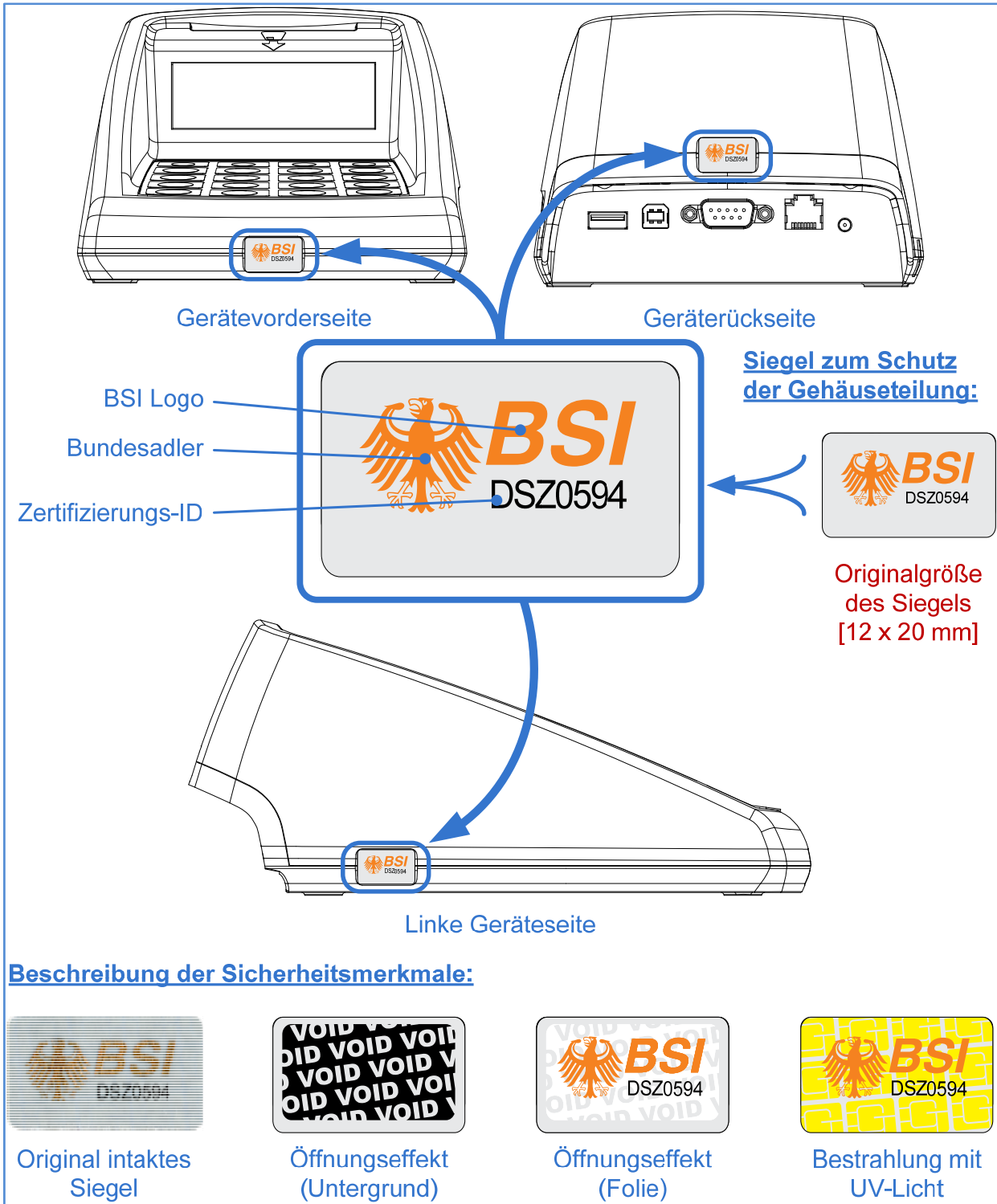


GT German Telematics GmbH

Kartenterminal eHealth GT900 – Benutzerhandbuch –

Version 2.0.9 / Deutsch





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

Das vorliegende Benutzerhandbuch gilt für alle Kartenterminals eHealth GT900 mit der Firmware-Version 1.22.1. Angaben zur Firmware-Version finden Sie über die Menüsteuerung des Terminals (siehe vorliegendes Handbuch Kapitel 4.13.1) sowie für die Hardware auf dem Typenschild an der Unterseite des Gerätes.

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

Benutzerhandbuch Identifikation:

Titel:

Kartenterminal
eHealth GT900
Benutzerhandbuch

Handbuchversion:

2.0.9

Ausgabedatum:

7.Mai 2020

Hersteller:

gt german telematics gesellschaft
für telematikdienste
Libellenstraße 9
14129 Berlin

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

Inhaltsverzeichnis

Rollenzuordnung	VII
1 Sicherheitshinweise und allgemeine Informationen	8
1.1 Sichere Lieferkette	11
1.2 Lieferumfang	13
1.3 Sicherheitskonzept des Terminals.....	14
1.3.1 Gehäuseprüfung.....	14
1.3.2 Siegelprüfung	15
1.3.3 Netzteilprüfung	16
1.3.4 Start PIN	17
1.4 Aufstellungshinweise	22
1.5 Anschluss des Gerätes.....	23
1.6 Inbetriebnahme des Kartenterminals	26
1.6.1 Setzen der Admin PIN.....	27
1.6.2 Setzen des PUK.....	29
1.6.3 Erzeugung einer Start PIN.....	30
1.6.4 Setzen der SICCT PIN	31
1.7 Ein- und Ausschalten des Kartenterminals.....	33
1.8 Reinigen und Desinfizieren des Gerätes.....	34
2 Bedienelemente	35
2.1 Tastatur	35
2.2 Kartenslots	37
2.2.1 Kontakteinheit 1: Einstecken einer eGK/KVK	38
2.2.2 Kontakteinheit 2: Einstecken eines HBA/SMC-B	39
2.2.3 SIM-Slots.....	40

2.3	Aufbau der Displayanzeige	44
3	Betrieb als eHealth Kartenterminal am Konnektor	47
3.1	Pairing	47
3.2	Eingabe einer Karten-PIN	49
4	Geräteeinstellungen	51
4.1	Admin-Menü	51
4.2	Netzwerkconfiguration	56
4.3	Ändern der Admin PIN	59
4.4	Pairing	61
4.4.1	Pairing anzeigen	62
4.4.2	Block löschen	62
4.4.3	Schlüssel löschen	64
4.4.4	Alle Pairings löschen	65
4.5	SICCT Update ein- oder ausschalten	67
4.6	SICCT Konfiguration ein- oder ausschalten	69
4.7	Ändern der SICCT PIN	69
4.8	Web Admin Schnittstelle ein- oder ausschalten	72
4.9	Selbsttest ausführen	74
4.10	Werksreset ausführen	74
4.11	Alternativen Werksreset einschalten	75
4.12	Neue Start PIN vergeben	75
4.13	Firmware-Version und Firmware-Update	76
4.13.1	Anzeige der aktuellen Firmware-Version	77
4.13.2	Durchführung eines Firmware-Updates	79
4.13.3	Durchführung eines Firmware-Downgrade	85

4.13.4	Speichern von Update-Freischaltcodes	86
4.13.5	Anzeigen der installierten CA-Zertifikate	88
4.13.6	Update der CA-Liste.....	88
4.14	Aktuelle IP-Adresse anzeigen	89
4.15	Keep Alive senden	90
5	Gerät zurücksetzen.....	91
5.1	Zurücksetzen mit Kenntnis der Admin PIN.....	91
5.2	Zurücksetzen ohne Kenntnis der Admin PIN.....	93
5.2.1	Zurücksetzen mittels PUK.....	93
5.2.2	Zurücksetzen ohne Kenntnis des PUK	94
6	Weboberfläche nutzen	95
6.1	Netzwerkeinstellungen vornehmen.....	99
6.2	Kennwort der Web Admin Schnittstelle ändern	99
6.3	SICCT Kennwort ändern	101
6.4	Pairings einsehen und löschen	102
6.5	SICCT Einstellungen.....	103
6.6	Konfiguration	103
7	Qualifizierte elektronische Signaturen.....	105
8	Produktregistrierung	105
9	Problembehebung.....	106
10	Kontakt	114
11	Außerbetriebnahme, Rückversand und Entsorgung.....	114

Rollenzuordnung

Im Folgenden wird eine Rollenzuordnung der einzelnen Kapitel dieses Handbuchs vorgenommen.



Administrator

Alle Kapitel dieses Handbuchs sind für Geräteadministratoren relevant.



Benutzer

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

- 1 „Sicherheitshinweise und allgemeine Informationen“ (S. 8)
- 1.3 „Sicherheitskonzept des Terminals“ (S. 14)
- 1.7 „Ein- und Ausschalten des Kartenterminals“ (S. 33)
- 1.8 „Reinigen und Desinfizieren des Gerätes“ (S. 34)
- Das gesamte Kapitel 2 „Bedienelemente“ (S. 35)
- 3.2 „Eingabe einer Karten-PIN“ (S. 49)
- Das gesamte Kapitel 7 „Qualifizierte elektronische Signaturen“ (S. 105)
- Das gesamte Kapitel 9 „Problembehebung“ (S. 106)



Reset-Administrator

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

- 1 „Sicherheitshinweise und allgemeine Informationen“ (S. 8)
- 1.6.2 „Setzen des PUK“ (S. 29)
- Das Kapitel 5 „Gerät zurücksetzen“ (S. 91) und hier insbesondere Kapitel 5.2 „Zurücksetzen ohne Kenntnis der Admin PIN“ (S. 93)

1 Sicherheitshinweise und allgemeine Informationen

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

- Lesen Sie vor Inbetriebnahme des Gerätes die Bedienungsanleitung sorgfältig durch.
- Bevor Sie mit der Installation und Inbetriebnahme des Gerätes und der erforderlichen Komponenten beginnen, versichern Sie sich der Unversehrtheit des Gerätes. Lesen Sie auch das Kapitel 1.1 „Sichere Lieferkette“ sorgfältig durch.
- Überprüfen Sie regelmäßig vor der Nutzung und nach Abwesenheit die Unversehrtheit des 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 für einen Zeitraum von mindestens 10 Minuten verhindert.
- Das Kartenterminal eHealth GT900 führt alle sicherheitsrelevanten Aktionen ausschließlich in einem vertrauenswürdigen Zustand aus. Im vertrauenswürdigen Zustand befindet sich das eHealth-Kartenterminal in einem Modus, bei dem keine Beeinflussung und keine Informationsabschöpfung durch Komponenten (dazu zählt auch Software), welche nicht über eine Zulassung durch die gematik verfügen, möglich ist.

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

- Verwenden Sie für den Wiederversand und sonstigen Transport des Gerätes die Originalverpackung oder eine andere geeignete Verpackung, die Schutz gegen Stoß, Schlag, Feuchtigkeit und elektrostatische Entladung gewährt.
- Beachten Sie bei Außerbetriebnahme und Wiederversand des Gerätes das Kapitel 11 „Außerbetriebnahme, Rückversand und Entsorgung“.
- Bewahren Sie das Gerät außerhalb der Reichweite von Kindern auf.
- Angaben zur Version finden Sie für die Hardware auf dem Typenschild an der Unterseite des Geräts sowie für die Firmware über die Menüsteuerung des Geräts (s. Kapitel 4.13.1).
- Vergewissern Sie sich vor dem ersten Einlesen einer Versichertenkarte oder HBA/SMC-B, dass diese Versionsangaben mit den Angaben zur Firmware- und Hardwareversion auf Seite 3 dieses Handbuches übereinstimmen.
- Neben der Hardware ist die Firmware ein sicherheitssensibles Element. Verwenden Sie aus diesem Grund nur zugelassene Firmware-Versionen. Spielen Sie eine neue Firmware ein, so kann der Vorgang nicht abgebrochen werden. Es ist nicht möglich, eine alte Vorgänger-Firmware-Version, die sich nicht in der Firmwaregruppe (Liste der zulässigen Firmware-Versionen) befindet, einzuspielen. Das Gerät prüft vor dem Anwenden der neuen Firmware, ob es sich um eine unveränderte, integere Version von german telematics handelt.
- Sorgen Sie für eine umweltgerechte Entsorgung des eHealth GT900 Kartenterminals, wenn dieses endgültig nicht mehr benutzt werden soll. Lesen Sie hierzu auch die Hinweise in Kapitel 11 „Außerbetriebnahme, Rückversand und Entsorgung“.

1.1 Sichere Lieferkette

Ihr Kartenterminal und Ihre gSMC-KT (optional)¹ werden von german telematics auf einem sicheren Lieferweg an Sie ausgeliefert. Um die Unversehrtheit des Kartenterminals und der gSMC-KT (optional)¹ beim Erreichen des endgültigen Aufstellungsortes, bspw. einer Arztpraxis, sicherzustellen, muss vor der Inbetriebnahme eine Überprüfung der Sendung durch Sie durchgeführt werden.

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

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

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

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

Sollten Sie begründete Zweifel an der Unversehrtheit und Echtheit der Sendung haben, folgen Sie den Anweisungen auf unserer Internetseite unter <https://www.germantelematics.de/sichere-lieferkette> und der dort befindlichen

¹ Eine gSMC-KT ist für den Betrieb Ihres Kartenterminals notwendig und bei Bedarf gesondert zu bestellen (wenn nicht bereits eine gültige gSMC-KT vorhanden ist). Sofern Sie zusammen mit dem Kartenterminal eine gSMC-KT bei german telematics bestellt haben, erhalten Sie diese zusammen mit dem Kartenterminal. Zur Prüfung der Authentizität und Integrität einer german telematics gSMC-KT besuchen Sie unsere Internetseite <https://www.germantelematics.de/sichere-lieferkette>.

Checkliste Sichere Lieferkette. Verständigen Sie den Verkäufer des Gerätes. Das Kartenterminal darf bei Verdacht auf Manipulationen nicht in Betrieb genommen werden!

1.2 Lieferumfang

Im Lieferumfang Ihres Gerätes sind enthalten:

- ein eHealth GT900 Kartenterminal
- ein GS (Geprüfte Sicherheit) zertifiziertes Netzteil (5V / 1200 mA)
- ein Ethernet-Kabel (2m)
- eine Bedienungsanleitung (ggf. in elektronischer Form auf einem Datenträger)
- 4 SIM-Slotsiegel zur Versiegelung der SMC SIM-Slots. Bitte verwahren Sie diese Siegel bis zu Ihrer Verwendung an einem sicheren Ort² auf!
- Optional¹: Eine gSMC-KT (gerätespezifische Security Module Card Kartenterminal)

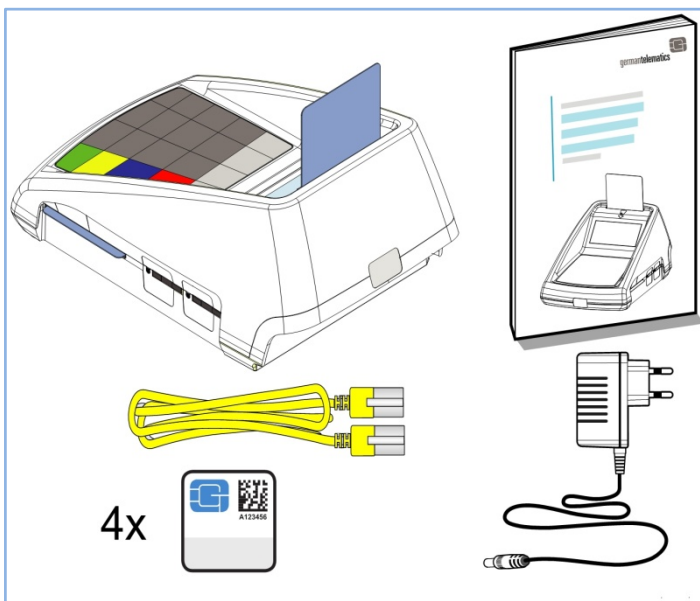


Abbildung 1: Lieferumfang

² Ein sicherer Ort ist dadurch gekennzeichnet, dass unbefugte Personen keinen Zugang dazu haben und das Eindringen unbefugter Personen erkannt wird. Dies kann beispielsweise ein verschließbares Schubfach oder ein Tresor sein.

1.3 Sicherheitskonzept des Terminals

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

Sollten Sie begründete Zweifel an der Unversehrtheit und Echtheit des Gerätes haben, folgen Sie den Anweisungen auf unserer Internetseite unter <https://www.germantelematics.de/sichere-lieferkette> und der dort befindlichen **Checkliste Sichere Lieferkette**. Verständigen Sie den Verkäufer des Geräts. Das Kartenterminal darf bei Verdacht auf Manipulationen nicht in Betrieb genommen werden!

Das Terminal verhindert im Betrieb den Diebstahl geschützter Daten durch einen elektronischen Sicherheitsmechanismus. Beachten Sie dazu das Kapitel 1.3.4 „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! Kontrollieren Sie, dass das Gerätelabel auf der Geräteunterseite unversehrt ist und glattflächig auf der Klebefläche aufliegt.

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

1.3.2 Siegelprüfung

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

- 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. Sind bereits SIM-Karten im Terminal gesteckt, prüfen Sie auch das/die durch den Administrator aufgebrachte/n SIM-Slotsiegel an der Seite des

Gerätes auf Unversehrtheit und lassen Sie bei Manipulationsverdacht die korrekte/n Siegelnummer/n durch den Administrator prüfen.

Ziehen Sie die Abbildung auf der Umschlagseite 2 (Gehäusesiegel) und auf Seite 42 (SIM-Slotsiegel) dieses Benutzerhandbuchs zu Rate, um die Lage, die Form und Größe sowie die Merkmale der Geräteversiegelung abzugleichen.

1.3.3 Netzteilprüfung

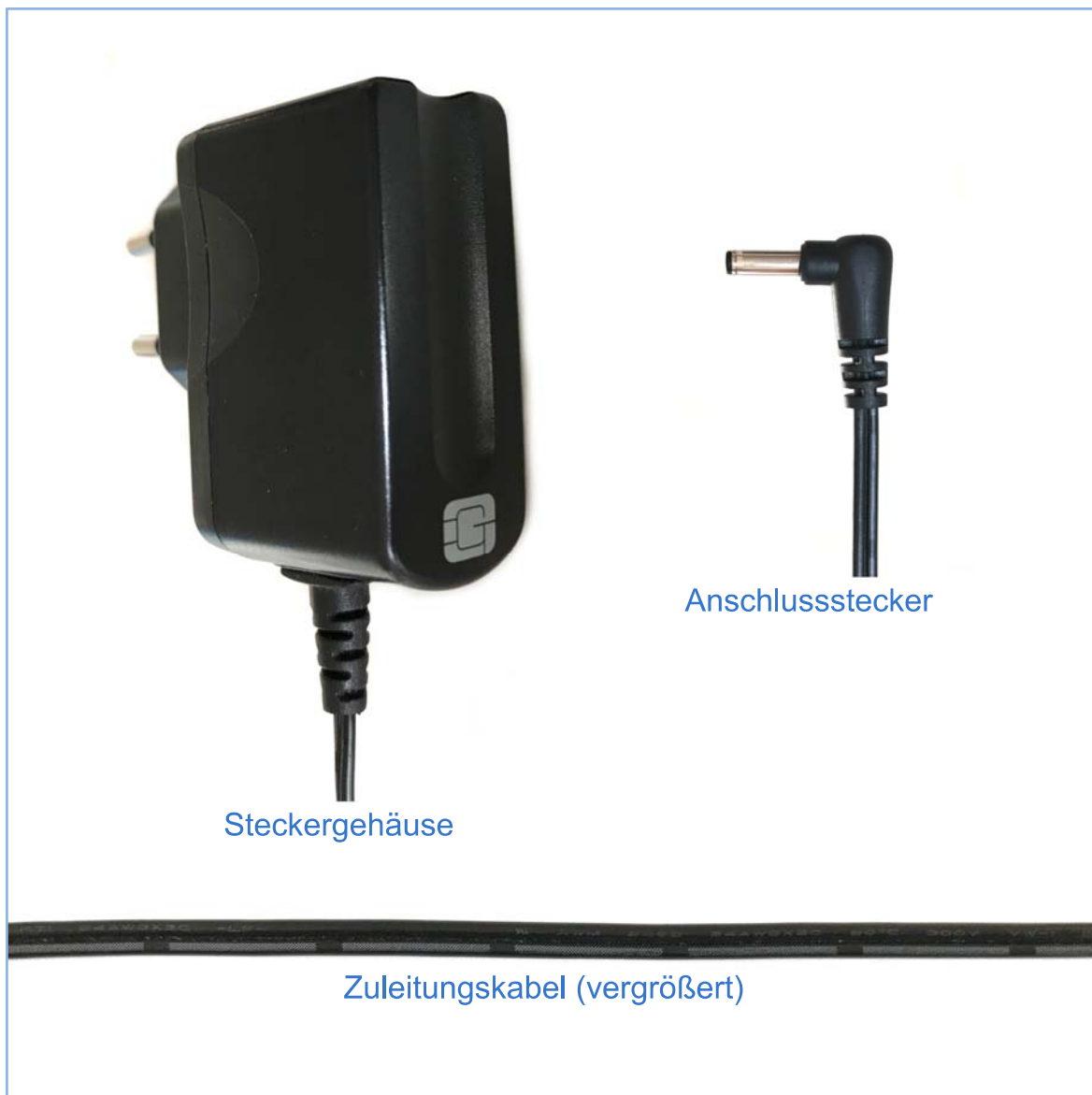


Abbildung 2: Detailansichten des Netzteils

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

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

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

1.3.4 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 Kartenterminals“ 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. Als Benutzer dürfen Sie die Start PIN nur dann eingeben, wenn Sie den stromlosen Zustand selbst herbeigeführt haben und das Terminal während der stromlosen Zeit stets unter Ihrer Kontrolle war. Ist dies nicht der Fall, ist nur der Administrator berechtigt, die Start PIN einzugeben.

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 nach einer unerwarteten Aufforderung die Start PIN einzugeben, das Gehäuse die Siegel und das Netzteil sorgfältig auf Veränderungen und Manipulationsspuren zu überprüfen (siehe Kapitel 1.3.1 „Gehäuseprüfung“, Kapitel 1.3.2 „Siegelprüfung“ und Kapitel 1.3.3 „Netzteilprüfung“)! 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, 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 3). Drücken Sie die -Taste, um dies zu bestätigen. Bestätigen Sie diesen Dialog nicht, kann das Terminal nicht weiter genutzt werden.

ADMIN:
Start-PIN Eingabe:
Sicherheitshinweise
im Handbuch beachten
und bestätigen!

Beachten Sie die Hinweise zum Umgang mit der Start PIN.



Abbildung 3: Bestätigung der Beachtung der Sicherheitshinweise

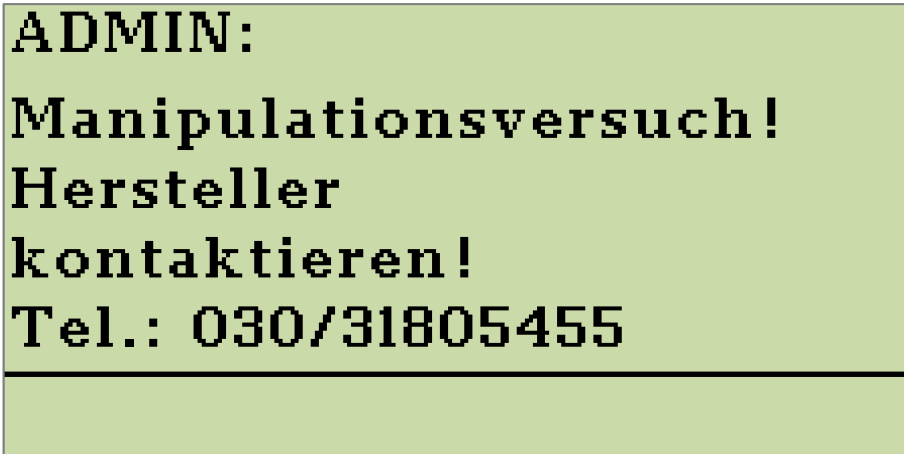
Nachdem Sie diesen Dialog bestätigt haben, werden Sie aufgefordert, die im Display des Gerätes angezeigte MAC Adresse (s. Abbildung 4) mit der auf dem Gerätelabel auf der Gehäuseunterseite aufgedruckten MAC Adresse zu vergleichen. Vergleichen Sie die MAC Adresse auch mit dem während der Akzeptanzprozedur archivierten Dokument.

ADMIN:
Start-PIN Eingabe:
Vergleich MAC Adresse
00:25:0E:00:01:30
Identisch/Abbruch?

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

Abbildung 4: 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 5 und darf nicht in Betrieb genommen werden! Kontaktieren Sie den Hersteller.

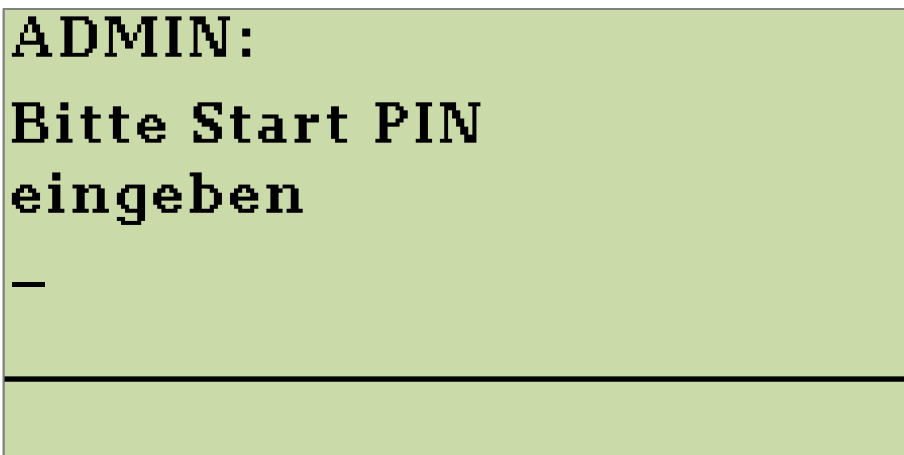


```
ADMIN:  
Manipulationsversuch!  
Hersteller  
kontaktieren!  
Tel.: 030/31805455
```

Anzeige bei nicht
erfolgter
Bestätigung der
Übereinstimmung
der MAC Adressen.

Abbildung 5: Manipulationsversuch

Nachdem Sie die MAC Adresse erfolgreich validiert haben, können Sie Ihre Start PIN eingeben (s. Abbildung 6).



```
ADMIN:  
Bitte Start PIN  
eingeben  
_
```

Aufforderung zur
Eingabe der
Start PIN.

Abbildung 6: Eingabe der Start PIN

Bestätigen Sie die Eingabe mit der -Taste. Wenn Ihre Eingabe korrekt ist, ist das Terminal betriebsbereit. Sollten Sie die Start 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.

1.4 Aufstellungshinweise

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

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

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

Machen Sie sich bewusst, dass für regelmäßige Überprüfungen an den Siegeln ein leichter Zugang zum Gerät gewährleistet sein muss. Das Kartenterminal sollte zudem Patienten zugänglich gemacht werden, insofern diese Eingaben an dem Gerät tätigen müssen.

1.5 Anschluss des Gerätes

Das eHealth GT900 Kartenterminal 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 Kartenterminal. In Abbildung 7 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 Kartenterminal im selben Netzwerk befinden müssen. Das Kartenterminal 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 Kapitel 2.2.3 „SIM-Slots“.

Schließen Sie nun das mitgelieferte Netzteil an den dafür vorgesehenen Anschluss an Ihrem Kartenterminal an. Der Netzteil-Anschluss ist in Abbildung 7 mit der Position ⑤ gekennzeichnet. Stecken Sie abschließend das Netzteil in eine Steckdose (230V / 50 Hz)³. Ihr Gerät ist nun für die Erstinbetriebnahme bereit, beachten Sie daher die Hinweise in Kapitel 1.6 „Inbetriebnahme des Kartenterminals“. Die Anschlüsse mit der Position ② (USB Typ B) und ③ (RS232) sind in dieser Firmware funktionslos.

³ 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 Kartenlesegerätes 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 Kapitel 2.2.3 „SIM-Slots“ beschrieben ist.

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

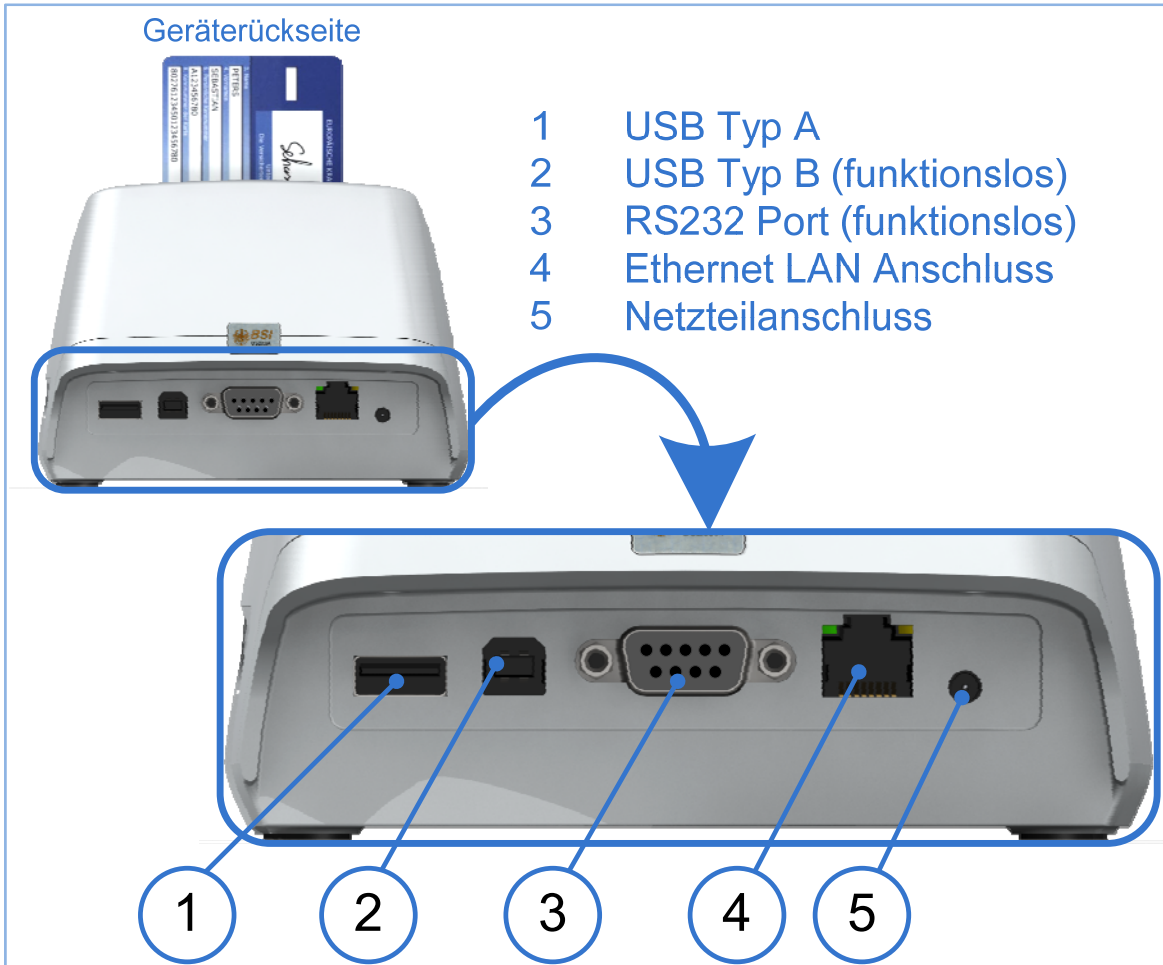


Abbildung 7: Belegung der Anschlüsse

1.6 Inbetriebnahme des Kartenterminals

Die Inbetriebnahme des Kartenterminals ist durch einen Administrator vorzunehmen. Es ist zudem sicherzustellen, dass das LAN-Netzwerk in dem das Kartenterminal in Betrieb genommen wird, vor unbefugtem Zugriff abgesichert ist. Legen Sie vor der Inbetriebnahme alle notwendigen SMC in das Gerät ein (s. Kapitel 2.2.3). **Das Gerät sollte sich durch den Anschluss der Stromversorgung selbst eingeschaltet haben** (siehe Kapitel 1.5 „Anschluss des Gerätes“). Bei der Erstinbetriebnahme des Gerätes werden Sie nach einem kurzen Systemtest gebeten, eine Admin PIN⁴ zu vergeben. Nach dem Vergeben der Admin PIN müssen Sie zudem einen PUK vergeben, mit dem das Gerät beim Verlust der Admin PIN wieder in den Werkszustand zurückgesetzt werden kann. 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 Kapitel 5 „Gerät zurücksetzen“.

⁴ Die Bezeichnung Admin PIN ist als Abkürzung des Begriffes Administrator PIN zu verstehen.

1.6.1 Setzen der Admin PIN

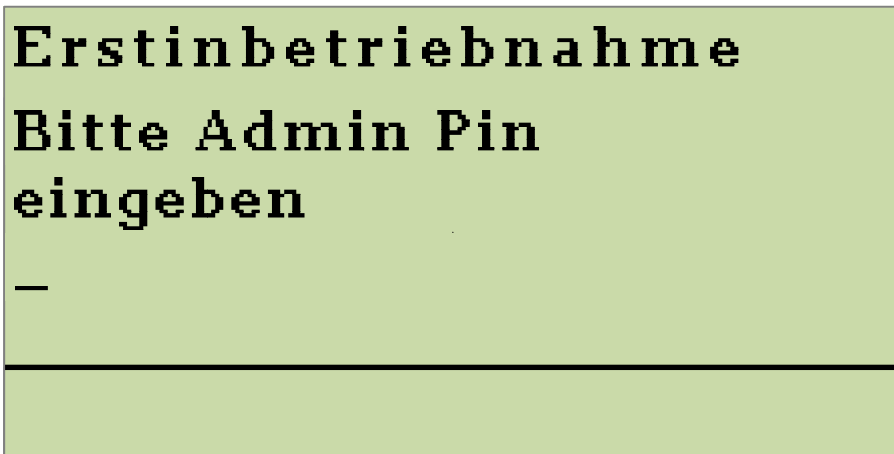




Abbildung 8: PIN-Eingabe bei der Erstinbetriebnahme

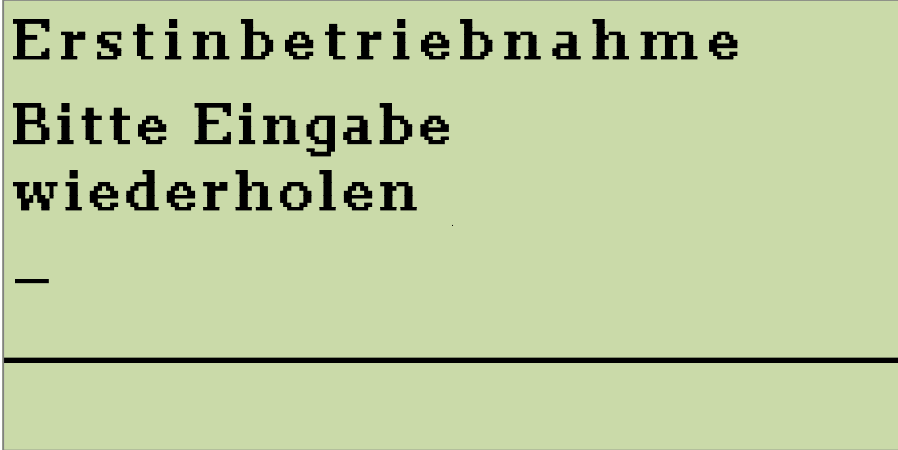
Nach dem erstmaligen Einschalten des Kartenterminals werden Sie gebeten, eine Admin PIN zu vergeben.

Die PIN muss aus **mindestens 8 und höchstens 16 numerischen Zeichen** bestehen.

Die Zeichen  und  können nicht verwendet werden. Bewahren Sie die PIN an einem sicheren Ort auf. Vermeiden Sie es, die Admin PIN in der Nähe des Gerätes aufzubewahren, insbesondere sollten Sie sie **nicht** auf dem Gerätegehäuse notieren.

Verwenden Sie zudem keine Trivial-PIN⁵. Lesen Sie hierzu bitte auch die Hinweise zum Umgang mit der Admin PIN am Ende des Kapitels 4.1 „Admin-Menü“. Sie werden anschließend zu einer Wiederholung der PIN aufgefordert.

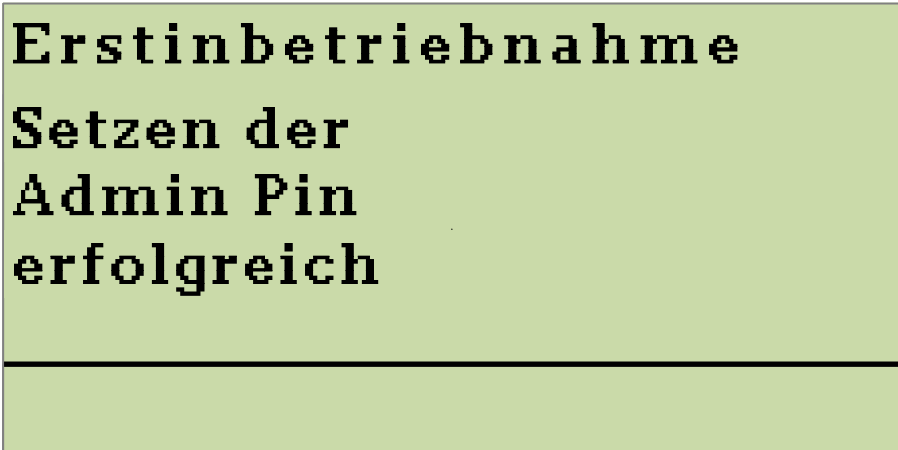
⁵ Trivial-PINs und PUKs werden vom Gerät nicht angenommen und durch die Anzeige einer entsprechenden Fehlermeldung abgewiesen. Es werden alle Eingaben als Trivial-PIN bzw. –PUK abgelehnt, die nur aus einer Ziffer bestehen, wie z.B.11111111, sowie streng auf- oder absteigende Ziffernfolgen wie 01234567 oder 98765432.



Erstinbetriebnahme
Bitte Eingabe
wiederholen

Abbildung 9: Bestätigung der PIN-Eingabe

Haben Sie die Admin PIN erfolgreich vergeben und Ihre Eingabe aus Sicherheitsgründen wiederholt bzw. bestätigt (siehe Abbildung 9), können Sie nach einer kurzen Bestätigungsanzeige, wie sie in Abbildung 10 dargestellt ist, mit der Vergabe eines PUK fortfahren. Sollten die von Ihnen eingegebenen PINs nicht identisch sein, werden Sie zur erneuten Eingabe aufgefordert.




Erstinbetriebnahme
Setzen der
Admin Pin
erfolgreich

Abbildung 10: Erfolgreiche Vergabe der Admin PIN



1.6.2 Setzen des PUK

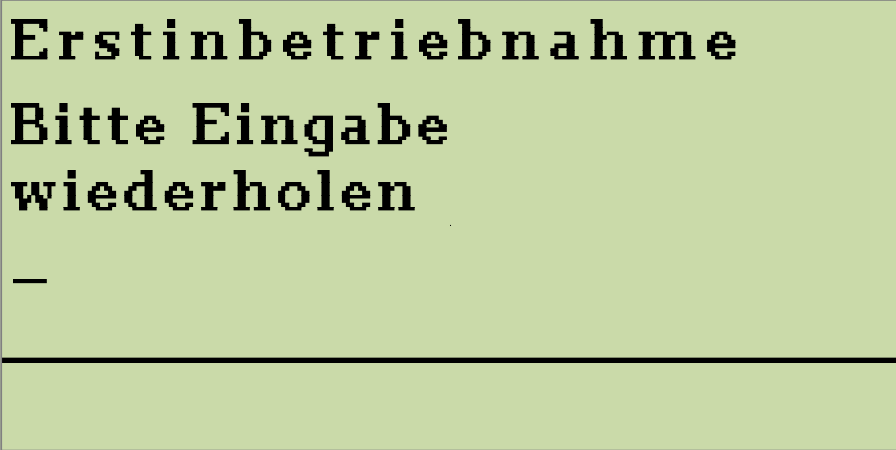
Mit Hilfe des PUK können Sie das Kartenterminal später in den Auslieferungszustand zurücksetzen, sollte dies notwendig werden. Eine Person mit Kenntnis des PUK wird als Reset-Administrator bezeichnet. Wie Sie mittels PUK einen Werksreset auslösen, erfahren Sie in Kapitel 5.2.1 „Zurücksetzen mittels PUK“.



Erstinbetriebnahme
Bitte Geräte PUK
eingeben
—

Abbildung 11: PUK-Eingabe bei der Erstinbetriebnahme

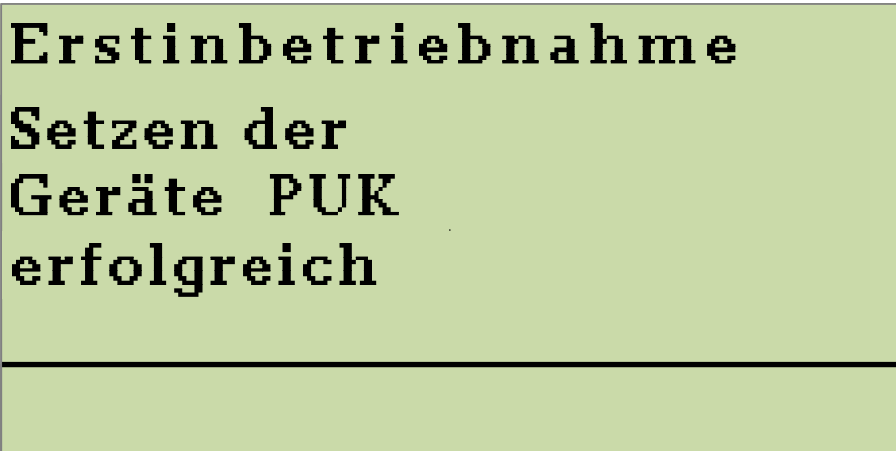
Der PUK muss aus **mindestens 8 und höchstens 16 numerischen Zeichen** bestehen. Die Zeichen  und  können nicht verwendet werden. Bewahren Sie den PUK an einem sicheren Ort auf. Vermeiden Sie es, den PUK in der Nähe des Gerätes aufzubewahren, insbesondere sollten Sie ihn **nicht** auf dem Gerätegehäuse notieren und sie nicht in der Nähe der Admin PIN aufbewahren. **Verwenden Sie zudem keinen Trivial-PUK⁵**. Lesen Sie hierzu bitte auch die Hinweise zum Umgang mit der Admin PIN und des PUK am Ende des Kapitels 4.1 „Admin-Menü“. Sie werden anschließend zu einer Wiederholung des soeben vergebenen PUK aufgefordert. Sollten die von Ihnen eingegebenen PUKs nicht identisch sein, werden Sie zur erneuten Eingabe aufgefordert.



Erstinbetriebnahme
Bitte Eingabe
wiederholen
—

Abbildung 12: Bestätigung der PUK-Eingabe

Haben Sie den PUK erfolgreich vergeben und Ihre Eingabe wiederholt bzw. bestätigt (siehe Abbildung 12), wird nach einer kurzen Bestätigungsanzeige, wie sie in Abbildung 13 dargestellt ist, die Start PIN generiert .

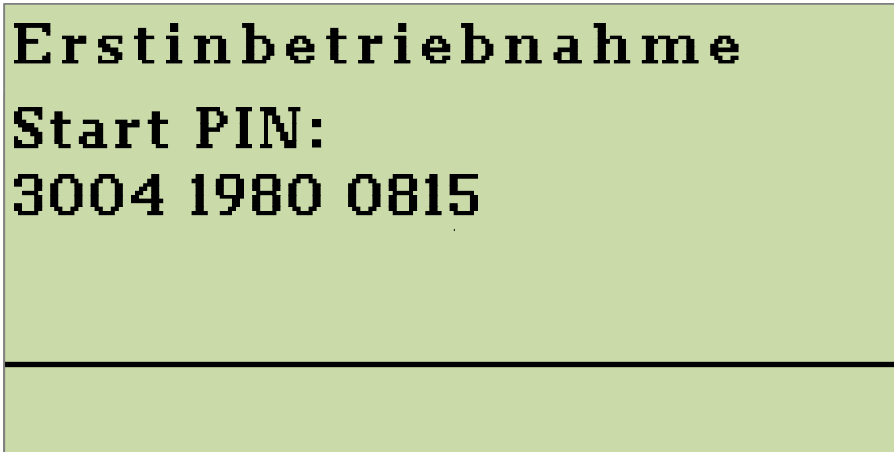


Erstinbetriebnahme
Setzen der
Geräte PUK
erfolgreich

Abbildung 13: Erfolgreiche Vergabe des PUK

1.6.3 Erzeugung einer Start PIN

Nachdem Sie eine Admin PIN und einen 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.



Die Start PIN in dieser Abbildung ist beispielhaft.

Ihr Kartenterminal zeigt die dann gültige erzeugte Start PIN an.

Abbildung 14: 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 Kapitel 1.3.4. Bei einer Inbetriebnahme nach einem stromlosen Zustand muss sich der Nutzer durch die Eingabe der Start PIN als berechtigter Nutzer identifizieren.

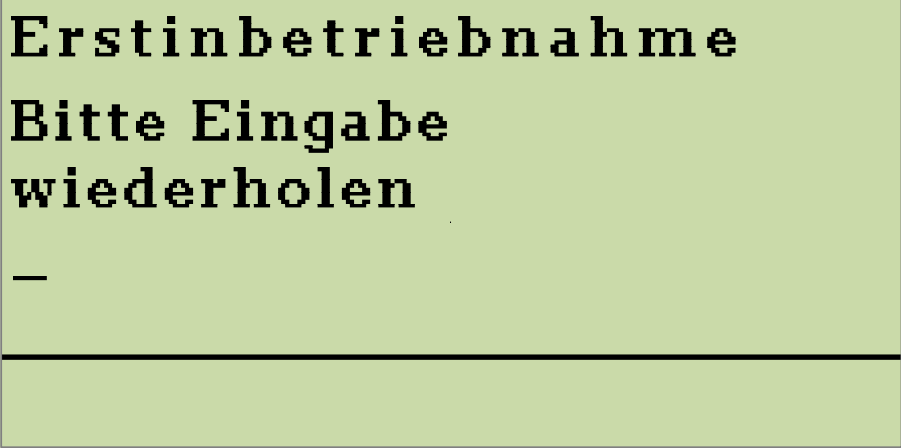
1.6.4 Setzen der SICCT PIN

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 das Kapitel 3.1.




Abbildung 15: 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-PIN⁵**. Lesen Sie hierzu bitte auch die Hinweise zum Umgang mit der Admin PIN und dem PUK am Ende des Kapitels 4.1 „Admin-Menü“. Sie werden anschließend zu einer Wiederholung der soeben vergebenen SICCT PIN aufgefordert.



Erstinbetriebnahme
Bitte Eingabe
wiederholen

Abbildung 16: Bestätigung der SICCT PIN Eingabe





Erstinbetriebnahme
Setzen der
der SICCT PIN
erfolgreich

Abbildung 17: Erfolgreiche Vergabe der SICCT PIN

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 Kartenterminals

Schalten Sie das Gerät durch Drücken der -Taste ein⁶. 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 Kartenterminal feucht reinigen, trennen Sie das Gerät immer zuerst vom Stromnetz. Lassen Sie nach einer erfolgten Reinigung das Gerät trocknen. Für die Reinigung des Kartenterminals reicht ein feuchtes Tuch (feuchtes Desinfektionstuch), welches vorher gut ausgewrungen werden sollte, damit keine Nässe an empfindliche elektronische Bauteile gelangen kann. Achten Sie insbesondere darauf, dass keine Flüssigkeit durch die Öffnungen der Kartenslots in das Innere des Gerätes gelangt. Sollten Sie zur Reinigung eine spezielle Desinfektionsdispersion verwenden, benutzen Sie diese nie direkt auf dem Gerät, sondern benetzen Sie ein dafür geeignetes Tuch und benutzen Sie dieses. Feiner Sprühnebel beziehungsweise Tropfen könnten sonst an empfindliche Bauteile gelangen und dadurch Ihr Gerät zerstören beziehungsweise unbrauchbar machen. Achten Sie bei der Reinigung darauf, die Siegel auf dem Gerätegehäuse keiner erhöhten mechanischen sowie fluiden Belastung auszusetzen. Dies könnte die Siegel auf Ihrem Gerät unter Umständen beschädigen und dazu führen, dass eine sichere Benutzung nach den gesetzlichen Vorgaben nicht mehr gewährleistet ist. Sollten Sie sich nicht sicher sein, ob es eventuell zu einer Beschädigung eines Siegels gekommen ist, so lesen Sie bitte Kapitel 1.3.2 „Siegelprüfung“.

2 Bedienelemente

2.1 Tastatur

Das eHealth GT900 Kartenterminal verfügt über eine integrierte Folientastatur, die Ihnen eine sichere PIN-Eingabe garantiert. Die folgende Abbildung 18 (Gerätetastatur) und Tabelle 1 (Tastaturbelegung) sollen Sie mit den Funktionen der Tastatur vertraut machen.

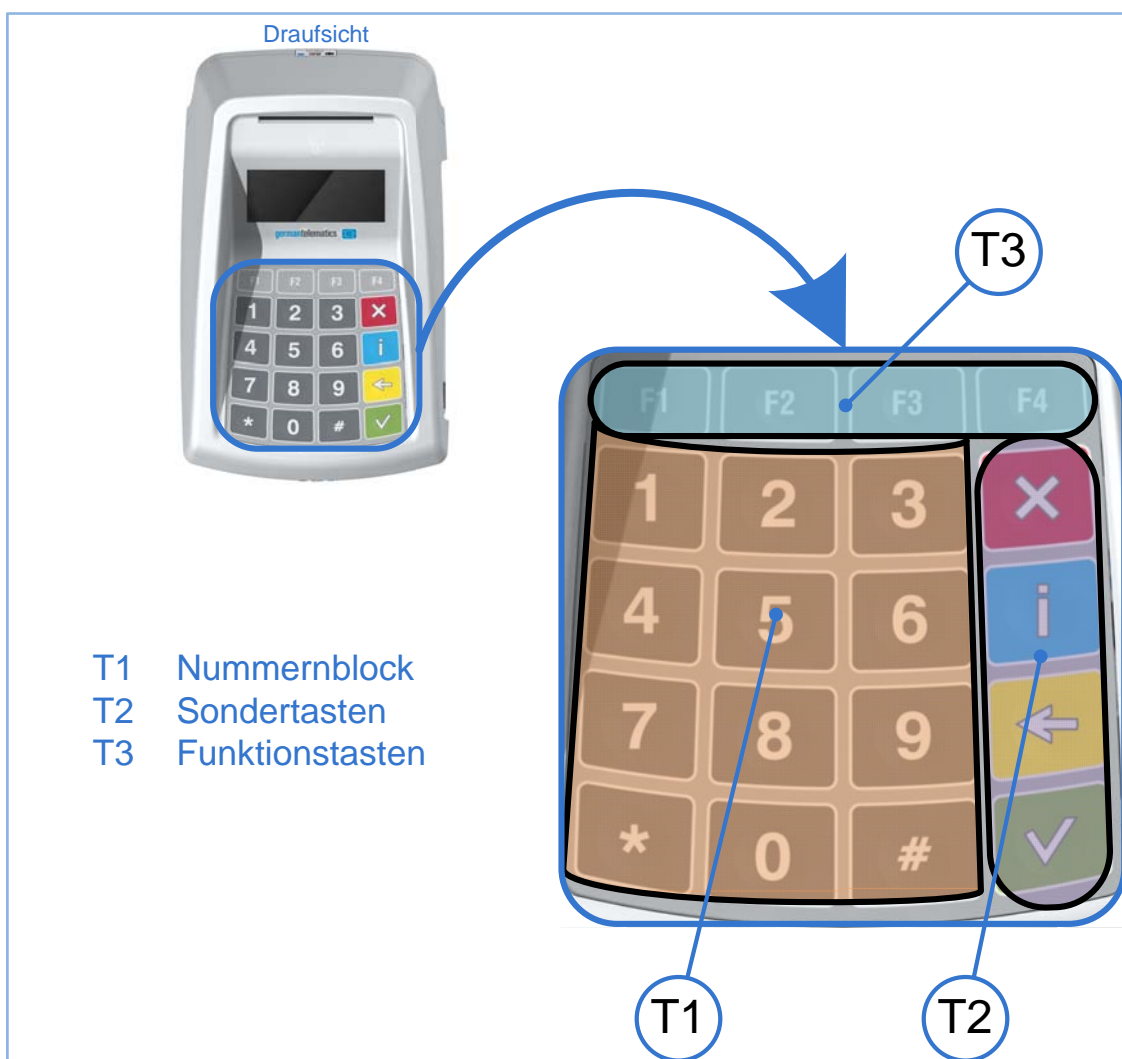




Abbildung 18: Tastatur des eHealth GT900 Kartenterminal

Tabelle 1: Tastaturbelegung des eHealth GT900 Kartenterminal

Symbol	In Abb.2	Funktion	Bemerkung
	T1	Nummerntasten 0, .., 9	
	T3	Funktionstaste F1	Halten Sie die F1 Taste länger gedrückt, um zum Admin-Modus zu gelangen.
	T3	Funktionstaste F2	Aufruf des Update-PIN cache (s. Kapitel 4.13.4) sowie Navigationstaste im Admin-Modus.
	T3	Funktionstaste F3	Navigationstaste im Admin-Modus.
	T3	Funktionstaste F4	Kurz drücken, um die Hintergrundbeleuchtung des Displays ein- oder auszuschalten.
	T1	derzeit funktionslos	
	T1	derzeit funktionslos	
	T2	Abbruch / Gerät ausschalten	Halten Sie die Taste min. 5 s gedrückt, um das Gerät auszuschalten.
	T2	Name des Terminals	Drücken Sie die Taste, um den Namen des Terminals anzuzeigen.
	T2	Zurück / Löschen / Korrektur	
	T2	Bestätigen / Gerät einschalten	Bei ausgeschaltetem Gerät kurz drücken, um das Gerät einzuschalten.

Durch die Verwendung einer Folientastatur ist eine einfache und schnelle Reinigung und Desinfektion dieser häufig durch Patienten oder Personal berührten Fläche möglich. Hinweise zum Reinigen und gegebenenfalls Desinfizieren des Kartenterminals finden sich in Kapitel 1.8 „Reinigen und Desinfizieren des Gerätes“.

2.2 Kartenslots

Das eHealth GT900 Kartenterminal ist mit zwei Chipkarten-Kontakteinheiten ausgestattet, um die Verwendung der Krankenversichertenkarte (KVK), der elektronischen Gesundheitskarte (eGK) sowie des Heilberufsausweises (HBA) und der Institutionenkarte (SMC-B) zu ermöglichen. Bestimmungsgemäß ist es nicht von Belang, in welcher Chipkarten-Kontakteinheit sich eine bestimmte Karte befindet. Das heißt insbesondere, dass jede der o.g. Karten in jeder Chipkarten-Kontakteinheit des Gerätes problemlos angenommen wird. Aus Gründen des einfacheren Umgangs mit dem Kartenterminal sei im Folgenden die Kontakteinheit 1 vornehmlich als eGK/KVK-Slot und die Kontakteinheit 2 vornehmlich als HBA-Slot bezeichnet. Ziehen Sie für diese Zuweisung auch Abbildung 20 zu Rate.

Des Weiteren verfügt das Kartenterminal über 2 SIM-Slots für SMC-Karten (Secure Module Cards) auf der rechten Geräteseite. In die SIM-Slots des Kartenterminals können auch sogenannte gSMC-KT Karten eingelegt werden. Das Kartenterminal nutzt eine eingelegte gSMC-KT Karte, welche die kryptografische Identität des Kartenterminals in Form eines X.509 Zertifikates darstellt. Die kryptografischen Schlüssel der gSMC-KT Karte müssen eine hohe Güte aufweisen und der Prozess der Schlüssel- und Zertifikatgenerierung muss entsprechend abgesichert werden, um die Vertraulichkeit, Authentizität und Integrität der kryptografischen Schlüssel und Zertifikate zu gewährleisten. Aus diesem Grund bedarf die gSMC-KT gesonderter Sicherheitsmaßnahmen. Stellen Sie, sicher, dass Ihre gSMC-KT durch die gematik zugelassen ist und über die entsprechenden Kennungen und Sicherheitsmerkmale verfügt. Beachten Sie bitte die Hinweise in Kapitel 2.2.3 „SIM-Slots“ und lesen Sie bitte auch die Info-Box „Wichtige Hinweise zum Umgang mit den SMC“ auf S. 43.

2.2.1 Kontakteinheit 1: Einstecken einer eGK/KVK



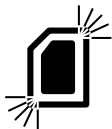
Eine KVK beziehungsweise eGK kann in der Chipkarten-Kontakteinheit 1 (eGK/KVK-Slot) des Gerätes bearbeitet werden. Die Karte wird von oben in die Kontakteinheit eingesteckt und nach unten gedrückt bis sie leicht einrastet. Dazu muss das Kontaktfeld (Chip) auf der Karte für Sie sichtbar sein und nach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



Das nebenstehende Symbol wird Ihnen in der oberen Statuszeile des Displays angezeigt (siehe Abbildung 21). Es repräsentiert den Chipkartenslot der Chipkarten-Kontakteinheit 1.



Wenn sich eine aktivierbare⁷ 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.

⁷ Sobald eine Chipkarte in die Kontakteinheit gesteckt wird, wird diese durch das Kartenterminal kurzzeitig elektrisch aktiviert um die Chipkarte auf grundsätzliche Funktion zu überprüfen. Haben Sie die Chipkarte korrekt gesteckt und das Kartensymbol wird nicht ausgefüllt dargestellt, so ist die Chipkarte defekt.

2.2.2 Kontakteinheit 2: Einstecken eines HBA/SMC-B

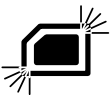
Eine HBA oder SMC-B kann vorzugsweise in der Chipkarten-Kontakteinheit 2 (HBA-Slot), seitlich rechts am Gerät, zur Verwendung kommen. Die Karte wird mit nach unten und zum Gerät zeigenden Kontaktfeld von rechts in die Kontakteinheit bis zum Anschlag eingeführt.



Das nebenstehende Symbol wird Ihnen in der oberen Statuszeile des Displays angezeigt (siehe Abbildung 21). Es repräsentiert den Chipkartenslot der Chipkarten-Kontakteinheit 2.



Wenn sich eine aktivierbare⁷ Chipkarte in der Kontakteinheit 2 befindet, wird dieses Symbol ausgefüllt im Display dargestellt.



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



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

2.2.3 SIM-Slots

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

Ein Entfernen der Chipkartenhalter führt, sofern das Gerät mit der Stromversorgung verbunden ist, zu einer Hinweismeldung im Display des Gerätes (s. Kapitel 9). Eine eventuell zum Konnektor bestehende Verbindung wird dabei beendet. Dabei ist es unerheblich, ob bereits eine Chipkarte eingelegt war oder der Chipkartenhalter leer ist. Um das Gerät weiterzubetreiben, müssen Sie einen Neustart ausführen wobei aus Sicherheitsgründen die korrekte Start PIN eingegeben werden muss. **Entfernen Sie diese Chipkartenhalter daher niemals leichtfertig.** Legen Sie die SMC Karte(n) nach Möglichkeit vor der Erstinbetriebnahme in das Gerät ein.

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

Nachdem Sie eine SMC in einen der SIM-Slots des Gerätes geschoben haben, versiegeln Sie diesen SIM-Slot mit den im Lieferumfang enthaltenen SIM-Slotsiegeln. Der Administrator des Gerätes unterschreibt auf dem Siegel bevor dieses auf dem Gerät angebracht wird in dem dafür vorgesehenen Feld (siehe Abbildung 19).

Darüber hinaus muss sich der Administrator die Siegel-Nr. notieren und diese Notiz an einem sicheren Ort verwahren⁸.

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

Das nebenstehende Symbol wird Ihnen in der oberen Statuszeile des Displays angezeigt (siehe Abbildung 21). Es repräsentiert jeweils einen der zur Verfügung stehenden SIM-Slots des Kartenterminals. Das obere der beiden SIM-Slot Symbole repräsentiert den hinteren SIM-Slot des Gerätes. Das untere der beiden SIM-Slot Symbole repräsentiert den vorderen SIM-Slot des Gerätes.



Wenn sich eine aktivierbare⁷ SMC in einem der SIM-Slots befindet, so wird dieses Symbol teilweise ausgefüllt im Display dargestellt.



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



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



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



⁸ Bevor Sie einen SIM-Slot versiegeln, sollten Sie die mit den eingelegten Karten in Verbindung stehenden Aufgaben durchführen. Dazu zählt z.B. das Pairing des Kartenterminals mit dem Konnektor für die eingelegte gSMC-KT, die Vergabe einer Echt-PIN für eine eventuell eingelegte SMC-B oder die Registrierung des Konnektors am VPN-Zugangsdienst mit einer eventuell eingelegten SMC-B.

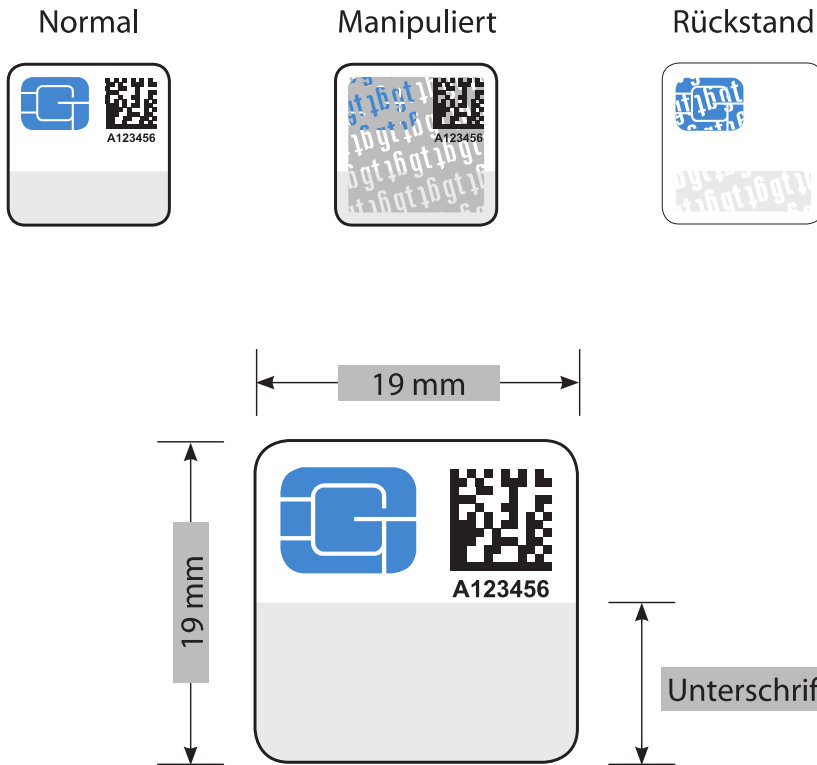


Abbildung 19: Sicherheitsmerkmale der SIM-Slotsiegel⁹

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

⁹ 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 SMC befindet. Wenn Sie eine SMC in einen der SIM-Slots eingelegt haben, muss dieser SIM-Slot durch den berechtigten Administrator mit einem Siegel verschlossen werden. Darüber hinaus muss sich der Administrator die Siegel-Nr. notieren und diese Notiz verwahren. 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 eingelegten SMC und nicht versiegelten SIM-Slots dürfen nicht verwendet werden! Überprüfen Sie auch die SIM-Slotsiegel regelmäßig auf mögliche Manipulationen! Bei Manipulationsverdacht muss der Administrator die Siegel-Nr. mit seinen Aufzeichnungen auf Übereinstimmung kontrollieren.

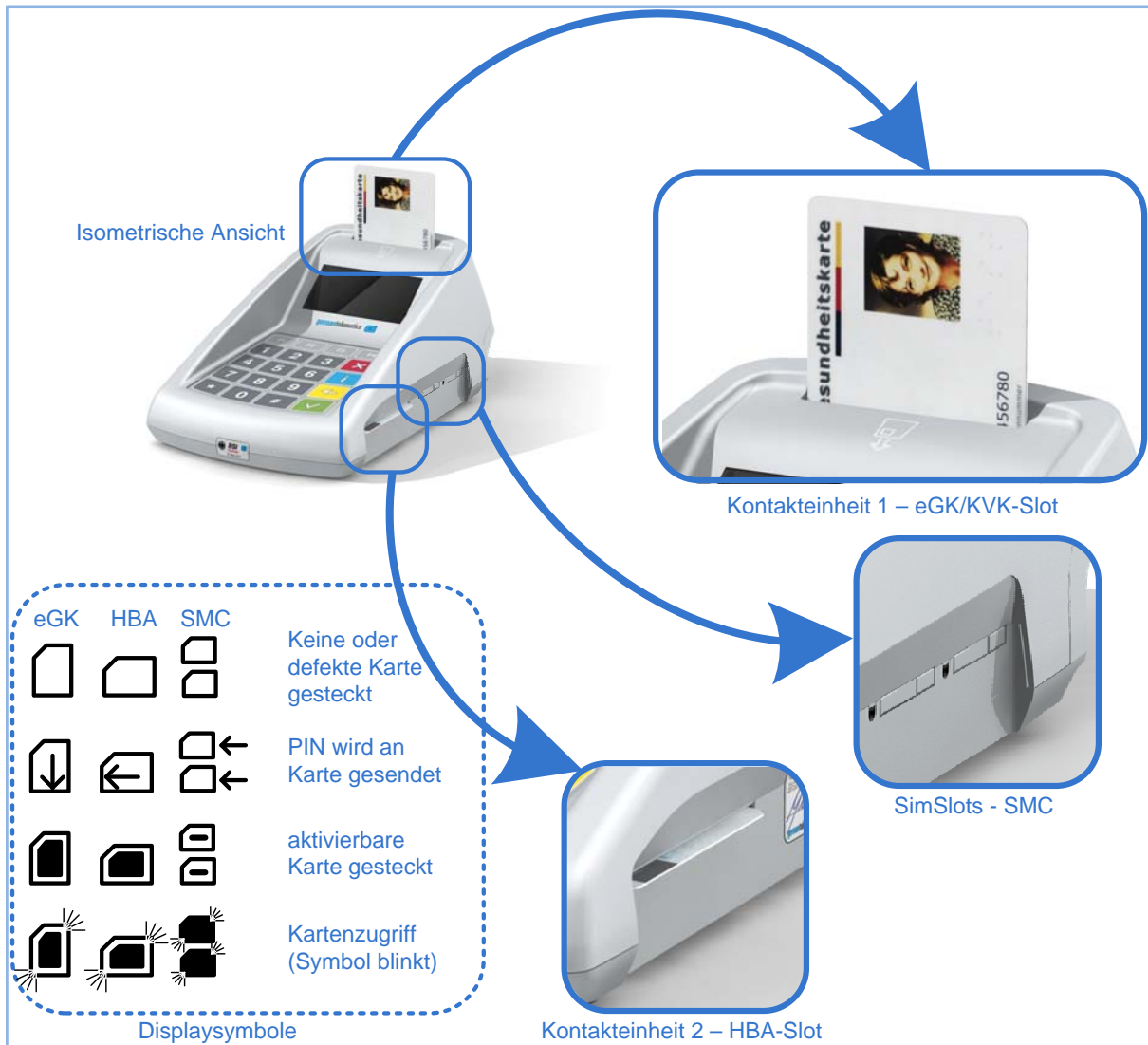


Abbildung 20: Anordnung und Benennung der Kartenslots

2.3 Aufbau der Displayanzeige

Auf dem Display des Gerätes werden Ihnen Informationen und Anweisungen angezeigt, die für die Arbeit mit dem Kartenterminal notwendig sind. Das Display gliedert sich, wie in Abbildung 21 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.

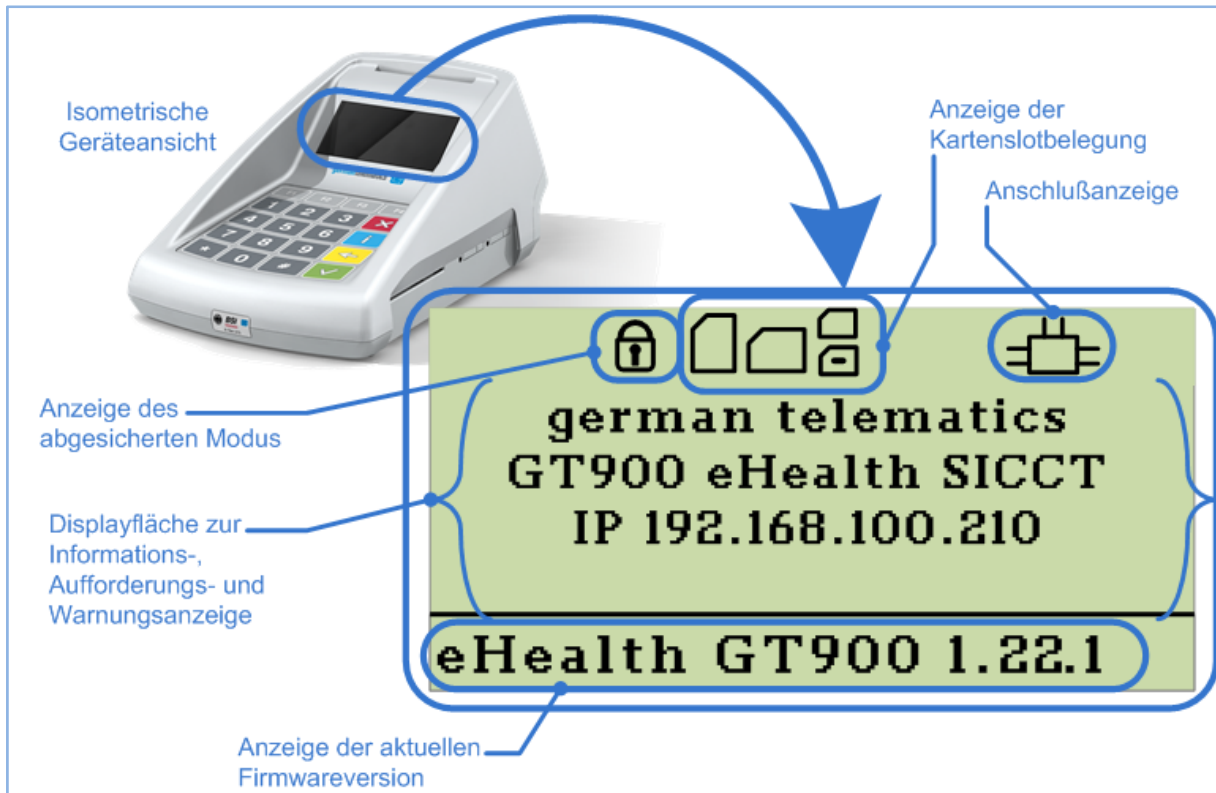
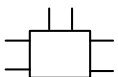
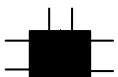


Abbildung 21: Displayaufbau des eHealth GT900 Kartenterminal

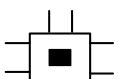
Der Anschluss des Kartenterminals an ein Netzwerk wird in der oberen Statusleiste rechts im Display angezeigt. Hierbei bedeutet:



Eine physikalische Ethernetverbindung ist vorhanden.



Eine SICCT-Session zu einem gepairten Konnektor ist aufgebaut.



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

Die Anzeige des abgesicherten Modus¹⁰ befindet sich in der oberen Statusleiste links im Display. In der Displaymitte werden Ihnen Informationen, Aufforderungen oder

¹⁰ Der abgesicherte Modus garantiert Ihnen eine sichere PIN-Eingabe für sämtliche Chipkarten-Geheimnummern (PIN) für eGK, HBA, SMC-B oder Standardsignaturkarten zu deren Eingabe das Kartenterminal auffordert. Der sichere PIN-Modus besagt, dass PIN-Eingaben am Kartenterminal nicht in die unsichere Umgebung des Personalcomputers oder über offene Übertragungswege an den Client gelangen.

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 22 dargestellt.

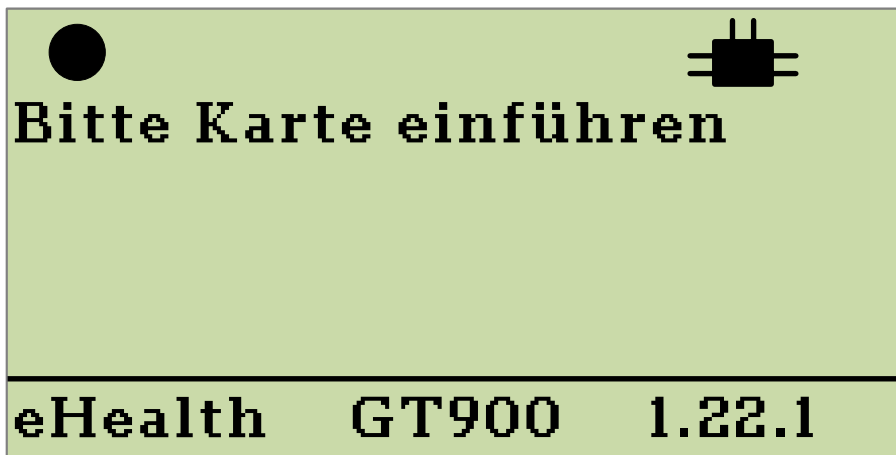


Abbildung 22: Beispielhafte Anzeige

In der oberen linken Ecke wird Ihnen, gesteuert durch den Konnektor und Ihre Software, eventuell zeitgleich mit einer Displaymeldung ein blinkender Punkt angezeigt. Dieser optische Hinweis dient dazu, Ihre Aufmerksamkeit auf die angezeigte Meldung zu lenken.

In der unteren Statusleiste des Displays werden Sie über die aktuelle Firmware-Version informiert.

3 Betrieb als eHealth Kartenterminal am Konnektor

Als eHealth Kartenterminal wird das Kartenterminal in ein LAN-Netzwerk eingebunden. Das Kartenterminal 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 Kartenterminal 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 Kapitel 2.2.3 „SIM-Slots“.

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

3.1 Pairing

Um Ihr Kartenterminal als eHealth Kartenterminal mit einem Konnektor zu koppeln, muss ein sogenannter Pairingprozess¹¹ eingeleitet werden. Der Pairingprozess wird

¹¹ Als Pairing bezeichnet man die logische Verbindung zwischen Kartenterminal, der darin eingelegten gSMC-KT und dem Konnektor. Das Pairing verhindert somit das eine dieser Komponenten unberechtigter Weise ausgetauscht werden kann.

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 Kartenterminals angezeigt. Diese Anweisungen müssen Sie befolgen, um einen erfolgreichen Pairingprozess von Konnektor und Kartenterminal 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 Kapitel 4.7 nachlesen.

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

Wichtige Hinweise zum Pairing-Prozess:



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

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 Kartenlesegerätes. Daher müssen PINs stets unbeobachtet eingegeben werden! Um die Sicherheit während der PIN-Eingabe zu gewährleisten, wird Ihnen im Display des Kartenterminals ein **Schlosssymbol** angezeigt. Dieses Symbol befindet sich während einer PIN-Eingabe **in der oberen Statusleiste links im Display**.

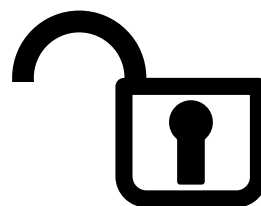
Die Eingabe einer PIN darf nur dann erfolgen, wenn das geschlossene Schlosssymbol anzeigt, dass eine PIN-Eingabe erwartet wird und keine Fehlermeldung des Konnektors vorliegt, dass die TLS-Verbindung zwischen Kartenterminal und Konnektor unterbrochen ist. Die PIN wird dann sicher an die Karte übertragen.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

Das Kartenterminal befindet sich in einem abgesicherten Betriebszustand und ermöglicht somit:



Die sichere Eingabe einer Karten-PIN

Das Kartenterminal befindet sich in einem **nicht** abgesicherten Betriebszustand.



Eine beispielhafte Aufforderung zur PIN-Eingabe ist in Abbildung 23 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 wird¹⁰.** Geben Sie Ihre PIN nicht ein, wenn der abgesicherte Modus nicht durch ein geschlossenes Schlosssymbol angezeigt wird.

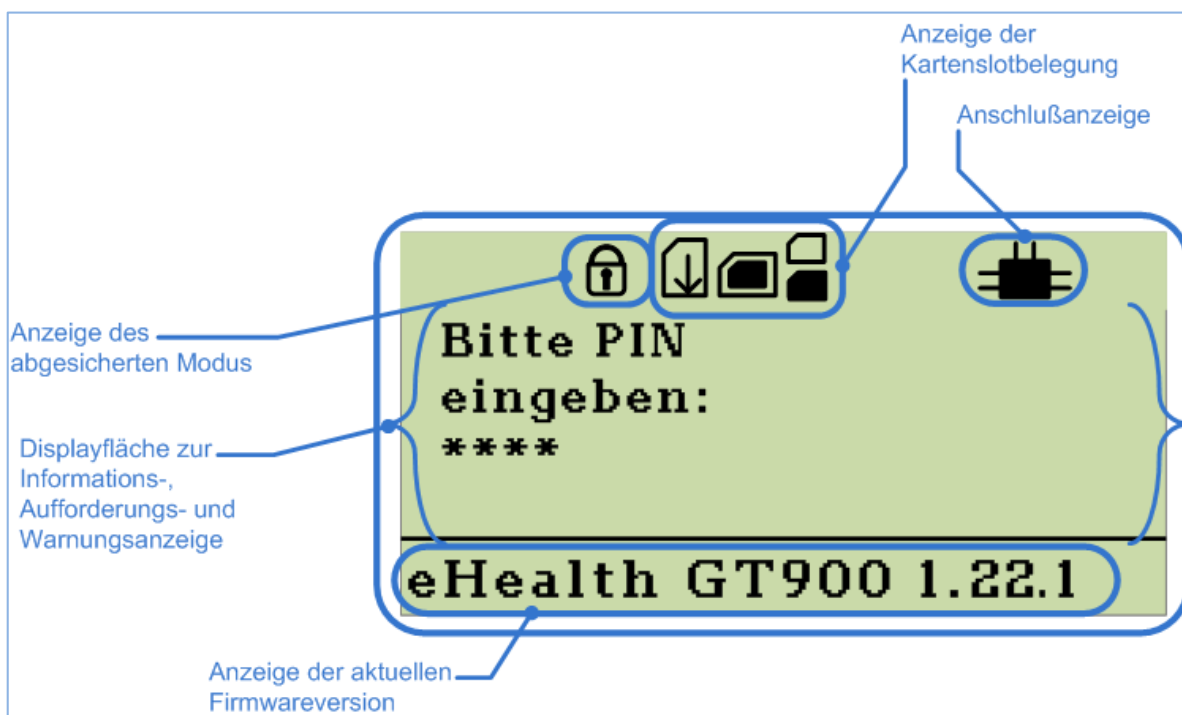


Abbildung 23: Mögliche Displayanzeige des Kartenterminals bei der Eingabe einer Karten PIN. In diesem Beispiel wird die Karten-PIN an die Karte im eGK-Slot gesendet (zusätzlich sind ein HBA und eine gSMC-KT eingelegt).


4 Geräteeinstellungen


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

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

4.1 Admin-Menü

Das Administrator-Menü kann geöffnet werden, solange keine SICCT-Session zwischen Terminal und Konnektor besteht. Eine bestehende Verbindung erkennen Sie an der voll oder teilweise ausgefüllten Anschlussanzeige (Abbildung 23). 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 -Taste des eingeschalteten Kartenterminals für mindestens 5 Sekunden. Sie werden aufgefordert, die Admin PIN einzugeben. Zu der Vergabe der Admin PIN lesen Sie bitte den Kapitel 1.6 „Inbetriebnahme des Kartenterminals“.

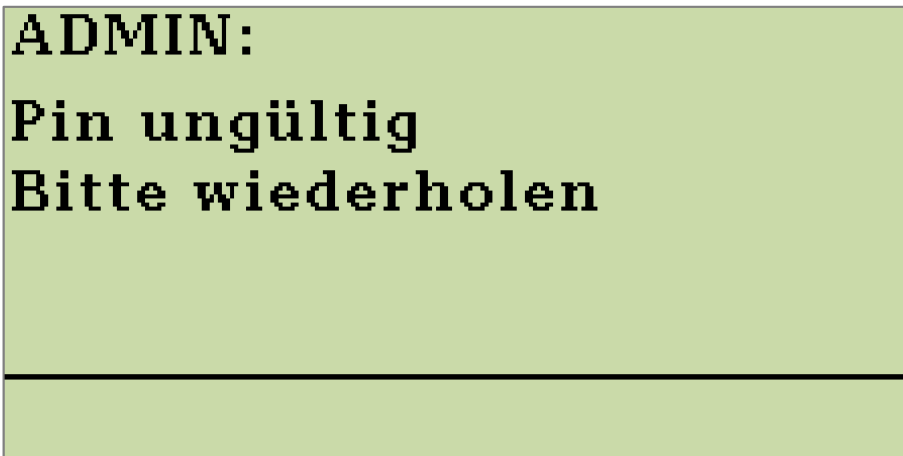


ADMIN:
Bitte Admin Pin
eingeben
—

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

Abbildung 24: Abfrage der Admin PIN

Bestätigen Sie die PIN-Eingabe mit der -Taste. Ist Ihre Eingabe nicht korrekt, wird Ihnen die Displaymeldung in Abbildung 25 angezeigt.

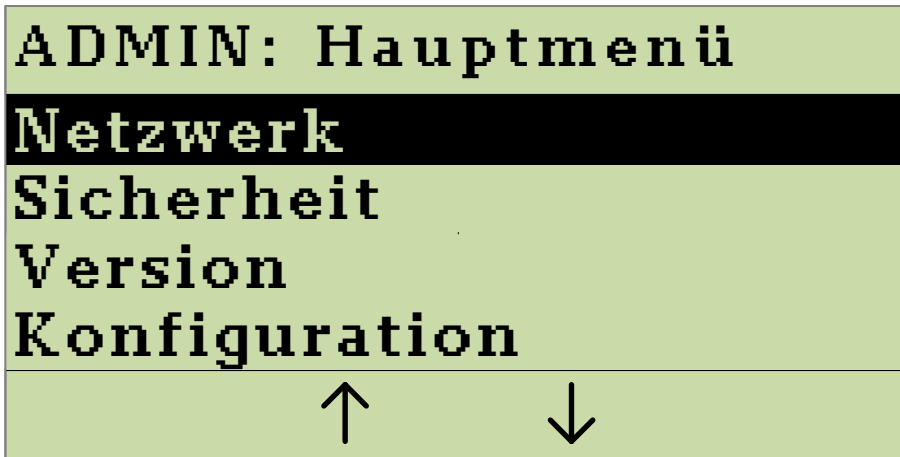


ADMIN:
Pin ungültig
Bitte wiederholen

Die von Ihnen eingegebene Admin PIN ist falsch.

Abbildung 25: Anzeige bei Eingabe einer falschen PIN

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







Im Admin-Menü finden Sie verschiedene Optionen zur Geräteinstellung.

Abbildung 26: Anzeige Admin-Menü

Im Admin-Menü haben Sie vier Optionen zur Geräteinstellung:

- Netzwerk:** Netzwerkkonfiguration des Kartenterminals
- Sicherheit:** Ändern sicherheitsrelevanter Einstellungen
- Version:** Anzeige und Aktualisieren der Firmware-Version
- Konfiguration:** Konfiguration für Displayanzeige und Keep-Alive¹²

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 27 finden Sie den vollständigen Aufbau des Admin-Menüs.

¹² Für eine Beschreibung des Keep-Alive Mechanismus siehe Kapitel 4.15 „Keep Alive senden“

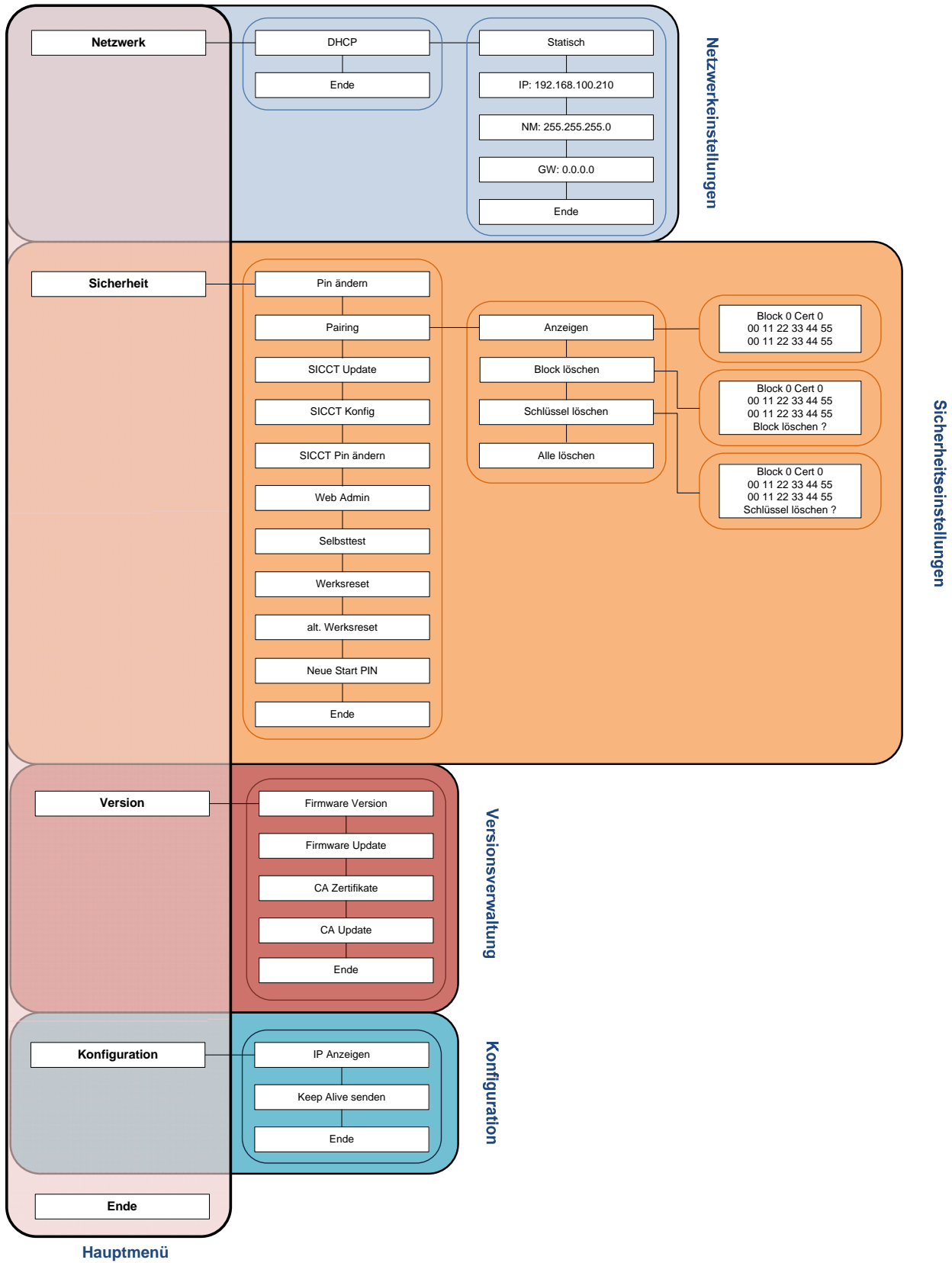


Abbildung 27: Struktur des Admin-Menüs

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

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

Hinweise zum Umgang mit der Admin PIN und dem PUK:



Halten Sie die Admin PIN, Start PIN und PUK geheim. Stellen Sie bei der Eingabe der PIN bzw. des PUK sicher, dass niemand sonst diese lesen kann. **Verwenden Sie keine/n Trivial-PIN/PUK wie beispielsweise 11111111 oder 12345678⁵. Vermeiden Sie es, die Admin PIN, Start PIN und den PUK in der Nähe des Gerätes aufzubewahren, insbesondere sollten Sie sie nicht auf dem Gerätegehäuse notieren.** Die Admin PIN ermöglicht Ihnen den Zugriff auf die Managementschnittstellen Ihres Kartenterminals und erlaubt somit das Abfragen und Ändern von sicherheitskritischen Konfigurationen.




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

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

4.2 Netzwerkkonfiguration

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

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

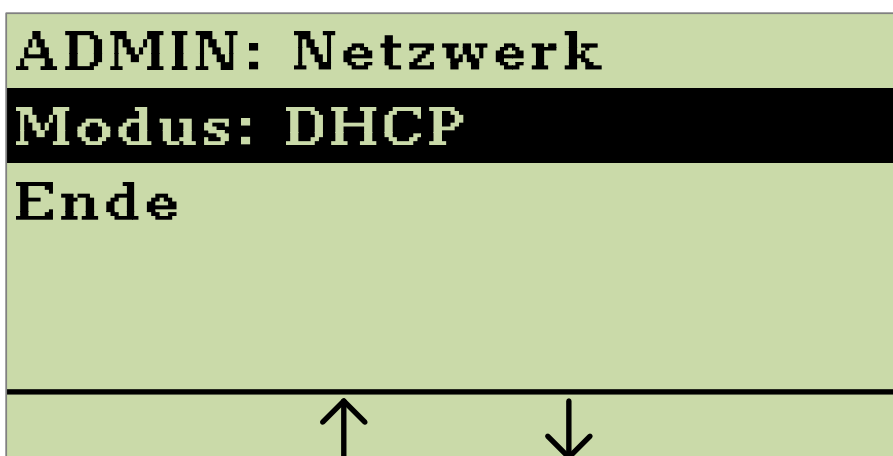

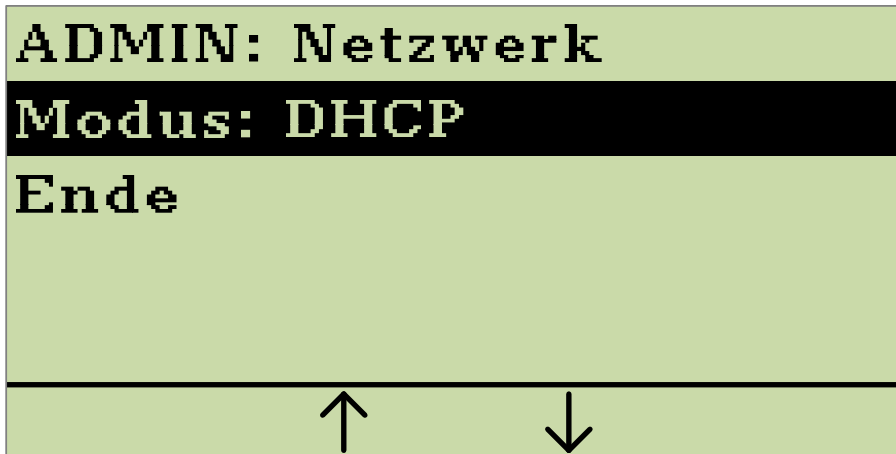



Abbildung 28: Beispielhafte Anzeige des Submenüs "Netzwerk"

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**.

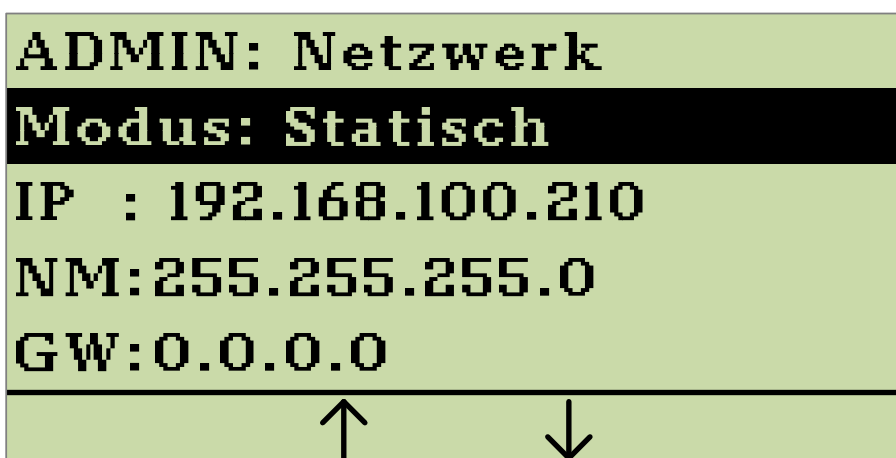


Wählen Sie den Parameter **DHCP**, um eine dynamische Netzwerk-konfiguration einzuleiten.

Abbildung 29: 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 4.14.

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 30: Anzeige bei Auswahl des Parameters "Statisch"

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

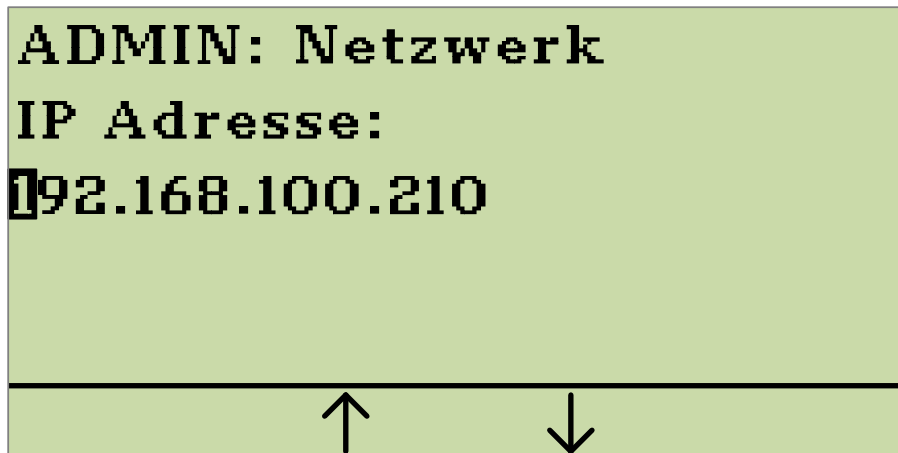






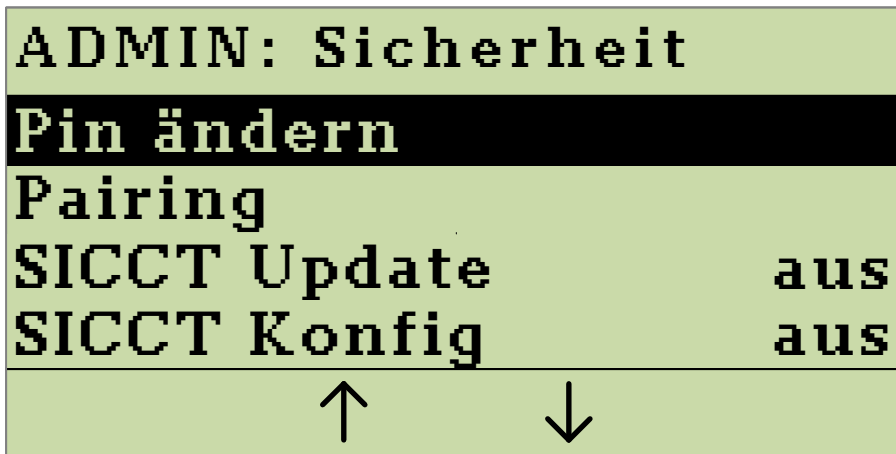
Abbildung 31: Beispiel für eine statische IP-Adresse

In Abbildung 31 ist die Eingabe einer beispielhaften IP-Adresse dargestellt. Für jeden Wert sind vier Felder **x.x.x.x** vorgesehen. In jedes Feld können drei numerische Zeichen eingegeben werden. Falls die Eingabe für ein Feld kürzer als drei Zeichen ist, muss die -Taste gedrückt werden, um die Eingabe im nächsten Feld fortzusetzen. Um einen vollständig eingegebenen Wert zu bestätigen, drücken Sie die -Taste. Nachdem die Eingabe des letzten Feldes bestätigt wurde gelangen Sie zurück zur Übersicht der Netzwerkparameter. Entspricht Ihre Eingabe jedoch nicht der vorgegebenen Notation für IP-Adressen, erhalten Sie eine Fehlermeldung.

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

4.3 Ändern der Admin PIN

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









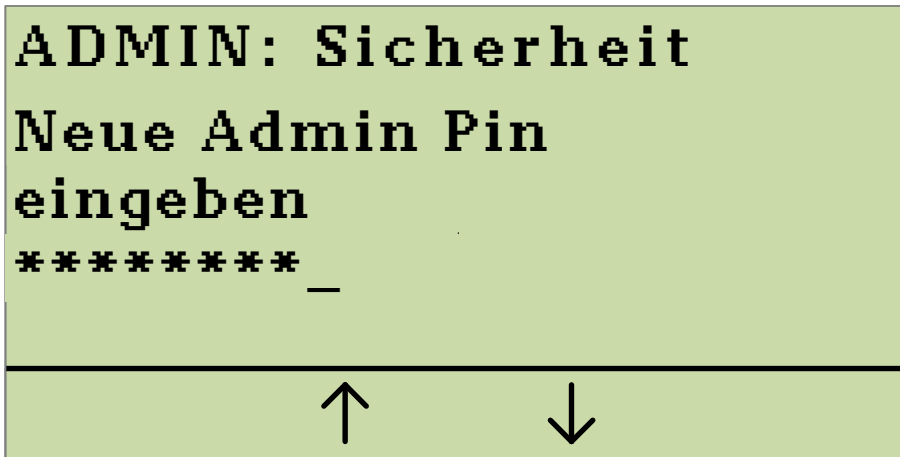
Drücken Sie die -Taste, um die aktuelle Admin PIN zu ändern.

Abbildung 32: 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 33 und Abbildung 34). Sollten die von Ihnen eingegebenen PINs nicht identisch sein, werden Sie zur erneuten Eingabe aufgefordert. Jede Eingabe können Sie durch Drücken der -Taste korrigieren. Die neue PIN muss aus **mindestens 8 und höchstens 16 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 12345678⁵.**




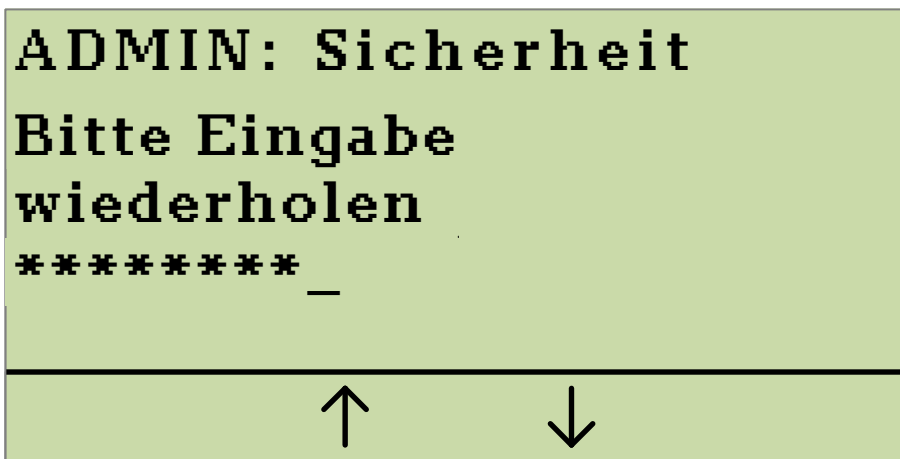
Eingabe der neuen PIN. Bestätigen Sie mit der -Taste.

Abbildung 33: Eingabe einer neuen Admin PIN




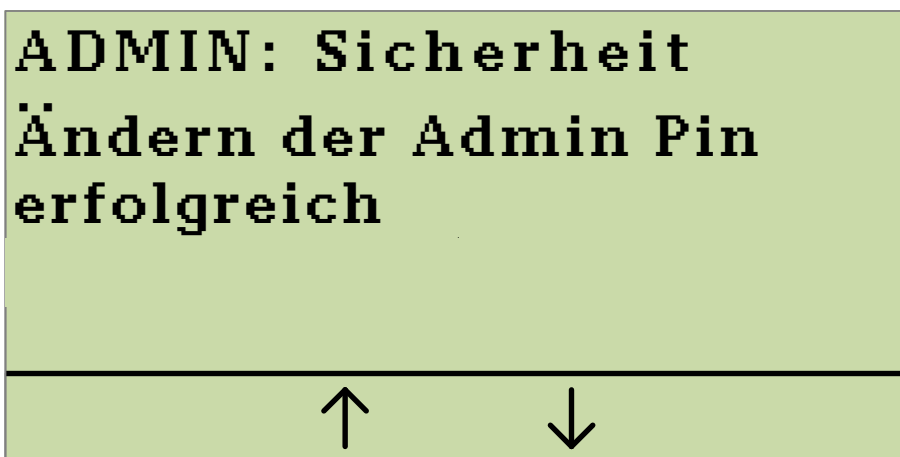
Wiederholen Sie Ihre PIN-Eingabe. Bestätigen Sie mit der -Taste.


Abbildung 34: Wiederholte Eingabe der Admin PIN

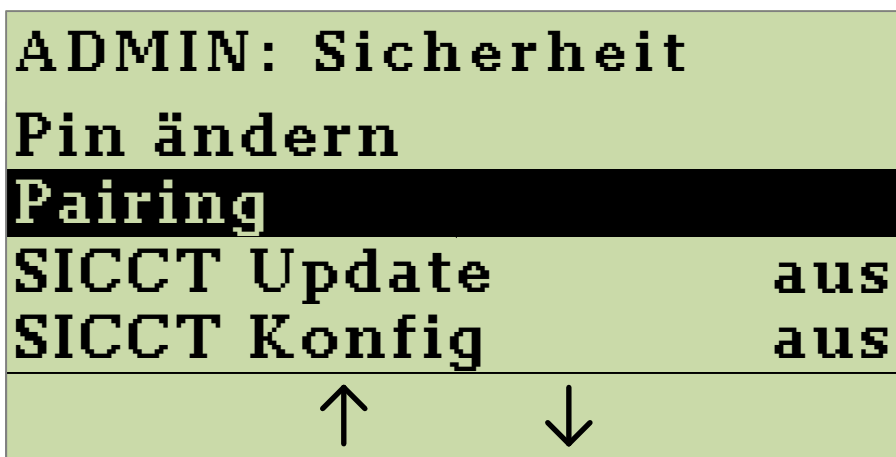


Ihnen wird anschließend eine kurze Bestätigung angezeigt und Sie kehren zum Admin-Menü zurück.

Abbildung 35: 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 das Kapitel 3.1 „Pairing“. Daher sollte das bestehende Pairing zu einem Konnektor nicht leichtfertig gelöscht werden. Um das derzeitige Pairing mit einem Konnektor zu löschen, wählen Sie in dem Admin-Menü die Option **Sicherheit** und bestätigen Sie mit der -Taste. Auf dem Display wird Ihnen das Submenü **ADMIN: Sicherheit** angezeigt.





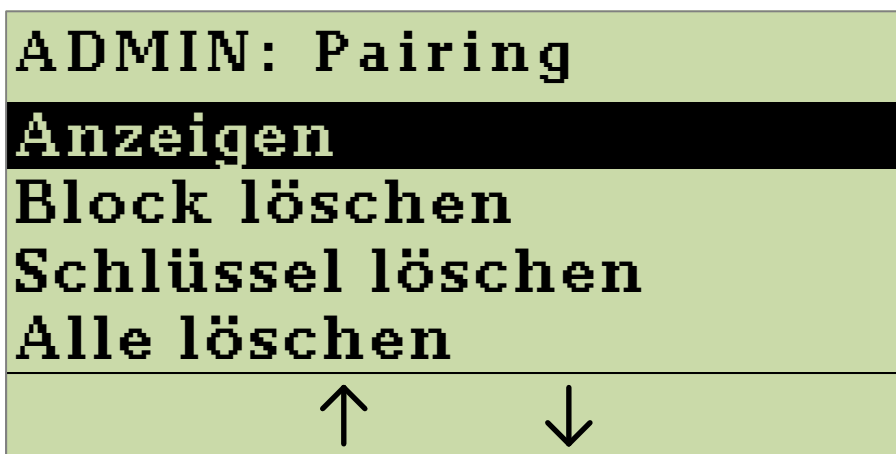
Drücken Sie die -Taste, um ins Menü Pairing zu gelangen.

Abbildung 36: 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 37 gezeigten Optionen ausführen können.







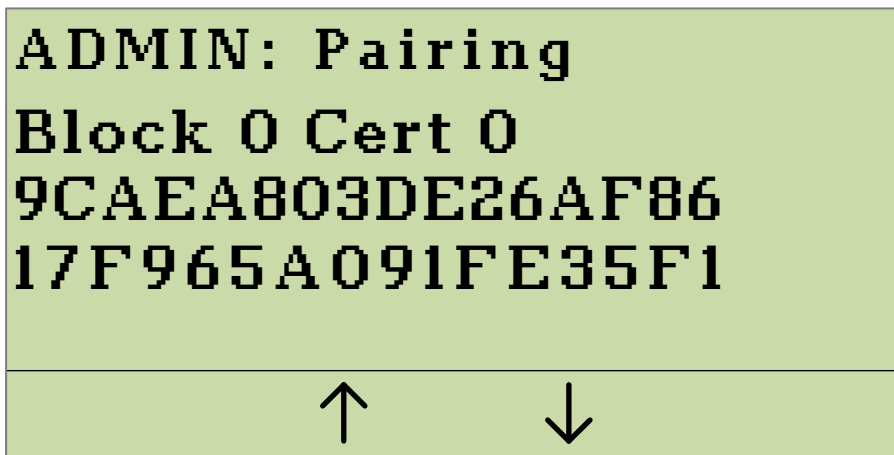
Drücken Sie die -Taste, um einen Menüpunkt auszuwählen.



Abbildung 37: Menü zum Bearbeiten bestehender Pairings

4.4.1 Pairing anzeigen

Das Submenü **Anzeigen** zeigt für jedes bestehende Pairing den Pairingblock und die zugehörigen Fingerprints¹³ an. Um in das Submenü **Anzeigen** zu gelangen, wählen Sie im Submenü **Pairing** die Option **Anzeigen** und bestätigen Sie durch Drücken der -Taste. Abbildung 38 stellt eine beispielhafte Anzeige eines Pairingblocks mit dem Fingerprint eines Zertifikates dar. Mit den Tasten  und  können Sie zwischen verschiedenen Fingerprints wählen.



Drücken Sie die

 oder die 

Taste, um sich
verschiedene



Fingerprints

anzeigen zu lassen.

(Beispielhafte

Daten)





Abbildung 38: Menü zum Anzeigen vorhandener Fingerprints

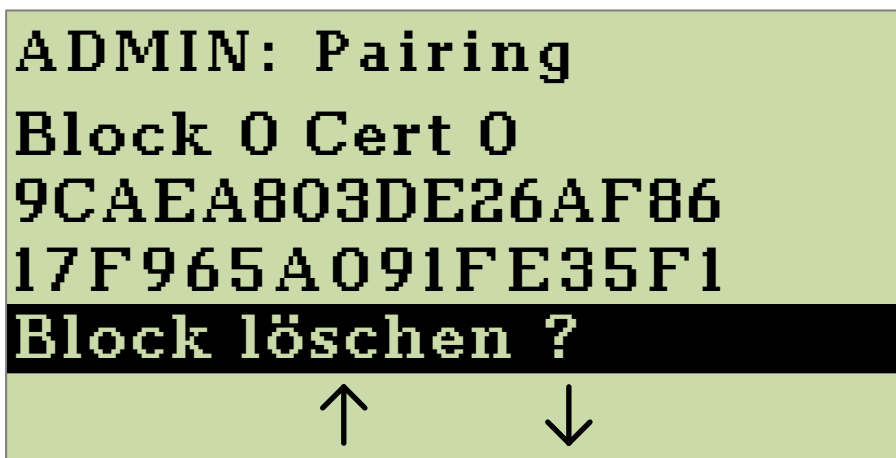
Durch Drücken der -Taste oder der -Taste können Sie in das Untermenü **Pairing** zurückkehren.

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

¹³ 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 39 stellt eine beispielhafte Anzeige eines Pairingblocks mit dem zugehörigen Fingerprint dar. Mit den Tasten  und  können Sie zwischen verschiedenen Pairingblöcken wählen. Durch Drücken der -Taste können Sie einzelne Pairingblöcke durch Auswahl und Bestätigen der Option **Block löschen ?** permanent vom Gerät entfernen.






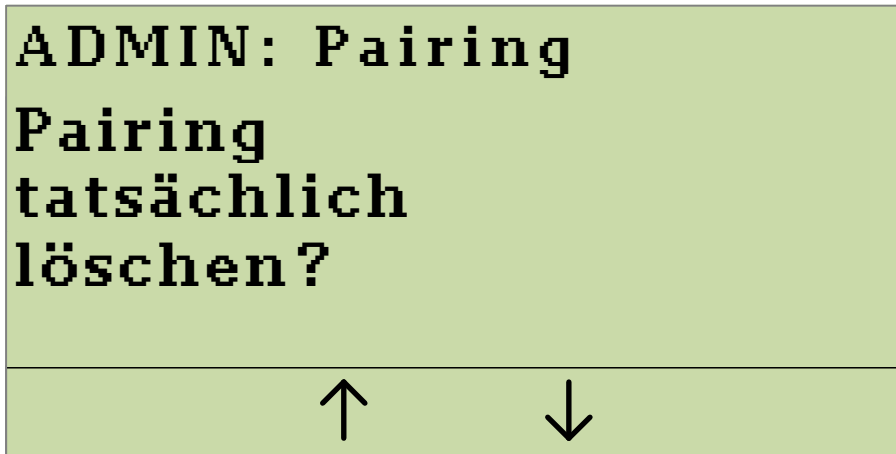
Drücken Sie die -Taste, um vorhandene Pairingblöcke zu löschen. (Beispielhafte Daten)

Abbildung 39: Menü zum Anzeigen vorhandener Pairingblöcke

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








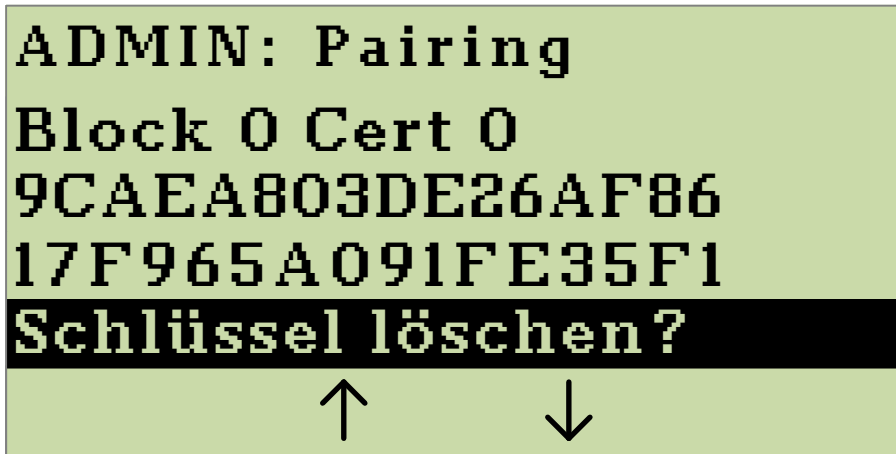
Drücken Sie die -Taste, um das Löschen eines Pairings zu bestätigen.

Abbildung 40: 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 41 stellt eine beispielhafte Anzeige eines Pairingblocks mit dem Fingerprint eines Zertifikates dar. Mit den Tasten  und  können Sie zwischen verschiedenen Fingerprints wählen. Durch Drücken der -Taste können Sie die einzelnen öffentlichen Schlüssel durch Auswahl und Bestätigen der Option **Schlüssel löschen ?** permanent vom Gerät entfernen.






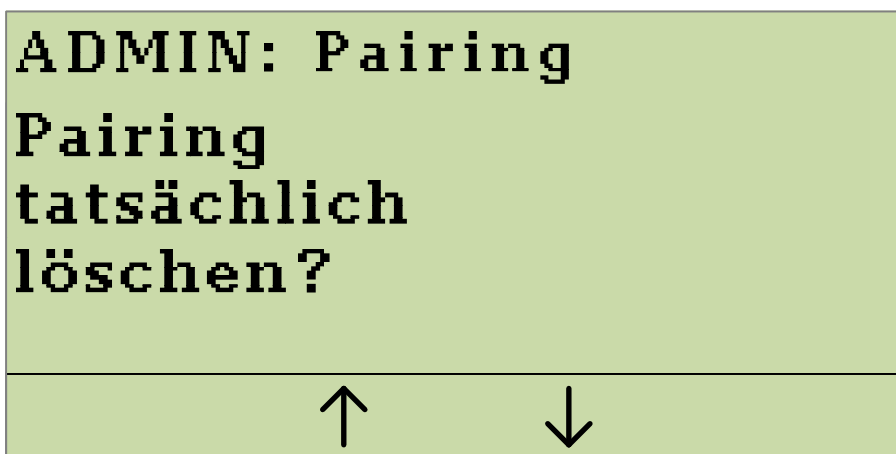
Drücken Sie die -Taste, um vorhandene Schlüssel zu löschen. (Beispielhafte Daten)

Abbildung 41: 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.







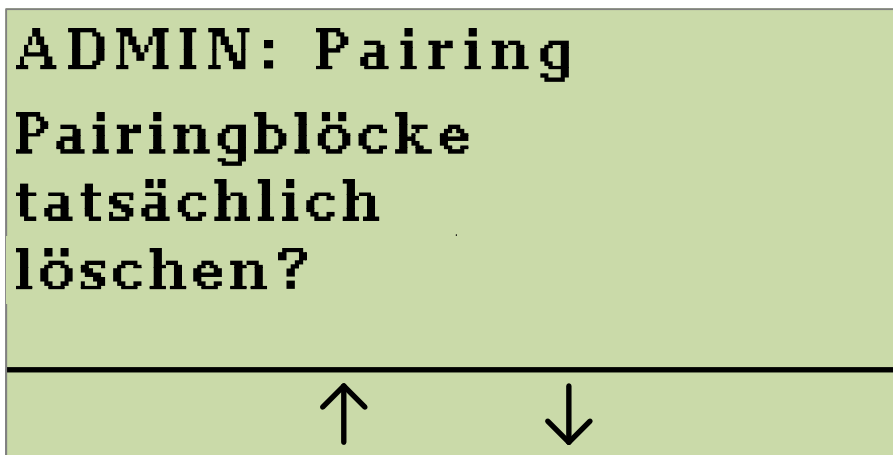
Drücken Sie die -Taste, um das Löschen eines Schlüssels aus einem Pairingblock zu bestätigen.

Abbildung 42: 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.





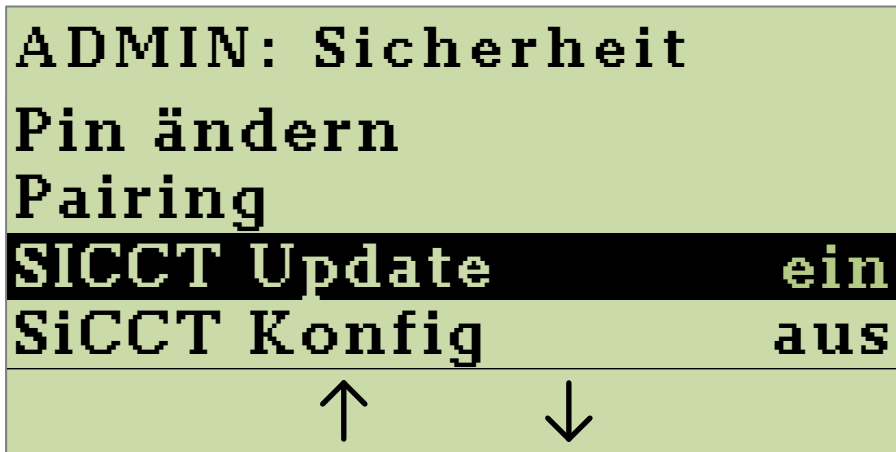
Drücken Sie die -Taste, um das Löschen der Pairings zu bestätigen.

Abbildung 43: 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 44: Anzeige des Submenüs "Sicherheit"

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


Wichtiger Hinweis zum Autoupdate

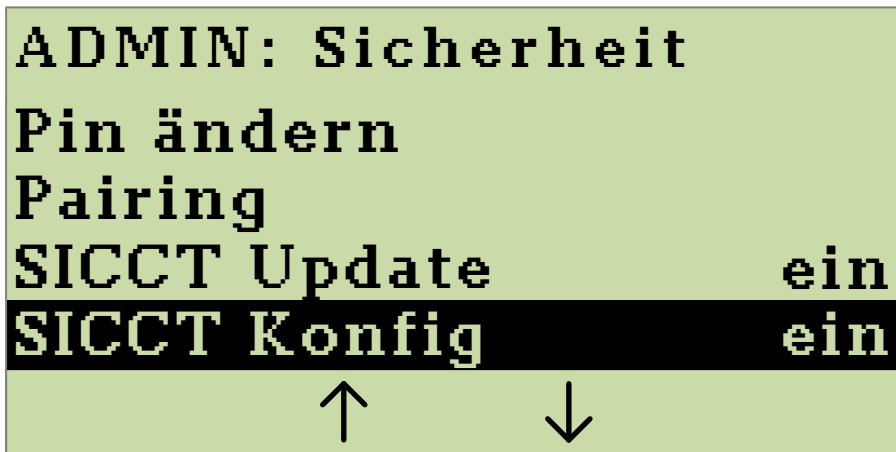


Ihre IT-Infrastruktur muss die durch die gematik spezifizierte automatische Durchführung von Updates unterstützen, damit diese Funktion genutzt werden kann. Der Administrator ist auch für den Betrieb eines Push-Servers verantwortlich und kann auf diesem eine entsprechende Firmware aussuchen die anschließend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

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

4.6 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 45: Anzeige des Submenüs "Sicherheit"

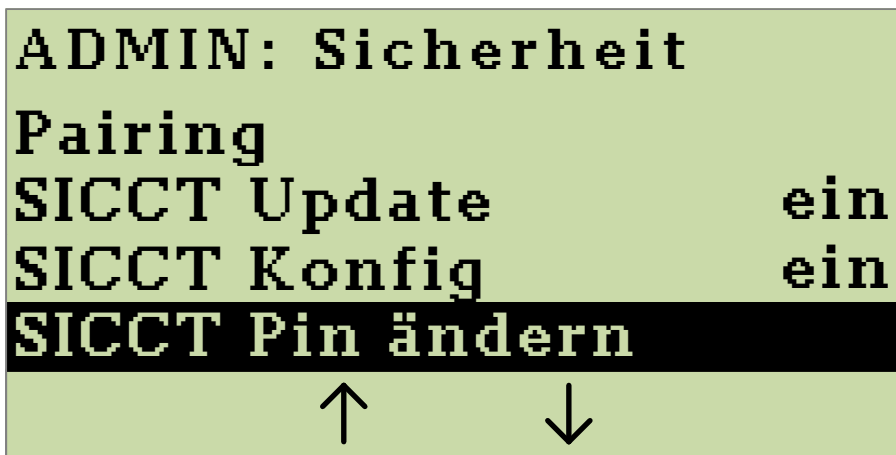
Wählen Sie die Option **SICCT Konfig** und wählen Sie durch Drücken der -Taste, ob die betreffende Option **Ein** oder **Aus** geschaltet werden soll. Unter dem betreffenden Menüpunkt wird Ihnen hinter dem Eintrag **SICCT Konfig** direkt angezeigt, welche Option gewählt wurde. Sie können das Menü über 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 Kartenterminals 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 Kartenterminal die gleiche SICCT 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 46: Anzeige des Submenüs "Sicherheit"

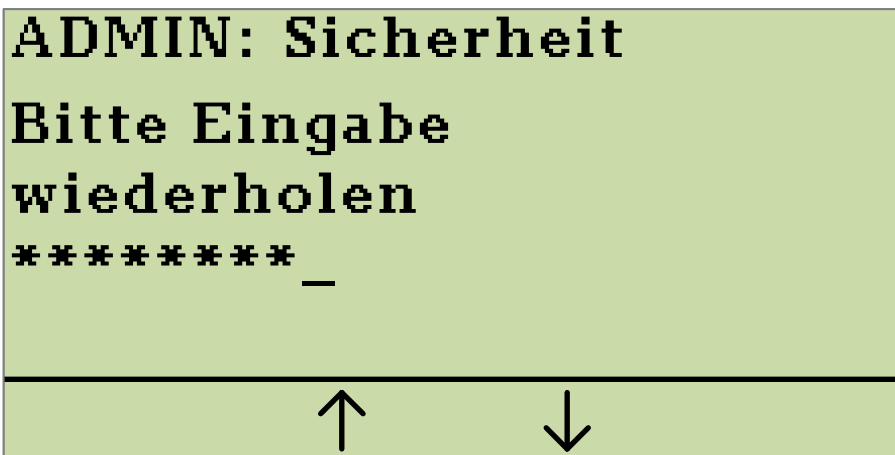
Wählen Sie die Option **SICCT Pin ändern** und bestätigen Sie durch Drücken der -Taste. Sie werden nun aufgefordert, die neue PIN einzugeben und anschließend die Eingabe zu wiederholen (s. Abbildung 47 bis Abbildung 49). Sollten die von Ihnen eingegebenen PINs nicht identisch sein, werden Sie zur erneuten 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. **Hinweis:** Verwenden Sie keine trivialen PINs wie beispielsweise 11111111 oder 12345678⁵.



Eingabe der neuen SICCT PIN.

Bestätigen Sie mit der -Taste.

Abbildung 47: Eingabe einer neuen SICCT PIN




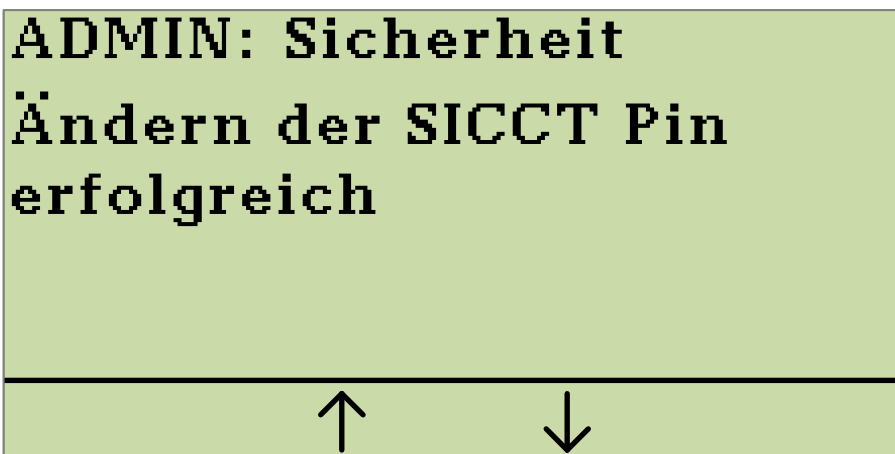
Wiederholen Sie Ihre SICCT PIN-Eingabe. Bestätigen Sie mit der -Taste.

Abbildung 48: Wiederholte Eingabe der SICCT PIN




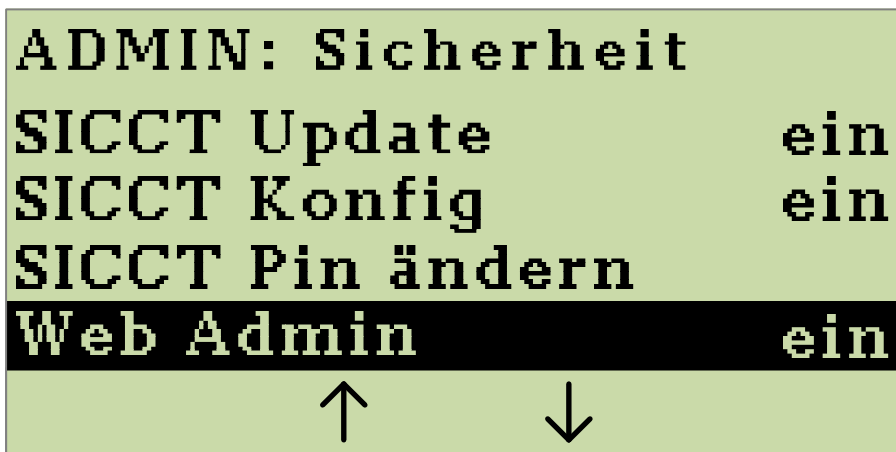
Ihnen wird anschließend eine kurze Bestätigung angezeigt und Sie kehren zum Admin-Menü zurück.

Abbildung 49: Bestätigung der erfolgreichen Änderung der SICCT PIN

4.8 Web Admin Schnittstelle ein- oder ausschalten

Ihr Kartenterminal 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 Kartenterminal aus der Ferne konfigurieren, schalten Funktionen ein oder aus und erhalten Informationen über ihr Kartenterminal und zu bestehenden Pairings.

Um Einstellungen am Kartenterminal 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.




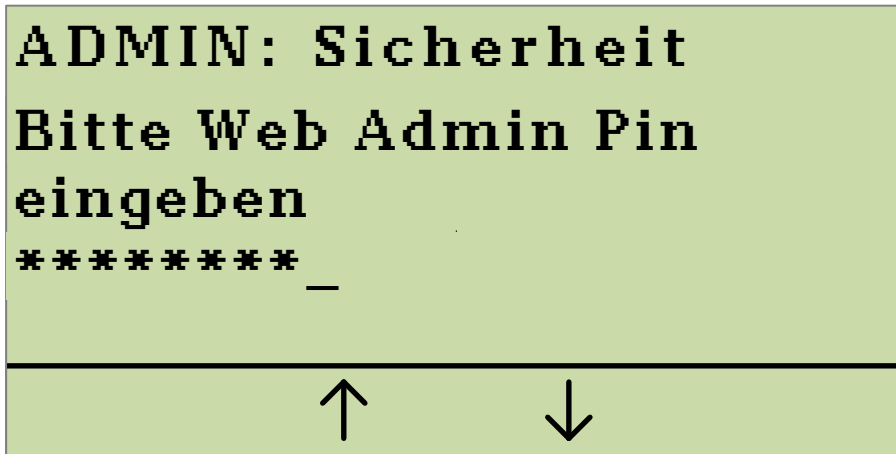
Drücken Sie die



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

Abbildung 50: Einstellung Web Admin

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 Kartenterminals anmelden zu können. Für die Web Admin PIN gelten die gleichen Vorgaben wie für die Admin PIN.






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



Abbildung 51: Eingabe der Web Admin Pin

Die Web Admin PIN muss aus **mindestens 8 und höchstens 16 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 12345678⁵**. Lesen Sie hierzu bitte auch die Hinweise zum Umgang mit der Admin PIN am Ende des Kapitels 4.1 „Admin-Menü“. Sie werden anschließend zu einer Wiederholung der PIN aufgefordert. Das erfolgreiche Setzen einer Web Admin PIN wird Ihnen mit einer entsprechenden Meldung im Display des Terminals bestätigt.

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

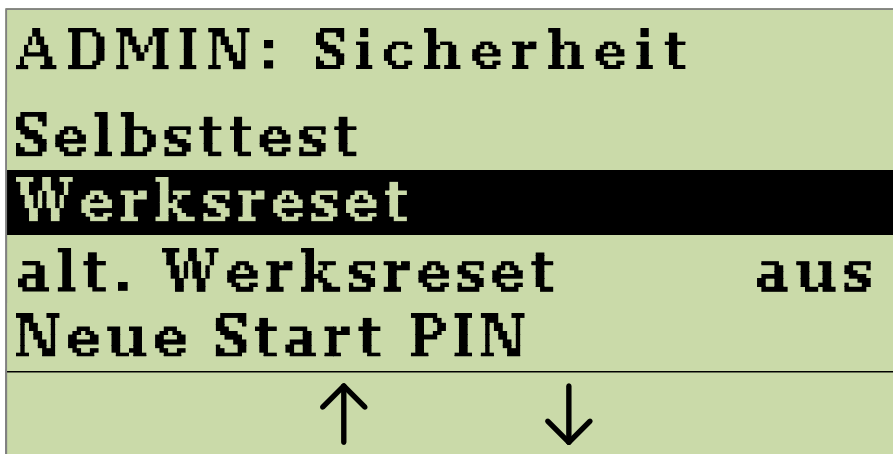
Informationen zum Zugriff auf die Weboberfläche und wie Sie damit Einstellungen an Ihrem Kartenterminal vornehmen können, entnehmen Sie bitte dem Kapitel 6 „Weboberfläche nutzen“.

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.

4.10 Werksreset ausführen

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



Drücken Sie die



-Taste, um die

Durchführung eines

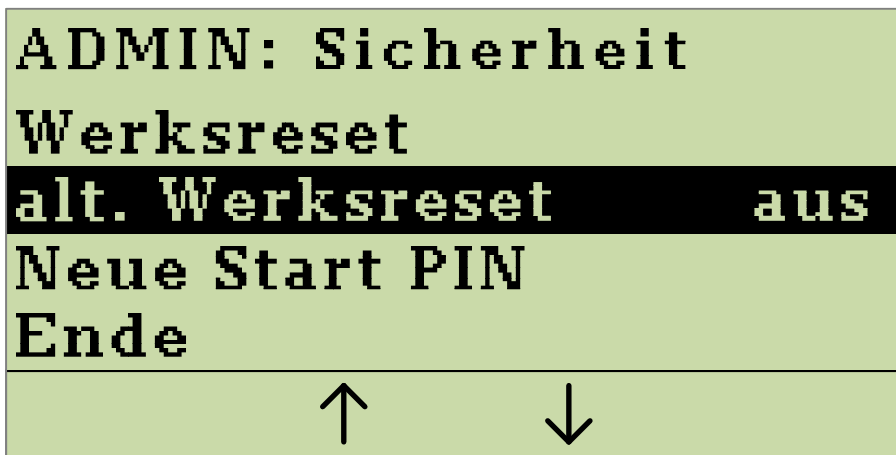
Werksresets zu

starten.

Abbildung 52: Anzeige Werksreset"

4.11 Alternativen Werksreset einschalten

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



Drücken Sie die





-Taste, um den alternativen Werksreset einzuschalten.

Abbildung 53: Anzeige alternativer Werksreset

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

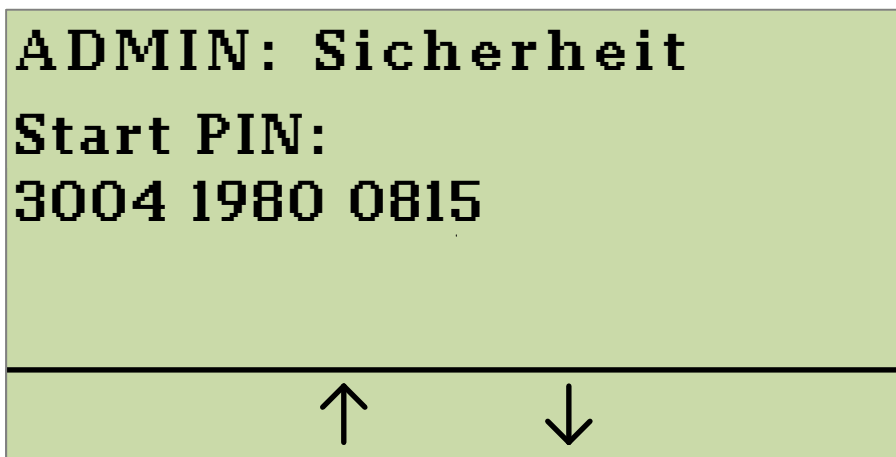
Hinweis: Sollte der alternative Werksreset nicht eingeschaltet sein und die PIN und die PUK verloren gehen, gibt es keine Möglichkeit mehr das Gerät in den Auslieferungszustand zurück zu versetzen!

4.12 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

Kartenterminal erzeugt nun eine zufällige 12-stellige PIN und zeigt Ihnen diese im Display an. **Notieren Sie die neue 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 Kapitel 1.3.4.**

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 Kapitel 4.4.4 “Alle Pairings löschen”.



Die Start PIN in dieser Abbildung ist beispielhaft.

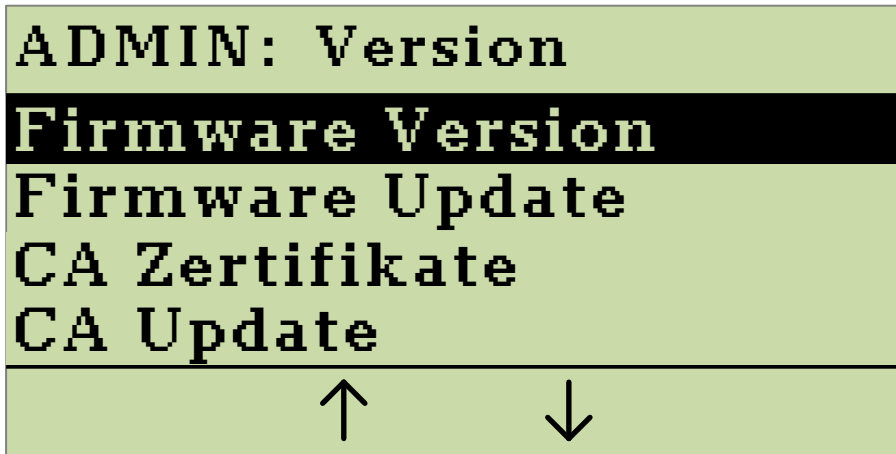
Ihr Kartenterminal zeigt die dann gültige erzeugte Start PIN an.

Abbildung 54: Anzeige des Submenüs "Sicherheit" bei Erzeugung einer neuen Start PIN

4.13 Firmware-Version und Firmware-Update

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

Für die Anzeige der aktuellen Firmware-Version lesen Sie bitte das Kapitel 4.13.1 „Anzeige der aktuellen Firmware-Version“. Um ein Firmware-Update durchzuführen, lesen Sie bitte das Kapitel 4.13.2 „Durchführung eines Firmware-Updates“








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

Abbildung 55: Anzeige des Submenüs "FW-Version"

4.13.1 Anzeige der aktuellen Firmware-Version

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

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

```
ADMIN: Version  
GERTE   GT900  
Version:  
1.22.1:2.0.0  
FWGruppe: 15
```



Abbildung 56: Anzeige der aktuellen Firmware-Version

```
ADMIN: Version  
Produkttypversion:  
1.4.0  
Produkttyp:  
EHEALTH-TERMINAL
```

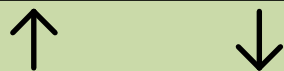


Abbildung 57: Anzeige der Produkttypversion und des Produkttyps

4.13.2 Durchführung eines Firmware-Updates

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


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

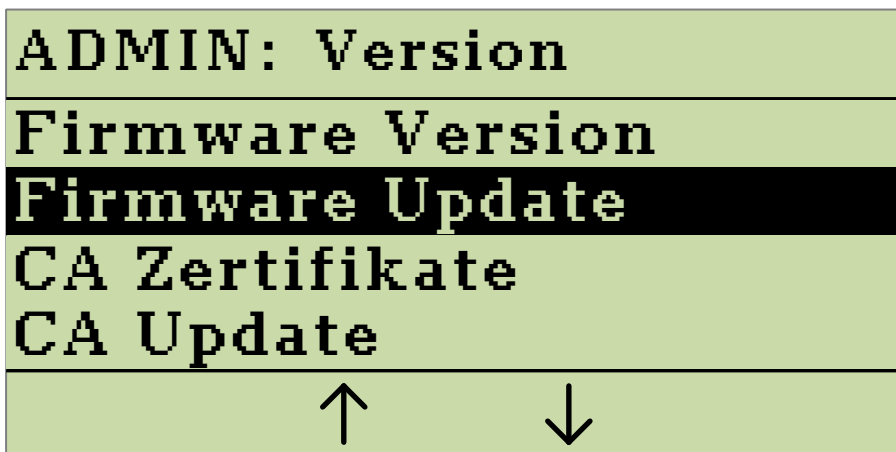
Neben der Hardware ist die Firmware ein sicherheitssensibles Element. Verwenden Sie aus diesem Grund nur zugelassene Firmware-Versionen. Spielen Sie eine neues Update ein, so kann der Vorgang nicht abgebrochen werden. Es ist nicht möglich eine alte Vorgänger-Firmware-Version, die sich nicht in der Firmwaregruppe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

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

Es sei an dieser Stelle darauf hingewiesen, dass durch die Installation einer neuen Firmware dieses Benutzerhandbuch seine Gültigkeit verlieren kann. Informieren Sie sich auf der Herstellerseite: <https://www.germantelematics.de> über Versionsänderungen 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 auf ihren Internetseiten ein Software-Tool „GT900 LAN Setup“ an, mit dem es möglich ist, ein eHealth GT900 über die LAN-Schnittstelle mit einem Firmwareupdate (oder auch Downgrade) zu versorgen. Ob Sie die Aktualisierung der Firmware lokal mittels USB-Stick oder über das Netzwerk durchführen, bleibt dabei Ihnen überlassen.

Es handelt sich bei der Update-Datei um eine Datei im Format *.bin. Der Dateiname lautet gt900-[Firmwareversion].bin, wobei [Firmwareversion] für die Versionsnummer steht, die Sie installieren wollen (siehe auch Abbildung 60). 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 Kapitel 4.1 „Admin-Menü“ beschrieben in den Administrator-Modus. Wählen Sie nun im Submenü **ADMIN: Version** die Option **Firmware Update** aus und bestätigen sie ihre Auswahl mit der -Taste (siehe Abbildung 58).

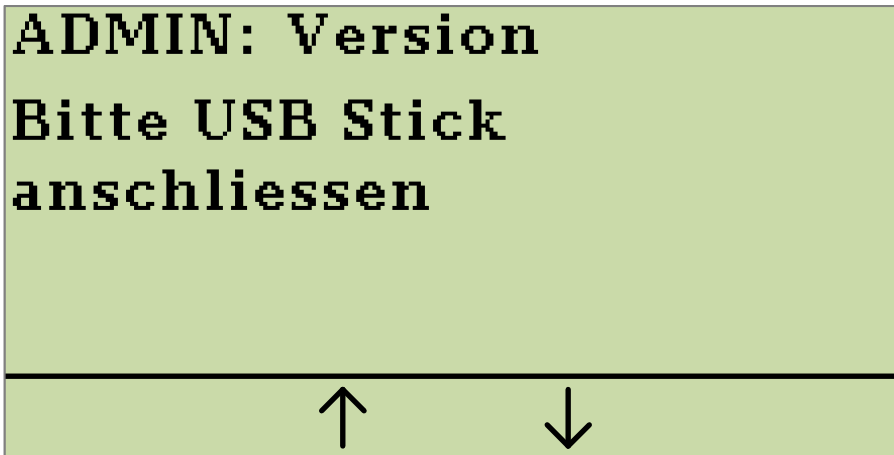


Drücken Sie die



-Taste, um das Firmwareupdate zu starten.

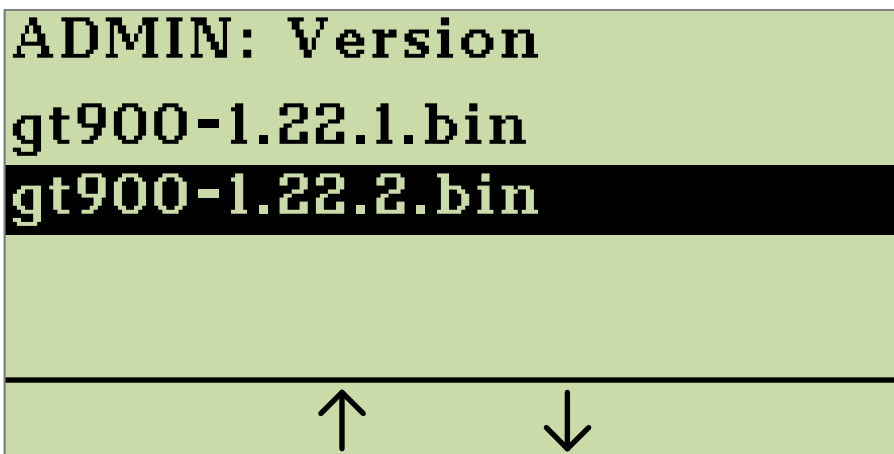
Abbildung 58: Submenü Admin:Version Firmware Update



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


Abbildung 59: Gerät ist bereit für Firmware Update

Stecken Sie den zuvor präparierten USB-Stick in die USB-Typ-A-Buchse Ihres Kartenterminals. In Abbildung 7 (Geräteanschlussbelegung) ist dieser Anschluss mit Position ① gekennzeichnet. Machen Sie sich gegebenenfalls nochmals mit den Anschlüssen des Kartenterminals vertraut (s. Kapitel 1.5 „Anschluss des Gerätes“). Nachdem der angesteckte USB-Stick nach gültigen Firmwaredateien durchsucht wurde, werden Ihnen diese zur Auswahl angezeigt.



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

Abbildung 60: 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 60). Diese wird nun in den Speicher des Gerätes kopiert (siehe Abbildung 61).

Kopiere Update

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

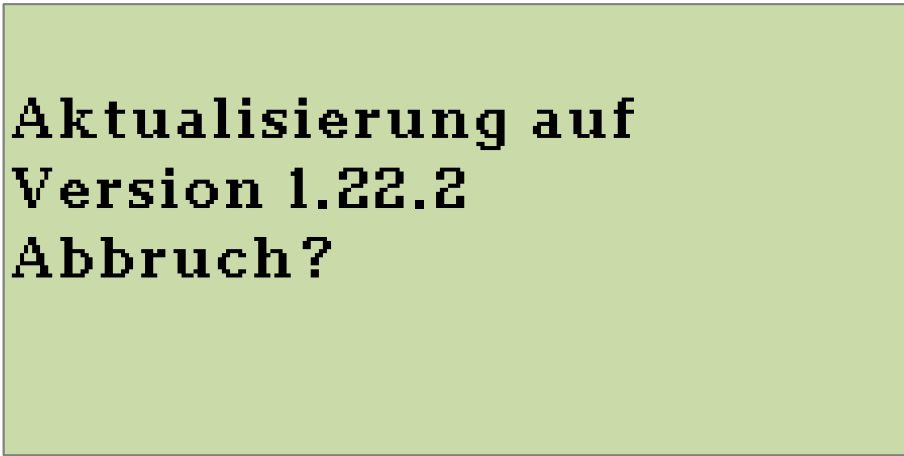
Abbildung 61: Die Firmwaredatei wird in den Speicher kopiert.

Die sich nun im Speicher befindende Firmwaredatei wird, wie in Abbildung 62 dargestellt, einer Prüfung unterzogen. Wurde eine korrekt signierte Firmware gefunden, wird Ihnen die zu installierende Firmware-Version in einer Displaymeldung angezeigt.

Verifiziere Update

Nach dem Kopiervorgang wird die Firmwaredatei einer Prüfung unterzogen.


Abbildung 62: Überprüfen des Firmware Updates



Aktualisierung auf
Version 1.22.2
Abbruch?

Abbildung 63: Anzeige der zu installierenden Firmware-Version

Im Display wird die Versionsnummer der zu installierenden Firmware angezeigt. (Beispielhafte Versionsnummer)

Überzeugen Sie sich, ob Sie die Firmware mit der angezeigten Versionsnummer installieren wollen (s.). 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 Kapitel 4.13.3 „Durchführung eines Firmware-Downgrade“. Die Versionsnummer der derzeit installierten Firmware wird Ihnen auf dem Display des einsatzbereiten Gerätes angezeigt (siehe Abbildung 21), oder Sie informieren sich über die Option **Version** im Admin-Menü.

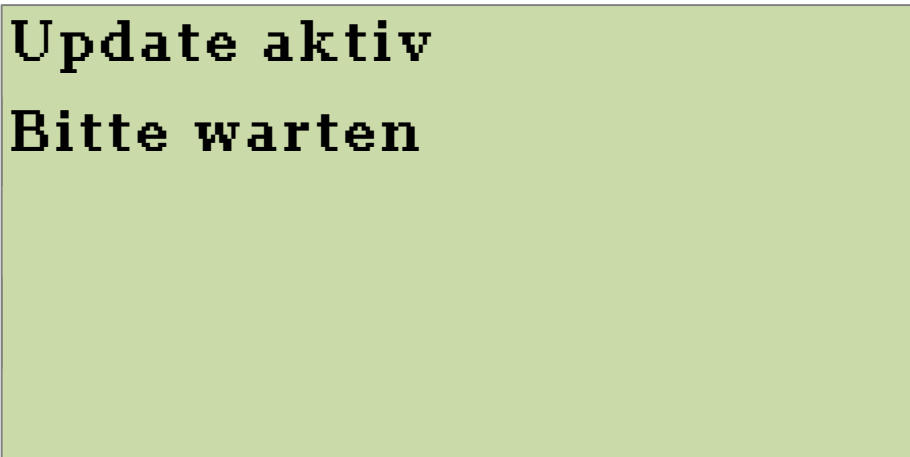
Sollte eine falsch signierte Firmware erkannt werden oder ein Verdacht auf Kompromittierung bestehen, so wird die bestehende Firmware des Gerätes nicht geändert und das Gerät startet nach einer kurzen Statusanzeige („Verifikation Fehlgeschlagen“) neu. Daraufhin können Sie wie gewohnt mit der alten Firmware weiterarbeiten.

Wurde eine korrekt signierte Firmwaredatei eingespielt, werden Sie aufgefordert, einen Freischaltcode einzugeben. Diesen erhalten Sie auf Antrag bei german telematics (s. Kapitel 10 „Kontakt“). Halten Sie dazu die Seriennummer und die MAC Adresse Ihres Terminals sowie die Versionsnummern der Ausgangsfirmware und der neuen Firmware bereit. Nach erfolgreicher Eingabe des Freischaltcodes erfolgt eine Mitteilung über den Beginn des Updateprozesses (siehe Abbildung 64). Anschließend wird für die Dauer des Updates eine Mitteilung im Display angezeigt, wie sie in Abbildung 65 zu sehen ist.



Update gestartet

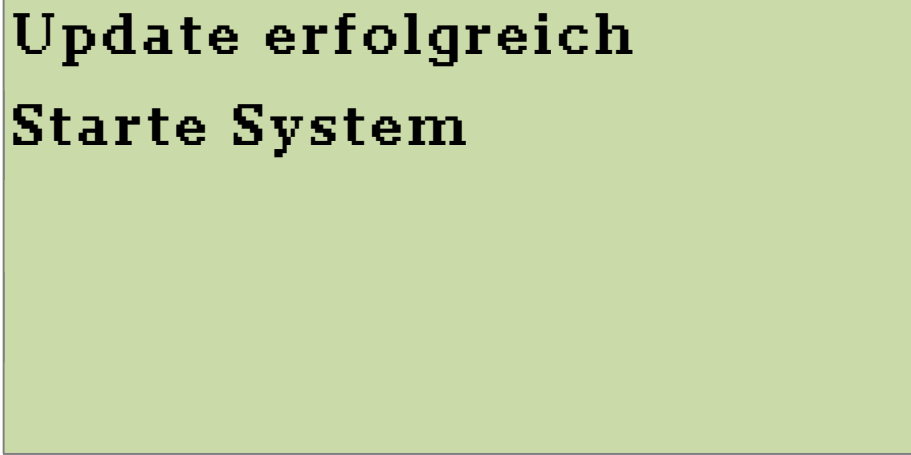
Abbildung 64: Der Updateprozess wird gestartet.



Update aktiv
Bitte warten

Während des Updatevorganges wird Ihnen diese Mitteilung angezeigt.

Abbildung 65: Das Update wird durchgeführt.



Update erfolgreich
Starte System

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

Abbildung 66: Anzeige nach erfolgreichem Firmware-Update

Nach der erfolgreichen Installation wird Ihnen dies im Display des Kartenterminals angezeigt (siehe Abbildung 66). 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.



4.13.3 Durchführung eines Firmware-Downgrade

Unter besonderen Voraussetzungen ist ein sogenanntes Firmware-Downgrade zulässig. Dies bedeutet, dass Sie einen niedrigeren Firmwarestand als den derzeit installierten auf das Gerät aufspielen können. Ein solches Vorgehen ist nur innerhalb einer sogenannten Firmwaregruppe möglich. Eine Firmwaregruppe umfasst somit die Gesamtheit aller Firmware-Versionen, zwischen denen beliebig gewechselt werden kann. Beachten Sie, dass nach dem Einspielen einer älteren Firmware-Version der störungsfreie Betrieb des Terminals innerhalb der Telematikinfrastruktur nicht garantiert werden kann. Das Einspielen eines niedrigeren Firmwarestands folgt der gleichen Vorgehensweise wie in Kapitel 4.13.2 „Durchführung eines Firmware-Updates“ beschrieben. Während der Überprüfung der Firmware wird Ihnen jedoch der folgende Hinweis angezeigt werden:


**Aktualisierung auf
Version 1.20.9.
Achtung Downgrade!
S. Handbuch. Abbruch?**

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

Abbildung 67: Abfrage zur Fortführung des Downgrades

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

4.13.4 Speichern von Update-Freischaltcodes

Um die automatische Durchführung von Firmwareupdates zu ermöglichen, können Sie einen Freischaltcode für ein zukünftiges Update im Update-PIN cache speichern. Drücken Sie dazu die -Taste bis die Eingabeaufforderung für den Freischaltcode erscheint (s. Abbildung 68). Wenn Sie keinen oder einen falschen Freischaltcode speichern, wird das Kartenterminal während des Updatevorgangs (s. Kapitel 4.13.2) zur Eingabe des Freischaltcodes auffordern, sofern dieser für die Durchführung des Updates erforderlich ist.

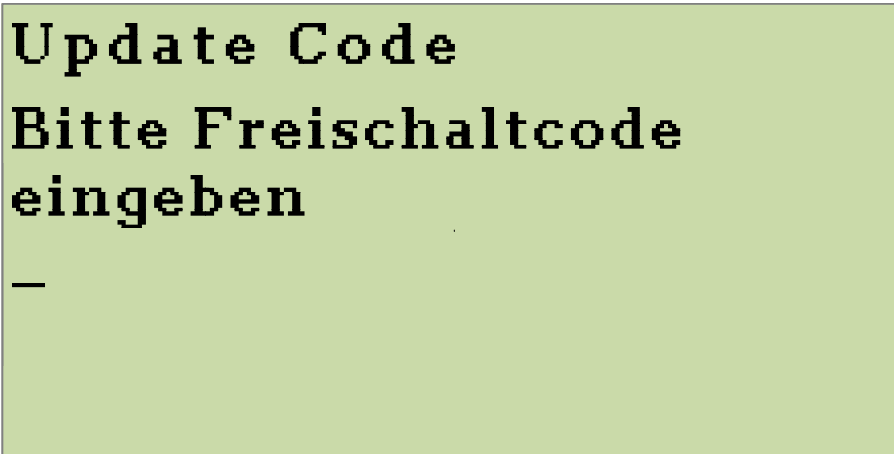






Abbildung 68: Eingabeaufforderung für den Freischaltcode

Geben Sie nun den Freischaltcode ein und bestätigen Sie Ihre Eingabe mit der -Taste. Durch Drücken der -Taste können Sie Ihre Eingabe korrigieren und mit der -Taste abbrechen. Um einen gespeicherten Freischaltcode anzuzeigen, halten Sie abermals die -Taste gedrückt (s. Abbildung 69, abgebildeter Freischaltcode ist beispielhaft). In dieser Ansicht können Sie den Freischaltcode nochmals verändern.

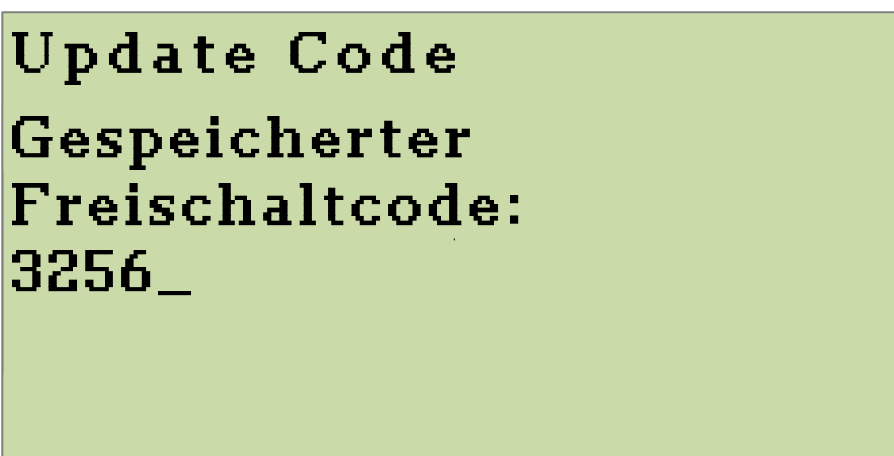






Abbildung 69: Anzeige des gespeicherten Freischaltcodes

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

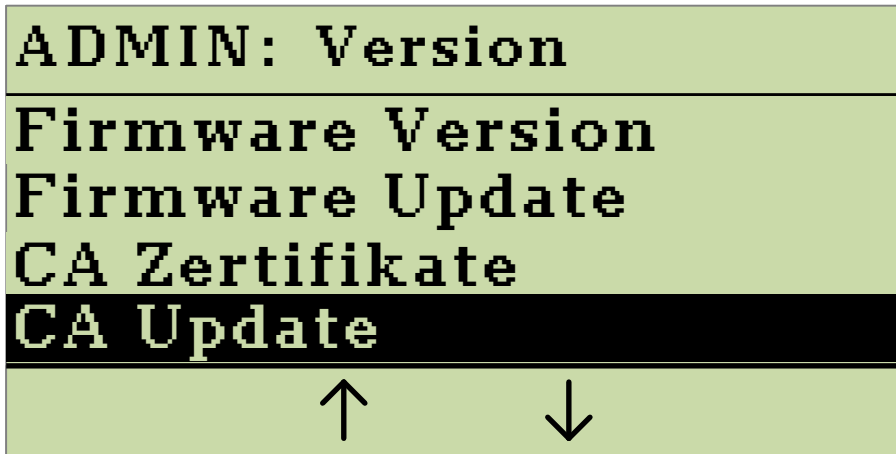
4.13.5 Anzeigen der installierten CA-Zertifikate

Um die installierten CA-Zertifikate anzuzeigen, wählen sie im Admin-Menü die Option **Version** und danach **CA Zertifikate** (siehe auch Abbildung 70).

4.13.6 Update der CA-Liste

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

Schließen Sie, wie bei einem Firmwareupdate auch, einen USB-Stick mit den Zertifikatdateien an Ihr Kartenterminal an. Lesen Sie hierzu ggf. das Kapitel 4.13.2 „Durchführung eines Firmware-Updates“. Mit den Tasten  und  können Sie zwischen verschiedenen Zertifikatdateien wählen. Durch Drücken der -Taste bestätigen Sie die Installation der im Display hervorgehobenen Zertifikatdatei (siehe Abbildung 71). 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.




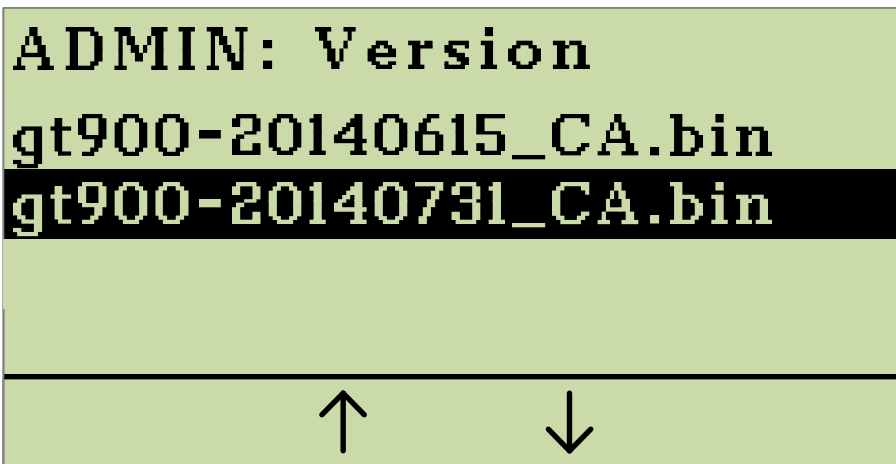
Drücken Sie die -Taste, um die CA Liste zu aktualisieren.

Abbildung 70: Anzeige des Submenüs "Version"; CA Update





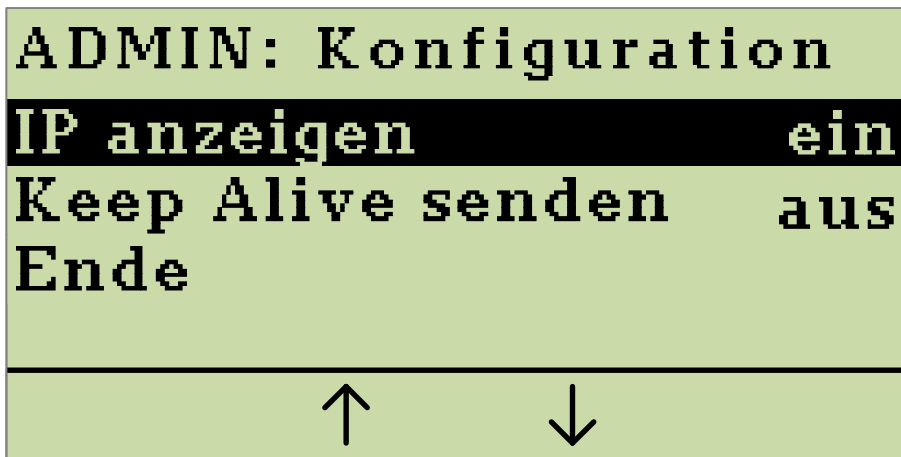
Wählen Sie eine Datei aus und drücken Sie die -Taste, um die Zertifikatdatei zu installieren. (Beispielhafte Daten)

Abbildung 71: Wählen Sie die zu installierende Zertifikatdatei aus.

4.14 Aktuelle IP-Adresse anzeigen

Sie können sich in der Hauptdisplayanzeige (Abbildung 21) wahlweise die aktuell vergebene IP-Adresse des Kartenterminals 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.

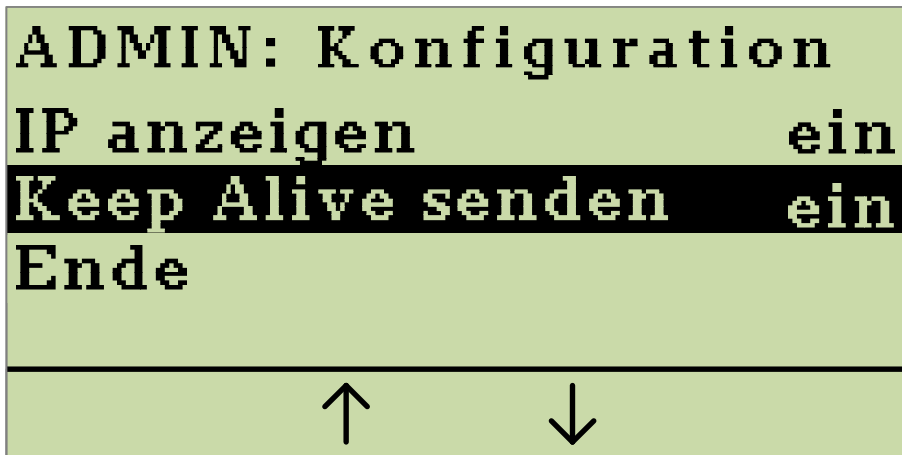
Abbildung 72: Anzeige des Submenüs "Konfiguration"; IP anzeigen

Mit den Tasten  und  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.

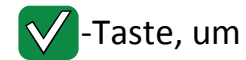
4.15 Keep Alive senden

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

Taste. Auf dem Display wird Ihnen das Submenü **ADMIN: Konfiguration** angezeigt.





Drücken Sie die



Keep Alive ein- oder auszuschalten.

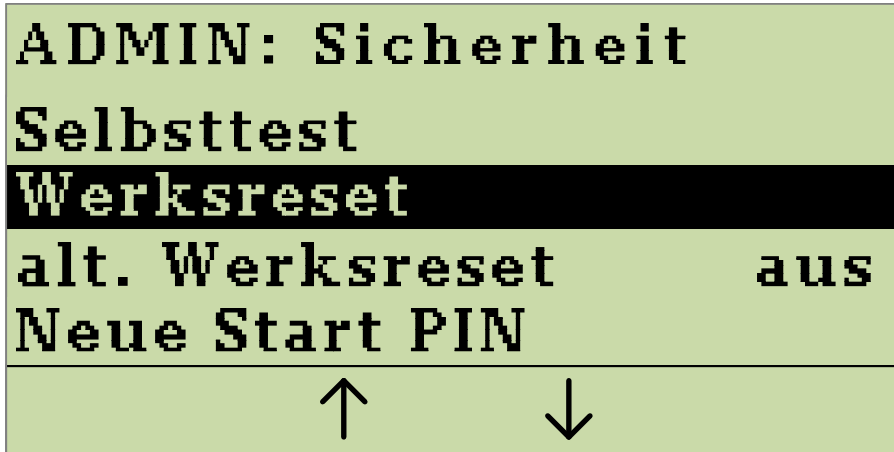
Abbildung 73: Anzeige des Submenüs "Konfiguration"; Keep Alive

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

5 Gerät zurücksetzen

5.1 Zurücksetzen mit Kenntnis der Admin PIN

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







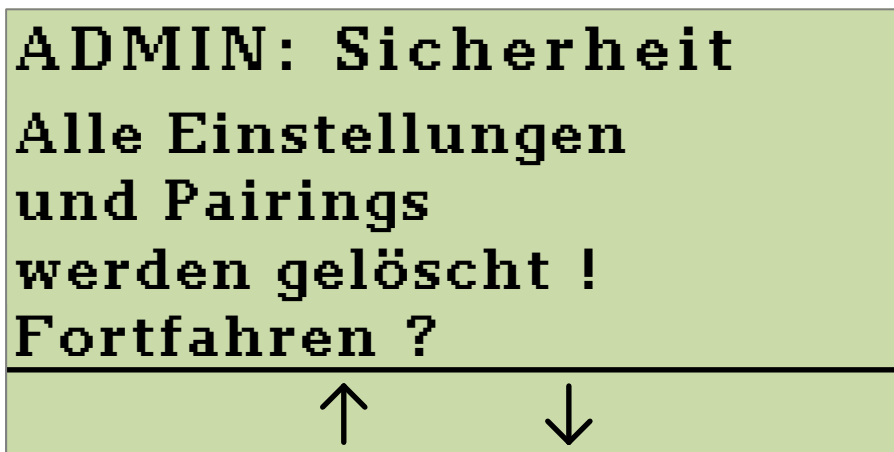
Drücken Sie die -Taste, um einen Werksreset auszuführen.


Abbildung 74: Anzeige des Submenüs "Sicherheit"

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



Sicherheitsabfrage beim Zurücksetzen des Gerätes in den Auslieferungszustand.



Abbildung 75: Sicherheitsabfrage beim Werksreset

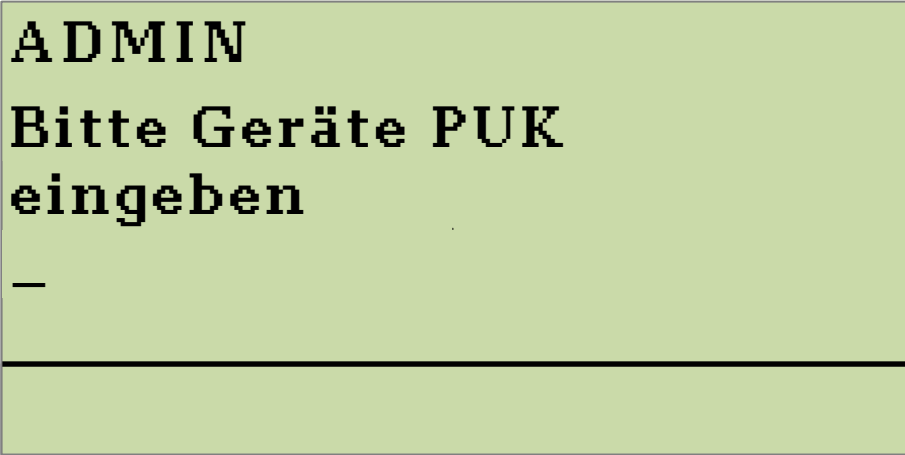
Haben Sie die Sicherheitsabfrage durch Drücken der -Taste bestätigt, wird das Gerät in den Auslieferungszustand zurückversetzt.

5.2 Zurücksetzen ohne Kenntnis der Admin PIN

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



5.2.1 Zurücksetzen mittels PUK


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



ADMIN
Bitte Geräte PUK
eingeben
—

Abbildung 76: Eingabeaufforderung des PUK

Wenn Sie den PUK korrekt eingegeben haben werden Sie gebeten, das Zurücksetzen des Gerätes in den Auslieferungszustand zu bestätigen, so wie es in Abbildung 75 dargestellt ist. Sie können diesen Dialog durch Drücken der -Taste bestätigen oder durch Betätigen der -Taste abbrechen. Sollten Sie den PUK dreimal falsch eingeben, ist ein erneuter Eingabeversuch erst nach einem gewissen Zeitraum möglich. Bei mehreren Falscheingaben verlängert sich der Zeitraum entsprechend,

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

5.2.2 Zurücksetzen ohne Kenntnis des PUK

Um das Kartenterminal ohne Kenntnis der Admin PIN und des PUK in den Auslieferungszustand zurückzusetzen, muss der alternative Werksreset gemäß Kapitel 4.11 „Alternativen Werksreset einschalten“ vom Administrator aktiviert worden sein.

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

6 Weboberfläche nutzen

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

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

Wie Sie diese Weboberfläche zur Benutzung freischalten, erfahren Sie im Kapitel 4.8 „Web Admin Schnittstelle ein- oder ausschalten“. Schalten Sie die Weboberfläche nur dann ein, wenn das Netzwerk unter Ihrer vollständigen Kontrolle steht.

Um auf die Weboberfläche zugreifen zu können, benötigen Sie einen Computer mit installiertem Webbrowser. Zudem muss sich das Kartenterminal im selben Netzwerk befinden, wie der Computer, von dem Sie auf das Kartenterminal zugreifen möchten. Bitte beachten Sie, dass Ihr Webbrowser zum erfolgreichen Verbindungsaufbau die Transportschichtssicherheit TLS 1.2 unterstützen muss. Ein erfolgreicher Verbindungsaufbau wurde mit den folgenden Webbrowsern getestet:

- Google Chrome [Version 81.0.4044.138]
- Firefox [Version 75.0]
- Internet Explorer [11.0.9600.19596]

Geben Sie Folgendes in die Adresszeile Ihres Webbrowsers ein:

https://[IP-Adresse des Kartenterminals]

Wie Sie sich die IP-Adresse im Display des Terminals anzeigen lassen können, entnehmen Sie ggf. dem Kapitel 4.14 „Aktuelle IP-Adresse anzeigen“.

Abbildung 78 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 Kartenterminal zur Kommunikationsabsicherung (TLS 1.2) das Zertifikat einer eingelegten gSMC-KT verwendet. Da dieses Zertifikat den Internetzertifizierungsstellen unbekannt ist, wird korrekterweise vor einem Aufbau der Verbindung gewarnt. Stellen Sie daher zunächst sicher, dass keine Manipulation an der gSMC-KT vorgenommen wurde und die SIM-Slotversiegelung intakt ist. Sie können die Zertifikatwarnung nun in den meisten Browsern manuell übergehen und dadurch einen Verbindungsaufbau einleiten. Ein entsprechender Dialog ist in Abbildung 77 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 192.168.111.187 (unsicher)“.

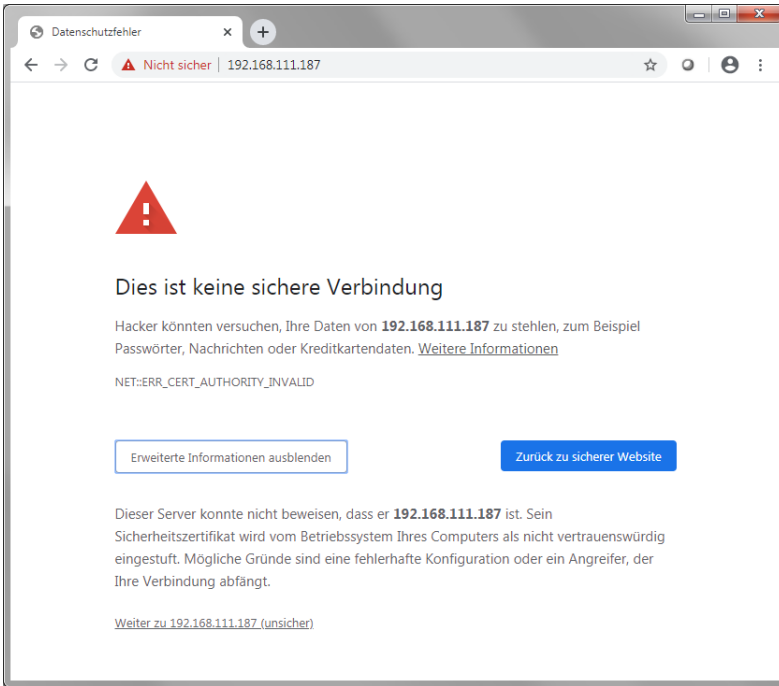


Abbildung 77: Mögliche Anzeige eines Zertifikatfehlers im Browser.

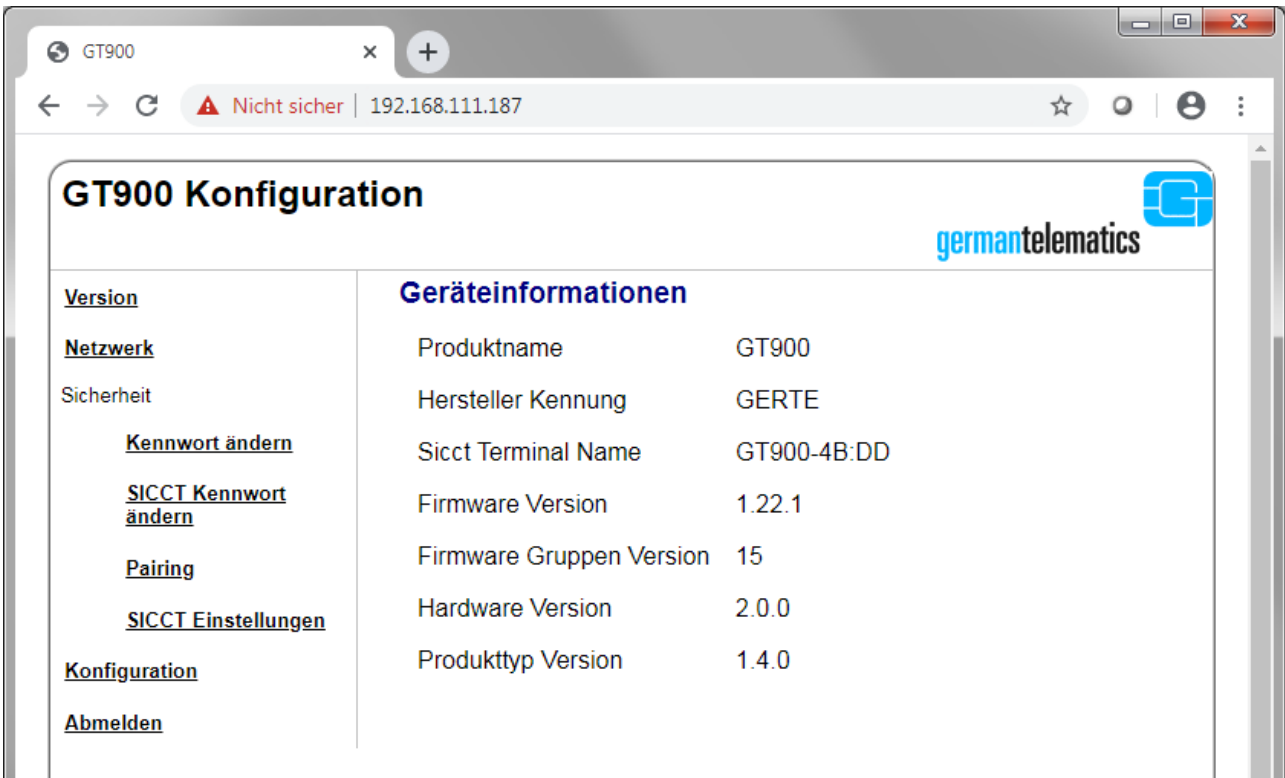


Abbildung 78: Weboberfläche des Kartenterminals nach dem Verbindungsaufbau.

Die Weboberfläche bietet Ihnen nach Eingabe Ihrer Web Admin PIN (siehe Abbildung 79) 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 Kartenterminal vergebene Web Admin PIN ein (siehe Kapitel 4.8).



Bitte Kennwort eingeben

Kennwort:

Abbildung 79: 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 Kartenterminals angezeigt.



Abbildung 80: Netzwerkkonfiguration 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 Kartenterminals beschränkt und können daher auch Kennwörter anstelle der sonst üblichen PIN vergeben.

Auch das Kennwort muss aus mindestens 8 und höchstens 16 Zeichen bestehen, kann nun aber auch Buchstaben und Sonderzeichen enthalten. Für das Kennwort werden die Zeichen der UTF-8 Zeichentabelle akzeptiert. Sie können jedoch keine

Teilzeichenkette von „Administrator“ als Bestandteil des Passworts wählen. So wird z.B. „Admin123“ als Passwort abgelehnt.



Abbildung 81: 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 trivialen⁵ 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, mindestens eine Zahl enthalten müssen.

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 Kartenterminals 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.

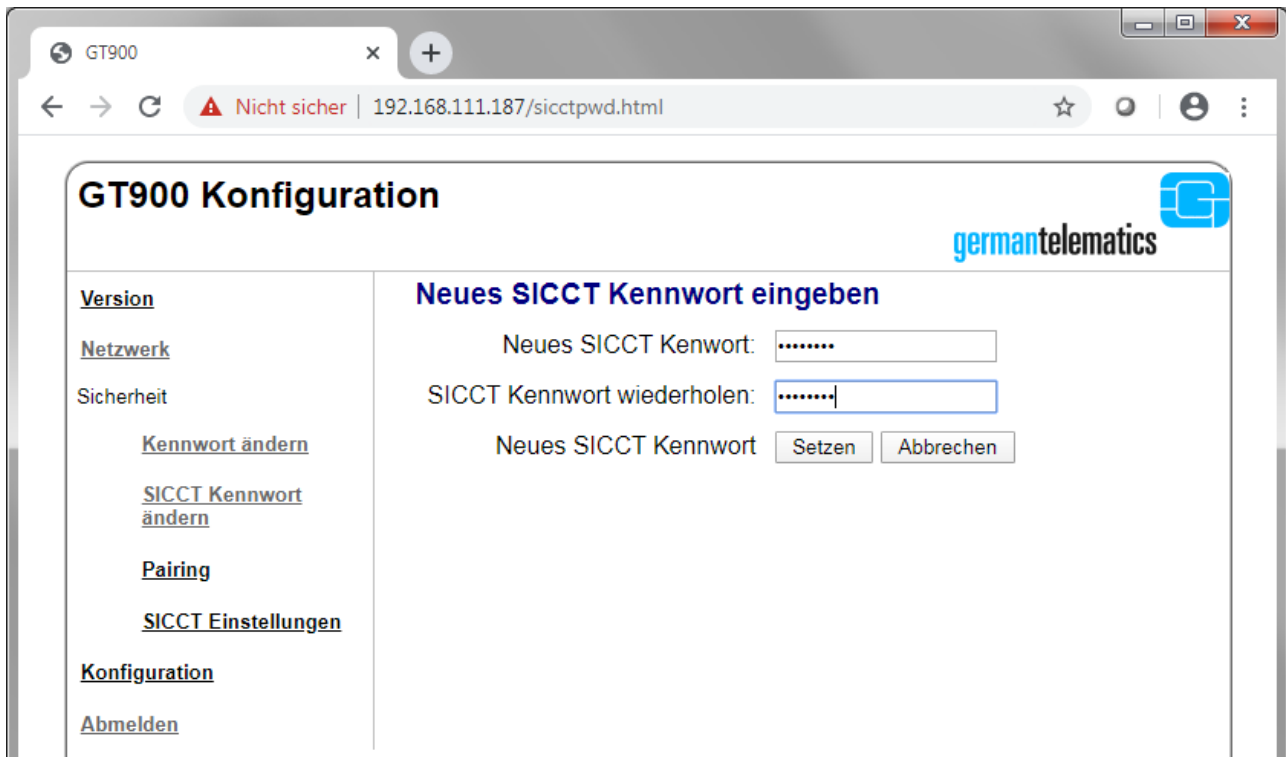


Abbildung 82: Setzen eines neuen SICCT Kennwortes

6.4 Pairings einsehen und löschen

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

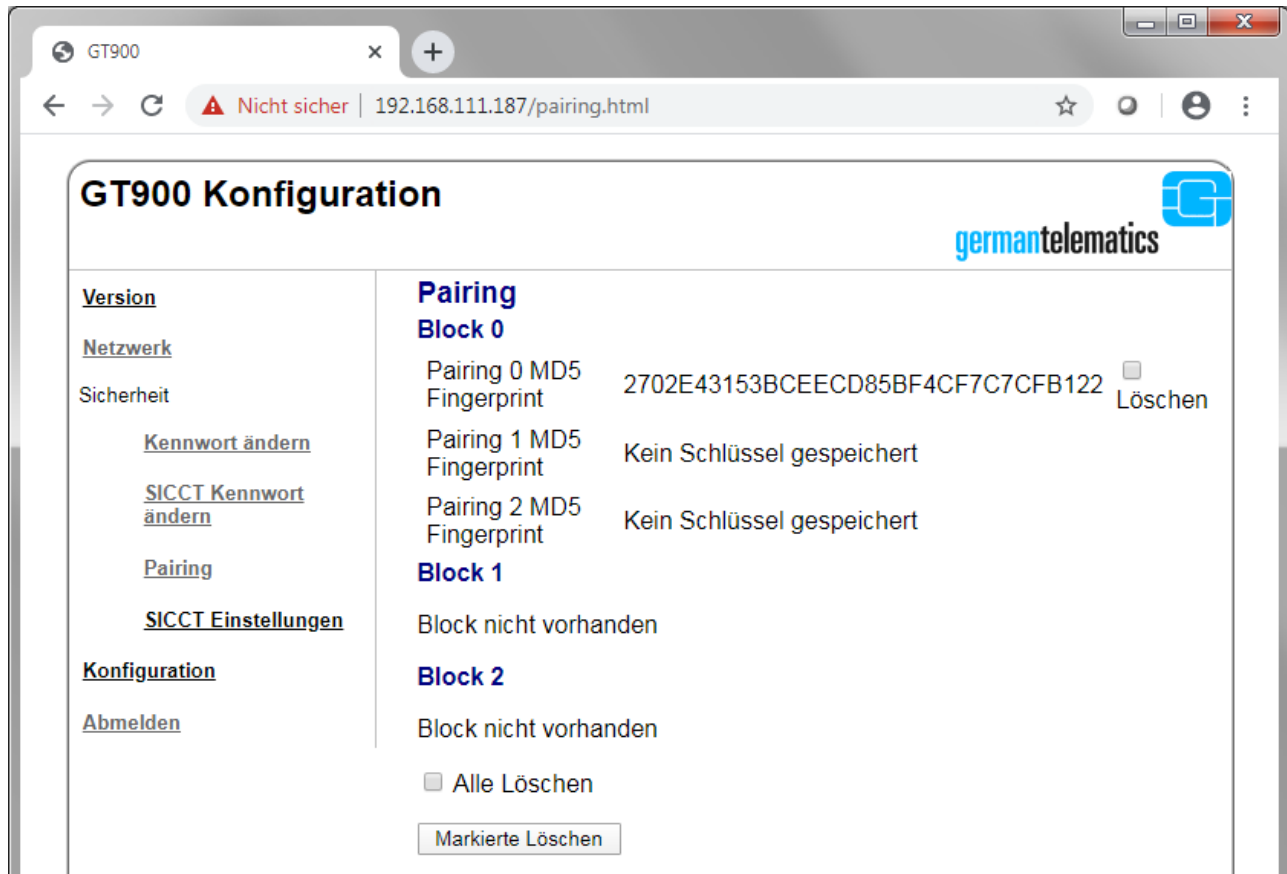


Abbildung 83: Einsehen der Pairings des Kartenterminals

6.5 SICCT Einstellungen

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

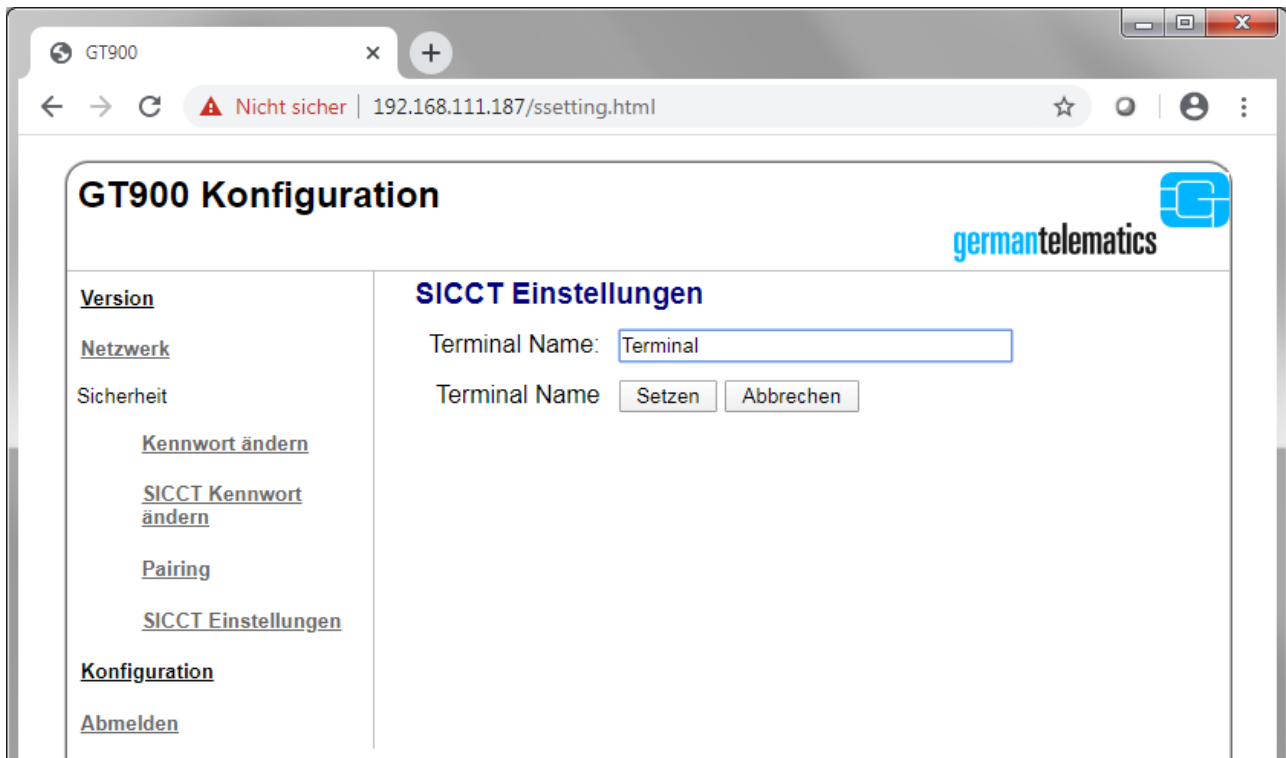


Abbildung 84: SICCT Einstellungen vornehmen

6.6 Konfiguration

Um die Keep Alive-Funktion zu nutzen, aktivieren Sie die entsprechende Checkbox. Zur Funktionsweise von Keep Alive lesen Sie bitte Kapitel 4.15 „Keep Alive senden“.

Sie können sich in der Hauptdisplayanzeige (Abbildung 21) wahlweise die aktuell vergebene IP-Adresse des Kartenterminals anzeigen lassen. Um die IP-Adresse anzuzeigen, aktivieren Sie die entsprechende Checkbox. Klicken Sie anschließend auf „Übernehmen.“

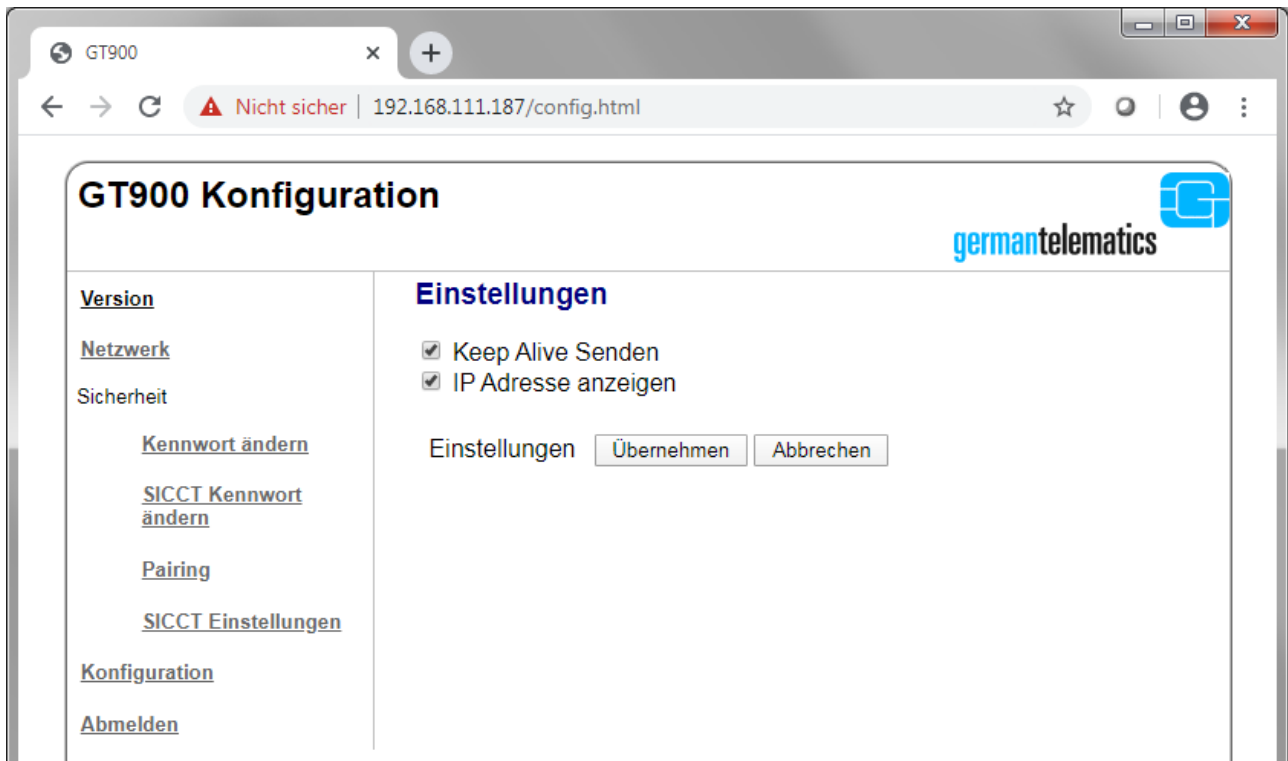


Abbildung 85: Gerätekonfiguration vornehmen


7 Qualifizierte elektronische Signaturen

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

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

8 Produktregistrierung

Auf der hinteren Umschlagseite dieses Benutzerhandbuches befindet sich ein Registrierungsformular. Durch das Ausfüllen und Zurücksenden dieses Registrierungsformulars registrieren Sie Ihr Kartenterminal, 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
<p>Nach einem Neustart oder während des Betriebs erscheint eine der folgenden Statusanzeigen:</p> <div data-bbox="148 719 549 920" style="background-color: #d9ead3; padding: 5px; margin-bottom: 5px;"> Fehler Systemfehler </div> <div data-bbox="148 943 549 1144" style="background-color: #d9ead3; padding: 5px; margin-bottom: 5px;"> Fehler Einbruchsicherung Gerät überprüfen </div> <div data-bbox="148 1167 549 1368" style="background-color: #d9ead3; padding: 5px; margin-bottom: 5px;"> Fehler Tastaturfehler Gerät überprüfen </div> <div data-bbox="148 1391 549 1592" style="background-color: #d9ead3; padding: 5px;"> Fehler Selbsttest fehlgeschlagen </div>	<p>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.</p>	<p>Kontaktieren Sie einen zertifizierten Techniker oder den Hersteller. Geben Sie die Fehlerbeschreibung an und erbitten Sie weitere Hilfe.</p>



Fehlerbeschreibung	Ursache	Behebung
<p>Es erscheint folgende Statusanzeige:</p> <div data-bbox="148 338 549 539" style="border: 1px solid black; padding: 5px; background-color: #d9ead3;"> <p>Fehler Sim nicht gesteckt</p> </div>	<p>Eine der SIM-Karten aus den am Gerät rechtsseitigen SIM-Slots wurde, während das Gerät mit der Stromversorgung verbunden ist, entfernt. Eine Sicherheitsfunktion hat dies erkannt und informiert Sie darüber.</p>	<p>Stecken Sie die SIM-Karte und/ oder den Simkartenträger wieder in den SIM-Slot. Stellen Sie sicher, dass sich in beiden SIM-Slots des Gerätes die Simkartenträger befinden. Starten Sie das Gerät mit der -Taste neu. Sie benötigen dann die Start PIN um das Gerät weiter zu betreiben. Sollten weiterhin Probleme auftauchen, so kontaktieren Sie einen zertifizierten Techniker oder den Hersteller. Geben Sie die Fehlerbeschreibung an und erbitten Sie weitere Hilfe.</p>
<p>Das Gerät lässt sich nicht in den Administrator-Modus schalten.</p>	<p>Sie haben die Admin PIN mehrfach falsch eingegeben. Der Zugang zum Administrator-Menü ist für eine bestimmte Zeit gesperrt.</p>	<p>Die Sperrzeit wird im Display angezeigt. Danach ist der Administrator-Modus wieder freigeschaltet. Stellen Sie sicher, dass Sie die richtige PIN verwenden. Lesen Sie hierzu auch Kapitel 4.1 „Admin-Menü“ und dort insbesondere Tabelle 2.</p>
	<p>Die -Taste ist defekt.</p>	<p>Kontaktieren Sie einen zertifizierten Techniker oder den Hersteller. Geben Sie die Fehlerbeschreibung an, und erbitten Sie weitere Hilfe.</p>
<p>Es erscheint eine der folgenden Statusanzeigen:</p> <div data-bbox="148 1308 549 1509" style="border: 1px solid black; padding: 5px; background-color: #d9ead3;"> <p>Fehler: Verifikation fehlgeschlagen</p> </div> <div data-bbox="148 1532 549 1733" style="border: 1px solid black; padding: 5px; background-color: #d9ead3;"> <p>Verifikation fehlgeschlagen</p> </div> <div data-bbox="148 1756 549 1957" style="border: 1px solid black; padding: 5px; background-color: #d9ead3;"> <p>Achtung Keine Firmwaregruppe in Updatedatei!</p> </div>	<p>Die Firmware, die Sie zu installieren versuchen, ist beschädigt.</p>	<p>Laden Sie die entsprechende FW-Datei erneut von der Herstellerseite.</p>

Fehlerbeschreibung	Ursache	Behebung
<p>Das Firmware-Update wird abgebrochen. Es erscheint folgende Statusanzeige:</p> <div data-bbox="148 414 549 613" style="background-color: #d9ead3; padding: 10px; border: 1px solid #d9ead3;"> <p>Falsche Version</p> </div>	<p>Sie versuchen eine Firmware zu installieren, die in der aktuellen Firmwaregruppe nicht gelistet ist.</p>	<p>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.</p>
<p>Nach Eingabe des Freischaltcodes für ein Update erscheint folgende Meldung:</p> <div data-bbox="148 792 549 992" style="background-color: #d9ead3; padding: 10px; border: 1px solid #d9ead3;"> <p>Ungültiger Code Update abgebrochen</p> </div>	<p>Sie haben dreimal einen falschen Freischaltcode eingegeben.</p>	<p>Geben Sie den korrekten Freischaltcode ein, den Sie von german telematics erhalten haben.</p> <p>Überprüfen Sie, ob die Sie die Daten zur Erlangung des Freischaltcodes richtig weitergegeben haben und beantragen Sie einen neuen Freischaltcode.</p>
<p>Während eines Firmwareupdates oder beim Neustart des Terminals erscheint folgende Statusanzeige:</p> <div data-bbox="148 1173 549 1373" style="background-color: #d9ead3; padding: 10px; border: 1px solid #d9ead3;"> <p>Fehler Update Fehler</p> </div>	<p>Der Firmwareupdateprozess wurde mit einem Fehler beendet.</p>	<p>Kontaktieren Sie einen zertifizierten Techniker oder den Hersteller. Geben Sie die Fehlerbeschreibung an und erbitten Sie weitere Hilfe.</p>
<p>Beim Neustart des Terminals erscheint folgende Statusanzeige:</p> <div data-bbox="148 1516 549 1715" style="background-color: #d9ead3; padding: 10px; border: 1px solid #d9ead3;"> <p>Unvollständiges Update gefunden</p> </div>	<p>Während eines Firmwareupdates wurde die Stromversorgung des Terminals unterbrochen. Beim Neustart des Terminals wird das unvollständig durchgeführte Update erkannt und erneut vom USB-Stick geladen.</p>	<p>Stecken Sie den USB-Stick mit der ursprünglichen Updatedatei, welche beim unterbrochenen Firmwareupdate genutzt wurde, in den USB Typ A Anschluss des Terminals.</p>

Fehlerbeschreibung	Ursache	Behebung
<p>Am Beginn des Updates oder beim Neustart des Terminals erscheint eine der folgenden Statusanzeigen:</p> <div data-bbox="148 416 549 622" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Kein Update gefunden</p> </div> <div data-bbox="148 645 549 851" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Fehler Update konnte nicht geladen werden.</p> </div> <div data-bbox="148 873 549 1079" style="border: 1px solid black; padding: 5px;"> <p>Keine Datei für Update gefunden</p> </div>	<p>Es ist kein USB-Stick gesteckt, auf dem USB-Stick befindet sich keine Firmwareupdate-datei oder der USB-Stick wurde während des Kopiervorgangs der Firmwareupdatedatei aus dem Terminal gezogen.</p> <p>Während eines Firmwareupdates wurde die Stromversorgung des Terminals unterbrochen. Beim Neustart des Terminals wird das unvollständig durchgeführte Update erkannt und erneut vom USB-Stick geladen. Es ist kein USB-Stick gesteckt, auf dem USB-Stick befindet sich keine Firmwareupdatedatei oder der USB-Stick wurde während des Kopiervorgangs der Firmwareupdatedatei aus dem Terminal gezogen.</p>	<p>Stecken Sie den USB-Stick mit der ursprünglichen Updatedatei, welche beim unterbrochenen Firmwareupdate genutzt wurde, in den USB Typ A Anschluss des Terminals.</p>
<p>Beim Neustart des Terminals erscheint folgende Statusanzeige:</p> <div data-bbox="148 1234 549 1440" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Unvollständiges Update [Version]</p> </div> <div data-bbox="148 1462 549 1668" style="border: 1px solid black; padding: 5px;"> <p>Falsche Version [Version]</p> </div> <p>[Version] stellt in der tatsächlichen Anzeige die Versionsnummer des nicht vollständig installierten Updates dar.</p>	<p>Während eines Firmwareupdates wurde die Stromversorgung des Terminals unterbrochen. Beim Neustart des Terminals wird das unvollständig durchgeführte Update erkannt und erneut vom USB-Stick geladen. Auf dem USB-Stick befindet sich nicht die ursprüngliche Updatedatei.</p>	<p>Stecken Sie den USB-Stick mit der ursprünglichen Updatedatei, welche beim unterbrochenen Firmwareupdate genutzt wurde, in den USB Typ A Anschluss des Terminals.</p>

Fehlerbeschreibung	Ursache	Behebung
<p>Es erscheint folgende Statusanzeige:</p> <div style="border: 1px solid black; padding: 5px; background-color: #e0f0e0;"> <p>Keine gSMC-KT gefunden! Verbindung über Netzwerk nicht mögl.!</p> </div>	<p>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.</p>	<p>Schalten Sie das Gerät aus und legen Sie eine gSMC-KT in einen der SIM-Slots des Kartenterminals ein. Lesen Sie hierzu auch Kapitel 2.2.3 „SIM-Slots“. Wahlweise können Sie auch in das Admin-Menü wechseln, um z.B. Netzwerkeinstellungen vorzunehmen.</p>
<p>Es erscheint folgende Statusanzeige:</p> <div style="border: 1px solid black; padding: 5px; background-color: #e0f0e0;"> <p>gSMC-KT entfernt! Pairing löschen oder passende gSMC-KT wieder einlegen.</p> </div>	<p>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.</p>	<p>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  -Taste auf und geben Sie Ihre Admin PIN ein. Hier können Sie das entsprechende Pairing löschen. Lesen Sie hierzu auch Kapitel 4.4. Durch Drücken der  -Taste schalten Sie das Gerät aus.</p>
<p>Es erscheint folgende Statusanzeige:</p> <div style="border: 1px solid black; padding: 5px; background-color: #e0f0e0;"> <p>Start PIN wurde nicht eingegeben! Neustart oder Start PIN ändern, s. Handbuch.</p> </div>	<p>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.</p>	<p>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  -Taste das Admin-Menü und generieren Sie wie in Kapitel 4.12 „Neue Start PIN vergeben“ beschrieben eine neue Start PIN.</p>

Fehlerbeschreibung	Ursache	Behebung
<p>Es erscheint folgende Statusanzeige:</p> <div data-bbox="150 338 549 535" style="border: 1px solid black; background-color: #d9ead3; padding: 5px; margin-bottom: 5px;"> Gerätefehler! Setzen der Admin Pin fehlgeschlagen </div> <div data-bbox="150 562 549 759" style="border: 1px solid black; background-color: #d9ead3; padding: 5px; margin-bottom: 5px;"> Gerätefehler! Setzen der Geräte PUK fehlgeschlagen </div> <div data-bbox="150 786 549 983" style="border: 1px solid black; background-color: #d9ead3; padding: 5px; margin-bottom: 5px;"> Gerätefehler! Setzen der SICCT Pin fehlgeschlagen </div> <div data-bbox="150 1010 549 1207" style="border: 1px solid black; background-color: #d9ead3; padding: 5px;"> Fehler: Generieren der Start PIN fehlgeschlagen </div>	<p>Während der Erstinbetriebnahme des Terminals konnte die Admin PIN, den PUK, die Start PIN oder die SICCT PIN nicht erfolgreich gesetzt werden.</p>	<p>Kontaktieren Sie einen zertifizierten Techniker oder den Hersteller. Geben Sie die Fehlerbeschreibung an und erbitten Sie weitere Hilfe.</p>

Fehlerbeschreibung	Ursache	Behebung
<p>Es erscheint eine der folgenden Statusanzeigen:</p> <div style="border: 1px solid black; background-color: #d9ead3; padding: 5px; margin-bottom: 5px;"> Gerätefehler! Ändern der Admin Pin fehlgeschlagen </div> <div style="border: 1px solid black; background-color: #d9ead3; padding: 5px; margin-bottom: 5px;"> Gerätefehler! Ändern der SICCT Pin fehlgeschlagen </div> <div style="border: 1px solid black; background-color: #d9ead3; padding: 5px; margin-bottom: 5px;"> Gerätefehler! Setzen der Web Admin Pin fehlgeschlagen </div> <div style="border: 1px solid black; background-color: #d9ead3; padding: 5px;"> Fehlgeschlagen </div>	<p>Im Admin-Menü des Terminals konnte die Admin Pin, die SICCT Pin, die Web Admin Pin bzw die Start PIN nicht erfolgreich geändert bzw. gesetzt werden.</p>	<p>Kontaktieren Sie einen zertifizierten Techniker oder den Hersteller. Geben Sie die Fehlerbeschreibung an und erbitten Sie weitere Hilfe.</p>
<p>Obwohl eine Chipkarte gesteckt ist, wird das zugehörige Kartensymbol im Display nicht ausgefüllt.</p> <div style="border: 1px solid black; background-color: #d9ead3; padding: 5px; margin-bottom: 5px;">   german telematics GT900 eHealth SICCT IP 192.168.100.210 </div> <div style="border: 1px solid black; background-color: #d9ead3; padding: 5px;"> eHealth GT900 1.22.1 </div>	<p>Mögliche Ursachen sind:</p> <ul style="list-style-type: none"> • Die Karte steckt falsch herum • Die Karte ist defekt • Die Kontaktiereinheit ist verschmutzt oder defekt 	<p>Prüfen Sie, ob die Chipkarte wie in Kapitel Fehler! Verweisquelle konnte nicht gefunden werden. „Kartenslots“ beschrieben korrekt gesteckt ist. Wenn ja, überprüfen Sie, ob die Chipkarte in einem anderen Kartenslot oder in anderem, funktionsfähigen, Kartenterminal gelesen werden kann. Wenn dies nicht der Fall ist, ist die Karte defekt. Wenn die Karte in einem anderen Slot oder Kartenterminal gelesen werden kann, ist die Kontaktiereinheit Ihres Terminals defekt oder verschmutzt. Nehmen Sie in diesem Fall für eine Reparatur oder einen Austausch des Gerätes Kontakt mit Ihrem Lieferanten auf.</p>

10 Kontakt

GT German Telematics Gesellschaft für Telematikdienste mbH

Libellenstraße 9

14129 Berlin

Fax.: +49 (0)30 – 31805454

E-Mail: service@germantelematics.de

Internetpräsenz: <https://www.germantelematics.de>

11 Außerbetriebnahme, Rückversand und Entsorgung

Bei Außerbetriebnahme oder Rückversand des Gerätes (z.B. im Fall eines Austauschs) stellen Sie sicher, dass sich keine Chipkarten mehr in den Kartenslots befinden und das alle Pairings gelöscht sind. Die Pairings können Sie im Administrator Menü (s. Kapitel 4.4.4) oder mittels eines Werksresets (s. Kapitel 5) löschen. Löschen Sie auch die Pairinginformationen des betroffenen Kartenterminals im Konnektor.

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



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 Telematik-Anwendungen der Gesundheitskarte mbH

Zulassungsurkunde

Die gematik Gesellschaft für Telematik-Anwendungen der Gesundheitskarte mbH hat
der

gt german telematics GmbH

mit Bescheid vom . . .

für das

PLATZHALTER FÜR ZERTIFIKAT

die Zulassung für den Einsatz in der Telematik-Infrastruktur erteilt.

Zulassungsnummer: gematik_ _ _ 1

Berlin, . . .

Geschäftsbereich

Geschäftsbereich

gematik - Gesellschaft für Telematik-Anwendungen der Gesundheitskarte mbH
Friedrichstraße 135 10117 Berlin • Telefon: 30 66 41 00 • Fax: 30 66 41 111
www.gematik.de

Kapitel: Außerbetriebnahme, Rückversand und Entsorgung



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

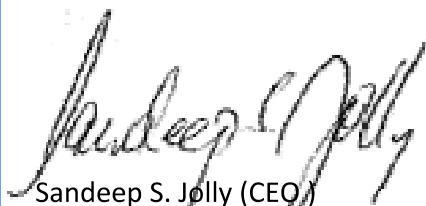
Immunity: EN 55 024: 10.2003

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/markings.



Sandeep S. Jolly (CEO)
 Date: 7th Apr, 2009

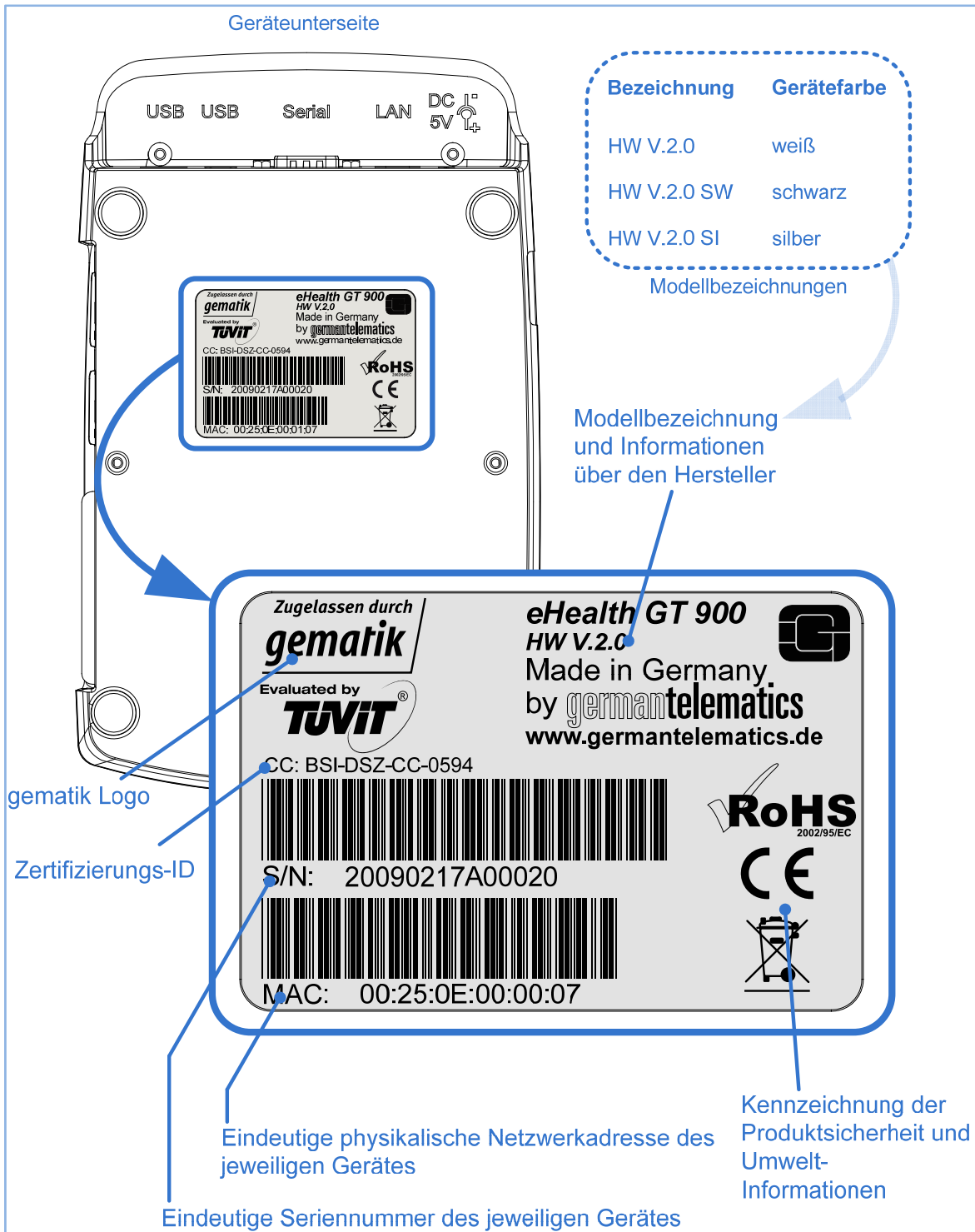


Abbildung 86: Geräteunterseite

©2020 GT German Telematics Gesellschaft für Telematikdienste mbH.

Alle Rechte vorbehalten. Irrtümer und technische Änderungen vorbehalten.

Dieses Produkt beinhaltet Software lizenziert unter GPLv2 und LGPL. Weitere Details finden Sie auf der mitgelieferten Treiber-CD.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

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 das Kapitel 8 „Produktregistrierung“ dieses Benutzerhandbuchs.

Ihre Anmeldedaten (bitte in Blockschrift ausfüllen):

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

Datenschutzerklärung :

Die GT German Telematics GmbH 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 an. Geben Sie bei der Registrierung an, dass Sie produktspezifische Informationen der German Telematics erhalten möchten, senden wir Ihnen diese von Zeit zu Zeit per E-Mail oder Fax zu. Nur die German Telematics wird Ihnen solche E-Mails oder Faxe direkt senden. Informationen, die German Telematics von den Benutzern zur Verfügung gestellt werden, werden von der German Telematics weder an Dritte verkauft noch diesen gegenüber offen gelegt. <https://www.germantelematics.de/datenschutz/>

Unterschrift / Praxisstempel



germantelematics

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 eHealth GT900 Kartenterminals informiert werden.

Platzhalter
Gerätelabel

