt.

Wichtige Hinweise zum Umgang mit der Karten-PIN:

Halten Sie Ihre PIN geheim. Stellen Sie bei der Eingabe der PIN sicher, dass niemand sonst die PIN lesen kann. Nutzen Sie bei der PIN-Eingabe ggf. Ihren Körper als Sichtschutz. **Achten Sie darauf, dass Ihnen bei der PIN-Eingabe ein geschlossenes Schlosssymbol in der oberen Statusleiste links im Display angezeigt wird[11]. Geben Sie Ihre PIN nicht ein, wenn der abgesicherte Modus nicht durch ein geschlossenes Schlosssymbol angezeigt wird.**

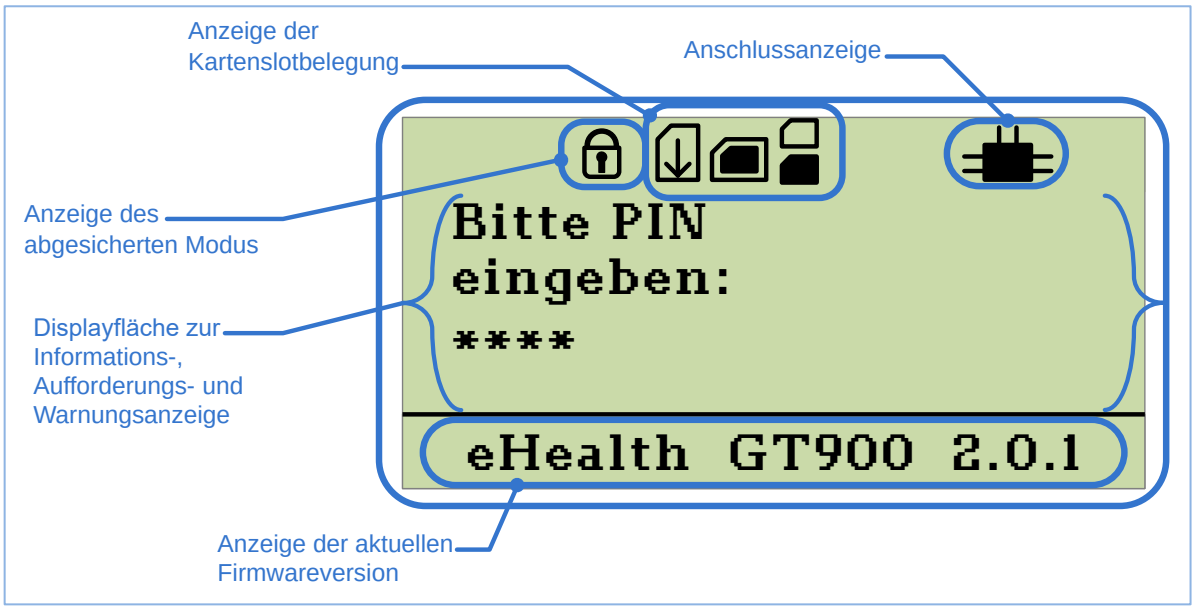


Abbildung 15: Mögliche Displayanzeige des Kartenterminals bei der Eingabe einer Karten-PIN. In diesem Beispiel wird die Karten-PIN an die Karte im eGK-Slot gesendet (zusätzlich sind ein Karte im eHBA/SMC-B-Slot und eine gSMC-KT eingelegt).

4 Geräteeinstellungen

Es wird in diesem Benutzerhandbuch davon ausgegangen, dass es sich bei Administratoren um gut geschultes IT-Personal handelt. Der Administrator ist in der Verwaltungsverantwortung aller sicherheitsrelevanten Funktionen des Kartenterminals sowie mit der Dokumentation und dem Betrieb des Kartenterminals vertraut. Darunter fällt insbesondere die Durchführung eines Firmware-Updates.

Konfigurationseinstellungen für das Kartenterminal können im Administrator-Menü direkt am Kartenterminal vorgenommen werden. Das Administrator-Menü (Admin-Menü) ist über eine PIN (Admin PIN) geschützt. Wenn Sie in Ihrem Netzwerk mehrere Geräte betreiben, so muss der Administrator sicherstellen, dass jedes dieser Geräte individuelle Passwörter und PINs aufweist. Änderungsprotokollierung und Logging sind für spätere Firmwareversionen vorgesehen und werden von dieser Firmwareversion nicht angeboten.

4.1 Admin-Menü

Das Administrator-Menü kann geöffnet werden, solange keine SICCT-Session zwischen Terminal und Konnektor besteht. Eine bestehende Verbindung erkennen Sie an der voll oder teilweise ausgefüllten Anschlussanzeige (Abbildung 15). Trennen Sie in dem Fall die Netzwerkverbindung eines der Geräte oder deaktivieren Sie das Terminal im Kartenterminaldienst des Konnektors.

Um in das Administrator-Menü zu gelangen, drücken Sie die F1 -Taste des eingeschalteten Kartenterminals für mindestens 5 Sekunden. Sie werden aufgefordert, die Admin PIN einzugeben. Zu der Vergabe der Admin PIN lesen Sie bitte das Kapitel 1.7 „Inbetriebnahme des Kartenterminals“.

Geben Sie die Admin PIN ein, um in das Admin-Menü zu gelangen.

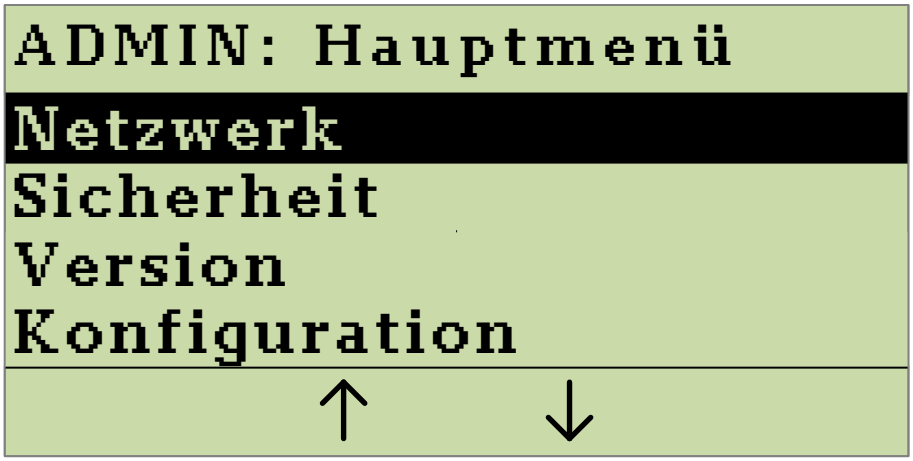
Abbildung 16: Abfrage der Admin PIN

Bestätigen Sie die PIN-Eingabe mit der ✅-Taste. Ist Ihre Eingabe nicht korrekt, wird Ihnen die Displaymeldung in Abbildung 17 angezeigt.

Die von Ihnen eingegebene Admin PIN ist falsch.

Abbildung 17: Anzeige bei Eingabe einer falschen PIN

Sollten Sie die Admin PIN dreimal falsch eingeben, ist ein erneuter Eingabeversuch erst nach einem gewissen Zeitraum möglich. Bei mehreren Falscheingaben verlängert sich der Zeitraum entsprechend, siehe Tabelle 2. Bei korrekter Eingabe der Admin PIN wird Ihnen das Admin-Menü im Display angezeigt.



Im Admin-Menü finden Sie verschiedene Optionen zur Geräteinstellung.

Abbildung 18: Anzeige Admin-Menü

Im Admin-Menü haben Sie vier Optionen zur Geräteinstellung:

Netzwerk: Netzwerkkonfiguration des Kartenterminals

Sicherheit: Ändern sicherheitsrelevanter Einstellungen

Version: Anzeige und Aktualisieren der Firmware-Version

Konfiguration: Konfiguration für Displayanzeige und Keep-Alive[13]

Mit den Tasten F2 und F3 wählen Sie eine Option aus. Drücken Sie die ✓-Taste, um die gewünschte Einstellung vorzunehmen. In den meisten Fällen wird Ihnen ein Submenü angezeigt. Durch Drücken der ✗-Taste verlassen Sie das Submenü und kehren zum übergeordneten Menü zurück. Das Administrator-Menü verlassen Sie ebenfalls durch Drücken der ✗-Taste, oder Sie wählen die Option **Ende** und bestätigen diese mit der ✓-Taste. In Abbildung 19 finden Sie den vollständigen Aufbau des Admin-Menüs.

[13] Für eine Beschreibung des Keep Alive Mechanismus siehe Kapitel 4.13 „Keep Alive senden“

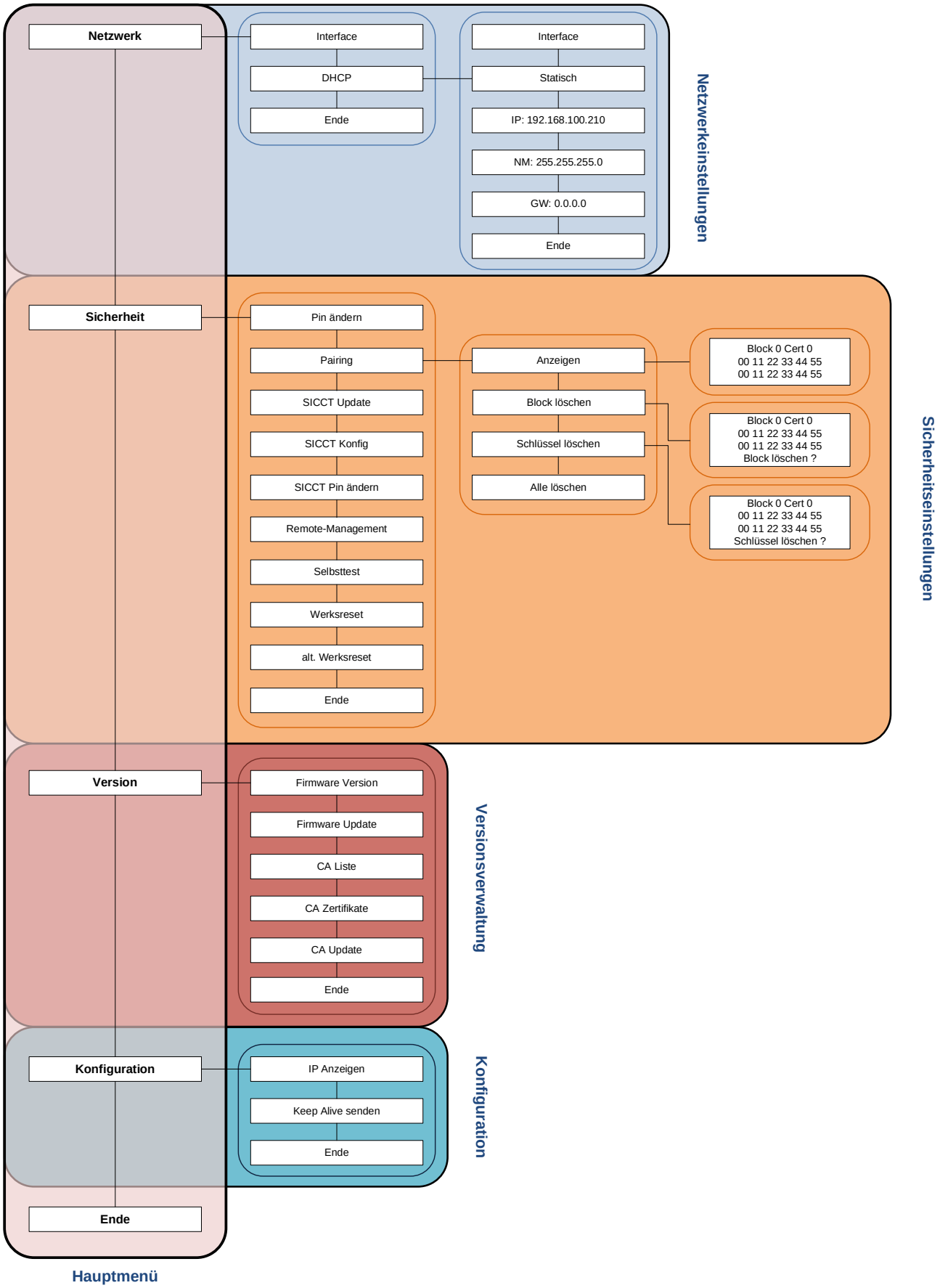


Abbildung 19: Struktur des Admin-Menüs

Tabelle 2: Zeitangaben für Fehlversuche bei der PIN- und PUK-Eingabe

Anzahl der aufeinander folgenden ungültigen Kennworteingaben	Mindestsperrzeiten für die Kennworteingabe
3-6	1 Minute
7-10	10 Minuten
11-20	1 Stunde
ab 21	1 Tag

Hinweise zum Umgang mit der Admin PIN und dem PUK:

Halten Sie die Admin PIN und PUK geheim. Stellen Sie bei der Eingabe der PIN bzw. des PUK sicher, dass niemand sonst diese lesen kann. **Verwenden Sie keine/n Trivial-PIN/PUK wie beispielsweise 11111111 oder 12345678[6]. Vermeiden Sie es, die Admin PIN und den PUK in der Nähe des Gerätes aufzubewahren, insbesondere sollten Sie sie nicht auf dem Gerätegehäuse notieren.** Die Admin PIN ermöglicht Ihnen den Zugriff auf die Managementschnittstellen Ihres Kartenterminals und erlaubt somit das Abfragen und Ändern von sicherheitskritischen Konfigurationen.

Verwahren Sie die Admin PIN und den PUK daher sorgsam und sicher! **Sollten Sie die Admin PIN dennoch verlieren bzw. vergessen, so können Sie mit Hilfe des Geräte PUK Ihr Gerät in den Auslieferungszustand zurückversetzen.** Bewahren Sie daher die Admin PIN und den PUK wenn möglich an unterschiedlichen Orten auf.

Wenn Sie in Ihrem Netzwerk mehrere Geräte betreiben, so müssen Sie sicherstellen, dass jedes dieser Geräte individuelle Passwörter und PINs aufweist.

4.2 Netzwerkkonfiguration

Das Kartenterminal muss zum Betrieb als eHealth Kartenterminal in ein Netzwerk eingebunden werden. Um innerhalb dieses Netzwerkes mit einem Konnektor abgesichert kommunizieren zu können, muss das Kartenterminal über seine Ethernet-Schnittstelle mit einem Netzwerk verbunden sein. Alternativ ist es möglich diese Netzwerkverbindung über einen Windows PC, den man per USB mit dem Kartenterminal verbindet, herzustellen. Die Vergabe einer IP-Adresse an das Kartenterminal kann entweder statisch (durch manuelle Eingabe) oder dynamisch über einen DHCP-Server erfolgen. Es wird empfohlen, eine statische IP-Adresse zu vergeben, um unbeabsichtigte Konfigurationsänderungen des Netzwerkes zu verhindern.

Um das Kartenterminal entsprechend zu konfigurieren, wählen Sie im Admin-Menü die Option **`Netzwerk`** aus und bestätigen mit der ✓-Taste. Auf dem Display wird Ihnen das Submenü **`ADMIN: Netzwerk`** angezeigt.

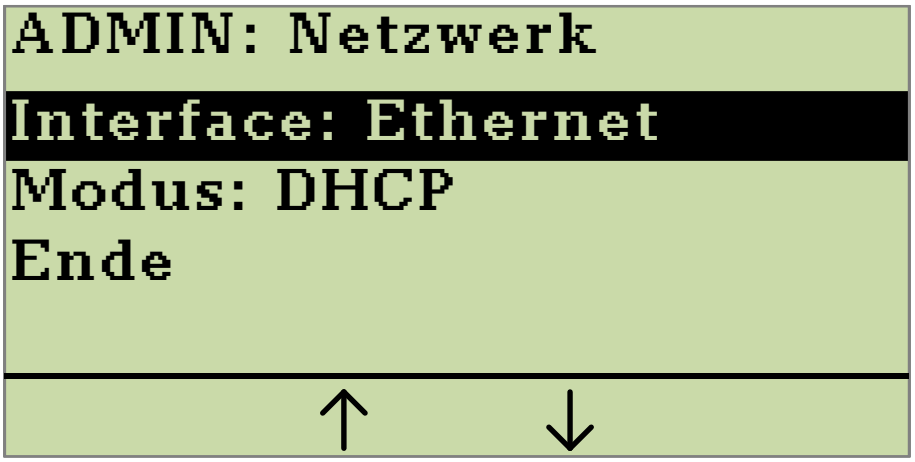
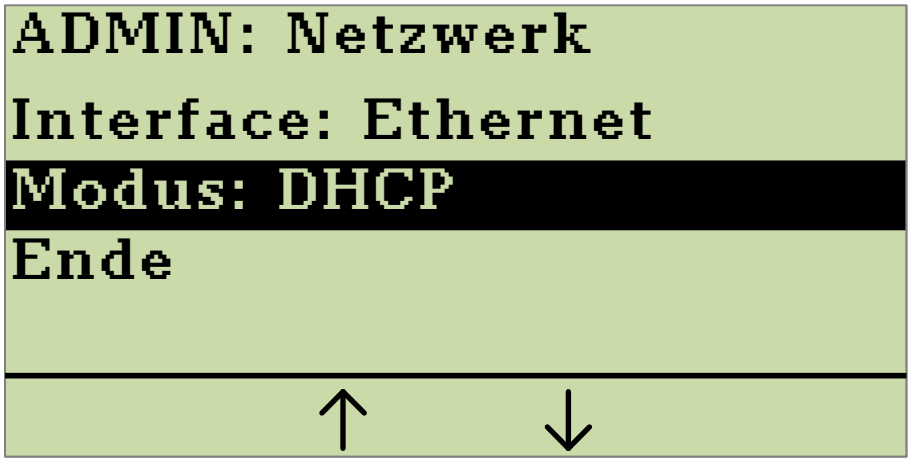


Abbildung 20: Auswahl des Parameters "Ethernet" als Netzwerkschnittstelle

Durch Drücken der ✓-Taste bei der Option **`Interface`** wechseln Sie die Einstellung für die Netzwerk-Schnittstelle zwischen den Parametern **`Ethernet`** und

USB RNDIS. Wenn **USB RNDIS** gewählt ist, muss in den Windows-Einstellungen eine Netzwerkbrücke zwischen dem Ethernetanschluss des PC's und dem USB RNDIS Adapter hergestellt werden. Hierzu muss das Kartenterminal per USB mit dem Windows PC verbunden sein (siehe Kapitel 1.5 „Anschluss des Gerätes"). Falls das Kartenterminal von Windows nicht automatisch als RNDIS-Gerät erkannt wird, muss im Gerätemanager ein Treiber aktualisiert werden. Der Administrator wird die notwendigen Einstellungen vornehmen.

Durch Drücken der ✓-Taste bei der Option **Modus** wechseln Sie zwischen den Einstellungen für die IP-Adressvergabe **DHCP** oder **Statisch**. Für eine dynamische Netzwerkkonfiguration wählen Sie den Parameter **DHCP**.

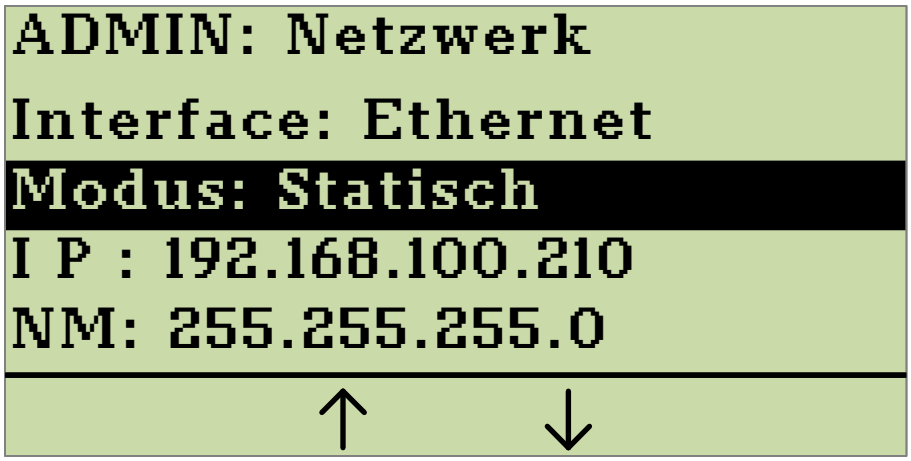


Wählen Sie den Parameter **DHCP**, um eine dynamische Netzwerk-konfiguration einzuleiten.

Abbildung 21: Auswahl des Parameters "DHCP"

Um die dynamische Netzwerkkonfiguration zu aktivieren, wählen Sie anschließend die Option **Ende** und bestätigen dies mit der ✓-Taste. Das Verlassen des Menüs wird einige Sekunden in Anspruch nehmen, da dem Terminal nun von Ihrem DHCP-Server eine IP-Adresse zugewiesen wird. Um die erfolgreiche Vergabe einer IP-Adresse zu überprüfen, aktivieren Sie die Option „Aktuelle IP-Adresse anzeigen" gemäß Kapitel 4.12.

Für eine statische Netzwerkkonfiguration wählen Sie den Parameter **Statisch**. Im Submenü **ADMIN: Netzwerk** erscheinen dann zusätzlich die Netzwerkparameter IP-Adresse (IP), Netzmaske (NM) und Gateway (GW):



Wählen Sie den Parameter **Statisch**, um die Netzwerk-konfiguration manuell festzulegen.

Abbildung 22: Anzeige bei Auswahl des Parameters "Statisch"

Die Werte der einzelnen Netzwerkparameter können Sie manuell eingeben. Mit den Tasten F2 und F3 wählen Sie den Netzwerkparameter aus. Drücken Sie die ✓-Taste. Geben Sie den Wert für den ausgewählten Netzwerkparameter über die Ziffern-Tastatur ein. Jede Eingabe kann durch Drücken der ⇦-Taste korrigiert werden.

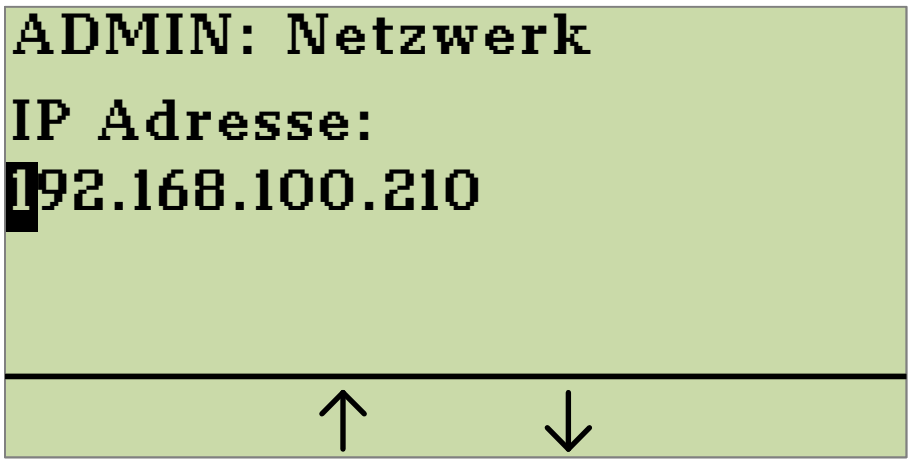


Abbildung 23: Beispiel für eine statische IP-Adresse

In Abbildung 31 ist die Eingabe einer beispielhaften IP-Adresse dargestellt. Für jeden Wert sind vier Felder **x.x.x.x** vorgesehen. In jedes Feld können maximal drei Ziffern

eingegeben werden. Falls die Eingabe für ein Feld kürzer als drei Ziffern ist, muss die ✓-Taste gedrückt werden, um die Eingabe im nächsten Feld fortzusetzen. Um einen vollständig eingegebenen Wert zu bestätigen, drücken Sie die ✓-Taste. Nachdem die Eingabe des letzten Feldes bestätigt wurde gelangen Sie zurück zur Übersicht der Netzwerkparameter. Entspricht Ihre Eingabe jedoch nicht der vorgegebenen Notation für IP-Adressen, erhalten Sie eine Fehlermeldung.

Sobald alle Werte für die Netzwerkparameter eingegeben wurden, wählen Sie die Option **Ende** und drücken die ✓-Taste zur Bestätigung. Die eingestellte Netzwerk-konfiguration wird nun aktiviert und im Display erscheint kurz die Meldung „**Netzwerk wird neu gestartet ...**“.

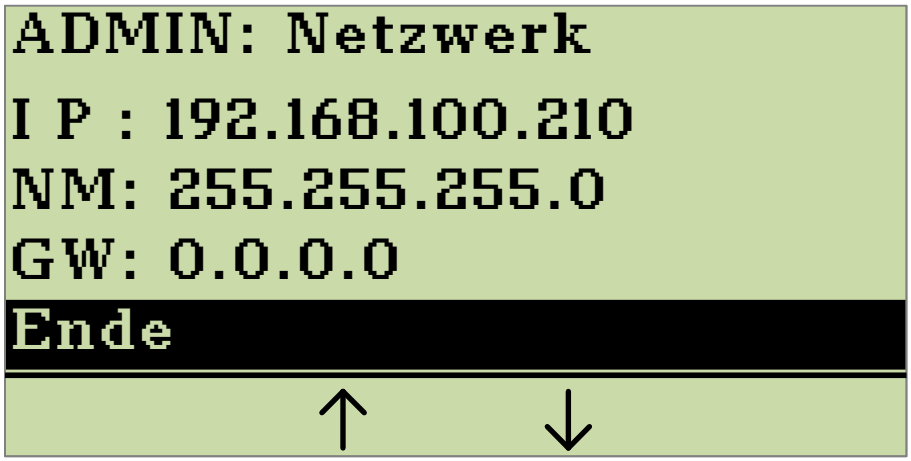
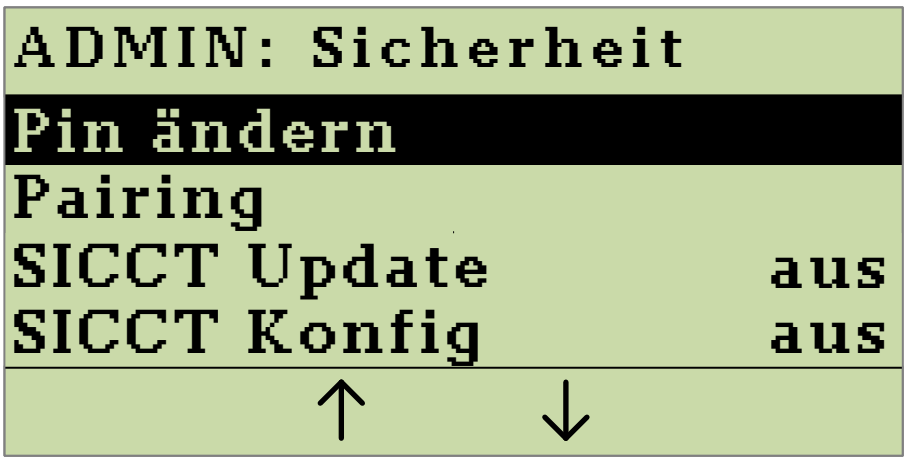


Abbildung 24: Bestätigung und Übernahme der Netzwerkparameter mit „Ende“

Durch Drücken der ✗ -Taste verlassen Sie das Submenü, vorgenommene Änderungen werden nicht übernommen und kehren zum übergeordneten Menü zurück.

4.3 Ändern der Admin PIN

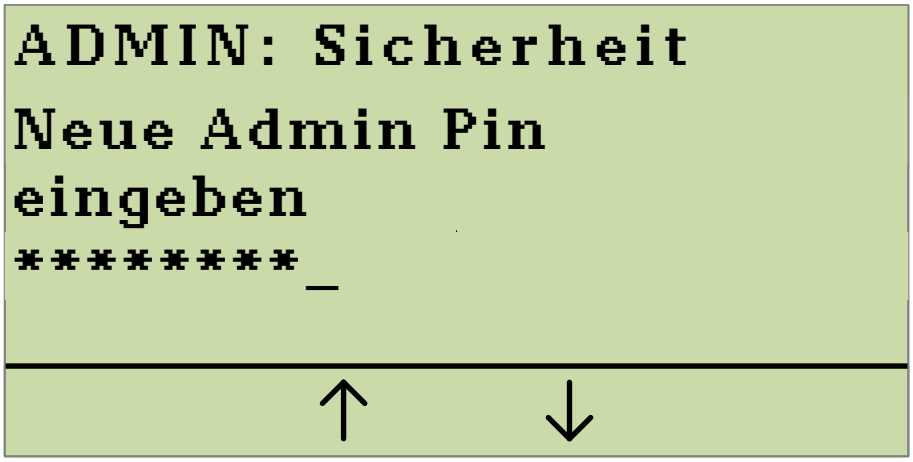
Um eine neue Admin PIN zu vergeben, müssen Sie die aktuelle Admin PIN kennen. Um die aktuelle Admin PIN zu ändern, wählen Sie in dem Admin-Menü die Option **`Sicherheit`** und bestätigen Sie mit der ✓-Taste. Auf dem Display wird Ihnen das Submenü **`ADMIN: Sicherheit`** angezeigt.



Drücken Sie die ✓-Taste, um die aktuelle Admin PIN zu ändern.

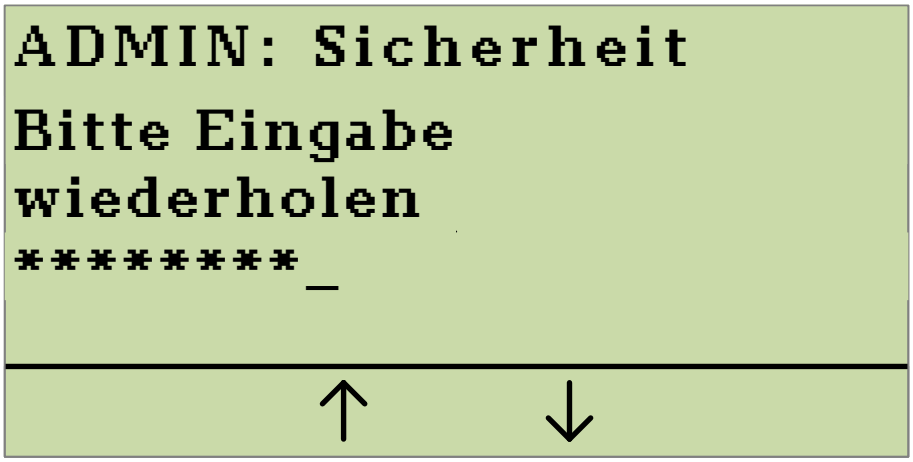
Abbildung 25: Anzeige des Submenüs "Sicherheit"

Wählen Sie die Option **`Pin ändern`** und bestätigen Sie durch Drücken der ✓-Taste. Sie werden nun aufgefordert, die neue PIN einzugeben und anschließend die Eingabe zu wiederholen (siehe Abbildung 26 und Abbildung 27). Sollten die von Ihnen eingegebenen PINs nicht identisch sein, werden Sie zur erneuten Eingabe aufgefordert. Jede Eingabe können Sie durch Drücken der ←-Taste korrigieren. Die neue PIN muss aus **mindestens 8 und höchstens 16 Ziffern** bestehen. Die Zeichen * und # können nicht verwendet werden. Durch Drücken der ✓-Taste bestätigen Sie Ihre Eingabe. **Hinweis: Verwenden Sie keine trivialen PINs wie beispielsweise 11111111 oder 12345678**[6]**.**



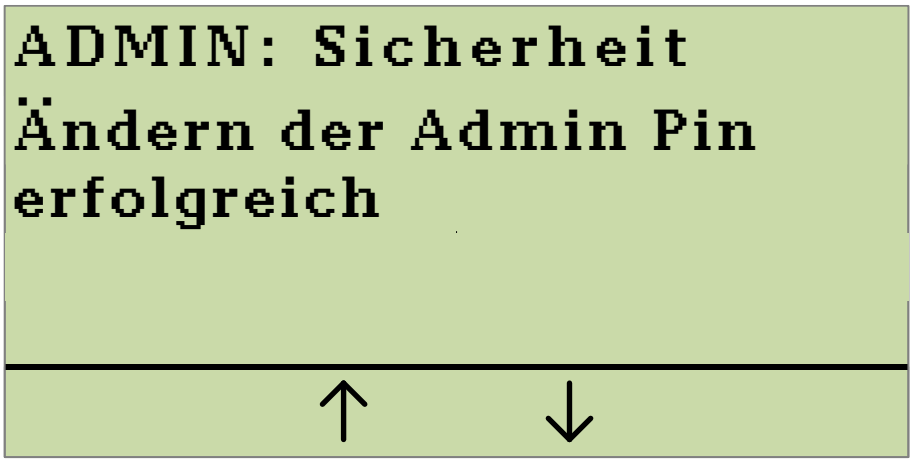
Eingabe der neuen PIN. Bestätigen Sie mit der ✅-Taste.

Abbildung 26: Eingabe einer neuen Admin PIN



Wiederholen Sie Ihre PIN-Eingabe. Bestätigen Sie mit der ✅-Taste.

Abbildung 27: Wiederholte Eingabe der Admin PIN

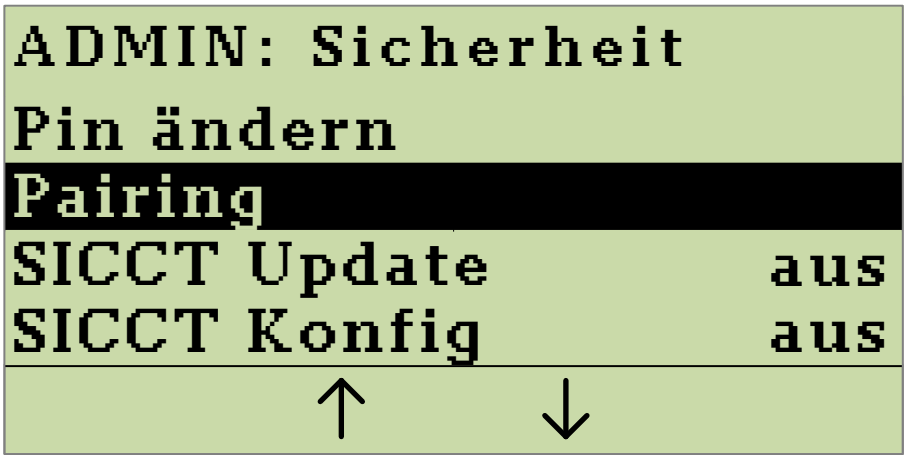


Ihnen wird anschließend eine kurze Bestätigung angezeigt und Sie kehren zum Admin-Menü zurück.

Abbildung 28: Bestätigung der erfolgreichen Änderung der Admin PIN

4.3.1 Pairing

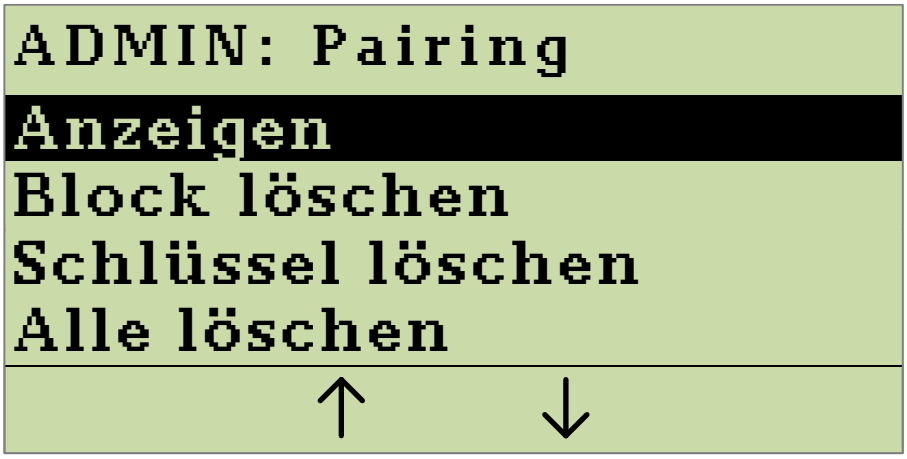
Das Pairing mit einem Konnektor ist für den Betrieb Ihres eHealth Kartenterminals unabdingbar. Lesen Sie hierzu auch das Kapitel 3.1 „Pairing“. Daher sollte das bestehende Pairing zu einem Konnektor nicht leichtfertig gelöscht werden. Um das derzeitige Pairing mit einem Konnektor zu löschen, wählen Sie in dem Admin-Menü die Option **`Sicherheit`** und bestätigen Sie mit der ✓-Taste. Auf dem Display wird Ihnen das Submenü **`ADMIN: Sicherheit`** angezeigt.



Drücken Sie die ✓-Taste, um ins Menü Pairing zu gelangen.

Abbildung 29: Anzeige des Submenüs "Sicherheit"

Wählen Sie die Option **`Pairing`** und bestätigen Sie durch Drücken der ✓-Taste. Sie gelangen nun in ein Submenü, in welchem Sie die in Abbildung 30 gezeigten Optionen ausführen können.



Drücken Sie die ✓-Taste, um einen Menüpunkt auszuwählen.

Abbildung 30: Menü zum Bearbeiten bestehender Pairings

4.3.2 Pairing anzeigen

Das Submenü **Anzeigen** zeigt für jedes bestehende Pairing den Pairingblock und die zugehörigen Fingerprints[14] an. Um in das Submenü **Anzeigen** zu gelangen, wählen Sie im Submenü **Pairing** die Option **Anzeigen** und bestätigen Sie durch Drücken der ✓-Taste. Abbildung 31 stellt eine beispielhafte Anzeige eines Pairingblocks mit dem Fingerprint eines Zertifikates dar. Mit den Tasten F2 und F3 können Sie zwischen verschiedenen Fingerprints wählen.

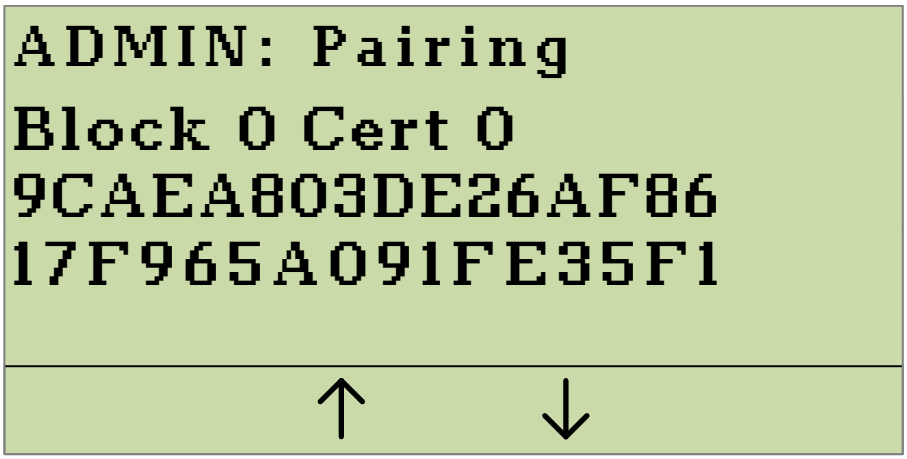


Abbildung 31: Menü zum Anzeigen vorhandener Fingerprints

Drücken Sie die F2 oder die F3 Taste, um sich verschiedene Fingerprints anzeigen zu lassen. (Beispielhafte Daten)

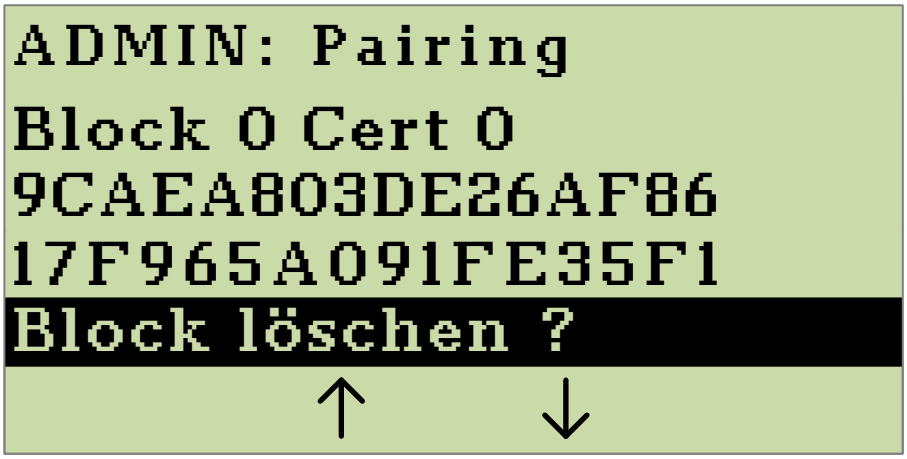
Durch Drücken der ✗-Taste oder der ✓-Taste können Sie in das Untermenü **Pairing** zurückkehren.

4.3.3 Block löschen

Das Submenü **Block löschen** zeigt für jedes bestehende Pairing den Pairingblock und die Fingerprints der zugehörigen Zertifikate an. Zusätzlich besteht in diesem Menü die Möglichkeit, die einzelnen Pairingblöcke zu löschen. Um in das Submenü **Block löschen** zu gelangen, wählen Sie im Submenü **Pairing** die Option

[14] Der Fingerprint ist der MD5-Hashwert über das gesamte X.509 Zertifikat des jeweilig gepairten Konnektors. Pro Pairingblock können bis zu drei Zertifikate (also auch 3 Fingerprints) enthalten sein.

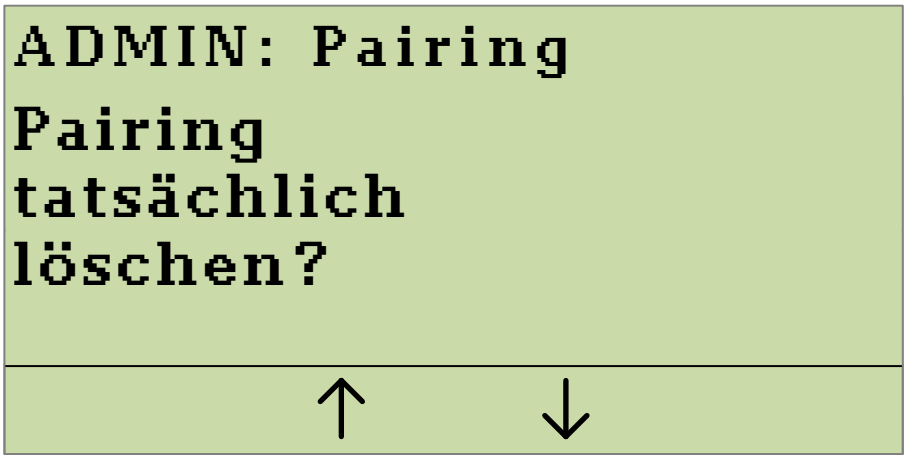
Block löschen und bestätigen Sie durch Drücken der ✓-Taste. Abbildung 32 stellt eine beispielhafte Anzeige eines Pairingblocks mit dem zugehörigen Fingerprint dar. Mit den Tasten F2 und F3 können Sie zwischen verschiedenen Pairing-blöcken wählen. Durch Drücken der ✓-Taste können Sie einzelne Pairingblöcke durch Auswahl und Bestätigen der Option **Block löschen ?** permanent vom Gerät entfernen.



Drücken Sie die ✓-Taste, um vorhandene Pairingblöcke zu löschen. (Beispielhafte Daten)

Abbildung 32: Menü zum Anzeigen vorhandener Pairingblöcke

Um ein versehentliches Löschen eines Pairings zu einem Konnektor zu vermeiden, müssen Sie durch eine zusätzliche Sicherheitsabfrage nochmals bestätigen, dass Sie das betreffende Pairing tatsächlich löschen wollen. Bestätigen Sie die Sicherheitsabfrage durch Drücken der ✓-Taste. Durch Drücken der ✗-Taste können Sie das Löschen des Pairings auch wahlweise abbrechen.

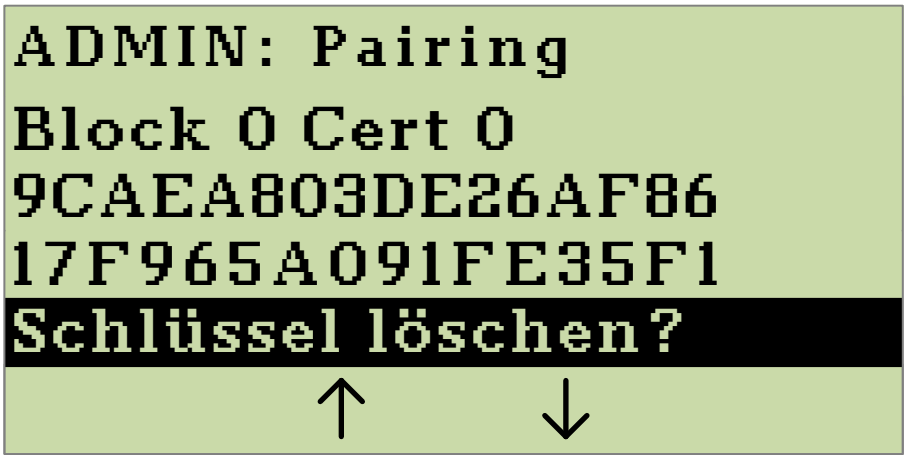


Drücken Sie die ✓-Taste, um das Löschen eines Pairings zu bestätigen.

Abbildung 33: Sicherheitsabfrage zum Löschen eines Pairings

4.3.4 Schlüssel löschen

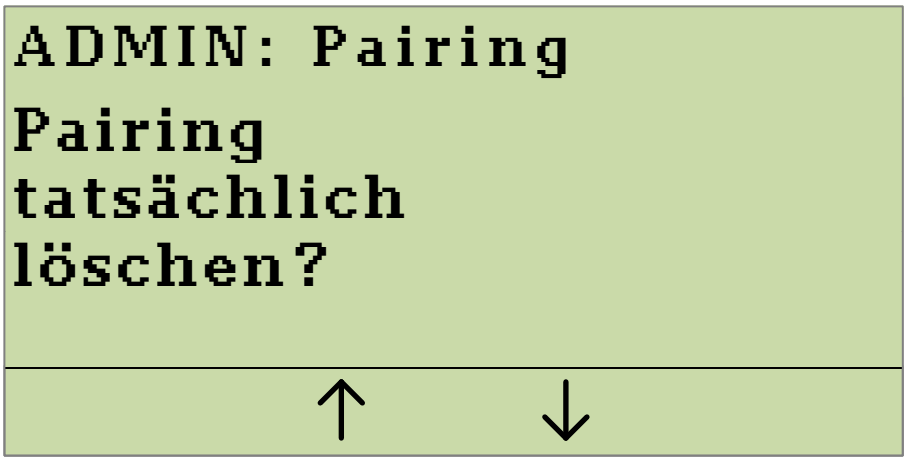
Das Submenü **Schlüssel löschen** zeigt für jedes bestehende Pairing den Pairingblock und die Fingerprints der Zertifikate an. Zusätzlich besteht in diesem Menü die Möglichkeit die einzelnen öffentlichen Schlüssel der Konnektorzertifikate (bis zu drei) zu löschen. Um in das Submenü **Schlüssel löschen** zu gelangen, wählen Sie im Submenü **Pairing** die Option **Schlüssel löschen** und bestätigen Sie durch Drücken der ✓-Taste. Abbildung 34 stellt eine beispielhafte Anzeige eines Pairingblocks mit dem Fingerprint eines Zertifikates dar. Mit den Tasten F2 und F3 können Sie zwischen verschiedenen Fingerprints wählen. Durch Drücken der ✓-Taste können Sie die einzelnen öffentlichen Schlüssel durch Auswahl und Bestätigen der Option **Schlüssel löschen ?** permanent vom Gerät entfernen.



Drücken Sie die ✓-Taste, um vorhandene Schlüssel zu löschen. (Beispielhafte Daten)

Abbildung 34: Menü zum Anzeigen vorhandener Fingerprints

Um ein versehentliches Löschen eines Pairings zu einem Konnektor zu vermeiden, müssen Sie durch eine zusätzliche Sicherheitsabfrage nochmals bestätigen, dass Sie den betreffenden Schlüssel tatsächlich löschen wollen. Bestätigen Sie die Sicherheitsabfrage durch Drücken der ✓-Taste. Durch Drücken der ✗-Taste können Sie das Löschen des Pairings auch wahlweise abbrechen.



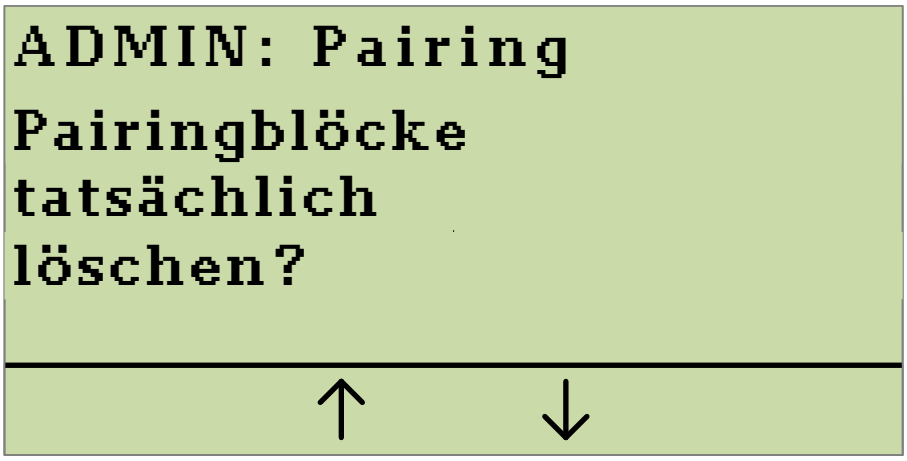
Drücken Sie die ✓-Taste, um das Löschen eines Schlüssels aus einem Pairingblock zu bestätigen.

Abbildung 35: Sicherheitsabfrage zum Löschen eines Schlüssels

4.3.5 Alle Pairings löschen

Um alle Pairings zu löschen, wählen Sie im Submenü **`Pairing`** die Option **`Alle löschen`** und bestätigen Sie durch Drücken der ✓-Taste. Um ein

versehentliches Löschen aller Pairings zu vermeiden, müssen Sie durch eine zusätzliche Sicherheitsabfrage nochmals bestätigen, dass Sie die Pairings tatsächlich löschen wollen. Bestätigen Sie die Sicherheitsabfrage durch Drücken der ✓-Taste. Durch Drücken der ✗-Taste können Sie das Löschen der Pairings wahlweise abbrechen.

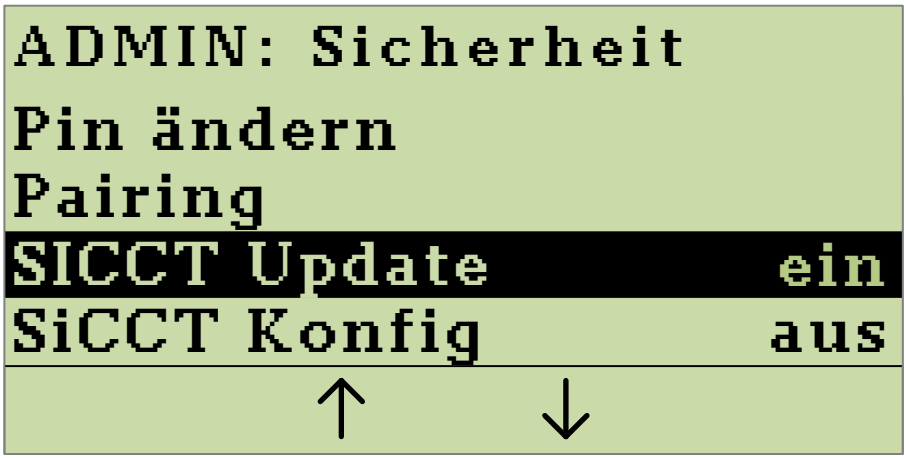


Drücken Sie die ✓-Taste, um das Löschen der Pairings zu bestätigen.

Abbildung 36: Sicherheitsabfrage zum Löschen aller Pairings

4.4 SICCT Update ein- oder ausschalten

Um die Durchführung von Updates durch den Konnektor ein- oder auszuschalten, wählen Sie in dem Admin-Menü die Option **`Sicherheit`** und bestätigen dies mit der ✓-Taste. Auf dem Display wird Ihnen das Submenü **`ADMIN: Sicherheit`** angezeigt.



Drücken Sie die ✓-Taste, um SICCT Update ein- oder auszuschalten.

Abbildung 37: Anzeige des Submenüs "Sicherheit"

Wählen Sie die Option **SICCT Update** und wählen Sie durch Drücken der ✓-Taste, ob die betreffende Option **Ein** oder **Aus** geschaltet werden soll. Unter dem betreffenden Menüpunkt wird Ihnen hinter dem Eintrag **SICCT Update** direkt angezeigt, welche Option gewählt wurde. Sie können das Menü über den Menüpunkt **Ende** oder durch Drücken der ✗-Taste verlassen. Um **SICCT Update** nutzen zu können, muss **SICCT Konfig** aktiviert sein.

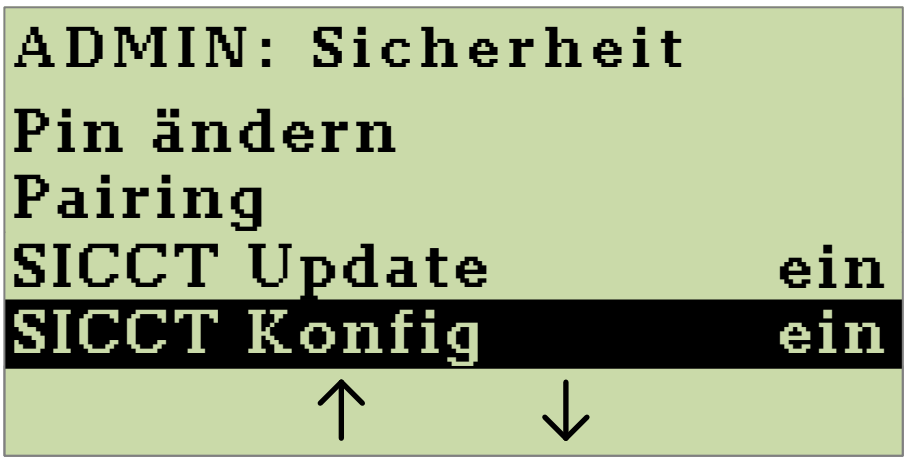
Wichtiger Hinweis zum Autoupdate

Ihre IT-Infrastruktur muss die durch die gematik spezifizierte automatische Durchführung von Updates unterstützen, damit diese Funktion genutzt werden kann. Der Administrator ist auch für den Betrieb eines Push-Servers verantwortlich und kann auf diesem eine entsprechende Firmware aussuchen die anschließend auf Kartenterminals innerhalb der IT-Infrastruktur installiert wird.

Bei jedem Updatevorgang für ein Kartenterminal logt dieser Push-Server die folgenden Informationen: Identifikation des entsprechenden Kartenterminals, Version der zu installierenden Firmware, Ergebnis des Update-Prozesses. Bei dem Push-Server kann es sich um einen Konnektor handeln. **Lesen Sie die Bedienungsanleitung des Konnektors, um zu erfahren, wie die SICCT-Update Funktion genutzt werden kann.**

4.5 SICCT Konfiguration ein- oder ausschalten

Um die Nutzung der SICCT Konfiguration zu ermöglichen und damit dem Konnektor administrativen Zugriff auf das Terminal zu erlauben, wählen Sie in dem Admin-Menü die Option **`Sicherheit`** und bestätigen mit der ✓-Taste. Auf dem Display wird Ihnen das Submenü **`ADMIN: Sicherheit`** angezeigt.



Drücken Sie die ✓-Taste, um SICCT Konfig ein- oder auszuschalten.

Abbildung 38: Anzeige des Submenüs "Sicherheit"

Wählen Sie die Option **`SICCT Konfig`** und wählen Sie durch Drücken der ✓-Taste, ob die betreffende Option **Ein** oder **Aus** geschaltet werden soll. Unter dem betreffenden Menüpunkt wird Ihnen hinter dem Eintrag **`SICCT Konfig`** direkt angezeigt, welche Option gewählt wurde. Sie können das Menü über den Menüpunkt **Ende** oder durch Drücken der ✗-Taste verlassen.

4.6 Ändern der SICCT PIN

Die SICCT PIN wird vom Konnektor benötigt, um sich per Netzwerk am SICCT-Port des Kartenterminals als Administrator zu identifizieren. Er kann so über die SICCT Schnittstelle Firmwareupdates und Konfigurationsänderungen am Terminal durchführen.

Hinweis: Bitte beachten Sie, dass, für die administrative Nutzung des SICCT-Ports an Ihrem Kartenterminal, im Konnektor die gleiche SICCT PIN als Passwort/PIN und der SICCT-Benutzername „admin“ für dieses Kartenterminal hinterlegt sein müssen.

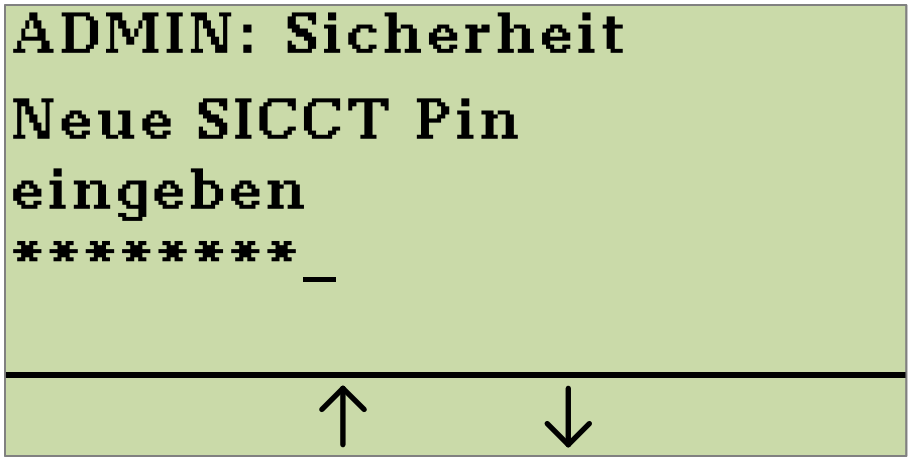
Bei der Erstinbetriebnahme des Kartenterminals wurde die SICCT PIN automatisch mit der Admin PIN vorbelegt.

Um die aktuelle SICCT PIN zu ändern, wählen Sie in dem SICCT-Menü die Option **`Sicherheit`** und bestätigen Sie mit der ✓-Taste. Auf dem Display wird Ihnen das Submenü **`ADMIN: Sicherheit`** angezeigt.

Drücken Sie die ✓-Taste, um die aktuelle SICCT PIN zu ändern.

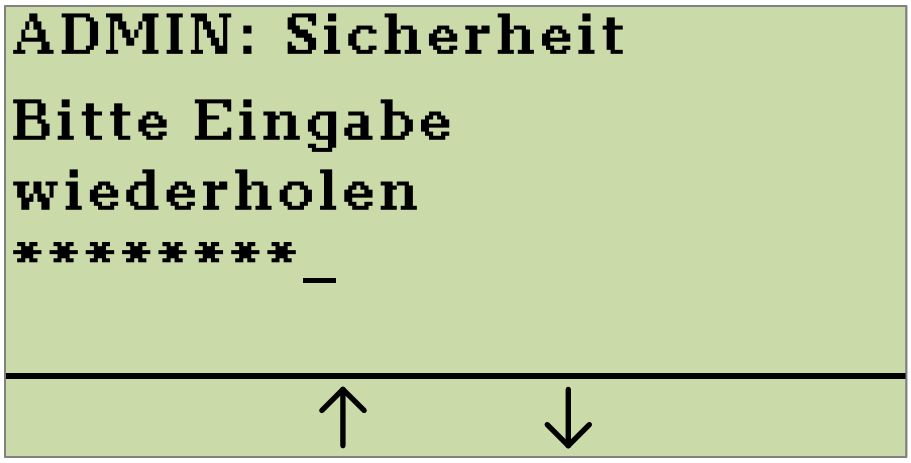
Abbildung 39: Anzeige des Submenüs "Sicherheit"

Wählen Sie die Option **`SICCT Pin ändern`** und bestätigen Sie durch Drücken der ✓-Taste. Sie werden nun aufgefordert, die neue PIN einzugeben und anschließend die Eingabe zu wiederholen (s. Abbildung 40 bis Abbildung 42). Sollten die von Ihnen eingegebenen PINs nicht identisch sein, werden Sie zur erneuten Eingabe aufgefordert. Jede Eingabe können Sie durch Drücken der ⇦-Taste korrigieren. Die neue PIN muss aus **8 bis 12 Ziffern** bestehen. Die Zeichen * und # können nicht verwendet werden. Durch Drücken der ✓-Taste bestätigen Sie Ihre Eingabe. **Hinweis: Verwenden Sie keine trivialen PINs wie beispielsweise 11111111 oder 12345678[6].**



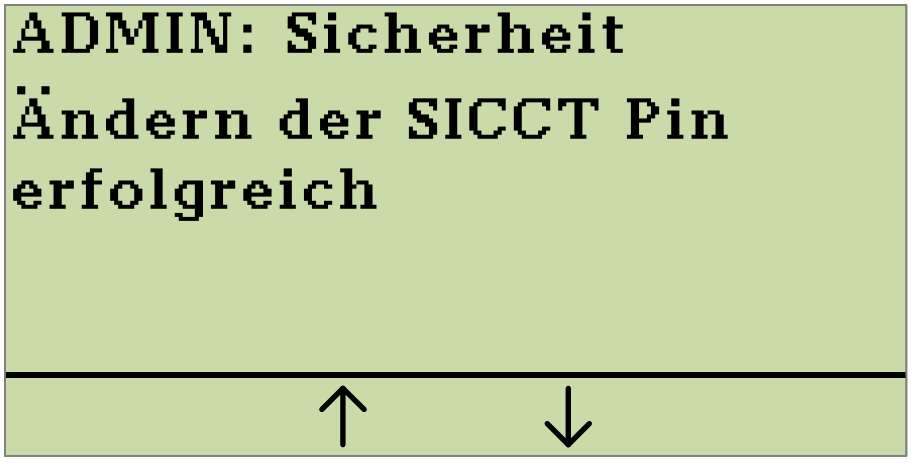
Eingabe der neuen SICCT PIN. Bestätigen Sie mit der ✅-Taste.

Abbildung 40: Eingabe einer neuen SICCT PIN



Wiederholen Sie Ihre SICCT PIN-Eingabe. Bestätigen Sie mit der ✅-Taste.

Abbildung 41: Wiederholte Eingabe der SICCT PIN



Ihnen wird anschließend eine kurze Bestätigung angezeigt und Sie kehren zum Admin-Menü zurück.

Abbildung 42: Bestätigung der erfolgreichen Änderung der SICCT PIN

4.7 Remote-Management Schnittstelle aus- oder einschalten

Ihr Kartenterminal verfügt über eine Weboberfläche zur Geräteadministrierung, die Sie am Computer in einem Internetbrowser öffnen können. Nach der Erstinbetriebnahme des Kartenterminals ist die Weboberfläche automatisch aktiviert und die Remote-Management PIN mit der Admin PIN vorbelegt.

Den Zugriff auf diese Weboberfläche können Sie aus- oder einschalten. In der Weboberfläche können Sie das Kartenterminal aus der Ferne konfigurieren, schalten Funktionen ein oder aus und erhalten Informationen über ihr Kartenterminal und zu bestehenden Pairings.

Um das Remote-Management aus- oder einzuschalten, wählen Sie im Admin-Menü die Option **`Sicherheit`** und bestätigen dies mit der ✓-Taste. Auf dem Display wird Ihnen das Submenü **`ADMIN: Sicherheit`** angezeigt.

Drücken Sie die ✓-Taste, um die Remote-Management Schnittstelle ein- oder auszuschalten.

Abbildung 43: Einstellung Remote-Management

Wählen Sie die Option **`Remote-Management`** aus und wählen Sie durch Drücken der ✓-Taste, ob die betreffende Option **`aus`** oder **`ein`** geschaltet werden soll. Wenn Sie die Remote-Management Schnittstelle einschalten, werden Sie zudem aufgefordert, eine Remote-Management PIN zu vergeben. Diese benötigen Sie, um sich als berechtigter Administrator an der Weboberfläche des Kartenterminals

anmelden zu können. Für die Remote-Management PIN gelten die gleichen Vorgaben wie für die Admin PIN.

Abbildung 44: Eingabe der Remote-Management Pin

Vergeben Sie eine Remote-Management PIN und drücken Sie anschließend die ✓-Taste, um den Vorgang abzuschließen.

Die Remote-Management PIN muss aus **mindestens 8 und höchstens 16 Ziffern** bestehen. Die Zeichen * und # können nicht verwendet werden. Bewahren Sie die PIN an einem sicheren Ort auf. Vermeiden Sie es, die Remote-Management PIN in der Nähe des Gerätes aufzubewahren, insbesondere sollten Sie sie **nicht** auf dem Gerätegehäuse notieren. **Verwenden Sie zudem keine Trivial-PIN wie beispielsweise 11111111 oder 12345678**[6]. Lesen Sie hierzu bitte auch die Hinweise zum Umgang mit der Admin PIN am Ende des Kapitels 4.1 „Admin-Menü“. Sie werden anschließend zu einer Wiederholung der PIN aufgefordert. Das erfolgreiche Setzen einer Remote-Management PIN wird Ihnen mit einer entsprechenden Meldung im Display des Terminals bestätigt.

Wenn Sie die Weboberfläche des Kartenterminals deaktivieren wird die Remote-Management PIN gelöscht. Beim erneuten Einschalten der Weboberfläche werden Sie dann gebeten, eine neue Remote-Management PIN zu vergeben.

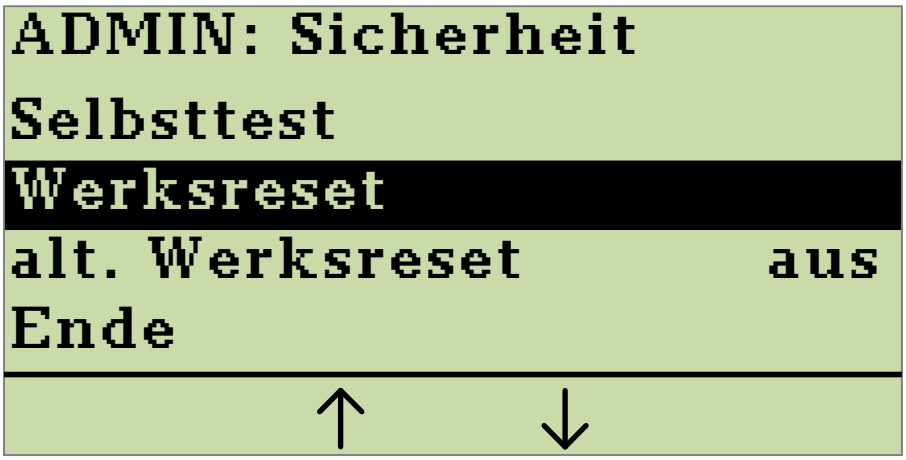
Informationen zum Zugriff auf die Weboberfläche und wie Sie damit Einstellungen an Ihrem Kartenterminal vornehmen können, entnehmen Sie bitte dem Kapitel 6 „Weboberfläche nutzen“.

4.8 Selbsttest ausführen

Um einen automatischen Selbsttest des Gerätes zu initialisieren, wählen Sie in dem Admin-Menü die Option **Sicherheit** und bestätigen dies mit der ✅-Taste. Auf dem Display wird Ihnen das Submenü **ADMIN: Sicherheit** angezeigt. Wählen Sie die Option **Selbsttest** aus und bestätigen Sie durch Drücken der ✅-Taste die sofortige Durchführung eines Geräte-Selbsttests. Das Terminal führt dazu einen Neustart durch.

4.9 Werksreset ausführen

Sie können über das Auswählen der Option **Sicherheit** im Admin-Menü und anschließendes Auswählen der Option **Werksreset** das Kartenterminal in den Auslieferungszustand zurückversetzen. Lesen Sie hierzu bitte das Kapitel 5.1 „Zurücksetzen mit Kenntnis der Admin PIN“.



Drücken Sie die ✅-Taste, um die Durchführung eines Werksresets zu starten.

Abbildung 45: Anzeige Werksreset"

4.10 Alternativen Werksreset einschalten

Wenn der alternative Werksreset aktiviert ist, kann auch ohne Kenntnis der Admin PIN oder des PUK das Terminal auf Werkseinstellungen zurückgesetzt werden. Die Person, die das Terminal mittels alternativem Werksreset zurücksetzt, wird als Reset-Administrator bezeichnet. Lesen Sie dazu auch Kapitel 5.2.2 „Zurücksetzen ohne Kenntnis des PUK“.

Drücken Sie die ✓-Taste, um den alternativen Werksreset einzuschalten.

Abbildung 46: Anzeige alternativer Werksreset

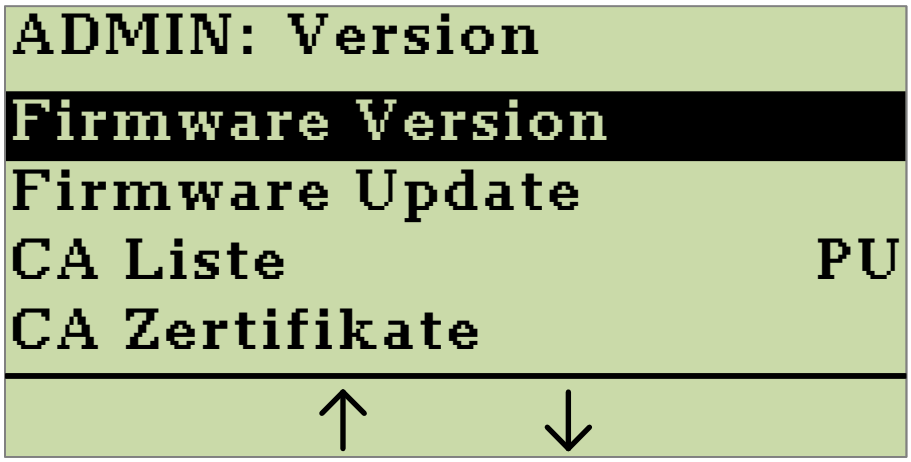
Der alternative Werksreset ist per Werkseinstellung deaktiviert. Bei Aktivierung wird vom Terminal eine individuelle Challenge erzeugt und abrufbar gemacht.

Hinweis: Sollte der alternative Werksreset nicht eingeschaltet sein und die PIN und die PUK verloren gehen, gibt es keine Möglichkeit mehr das Gerät in den Auslieferungszustand zurück zu versetzen!

4.11 Firmware-Version und Firmware-Update

Über die Option **`Version`** im Admin-Hauptmenü können Sie sich die aktuelle Version der Firmware anzeigen lassen und ein Update der Firmware initiieren.

Für die Anzeige der aktuellen Firmware-Version lesen Sie bitte das Kapitel 4.11.1 „Anzeige der aktuellen Firmware-Version“. Um ein Firmware-Update durchzuführen, lesen Sie bitte das Kapitel 4.11.2 „Durchführung eines Firmware-Updates“



Drücken Sie die ✓-Taste, um sich die Firmware-Version anzeigen zu lassen.

Abbildung 47: Anzeige des Submenüs "Version"

4.11.1 Anzeige der aktuellen Firmware-Version

Vor und gegebenenfalls nach einem Firmware-Update kann es erforderlich sein, die Versionsnummer der aktuell auf dem Kartenterminal installierten Firmware zu überprüfen.

Zur Anzeige der aktuellen Firmware-Version wählen Sie in dem Submenü **ADMIN: Version** die Option **Firmware-Version** und bestätigen dies mit der ✓-Taste. Im Display werden Ihnen die Hersteller ID und das Gerätekürzel in der ersten Zeile; Firmware-Version und die Hardware Version in der zweiten Zeile; sowie die Firmwaregruppe in der dritten Zeile Ihres eHealth GT900 Kartenterminals angezeigt. Mit den Tasten F2 und F3 können Sie sich weitere Informationen zu Ihrem Kartenterminal anzeigen lassen. Um die Anzeige zu verlassen und in das Submenü **ADMIN: Version** zurückzukehren, drücken Sie bitte die ✗-Taste.

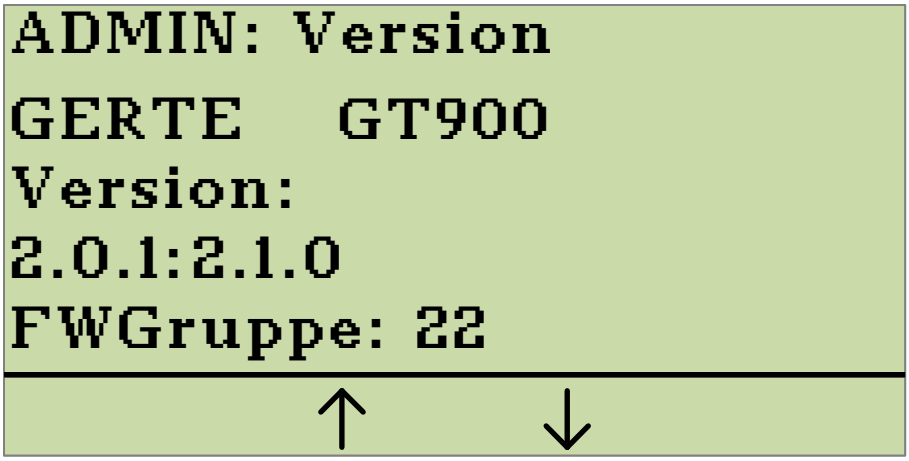


Abbildung 48: Anzeige der aktuellen Firmware-Version

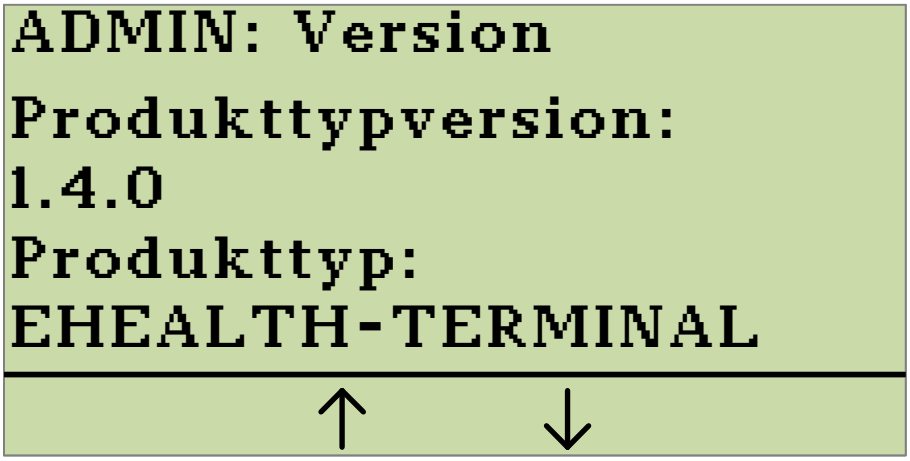


Abbildung 49: Anzeige der Produkttypversion und des Produkttyps

4.11.2 Durchführung eines Firmware-Updates

Um ein sicheres Firmware-Update vorzunehmen, müssen Sie Folgendes beachten:

- Nur autorisierte Personen, wie z. B: Administratoren, dürfen ein Firmware-Update durchführen.
- Ein Firmware-Update muss in einer gesicherten Umgebung durchgeführt werden, siehe Kapitel 1.4 „Aufstellungshinweise“.

Neben der Hardware ist die Firmware ein sicherheitssensibles Element. Verwenden Sie aus diesem Grund nur zugelassene Firmware-Versionen. Spielen Sie ein neues Update ein, so kann der Vorgang nicht abgebrochen werden. Es ist nicht möglich eine alte Vorgänger-Firmware-Version, die sich nicht in der Firmwaregruppe (Liste der zulässigen Firmware-Versionen) befindet, einzuspielen. Das Gerät prüft vor dem Anwenden der neuen Firmware, ob es sich um eine unveränderte, integere Version der german telematics handelt.

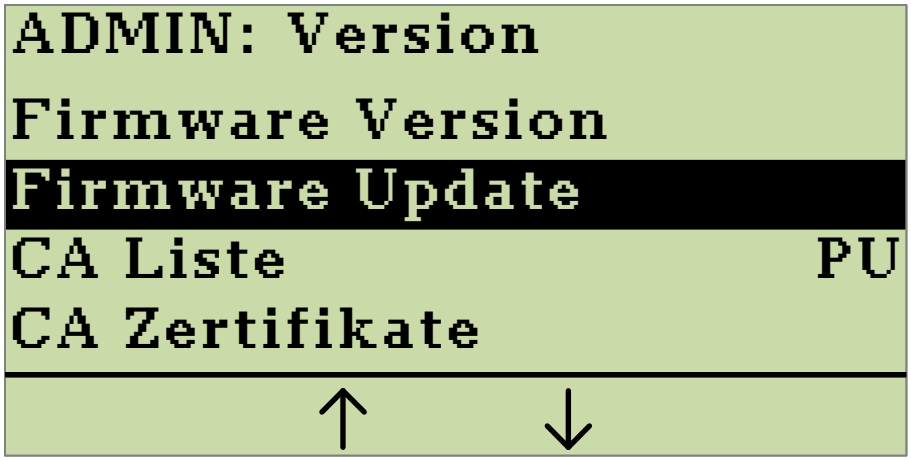
Laden Sie gegebenenfalls eine neue und zugelassene Firmware-Version Ihres Kartenterminals von der Herstellerseite https://www.germantelematics.de.

Es sei an dieser Stelle darauf hingewiesen, dass durch die Installation einer neuen Firmware dieses Benutzerhandbuch seine Gültigkeit verlieren kann. Informieren Sie sich auf der Herstellerseite: https://www.germantelematics.de über Versions-änderungen des Handbuchs im Zusammenhang mit Firmware-Updates.

Neben der im Folgenden behandelten Möglichkeit, ein Terminal direkt per USB-Schnittstelle mit einem Update zu versehen, werden Firmwareupdates primär durch den Konnektor durchgeführt. Hierzu kann der Konnektor stets auf alle zugelassenen Firmware-Versionen innerhalb der sicheren Umgebung der Telematik-Infrastruktur zugreifen. Ein durch den Konnektor angestoßenes Update läuft analog wie hier beschrieben ab, es entfallen nur die manuellen Schritte mit dem USB-Stick und der Updatevorgang beginnt mit dem Laden und der Überprüfung des geladenen Updates. Die weiteren Schritte sind dann identisch.

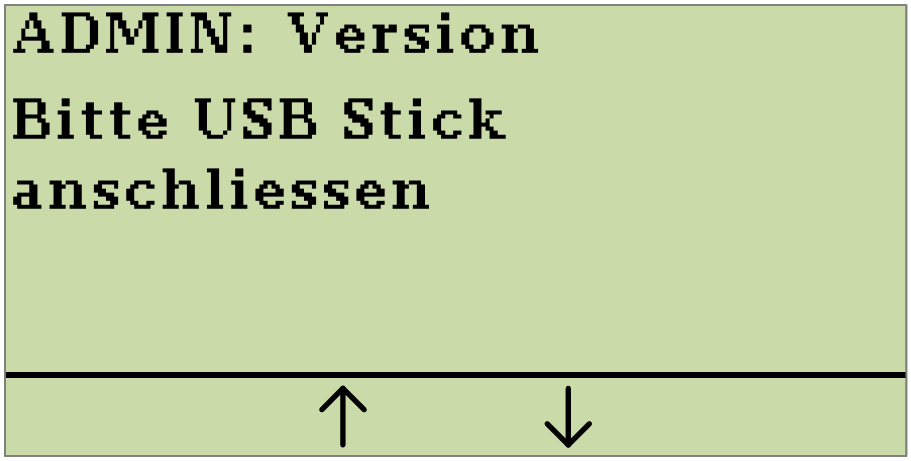
Weiterhin bietet die german telematics auf ihren Internetseiten ein Software-Tool „GT900 LAN Setup“ an, mit dem es möglich ist, ein eHealth GT900 über die LAN-Schnittstelle mit einem Firmwareupdate (oder auch Downgrade) zu versorgen. Ob Sie die Aktualisierung der Firmware lokal mittels USB-Stick oder über das Netzwerk durchführen, bleibt dabei Ihnen überlassen.

Es handelt sich bei der Update-Datei um eine Datei im Format *.bin. Der Dateiname lautet gt900-[Firmwareversion].bin, wobei [Firmwareversion] für die Versionsnummer steht, die Sie installieren wollen (siehe auch Abbildung 52). Kopieren Sie die Datei auf einen handelsüblichen USB-Stick (nicht im Lieferumfang enthalten, FAT32 formatiert). Dieser USB-Stick muss vorher von allen Dateien befreit werden, d.h. er muss leer sein. Halten Sie den so präparierten USB-Stick für die nun folgende Update-Prozedur bereit. Wechseln Sie zunächst wie in Kapitel 4.1 „Admin-Menü“ beschrieben in den Administrator-Modus. Wählen Sie nun im Submenü **`ADMIN: Version`** die Option **`Firmware Update`** aus und bestätigten Sie ihre Auswahl mit der ✅-Taste (siehe Abbildung 50).



Drücken Sie die ✅-Taste, um das Firmwareupdate zu starten.

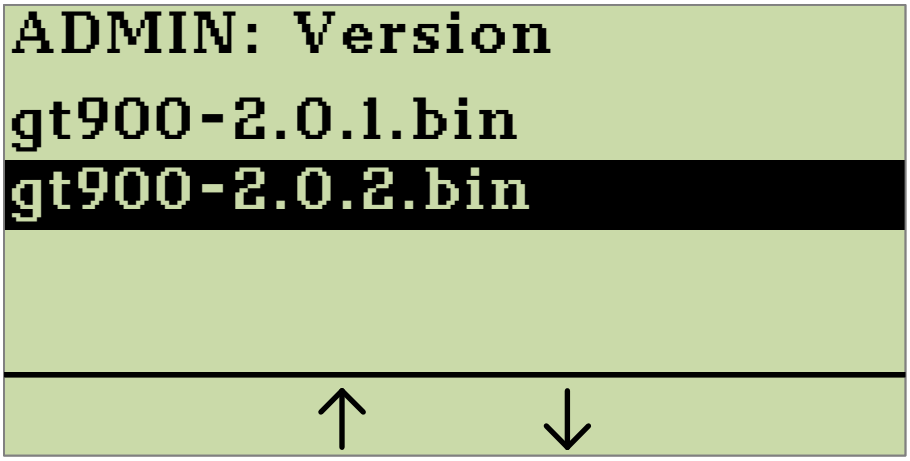
Abbildung 50: Submenü Admin:Version Firmware Update



Es wird das Einstecken eines USB-Sticks zur Durchführung eines Firmware-Updates erwartet.

Abbildung 51: Gerät ist bereit für Firmware Update

Stecken Sie den zuvor präparierten USB-Stick in die USB-Typ-A-Buchse Ihres Kartenterminals. In Abbildung 3 (Geräteanschlussbelegung) ist dieser Anschluss mit Position ① gekennzeichnet. Machen Sie sich gegebenenfalls nochmals mit den Anschlüssen des Kartenterminals vertraut (s. Kapitel 1.5 „Anschluss des Gerätes“). Nachdem der angesteckte USB-Stick nach gültigen Firmwaredateien durchsucht wurde, werden Ihnen diese zur Auswahl angezeigt.



Wählen Sie die Firmwaredatei aus, die Sie installieren möchten. (Beispielhafte Daten)

Abbildung 52: Auswählen der Firmwaredatei.

Mit den Tasten F2 und F3 können Sie zwischen verschiedenen Firmwaredateien wählen. Durch Drücken der ✓-Taste bestätigen Sie die Installation der im Display

hervorgehobenen Firmwaredatei (siehe Abbildung 52). Diese wird nun in den Speicher des Gerätes kopiert (siehe Abbildung 53).

Die zuvor ausgewählte Firmwaredatei wird nun in den Speicher des Gerätes kopiert.

Abbildung 53: Die Firmwaredatei wird in den Speicher kopiert.

Die sich nun im Speicher befindende Firmwaredatei wird, wie in Abbildung 54 dargestellt, einer Prüfung unterzogen. Wurde eine korrekt signierte Firmware gefunden, wird Ihnen die zu installierende Firmware-Version in einer Displaymeldung angezeigt.

Nach dem Kopiervorgang wird die Firmwaredatei einer Prüfung unterzogen.

Abbildung 54: Überprüfen des Firmware Updates

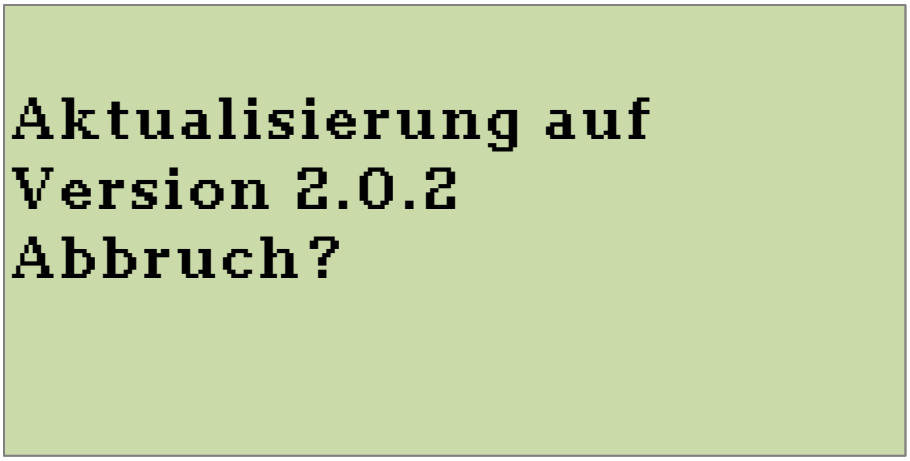


Abbildung 55: Anzeige der zu installierenden Firmware-Version

Überzeugen Sie sich, ob Sie die Firmware mit der angezeigten Versionsnummer installieren wollen. Sie können den Vorgang innerhalb von 10 Sekunden durch Drücken der -Taste abbrechen. Wenn Sie den Vorgang nicht abbrechen, wird nach 10 Sekunden die Firmware automatisch installiert. Bitte beachten Sie, dass eine Firmware mit niedriger Versionsnummer nur installiert werden kann, wenn diese zur gleichen Firmwaregruppe gehört. Lesen Sie dazu auch Kapitel 4.11.3 „Durchführung eines Firmware-Downgrade“. Die Versionsnummer der derzeit installierten Firmware wird Ihnen auf dem Display des einsatzbereiten Gerätes angezeigt (siehe Abbildung 13), oder Sie informieren sich über die Option **`Version`** im Admin-Menü.

Sollte eine falsch signierte Firmware erkannt werden oder ein Verdacht auf Kompromittierung bestehen, so wird die bestehende Firmware des Gerätes nicht geändert und das Gerät zeigt dies mit einer kurzen Statusanzeige („Verifikation Fehlgeschlagen“) an.

Wurde eine korrekt signierte Firmwaredatei erkannt, werden Sie eventuell aufgefordert, einen Freischaltcode einzugeben. Diesen erhalten Sie auf Antrag bei german telematics (s. Kapitel 9 „Kontakt“). Halten Sie dazu die Seriennummer und die MAC Adresse Ihres Terminals sowie die Versionsnummern der Ausgangsfirmware und

der neuen Firmware bereit. Nach erfolgreicher Eingabe des Freischaltcodes startet das Update.

Eine Mitteilung zeigt den Beginn des Updateprozesses an (siehe Abbildung 56). Anschließend wird für die Dauer des Updates eine Mitteilung im Display angezeigt, wie sie in Abbildung 57 zu sehen ist. Bitte unterbrechen Sie während des Updates nicht die Stromversorgung des Gerätes!

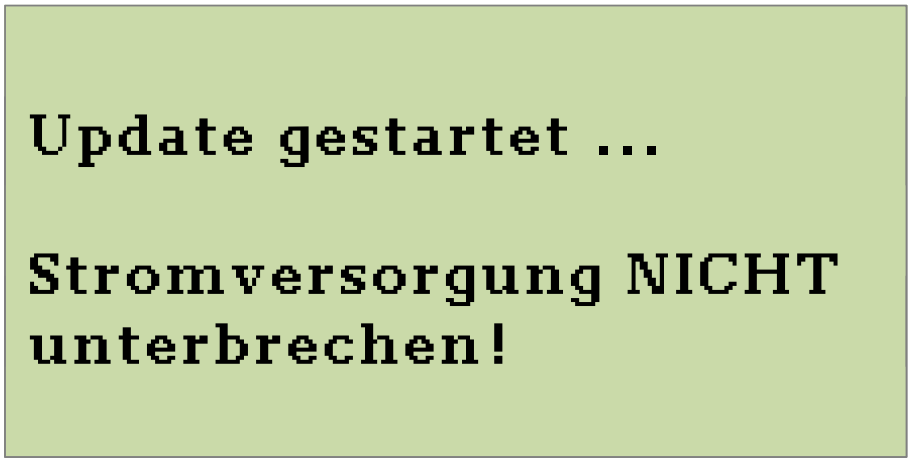
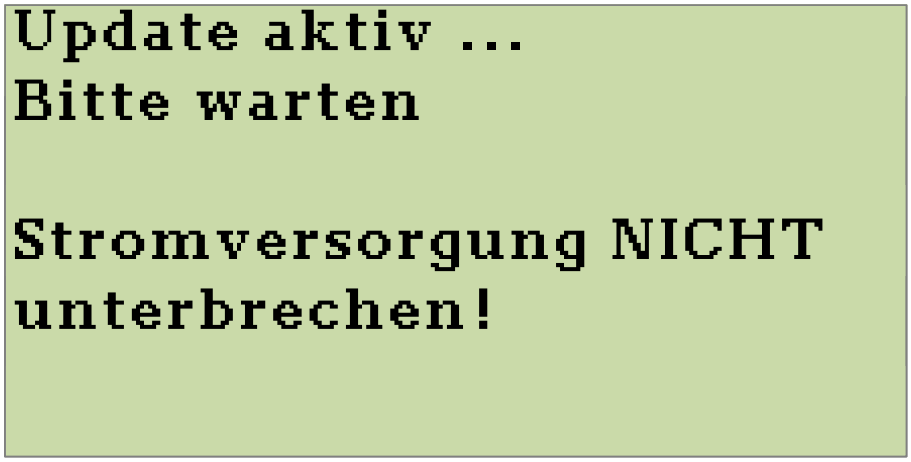
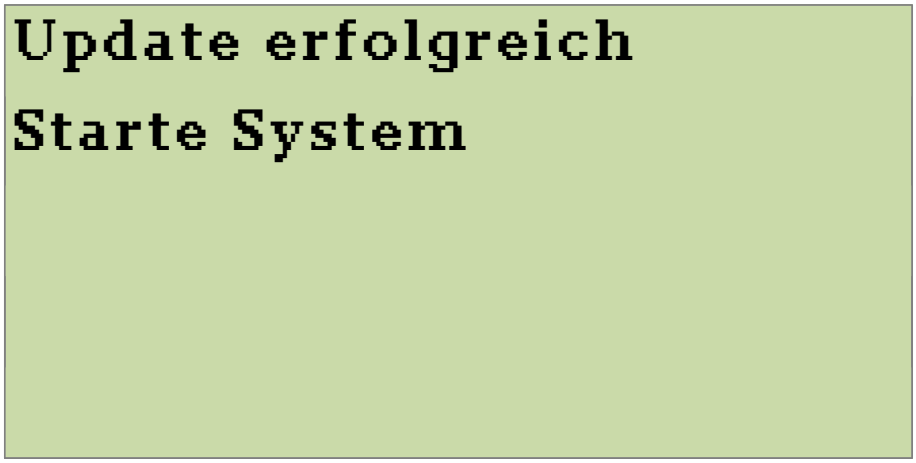


Abbildung 56: Der Updateprozess wird gestartet.



Während des Updatevorganges wird Ihnen diese Mitteilung angezeigt.

Abbildung 57: Das Update wird durchgeführt.



War das Firmware-Update erfolgreich, erscheint die nebenstehende Anzeige im Display.

Abbildung 58: Anzeige nach erfolgreichem Firmware-Update

Nach der erfolgreichen Installation wird Ihnen dies im Display des Kartenterminals angezeigt (siehe Abbildung 58). Die oben dargestellte Statusanzeige bleibt wenige Sekunden sichtbar; danach wird ein automatischer Neustart durchgeführt. Sie können nach dem Neustart die Versionsnummer der neu installierten Firmware in der unteren Statusleiste des Displays ablesen.

4.11.3 Durchführung eines Firmware-Downgrade

Unter besonderen Voraussetzungen ist ein sogenanntes Firmware-Downgrade zulässig. Dies bedeutet, dass Sie einen niedrigeren Firmwarestand als den derzeit installierten auf das Gerät aufspielen können. Ein solches Vorgehen ist nur innerhalb einer sogenannten Firmwaregruppe möglich. Eine Firmwaregruppe umfasst somit die Gesamtheit aller Firmware-Versionen, zwischen denen beliebig gewechselt werden kann. Beachten Sie, dass nach dem Einspielen einer älteren Firmware-Version der störungsfreie Betrieb des Terminals innerhalb der Telematikinfrastruktur nicht garantiert werden kann. Das Einspielen eines niedrigeren Firmwarestands folgt der gleichen Vorgehensweise wie in Kapitel 4.11.2 „Durchführung eines Firmware-Updates“ beschrieben. Während der Überprüfung der Firmware wird Ihnen jedoch der folgende Hinweis angezeigt werden:

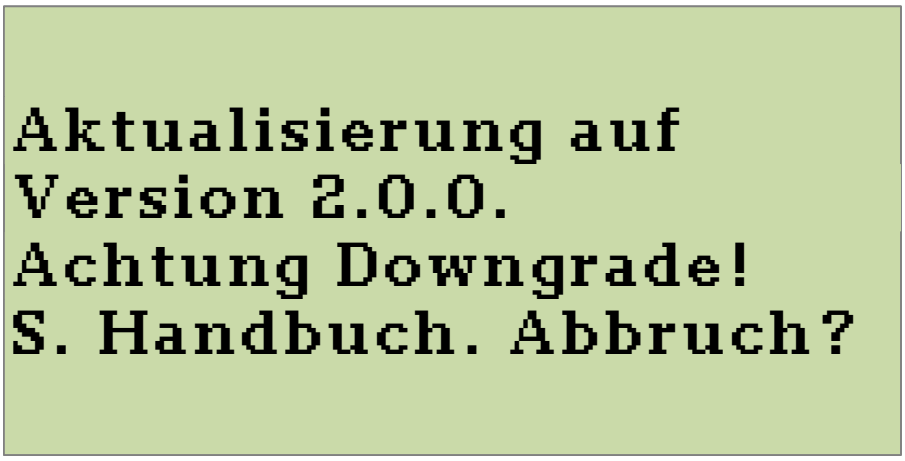


Abbildung 59: Abfrage zur Fortführung des Downgrades

Soll ein Downgrade ausgeführt werden, erhalten Sie die Möglichkeit, diesen vor der Ausführung abzubrechen. (Beispielhafte Versionsnummer)

Durch Drücken der ✗ -Taste können Sie das Einspielen des niedrigeren Firmwarestands abbrechen. Daraufhin wird das Gerät neu gestartet und Sie können wie gewohnt mit der alten Firmware weiterarbeiten. Die ✓ -Taste ist während dieser Anzeige funktionslos. Wenn Sie den Vorgang nicht abbrechen, wird nach 10 Sekunden automatisch die neue Firmware installiert.

4.11.4 Speichern von Update-Freischaltcodes

Um die automatische Durchführung von Firmwareupdates zu ermöglichen, können Sie einen Freischaltcode für ein zukünftiges Update im Update-PIN cache speichern. Drücken Sie dazu die F2 -Taste bis die Eingabeaufforderung für den Freischaltcode erscheint (s. Abbildung 60). Wenn Sie keinen oder einen falschen Freischaltcode speichern, wird das Kartenterminal während des Updatevorgangs (s. Kapitel 4.11.2) zur Eingabe des Freischaltcodes auffordern, sofern dieser für die Durchführung des Updates erforderlich ist.

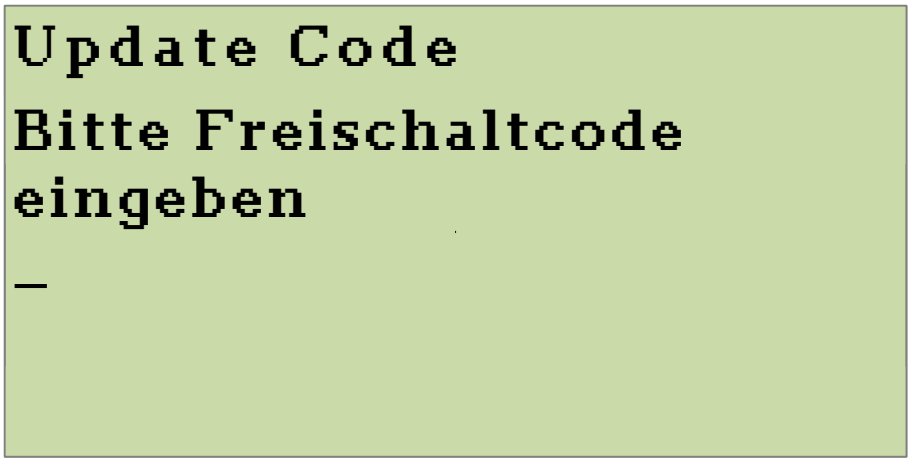


Abbildung 60: Eingabeaufforderung für den Freischaltcode

Geben Sie nun den Freischaltcode ein und bestätigen Sie Ihre Eingabe mit der ✓-Taste. Durch Drücken der ⇦-Taste können Sie Ihre Eingabe korrigieren und mit der ✗-Taste abbrechen. Um einen gespeicherten Freischaltcode anzuzeigen, halten Sie abermals die F2-Taste gedrückt (s. Abbildung 61, abgebildeter Freischaltcode ist Beispielhaft). In dieser Ansicht können Sie den Freischaltcode nochmals verändern.

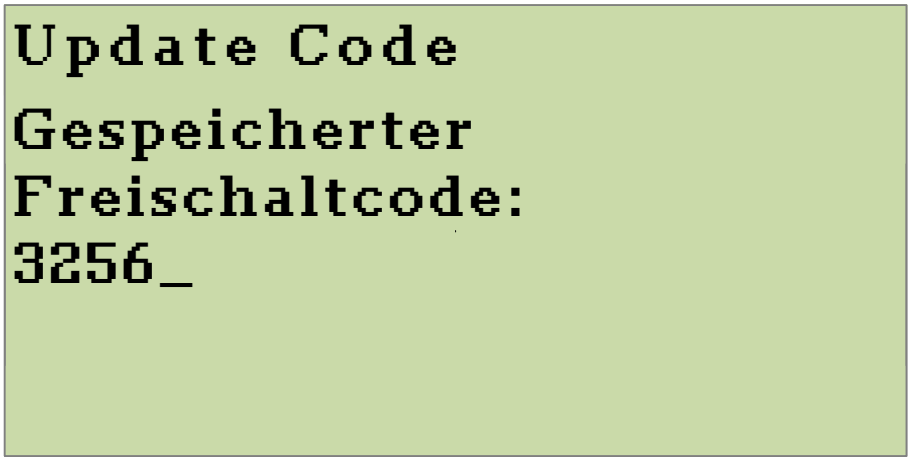


Abbildung 61: Anzeige des gespeicherten Freischaltcodes

Mit der ⇦-Taste können Sie den Freischaltcode löschen und mit der ✓-Taste eine neue Eingabe bestätigen. (Beispielhafter Code)

4.11.5 Auswahl der CA Liste (Vertrauensraum)

Das Kartenterminal kann in verschiedenen von der gematik vorgegeben Vertrauensräumen betrieben werden. Der momentan ausgewählte Vertrauensraum wird angezeigt, wenn Sie im Admin-Menü die Option **Version** wählen (siehe auch Abbildung 62). Hinter der Option **CA Liste** wird der gewählte Vertrauensraum angezeigt. Wenn Sie die Option mit der ✓ -Taste bestätigen, wird der Vertrauensraum umgeschaltet.

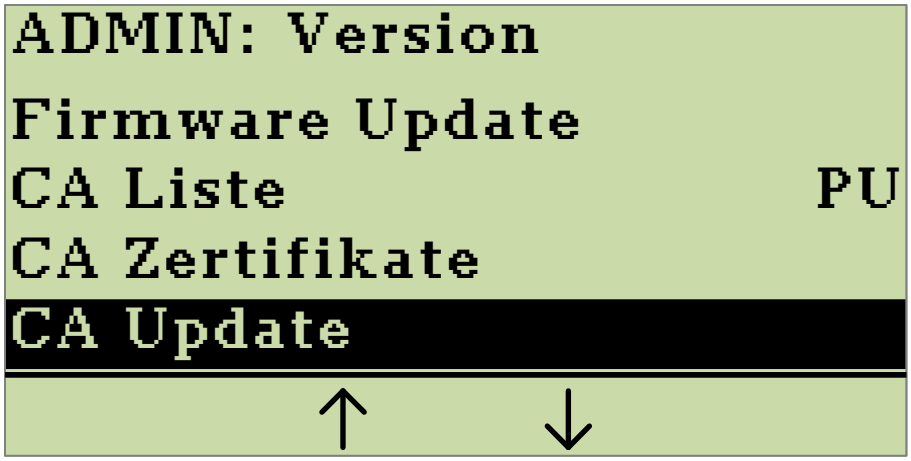
4.11.6 Anzeigen der installierten CA-Zertifikate

Um die installierten CA-Zertifikate anzuzeigen, wählen Sie im Admin-Menü die Option **Version** und danach **CA Zertifikate** (siehe auch Abbildung 62).

4.11.7 Update der CA-Liste

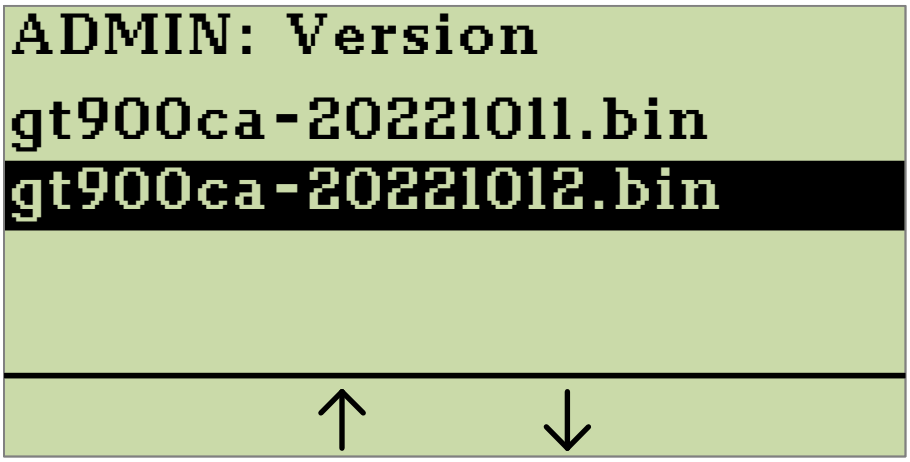
Sie können die Liste der Stammzertifizierungsstellen (CA) manuell aktualisieren. Um dies zu tun, wählen Sie in dem Admin-Menü die Option **Version** und bestätigen Sie mit der ✓-Taste. Auf dem Display wird Ihnen das Submenü **ADMIN: Version** angezeigt. Wählen Sie nun die Option **CA Update** und bestätigen Sie durch Drücken der ✓-Taste.

Schließen Sie, wie bei einem Firmwareupdate auch, einen USB-Stick mit den Zertifikatdateien an Ihr Kartenterminal an. Lesen Sie hierzu ggf. das Kapitel 4.11.2 „Durchführung eines Firmware-Updates“. Mit den Tasten F2 und F3 können Sie zwischen verschiedenen Zertifikatdateien wählen. Durch Drücken der ✓ -Taste bestätigen Sie die Installation der im Display hervorgehobenen Zertifikatdatei (siehe Abbildung 63). Das CA Update wird nun automatisch ausgeführt. Sollten falsch signierte Zertifikatdateien erkannt werden oder ein Verdacht auf Kompromittierung bestehen, so werden die bestehenden Zertifikate des Gerätes nicht geändert und das Gerät zeigt dies mit einer kurzen Statusanzeige („Verifikation Fehlgeschlagen“) an.



Drücken Sie die ✅-Taste, um die CA Liste zu aktualisieren.

Abbildung 62: CA Update

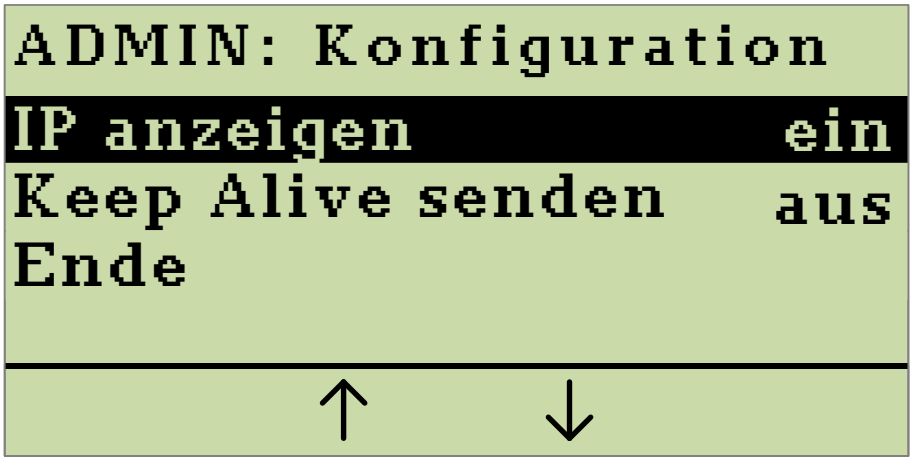


Wählen Sie eine Datei aus und drücken Sie die ✅-Taste, um die Zertifikatdatei zu installieren. (Beispielhafte Daten)

Abbildung 63: Wählen Sie die zu installierende Zertifikatdatei aus.

4.12 Aktuelle IP-Adresse anzeigen

Sie können sich in der Hauptdisplayanzeige (Abbildung 13) die aktuell vergebene IP-Adresse des Kartenterminals anzeigen lassen. Wenn diese Option eingeschaltet ist, wird bei einer bestehenden Netzwerkverbindung auch die IP-Adresse des verbundenen Konnektors angezeigt. Um die IP-Adresse anzuzeigen, wählen Sie in dem Admin-Menü die Option **`Konfiguration`** und bestätigen dies mit der ✅-Taste. Auf dem Display wird Ihnen das Submenü **`ADMIN: Konfiguration`** angezeigt.



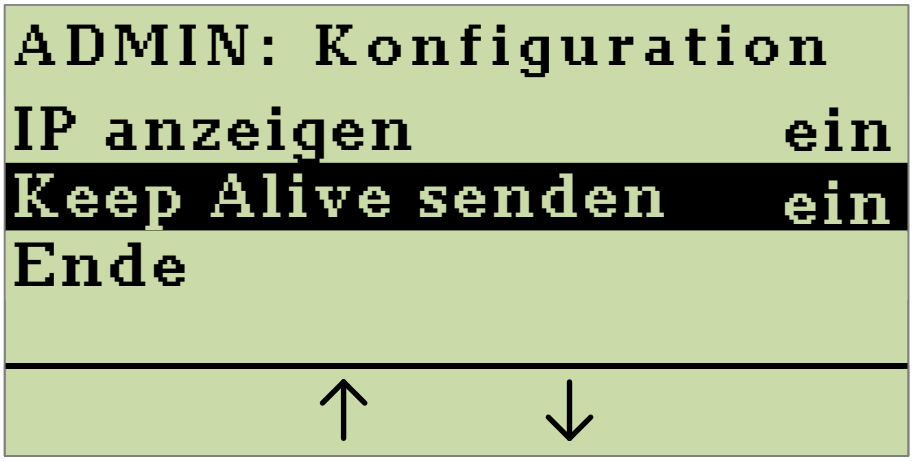
Drücken Sie die ✓-Taste, um die Anzeige der IP-Adresse ein- oder auszuschalten.

Abbildung 64: Anzeige des Submenüs "Konfiguration"; IP anzeigen

Mit den Tasten F2 und F3 wählen Sie die Option **IP anzeigen** aus. Drücken Sie nun die ✓-Taste, um die Option **IP anzeigen** wahlweise **Ein** oder **Aus** zu schalten. Sie können das Menü über den Menüpunkt **Ende** oder durch Drücken der ✗-Taste verlassen.

4.13 Keep Alive senden

Mechanismen der TCP Übertragungsprotokolle können bei Netzwerkfehlern unter Umständen dazu führen, dass lange Wartezeiten entstehen, bis ein entsprechender Fehler an höhere Schichten gemeldet wird. Um dem Kartenterminal zu ermöglichen, solche Fehler der Netzwerkschichten frühestmöglich zu erkennen, kann das Kartenterminal alle 10 Sekunden Keep Alive Ereignisse als „Heartbeat“ an den Konnektor versenden. Der Status des Versendens eines solchen Ereignisses gibt Auskunft über die Lebendigkeit der Verbindung. Werden vom Kartenterminal Keep Alive Ereignisse versandt, so wird das Kartenterminal die Netzwerkverbindung selbständig abbauen, wenn es vom Konnektor 120 Sekunden lang keinerlei Nachrichten empfangen hat. Um die Keep Alive-Funktion zu nutzen, wählen Sie in dem Admin-Menü die Option **Konfiguration** und bestätigen dies mit der ✓-Taste. Auf dem Display wird Ihnen das Submenü **ADMIN: Konfiguration** angezeigt.



Drücken Sie die ✓-Taste, um Keep Alive ein- oder auszuschalten.

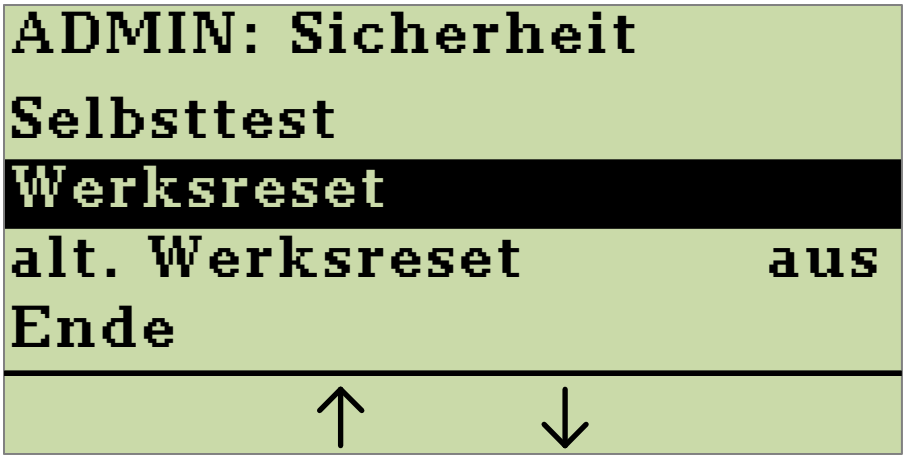
Abbildung 65: Anzeige des Submenüs "Konfiguration"; Keep Alive

Wählen Sie nun mit den Tasten F2 und F3 die Option **Keep Alive senden** aus. Drücken Sie die ✓-Taste, um die Option **Keep Alive senden** wahlweise **Ein** oder **Aus** zu schalten. Sie können das Menü über den Menüpunkt **Ende** oder durch Drücken der ✗ -Taste verlassen. Die Keep Alive Funktion ist per Werkseinstellung (d.h. nach der Erstinbetriebnahme) aktiviert.

5 Gerät zurücksetzen

5.1 Zurücksetzen mit Kenntnis der Admin PIN

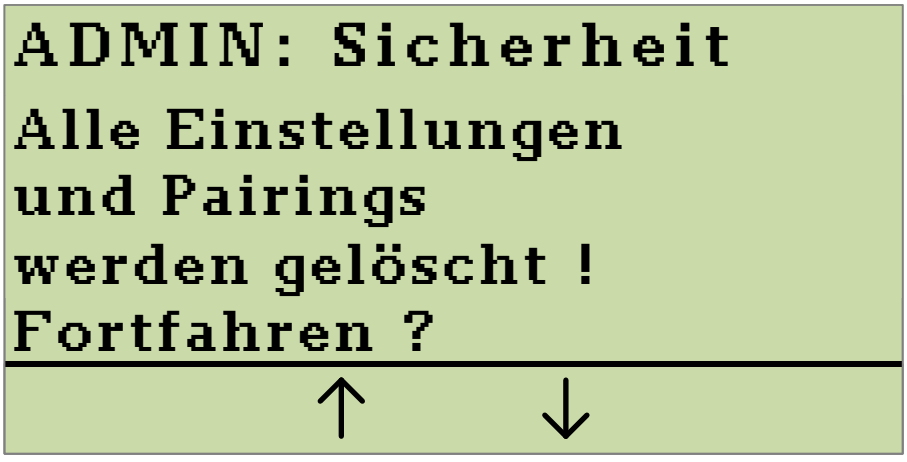
Um das Gerät in den Auslieferungszustand zu versetzen, wählen Sie im Admin-Menü (siehe Kapitel 4.1 „Admin-Menü“) die Option **Sicherheit** und bestätigen dies mit der OK-Taste. Auf dem Display wird Ihnen das Submenü **ADMIN: Sicherheit** angezeigt.



Drücken Sie die ✓-Taste, um einen Werksreset auszuführen.

Abbildung 66: Anzeige des Submenüs "Sicherheit"

Wählen Sie die Option **`Werksreset`** und bestätigen Sie diesen Menüpunkt durch Drücken der ✓-Taste. In dem daraufhin angezeigten Dialog werden Sie gebeten, die Durchführung des Werksresets zu bestätigen. Durch das Drücken der ✓-Taste wird der Werksreset gestartet. Durch Drücken der ✗-Taste können Sie den Dialog abbrechen und der Werksreset wird nicht durchgeführt.



Sicherheitsabfrage beim Zurücksetzen des Gerätes in den Auslieferungs-zustand.

Abbildung 67: Sicherheitsabfrage beim Werksreset

Haben Sie die Sicherheitsabfrage durch Drücken der ✓-Taste bestätigt, wird das Gerät in den Auslieferungszustand zurückversetzt.

5.2 Zurücksetzen ohne Kenntnis der Admin PIN

Als Reset-Administrator können Sie das Kartenterminal mittels PUK (siehe Kapitel 5.2.1) oder durch ein sicheres Challenge-Response-Verfahren (siehe Kapitel 5.2.2) auch ohne Kenntnis der Admin PIN in den Werkszustand zurücksetzen.

5.2.1 Zurücksetzen mittels PUK

Drücken Sie zunächst die F1 -Taste des eingeschalteten Kartenterminals für mindestens 5 Sekunden, bis Sie aufgefordert werden, die Admin PIN einzugeben. Drücken Sie die F1 -Taste nochmals (ohne vorher die Admin PIN eingegeben zu haben). Sie werden nun aufgefordert, den während der Erstinbetriebnahme vergebenen PUK einzugeben.

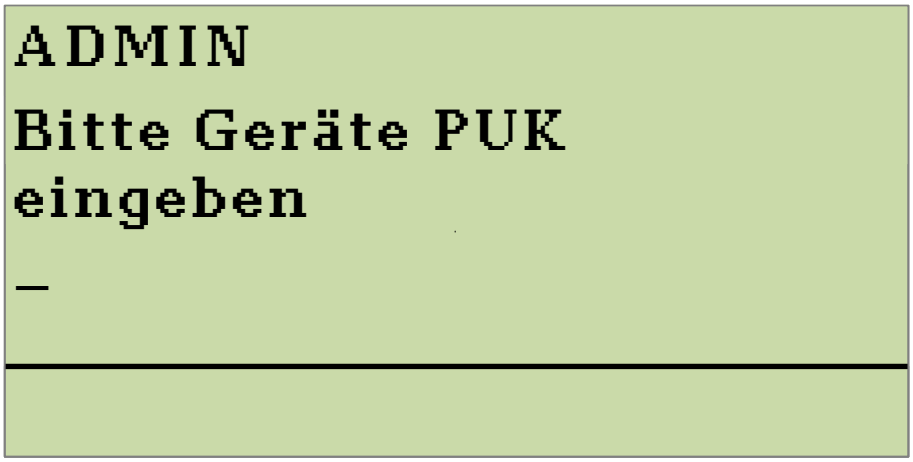


Abbildung 68: Eingabeaufforderung des PUK

Wenn Sie den PUK korrekt eingegeben haben werden Sie gebeten, das Zurücksetzen des Gerätes in den Auslieferungszustand zu bestätigen, so wie es in Abbildung 67 dargestellt ist. Sie können diesen Dialog durch Drücken der ✓ -Taste bestätigen oder durch Betätigen der ✗ -Taste abbrechen. Sollten Sie den PUK dreimal falsch eingeben, ist ein erneuter Eingabeversuch erst nach einem gewissen Zeitraum möglich. Bei mehreren Falscheingaben verlängert sich der Zeitraum entsprechend, siehe

Tabelle 2. Haben Sie die Sicherheitsabfrage durch Drücken der  -Taste bestätigt, wird das Gerät nun in den Auslieferungszustand zurückversetzt.

5.2.2 Zurücksetzen ohne Kenntnis des PUK

Um das Kartenterminal ohne Kenntnis der Admin PIN und des PUK in den Auslieferungszustand zurückzusetzen, muss der alternative Werksreset gemäß Kapitel 4.10 „Alternativen Werksreset einschalten“ vom Administrator aktiviert worden sein.

Für die Durchführung eines alternativen Werksresets wenden Sie sich bitte an Ihren Administrator. Dieser muss von Ihnen autorisiert sein und erhält dann auf Antrag bei german telematics die genauen Anweisungen und Daten, um den alternativen Werksreset durchführen zu können.

6 Weboberfläche nutzen

Ihr Kartenterminal verfügt über eine Weboberfläche zur Geräteadministration, die Sie am Computer in einem Internetbrowser öffnen können. Den Zugriff auf diese Weboberfläche können Sie ein- oder ausschalten. Diese Weboberfläche ist nur erreichbar, wenn eine gSMC-KT in das Kartenterminal eingelegt wurde, da das Zertifikat für den gesicherten Verbindungsaufbau von der gSMC-KT zur Verfügung gestellt wird.

In der Weboberfläche richten Sie das Kartenterminal ein, schalten Funktionen ein oder aus und erhalten Informationen über ihr Kartenterminal und zu bestehenden Pairings.

Wie Sie diese Weboberfläche zur Benutzung freischalten, erfahren Sie im Kapitel 4.7 „Remote-Management Schnittstelle aus- oder “. Schalten Sie die Weboberfläche nur dann ein, wenn das Netzwerk unter Ihrer vollständigen Kontrolle steht.

Um auf die Weboberfläche zugreifen zu können, benötigen Sie einen Computer mit installiertem Webbrowser. Zudem muss das Netzwerk in dem sich das Kartenterminal befindet von diesem Computer aus erreichbar sein. Bitte beachten Sie, dass Ihr Webbrowser zum erfolgreichen Verbindungsaufbau die Transportschichtsicherheit TLS 1.2 unterstützen muss. Alle gängigen Browser erfüllen das und sind geeignet. Die Nutzung des Firefox Browsers wird empfohlen.

Geben Sie Folgendes in die Adresszeile Ihres Webbrowsers ein:

https://<IP-Adresse des Kartenterminals>

Wie Sie sich die IP-Adresse im Display des Terminals anzeigen lassen können, entnehmen Sie ggf. dem Kapitel 4.12 „Aktuelle IP-Adresse anzeigen“.

Abbildung 70 zeigt die Darstellung der Weboberfläche in einem Browsertab des Firefox Browsers.

Bitte beachten Sie, dass es beim erstmaligen Aufbau der Verbindung zu einem Zertifikatfehler kommt. Dies ist der Tatsache geschuldet, dass das Kartenterminal zur Kommunikationsabsicherung (TLS 1.2) das Zertifikat einer eingelegten gSMC-KT verwendet. Da dieses Zertifikat den Internetzertifizierungsstellen unbekannt ist, wird korrekterweise vor einem Aufbau der Verbindung gewarnt. Stellen Sie daher zunächst sicher, dass keine Manipulation an der gSMC-KT vorgenommen wurde und die SIM-Slotversiegelung intakt ist. Sie können die Zertifikatwarnung übergehen indem Sie im Browser eine Ausnahme für diese Verbindung hinzufügen. Ein entsprechender Dialog ist in Abbildung 69 beispielhaft für den Firefox Browser dargestellt.

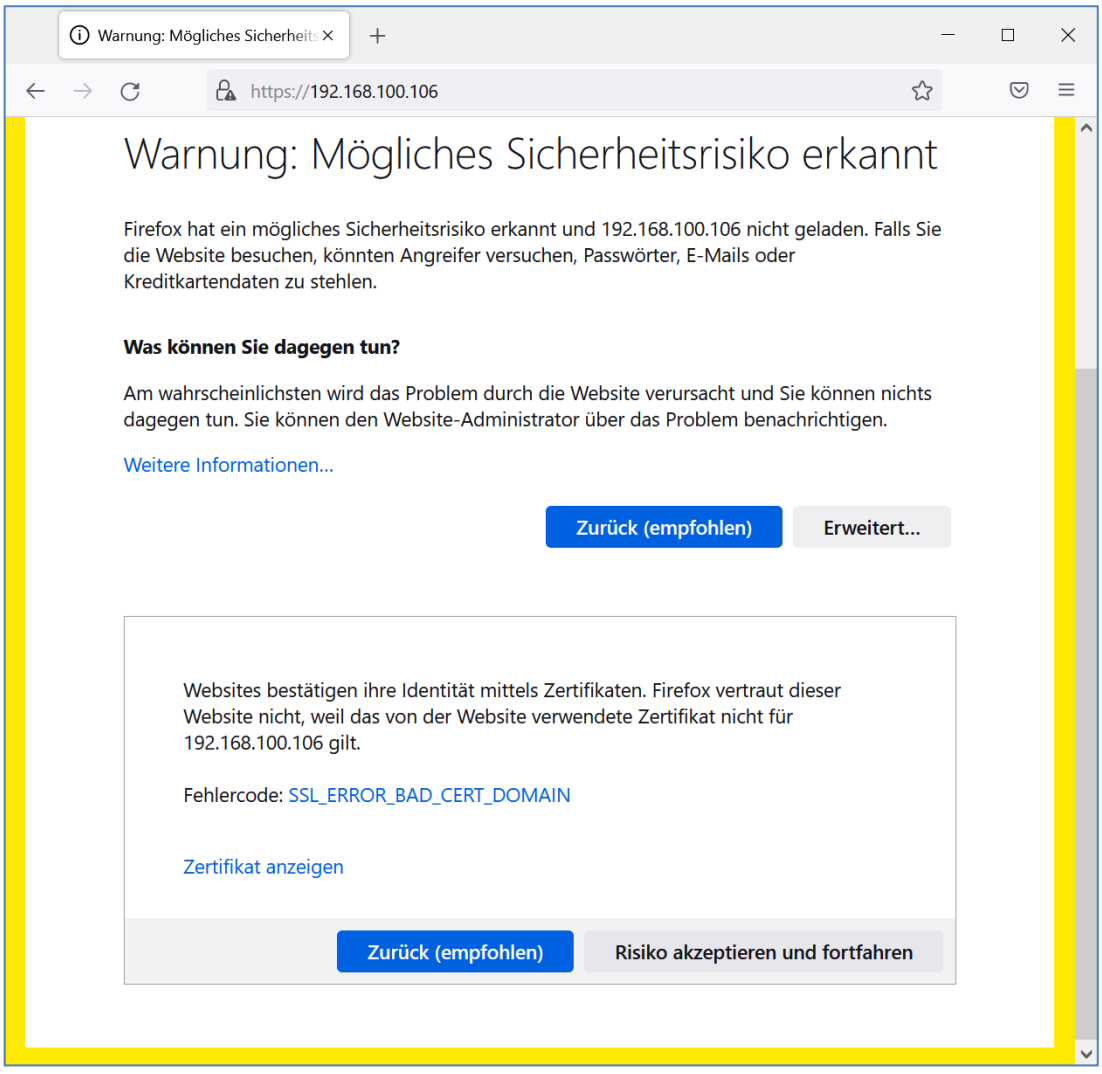


Abbildung 69: Mögliche Anzeige einer Zertifikatwarnung im Browser.

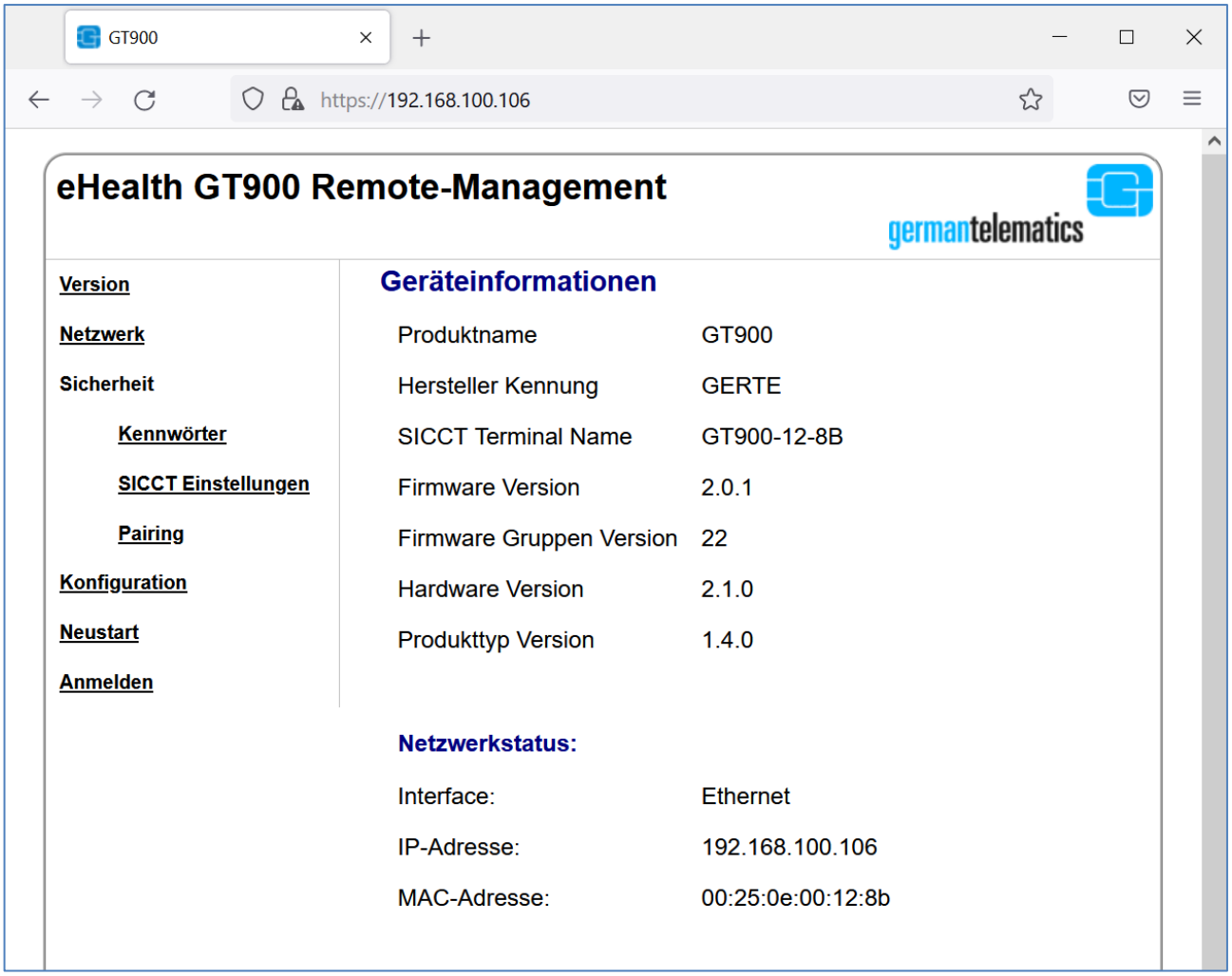


Abbildung 70: Weboberfläche des Kartenterminals nach dem Verbindungsaufbau.

Die Weboberfläche bietet Ihnen nach Eingabe Ihrer Remote-Management PIN (siehe Abbildung 71) die Möglichkeit, einige der Einstellungen, die Sie auch am Gerät vornehmen können, bequem aus der Ferne zu erledigen. Hierzu gehören insbesondere:

- Die Anzeige der Geräteinformationen,
- das Einstellen der Netzwerkparameter,
- die Änderung des Remote-Management Kennwortes (PIN),
- die Änderung des SICCT Kennwortes (PIN),
- das Anzeigen und Löschen vorhandener Pairings,
- das Vornehmen von SICCT Einstellungen,

- sowie das Ändern von Gerätekonfigurationen.

Sobald einer der Menüpunkte unterhalb „Version“ gewählt wird muss sich der Administrator anmelden. Geben Sie beim ersten Anmeldevorgang an der Weboberfläche die am Kartenterminal vergebene Remote-Management PIN ein (siehe Kapitel 4.7).

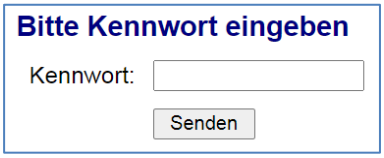


Abbildung 71: Eingabe der Remote-Management PIN zur Freigabe der Weboberfläche

6.1 Netzwerkeinstellungen vornehmen

Um in der Weboberfläche Einstellungen an den Netzwerkparametern vorzunehmen, wählen Sie den Menüpunkt „Netzwerk“. Ihnen werden nun die bereits bekannten Einstellungen für die Netzwerkparameter des Kartenterminals angezeigt. Zusätzlich wird der aktuelle Status angezeigt.

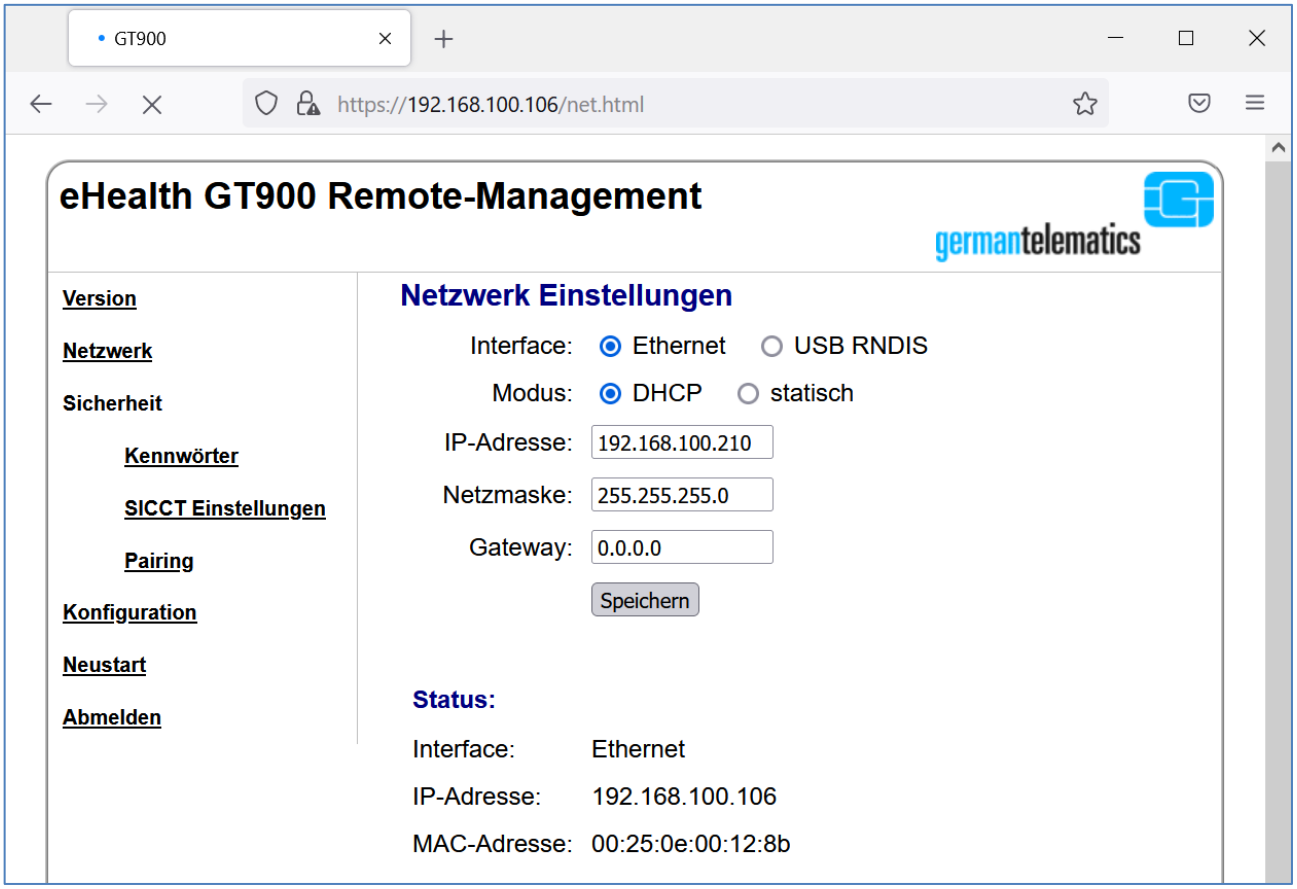


Abbildung 72: Netzwerkkonfiguration über die Weboberfläche

Sollte das Kartenterminal gerade mit einem Konnektor verbunden sein, wird ein entsprechender Hinweis angezeigt und ein Speichern ist nicht möglich. Dies verhindert ein versehentliches Trennen der Verbindung zum Konnektor.

Abbildung 73: Hinweis auf eine aktive Verbindung zu einem Konnektor

Trennen Sie in diesem Fall im Konnektor die Netzwerkverbindung zum Kartenterminal, z.B. durch Deaktivieren des Terminals, und rufen die Netzwerk Einstellungen erneut auf. Wenn Sie dann alle Änderungen vorgenommen haben und speichern, wird das Netzwerk im Kartenterminal sofort neu gestartet und die Einstellungen übernommen.

6.2 Kennwort der Remote-Management Schnittstelle ändern

Im Menüpunkt „Kennwörter“ können Sie im oberen Abschnitt ein neues Kennwort für die Remote-Management Schnittstelle vergeben. Sie sind an dieser Stelle nicht nur auf die Zahlentasten Ihres Kartenterminals beschränkt und können daher auch Kennwörter anstelle der sonst üblichen PIN vergeben.

Auch das Kennwort muss aus mindestens 8 und höchstens 16 Zeichen bestehen, kann nun aber zusätzlich zu Ziffern auch Buchstaben und Sonderzeichen enthalten. Sie können jedoch keine Teilzeichenkette von „Administrator“ als Bestandteil des Passworts wählen. So wird z.B. „Admin123“ als Passwort abgelehnt.

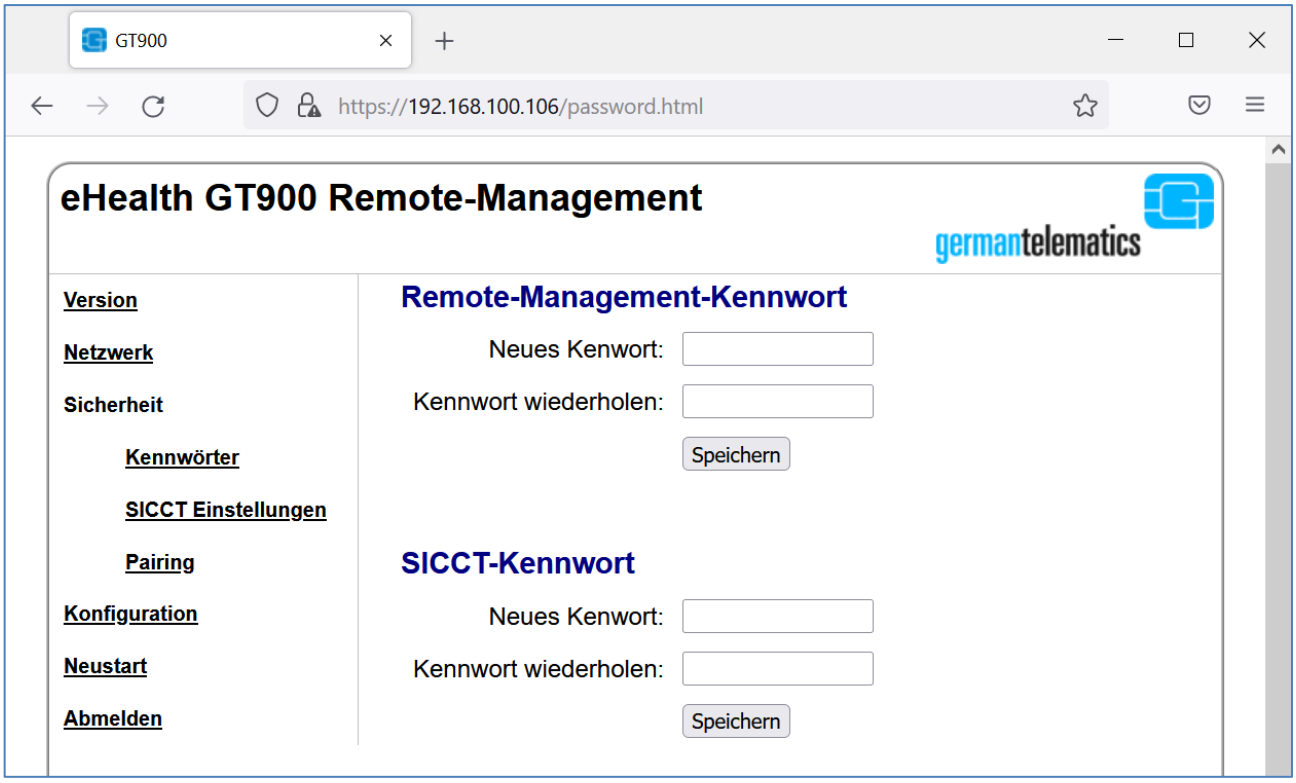


Abbildung 74: Setzen neuer Kennwörter für die Remote-Management Schnittstelle und für SICCT

Hinweise zum Umgang mit den Kennwörtern der Remote-Management Schnittstelle

Halten Sie die vergebenen Kennwörter geheim. Stellen Sie bei der Eingabe der Kennwörter sicher, dass niemand sonst diese lesen kann. **Verwenden Sie keine trivialen[6] Kennwörter**. **Vermeiden Sie es, die Kennwörter in der Nähe des Gerätes aufzubewahren.** Das Remote-Management Kennwort ermöglicht Ihnen den Zugriff auf die Managementschnittstellen Ihres Kartenterminals und erlaubt somit das Abfragen und Ändern von sicherheitskritischen Konfigurationen.

Bitte beachten Sie, dass alle Kennwörter, die Sie über die Remote-Management Schnittstelle vergeben, mindestens eine Zahl enthalten müssen.

6.3 SICCT Kennwort ändern

Im Menüpunkt „Kennwörter“ können Sie im unteren Abschnitt auch ein neues SICCT Kennwort als SICCT PIN (siehe Kapitel 4.6 „Ändern der SICCT PIN“) vergeben. Bei der Erstinbetriebnahme des Kartenterminals wurde die SICCT PIN automatisch mit der Admin PIN vorbelegt. Sie sind an dieser Stelle nicht nur auf die Zifferntasten Ihres Kartenterminals beschränkt und können daher auch Kennwörter anstelle der sonst üblichen Ziffernfolgen vergeben.

Das SICCT Kennwort muss aus 8 bis 12 Zeichen (A-Z, a-z, 0-9, ()-+=:‘,./? und Leerzeichen) bestehen, kann nun aber zusätzlich zu Ziffern auch Buchstaben und Sonderzeichen enthalten. Sie können jedoch keine Teilzeichenkette von „Administrator“ als Bestandteil des Passworts wählen. So wird z.B. „Admin123“ als Passwort abgelehnt.

6.4 Pairings einsehen und löschen

Über die Weboberfläche können Sie die Pairings Ihres Kartenterminals einsehen und ggf. einzelne Pairingschlüssel, einzelne Pairingblöcke oder alle Pairings löschen. Nach einem Löschen wird eine aktive Netzwerkverbindung vom Konnektor nicht getrennt. Erst bei einem erneuten Verbindungsaufbau wird das Pairing überprüft. Wurde das Pairing für diesen Konnektor gelöscht, scheitert dann bestimmungsgemäß der Verbindungsaufbau.

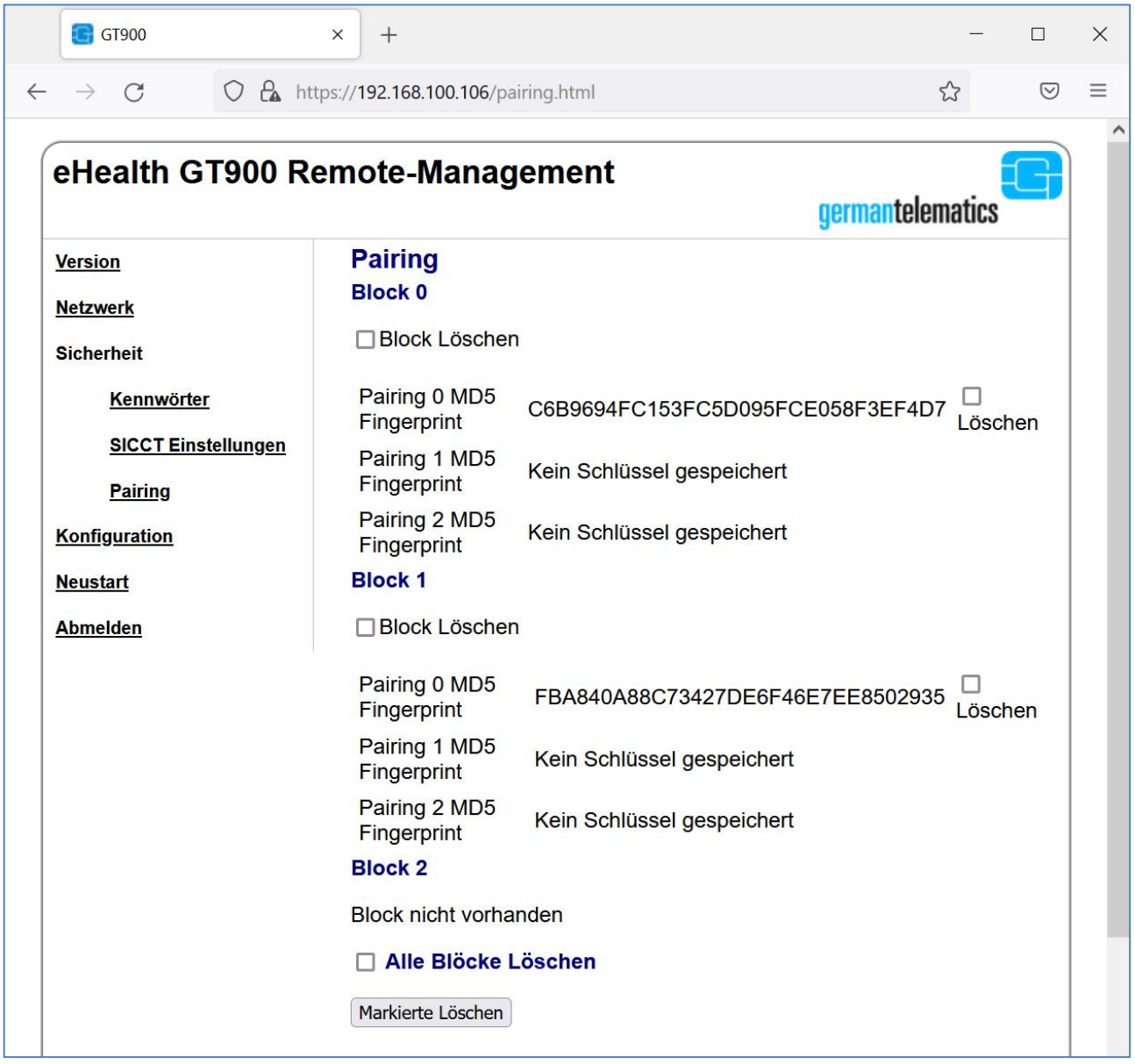


Abbildung 75: Einsehen der Pairings des Kartenterminals mit Lösch-Möglichkeiten

6.5 SICCT Einstellungen

Im Menüpunkt „SICCT-Einstellungen“ können Sie SICCT Update und SICCT Konfiguration aktivieren bzw. deaktivieren (siehe hierzu auch Kapitel 4.4 „SICCT Update ein- oder ausschalten“ und Kapitel 4.5 „SICCT Konfiguration ein- oder ausschalten“).

Zusätzlich können Sie den Namen Ihres Kartenterminals festlegen. Mit einem eindeutigen Namen lässt sich Ihr Kartenterminal einfacher in einer größeren SICCT-konformen Infrastruktur identifizieren. Der Terminalname kann maximal aus 32 Zeichen (Erlaubt: 'A-Z', 'a-z', '0-9'. Ebenso '_' und '.' (nicht an Anfang/Ende).) bestehen.

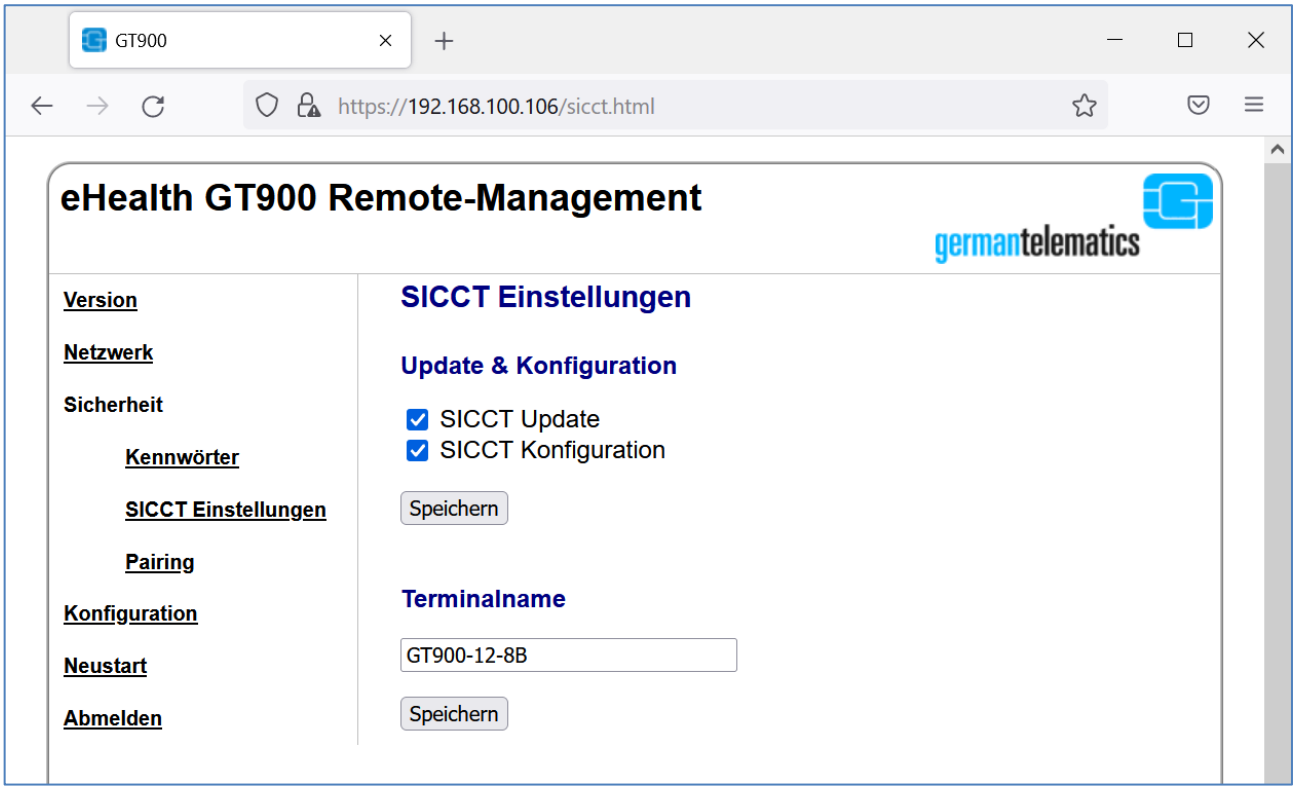


Abbildung 76: SICCT Einstellungen vornehmen

6.6 Konfiguration

Im Menüpunkt „Konfiguration“ können verschiedene Einstellungen vorgenommen werden.

Um die Keep Alive-Funktion zu nutzen, aktivieren Sie die entsprechende Checkbox. Zur Funktionsweise von Keep Alive lesen Sie bitte Kapitel 4.13 „Keep Alive senden“.

Sie können sich in der Hauptdisplayanzeige (Abbildung 13) die aktuell vergebene IP-Adresse des Kartenterminals anzeigen lassen. Um die IP-Adresse anzuzeigen, aktivieren Sie die entsprechende Checkbox. Klicken Sie anschließend auf „Speichern“.

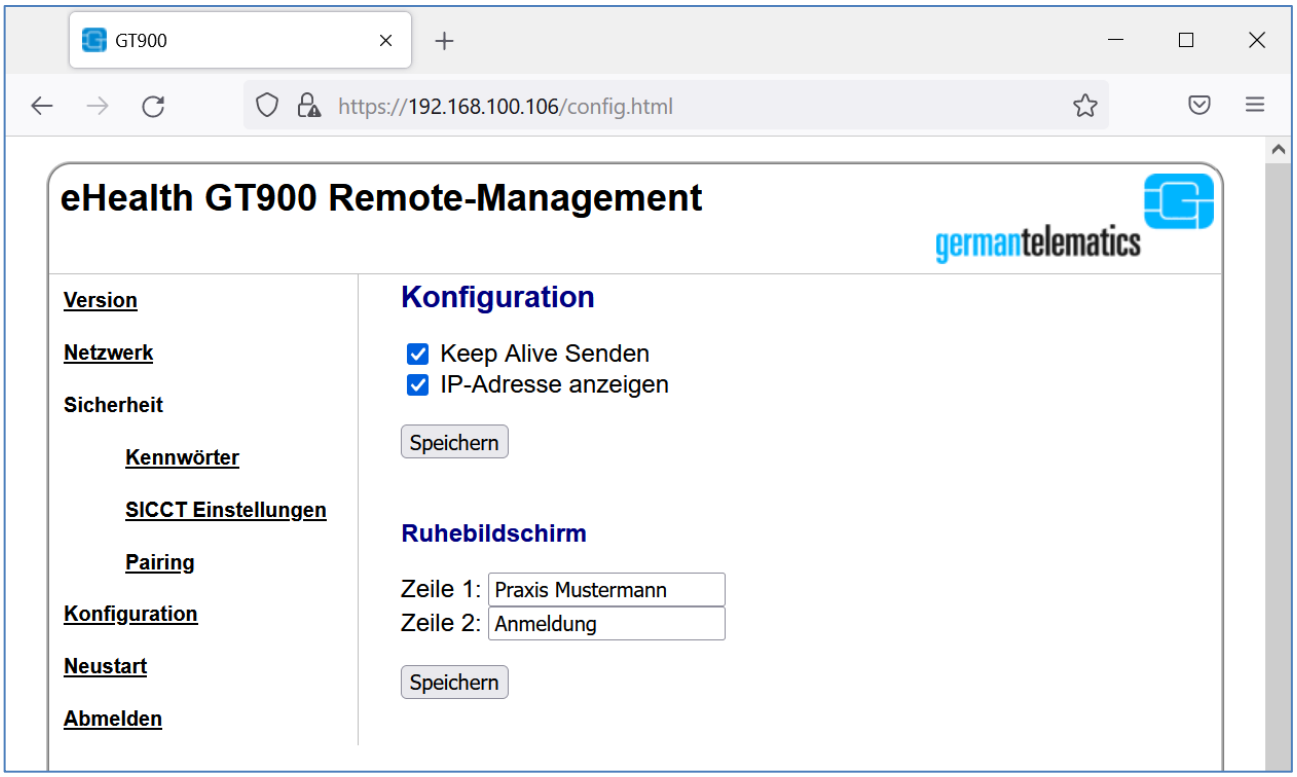


Abbildung 77: Gerätekonfiguration vornehmen

Außerdem können Sie einen Text für den Ruhebildschirm vorgeben. Dort werden nach der Erstinbetriebnahme die Zeilen „german telematics“ und „GT900 eHealth SICCT“ angezeigt. Sie können diese beiden Zeilen individuell ändern.

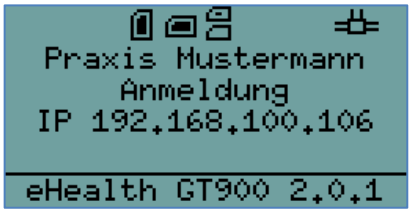


Abbildung 78: Displayanzeige nach Änderung wie in vorheriger Abbildung

6.7 Neustart

Im Menüpunkt „Neustart“ können Sie die Hardware der Kartenterminals komplett neustarten. Nach Klicken auf „Hardware-Neustart“ wird dieser ohne weitere Nachfrage sofort ausgeführt.

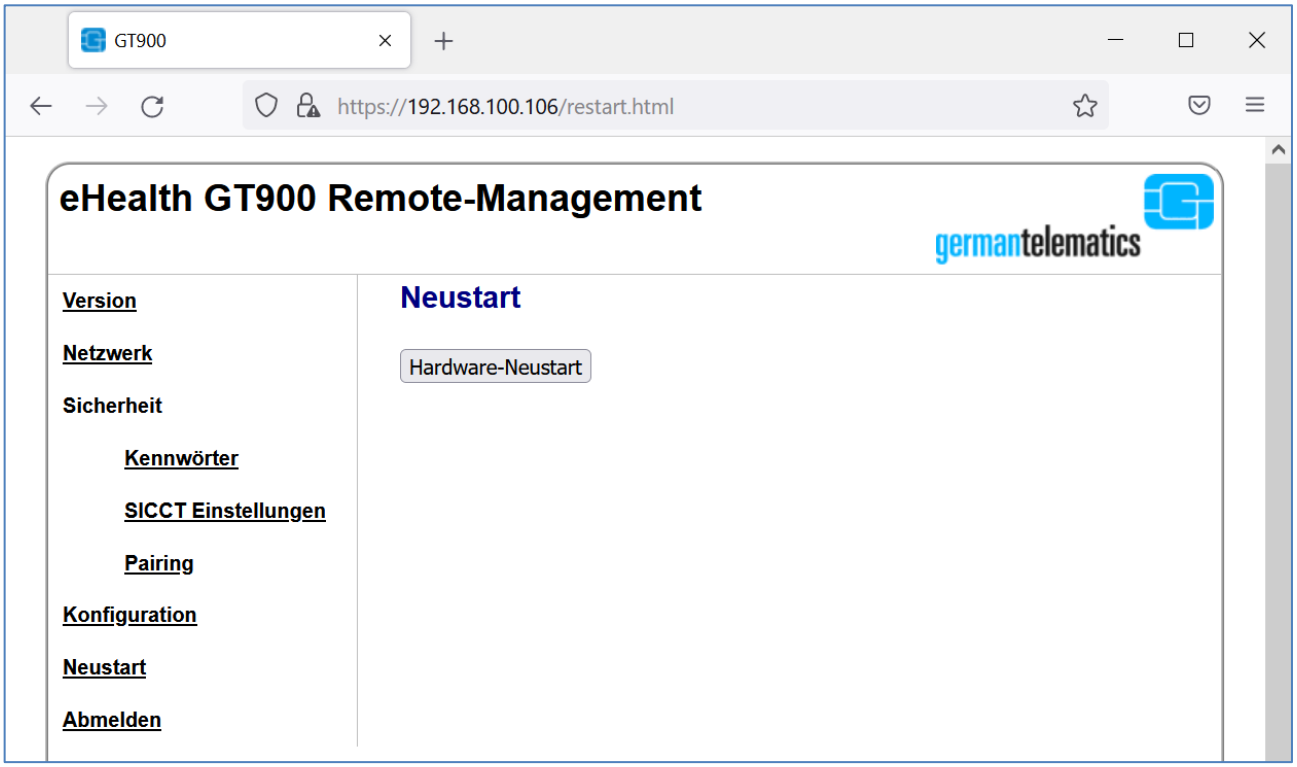


Abbildung 79: SICCT Einstellungen vornehmen

Sollte ein Konnektor aktiv mit dem Kartenterminal verbunden sein, ist der Neustart-Button erst einmal deaktiviert um ein versehentliches Trennen zu verhindern. Sollten Sie den Neustart dennoch durchführen wollen, können Sie den Button durch Ankreuzen der Warnmeldung aktivieren und danach den Neustart durchführen.

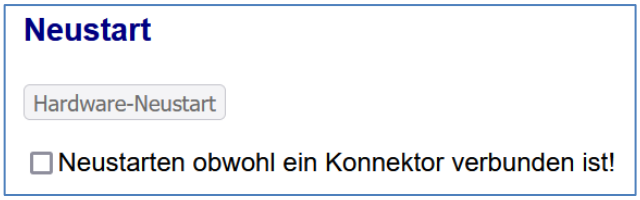


Abbildung 80: Warnung bei aktiver Konnektorverbindung

7 Qualifizierte elektronische Signaturen

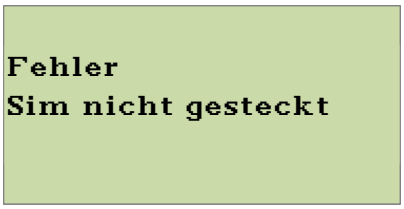
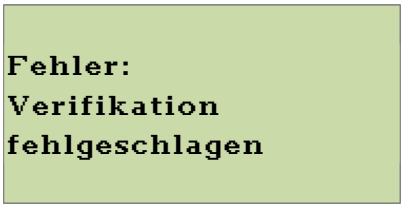
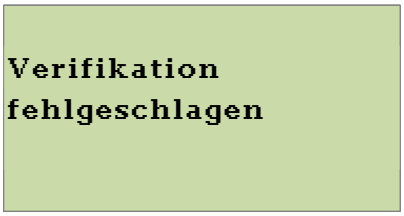
Um qualifizierte elektronische Signaturen (QES) zu erstellen, müssen Sie das Gerät mit einem QES-fähigen Konnektor sowie einer vom Konnektor unterstützten Signaturkarte (eHBA) betreiben.

Das Kartenterminal unterstützt die Erzeugung einer qualifizierten elektronischen Signatur durch die sichere Eingabe der QES-PIN und die dadurch erzeugte Freischaltung der Signaturkarte. Typischerweise sind diese angezeigten Informationen, Aufforderungen oder Warnungen zur PIN-Eingabe selbsterklärend und bedürfen keiner weiteren Erläuterung.

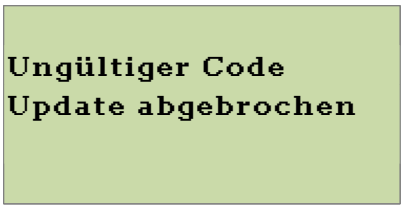
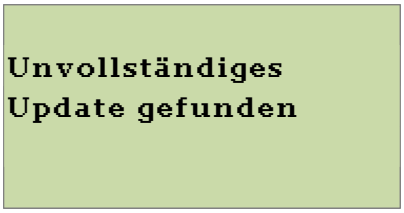
8 Problembehebung

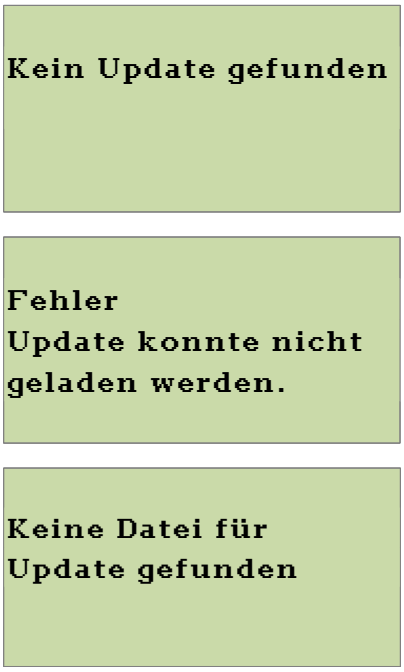
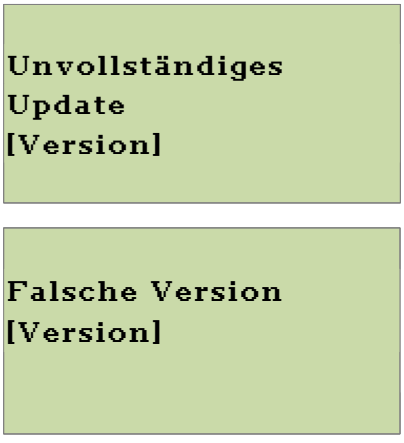
In diesem Kapitel wird auf mögliche Betriebsstörungen und deren Behebung eingegangen.

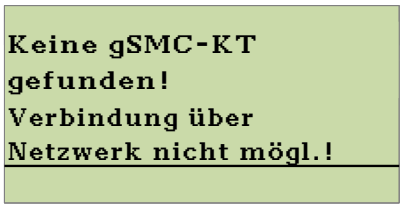
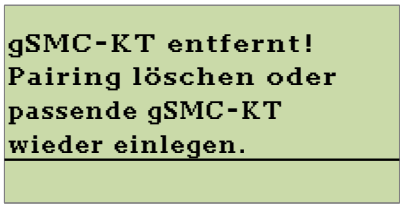
Fehlerbeschreibung	Ursache	Behebung
Nach einem Neustart oder während des Betriebs erscheint eine der folgenden Statusanzeigen: **Fehler** **Systemfehler** **Fehler [Nr]** **Einbruchsicherung** **Gerät überprüfen** **Fehler** **Tastaturfehler** **Gerät überprüfen** **Fehler** **Selbsttest** **fehlgeschlagen**	Auf Ihr Gerät könnte ein hardwareseitiger Angriff vorgenommen worden sein. Dies stellt eine direkte Bedrohung zu den mit diesem Gerät zu verarbeitenden Daten dar. Eine Sicherheitsfunktion hat dies erkannt und informiert Sie darüber.	Kontaktieren Sie einen zertifizierten Techniker oder den Hersteller. Geben Sie die Fehlerbeschreibung an und erbitten Sie weitere Hilfe.

Fehlerbeschreibung	Ursache	Behebung
Es erscheint folgende Statusanzeige: 	Eine der SIM-Karten aus den am Gerät rechtsseitigen SIM-Slots wurde, während das Gerät mit der Stromversorgung verbunden ist, entfernt. Eine Sicherheitsfunktion hat dies erkannt und informiert Sie darüber.	Stecken Sie die SIM-Karte und/ oder den Simkartenträger wieder in den SIM-Slot. Stellen Sie sicher, dass sich in beiden SIM-Slots des Gerätes die Simkartenträger befinden. Starten Sie das Gerät mit der ✓ -Taste neu. Sollten weiterhin Probleme auftauchen, so kontaktieren Sie einen zertifizierten Techniker oder den Hersteller. Geben Sie die Fehlerbeschreibung an und erbitten Sie weitere Hilfe.
Das Gerät lässt sich nicht in den Administrator-Modus schalten.	Es besteht eine SICCT-Session zwischen Terminal und Konnektor. Solange diese Session besteht ist der Zugang zum Admin-Menü gesperrt.	Beenden Sie die bestehende Verbindung. Siehe hierzu Kapitel 4.1 „Admin-Menü“.
	Sie haben die Admin PIN mehrfach falsch eingegeben. Der Zugang zum Administrator-Menü ist für eine bestimmte Zeit gesperrt.	Die Sperrzeit wird im Display angezeigt. Danach ist der Administrator-Modus wieder freigeschaltet. Stellen Sie sicher, dass Sie die richtige PIN verwenden. Lesen Sie hierzu auch Kapitel 4.1 „Admin-Menü“ und dort insbesondere Tabelle 2.
	Die F1 -Taste ist defekt.	Kontaktieren Sie einen zertifizierten Techniker oder den Hersteller. Geben Sie die Fehlerbeschreibung an, und erbitten Sie weitere Hilfe.
Es erscheint eine der folgenden Statusanzeigen:  	Die Firmware, die Sie zu installieren versuchen, ist beschädigt.	Laden Sie die entsprechende Firmware-Datei erneut von der Herstellerseite.

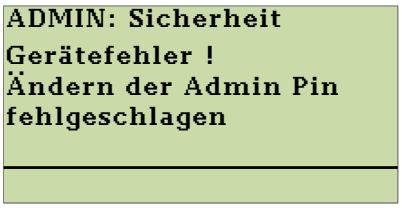
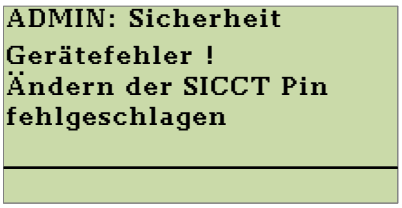
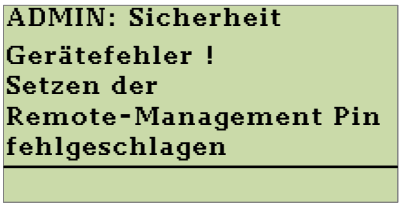
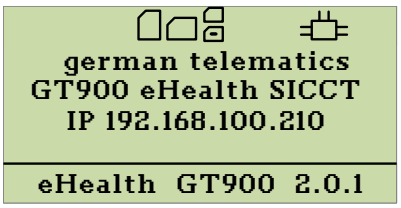
Achtung Keine Firmwaregruppe in Updatedatei!		

Fehlerbeschreibung	Ursache	Behebung
Das Firmware-Update wird abgebrochen. Es erscheint folgende Statusanzeige: 	Sie versuchen eine Firmware zu installieren, die in der aktuellen Firmwaregruppe nicht gelistet ist.	Die Installation der von Ihnen beabsichtigten Firmware ist nicht möglich. Sollten Sie Probleme mit einer neueren Firmware-Version haben und wollen daher auf die ältere Firmware-Version wechseln, so kontaktieren Sie bitte Ihren Lieferanten oder einen zertifizierten Techniker für weitere Unterstützung.
Nach Eingabe des Freischaltcodes für ein Update erscheint folgende Meldung: 	Sie haben dreimal einen falschen Freischaltcode eingeben.	Geben Sie den korrekten Freischaltcode ein, den Sie von german telematics erhalten haben. Überprüfen Sie, ob die Sie die Daten zur Erlangung des Freischaltcodes richtig weitergegeben haben und beantragen Sie einen neuen Freischaltcode.
Während eines Firmwareupdates oder beim Neustart des Terminals erscheint folgende Statusanzeige: 	Der Firmwareupdateprozess wurde mit einem Fehler beendet.	Kontaktieren Sie einen zertifizierten Techniker oder den Hersteller. Geben Sie die Fehlerbeschreibung an und erbitten Sie weitere Hilfe.
Beim Neustart des Terminals erscheint folgende Statusanzeige: 	Während eines Firmware-updates wurde die Strom-versorgung des Terminals unterbrochen. Beim Neustart des Terminals wird das unvollständig durchgeführte Update erkannt und erneut vom USB-Stick geladen.	Stecken Sie den USB-Stick mit der ursprünglichen Updatedatei, welche beim unterbrochenen Firmwareupdate genutzt wurde, in den USB Typ A Anschluss des Terminals.

Fehlerbeschreibung	Ursache	Behebung
Am Beginn des Updates oder beim Neustart des Terminals erscheint eine der folgenden Statusanzeigen: 	Es ist kein USB-Stick gesteckt, auf dem USB-Stick befindet sich keine Firmwareupdate-datei oder der USB-Stick wurde während des Kopiervorgangs der Firmwareupdatedatei aus dem Terminal gezogen. Während eines Firmware-updates wurde die Strom-versorgung des Terminals unterbrochen. Beim Neustart des Terminals wird das unvollständig durchgeführte Update erkannt und erneut vom USB-Stick geladen. Es ist kein USB-Stick gesteckt, auf dem USB-Stick befindet sich keine Firmwareupdatedatei oder der USB-Stick wurde während des Kopiervorgangs der Firmwareupdatedatei aus dem Terminal gezogen.	Stecken Sie den USB-Stick mit der ursprünglichen Updatedatei, welche beim unterbrochenen Firmwareupdate genutzt wurde, in den USB Typ A Anschluss des Terminals.
Beim Neustart des Terminals erscheint folgende Statusanzeige:  [Version] stellt in der tatsächlichen Anzeige die Versionsnummer des nicht vollständig installierten Updates dar.	Während eines Firmware-updates wurde die Strom-versorgung des Terminals unterbrochen. Beim Neustart des Terminals wird das unvollständig durchgeführte Update erkannt und erneut vom USB-Stick geladen. Auf dem USB-Stick befindet sich nicht die ursprüngliche Updatedatei.	Stecken Sie den USB-Stick mit der ursprünglichen Updatedatei, welche beim unterbrochenen Firmwareupdate genutzt wurde, in den USB Typ A Anschluss des Terminals.

Fehlerbeschreibung	Ursache	Behebung
Es erscheint folgende Statusanzeige: 	Bei der Inbetriebnahme des Gerätes wurde vor dem Einschalten keine gSMC-KT SIM Karte in einen der SIM-Slots des Gerätes eingelegt. Beachten Sie, dass ohne gSMC-KT kein Pairing mit einem Konnektor hergestellt werden kann und der Zugriff über die Weboberfläche nicht möglich ist.	Schalten Sie das Gerät aus und legen Sie eine gSMC-KT in einen der SIM-Slots des Kartenterminals ein. Lesen Sie hierzu auch Kapitel 2.2.3 „SIM-Slots“. Wahlweise können Sie auch in das Admin-Menü wechseln, um z.B. Netzwerkeinstellungen vorzunehmen.
Es erscheint folgende Statusanzeige: 	Die ursprünglich im Gerät eingelegte gSMC-KT wurde entfernt oder eine gSMC-KT wurde durch eine neue gSMC-KT ersetzt und es sind für die entfernte gSMC-KT noch Pairinginformationen im Gerät gespeichert.	Legen Sie die entfernte gSMC-KT wieder ins Terminal ein, wenn Sie die gespeicherten Pairinginformationen weiter nutzen wollen. Wenn Sie eine neue gSMC-KT verwenden, rufen Sie das Admin-Menü durch Drücken der F1 -Taste auf und geben Sie Ihre Admin PIN ein. Hier können Sie das entsprechende Pairing löschen. Lesen Sie hierzu auch Kapitel 4.3.1 „Pairing“. Durch Drücken der ✕ -Taste schalten Sie das Gerät aus.

Fehlerbeschreibung	Ursache	Behebung
Es erscheint folgende Statusanzeige: **Erstinbetriebnahme** **Gerätefehler!** **Setzen der** **initialen Pins** **fehlgeschlagen** **Erstinbetriebnahme** **Gerätefehler!** **Setzen der** **Geräte PUK** **fehlgeschlagen**	Während der Erstinbetriebnahme des Terminals konnten die initialen PINs (Admin PIN, SICCT PIN oder Remote-Management PIN) oder der PUK nicht erfolgreich gesetzt werden.	Kontaktieren Sie einen zertifizierten Techniker oder den Hersteller. Geben Sie die Fehlerbeschreibung an und erbitten Sie weitere Hilfe.

Fehlerbeschreibung	Ursache	Behebung
Es erscheint eine der folgenden Statusanzeigen:   	Im Admin-Menü des Terminals konnte die Admin PIN, die SICCT PIN oder die Remote-Management PIN nicht erfolgreich geändert bzw. gesetzt werden.	Kontaktieren Sie einen zertifizierten Techniker oder den Hersteller. Geben Sie die Fehlerbeschreibung an und erbitten Sie weitere Hilfe.
Obwohl eine Chipkarte gesteckt ist, wird das zugehörige Kartensymbol im Display nicht ausgefüllt. 	Mögliche Ursachen sind: • Die Karte steckt falsch herum • Die Karte ist defekt • Die Kontaktiereinheit ist verschmutzt oder defekt	Prüfen Sie, ob die Chipkarte wie in Kapitel 2.2 „Kartenslots“ beschrieben korrekt gesteckt ist. Wenn ja, überprüfen Sie, ob die Chipkarte in einem anderen Kartenslot oder in anderem, funktionsfähigen, Kartenterminal gelesen werden kann. Wenn dies nicht der Fall ist, ist die Karte defekt. Wenn die Karte in einem anderen Slot oder Kartenterminal gelesen werden kann, ist die Kontaktiereinheit Ihres Terminals defekt oder verschmutzt. Nehmen Sie in diesem Fall Kontakt mit Ihrem Lieferanten auf.

9 Kontakt

GT German Telematics Gesellschaft für Telematikdienste mbH

Libellenstraße 9

14129 Berlin

Fax.: +49 (0)30 – 31805454

E-Mail: service@germantelematics.de

Internetpräsenz: https://www.germantelematics.de

10 Außerbetriebnahme, Rückversand und Entsorgung

Bei Außerbetriebnahme oder Rückversand des Gerätes (z.B. im Fall eines Austauschs) stellen Sie sicher, dass sich keine Chipkarten mehr in den Kartenslots befinden und das alle Pairings gelöscht sind. Die Pairings können Sie im Administrator Menü (s. Kapitel 4.3.5) oder mittels eines Werksresets (s. Kapitel 5) löschen. Löschen Sie auch die Pairinginformationen des betroffenen Kartenterminals im Konnektor.

Beachten Sie beim Rückversand die Hinweise des Herstellers unter https://www.germantelematics.de/service .

Elektrogeräte, die mit diesem Symbol gekennzeichnet sind, dürfen in Europa nach dem 12. August 2005 nicht mehr über die öffentliche Abfallentsorgung entsorgt werden. In Übereinstimmung mit lokalen und nationalen europäischen Bestimmungen (EU-Richtlinie 2002/96/EC), müssen Benutzer von Elektrogeräten in Europa ab diesem Zeitpunkt alte bzw. zu verschrottende Geräte zur Entsorgung kostenfrei an den Hersteller zurückgeben.

Hinweis: Bitte wenden Sie sich an den Hersteller bzw. an den Händler, von dem Sie das Gerät bezogen haben, um Informationen für die Rückgabe des Altgerätes zur ordnungsgemäßen Entsorgung zu erhalten.

Wichtige Informationen - Bitte zusammen mit den Produktinformationen aufbewahren.

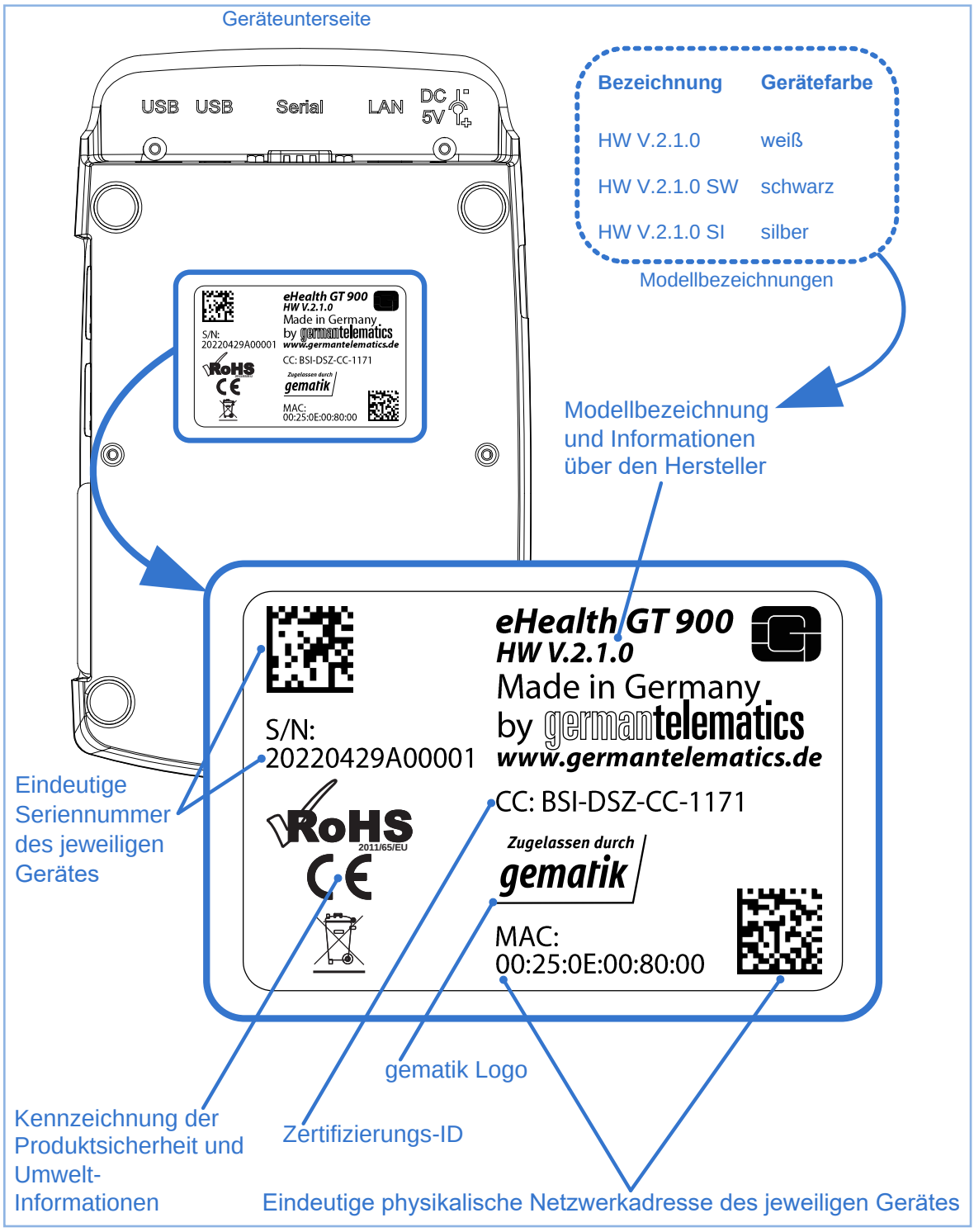


Abbildung 81: Geräteunterseite