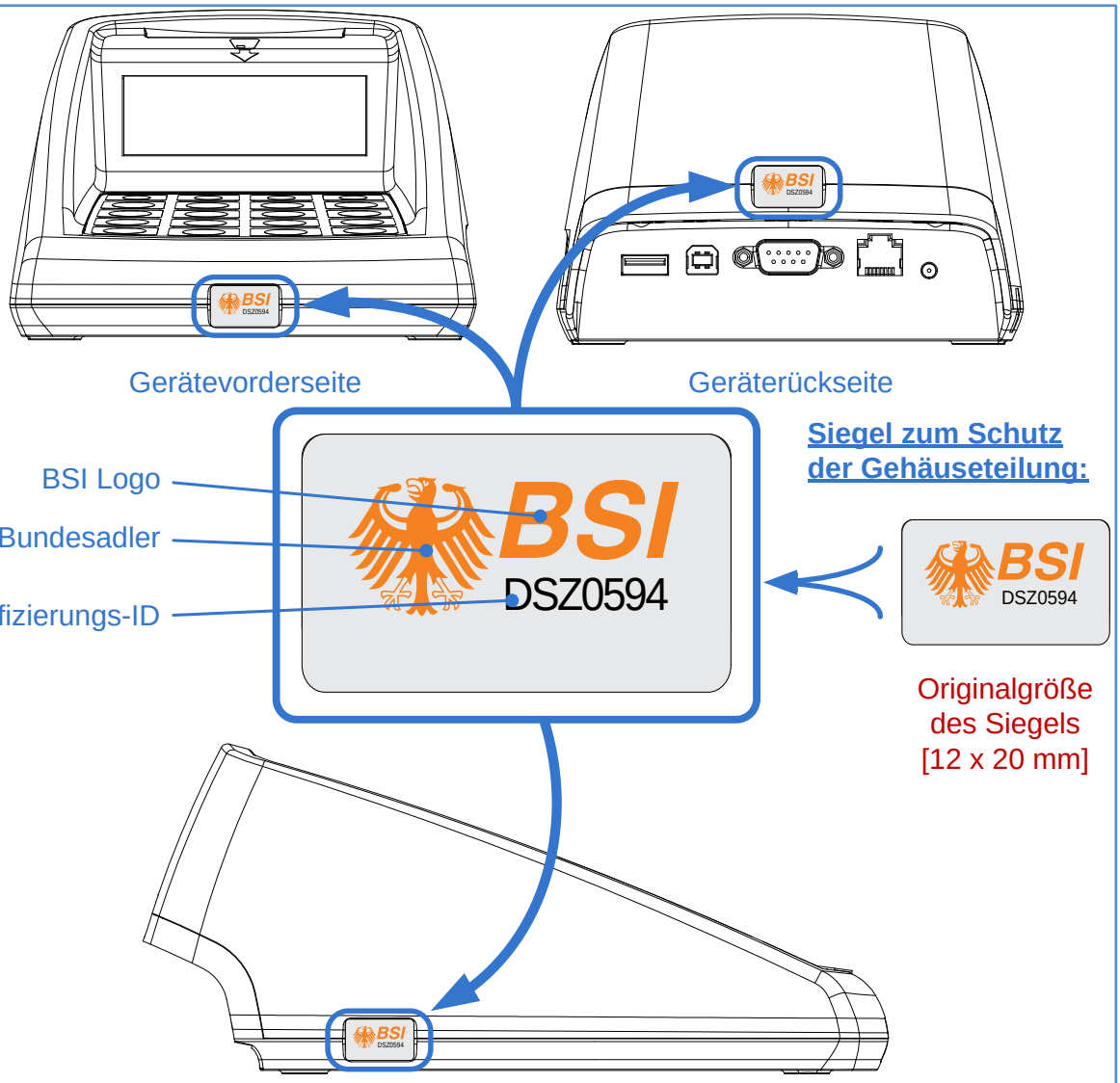
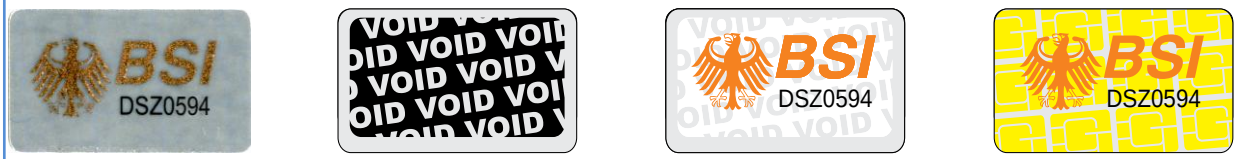
GT German Telematics GmbH

Chipkartenterminal eHealth GT900 –Benutzerhandbuch–

Version 2.0.3 / Deutsch



Beschreibung der Sicherheitsmerkmale:



Original intaktes Siegel | Öffnungseffekt (Untergrund) | Öffnungseffekt (Folie) | Bestrahlung mit UV-Licht

Bitte führen Sie vor jeder Nutzung des Chipkartenterminals eine Sichtprüfung des Gehäuses und der Siegel 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 Abschnitt 1.3 „Sicherheitskonzept des Terminals“.

Das vorliegende Benutzerhandbuch gilt für alle Chipkartenterminals eHealth GT900 mit Firmware-Version 1.20.9. Die Firmware-Versions-angaben in den Abbildungen sind teilweise beispielhaft. Angaben zur Firmware-Version finden Sie über die Menüsteuerung des Terminals (siehe vorliegendes Handbuch Kapitel 4.12.1) 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 Chipkartenterminal 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 der bereits im Umlauf befindlichen Krankenversicherten Karte (KVK) als auch mit der chipkartenbasierten elektronischen Gesundheitskarte (eGK) 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:

Chipkartenterminal
eHealth GT900
Benutzerhandbuch

Handbuchversion:

2.0.3

Ausgabedatum:

08.Dezember 2015

Hersteller:

gt german telematics gesellschaft
für telematikdienste
Rankestraße 26
10789 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 Abschnitte dieses Handbuchs vorgenommen. Die folgenden Symbole geben den jeweiligen Nutzer wieder, für den ein betreffender Abschnitt relevant ist.

Administrator

Alle Abschnitte dieses Handbuchs sind für Geräteadministratoren relevant.

Benutzer

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

- 1 „Sicherheitshinweise und allgemeine Informationen" (S. 8)
- 1.3 „Sicherheitskonzept des Terminals" (S. 13)
- 1.7 „Ein- und Ausschalten des Chipkartenterminals" (S. 30)
- 1.8 „Reinigen und Desinfizieren des Gerätes" (S. 31)
- Das gesamte Kapitel 2 „Bedienelemente" (S. 32)
- 3.2 „Eingabe einer Karten-PIN" (S. 46)
- Das gesamte Kapitel 7 „Qualifizierte elektronische Signaturen" (S. 104)
- Das gesamte Kapitel 9 „Problembehebung" (S. 107)

PUK-Administrator

Die folgenden Abschnitte sind für einen PUK-Administrator relevant:

- 1 „Sicherheitshinweise und allgemeine Informationen" (S. 8)
- 1.6.2 „Setzen einer PUK" (S. 26)
- Das Kapitel 5 „Gerät zurücksetzen" und hier insbesondere 5.1 „Zurücksetzen ohne Kenntnis der Admin PIN" (S. 89)

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 Chipkartenterminals 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 „Akzeptanzprozedur“ sorgfältig durch.
- Überprüfen Sie regelmäßig vor der Nutzung und nach Abwesenheit die Unversehrtheit des Geräts (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 in den meisten Fällen für einen Zeitraum von 30 Minuten verhindert.
- 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 Chipkartenterminal nur das mitgelieferte Netzteil und die beiliegenden Anschlusskabel.
- Halten Sie die Firmware des Kartenterminals sowie die zugehörigen Treiber und Administrationsprogramme stets aktuell. Prüfen Sie dazu regelmäßig unsere Homepage unter www.germantelematics.de. Die zu den Firmwaren zugehörigen Bestätigungen zur QES sowie die Sicherheitszertifizierung nach Common Criteria finden Sie unter www.bundesnetzagentur.de sowie unter www.bsi.bund.de.
- Um qualifizierte Signaturen zu erstellen, müssen Sie das Gerät mit einer bestätigten Signaturkarte sowie einer bestätigten Signaturanwendungs-komponente betreiben (Liste der bestätigten Komponenten siehe www.bundesnetzagentur.de)
- 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 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.
- Eine Notentnahme einer eGK/HBA/SMC-B/gSMC-KT erfolgt wie das normale Entnehmen der betreffenden Karte aus Ihrem Kartenhalter.
- 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.
- Achten Sie beim Wiederversand des Gerätes darauf, dass dieses vor Manipulationen Dritter geschützt ist, indem Sie geeignete Maßnahmen treffen.
- 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 Geräts sowie für die Firmware über die Menüsteuerung des Geräts (s. Kapitel 4.3).
- Neben der Hardware ist die Firmware ein sicherheitssensibles Element. Verwenden Sie aus diesem Grund nur zertifizierte und bestätigte 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 Terminals, wenn dieses endgültig nicht mehr benutzt werden soll. Lesen Sie hierzu auch die Hinweise in Kapitel 12 „Geräteentsorgung“.

1.1 Akzeptanzprozedur

Um die Integrität des Terminals beim Erreichen des endgültigen Aufstellungsortes, bspw. einer Arztpraxis, zu gewährleisten, führen Sie bitte vor der Inbetriebnahme die folgenden Maßnahmen durch:

1. Prüfen Sie den Karton und das Kartonsiegel auf Manipulationshinweise (Löcher, Einschnitte bzw. ungewöhnliche Klebereste).
2. Prüfen Sie den Lieferumfang gemäß Absatz 1.2 „Lieferumfang“.
3. Vergleichen Sie die Angaben auf dem Gerätelabel auf der Geräteunterseite mit dem Gerätelabel auf dem Verpackungskarton. Bewahren Sie das Gerätelabel des Verpackungskartons an einem sicheren Ort auf, um das Terminal zu einem späteren Zeitpunkt einer erneuten Identitätsprüfung zu unterziehen.
4. Prüfen Sie die Unversehrtheit des Gehäuses gemäß 1.3.1 „Gehäuseprüfung“ und der Geräteversiegelung gemäß Abschnitt 1.3.2 „Siegelprüfung“.

Sollten Sie begründete Zweifel an der Unversehrtheit und Echtheit des Gerätes haben, kontaktieren Sie den Support von german telematics per E-Mail an info@germantelematics.de oder telefonisch werktags zwischen 9:30 Uhr und 17 Uhr unter der Telefonnummer 030/31805455. Das Terminal darf in diesem Fall bis zur Freigabe durch den Hersteller nicht in Betrieb genommen werden!

Vergewissern Sie sich zudem nach der Inbetriebnahme des Gerätes, dass auf diesem die Firmware `1.20.9` installiert ist. Lesen Sie hierzu den Abschnitt 4.12.1 „Anzeige der aktuellen Firmware-Version“.

1.2 Lieferumfang

Im Lieferumfang Ihres Gerätes sind enthalten:

- ein eHealth GT900 Chipkartenterminal
- ein GS (Geprüfte Sicherheit) zertifiziertes Netzteil (5V / 1200 mA)
- ein Ethernet-Kabel (2m)
- eine Bedienungsanleitung (ggf. in elektronischer Form auf einem Datenträger)
- 4 SIM-Slot Siegel zur Versiegelung der SMC SIM-Slots. Bitte verwahren Sie diese Siegel bis zu Ihrer Verwendung an einem sicheren Ort auf!
- 1 gSMC-KT (gerätespezifische Security Module Card Kartenterminal)

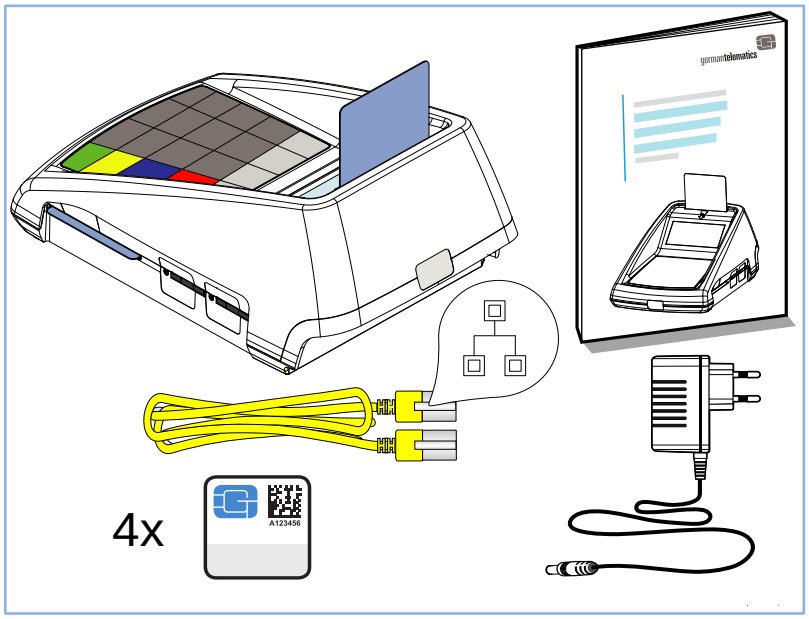


Abbildung 1: Lieferumfang

Terminals, die von Leistungserbringern im Rahmen des Erprobungsbetriebs ORS1 in den Testregionen betrieben werden, erhalten ihre gSMC-KT von Ihrem Vertragspartner im Erprobungsbetrieb. Das ist entweder die CompuGroup Medical Deutschland AG oder die T-Systems International GmbH.

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 30 Minuten) oder bei jedem neuen Pairing-Prozess, das Gehäuse und alle Siegel auf Unversehrtheit und Echtheit.

Sollten Sie begründete Zweifel an der Unversehrtheit und Echtheit des Gerätes haben, kontaktieren Sie den Support von german telematics per E-Mail an info@germantelematics.de oder telefonisch werktags zwischen 9:30 Uhr und 17 Uhr unter der Telefonnummer 030/31805455. Das Terminal darf in diesem Fall bis zur Freigabe durch den Hersteller nicht in Betrieb genommen werden!

Das Terminal verhindert im Betrieb den Diebstahl geschützter Daten durch einen elektronischen Sicherheitsmechanismus. Beachten Sie dazu das Kapitel 1.3.3 „Start PIN“

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!

Vergleichen Sie das Gerätelabel auf der Geräteunterseite mit dem aufbewahrten Gerätelabel des Verpackungskartons. Kontrollieren Sie, dass der Aufkleber unversehrt ist und glattflächig auf der Klebefläche aufliegt.

1.3.2 Siegelprüfung

Um Ihr Chipkartenterminal 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:

- Auf jedem Siegel sind unsichtbare Merkmale angebracht, die nur sichtbar werden, wenn das Siegel durch ein Geldschein-Prüfgerät beleuchtet wird.
- Achten Sie auf irreversible Veränderungen an dem Siegel wie zum Beispiel:
  - Manipulationsbotschaft (siehe hierzu auch Umschlagsseite 2)
  - mechanische Beschädigung
- Für die sofortige Echtheitsprüfung der Siegel ohne Hilfsgeräte können Sie die haptisch erfassbare, d.h. erhabene Ausgestaltung des Bundesadlers und des BSI- Logos nutzen.
- Achten Sie auf Farbveränderungen am Bundesadler und am BSI-Logo, durch Kippen kommt es zu einem Farbwechsel von Rot über Ocker nach Grün.

Um die Siegel zum Schutz der Gehäuseteilung einer genaueren Prüfung zu unterziehen, können diese mit UV-Licht bestrahlt werden. Hierfür reicht im Allgemeinen eine UV-Lampe, wie sie zur Prüfung von Geldscheinen verwendet wird, aus. Die Siegel zeigen bei der Bestrahlung mit UV-Licht das stilisierte Chiplogo der German Telematics GmbH. Ist bereits eine gSMC-KT im Terminal gesteckt, prüfen Sie auch das durch den Administrator aufgebrachte SIM-Slot-Siegel an der Seite des Gerätes auf Unversehrtheit und die korrekte Siegelnummer.

Ziehen Sie die Abbildung auf der Umschlagseite 2 (Gehäusesiegel) und auf Seite 39 (SIM-Slot-Siegel) dieses Benutzerhandbuchs zu Rate, um die Lage, die Form und Größe sowie die Merkmale der Geräteversiegelung abzugleichen.

1.3.3 Start PIN

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

Trennen Sie das Terminal daher auch bei Nichtnutzung (beispielsweise über Nacht oder am Wochenende) nicht von der Stromversorgung! Schalten Sie das Terminal immer gemäß Kapitel 1.7 „Ein- und Ausschalten des Chipkartenterminals“ aus und wieder ein. Sollten Sie das Terminal dennoch von der Stromversorgung trennen wollen, müssen Sie es manipulationssicher verschließen!

Beim Wiedereinschalten nach einem stromlosen Zustand müssen Sie dann am Terminal die Start PIN eingeben um das Gerät wieder in Betrieb zu nehmen.

Die Start PIN verhindert den unberechtigten Zugriff auf das Gerät, sollte dies einmal von der Versorgungsspannung getrennt gewesen sein. **Sollte das Gerät Sie unerwartet auffordern, die Start PIN einzugeben, so ist ein Angriffsversuch anzunehmen!**

Wichtige Hinweise zum Umgang mit der Start PIN:

!

Halten Sie Ihre Start PIN geheim. Vermeiden Sie es, die Start PIN in der Nähe des Gerätes aufzubewahren, insbesondere sollten Sie sie nicht auf dem Gerätegehäuse notieren. Es muss organisatorisch sichergestellt werden, dass die Start PIN nicht in den Besitz Unberechtigter gelangt. Beachten Sie, dass die Start PIN nur eingegeben werden darf, wenn die Integrität des Gerätes sichergestellt ist und ein Angriffsversuch ausgeschlossen werden kann. Daher sind insbesondere nach einer unerwarteten Aufforderung die Start PIN einzugeben, die Siegel und das Gehäuse sorgfältig auf Veränderungen und Manipulationsspuren zu überprüfen (siehe Kapitel 1.3.1 „Gehäuseprüfung“ und 1.3.2 „Siegelprüfung“)! Ein möglicher Stromausfall muss plausibel und nachvollziehbar sein! Die Einsatzumgebung ist auf Zutritt Unberechtigter zu prüfen (Einbruchspuren)!

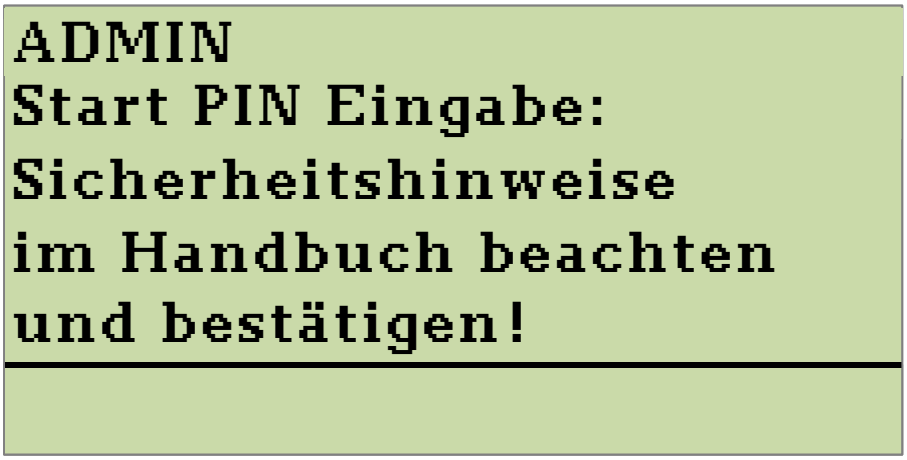
Im Zweifelsfall darf die Start PIN keinesfalls eingegeben werden und das Gerät ist zur Prüfung an den Hersteller zu senden.

ACHTUNG: Die Person (Administrator), die die Start PIN eingibt, trägt die Verantwortung für den sicheren Betrieb des Terminals.

HINWEIS: Die Start PIN muss nicht eingegeben werden, wenn das Terminal über die Tastatur ausgeschaltet wurde.

Wird die Eingabe der Start PIN notwendig, müssen Sie am Terminal bestätigen, dass Sie die Hinweise zum Umgang mit der Start PIN in diesem Handbuch beachtet haben

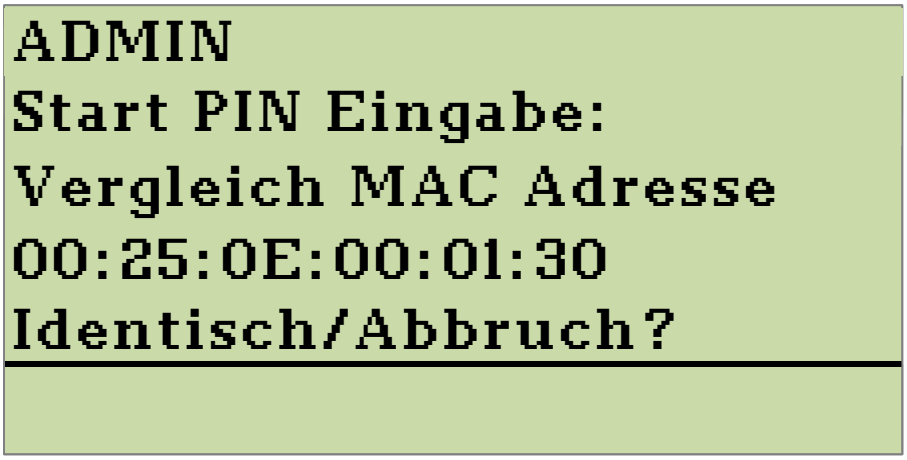
(s. Abbildung 2). Drücken Sie die ✅-Taste, um dies zu bestätigen. Bestätigen Sie diesen Dialog nicht, kann das Terminal nicht weiter genutzt werden.



Beachten Sie die Hinweise zum Umgang mit der Start PIN.

Abbildung 2: Bestätigung der Beachtung der Sicherheitshinweise

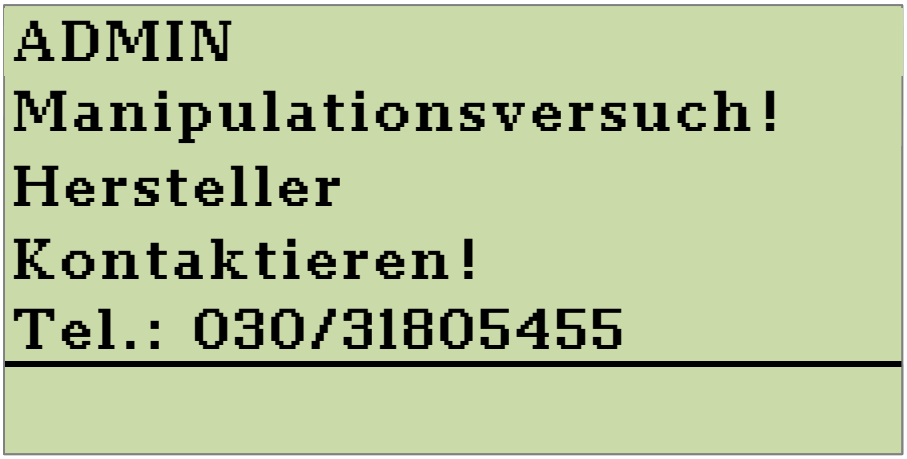
Nachdem Sie diesen Dialog bestätigt haben, werden Sie aufgefordert, die im Display des Gerätes angezeigte MAC Adresse (s. Abbildung 3) mit der auf dem Gerätelabel auf der Gehäuseunterseite aufgedruckten MAC Adresse zu vergleichen. Vergleichen Sie die MAC Adresse auch mit dem aufbewahrten Gerätelabel des Verpackungskartons.



Die MAC Adresse in dieser Abbildung ist beispielhaft. Ihr Terminal zeigt die gerätespezifische MAC Adresse an.

Abbildung 3: Vergleich der MAC Adresse

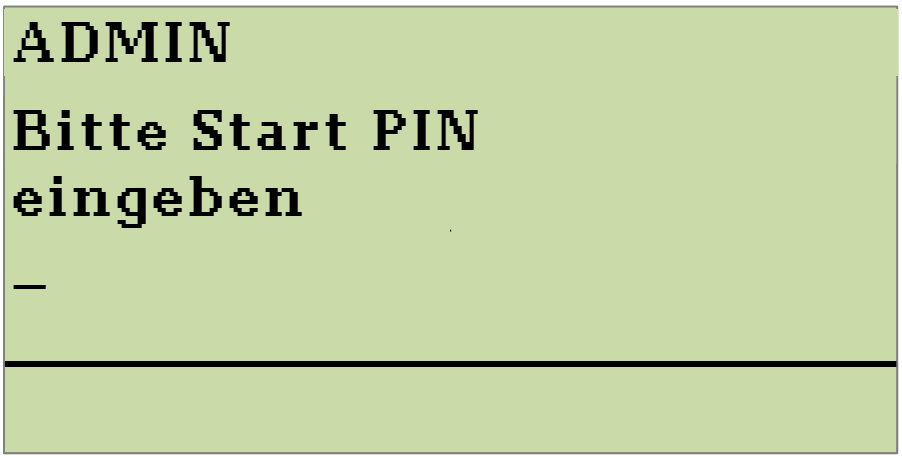
Drücken Sie die ✅-Taste um zu bestätigen. Stimmen die MAC Adressen nicht überein, brechen Sie den Vorgang mit der ❌-Taste ab. Das Terminal zeigt daraufhin die Displaymessage in Abbildung 4 und darf nicht in Betrieb genommen werden! Kontaktieren Sie den Hersteller.



Anzeige bei nicht erfolgter Bestätigung der Übereinstimmung der MAC Adressen.

Abbildung 4: Manipulationsversuch

Nachdem Sie die MAC Adresse erfolgreich validiert haben, können Sie Ihre Start PIN eingeben (s. Abbildung 5).



Aufforderung zur Eingabe der Start PIN.

Abbildung 5: Eingabe der Start PIN

Bestätigen Sie die Eingabe mit der ✅-Taste. Das Terminal ist nun betriebsbereit.

1.4 Aufstellungshinweise

Aus Gründen der Datensicherheit weisen wir darauf hin, dass das Chipkartenterminal nur in einem kontrollierten Bereich, wie zum Beispiel einer Arztpraxis oder vergleichbaren Räumlichkeiten, betrieben werden darf, sodass unbefugte Personen keine Manipulationen an dem Chipkartenterminal und daran angeschlossenen Systemeinheiten vornehmen können. Das Gerät muss darüber hinaus in einem Mindestabstand von 15cm 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 30 Minuten verhindert. Insbesondere bedeutet dies, dass sich das Gerät bei längerer Abwesenheit (auch nachts) in einem geschützten Bereich befindet, 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 Hersteller zu unterziehen.

Stellen Sie das Gerät auf eine glatte Oberfläche. Achten Sie auf ein ordnungsgemäßes Anschließen aller benötigten Kabel (siehe Abschnitt 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 Chipkartenterminal sollte zudem Patienten zugänglich gemacht werden, insofern diese Eingaben an dem Gerät tätigen müssen.

1.5 Anschluss des Gerätes

Das eHealth GT900 Chipkartenterminal kann ausschließlich über die Ethernet-LAN-Schnittstelle und in Verbindung mit einem Konnektor genutzt werden, ein direkter Anschluss an einen PC ist nicht vorgesehen. Um das Gerät über eine **Ethernet-LAN-Schnittstelle** zu betreiben, stecken Sie das mitgelieferte Ethernet-Kabel in den dafür vorgesehenen Anschluss an ihrem Chipkartenterminal. In Abbildung 6 ist dieser Anschluss mit Position ④ gekennzeichnet. Das andere Ende stecken Sie in einen freien Ethernet-Anschluss an Ihrem Switch oder einer entsprechenden Netzwerkdose. Bitte beachten Sie, dass sich sowohl der Konnektor als auch Ihr eHealth Chipkartenterminal im selben Netzwerk befinden müssen. Das Kartenlesegerät kann zudem nur mit einer eingelegten gSMC-KT in einem der Geräte-SIM-Slots über die Ethernet-LAN-Schnittstelle 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 Abschnitt 2.2.3 „SIM-Slots“.

Schließen Sie nun das mitgelieferte Netzteil an den dafür vorgesehenen Anschluss an Ihrem Chipkartenterminal an. Der Netzteil-Anschluss ist in Abbildung 6 mit der Position ⑤ gekennzeichnet. Stecken Sie abschließend das Netzteil in eine Steckdose (230V / 50 Hz)[1]. Ihr Gerät ist nun für die Erstinbetriebnahme bereit, beachten Sie daher die Hinweise in Abschnitt 1.6 „Inbetriebnahme des Chipkartenterminals“. Die Anschlüsse mit der Position ② (USB Typ B) und ③ (RS232) sind in dieser Firmware funktionslos.

[1] Das Gerät schaltet sich ein, sobald es mit Spannung versorgt wird.

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 Chipkarten-lesegerätes über die Ethernetschnittstelle 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 Abschnitt 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 LAN-Netzwerk, in dem das Chipkartenterminal 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.

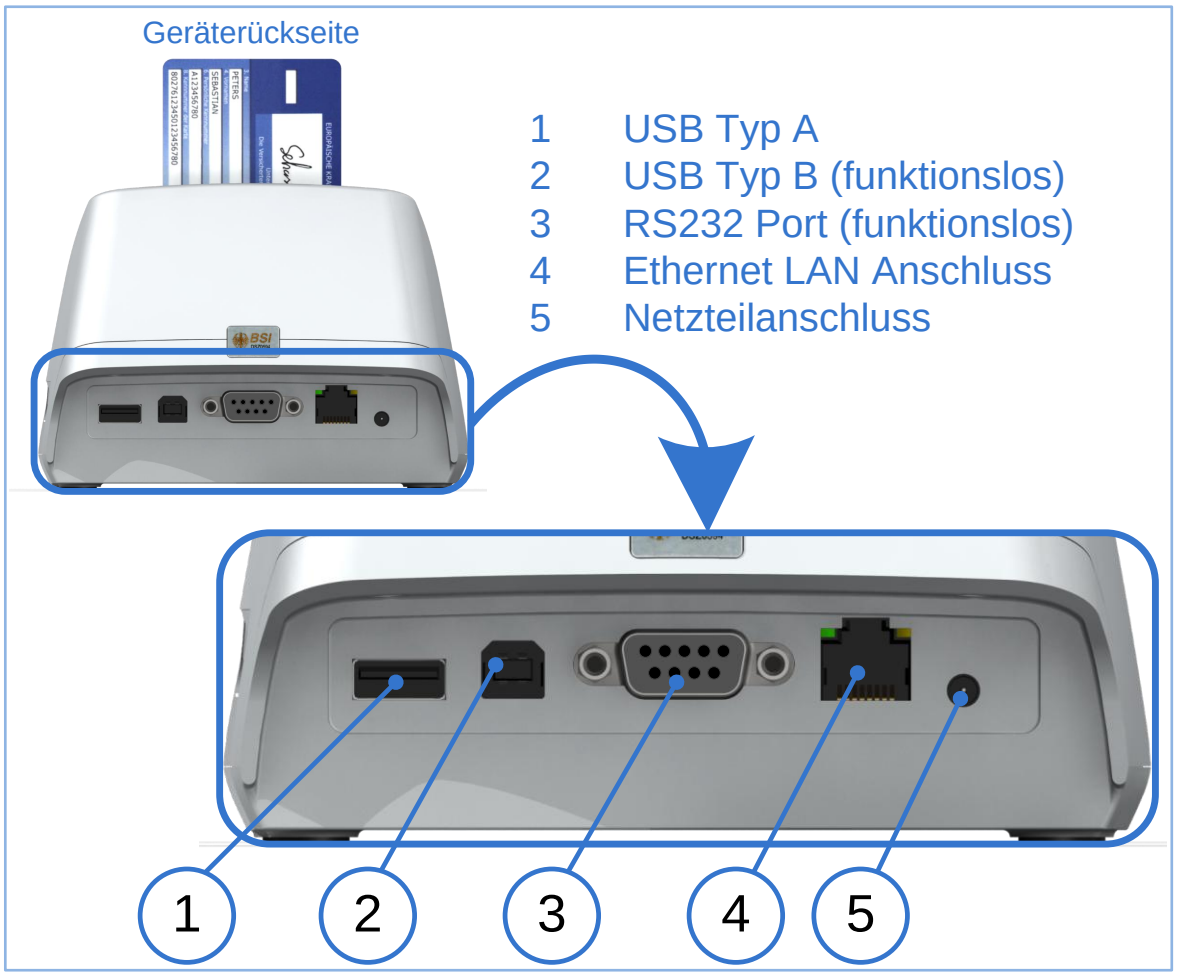


Abbildung 6: Belegung der Anschlüsse

1.6 Inbetriebnahme des Chipkartenterminals

Die Inbetriebnahme des Chipkartenterminals ist durch einen Administrator vorzunehmen. Es ist zudem sicherzustellen, dass das LAN-Netzwerk in dem das Chipkartenterminal in Betrieb genommen wird, vor unbefugtem Zugriff abgesichert ist. **Das Gerät sollte sich durch den Anschluss der Stromversorgung selbst eingeschaltet haben** (siehe Abschnitt 1.5 „Anschluss des Gerätes“). Bei der Erstinbetriebnahme des Gerätes werden Sie nach einem kurzen Systemtest gebeten, eine Admin PIN[2] zu vergeben. Nach dem Vergeben der Admin PIN müssen Sie zudem eine PUK vergeben, mit der das Gerät beim Verlust der Admin PIN wieder in den Werkszustand zurückgesetzt werden kann. Danach erzeugt das Terminal eine Start PIN zur Sicherung des Pairinggeheimnisses. Abschließend muss eine SICCT PIN vergeben werden, damit der Konnektor administrativ auf das Terminal zugreifen kann. Um das Gerät in den Auslieferungszustand zurückzusetzen, lesen Sie bitte Abschnitt 5 „Gerät zurücksetzen“.

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

1.6.1 Setzen der Admin PIN

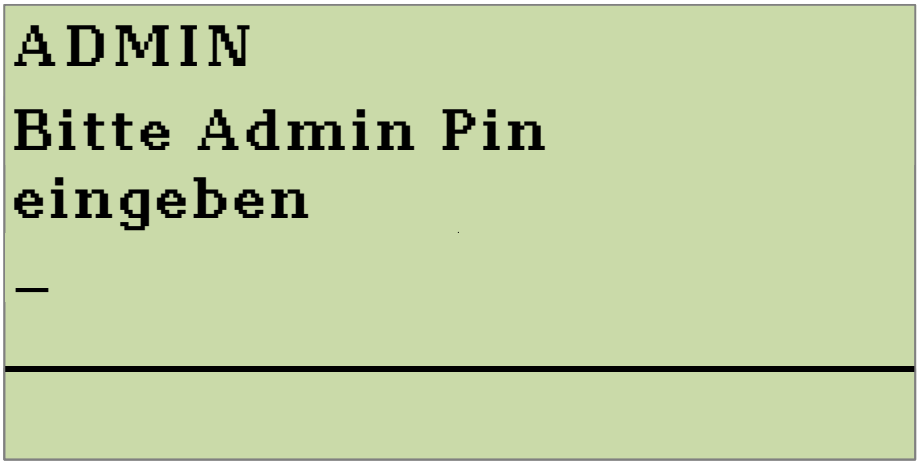


Abbildung 7: PIN-Eingabe bei der Erstinbetriebnahme

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

Die PIN muss aus **mindestens 8 numerischen Zeichen** bestehen. Die Zeichen * und # können nicht verwendet werden. Bewahren Sie die PIN an einem sicheren Ort auf. Vermeiden Sie es, die Administrator 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**[3]. Lesen Sie hierzu bitte auch die Hinweise zum Umgang mit der Administrator PIN am Ende des Abschnittes 4.1 „Admin-Menü“. Sie werden anschließend zu einer Wiederholung der PIN aufgefordert.

[3] Trivial-PINs werden vom Gerät nicht angenommen und durch die Anzeige einer entsprechenden Fehlermeldung abgewiesen.

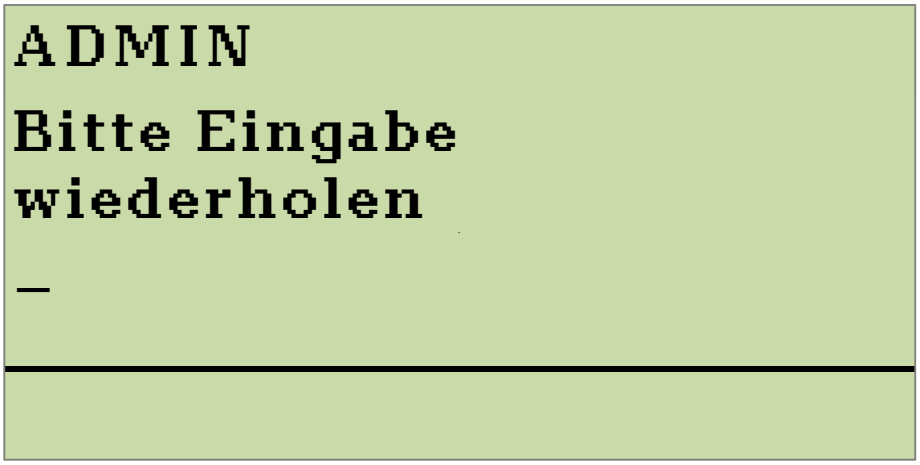


Abbildung 8: Bestätigung der PIN-Eingabe

Haben Sie die Administrator PIN erfolgreich vergeben und Ihre Eingabe aus Sicherheitsgründen wiederholt bzw. bestätigt (siehe Abbildung 8), können Sie nach einer kurzen Bestätigungsanzeige, wie sie in Abbildung 9 dargestellt ist, mit der Vergabe einer PUK fortfahren. Sollten die von Ihnen eingegebenen PINs nicht identisch sein, werden Sie zur erneuten Eingabe aufgefordert.

Abbildung 9: Erfolgreiche Vergabe der Admin PIN

1.6.2 Setzen einer PUK

Mit Hilfe der PUK können Sie das Chipkartenlesegerät in den Auslieferungszustand zurücksetzen, sollte dies notwendig werden.

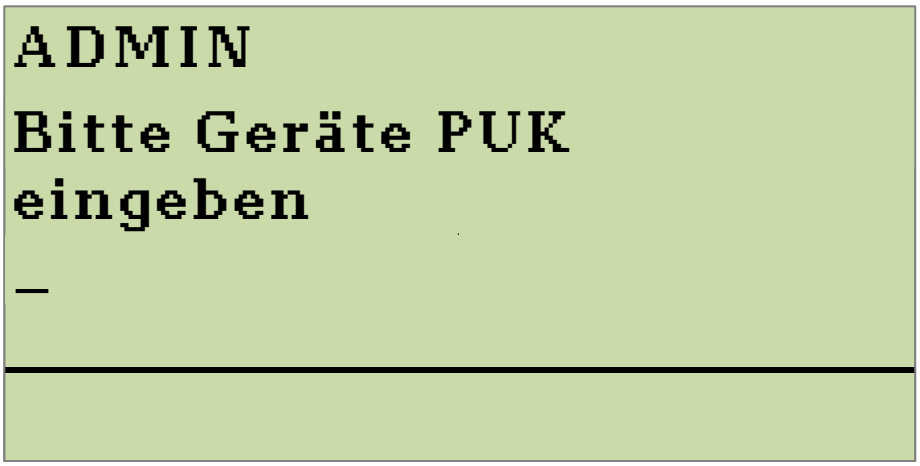


Abbildung 10: PUK-Eingabe bei der Erstinbetriebnahme

Die PUK muss aus **mindestens 8 numerischen Zeichen** bestehen. Die Zeichen * und # können nicht verwendet werden. Bewahren Sie die PUK an einem sicheren Ort auf. Vermeiden Sie es, die PUK in der Nähe des Gerätes aufzubewahren, insbesondere sollten Sie sie **nicht** auf dem Gerätegehäuse notieren und sie nicht in der Nähe der Admin PIN aufbewahren. **Verwenden Sie zudem keine Trivial-PUK wie beispielsweise 11111111 oder 12345678**[4]. Lesen Sie hierzu bitte auch die Hinweise zum Umgang mit der Administrator PIN und der PUK am Ende des Abschnittes 4.1 „Admin-Menü“. Sie werden anschließend zu einer Wiederholung der soeben vergebenen PUK aufgefordert. Sollten die von Ihnen eingegebenen PUKs nicht identisch sein, werden Sie zur erneuten Eingabe aufgefordert.

[4] Triviale PUKs werden vom Gerät nicht angenommen und durch die Anzeige einer entsprechenden Fehlermeldung abgewiesen.

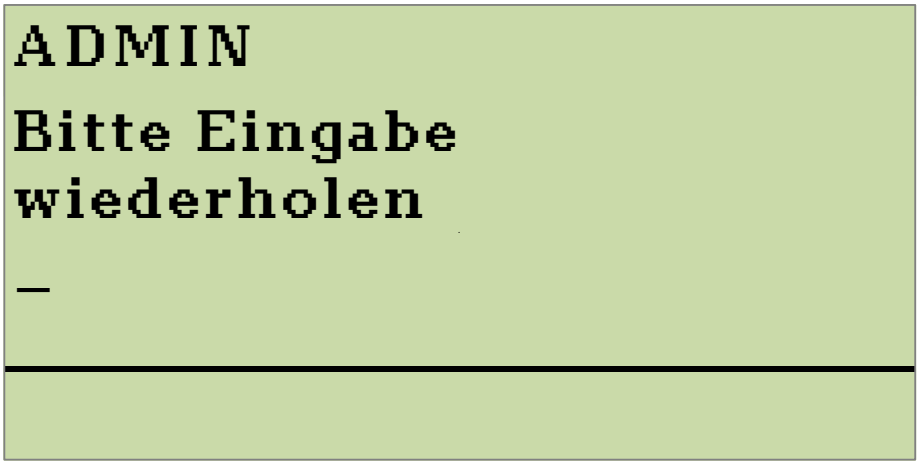


Abbildung 11: Bestätigung der PUK-Eingabe

Haben Sie die PUK erfolgreich vergeben und Ihre Eingabe wiederholt bzw. bestätigt (siehe Abbildung 11), wird nach einer kurzen Bestätigungsanzeige, wie sie in Abbildung 12 dargestellt ist, die Start PIN generiert .

Abbildung 12: Erfolgreiche Vergabe der PUK

1.6.3 Erzeugung einer Start PIN

Nachdem Sie eine Admin PIN und eine Geräte PUK vergeben haben, erzeugt das Gerät eine Start PIN. Die Start PIN verhindert einen unberechtigten Zugriff auf das Gerät, sollte dies einmal von der Spannungsversorgung getrennt gewesen sein.

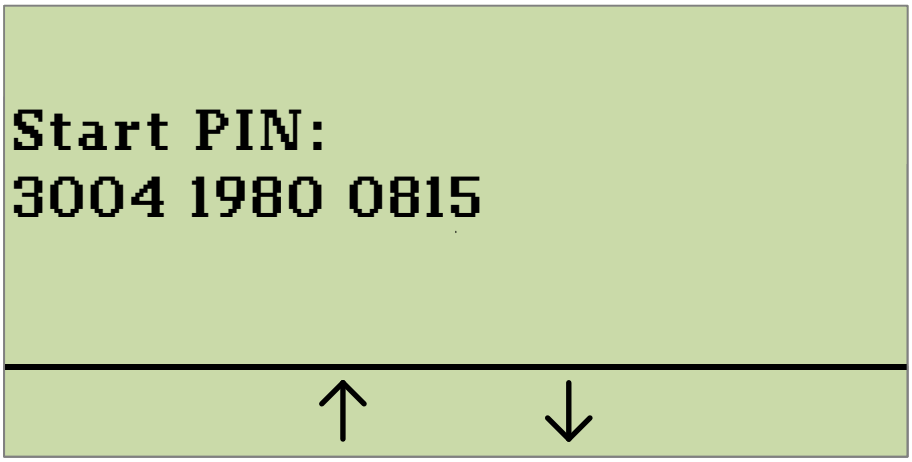


Abbildung 13: Anzeige bei Erzeugung einer neuen Start PIN

Notieren Sie diese Start PIN und bewahren Sie sie an einem sicheren Ort auf! Lesen Sie bitte auch die Hinweisbox „Wichtige Hinweise zum Umgang mit der Start PIN“ in Abschnitt 4.11. Bei einer Inbetriebnahme nach einem stromlosen Zustand muss sich der Nutzer durch die Eingabe der Start PIN als berechtigter Nutzer identifizieren.

1.6.4 Setzen der SICCT PIN

Nach dem Generieren der Start PIN werden Sie gebeten, eine SICCT PIN zu vergeben. Mit Hilfe der SICCT PIN wird der administrative Zugriff auf die SICCT-Schnittstelle des Gerätes beim Betrieb mit dem Konnektor sichergestellt. Lesen Sie hierzu auch Abschnitt 3.1.

Abbildung 14: SICCT PIN Eingabe bei Erstinbetriebnahme

Die SICCT PIN muss aus **8 bis 12 numerischen Zeichen** bestehen. Die Zeichen * und # können nicht verwendet werden. Bewahren Sie die SICCT PIN an einem sicheren Ort auf. Vermeiden Sie es, die SICCT PIN in der Nähe des Gerätes aufzubewahren, insbesondere sollten Sie sie **nicht** auf dem Gerätegehäuse notieren und sie nicht in der Nähe der Admin PIN aufbewahren. **Verwenden Sie zudem keine Trivial-PIN wie beispielsweise 11111111 oder 12345678**[5]. Lesen Sie hierzu bitte auch die Hinweise zum Umgang mit der Administrator PIN und der PUK am Ende des Abschnittes 4.1 „Admin-Menü“. Sie werden anschließend zu einer Wiederholung der soeben vergebenen SICCT PIN aufgefordert.

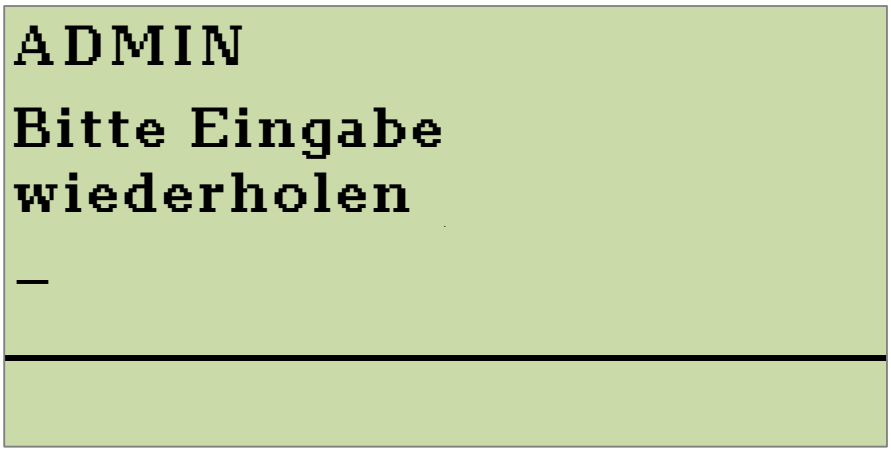


Abbildung 15: Bestätigung der SICCT PIN Eingabe

[5] Triviale SICCT PINs werden vom Gerät nicht angenommen und durch die Anzeige einer entsprechenden Fehlermeldung abgewiesen.

Abbildung 16: Erfolgreiche Vergabe der SICCT PIN Eingabe

Nachdem Sie die SICCT PIN erfolgreich vergeben haben, ist das Einrichten des eHealth GT900 abgeschlossen und das Gerät ist betriebsbereit.

1.7 Ein- und Ausschalten des Chipkartenterminals

Schalten Sie das Gerät durch Drücken der ✓-Taste ein[6]. Nach einem kurzen Systemtest ist das Gerät einsatzbereit. Sollte das Gerät von der Stromversorgung getrennt gewesen sein, werden Sie gebeten, die Start PIN einzugeben. Vergewissern Sie sich vor dem Ausschalten des Gerätes, dass die Kartenslots für KVK/eGK und HBA 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.

[6] Beachten Sie, dass sich das Gerät zunächst selbstständig einschaltet, sobald es mit Spannung versorgt wird. Bleibt die Stromversorgung erhalten und das Gerät wird ausgeschaltet, kann es wie beschrieben wieder eingeschaltet werden.

1.8 Reinigen und Desinfizieren des Gerätes

Bevor Sie das Chipkartenterminal feucht reinigen, trennen Sie das Gerät immer zuerst vom Stromnetz. Lassen Sie nach einer erfolgten Reinigung das Gerät trocknen. Für die Reinigung des Chipkartenterminals 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 ist. Sollten Sie sich nicht sicher sein, ob es eventuell zu einer Beschädigung eines Siegels gekommen ist, so lesen Sie bitte Abschnitt 1.3.2 „Siegelprüfung“.

2 Bedienelemente

2.1 Tastatur

Das eHealth GT900 Chipkartenterminal verfügt über eine integrierte Folientastatur, die Ihnen eine sichere PIN-Eingabe garantiert. Die folgende Abbildung 17 (Gerätetastatur) und Tabelle 1 (Tastaturbelegung) sollen Sie mit den Funktionen der Tastatur vertraut machen.

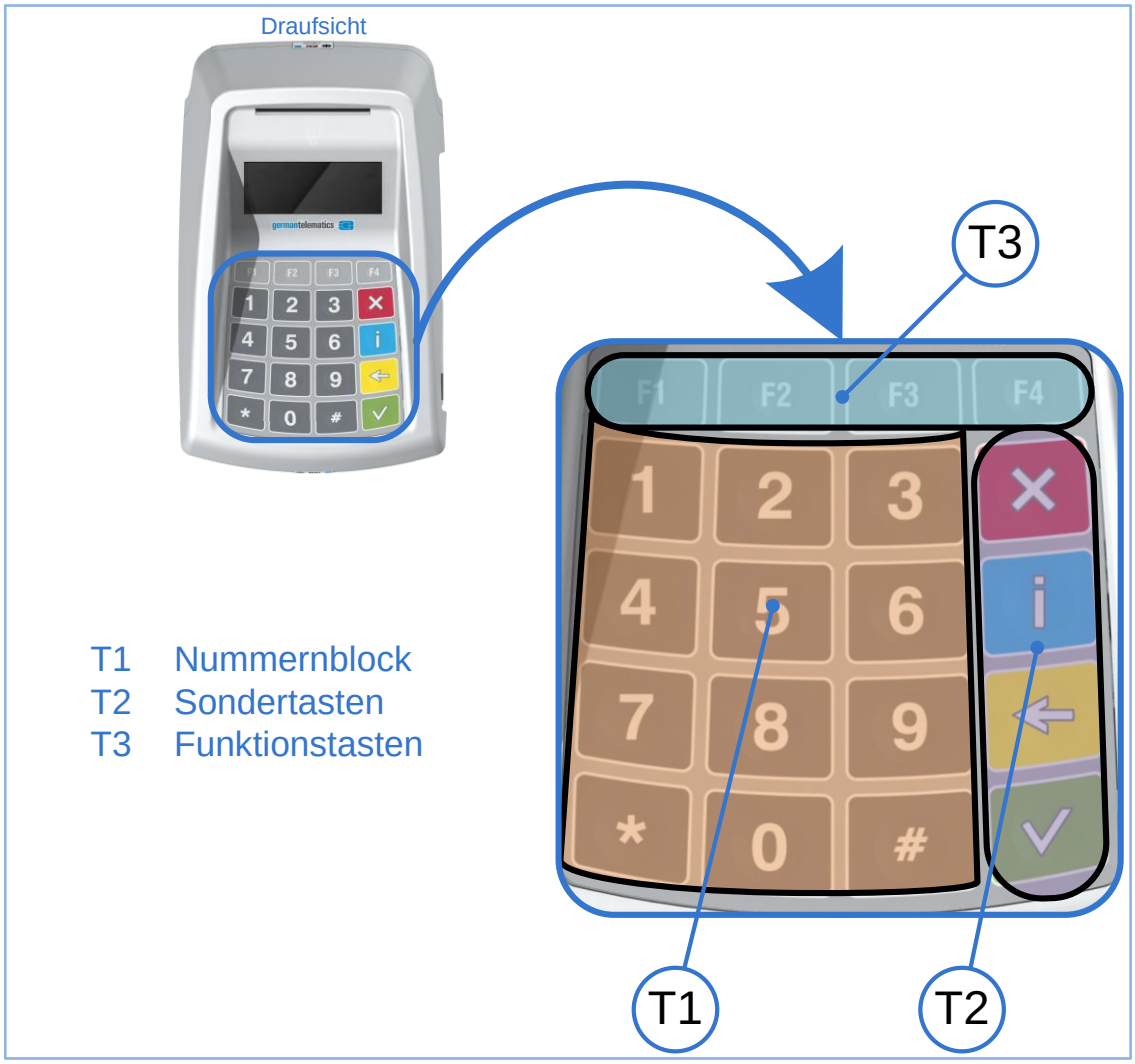


Abbildung 17: Tastatur des eHealth GT900 Chipkartenterminal

Tabelle 1: Tastaturbelegung des eHealth GT900 Chipkartenterminal

Symbol	In Abb.2	Funktion	Bemerkung
1	**T1**	Nummerntasten 0, .., 9	
F1	**T3**	Funktionstaste F1	**Halten Sie die F1 Taste länger gedrückt, um zum Admin-Modus zu gelangen.**
F2	**T3**	Funktionstaste F2	**Navigationstaste im Admin-Modus**
F3	**T3**	Funktionstaste F3	**Navigationstaste im Admin-Modus**
F4	**T3**	Funktionstaste F4	**Kurz drücken, um 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 Chipkartenterminals finden sich in Abschnitt 1.8 „Reinigen und Desinfizieren des Gerätes“.

2.2 Kartenslots

Das eHealth GT900 Chipkartenterminal ist mit zwei Chipkarten-Kontakteinheiten ausgestattet, um die Verwendung der Krankenversichertenkarte (KVK), der elektronischen Gesundheitskarte (eGK) sowie des Heilberufsausweises (HBA) oder Institutionenkarte (SMC-B) sicherzustellen. 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 Chipkartenlesegerät sei im Folgenden die Kontakteinheit 1 vornehmlich als eGK/KVK-Slot und die Kontakteinheit 2 vornehmlich als HBA-Slot bezeichnet. Ziehen Sie für diese Zuweisung auch Abbildung 19 zu Rate.

Des Weiteren verfügt das Chipkartenterminal über 2 SIM-Slots für SMC-Karten (Secure Module Cards) auf der rechten Geräteseite. In die SIM-Slots des Chipkartenlesegerätes können auch sogenannte gSMC-KT Karten eingelegt werden. Das Chipkartenlesegerät nutzt eine eingelegte gSMC-KT Karte, welche die kryptografische Identität des Chipkartenlesegerätes 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 zertifiziert wurde, und über die entsprechenden Kennungen und Sicherheits-merkmale verfügt. Beachten Sie bitte die Hinweise in Abschnitt 2.2.3 „SIM-Slots“ und lesen Sie bitte auch die Info-Box „Wichtige Hinweise zum Umgang mit den SMC“ auf S. 40.

2.2.1 Kontakteinheit 1: Einstecken einer eGK/KVK

Eine KVK beziehungsweise eGK 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 20). Es repräsentiert den Chipkartenslot der Chipkarten-Kontakteinheit 1.

Wenn sich eine 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.

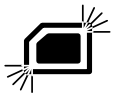
Das nebenstehende Symbol wird Ihnen angezeigt sobald eine PIN an die betreffende Karteneinheit gesendet wird.

2.2.2 Kontakteinheit 2: Einstecken eines HBA/SMC-B

Eine HBA oder SMC-B kann vorzugsweise in der Chipkarten-Kontakteinheit 2 (HBA-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 20). Es repräsentiert den Chipkartenslot der Chipkarten-Kontakteinheit 2.

Wenn sich eine 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 Chipkartenterminal 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 ein Slot, in dem sich eine gSMC-KT befindet, mit einem Administratorsiegel versehen sein muss.

Schalten Sie das Gerät aus, bevor Sie eine SMC einlegen! Beachten Sie, dass ein Entfernen der Chipkartenhalter im Betrieb zu einer Sicherheitsverletzung führt. **Entfernen Sie diese Chipkartenhalter daher niemals leichtfertig.** Lesen Sie bei einer Sicherheitsverletzung Kapitel 9 „Problembehebung“.

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.

Nachdem Sie eine gSMC-KT in einen der SIM-Slots des Gerätes geschoben haben, versiegeln Sie diesen SIM-Slot mit den im Lieferumfang enthaltenen SIM-Slot-Siegeln. Der Administrator des Gerätes unterschreibt auf dem Siegel bevor dieses auf dem Gerät angebracht wird in dem dafür vorgesehenen Feld (siehe Abbildung 18). Darüber hinaus muss sich der Administrator die Siegel-Nr. notieren und diese Notiz verwahren.

Die SIM-Slot-Siegel müssen beim Tausch einer gSMC-KT erneuert werden. Zu diesem Zweck ist im Lieferumfang des Chipkartenlesegerätes eine entsprechende Anzahl an überzähligen SIM-Slot-Siegeln vorhanden.

Das nebenstehende Symbol wird Ihnen in der oberen Statuszeile des Displays angezeigt (siehe Abbildung 20). Es repräsentiert jeweils einen der zur Verfügung stehenden SIM-Slots des Kartenlesegerätes. 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 SMC in einem der SIM-Slots befindet, so wird dieses Symbol ausgefüllt im Display dargestellt.

Bei einem Datenzugriff auf die 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.

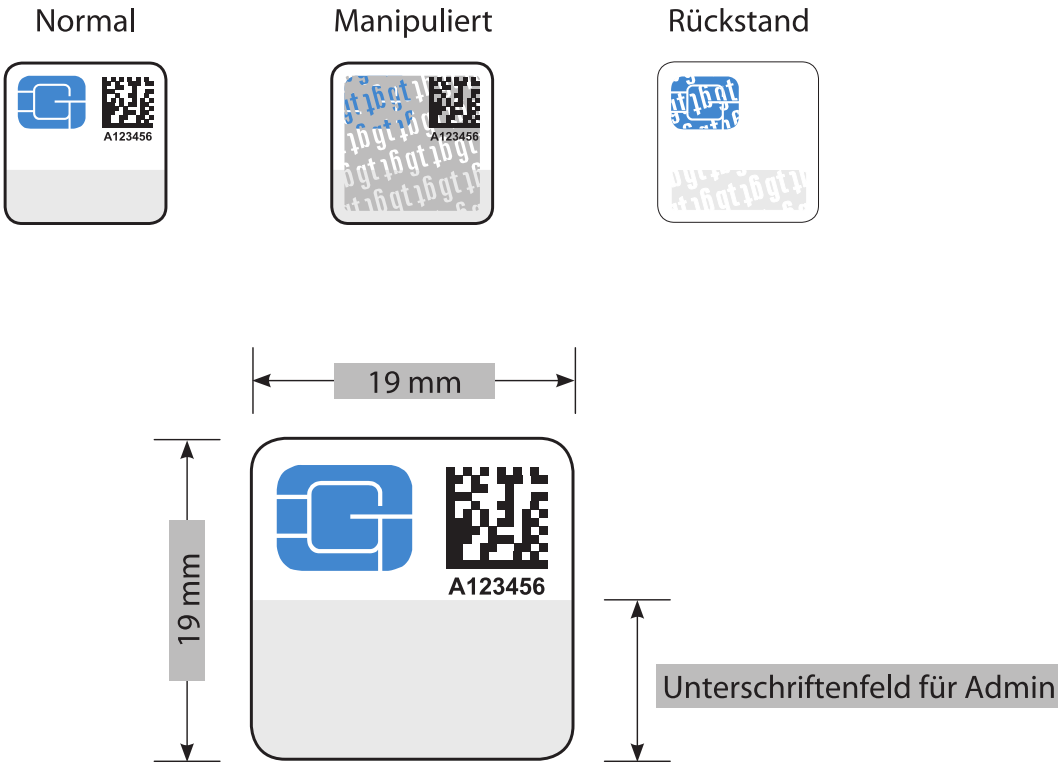


Abbildung 18:Sicherheitsmerkmale der SIM-Slot Siegel[7]

Wird das Anbringen eines neuen Siegels durch den Wechsel der gSMC-KT nötig, entfernen Sie vorher die Klebereste des alten Siegels.

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

Wichtige Hinweise zum Umgang mit den SMC:

SMC SIM-Slots müssen versiegelt werden, wenn sich darin eine gSMC-KT befindet. Wenn Sie eine gSMC-KT 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. Wurden Ihnen bei Auslieferung der gSMC-KT oder des Gerätes keine Siegel zur Verfügung gestellt, so wenden Sie sich bitte an Ihren zuständigen Systemdienstleister.

Geräte mit eingelegter gSMC-KT und nicht versiegelten SIM-Slots dürfen nicht verwendet werden! Überprüfen Sie auch die SIM-Slot Siegel regelmäßig auf mögliche Manipulationen!

2.2.4 Notentnahme einer eGK/HBA/SMC-B/gSMC-KT

Sollte die Notentnahme einer eGK/HBA/SMC-B/ gSMC-KT notwendig werden, so können Sie die Karte auf normalem Wege aus dem jeweiligen Kartenslot entfernen. Wenden Sie hierzu keine Gewalt an. Die Karten sollten sich genauso einfach aus dem Kartenhalter entfernen lassen wie sie eingesteckt wurden.

Zur Notentnahme einer Karte aus einem der seitlichen SIM-Slots entfernen Sie zuerst das Siegel des Slots. Drücken Sie dann den Entriegelungsstift neben dem Slot vorsichtig mit einem spitzen Gegenstand in das Gehäuseinnere. Der SIM-Slot-Schlitten wird dann aus dem Gerät herausgleiten und Sie können diesen entnehmen.

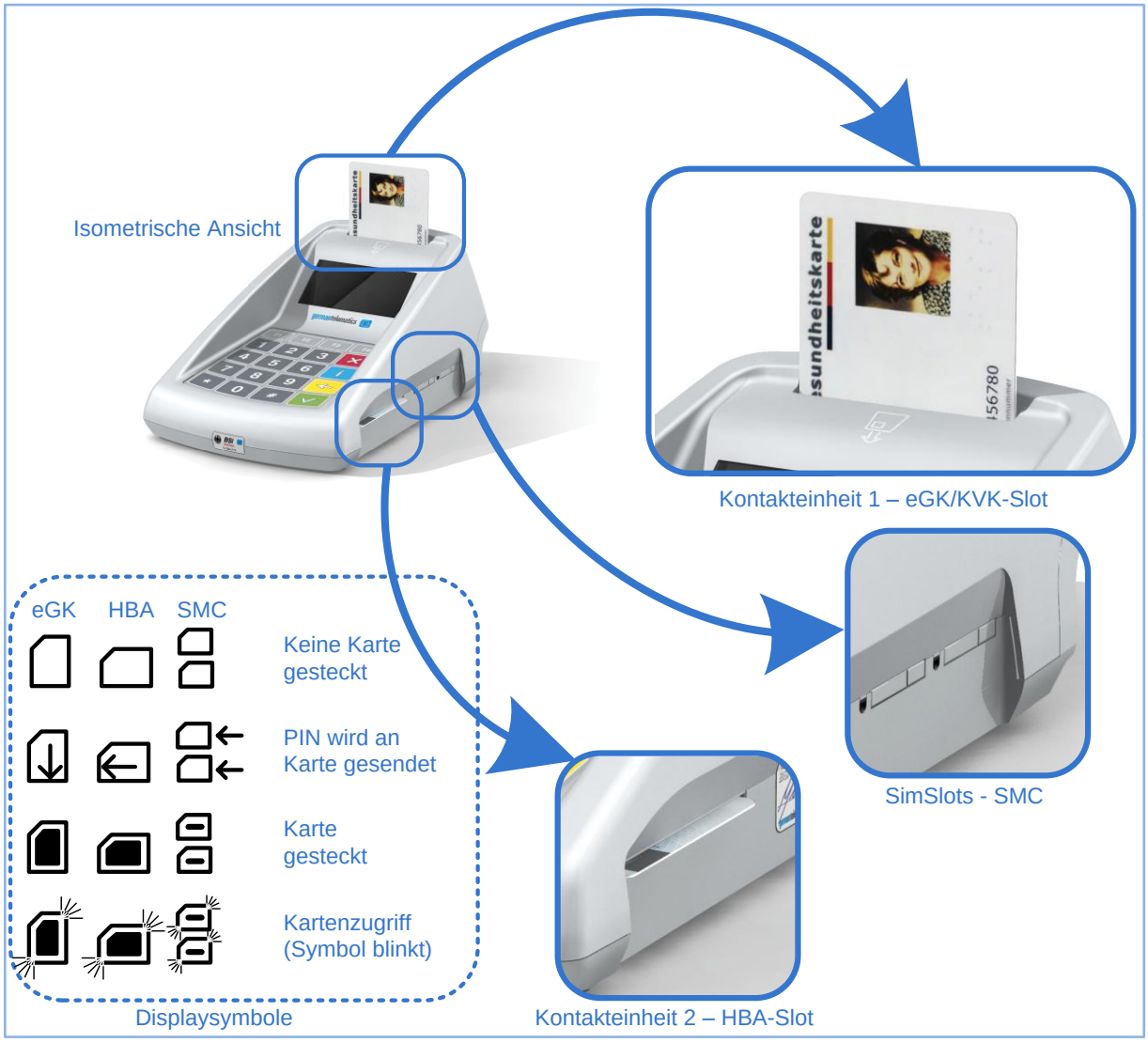


Abbildung 19: Anordnung und Benennung der Kartenslots

2.3 Aufbau der Displayanzeige

Auf dem Display des Gerätes werden Ihnen Informationen und Anweisungen angezeigt, die für die Arbeit mit dem Chipkartenterminal notwendig sind. Das Display gliedert sich, wie in Abbildung 20 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.

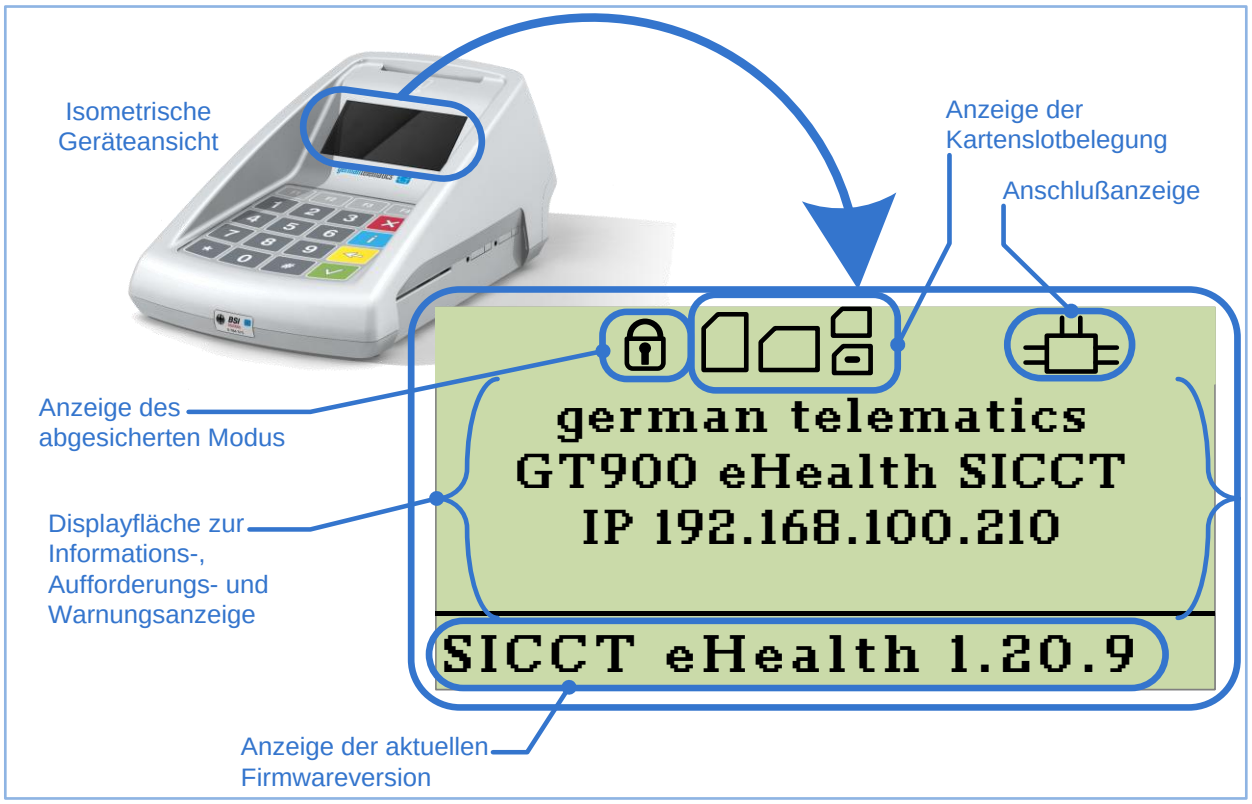
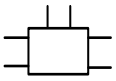
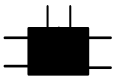
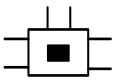


Abbildung 20: Displayaufbau des eHealth GT900 Chipkartenterminal

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


Eine physikalische Ethernetverbindung ist vorhanden.


Eine SICCT-Session zu einem Konnektor ist aufgebaut.


Eine TLS-Verbindung zu einem Konnektor ist aufgebaut.

Die Anzeige des abgesicherten Modus[8] befindet sich in der oberen Statusleiste links im Display. In der Displaymitte werden Ihnen Informationen, Aufforderungen oder

[8] Der abgesicherte Modus garantiert Ihnen eine sichere PIN-Eingabe für Ihre eGK oder HBA Geheimnummer (PIN).

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 21 dargestellt.

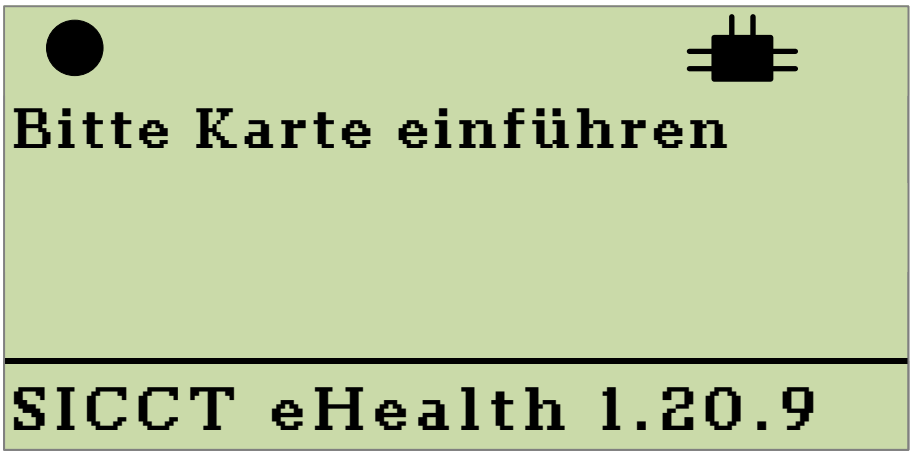


Abbildung 21: Beispielhafte Anzeige

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 Chipkartenterminal in ein LAN-Netzwerk eingebunden. Das Chipkartenterminal wird somit ausschließlich über die Ethernet-Schnittstelle 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 Chipkartenterminal kann in einer LAN-Umgebung gemäß den Bestimmungen der gematik zum Aufbau einer IT-Infrastruktur für das deutsche Gesundheitswesen verwendet werden. Um sich innerhalb der eHealth Infrastruktur zu identifizieren, muss zudem eine gSMC-KT in das Gerät eingelegt sein. Lesen Sie hierzu auch den Abschnitt 2.2.3 „SIM-Slots“.

Der Konnektor, der sich, wie auch das Karteterminal, innerhalb eines kontrollierten Bereiches befindet, muss durch die gematik zugelassen sein. Der Konnektor muss in der Lage sein, eine gesicherte Verbindung zum Chipkartenterminal 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 Chipkartenterminals 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 Chipkartenterminal als eHealth Kartenterminal mit einem Konnektor zu koppeln, muss ein sogenannter Pairingprozess [9] eingeleitet werden. Der Pairingprozess wird durch den Konnektor angestoßen. Lesen Sie daher bitte im Handbuch des Konnektors nach, wie dieser Pairingprozess in Gang gesetzt werden kann. Während des Pairingprozesses werden Ihnen, gesteuert durch den Konnektor, Anweisungen im Display des Chipkartenterminals angezeigt. Diese Anweisungen müssen Sie befolgen, um einen erfolgreichen Pairingprozess von Konnektor und

[9] Als Pairing bezeichnet man die logische Verbindung zwischen Chipkartenterminal, der darin eingelegten gSMC-KT und dem Konnektor. Das Pairing verhindert somit das eine dieser Entitäten unberechtigter Weise ausgetauscht werden kann.

Chipkartenterminal durchzuführen. Darüber hinaus kann sich der Konnektor, um Firmwareupdates und Konfigurationsänderungen am Terminal durchzuführen, in der Administrator-Rolle am Terminal anmelden. Dafür geben Sie in den Einstellungen des Konnektors als Anmeldedaten für die SICCT Admin Authentifizierung den SICCT-Benutzernamen "admin" und Ihr SICCT Admin-Passwort ein. Folgen Sie des Weiteren der Anleitung Ihres Konnektors. Wie Sie das SICCT Admin-Passwort ändern, können Sie in Abschnitt 4.7 nachlesen.

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

Wichtige Hinweise zum Pairing-Prozess:

!

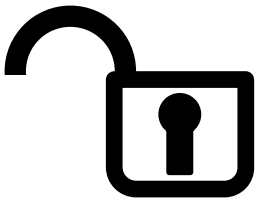
Stellen Sie als Administrator des Chipkartenlesegerätes sicher, dass während des Pairing-Prozesses, d.h. während des Pairings des Chipkartenterminals mit einem Konnektor, keine unautorisierten Personen Zugang zum Kartenterminal oder zum Konnektor erlangen können.

Um den initialen Pairing-Prozess zu autorisieren, müssen Sie nach der Pairing-Abfrage am Terminal Ihre Admin PIN eingeben.

3.2 Eingabe einer Karten-PIN

Die sichere und vertrauliche Eingabe einer entsprechenden PIN (eGK, HBA oder SMC-B) ist elementarer Bestandteil des Sicherheitskonzeptes dieses Chipkartenlesegerätes. Daher müssen PINs stets unbeobachtet eingegeben werden! Um die Sicherheit während der PIN-Eingabe zu gewährleisten, wird Ihnen im Display des Chipkartenterminals 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. Die PIN wird dann sicher an die Karte übertragen. Eine Übertragung der PIN an ein anderes Gerät findet so unter keinen Umständen statt.

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

Eine beispielhafte Aufforderung zur PIN-Eingabe ist in Abbildung 22 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. Geben Sie Ihre PIN nicht ein, wenn der abgesicherte Modus nicht durch ein geschlossenes Schlosssymbol angezeigt wird.**

Das Chipkartenlesegerät GT900 führt alle sicherheitsrelevanten Aktionen ausschließlich in einem vertrauenswürdigen Modus aus. Darunter fällt insbesondere die Verifizierung einer Karten-PIN.

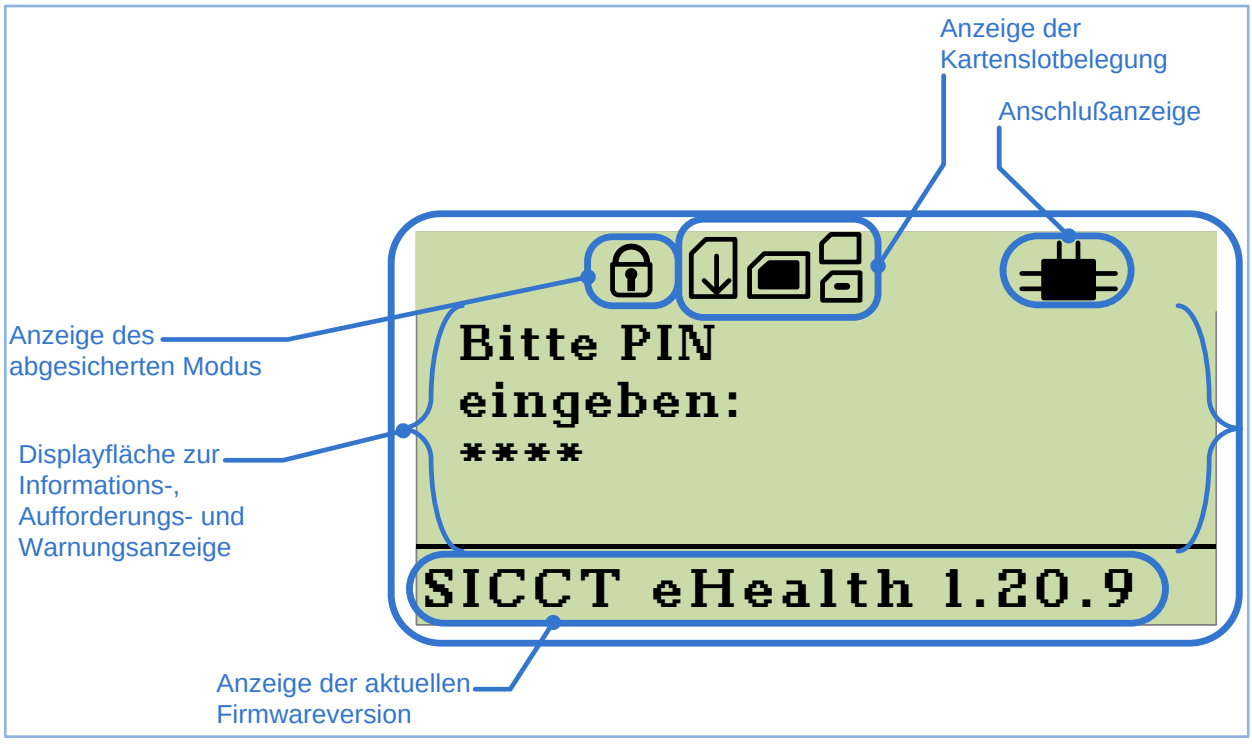


Abbildung 22: Mögliche Displayanzeige des Chipkartenterminals bei der Eingabe einer Karten PIN. In diesem Beispiel wird die Karten-PIN an die Karte im eGK-Slot gesendet (zusätzlich sind ein HBA und eine SMC eingelegt).

4 Geräteeinstellungen

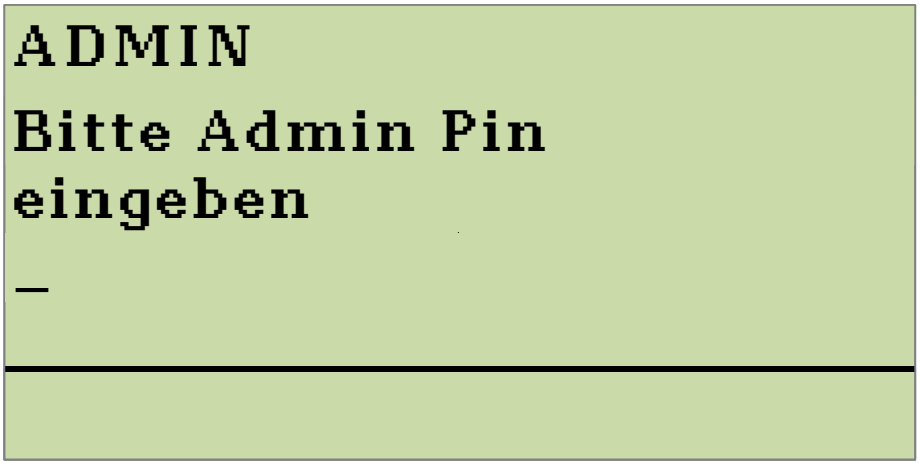
Es wird in diesem Benutzerhandbuch davon ausgegangen, dass es sich bei Administratoren um gut geschultes IT-Personal handelt. Der Administrator ist in der Verwaltungsverantwortung aller sicherheitsrelevanten Funktionen des Chipkartenterminals sowie mit der Dokumentation und dem Betrieb des Kartenterminals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

Konfigurationseinstellungen für das Chipkartenterminal können im Administrator-Menü direkt am Chipkartenterminal 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.

4.1 Admin-Menü

Das Administrator-Menü kann geöffnet werden, solange keine TLS-Verbindung oder SICCT-Session zwischen Terminal und Konnektor besteht. Eine bestehende Verbindung erkennen Sie an der voll oder teilweise ausgefüllten Anschlussanzeige (Abbildung 22). Trennen Sie in dem Fall die Netzwerkverbindung eines der Geräte oder deaktivieren Sie das Terminal im Kartenterminaldienst des Konnektors.

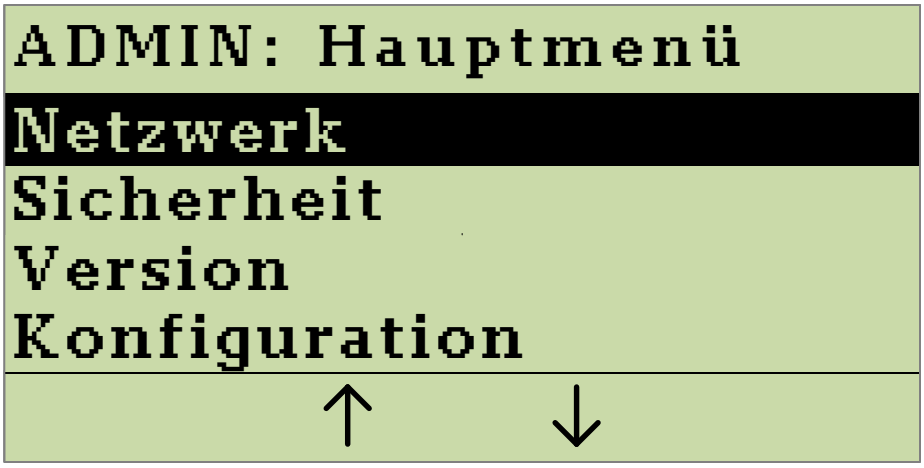
Um in das Administrator-Menü zu gelangen, drücken Sie die F1 -Taste des eingeschalteten Chipkartenterminals für mindestens 5 Sekunden. Sie werden aufgefordert, die Administrator PIN einzugeben. Zu der Vergabe der Admin PIN lesen Sie bitte den Abschnitt 1.6 „Inbetriebnahme des Chipkartenterminals“.



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

Abbildung 23: Abfrage der Admin PIN

Bestätigen Sie die PIN-Eingabe mit der ✓-Taste. Sollten Sie die Administrator 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 Administrator PIN wird Ihnen das Admin-Menü im Display angezeigt.



Im Admin-Menü finden Sie verschiedene Optionen zur Geräteinstellung.

Abbildung 24: Anzeige Admin-Menü

Im Admin-Menü haben Sie vier Optionen zur Geräteinstellung:

Netzwerk: Netzwerkkonfiguration des Chipkartenterminals

Sicherheit: Ändern sicherheitsrelevanter Einstellungen

Version: Anzeige und Aktualisieren der Firmware-Version

Konfiguration: Konfiguration für Displayanzeige und Keep-Alive

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 25 finden Sie den vollständigen Aufbau des Admin-Menüs.

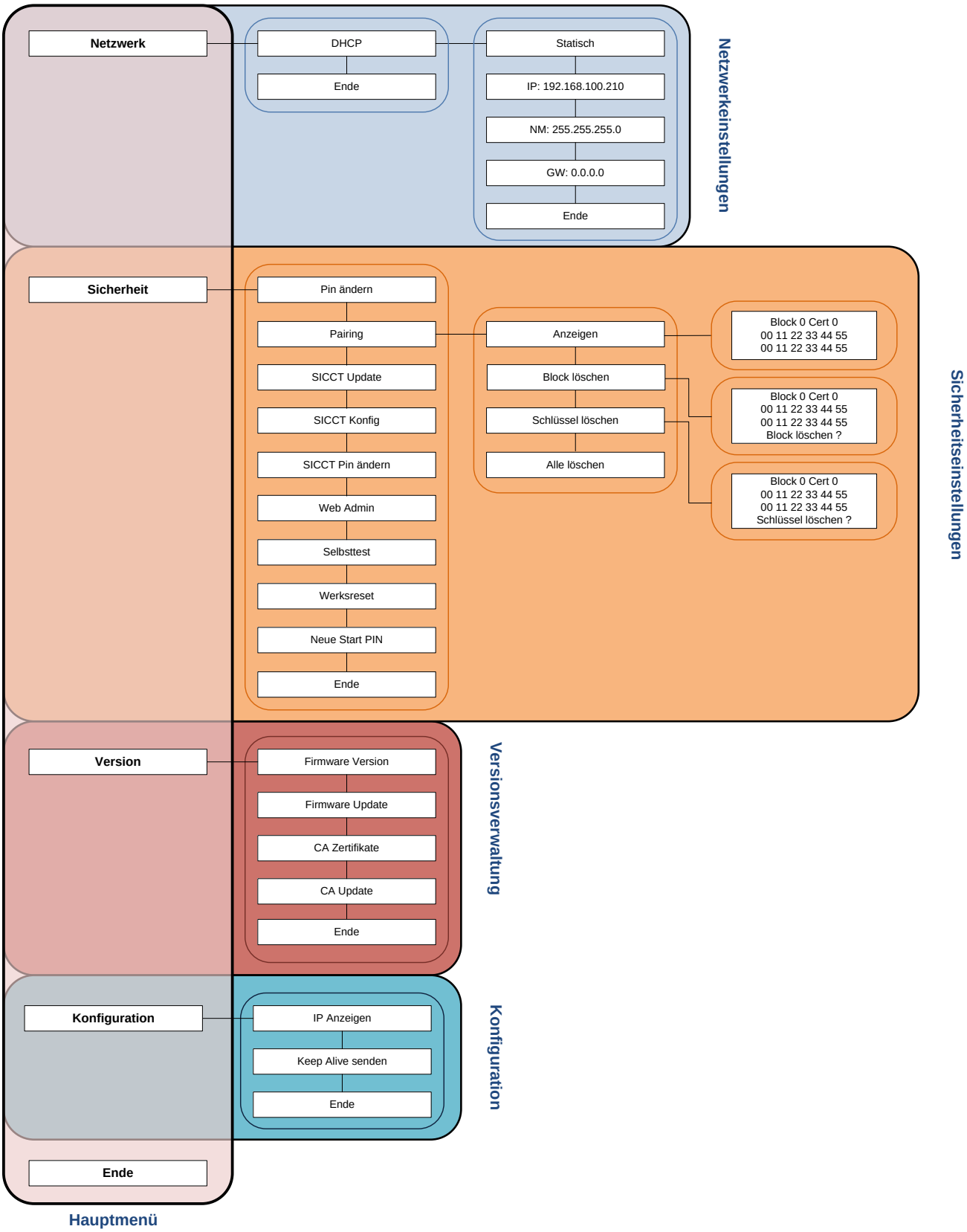


Abbildung 25: Struktur des Admin-Menüs

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

! **Halten Sie die Administrator PIN, Start PIN und PUK geheim.** Stellen Sie bei der Eingabe der PIN bzw. PUK sicher, dass niemand sonst diese lesen kann. **Verwenden Sie keine Trivial-PIN/PUK wie beispielsweise 11111111 oder 12345678[10]. Vermeiden Sie es, die Administrator PIN, Start PIN und PUK in der Nähe des Gerätes aufzubewahren, insbesondere sollten Sie sie nicht auf dem Gerätegehäuse notieren.** Die Administrator PIN ermöglicht Ihnen den Zugriff auf die Managementschnittstellen Ihres Kartenterminals und erlaubt somit das Abfragen und Ändern von sicherheitskritischen Konfigurationen.

! Verwahren Sie die Administrator PIN, Start PIN und die PUK daher sorgsam und sicher! **Sollten Sie die Administrator PIN dennoch verlieren bzw. vergessen, so können Sie mit Hilfe der Geräte PUK Ihr Gerät in den Auslieferungszustand zurückversetzen.** Bewahren Sie daher die Administrator PIN und die 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.

[10] Trivial-PINs und PUKs werden vom Gerät nicht angenommen und durch die Anzeige einer entsprechenden Fehlermeldung abgewiesen.

4.2 Netzwerkkonfiguration

Das Chipkartenterminal muss zum Betrieb als eHealth Kartenterminal in ein LAN-Netzwerk eingebunden werden. Um innerhalb dieses Netzwerkes mit einem Konnektor abgesichert kommunizieren zu können, muss das Chipkartenterminal über seine Ethernet-Schnittstelle mit dem lokalen Netzwerk verbunden sein. Die Vergabe einer IP-Adresse an das Chipkartenterminals 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 Chipkartenterminal 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.

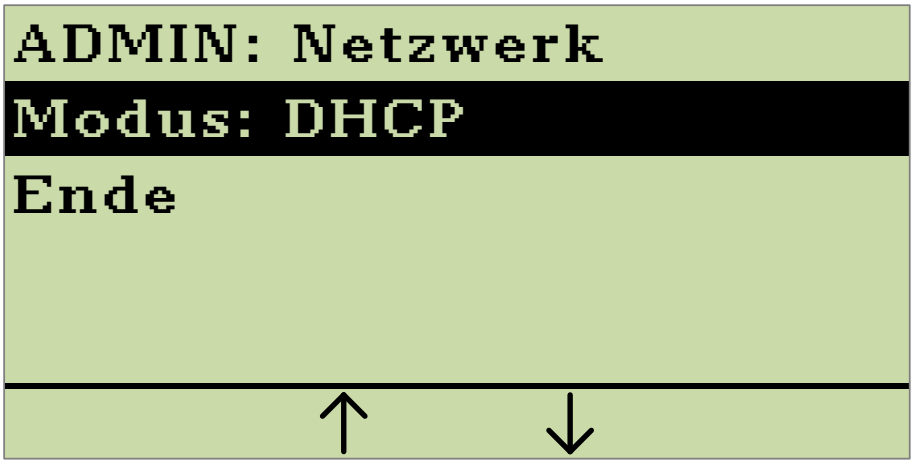
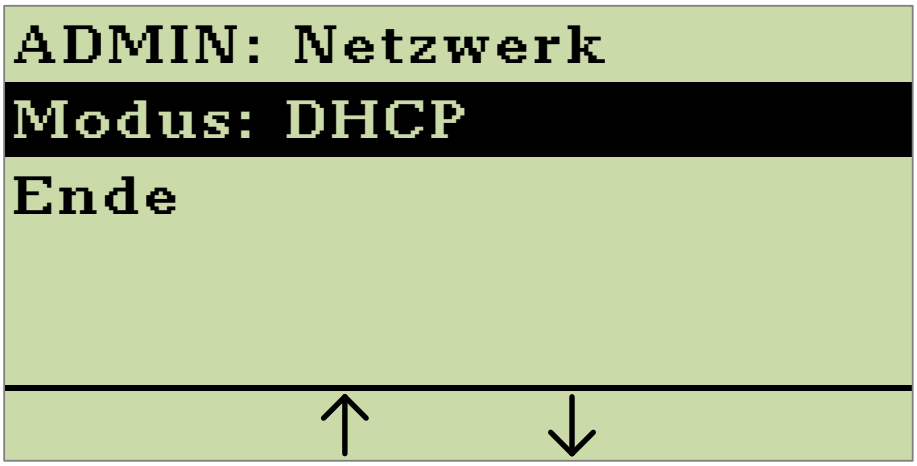


Abbildung 26: Beispielhafte Anzeige des Submenüs "Netzwerk"

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**.

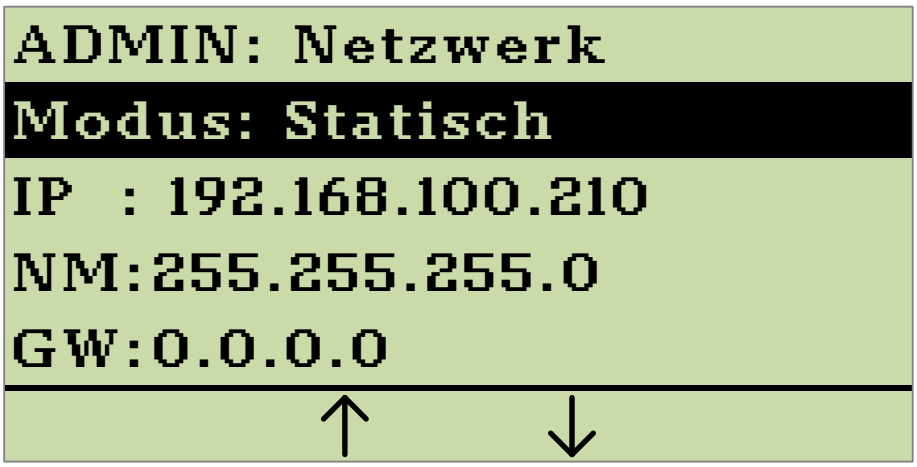


Wählen Sie den Parameter **DHCP**, um eine dynamische Netzwerk-konfiguration einzuleiten.

Abbildung 27: 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 4.13.

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 28: 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. Falls die Eingabe für ein Feld kürzer als drei Zeichen ist, muss die ✓-Taste gedrückt werden, um die Eingabe im nächsten Feld fortzusetzen.

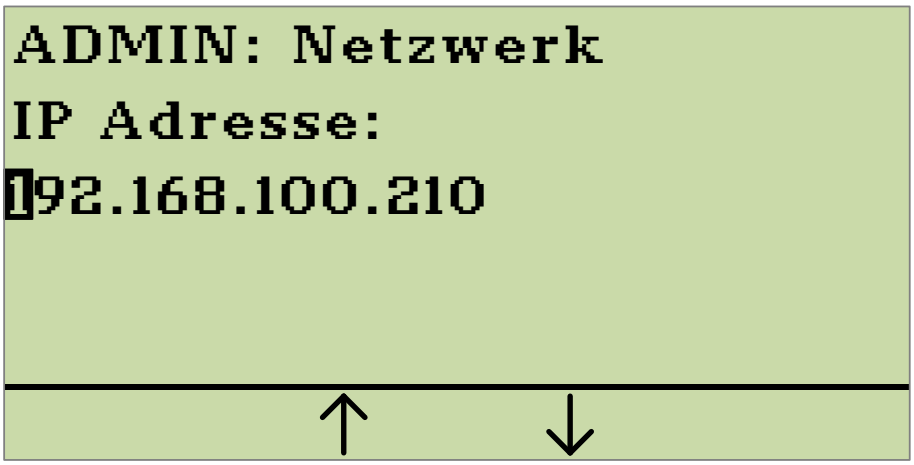


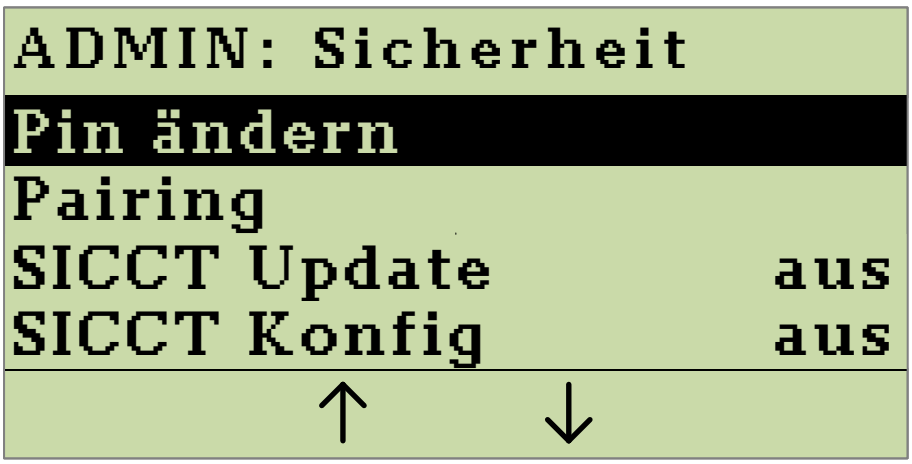
Abbildung 29: Beispiel für eine statische IP-Adresse

In Abbildung 29 ist die Eingabe einer beispielhaften IP-Adresse dargestellt. Für jeden Wert sind vier Felder **x.x.x.x** vorgesehen. In jedes Feld können drei numerische Zeichen eingegeben werden. Um einen vollständig eingegebenen Wert zu bestätigen, drücken Sie die ✓-Taste.

Sobald alle Werte für die Netzwerkparameter eingegeben wurden, wählen Sie die Option **Ende** und drücken die ✓-Taste zur Bestätigung. Die statische Netzwerk-konfiguration ist nun aktiviert.

4.3 Ändern der Admin PIN

Um eine neue Administrator PIN zu vergeben, müssen Sie die aktuelle Administrator 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.

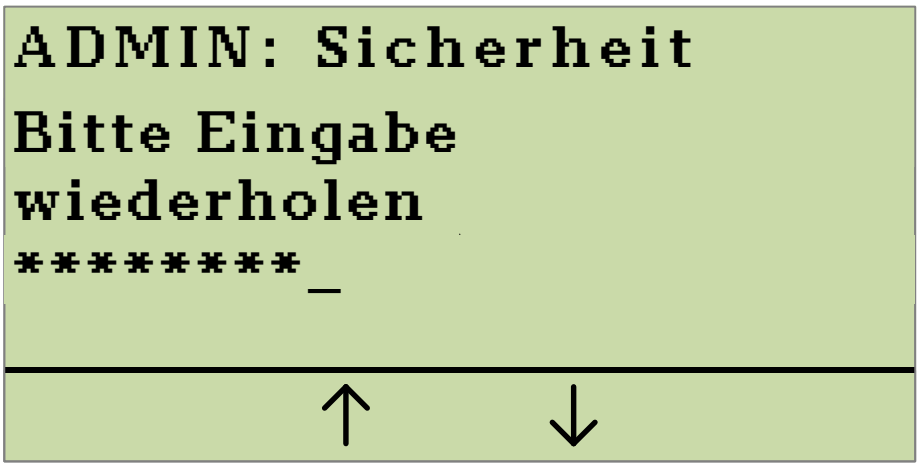
Abbildung 30: Anzeige des Submenüs "Sicherheit"

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 31 und Abbildung 32). 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 numerischen Zeichen** 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[11].**

[11] Trivial-PINs werden vom Gerät nicht angenommen und durch die Anzeige einer entsprechenden Fehlermeldung abgewiesen.

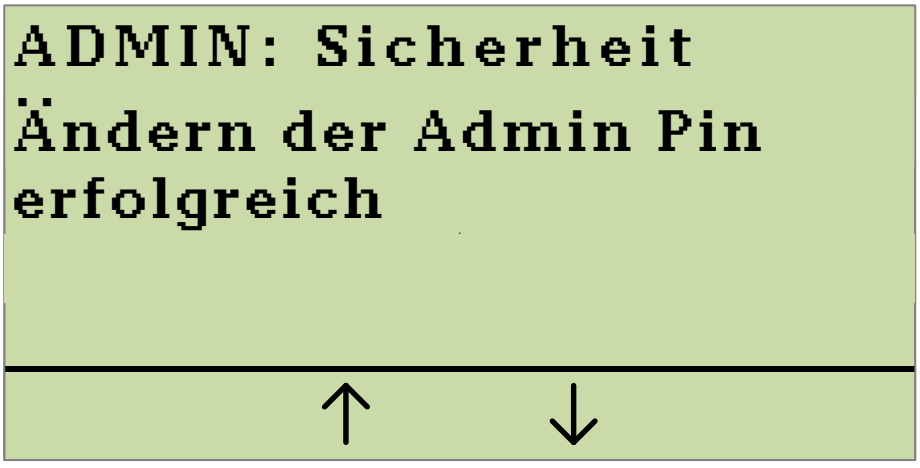
Eingabe der neuen PIN. Bestätigen Sie mit der ✅-Taste.

Abbildung 31: Eingabe einer neuen Admin PIN



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

Abbildung 32: Wiederholte Eingabe der Admin PIN

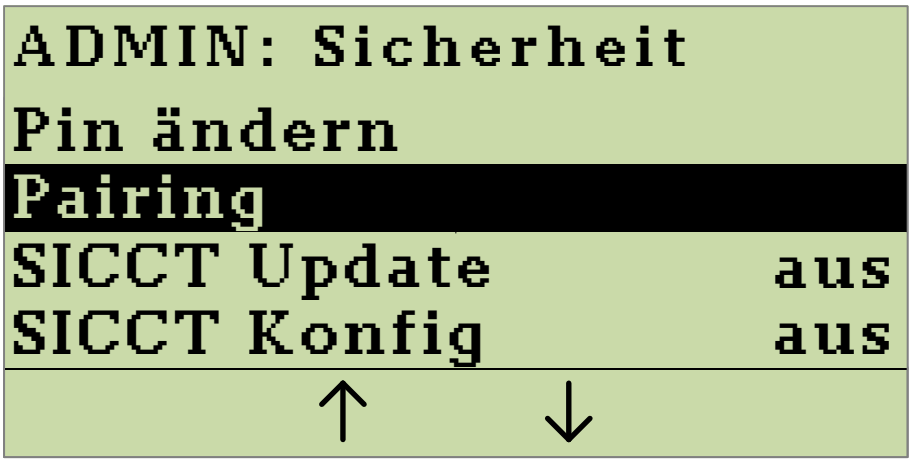


Ihnen wird anschließend eine kurze Bestätigung angezeigt und Sie kehren zum Admin-Menü zurück.

Abbildung 33: Bestätigung der erfolgreichen Änderung der Admin PIN

4.4 Pairing

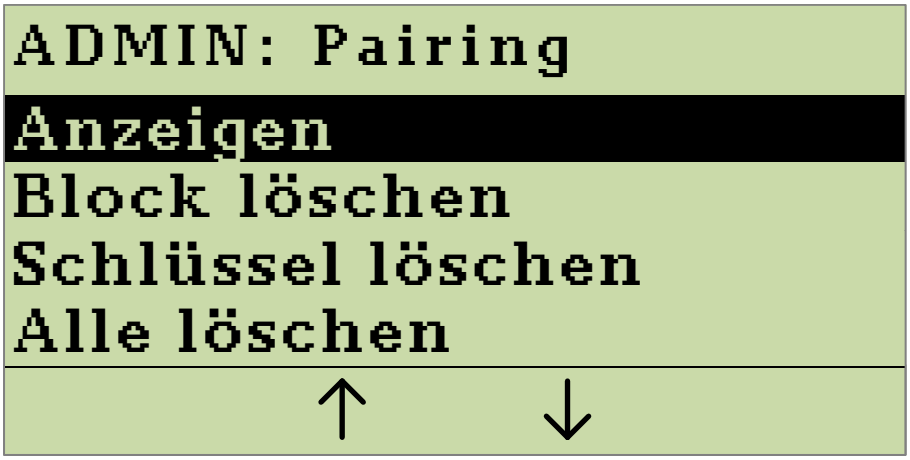
Das Pairing mit einem Konnektor ist für den Betrieb Ihres eHealth Kartenterminals unabdingbar. Lesen Sie hierzu auch den Abschnitt 3.1 „Pairing“. Daher sollte das bestehende Pairing zu einem Konnektor nicht leichtfertig gelöscht werden. Um das derzeitige Pairing mit einem Konnektor zu löschen, wählen 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 34: 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 35 gezeigten Optionen ausführen können.

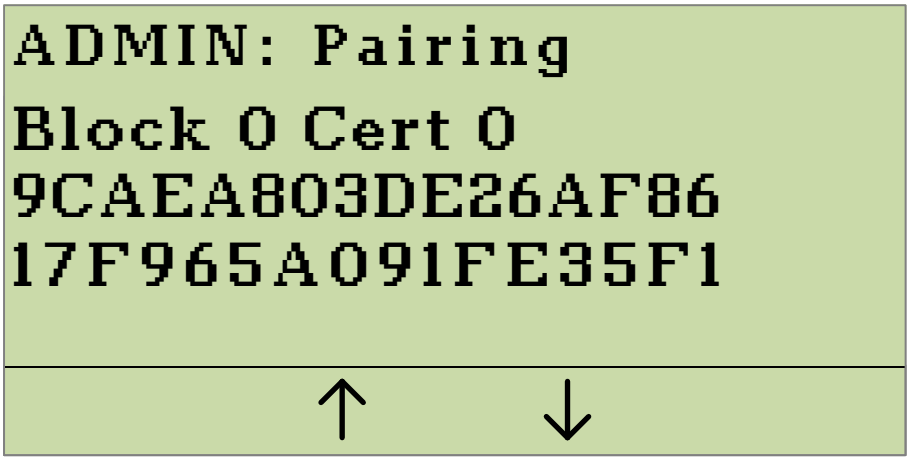


Drücken Sie die ✓-Taste, um einen Menüpunkt auszuwählen.

Abbildung 35: Menü zum Bearbeiten bestehender Pairings

4.4.1 Pairing anzeigen

Das Submenü **Anzeigen** zeigt für jedes bestehende Pairing den Pairingblock und die zugehörigen Fingerprints[12] an. Um in das Submenü **Anzeigen** zu gelangen, wählen Sie im Submenü **Pairing** die Option **Anzeigen** und bestätigen Sie durch Drücken der ✓-Taste. Abbildung 36 stellt eine beispielhafte Anzeige eines Pairingblocks mit dem Fingerprint eines Zertifikates dar. Mit den Tasten F2 und F3 können Sie zwischen verschiedenen Fingerprints wählen.



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

Abbildung 36: Menü zum Anzeigen vorhandener Fingerprints

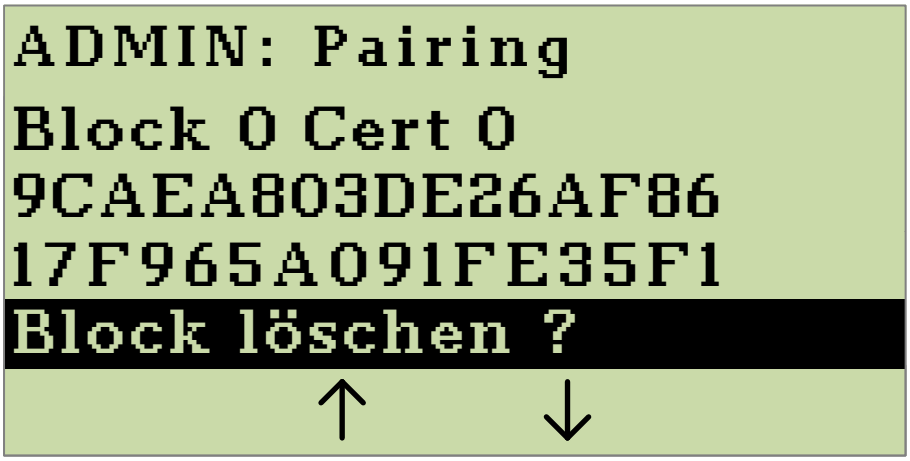
Durch Drücken der ✗-Taste oder der ✓-Taste können Sie in das Untermenü **Pairing** zurückkehren.

4.4.2 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

[12] 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.

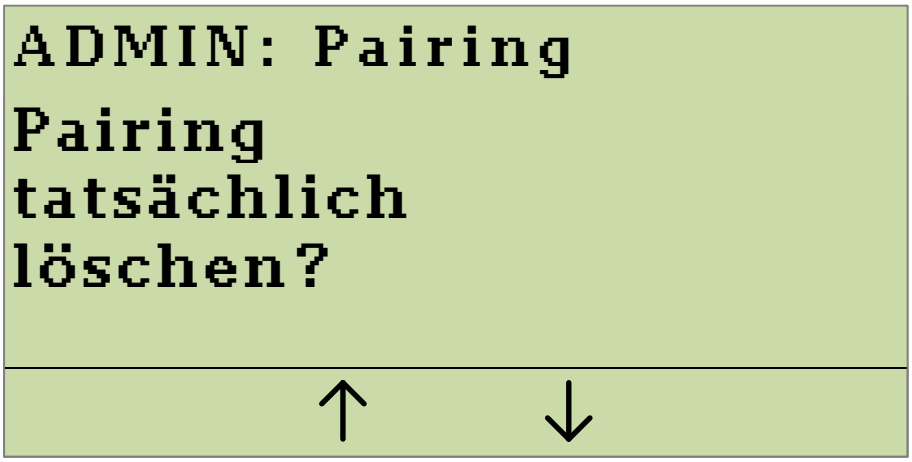
Block löschen und bestätigen Sie durch Drücken der ✓-Taste. Abbildung 37 stellt eine beispielhafte Anzeige eines Pairingblocks mit dem zugehörigen Fingerprint dar. Mit den Tasten F2 und F3 können Sie zwischen verschiedenen Pairing-blöcken wählen. Durch Drücken der ✓-Taste können Sie einzelne Pairingblöcke durch Auswahl und Bestätigen der Option **Block löschen ?** permanent vom Gerät entfernen.



Drücken Sie die ✓-Taste, um vorhandene Pairingblöcke zu löschen.

Abbildung 37: 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 Sicherheits-abfrage durch Drücken der ✓-Taste. Durch Drücken der ✗-Taste können Sie das Löschen des Pairings auch wahlweise abbrechen.

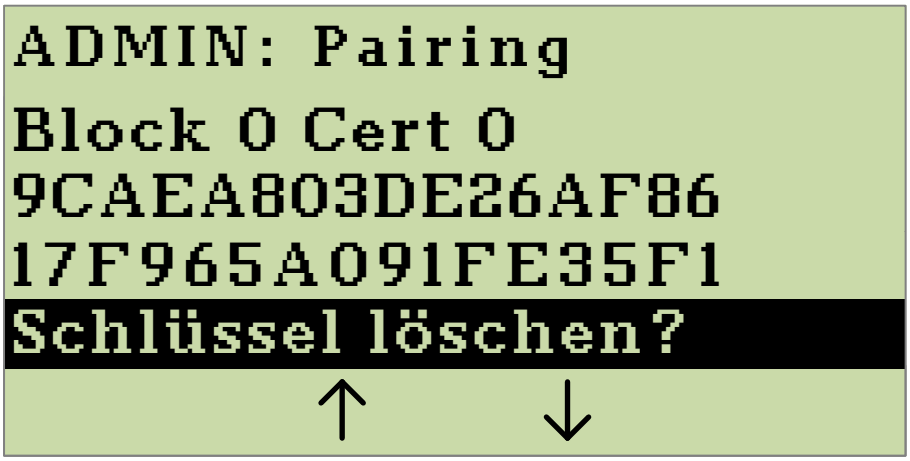


Drücken Sie die ✓-Taste, um das Löschen eines Pairings zu bestätigen.

Abbildung 38: Sicherheitsabfrage zum Löschen eines Pairings

4.4.3 Schlüssel löschen

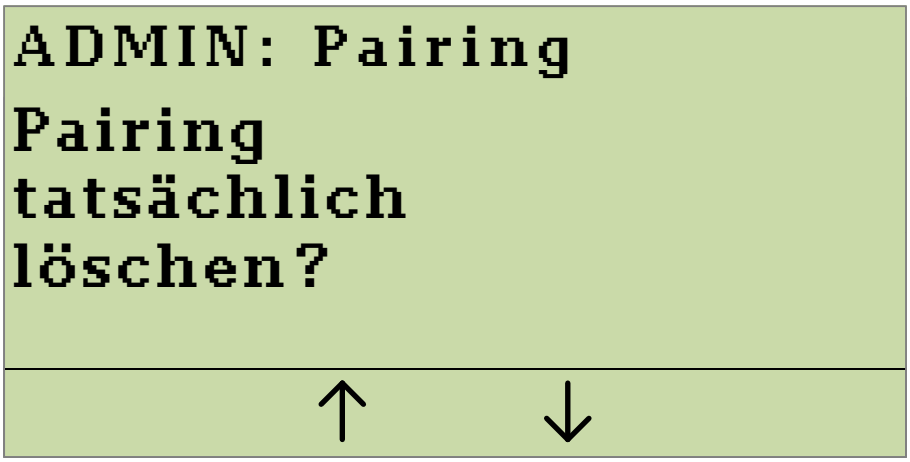
Das Submenü **Schlüssel löschen** zeigt für jedes bestehende Pairing den Pairingblock und die Fingerprints der Zertifikate an. Zusätzlich besteht in diesem Menü die Möglichkeit die einzelnen öffentlichen Schlüssel der Konnektorzertifikate (bis zu drei) zu löschen. Um in das Submenü **Schlüssel löschen** zu gelangen, wählen Sie im Submenü **Pairing** die Option **Schlüssel löschen** und bestätigen Sie durch Drücken der ✓-Taste. Abbildung 39 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.

Abbildung 39: 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.



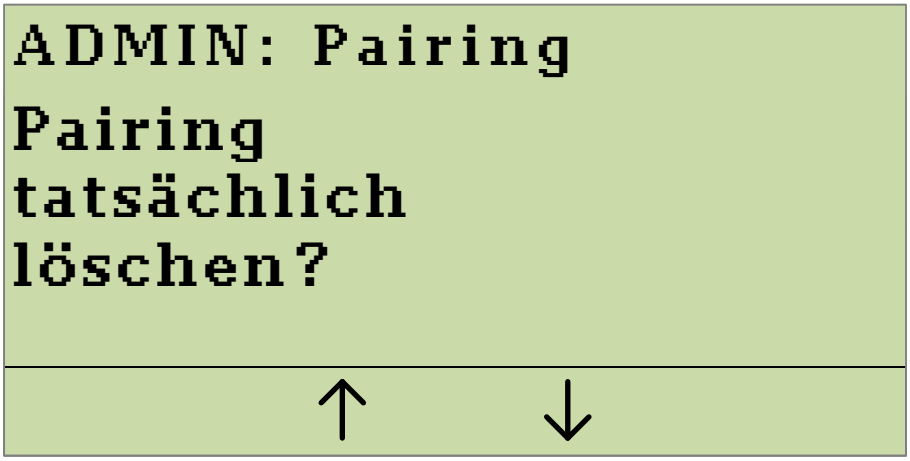
Drücken Sie die ✓-Taste, um das Löschen eines Schlüssels aus einem Pairingblock zu bestätigen.

Abbildung 40: Sicherheitsabfrage zum Löschen eines Schlüssels

4.4.4 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.

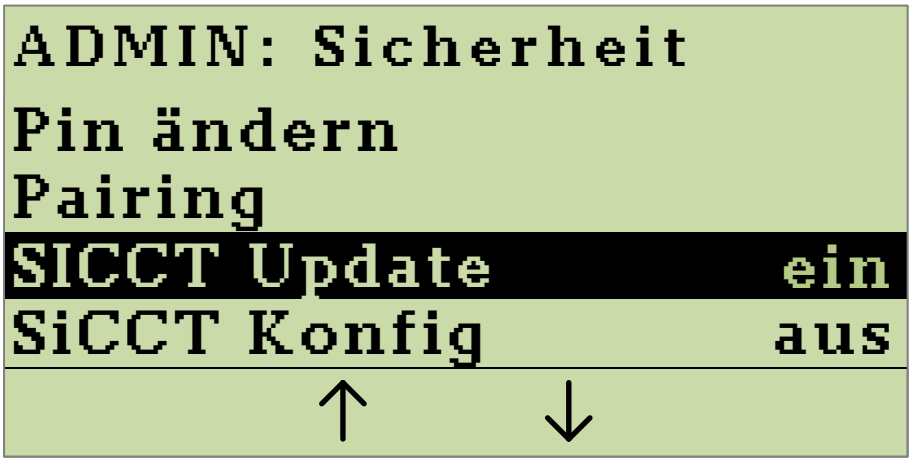


Drücken Sie die ✅-Taste, um das Löschen der Pairings zu bestätigen.

Abbildung 41: Sicherheitsabfrage zum Löschen aller Pairings

4.5 SICCT Update ein- oder ausschalten

Um die Durchführung automatischer 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 42: 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.

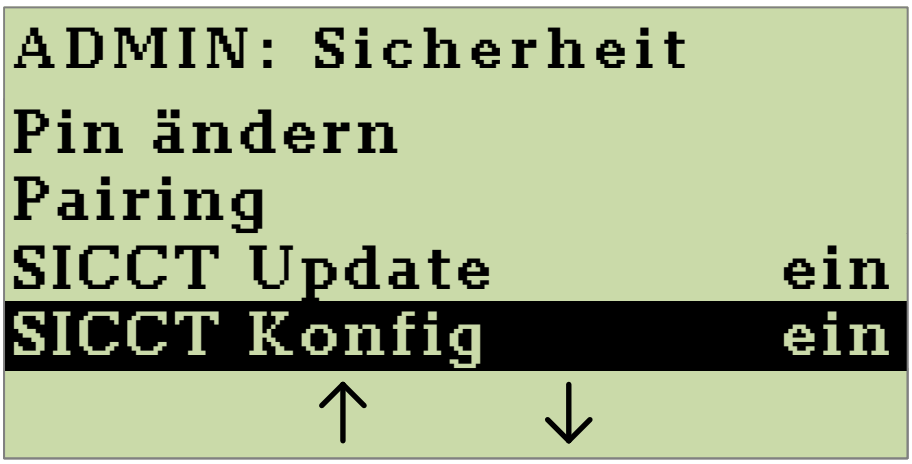
Wichtiger Hinweis zum Autoupdate

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 Chipkartenterminal 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.**

4.6 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 43: 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.

4.7 Ändern der SICCT PIN

Die SICCT PIN ermöglicht es einem Administrator, sich per Netzwerk am SICCT-Port des Chipkartenterminals als Administrator zu identifizieren. Er kann so über die SICCT Schnittstelle ein neues Firmwareupdate einspielen oder den Terminalnamen ändern.

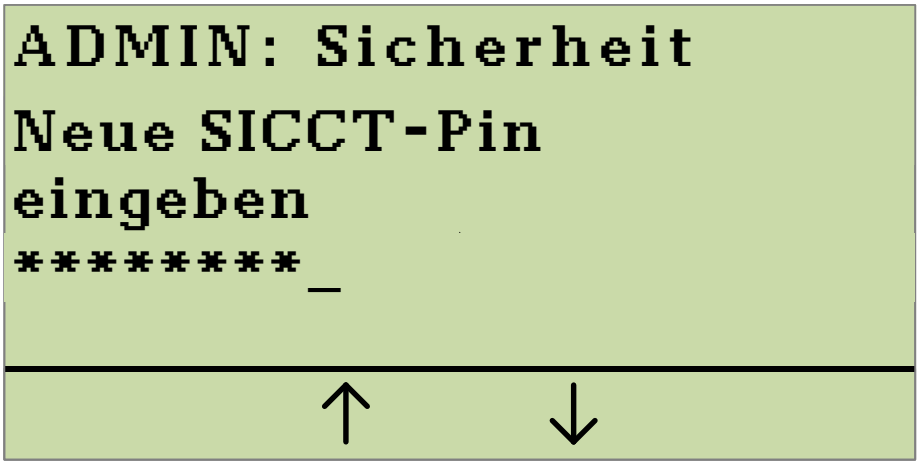
Hinweis: Bitte beachten Sie, dass für die administrative Nutzung des SICCT-Ports an Ihrem Chipkartenterminal die gleiche SICCT-Admin PIN vergeben sein muss, wie sie für den SICCT-Port am Konnektor für dieses Terminal eingestellt wurde.

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.

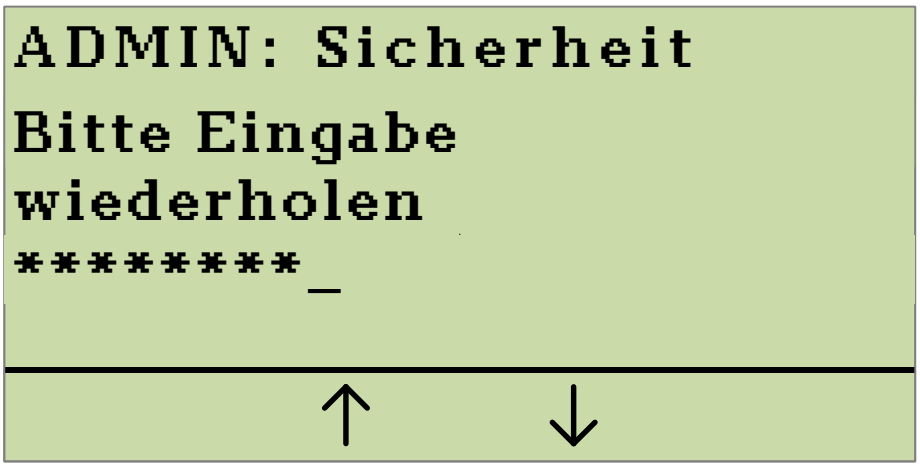
Abbildung 44: Anzeige des Submenüs "Sicherheit"

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 45 bis Abbildung 47). 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 numerischen Zeichen** bestehen. Die Zeichen * und # können nicht verwendet werden. Durch Drücken der ✓-Taste bestätigen Sie Ihre Eingabe.



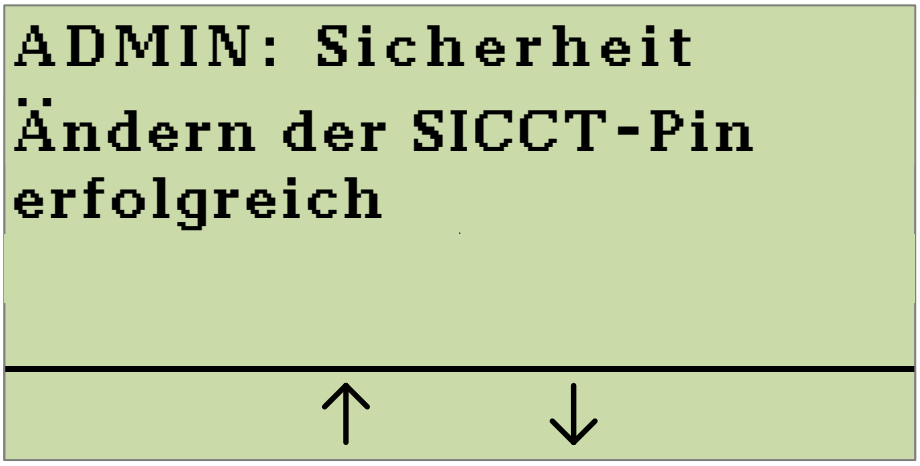
Eingabe der neuen SICCT PIN. Bestätigen Sie mit der ✅-Taste.

Abbildung 45: Eingabe einer neuen SICCT PIN



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

Abbildung 46: Wiederholte Eingabe der SICCT PIN



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

Abbildung 47: Bestätigung der erfolgreichen Änderung der SICCT PIN

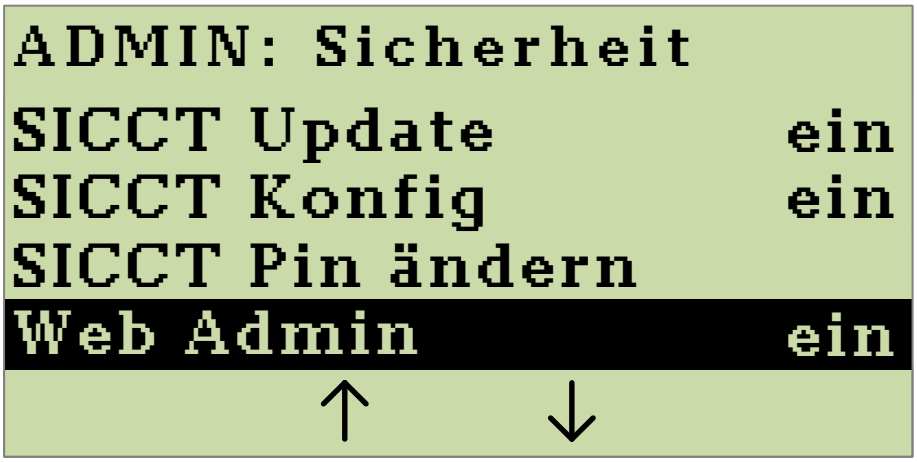
Hinweis: Verwenden Sie keine trivialen PINs wie beispielsweise 11111111 oder 12345678[13].

4.8 Web Admin Schnittstelle ein- oder ausschalten

Ihr Chipkartenterminal verfügt über eine Weboberfläche zur Geräteadministrierung, die Sie am Computer in einem Internetbrowser öffnen können. Den Zugriff auf diese Weboberfläche können Sie ein- oder ausschalten. In der Weboberfläche können Sie das Chipkartenterminal aus der Ferne konfigurieren, schalten Funktionen ein oder aus und erhalten Informationen über ihr Chipkartenterminal und zu bestehenden Pairings.

Um Einstellungen am Chipkartenterminal über eine Weboberfläche aus der Ferne vornehmen zu können, wählen Sie im Admin-Menü die Option **`Sicherheit`** und bestätigen dies mit der ✓-Taste. Auf dem Display wird Ihnen das Submenü **`ADMIN: Sicherheit`** angezeigt.

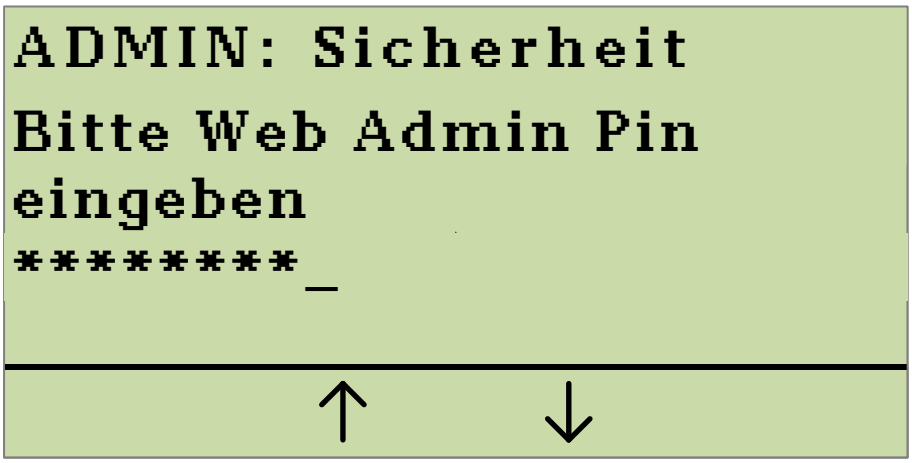
[13] Trivial-PINs werden vom Gerät nicht angenommen und durch die Anzeige einer entsprechenden Fehlermeldung abgewiesen.



Drücken Sie die ✓-Taste, um die Web-Admin Schnittstelle ein- oder auszuschalten.

Abbildung 48: Anzeige des Submenüs "Sicherheit"

Wählen Sie die Option **Web Admin** aus und wählen Sie durch Drücken der ✓-Taste, ob die betreffende Option **Ein** oder **Aus** geschaltet werden soll. Wenn Sie die Web-Admin Schnittstelle einschalten, werden Sie zudem aufgefordert, einen Web-Admin PIN zu vergeben. Diese benötigen Sie, um sich als berechtigter Administrator an der Weboberfläche des Chipkartenterminals anmelden zu können. Für die Web-Admin PIN gelten dieselben Vorgaben wie für die Administrator PIN.



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

Abbildung 49: Anzeige des Submenüs "Sicherheit"

Die Web Admin PIN muss aus **mindestens 8 numerischen Zeichen** bestehen. Die Zeichen * und # können nicht verwendet werden. Bewahren Sie die PIN an einem sicheren Ort auf. Vermeiden Sie es, die Web Admin 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**[14]. Lesen Sie hierzu bitte auch die Hinweise zum Umgang mit der Administrator PIN am Ende des Abschnittes 4.1 „Admin-Menü“. Sie werden anschließend zu einer Wiederholung der PIN aufgefordert. Das erfolgreiche Setzen einer Web Admin PIN wird Ihnen mit einer entsprechenden Meldung im Display des Terminals bestätigt.

Wenn Sie zu einem späteren Zeitpunkt die Weboberfläche des Chipkartenterminals deaktivieren wird die Web Admin PIN gelöscht. Beim erneuten Einschalten der Weboberfläche werden Sie dann gebeten, eine neue Web Admin PIN zu vergeben.

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

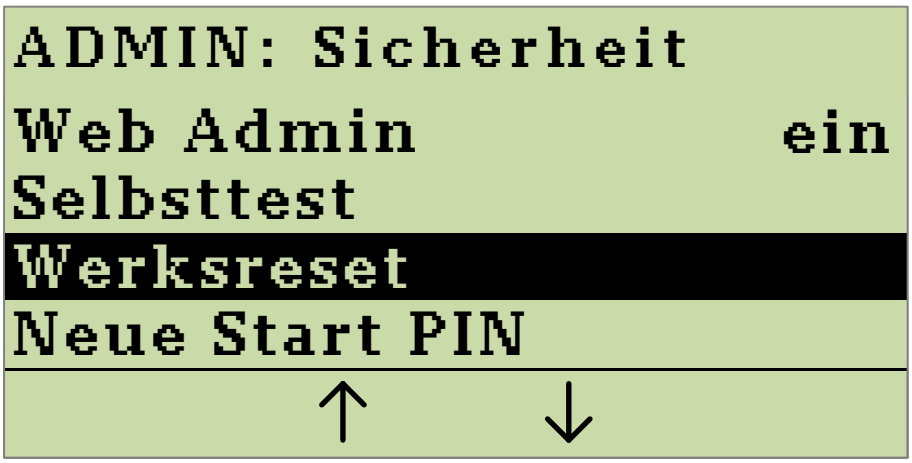
4.9 Selbsttest ausführen

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.

[14] Trivial-PINs werden vom Gerät nicht angenommen und durch die Anzeige einer entsprechenden Fehlermeldung abgewiesen.

4.10 Werksreset ausführen

Sie können über das Auswählen der Option **Sicherheit** im Admin-Menü und anschließendes Auswählen der Option **Werksreset** das Chipkartenlesegerät in den Auslieferungszustand zurückversetzen. Lesen Sie hierzu bitte den Abschnitt 5.2 „Zurücksetzen mit Kenntnis der Admin PIN“.



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

Abbildung 50: Anzeige des Submenüs "Sicherheit"

4.11 Neue Start PIN vergeben

Um eine neue Start PIN zu vergeben, 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 **Neue Start PIN** aus und bestätigen Sie durch Drücken der ✓-Taste. Das Chipkartenlesegerät erzeugt nun eine zufällige 12-stellige PIN und zeigt Ihnen diese im Display an. **Notieren Sie diese Start PIN und bewahren Sie sie an einem sicheren Ort auf!**

Aus Sicherheitsgründen müssen Sie vor der Erzeugung einer neuen Start PIN alle Pairings Ihres Gerätes löschen. Das Gerät weist Sie darauf hin, sollten noch aktive Pairings bestehen. Wie Sie diese löschen können, erfahren Sie in Abschnitt 4.4.4 “Alle Pairings löschen”.

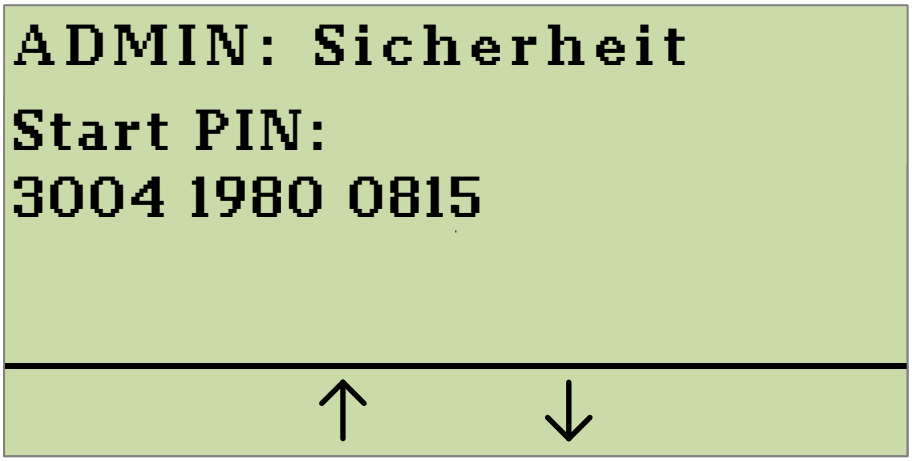


Abbildung 51: Anzeige des Submenüs "Sicherheit" bei Erzeugung einer neuen Start PIN

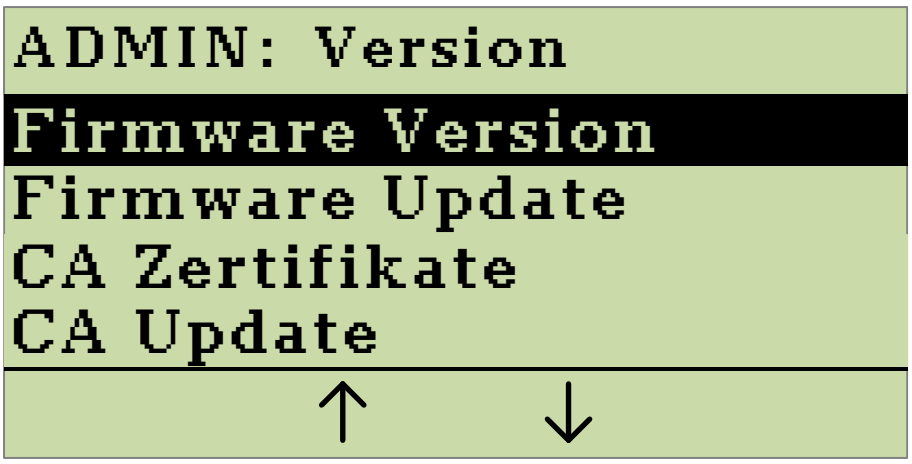
4.12 Firmware-Version und Firmware-Update

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

Prüfen Sie vor einem Firmwareupdate den Ausgangszustand des Terminals (BCS oder SICCT) und führen Sie anschließend ein Update durch, wie es in den entsprechenden Handbuchkapiteln für die jeweilige Ausgangsfirmware beschrieben ist. Für die Anzeige der aktuellen Firmware-Version lesen Sie bitte den Abschnitt 4.12.1 „Anzeige der aktuellen Firmware-Version“. Um ein Firmware-Update durchzuführen, lesen Sie bitte den Abschnitt 4.12.2 „Durchführung eines Firmware-Updates“ bzw. den Abschnitt:

- 4.12.2.1 „Updatevorgang für ein BCS-Terminal GT900“, oder

- 4.12.2.2 „Updatevorgang für ein SICCT-Terminal eHealth GT900“.



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

Abbildung 52: Anzeige des Submenüs "FW-Version"

4.12.1 Anzeige der aktuellen Firmware-Version

Vor und gegebenenfalls nach einem Firmware-Update kann es erforderlich sein, die Versionsnummer der aktuell auf dem Chipkartenterminal 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 Chipkartenterminals angezeigt. Mit den Tasten F2 und F3 können Sie sich weitere Informationen zu Ihrem Chipkartenterminal anzeigen lassen. Um die Anzeige zu verlassen und in das Submenü **ADMIN: Version** zurückzukehren, drücken Sie bitte die ✗-Taste.

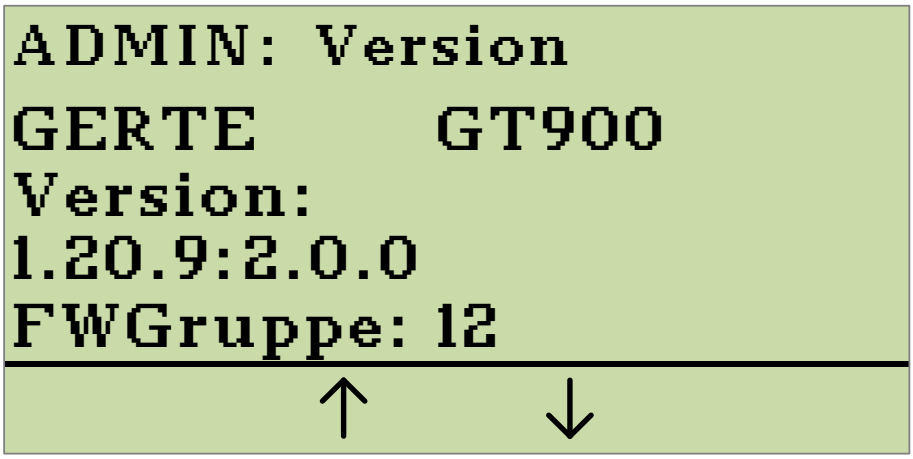


Abbildung 53: Anzeige der aktuellen Firmware-Version

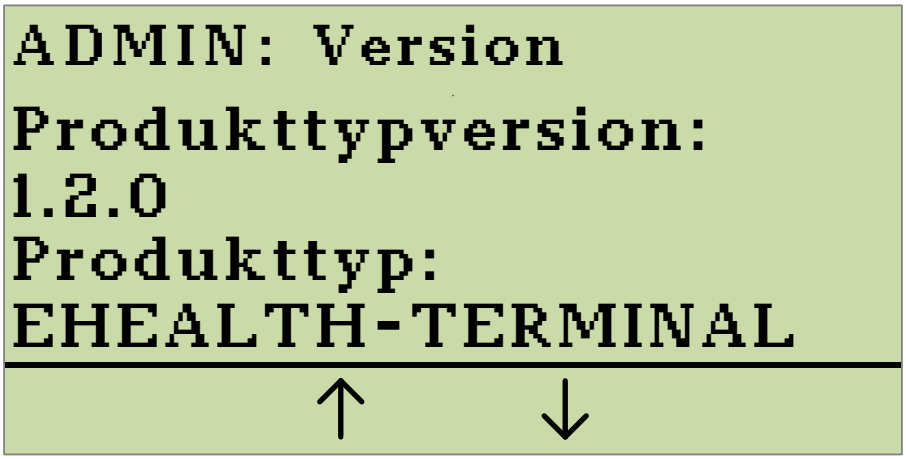


Abbildung 54: Anzeige der Produkttypversion und des Produkttyps

4.12.2 Durchführung eines Firmware-Updates

Um im Sinne der Zertifizierung dieses Gerätes 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 Abschnitt 1.4 „Aufstellungshinweise“.

Neben der Hardware ist die Firmware ein sicherheitssensibles Element. Verwenden Sie aus diesem Grund nur zertifizierte und bestätigte 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 der German Telematics GmbH handelt.

Laden Sie gegebenenfalls eine neue und zertifizierte Firmware-Version Ihres Chipkartenterminals von der Herstellerseite http://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: http://www.germantelematics.de über Versions-änderungen des Handbuchs im Zusammenhang mit Firmware-Updates.

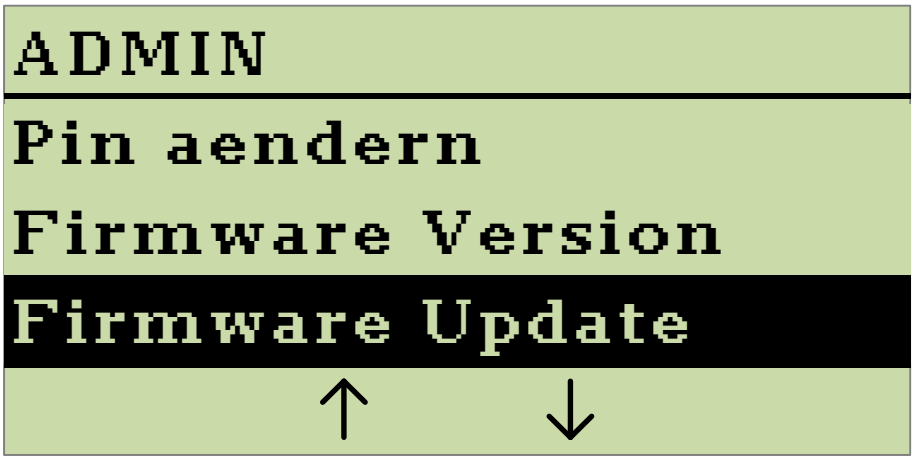
Neben den im Folgenden behandelten Möglichkeiten, ein Terminal direkt per USB-Schnittstelle mit einem Update zu versehen, bietet die german telematics GmbH auf ihren Internetseiten ein Software-Tool „GT900 LAN Setup“ an, mit dem es möglich ist, ein GT900 über die LAN-Schnittstelle mit einem Firmwareupdate (oder auch Downgrade) zu versorgen. Das Tool kann nur bei Terminals eingesetzt werden, die schon über eine SICCT eHealth Firmware verfügen. Das Tool und die Dokumentation

dazu werden auf den Internetseiten der german telematics GmbH stets auf dem aktuellsten Stand gehalten.

4.12.2.1 Updatevorgang für ein BCS-Terminal GT900

Es handelt sich hierbei um zwei Dateien: eine Firmwaredatei und die Signatur dieser Firmwaredatei. Beide Dateien müssen heruntergeladen werden, um die erfolgreiche Durchführung eines Firmware-Updates zu gewährleisten. Wenn Sie die beiden Dateien in Form einer *.zip Datei erhalten haben, dekomprimieren Sie diese auf Ihrem Computer in einem Ordner Ihrer Wahl. Kopieren Sie anschließend die dekomprimierten Dateien auf einen handelsüblichen USB-Stick (nicht im Lieferumfang enthalten, FAT32 formatiert, höchstens 8GB Kapazität). Dieser USB-Stick sollte nach Möglichkeit vorher von allen Dateien befreit werden, d. h. er sollte leer sein. Halten Sie den so präparierten USB-Stick für die nun folgende Update-Prozedur bereit.

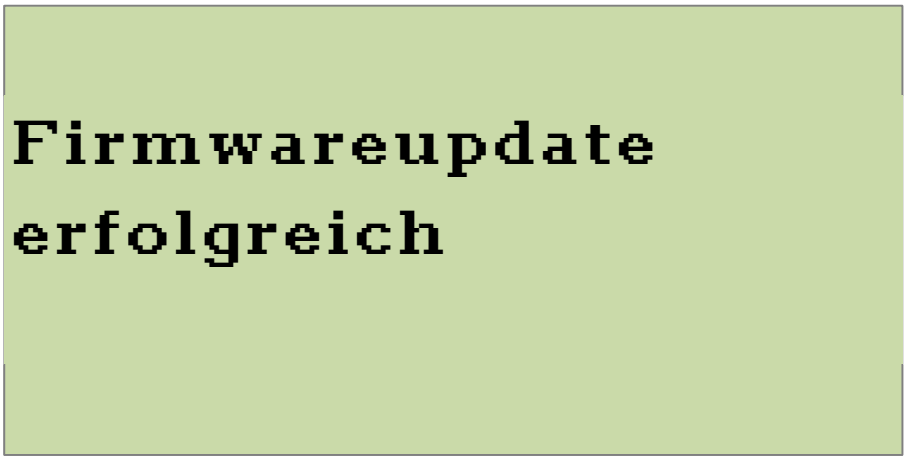
Wechseln Sie zunächst, wie in Abschnitt 4.1 „Admin-Menü“ beschrieben, in den Administrator-Modus. Wählen Sie nun im Menü den Menüpunkt **`Firmware Update`** aus und bestätigten Sie ihre Auswahl mit der ✓ -Taste (siehe Abbildung 55).



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

Abbildung 55: Ansicht Administrator Menü bei BCS-Geräten

Stecken Sie den zuvor präparierten USB-Stick in die USB-Typ-A-Buchse ihres Chipkartenterminals. In Abbildung 6 (Geräteanschlussbelegung) ist dieser Anschluss mit Position ① gekennzeichnet. Machen Sie sich gegebenenfalls nochmals mit den Anschlüssen des Chipkartenterminals vertraut (s. Abschnitt 1.5 „Anschluss des Gerätes“). Wurde eine korrekt signierte Firmware mit einer höheren Versionsnummer als der derzeitig installierten gefunden, werden Sie aufgefordert einen Freischaltcode einzugeben. Diesen erhalten Sie auf Anfrage bei German Telematics. Halten Sie dazu die MAC Adresse Ihres Terminals bereit. 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 schaltet sich nach einer kurzen Statusanzeige („Verifikation Fehlgeschlagen“) aus. Daraufhin können Sie das Gerät neu starten und wie gewohnt mit der alten Firmware weiterarbeiten.



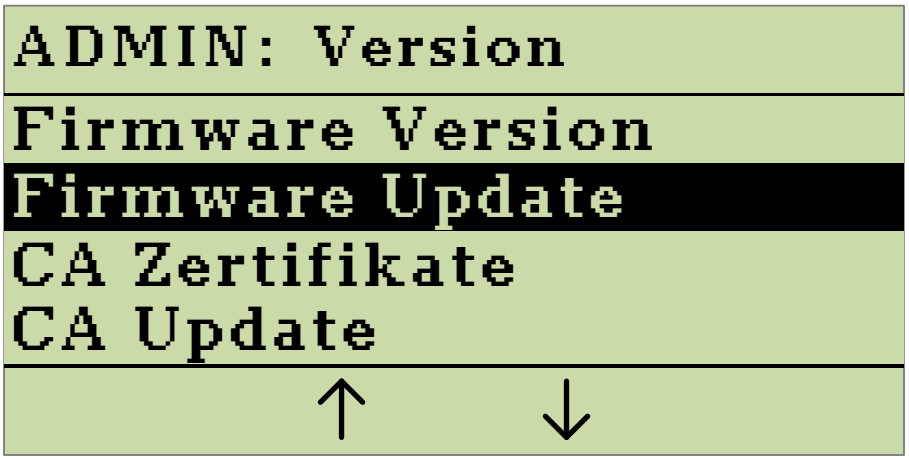
War das Firmware-Update erfolgreich, so erscheint die nebenstehende Anzeige im Display.

Abbildung 56: Anzeige nach dem erfolgreichen Durchführen eines Firmware-Updates bei BCS Geräten

Während der Installation werden Ihnen die Statusmeldungen gemäß Abbildung 60, Abbildung 61, Abbildung 63 und Abbildung 64 dargestellt. Nach einer erfolgreichen Installation einer neuen Firmware wird Ihnen dies im Display des Chipkartenterminals angezeigt (siehe Abbildung 56). Diese Statusanzeige bleibt wenige Sekunden sichtbar; danach startet sich das Gerät neu. Sie können nun die Versionsnummer der neu installierten Firmware in der unteren Statusleiste des Displays ablesen.

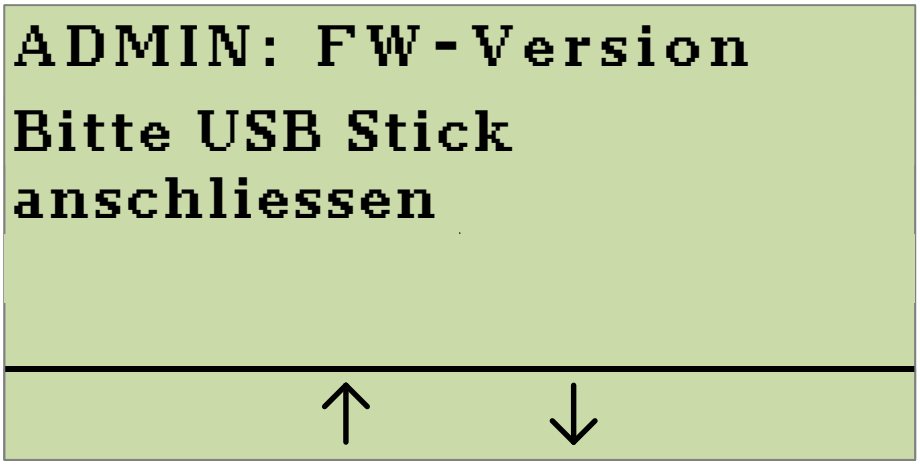
4.12.2.2 Updatevorgang für ein SICCT-Terminal eHealth GT900

Es handelt sich bei der Update-Datei um eine Datei im Format *.bin. Kopieren Sie die Datei auf einen handelsüblichen USB-Stick (nicht im Lieferumfang enthalten, FAT32 formatiert, höchstens 8GB Kapazität). 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 Abschnitt 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 57).



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

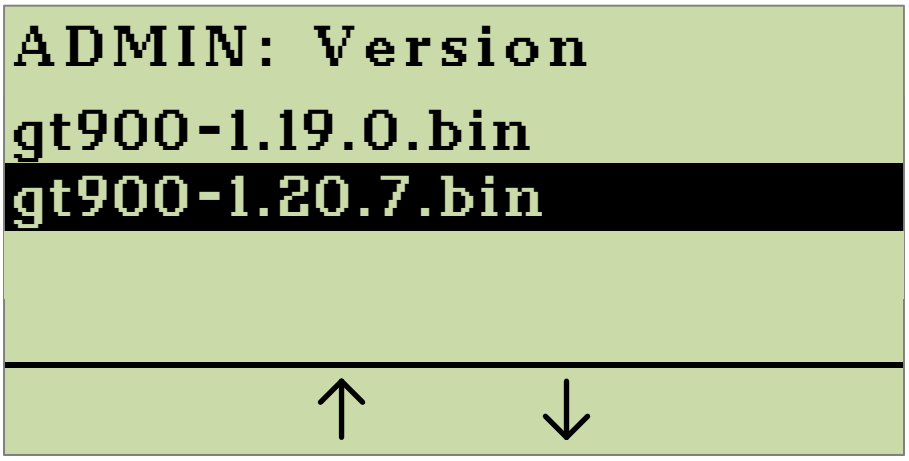
Abbildung 57: Submenü Admin:Version Firmware Update



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

Abbildung 58: Gerät ist bereit für Firmware Update

Stecken Sie den zuvor präparierten USB-Stick in die USB-Typ-A-Buchse Ihres Chipkartenterminals. In Abbildung 6 (Geräteanschlussbelegung) ist dieser Anschluss mit Position ① gekennzeichnet. Machen Sie sich gegebenenfalls nochmals mit den Anschlüssen des Chipkartenterminals vertraut (s. Abschnitt 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.

Abbildung 59: 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 59). Diese wird nun in den Speicher des Gerätes kopiert (Abbildung 60).

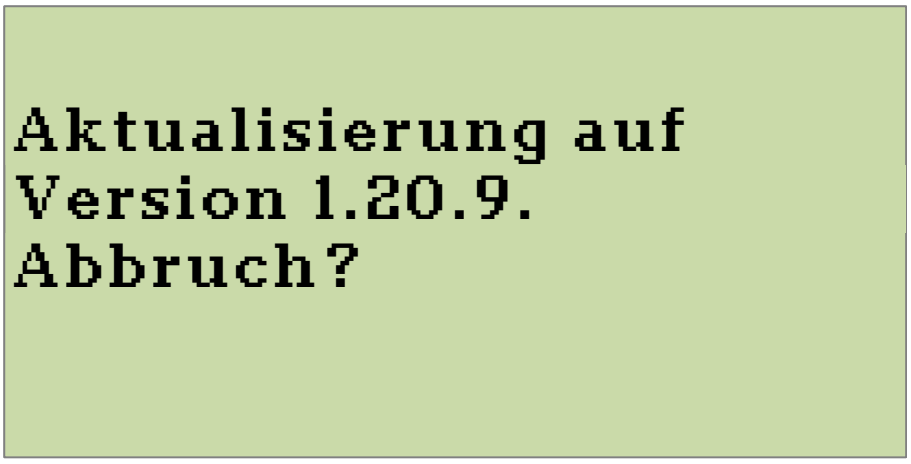
Die zuvor ausgewählte Firmwaredatei wird nun in den Speicher des Gerätes kopiert.

Abbildung 60: Die Firmwaredatei wird in den Speicher kopiert.

Nach dem Kopiervorgang wird die Firmwaredatei einer Prüfung unterzogen.

Abbildung 61: Überprüfen des Firmware Updates

Die sich nun im Speicher befindende Firmwaredatei wird, wie in Abbildung 61 dargestellt, einer Prüfung unterzogen. Wurde eine korrekt signierte Firmware gefunden, wird Ihnen die zu installierende Firmware-Version in einer Displaymeldung angezeigt.



Im Display wird die Versions-nummer der zu installierenden Firmware angezeigt.

Abbildung 62: Anzeige der zu installierenden Firmware-Version

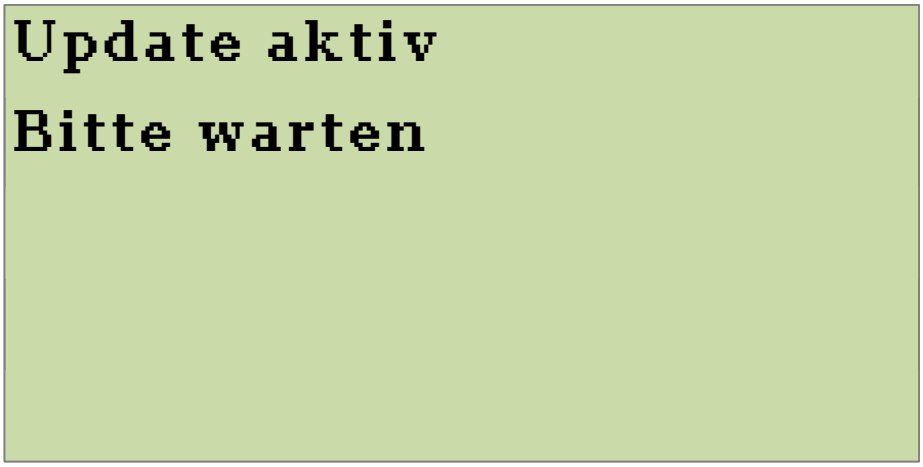
Überzeugen Sie sich, ob Sie die Firmware mit der angezeigten Versionsnummer installieren wollen. Sie können den Vorgang innerhalb von 10 Sekunden durch Drücken der -Taste abbrechen. Wenn Sie den Vorgang abbrechen, startet das Terminal ohne Aktualisierung der Firmware neu. Wenn Sie den Vorgang nicht abbrechen, 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 Abschnitt 4.12.3 „Durchführung eines Firmware-Downgrade“. Die Versionsnummer der derzeit installierten Firmware wird Ihnen auf dem Display des einsatzbereiten Gerätes angezeigt (siehe Abbildung 20), 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 startet nach einer kurzen Statusanzeige („Verifikation Fehlgeschlagen“) neu. Daraufhin können Sie wie gewohnt mit der alten Firmware weiterarbeiten.

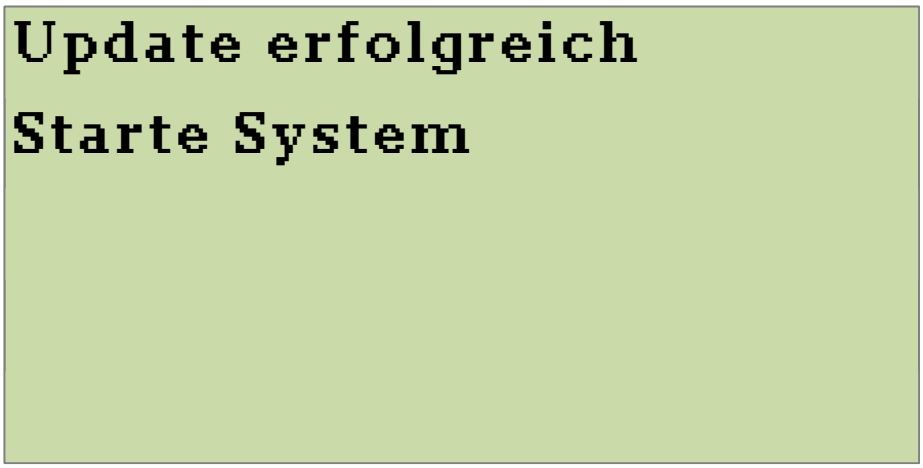
Wurde eine korrekt signierte Firmwaredatei eingespielt, erfolgt eine Mitteilung über den Beginn des Updateprozesses (siehe Abbildung 63). Anschließend wird für die Dauer des Updates eine Mitteilung im Display angezeigt, wie sie in Abbildung 64 zu sehen ist.

Abbildung 63: Der Updateprozess wird gestartet.



Während des Updatevorganges wird Ihnen diese Mitteilung angezeigt.

Abbildung 64: Das Update wird durchgeführt.



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

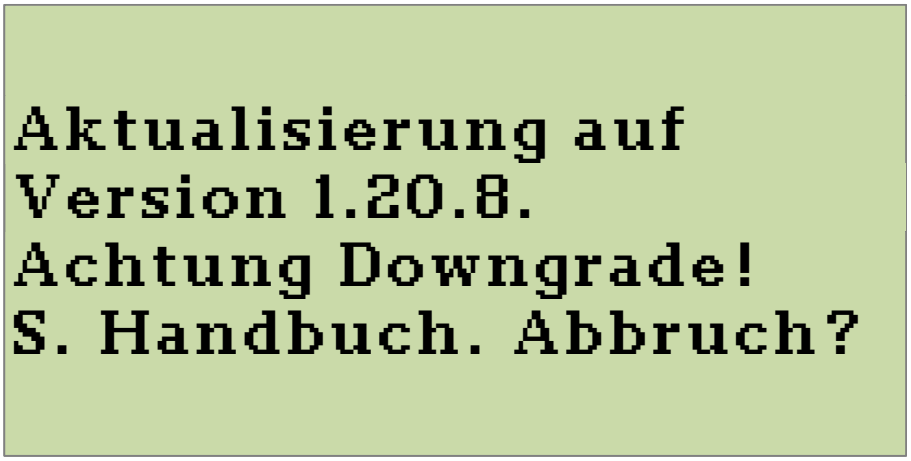
Abbildung 65: Anzeige nach erfolgreichem Firmware-Update

Nach der erfolgreichen Installation wird Ihnen dies im Display des Chipkartenterminals angezeigt (siehe Abbildung 65). 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.

4.12.3 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 Abschnitt 4.12.2 „Durchführung eines Firmware-Updates“ beschrieben. Während der Überprüfung der Firmware kann Ihnen jedoch der folgende Hinweis angezeigt werden:



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

Abbildung 66: Abfrage zur Fortführung des Downgrades

Durch Drücken der  -Taste können Sie das Einspielen des niedrigeren Firmwarestands auch abbrechen. Daraufhin wird das Gerät neu gestartet und Sie können wie gewohnt mit der alten Firmware weiterarbeiten.

4.12.4 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 67).

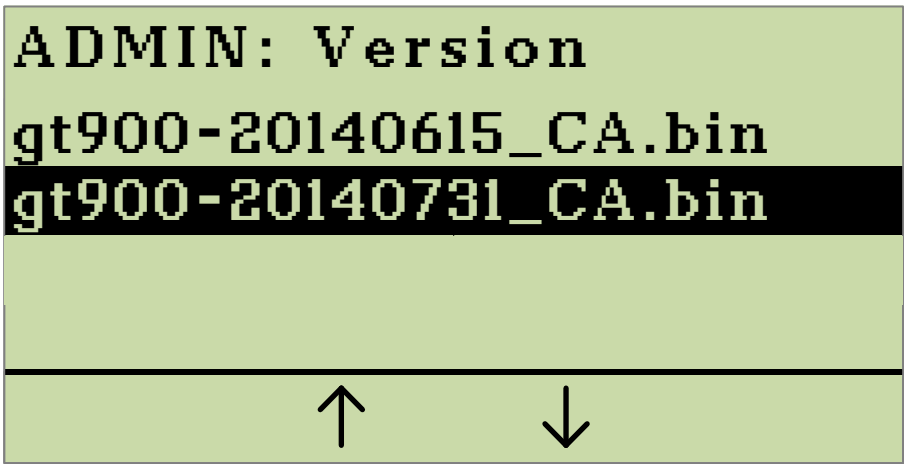
4.12.5 Update der CA-Liste

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 Chipkartenlesegerät an. Lesen Sie hierzu ggf. den Abschnitt 4.12.2 „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 68). 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 schaltet sich nach einer kurzen Statusanzeige („Verifikation Fehlgeschlagen“) aus. Daraufhin können Sie das Gerät neu starten und wie gewohnt mit den alten Zertifikatdateien weiterarbeiten.

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

Abbildung 67: Anzeige des Submenüs "Version“; CA Update

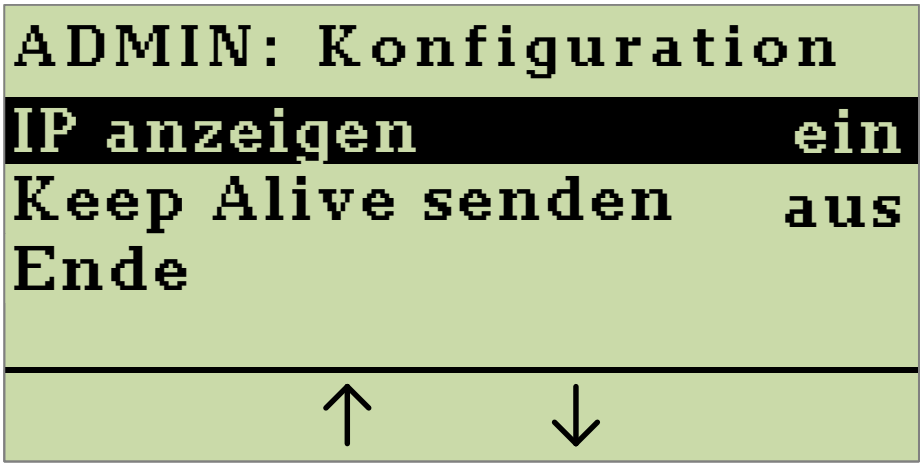


Wählen Sie eine Datei aus und drücken Sie die ✓-Taste, um die Zertifikatdatei zu installieren.

Abbildung 68: Wählen Sie die zu installierende Zertifikatdatei aus.

4.13 Aktuelle IP-Adresse anzeigen

Sie können sich in der Hauptdisplayanzeige (Abbildung 20) wahlweise die aktuell vergebene IP-Adresse des Chipkartenterminals anzeigen lassen. 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.



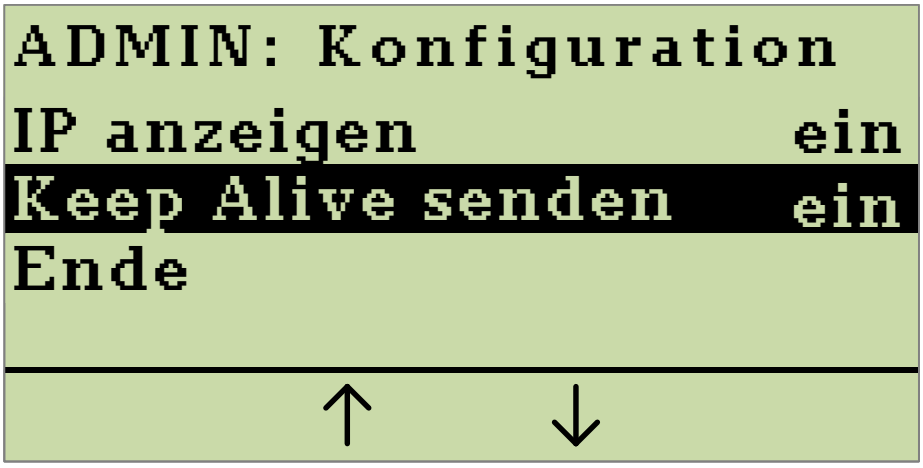
Drücken Sie die ✓-Taste, um die Anzeige der IP-Adresse ein- oder auszuschalten.

Abbildung 69: 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.

4.14 Keep Alive senden

Innerhalb einer Netzwerkstruktur kann es notwendig werden, dass das Chipkartenterminal einen sogenannten „Keep Alive“ sendet. Das „Keep Alive“-Signal wird gesendet, um zum einen eine Netzwerkverbindung zu erhalten und um desweiteren sicherzustellen, dass die Erreichbarkeit und Funktion eines Kommunikationspartners noch gegeben ist. Für Ihr Chipkartenterminal bedeutet dies, dass bei bestehender SICCT-Verbindung SICCT Keep Alive-Pakete gesendet werden. 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 70: 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.

5 Gerät zurücksetzen

Durch die Vergabe einer PUK während der Erstinbetriebnahme des Gerätes ist es möglich, das Chipkartenlesegerät in den Auslieferungszustand zu versetzen. Dies kann unter Umständen notwendig werden, wenn die Administrator PIN des Gerätes verloren gegangen ist. Sie können das Gerät auch über den Menüpunkt „Werksreset“ im Untermenü „Sicherheit“ des Administrator-Menüs zurücksetzen.

5.1 Zurücksetzen ohne Kenntnis der Admin PIN

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

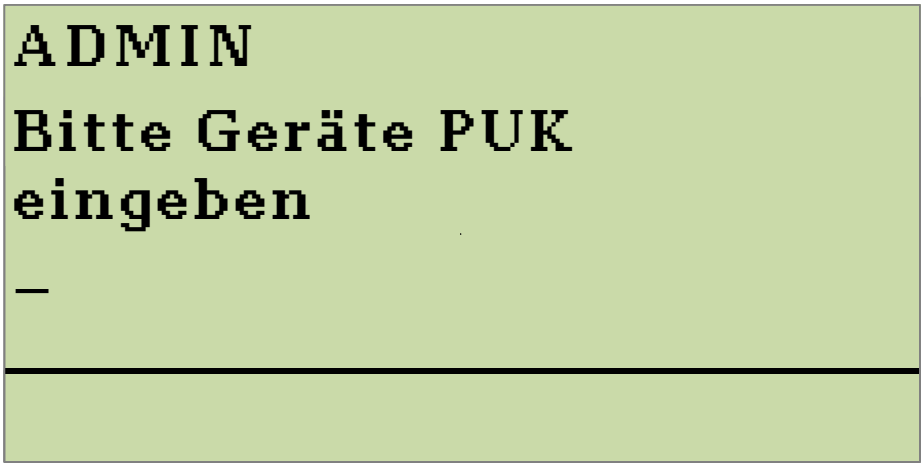
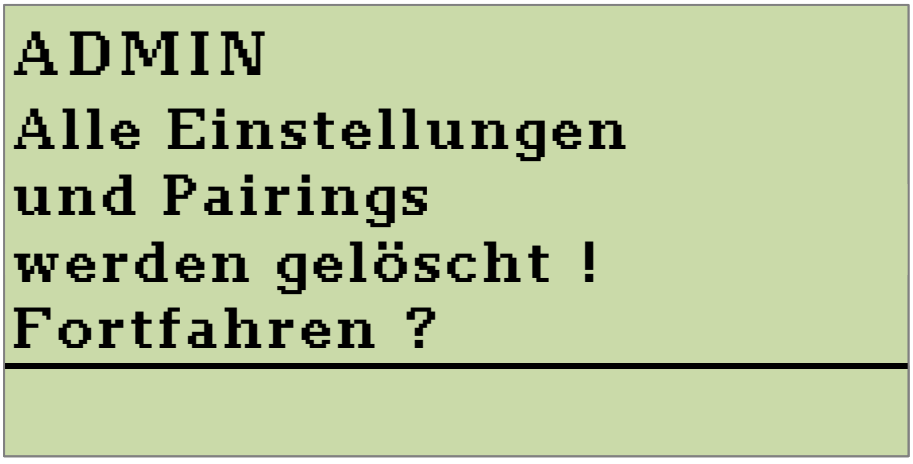


Abbildung 71: Eingabeaufforderung der PUK zum Zurücksetzen des Gerätes

Wenn Sie die PUK korrekt eingegeben haben, werden Sie gebeten, das Zurücksetzen des Gerätes in den Auslieferungszustand zu bestätigen, so wie es in Abbildung 72 dargestellt ist. Sie können diesen Dialog durch Drücken der ✓-Taste bestätigen oder durch Betätigen der ✗-Taste abbrechen.



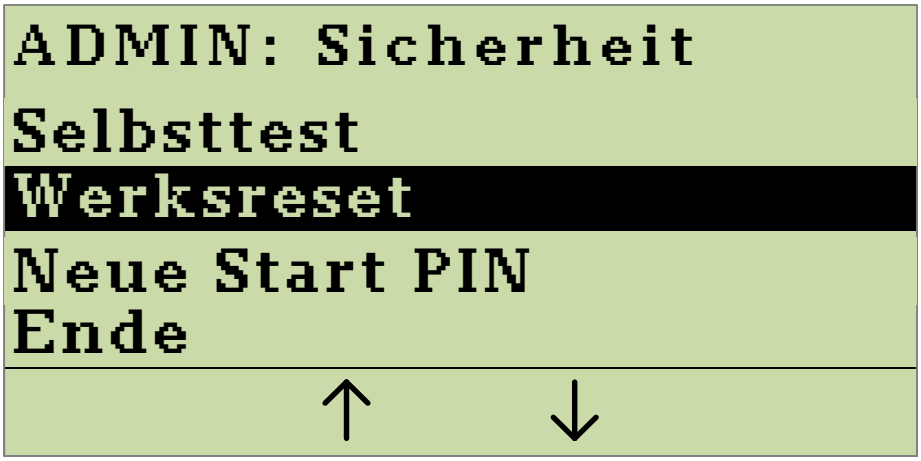
Sicherheitsabfrage beim Zurücksetzen des Gerätes in den Auslieferungs-zustand.

Abbildung 72: Sicherheitsabfrage

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

5.2 Zurücksetzen mit Kenntnis der Admin PIN

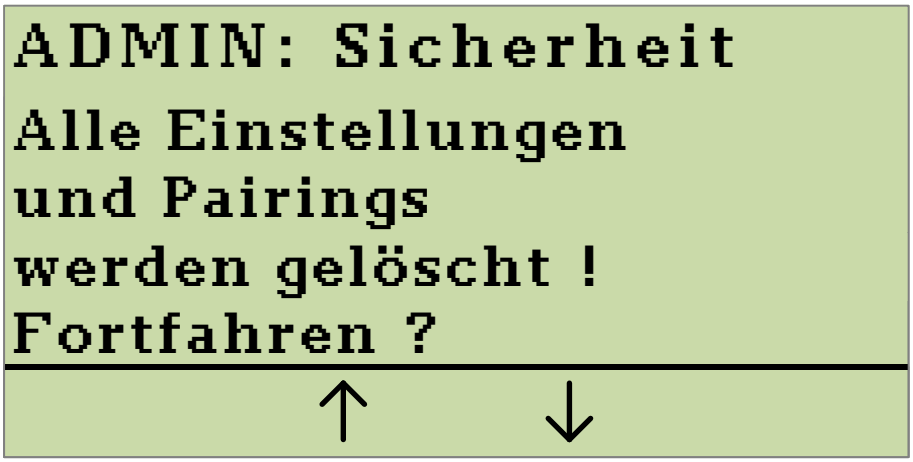
Über den Menüpunkt **Werksreset** im Untermenü „Sicherheit“ im Administrator-Menü können sie Ihr Chipkartenlesegerät ebenfalls in den Auslieferungszustand zurücksetzen. Um das Gerät in den Auslieferungszustand zu versetzen, wählen Sie in dem Admin-Menü die Option **Sicherheit** und bestätigen dies mit der ✓-Taste. Auf dem Display wird Ihnen das Submenü **ADMIN: Sicherheit** angezeigt.



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

Abbildung 73: Anzeige des Submenüs "Sicherheit"

Wählen Sie die Option **Werksreset** und wählen Sie diesen Menüpunkt durch Drücken der ✓-Taste aus. In einem 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 74: Sicherheitsabfrage

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

6 Weboberfläche nutzen

Ihr Chipkartenterminal 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 Chipkartenterminal eingelegt wurde, da das Zertifikat für den gesicherten Verbindungsaufbau von der gSMC-KT zur Verfügung gestellt wird.

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

Wie Sie diese Weboberfläche zur Benutzung freischalten, erfahren Sie in Abschnitt 4.8 „Web Admin Schnittstelle ein- oder ausschalten“.

Um auf die Weboberfläche zugreifen zu können, benötigen Sie einen Computer mit installiertem Webbrowser. Zudem muss sich das Chipkartenlesegerät im selben Netzwerk befinden, wie der Computer, von dem Sie auf das Chipkartenlesegerät zugreifen möchten. Geben Sie in die Adresszeile des Webbrowsers die IP-Adresse des Chipkartenlesegerätes ein. Wie Sie sich die IP-Adresse im Display des Terminals anzeigen lassen können, entnehmen Sie ggf. dem Abschnitt 4.13 „Aktuelle IP-Adresse anzeigen“. Bitte beachten Sie, dass Ihr Webbrowser zum erfolgreichen Verbindungsaufbau die Transportschichtsicherheit TLS 1.1 oder TLS 1.2 unterstützen muss. Ein erfolgreicher Verbindungsaufbau wurde mit den folgenden Webbrowsern getestet:

- Google Chrome [Version 38.0.2125.104 m]
- Firefox [Version 33.0.1]

Geben Sie Folgendes in die Adresszeile Ihres Webbrowsers ein:

https://[IP-Adresse des Chipkartenterminals]

Abbildung 76 zeigt die Darstellung der Weboberfläche in einem Browsertab des Google-Chrome Browsers.

Bitte beachten Sie, dass es beim erstmaligen Aufbau der Verbindung zu einem Zertifikatfehler kommen kann. Dies ist der Tatsache geschuldet, dass das Chipkartenterminal zur Kommunikationsabsicherung (TLS 1.1 oder 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 Manipulationen an den gSMC-KT vorgenommen wurden und die SIM-Slotversiegelung intakt ist. Sie können die Zertifikatwarnung nun in den meisten Browsern manuell übergehen und dennoch einen Verbindungsaufbau einleiten. Ein entsprechender Dialog ist in Abbildung 75 beispielhaft für den Google-Chrome Browser dargestellt. Fügen Sie eine entsprechende Ausnahmeregel hinzu, um mit der Konfiguration über die Weboberfläche fortzufahren. Im gezeigten Beispiel klicken Sie hierzu auf „Weiter zu 192.168.178.29 (unsicher)“.

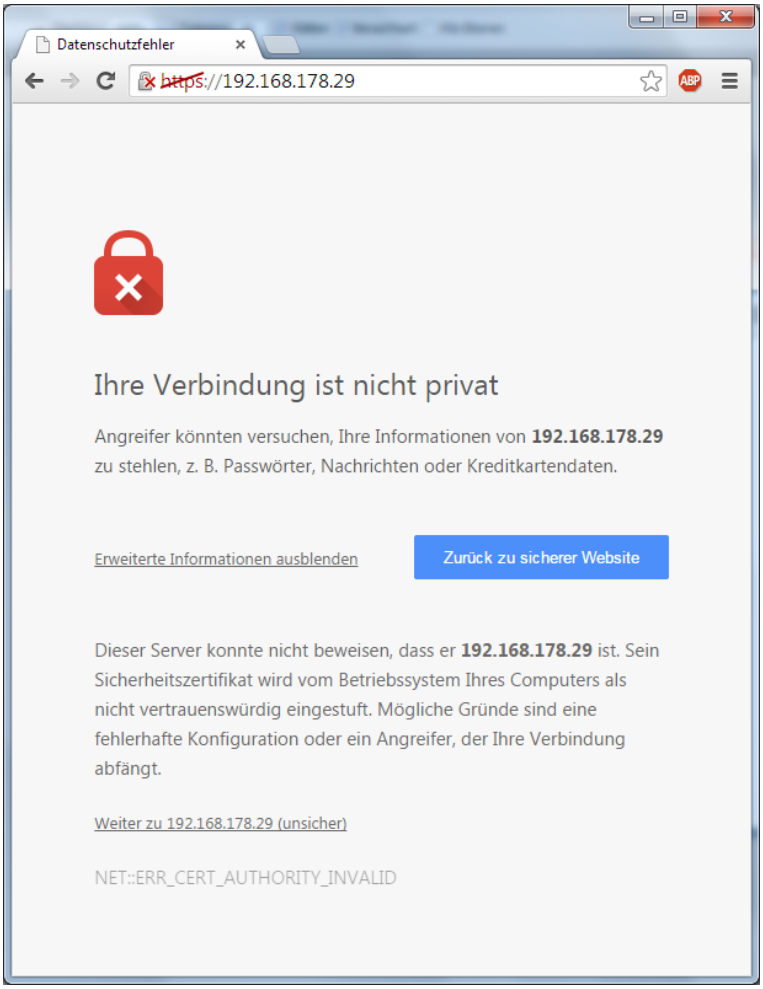


Abbildung 75: Mögliche Anzeige eines Zertifikatfehlers im Browser.

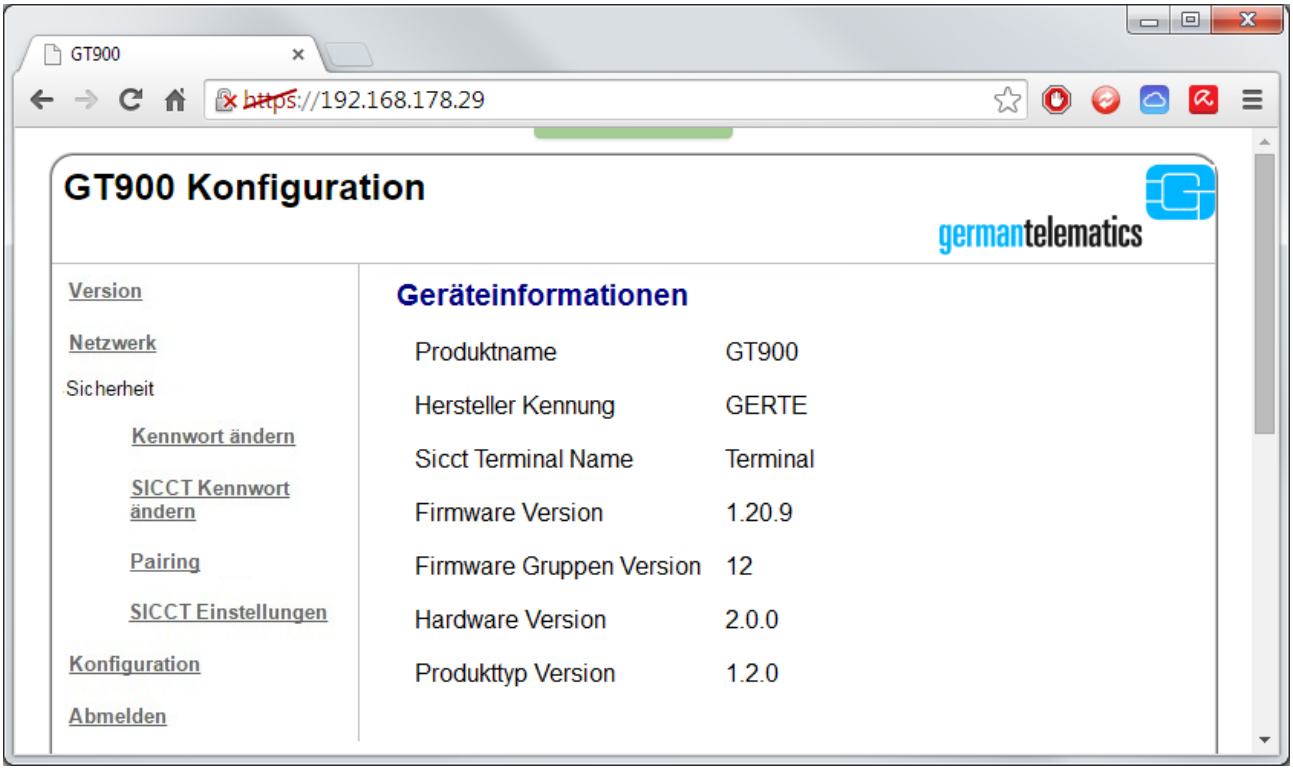


Abbildung 76: Weboberfläche des Chipkartenterminals nach dem Verbindungsaufbau.

Die Weboberfläche bietet Ihnen nach Eingabe Ihrer Web-Admin PIN (siehe Abbildung 77) 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 Web-Admin Kennwortes (PIN),
- die Änderung des SICCT Kennwortes (PIN),
- das Anzeigen und Löschen möglicherweise vorhandener Pairings,
- das Vornehmen von SICCT Einstellungen,
- sowie das Ändern von Gerätekonfigurationen.

Geben Sie beim ersten Anmeldevorgang an der Weboberfläche die am Chipkartenterminal vergebene Web-Admin PIN ein (siehe Abschnitt 4.8).

Abbildung 77: Eingabe der Web-Admin PIN zur Freigabe der Weboberfläche

6.1 Netzwerkeinstellungen vornehmen

Um in der Weboberfläche Einstellungen an den Netzwerkparametern vornehmen zu können, müssen Sie zunächst Ihre Web-Admin PIN eingeben und anschließend auf den „Senden“-Button drücken. Ihnen werden nun die bereits bekannten Einstellungen für die Netzwerkparameter des Chipkartenlesegerätes angezeigt.

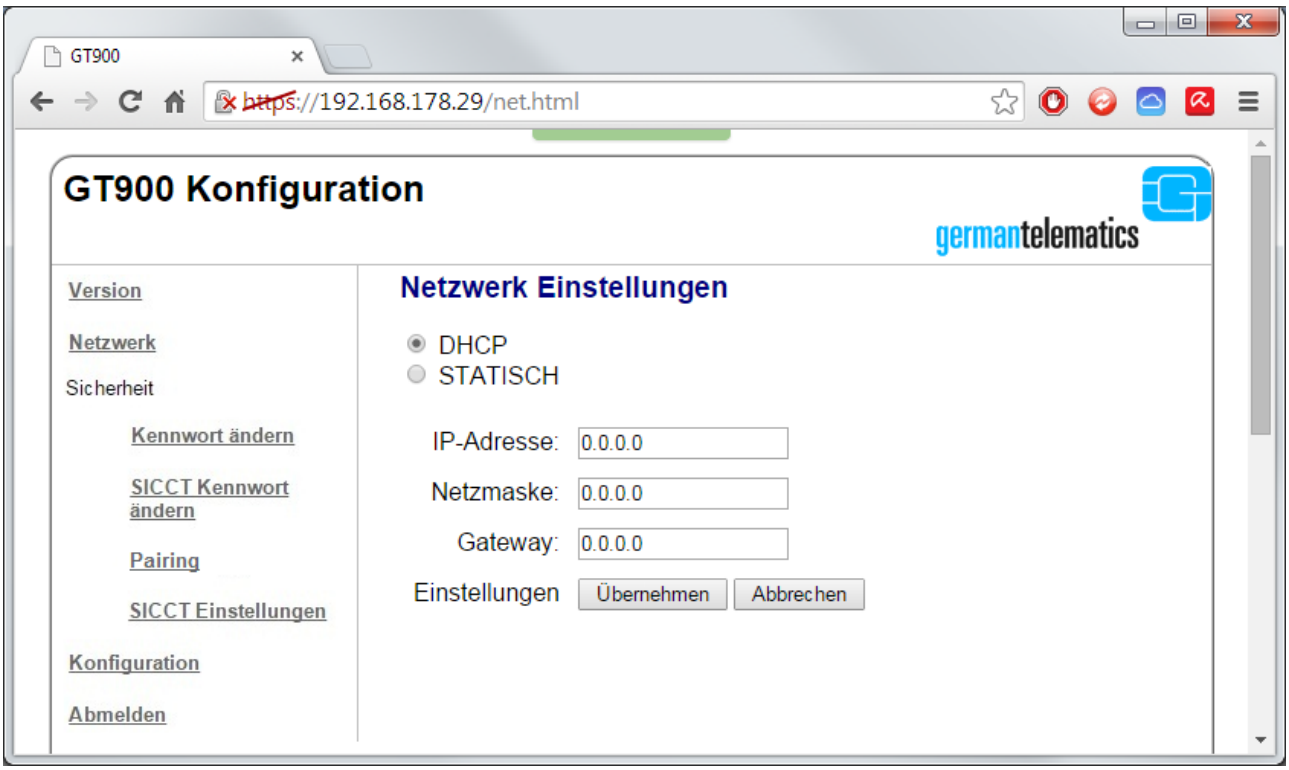


Abbildung 78: Netzwerkonfiguration über die Weboberfläche

6.2 Kennwort der Web-Admin Schnittstelle ändern

Über die Weboberfläche können Sie auch ein neues Kennwort für die Web-Admin Schnittstelle vergeben. Sie sind an dieser Stelle nicht nur auf die Zahlentasten Ihres Chipkartenterminals beschränkt und können daher auch Kennwörter anstelle der sonst üblichen PIN vergeben.

Auch das Kennwort muss aus mindestens 8 Zeichen bestehen, kann nun aber 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 79: Setzen einer neuen Kennwortes für die Web-Admin Schnittstelle

Hinweise zum Umgang mit den Kennwörtern der Web-Admin 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 Kennwörter**. **Vermeiden Sie es, die Kennwörter in der Nähe des Gerätes aufzubewahren.** Das Web-Admin 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 Web-Admin Schnittstelle vergeben, aus mind. 8 Zeichen bestehen muss. Zudem muss mindestens eine Zahl in Ihrem Kennwort enthalten sein.

6.3 SICCT Kennwort ändern

Über die Weboberfläche können Sie auch ein neues SICCT Kennwort vergeben. Sie sind an dieser Stelle nicht nur auf die Zahlentasten Ihres Chipkartenterminals beschränkt und können daher auch Kennwörter anstelle der sonst üblichen SICCT PIN vergeben.

Das SICCT Kennwort muss aus 8 bis 12 Zeichen (A-Z, a-z, 0-9, ()-+=:‘,./? und Leerzeichen) bestehen, kann nun aber 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.

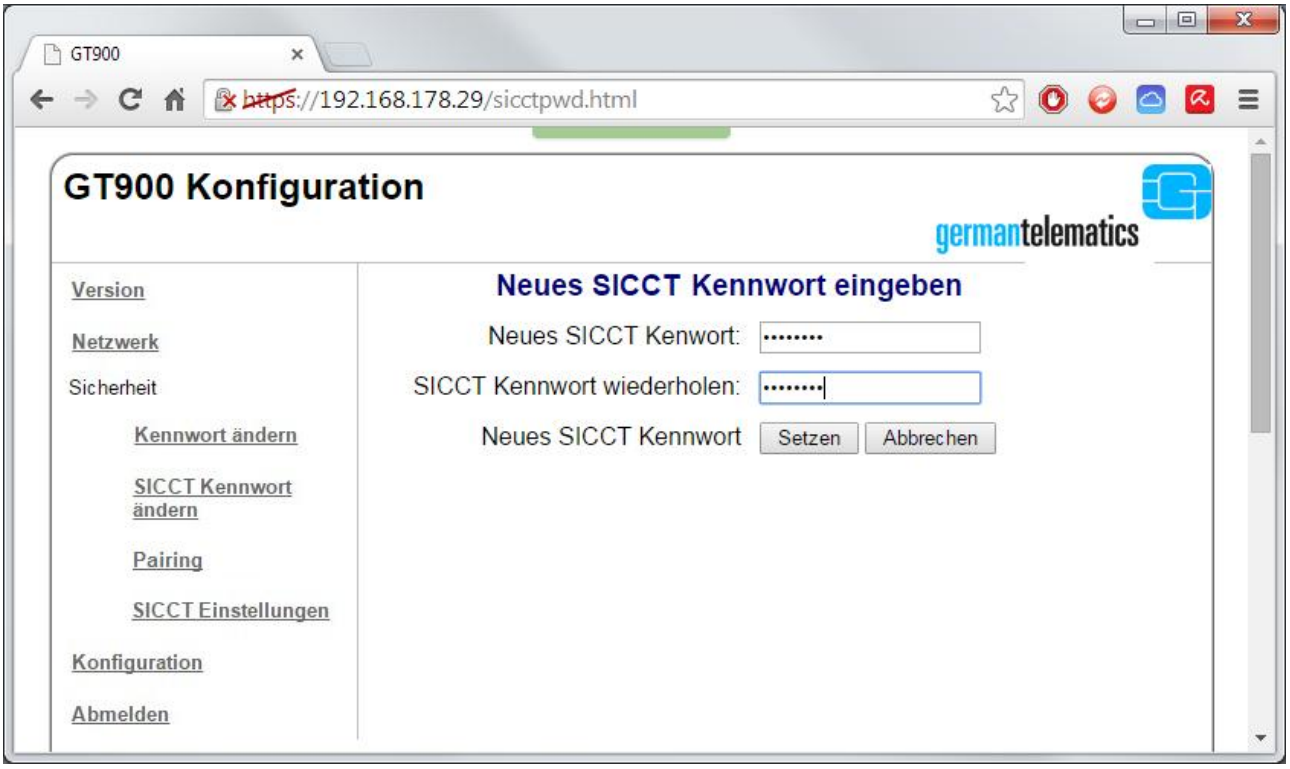


Abbildung 80: Setzen eines neuen SICCT Kennwortes

6.4 Pairings einsehen und löschen

Über die Weboberfläche können Sie die Pairings Ihres Chipkartenterminals einsehen und ggf. einzelne Pairings löschen. Ihnen wird auch die Option „Alle Pairings löschen“ zur Verfügung gestellt.

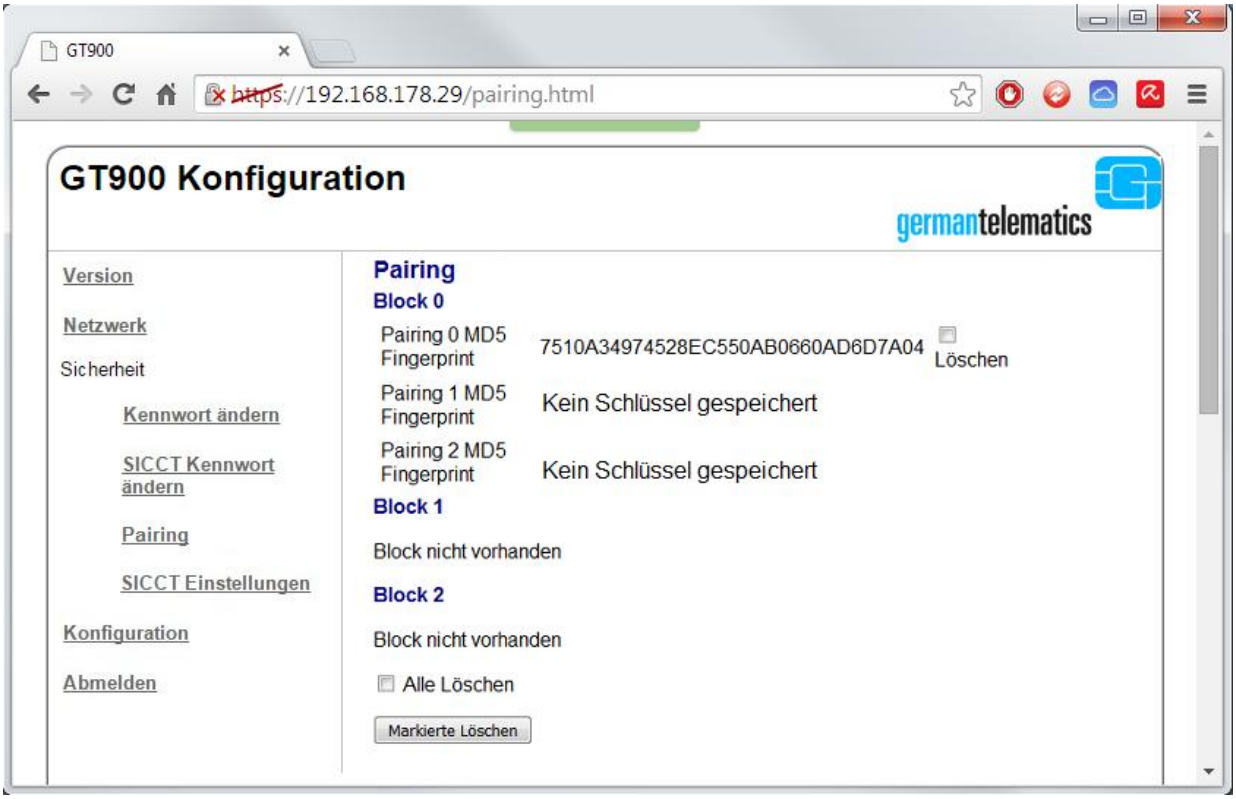


Abbildung 81: Einsehen der Pairings des Chipkartenterminals

6.5 SICCT Einstellungen

Im Menüpunkt SICCT-Einstellungen können Sie den Namen Ihres Chipkartenterminals festlegen. Mit einem eindeutigen Namen lässt sich Ihr Chipkartenterminal einfacher in einer größeren SICCT-konformen Infrastruktur identifizieren. Der Terminalname kann maximal aus 32 Zeichen (A-Z, a-z, 0-9, ()-+=:‘,./? und Leerzeichen) bestehen.

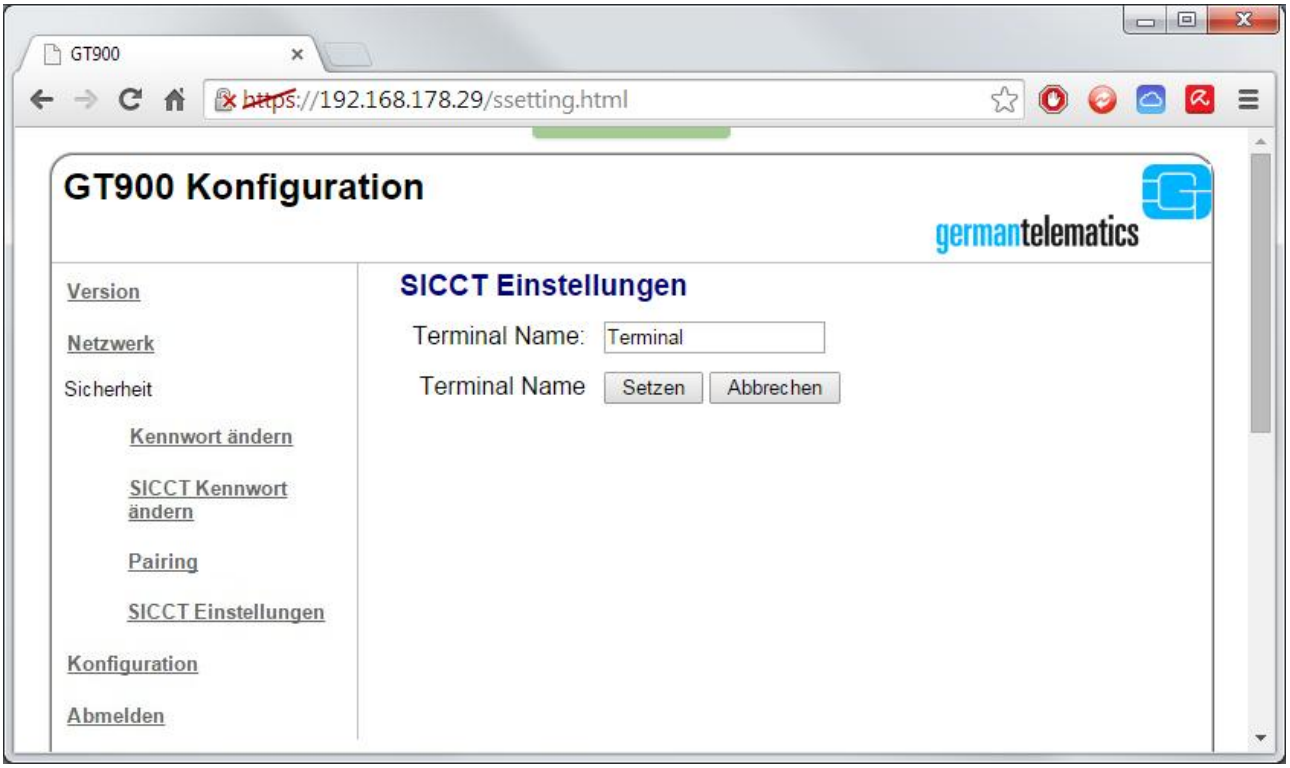


Abbildung 82: SICCT Einstellungen vornehmen

6.6 Konfigurationen

Innerhalb einer Netzwerkstruktur kann es notwendig werden, dass das Chipkartenterminal einen sogenannten „Keep Alive“ sendet. Das „Keep Alive“-Signal wird gesendet, um zum Einen eine Netzwerkverbindung zu erhalten und um des Weiteren sicherzustellen, dass die Erreichbarkeit und Funktion eines Kommunikationspartners noch gegeben ist. Für Ihr Chipkartenterminal bedeutet dies, dass bei bestehender SICCT-Verbindung SICCT Keep Alive-Pakete gesendet werden. Um die Keep Alive-Funktion zu nutzen, aktivieren Sie die entsprechende Checkbox.

Sie können sich in der Hauptdisplayanzeige (Abbildung 12) wahlweise die aktuell vergebene IP-Adresse des Chipkartenterminals anzeigen lassen. Um die IP-Adresse anzuzeigen, aktivieren Sie die entsprechende Checkbox. Klicken Sie anschließend auf „Übernehmen."

Abbildung 83: Gerätekonfigurationen vornehmen

7 Qualifizierte elektronische Signaturen

Qualifizierte elektronische Signaturen (QES) dürfen gemäß dem Signaturgesetz nur mit Komponenten erzeugt und geprüft werden, welche den Anforderungen, die ebenfalls im Signaturgesetz und in der Signaturverordnung festgelegt sind, genügen. Das Chipkartenlesegerät eHealth GT900 ist, abhängig von der installierten Firmware, in diesem Zusammenhang eine durch die Bundesnetzagentur veröffentlichte und somit bestätigte Teil-Signaturanwendungskomponente. Um qualifizierte elektronische Signaturen zu erzeugen, müssen Sie das Terminal in einem Verbund aus Signaturerstellungseinheit (Signaturkarte), Signaturanwendungskomponente (Signatur-Software bzw. Anwenderprogramm) und einem Hostsystem (Computer) betreiben.

Versichern Sie sich, dass die von Ihnen aktuell benutzte Firmware-Version als Signaturanwendungskomponente bestätigt wurde. Sie finden alle bestätigten Signaturanwendungskomponenten auf der Internetpräsenz der Bundesnetzagentur unter:

www.bundesnetzagentur.de

Auf den Internetseiten der Bundesnetzagentur werden Ihnen zudem umfangreiche Informationen zur qualifizierten elektronischen Signatur zur Verfügung gestellt. Eine Auflistung von sicherheitsbestätigten Signaturkarten findet sich ebenso auf der o. g. Internetpräsenz. Bitte informieren Sie sich auf den Seiten der Bundesnetzagentur über die bestätigten Komponenten und insbesondere über die Bestätigung Ihres Chipkartenlesegerätes eHealth GT900 als sogenannte Teil-Signaturanwendungs-komponente zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen.

Machen Sie sich bitte vor der Erzeugung und Prüfung einer qualifizierten elektronischen Signatur mit der Benutzung Ihres Chipkartenlesegerätes eHealth GT900 vertraut.

Lesen Sie hierzu insbesondere die Abschnitte:

- 1.3 „Sicherheitskonzept des Terminals“,
- 1.5 „Anschluss des Gerätes“
- 2.3 „Aufbau der Displayanzeige“
- 3.2 „Eingabe einer Karten-PIN“

Die Erzeugung und Prüfung einer qualifizierten elektronischen Signatur wird von der Signaturanwendungskomponente gesteuert. Auf Grund dessen kann an dieser Stelle auch keine allgemeingültige Anleitung zur Erzeugung und Prüfung einer QES gegeben werden. Das Chipkartenterminal unterstützt die Signaturanwendungskomponente (Signaturkarte) durch die Verifikation der Karten-PIN, d.h. durch die sichere PIN-Eingabe. Typischerweise sind diese angezeigten Informationen, Aufforderungen oder Warnungen zur PIN-Eingabe selbsterklärend und bedürfen keiner weiteren Erläuterung.

8 Produktregistrierung

Auf der hinteren Umschlagseite dieses Benutzerhandbuches befindet sich ein Registrierungsformular. Durch das Ausfüllen und Zurücksenden dieses Registrierungsformulars registrieren Sie Ihr Chipkartenterminal, um es mit Hilfe zukünftiger Produktupdates in der Telematikinfrastruktur uneingeschränkt zu verwenden. Füllen Sie hierzu bitte das Formular aus und schicken es unterschrieben und mit dem Praxisstempel versehen per Fax an die folgende Faxnummer:

: +49 (0)30 – 31805454

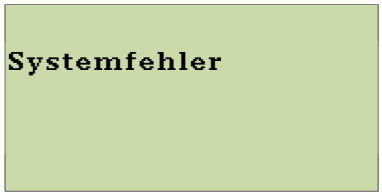
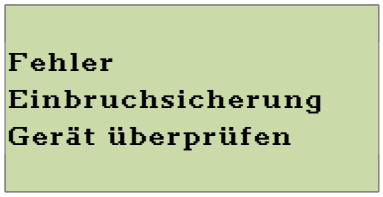
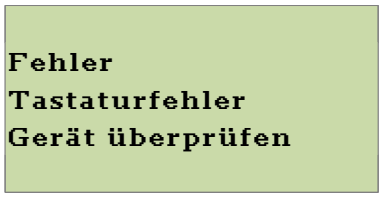
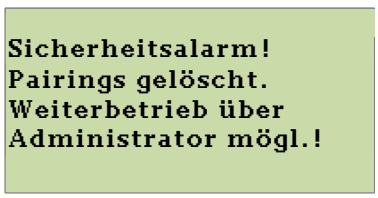
Für eine Registrierung per E-Mail scannen Sie die ausgefüllte Umschlagseite ein und schicken das eingescannte Bild im .jpg oder .pdf Format an die folgende

E-Mail-Adresse:

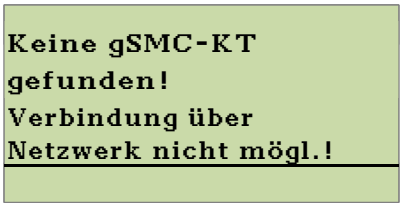
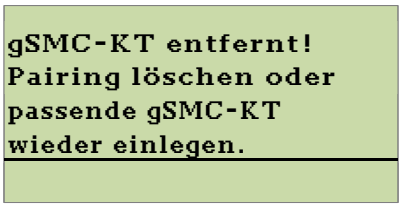
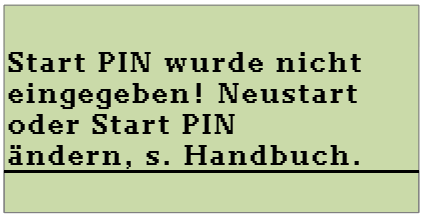
: registration@germantelematics.de

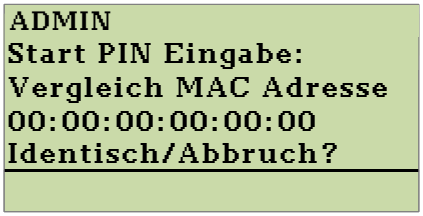
9 Problembehebung

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:   	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.
	Wurde ein möglicher Manipulationsversuch erkannt, kann nach einem Neustart das Terminal unter Umständen weiterbetrieben werden.	Der Administrator kann die Fehlermeldung mit der ✓ -Taste bestätigen (wird die Meldung schon länger angezeigt, führt das Terminal nochmal einen Neustart aus) und wird dann nach seiner Admin PIN gefragt. Vor der Eingabe muss sich der Admin unbedingt von der Unversehrtheit des Terminals überzeugen. Der sichere Betrieb des Terminals liegt einzig und allein in der Verantwortung des Administrators. Im Zweifel ist das Terminal auszutauschen. Nach der Eingabe der Admin PIN kommt die Aufforderung, die Start PIN einzugeben. Danach muss das Terminal neu initial gepairt werden und kann dann wieder benutzt werden.

Fehlerbeschreibung	Ursache	Behebung
Das Gerät lässt sich nicht in den Administrator-Modus schalten.	Sie haben die Administrator 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 Abschnitt 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 folgende Fehlermeldung: **Verifikation fehlgeschlagen!**	Die Firmware, die Sie zu installieren versuchen, ist beschädigt.	Laden Sie die entsprechende FW-Datei erneut von der Herstellerseite.
Das Firmware-Update wird abgebrochen. Es erscheint folgende Statusanzeige: **Falsche Version**	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 FW-Version wechseln, so kontaktieren Sie bitte Ihren Lieferanten oder einen zertifizierten Techniker für weitere Unterstützung.
Es erscheint folgende Fehlermeldung: **Fehler** **Sim nicht gesteckt**	Eine der SIM-Karten aus den am Gerät rechtsseitigen SIM-Slots wurde während des Betriebs 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 neu, indem Sie es für einige Sekunden vom Strom trennen. Sie benötigen dann die Start PIN. Sollten weiterhin Probleme auftauchen, so kontaktieren Sie einen zertifizierten Techniker oder den Hersteller. Geben Sie die Fehlerbeschreibung an und erbitten Sie weitere Hilfe.

Fehlerbeschreibung	Ursache	Behebung
Es erscheint folgende Fehlermeldung: 	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 Chipkartenlesegerätes ein. Lesen Sie hierzu auch Abschnitt 2.2.3 „SIM-Slots“. Wahlweise können Sie auch in das Admin-Menü wechseln, um z.B. Netzwerkeinstellungen vorzunehmen.
Es erscheint folgende Fehlermeldung: 	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 Abschnitt 4.4. Durch Drücken der ✗ -Taste schalten Sie das Gerät aus.
Es erscheint folgende Fehlermeldung: 	Sie haben beim Terminalstart nach einem stromlosen Zustand innerhalb von 2 Minuten keine Start PIN eingegeben oder die Start PIN Eingabe mit der ✗ -Taste abgebrochen.	Wenn Ihnen die Start PIN bekannt ist, schalten Sie das Terminal mit der ✗ -Taste aus und danach mit der ✓ -Taste wieder ein. Geben Sie dann die Start PIN ein. Ist Ihnen die Start PIN nicht bekannt, öffnen Sie mit der F1 -Taste das Admin-Menü und generieren Sie wie in Kapitel 4.11 „Neue Start PIN vergeben“ beschrieben eine neue Start PIN.
Es erscheint folgende Fehlermeldung: 	Sie haben bei der Erstinbetriebnahme das Setzen der Start PIN nicht bestätigt.	Führen Sie einen Werksreset gemäß Abschnitt 5 „Gerät zurücksetzen“ aus und nehmen Sie die Erstinbetriebnahme erneut vor. Sobald Ihnen die Start PIN angezeigt wird, notieren Sie diese und bestätigen Sie mit der ✓ -Taste.

Fehlerbeschreibung	Ursache	Behebung
Es erscheint folgende Meldung: 	Die Netzwerkeinstellungen des Terminals sind auf DHCP konfiguriert und es befindet sich kein DHCP Server im Netzwerk.	Aktivieren Sie den DHCP Server im Netzwerk oder stellen Sie am Terminal eine feste IP-Adresse ein.

10 Kontakt

gt german telematics gesellschaft für telematikdienste mbH

Rankestraße 26

10789 Berlin

Fax.: +49 (0)30 – 31805454

E-Mail: service@germantelematics.de

Internetpräsenz: www.germantelematics.de

Unter www.germantelematics.de finden Sie nach der erfolgreichen Registrierung auf unserer Plattform auch die jeweils aktuelle Version dieses eHealth GT900-Benutzerhandbuches sowie die aktuelle Firmware.

11 Außerbetriebnahme und Versand

Bei Außerbetriebnahme des Gerätes stellen Sie sicher, dass sich keine SMC-Karten mehr in den SIM-Slots befinden und dass alle Pairings gelöscht sind. Die Pairings können Sie im Administrator Menü oder mittels eines Werksresets löschen.

Sollten Sie das Gerät versenden, z.B. zu Wartungs- oder Reparaturzwecken, so stellen Sie bitte auch in diesem Fall sicher, dass die Pairings gelöscht sind. Entnehmen Sie zudem die SMC Karten aus dem Gerät und verwahren Sie diese sicher und vor unbefugtem Zugriff geschützt.

12 Geräteentsorgung

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.

gematik

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Zulassungsurkunde

Die gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH hat der

gt german telematics GmbH

Rankestraße 26
10789 Berlin
Deutschland

mit Bescheid vom . .

für das

PLATZHALTER FÜR ZERTIFIKAT

die Zulassung für den Einsatz in der Telematikinfrastruktur erteilt.

Zulassungsnummer: gematik_ _ _ 1
Berlin, . .

Geschäftsführer Geschäftsführer

gematik - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
Friedrichstraße 136 10117 Berlin Telefon: 030-400 41 -0 Fax: 030-400 41-111
info@gematik.de www.gematik.de

Declaration of Conformity

Supplier's Name:	GT German Telematics Gesellschaft für Telematikdienste mbH
Supplier's Address:	Rankestraße 26 10789 Berlin

Declares, that the product

Product Name:	e-Health GT900
Regulatory Model:	e-Health GT900

The product herewith conforms to the following Council Directives:

EMC Directive 2004/108/EC,

International Standard (s) to which Conformity is Declared

Emissions:	EN 55 022: 05.2008
Immunity:	EN 55 024: 10.2003
Basic Standards:	EN 61000-4-2:2001 EN 61000-4-3:2006 EN 61000-4-4:2005 EN 61000-4-5:2007 EN 61000-4-6:2008 EN 61000-4-7:2004 EN 61000-4-8:2001 EN 61000-4-11:2005
Environment: RoHS,	Restriction of Substances in Electrical & Electronic Equipment Directive (2002/95/EC).

Additional Information

The product herewith carries the CE, RoHS logos/marking.

Sandeep S. Jolly (CEO)

Date: 7th Apr, 2009

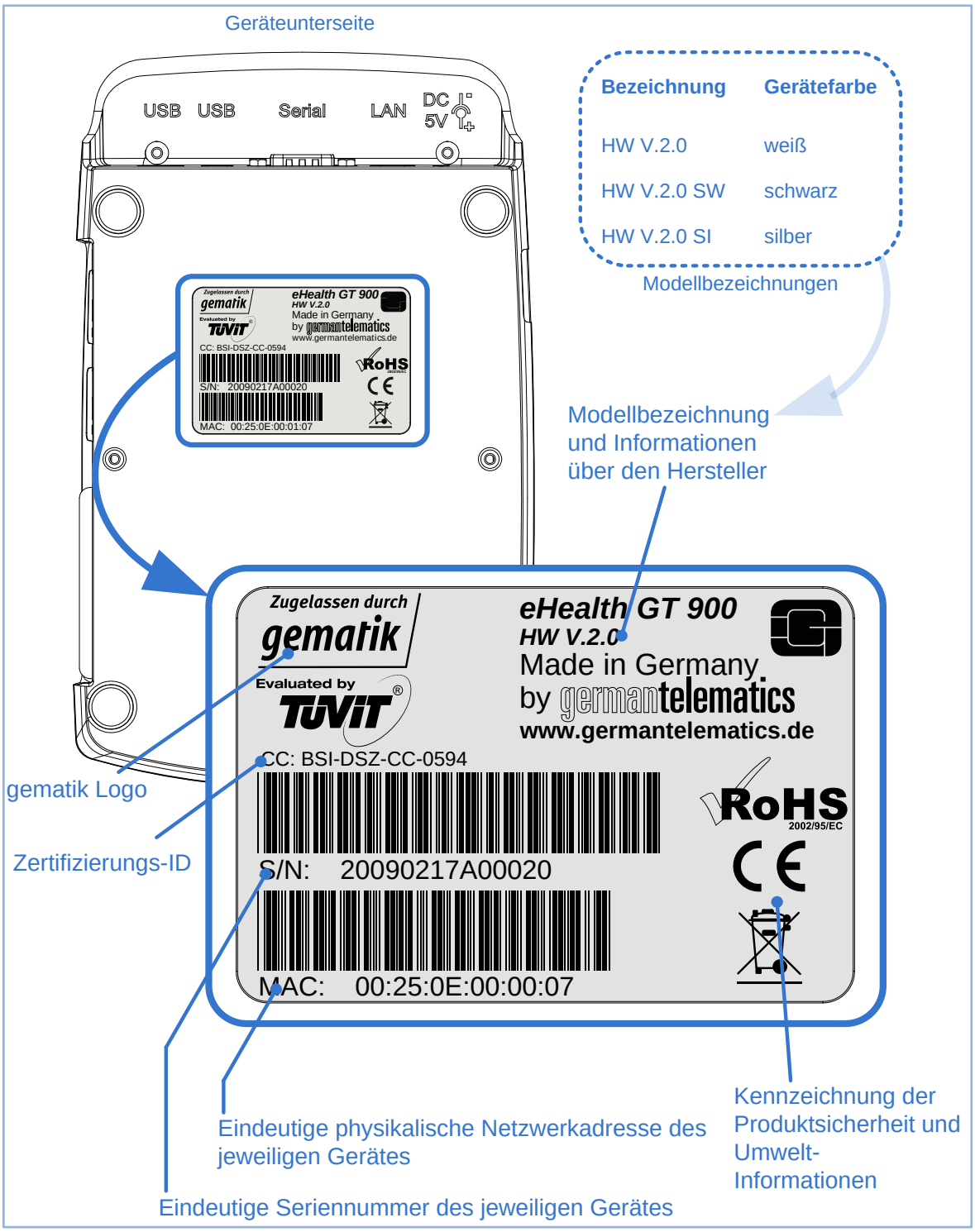


Abbildung 84: Geräteunterseite

FAX und E-Mail Registrierung

Zur Registrierung Ihres eHealth GT900-Terminals per FAX füllen Sie bitte die folgenden Felder aus, trennen das Blatt gegebenenfalls vorsichtig ab und senden es an die FAX-Nr.: 030 31805454.

Um sich per E-Mail zu registrieren, lesen Sie bitte den Abschnitt 8 „Produktregistrierung“ dieses Benutzerhandbuchs.

Ihre Anmeldedaten (bitte in Blockschrift ausfüllen):

Titel:
Name:
Vorname:
Praxis:
Straße.Nr.:
PLZ. Ort:
E-Mail:
Telefon:
Telefax:

Wenn vom Anwender abweichend, bitte ausfüllen!

Anmeldedaten des Administrators (bitte in Blockschrift ausfüllen):

Name:
Vorname
E-Mail:

☐ **Ich bin mit der Speicherung meiner Daten für Support- und Update-Zwecke einverstanden.**

☐ **Ja, ich möchte über Neuheiten und Aktualisierungen des GT900 Terminals informiert werden.**

Datenschutzerklärung :

Die German Telematics mbH sichert Ihnen die vertrauliche Behandlung der mitgeteilten Daten zu. Nach der elektronischen Erfassung der Daten bieten wir Ihnen einen sicheren und unkomplizierten Zugriff auf die produktbezogenen Service- und Supportseiten auf der Homepage der German Telematics mbH an. Geben Sie bei der Registrierung an, dass Sie produktspezifische Informationen der German Telematics mbH erhalten möchten, senden wir Ihnen diese von Zeit zu Zeit per E-Mail oder Fax zu. Nur die German Telematics mbH wird Ihnen solche E-Mails oder Faxe direkt senden. Informationen, die German Telematics mbH von den Benutzern zur Verfügung gestellt werden, werden von der German Telematics mbH weder an Dritte verkauft noch diesen gegenüber offen gelegt.

Platzhalter
Gerätelabel

Unterschrift / Praxisstempel