# Bedienungsanleitung

## Stationäres eHealth Kartenterminal ORGA 6141 online mit Firmware-Version 3.8.1




Version 21.12.1

# Vorwort

Sehr geehrte Anwenderin, sehr geehrter Anwender,

vielen Dank, dass Sie sich für ein Produkt von Ingenico Healthcare entschieden haben. Diese Bedienungsanleitung beschreibt das stationäre eHealth Kartenterminal ORGA 6141 online. Es ist für den stationären Onlinebetrieb am Konnektor oder an einer Signaturanwendungskomponente (SAK) entwickelt. Für diese Anwendungszwecke ist es bestens ausgestattet. Durch sein ergonomisches Design und seine für den Online-Produktivbetrieb durch die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) zugelassene Hard- und Software eignet es sich ausgezeichnet für die vielseitigen Einsatzzwecke in der heutigen und zukünftigen Online-Telematikinfrastruktur des deutschen Gesundheitswesens. Das stationäre ORGA 6141 online Terminal vereinfacht administrative Abläufe bei der Patienten-datenerfassung und Übergabe an die von Ihnen verwendete Primärsystemsoftware Ihres EDV Systems.
In den Geräteeinstellungen lässt sich jederzeit im Menü [**Integrität \3428**] ein Integritätstest des Gerätes durchführen.



ACHTUNG
Bitte lesen Sie sich vor der Inbetriebnahme des Terminals diese Bedienungs-anleitung sorgfältig durch und beachten Sie in jedem Fall die mit diesen Symbolen gekennzeichneten Sicherheits- und Datenschutzhinweise!



HINWEIS
Aus Gründen der leichteren Lesbarkeit wird in diesem Dokument die gewohnte männliche Sprachform bei personenbezogenen Substantiven und Pronomen verwendet. Dies impliziert jedoch keine Benachteiligung des weiblichen bzw. diversen Geschlechts, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral zu verstehen sein.

Wir wünschen Ihnen ein angenehmes, müheloses und zuverlässiges Erfassen Ihrer Patientendaten mit Ihrem neuen ORGA 6141 online eHealth Kartenterminal.

Ihr Ingenico Healthcare Team

Ingenico Healthcare GmbH
Konrad-Zuse-Ring 1
24220 Flintbek
Tel.: 04347 90 11 111
Internet: www.ingenico.de/healthcare
E-Mail: kontakt.ihc@ingenico.com

## Hinweise zur Bedienungsanleitung

Die vorliegende Bedienungsanleitung richtet sich an Leistungserbringer im Gesundheitswesen, das medizinische und pharmazeutische Personal und Administratoren. Des Weiteren gilt diese Beschreibung auch für die alternative Anwendung als Signaturterminal in Verbindung mit einer Signaturanwendungskomponente (SAK), da hier eine irreversible Umschaltung lediglich den Wechsel eines sogenannten Vertrauensraums (d.h. internen Betriebsdaten) bedeutet, ohne dass sich die Funktionsweise des SICCT-basierten Kartenterminals ändert.
Die Bedienungsanleitung beschreibt die Handhabung des stationären eHealth Kartenterminals ORGA 6141 online mit der für den gematik Online-Produktivbetrieb spezifizierten und zugelassenen Firmware-Version 3.8.1.
Sie vermittelt dem Administrator und Anwender notwendige Kenntnisse über Funktion, Installation, Bedienung, Wartung und Entsorgung des Gerätes.
Diese Anleitung beinhaltet alle für eine gefahrlose Benutzung erforderlichen Informationen und gibt bei auftretenden Störungen Hinweise auf mögliche Ursachen und deren Beseitigung.
Einige Menüpunkte und Funktionalitäten der Vorgängerversion für den bisherigen „Offline-Betrieb“ (ORGA 6141 mit Firmware 2.20) sind aufgrund neuer Sicherheitsanforderungen der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) für die Arbeit mit stationären eHealth-Kartenterminals im Online-Produktivbetrieb weggefallen und andere sind zum Betreiben des Gerätes am Konnektor in der neuen Betriebsart “eHealth-KT“ hinzugekommen.
Der Konnektor ist die dezentrale Komponente zur sicheren Anbindung von Clientsystemen der Institutionen (AIS, AVS) und der Kartenterminals im sicheren lokalen Netz (LAN) des Anwenders. Im LAN der Einsatzumgebung kommuniziert das Clientsystem mit dem Konnektor über dessen LAN-seitiges Ethernet-Interface. Der Konnektor ist anschließend verantwortlich für den Zugriff auf die in der Einsatzumgebung befindlichen Kartenterminals sowie Karten und protokolliert Fehlerzustände.
Der Konnektor regelt die sicheren Kommunikationsbeziehungen zwischen Clientsystem, Kartenterminals, Karten und zentralen Diensten der TI-Plattform sowie fachanwendungs-spezifischen Diensten.
Die zwischen den Funktionsmerkmalen der Komponenten bestehenden Wechselwirkungen (u.a. Die Erkennung einer gesteckten Karte im Kartenterminaldienst löst eine Reaktion im Konnektor-Kartendienst aus) werden hierzu durch den Konnektor-Administrator administrativ konfiguriert und müssen zur Gewähr eines sicheren Betriebs des Kartenterminals ebenfalls zyklisch überprüft und gepflegt werden.
Die Managementschnittstelle des Konnektors ermöglicht es dem (Konnektor-) Administrator, die Liste der verwalteten und verbundenen Kartenterminals einzusehen, den jeweiligen Verbindungsstatus zu kontrollieren sowie zum Firmware-Update eine Firmware-Image Datei an die Kartenterminals zu übertragen.
Die jeweilige Managementschnittstelle des Konnektors oder einer SAK ermöglicht es dem Konnektor- bzw. SAK-Administrator, die Liste der verwalteten und verbundenen Kartenterminals einzusehen, den jeweiligen Verbindungsstatus zu kontrollieren sowie zum Firmware-Update eine Firmware-Image Datei an die Kartenterminals zu übertragen.

Das Kapitel 1 »Allgemeine Informationen vor Inbetriebnahme« wendet sich sowohl an Administratoren wie auch an Anwender des Gerätes und enthält alle wichtigen Hinweise zum sicheren und ordnungsgemäßen Umgang mit diesem Gerät.
Das Kapitel 2 »Bedienungsanleitung für den Benutzer« wendet sich sowohl an Administratoren wie auch an Anwender des Gerätes und enthält alle Informationen zur Handhabung und einfachen Bedienung des Gerätes in der täglichen Praxis.
An einigen Stellen wird auf Abschnitte im Kapitel drei verwiesen.
Das Kapitel 3 »Bedienungsanleitung für den Administrator« wendet sich an Administratoren des Gerätes und der umgebenden IT-Infrastruktur. Es enthält alle Informationen zur Installation und Integration des Gerätes in die IT Infrastruktur, in der die gespeicherten Patientendaten an das Primärsystem übermittelt werden.

HINWEIS
In dieser Bedienungsanweisung werden die Menüs immer mit ihren jeweiligen Kurztastenkombination dargestellt (Beispiel [**Einstellungen \2**]. Sie können so direkt mit der entsprechenden Tastenkombination ins gewünschte Menü gelangen. Dies soll Ihnen die Navigation vereinfachen und dient zur Beschleunigung der Bedienung des Gerätes in der täglichen Praxis.
Die Menüstruktur mit den dazugehörenden Kurztastensequenzen finden Sie im Anhang dieser Bedienungsanleitung auf den Seiten 102 bis 106.

HINWEIS
Eine schnelle Übersicht und Einführung in die verschiedenen Funktionselemente des Gerätes finden Sie im Abschnitt 3 »Produktbeschreibung« auf Seite 39 dieser Bedienungsanleitung.

## Copyrights

Copyright © 2020/2021 ingenico a Worldline brand
Ingenico Healthcare GmbH. Alle Rechte vorbehalten.

Alle Produkte oder Dienstleistungen, die in diesem Dokument genannt werden, sind Marken, Dienstleistungsmarken, eingetragene Marken oder eingetragene Dienstleistungsmarken der entsprechenden Eigentümer.
Kein Teil dieser Veröffentlichung darf ohne schriftliche Genehmigung der Ingenico Healthcare GmbH kopiert, gesendet, übertragen, elektronisch gespeichert oder in eine andere Sprache übersetzt werden. Diese Bedienungsanleitung dient der allgemeinen Information und stellt keine technische Spezifikation dar.
Die Ingenico Healthcare GmbH behält sich das Recht auf die Änderung von Funktionen, Eigenschaften und technischen Angaben zu jeder Zeit und ohne vorherige Benachrichtigung vor.

## Versionsstand / Selbstauskunft des Terminals

Sie können den Versionsstand der Firmware Ihres Gerätes wie folgt ablesen:
Verbinden Sie das Gerät mit dem beiliegenden Netzteil mit dem Stromnetz. Das Gerät startet daraufhin automatisch. Sollte das Gerät bereits mit dem Stromnetz verbunden aber ausgeschaltet sein, können Sie das Gerät durch Drücken der OK-Taste einschalten. Sobald der Ruhebildschirm angezeigt wird, drücken Sie auf die MENU-Taste um ins Hauptmenü zu gelangen. Anschließend wählen Sie das Menü [**Service \3**] durch zwei Mal Drücken auf die ▼-Taste und anschließendem Betätigen der OK-Taste.
Verfahren Sie genau so bei der Wahl des Menüs [**Status \32**]: Einmal Drücken auf die ▼-Taste gefolgt von einem Druck auf die OK-Taste.
Mit den Cursor-Tasten ▲ und ▼ können Sie alle Informationen über das Gerät abrufen.

| Version | Änderung zur Vorgängerversion V3.7.2 |
|---|---|
| V3.7.4 | • Ergänzung der Zertifikatsliste TSL-PU vom 23.03.2018 |
| V3.8.0 | Änderung zur Vorgängerversion V3.7.4:<br>Neue Funktionen:<br>• Neue Bootsequenz direkt nach dem Einschalten des Terminals (weißes Ingenico Healthcare Logo auf schwarzem Hintergrund für ca. 5-6 Sekunden gefolgt von einem kreisumlaufenden Boot-Symbol)<br>• Betrieb des Terminals an einer Signaturanwendungskomponente (SAK).<br>• Verbindungsaufbau zu einem VPN-Gateway über eine IPsec VPN Verbindung<br>• Terminal Konfigurationen und Betriebszustände via QR-Codes auslesen<br>• Admin-Session Hinweis-Bildschirm bei Inbetriebnahme eines Neugerätes<br>• Im- und Export von Geräte-Parametern via USB-Stick<br>• Darstellung der aktuellen Uhrzeit und des Datums bei Konfiguration eines NTP Clients<br>• Hinweis auf nahes Ende der Gültigkeit der Zertifikate auf der gSMC-KT<br>• Auslesen der ICCSN und der Verfallsdaten der Zertifikate einer gSMC-KT beim Einzeltest der Kontaktiereinheiten<br>• Timeout-Watchdog: Gerät startet automatisch neu bei einem „System Freeze“<br>• Neues Schriftbild<br>• Anpassungen der Ausgabemöglichkeiten und Formate (u.a. Logo-Ausgabe, Font, weitere Schriftgrößen) für Display-Meldungen an den Bediener.<br>• Vergrößerung der Pop-Up-Textboxen für Status- und Fehlermeldungen am Terminal-Display.<br>• Ergänzung kleinerer Schriftgrößen für Anzeigen und einer Fortschrittsbalkendarstellung im Bereich der Download-Image-Inhalte.<br><br>Sonstige Änderungen in der Bedienungsanleitung:<br>• Neue Abschnitte zur Funktionsbeschreibung der neuen Funktionen des Terminals<br>• aktualisierte Bildschirm-Darstellungen<br>• aktualisierte Prozessbeschreibung bei der Außerbetriebnahme und im Reparaturfall<br>• Kleinere Korrekturen der Orthographie |
| V3.8.1 | Änderung zur Vorgängerversion V3.8.0:<br>• Formale Anpassungen FW-Version, Release Datum und FW Gruppe (FWG)<br>• 4.4 Der Ruhebildschirm – Ergänzung der Deaktivierungsoption der Warnmeldungsanzeige nach erkanntem gSMC-KT-Ablauf.<br>• 5.5 Werksvoreinstellungen – Aktualisierung Menüpunkte<br>• Anhang 4, 5 Aktualisierung Menüdarstellung<br>• 7.1.1.7.4 Aktualisierung Untermenüpunkte |

# Inhaltsverzeichnis

Vorwort ..... 2
Hinweise zur Bedienungsanleitung ..... 3
Copyrights ..... 4
Versionsstand / Selbstauskunft des Terminals ..... 5
Kapitel 1: Allgemeine Informationen vor Inbetriebnahme ..... 13
1. Einführung ..... 13
1.1. Verwendete Symbole und Signalwörter ..... 13
1.2. Prüfung der sicheren Anlieferung des eHealth Terminals auf einem vertrauenswürdigen Lieferweg ..... 14
1.3. Lieferumfang ..... 14
1.4. Funktionen der verschiedenen Tasten des Gerätes ..... 15
1.5. Displaysymbole und ihre Bedeutung ..... 18
1.5.1. Symbol 1 bis 4: Karten-Kontaktiereinheiten ..... 18
1.5.2. Symbol 6: Datenverkehr zu angeschlossenen Geräten ..... 19
1.5.3. Symbol 7: Interne Stützbatterie schwach ..... 19
1.5.4. Symbol 8: Konfiguration als Signaturterminal außerhalb der Telematikinfrastruktur 20
1.5.5. Symbol 9: Allgemeiner Gerätestatus ..... 20
1.5.6. Symbol 10: Datenverwaltung ..... 20
1.6. Begriffsbestimmung ..... 21
2. Sicherheit ..... 23
2.1. Gerätesicherheit ..... 23
2.2. Sicherheitsmerkmale ..... 23
2.2.1. Das Gehäusesiegel und seine Eigenschaften ..... 23
2.2.2. Das Slotsiegel und seine Eigenschaften ..... 25
2.2.3. Regelmäßiges Prüfen der Gehäuse- und Slotsiegel ..... 26
2.2.4. Geräteversion ..... 27
2.2.5. Integritätsprüfung ..... 27
2.2.6. Typenschild ..... 27
2.3. Sicherheit bei der Inbetriebnahme ..... 28
2.3.1. Aufstellungshinweise ..... 28
2.3.2. Admin-PIN Eingabe bei der Inbetriebnahme ..... 28
2.3.3. Eingabe einer Karten PIN nach Aufforderung ..... 28
2.3.3.1. Der sichere PIN Eingabe Modus ..... 29
2.3.3.2. Fehlerfreier Ablauf ..... 29

2.3.3.3. Ablauf bei inkorrekter Karten PIN Eingabe ..... 29
2.3.3.4. Ablauf bei Abbruch der Karten PIN Eingabe durch den Benutzer ..... 30
2.3.3.5. Ablauf im Fall von Zeitüberschreitung bei Eingabe der Karten PIN ..... 30
2.4. Logging und Änderungsprotokollierung ..... 30
2.5. Sicherheit bei der Außerbetriebnahme und im Reparaturfall ..... 30
2.6. Normen und Richtlinien ..... 33
2.7. Temperatur / Umgebungsbedingungen ..... 33
2.8. Allgemeine Regeln & Anforderungen zur Betriebssicherheit des Gerätes ..... 34
2.9. Sicherheit beim Anschluss an den Konnektor ..... 37
2.10. Reinigung und Pflege ..... 37
2.11. Desinfektion ..... 37
2.12. Entsorgung des Gerätes ..... 38
Kapitel 2: Bedienungsanleitung für den Benutzer ..... 39
3. Produktbeschreibung ..... 39
3.1. Die Vorderseite des ORGA 6141 online ..... 39
3.2. Die Rückseite des ORGA 6141 online ..... 40
3.3. Die Kontaktiereinheiten 3 und 4 für die SMC-Karten ..... 40
4. Bedienung des Gerätes ..... 41
4.1. Tastatur ..... 41
4.2. Ein- und Ausschalten des Gerätes ..... 41
4.3. Aufbau des Grafikdisplays ..... 42
4.4. Der Ruhebildschirm ..... 43
4.5. Menü-Navigation ..... 44
4.6. Das Hauptmenü ..... 44
4.7. Einstecken einer eGK in die Kontaktiereinheit 1 ..... 45
4.8. Einstecken eines HBA in die Kontaktiereinheit 2 ..... 45
4.9. Patientendatensatz einlesen ..... 46
Kapitel 3: Bedienungsanleitung für den Administrator ..... 47
5. Inbetriebnahme als eHealth-Terminal in der Telematikinfrastruktur ..... 47
5.1. Das erste Einschalten des Gerätes ..... 47
5.2. Admin-PIN Eingabe bei der ersten Inbetriebnahme ..... 47
5.3. Admin-PIN Zeitsperre ..... 48
5.4. Neue PIN anfordern ..... 48
5.5. Werksvoreinstellungen ..... 49
5.6. Authentizitäts- und Integritätsprüfung der gSMC-KT ..... 50
5.7. Einsetzen einer SMC-Karte und Versiegeln der Kontaktiereinheiten 3 und 4 ..... 52

5.8. Verbindung des Gerätes über eine LAN-Verbindung mit dem Konnektor ..... 54
5.9. Initiales Pairing des Terminals mit dem Konnektor ..... 55
5.10. Verbindung des Terminals mit dem Konnektor über ein Virtual Privat Network (VPN) 57
5.10.1. Syntax der VPN Import-Datei ..... 57
6. Inbetriebnahme als Signatur-Terminal außerhalb der Telematikinfrastruktur ..... 58
6.1. Initiales Pairing des Terminals mit einer Signaturanwendungskomponente (SAK) ..... 58
7. Die Menüoptionen (direkte Managementschnittstelle) für den Administrator im Detail ..... 59
7.1. Ausschalten des Gerätes [Ausschalten \1] ..... 59
7.2. Der Menüpunkt Einstellungen [Einstellungen \2] ..... 59
7.2.1. Die Konfiguration im lokalen Netzwerk [LAN Parameter \21] ..... 60
7.2.1.1. LAN Parameter: [Gerätename \211] ..... 60
7.2.1.2. LAN Parameter: [DHCP \212] ..... 60
7.2.1.2.1. DHCP: [Ein / Aus \2121] ..... 60
7.2.1.2.2. DHCP: [Erw. Optionen \2122] ..... 60
7.2.1.3. LAN Parameter: [IP Adresse \213] ..... 61
7.2.1.4. LAN Parameter: [Subnet Mask \214] ..... 61
7.2.1.5. LAN Parameter: [Gateway/DNS \215] ..... 61
7.2.1.6. LAN Parameter: [TCP/UDP Port \216] ..... 61
7.2.1.7. LAN Parameter: [IPsec VPN Konfiguration \217] ..... 62
7.2.1.7.1. VPN-Parameter: [VPN-Tunnel Ein/Aus \2171] ..... 62
7.2.1.7.2. VPN-Parameter: [VPN-Tunnel Neustart \2172] ..... 62
7.2.1.7.3. VPN-Parameter: [VPN-Gateway Adresse \2173] ..... 62
7.2.1.7.4. VPN-Parameter: [Zugangsdaten \2174] ..... 62
7.2.1.7.5. VPN-Parameter: [Status/Information \2175] ..... 63
7.2.1.7.6. VPN-Parameter: [Konfiguration löschen \2176] ..... 63
7.2.1.8. LAN Parameter: [NTP Client \218] ..... 63
7.2.1.8.1. NTP Client: [Ein/Aus \2181] ..... 64
7.2.1.8.2. NTP Client: [NTP Server IP Adresse \2182] ..... 64
7.2.1.8.3. NTP Client: [Timezone \2183] ..... 64
7.2.1.9. LAN Parameter: [Neustart \219] ..... 64
7.2.2. Die Konfiguration der SICCT Parameter [SICCT Parameter \22] ..... 64
7.2.2.1. SICCT - Grundsätzliche Funktionsweise ..... 64
7.2.2.2. SICCT Parameter: [Keep Alive \221] ..... 65
7.2.2.2.1. Keep Alive: [KA Intervall \2211] ..... 65
7.2.2.2.2. Keep Alive: [KA Timeout \2212] ..... 65
7.2.2.3. SICCT Parameter: [Protokoll \222] ..... 65

7.2.2.3.1. Protokoll: [Block read Timeout \2221] ... 65
7.2.2.3.2. Protokoll: [Message read Timeout \2222] ... 65
7.2.2.3.3. Protokoll: [Max. Protokollfehler \2223] ... 66
7.2.2.3.4. Protokoll: [SSL accept Timeout \2224] ... 66
7.2.2.4. SICCT Parameter: [TLS Einstellung \223] ... 66
7.2.2.4.1. TLS Einstellungen: [TLS Version \2231] ... 66
7.2.2.4.2. TLS Einstellungen: [TSL Liste \2232] ... 66
7.2.2.5. SICCT Parameter: [Announcement \224] ... 67
7.2.2.6. SICCT Parameter: [Pairings \225] ... 67
7.2.2.7. SICCT Parameter: [Session Admin \226] (zweite Managementschnittstelle) ... 68
7.2.2.8. SICCT Parameter: [Zugriffsrechte \227] ... 68
7.2.2.8.1. Zugriffsrechte: [Admin Session \2271] ... 68
7.2.2.8.2. Zugriffsrechte: [Set Status \2272] ... 69
7.2.2.8.3. Zugriffsrechte: [Download \2273] ... 69
7.2.2.9. SICCT Parameter: [Neustart \228] ... 70
7.2.3. Einstellen der Uhrzeit [Zeit \23] ... 70
7.2.4. Einstellen des Datums [Datum \24] ... 70
7.2.5. Einstellen der Menüsprache [Sprache \25] ... 70
7.2.6. Einstellen der Displayanzeige [Display \26] ... 70
7.2.6.1. Individueller Text im Ruhebildschirm [Freier Text \261] ... 70
7.2.6.2. Einstellen der Displayhelligkeit [Helligkeit \262] ... 71
7.2.6.3. Einstellen der Hintergrundfarbe [Hintergrundfarbe \263] ... 71
7.2.7. Einstellen der Signaltöne [Töne \27] ... 71
7.2.8. Einstellen des akustischen PIN Schutzes [Akustischer PIN Schutz \275] ... 71
7.2.9. Durchführung eines Firmware-Updates [Update \28] ... 72
7.2.9.1. Firmware Update via Konnektor ... 73
7.2.9.2. Firmware Update per USB-Stick (Pull-Verfahren) ... 74
7.2.9.2.1. Voraussetzungen zur Durchführung des Updates ... 74
7.2.9.2.2. Durchführung der Firmware-Aktualisierung per USB-Stick ... 75
7.2.9.3. Firmware Update per TFTP-Server (Pull-Verfahren) ... 76
7.2.9.3.1. Voraussetzungen zur Durchführung des Updates ... 76
7.2.9.3.2. Durchführung der Firmwareaktualisierung via TFTP Server im Pull-Verfahren ... 76
7.2.9.4. Firmware Update per Steuerfile am TFTP Server (Push Verfahren) ... 77
7.2.9.4.1. Voraussetzungen zur Durchführung des Updates ... 78
7.2.9.4.2. Syntax der Steuerdatei ... 79
7.2.9.4.3. Durchführung der Firmware-Aktualisierung via TFTP Server im Push-Verfahren 80

7.2.9.5. Firmware-Update: [Dateiname \281] ... 80
7.2.9.6. Firmware-Update: [TFTP Server IP Adresse \282] ... 80
7.2.9.7. Firmware-Update: [Poll Status \283] ... 80
7.2.9.8. Einstellmöglichkeiten über [Poll Window \284] ... 81
7.2.9.9. Firmware-Update: [Update starten \285] ... 81
7.2.10. Durchführung eines Updates der Konfigurationsparameter [Update \28] ... 82
7.3. Der Menüpunkt Service [Service \3] ... 83
7.3.1. Ändern der Admin-PIN [PIN ändern \31] ... 83
7.3.2. Die Terminalselbstauskunft [Status \32] ... 84
7.3.3. Zurücksetzen des Terminals in den Auslieferungszustand [Werkseinstellung \33] ... 85
7.3.3.1. Zurücksetzen des Terminals via Admin-PIN [via Admin-PIN \331] ... 85
7.3.3.2. Zurücksetzen des Terminals via Reset-Code [via Reset-Code \332] ... 85
7.3.4. Terminal-Funktionstests [Test \34] ... 86
7.3.4.1. Test: [Gesamttest \341] ... 86
7.3.4.2. Test: [Einzeltest \342] ... 86
7.3.4.2.1. Einzeltest: [Buzzer \3421] ... 87
7.3.4.2.2. Einzeltest: [Display \3422] ... 87
7.3.4.2.3. Einzeltest: [Tasten \3423] ... 87
7.3.4.2.4. Einzeltest: [Slot 1 \3424] ... 87
7.3.4.2.5. Einzeltest: [Slot 2 \3425] ... 87
7.3.4.2.6. Einzeltest: [Slot 3 \3426] und [Slot 4 \3427] ... 88
7.3.4.2.7. Einzeltest: [Integrität \3428] ... 88
7.3.5. Der Kiosk-Modus [Kiosk-Modus \35] ... 89
7.3.6. Konfiguration via USB-Stick im- und exportieren ... 89
7.3.6.1. Daten-Import: [Import von einem USB-Stick \361] ... 91
7.3.6.2. Daten-Export: [Export auf einem USB-Stick \362] ... 92
7.3.7. Terminal Konfigurationen und Betriebszustände via QR-Codes auslesen ... 92
7.3.7.1. QR-Code: [Info/Service \371] ... 94
7.3.7.2. QR-Code: [Status (Geräteselbstauskunft) \372] ... 94
7.3.7.3. QR-Code: [F1/F2 Tasten (Netzwerkstatus) \373] ... 94
7.3.7.4. QR-Code: [LAN-Parameter \374] ... 95
7.3.7.5. QR-Code: [SICCT-Parameter \375] ... 96
7.3.7.6. QR-Code: [Update Parameter \376] ... 96
7.3.7.7. QR-Code: [Service/Einstellungen \377] ... 96
7.3.7.8. QR-Code: [Betriebsdaten/Statistik \378] ... 97
ANHANG: ... 100

1. Technische Daten ..... 100
2. Musteranschreiben einer gSMC-KT ..... 101
3. Menüstruktur für den Anwender ..... 102
4. Menüstruktur für den Administrator - Teil 1: Allgemeine Einstellungen ..... 103
5. Menüstruktur für den Administrator - Teil 2: LAN Parameter ..... 104
6. Menüstruktur für den Administrator - Teil 3: SICCT Parameter ..... 105
7. Menüstruktur für den Administrator - Teil 4: Service Einstellungen ..... 106
8. Hinweise zur Problembeseitigung, Fehlererkennung, Verhalten im Fehlerfall und Fehlerbehandlung ..... 107
9. Programmatische 2D-Code-Ausgaben über SICCT-Kommandos ..... 115
10. Abbildungsverzeichnis ..... 116
11. Tabellenverzeichnis ..... 117
12. NOTIZEN ..... 118

# Kapitel 1: Allgemeine Informationen vor Inbetriebnahme

Das Kapitel 1 »Allgemeine Informationen vor Inbetriebnahme« wendet sich sowohl an Administratoren wie auch an Anwender des Gerätes und enthält alle wichtigen Hinweise zum sicheren und ordnungsgemäßen Umgang mit diesem Gerät.

## 1. Einführung

### 1.1. Verwendete Symbole und Signalwörter



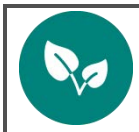
ACHTUNG!
Warnhinweis, den der Benutzer beachten muss, um einen sicheren Datentransfer des Gerätes und den Schutz von persönlichen Daten zu gewährleisten.



ACHTUNG!
Warnhinweis, den der Benutzer beachten muss, um einen sicheren Betrieb des Gerätes und die Sicherheit von Personen und Sachen zu gewährleisten.



HINWEIS
Auf diese Weise gekennzeichneter Text enthält nützliche Informationen und Tipps für eine sichere Anwendung des Gerätes.



HINWEIS
Wichtiger Hinweis zum Umweltschutz

## 1.2. Prüfung der sicheren Anlieferung des eHealth Terminals auf einem vertrauenswürdigen Lieferweg

Sie leisten als Ärztin oder Arzt bzw. Administrator einer medizinischen Betriebsstätte einen entscheidenden Beitrag zur Sicherheit der Online-Telematikinfrastruktur. In Ihrer Arbeitsumgebung in der eigenen Praxis, in einem medizinischen Versorgungszentrum oder in einer Klinik benötigt der Schutz der Patientendaten und der Komponenten der Online-TI besonderer Aufmerksamkeit und besonders hoher Schutzmaßnahmen.
Unsere sichere Lieferkette zwischen Ingenico Healthcare und Ihnen ist ein wichtiger Beitrag zur Sicherheit der gesamten Online-TI!
Um Manipulationen nicht erst während des Einsatzes der TI-Komponenten in der Arztpraxis zu verhindern ist bereits ein Schutz der Komponenten ab dem Moment der Fertigung in den Produktionsstätten notwendig. Hierzu wurde von uns eine sogenannte "Sichere Lieferkette" aufgebaut.
Unsere mobilen und stationären eHealth Terminals werden in einer versiegelten Verpackung geliefert, die Sie bei Empfang auf Unversehrtheit prüfen müssen, um Manipulationsversuche durch unerlaubtes Öffnen der Verpackung auszuschließen. Das angebrachte Siegelband verfügt über verschiedene Schutzmechanismen, die es Ihnen ermöglichen, die Unversehrtheit und Echtheit der Verpackung einfach zu überprüfen.
Sie haben nach der Lieferung eines mobilen oder stationären Gesundheitskartenterminals sowie einer gSMC-KT Karte die Möglichkeit, den lückenlosen Lieferweg zwischen uns und Ihnen zu überprüfen, um sicher zu stellen, dass die Ware ordnungsgemäß, sicher und frei von Manipulationsversuchen bei Ihnen in der Praxis angekommen ist. Hierzu stellen wir Ihnen auf unserer Internetseite **www.ingenico.de/healthcare/sichere-lieferkette** eine Liste unserer Handelspartner zur Verfügung, die sich vertraglich dazu verpflichtet haben, alle Anforderungen an die sichere Lieferkette einzuhalten. Wir liefern mobile und stationäre Gesundheitskartenterminals sowie gSMC-KT Karte für die Online-TI ausschließlich zu diesen Handelspartnern oder direkt in Leistungserbringerinstitutionen (Arztpraxis, MVZ, Krankenhaus).



ACHTUNG!
Ihr ORGA 6141 online wurde auf einem sicheren Lieferweg bis zu Ihnen transportiert. Um die Authentizität und Integrität des Versandgebindes überprüfen zu können hat Ingenico Healthcare alle notwendigen Informationen auf der Internetseite **www.ingenico.de/healthcare/sichere-lieferkette** zusammengestellt. Folgen Sie den dort beschriebenen Handlungsanweisungen und der Endbenutzer-Checkliste, bevor sie mit der Installation des Gerätes in der Praxis beginnen.

## 1.3. Lieferumfang

Folgende Dinge sind im Standard-Lieferumfang des Gerätes enthalten:

- Ein stationäres Kartenterminal ORGA 6141 online
- Ein LAN-Kabel zum Anschluss des Gerätes an den Konnektor
- Ein 7,5 V Steckernetzteil
- Eine transparente Dokumententasche mit
    - Kurzbedienungsanleitung und
    - vier Slotsiegel in einem Folienbeutel

## 1.4. Funktionen der verschiedenen Tasten des Gerätes

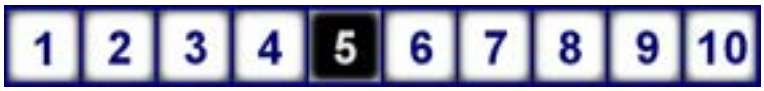
| Taste | Funktion |
|---|---|
|  | Taste 1:<br>• Eingabe des Wertes **1**<br>• Bei freier Texteingabe die Schriftzeichen **! ? # $ & * ß** oder **1** |
|  | Taste 2:<br>• Eingaben des Wertes **2**<br>• Bei freier Texteingabe Schriftzeichen **a b c ä A B C Ä** oder **2** |
|  | Taste 3:<br>• Eingabe des Wertes **3**<br>• Bei freier Texteingabe die Schriftzeichen **d e f D E F** oder **3** |
|  | Taste 4:<br>• Eingaben des Wertes **4**<br>• Bei freier Texteingabe die Schriftzeichen **g h i G H I** oder **4** |
|  | Taste 5:<br>• Eingabe des Wertes **5**<br>• Bei freier Texteingabe die Schriftzeichen **j k l J K L** oder **5** |
|  | Taste 6:<br>• Eingaben des Wertes **6**<br>• Bei freier Texteingabe die Schriftzeichen **m n o ö M N O Ö** oder **6** |
|  | Taste 7:<br>• Eingabe des Wertes **7**<br>• Bei freier Texteingabe die Schriftzeichen **p q r s P Q R S** oder **7** |
|  | Taste 8:<br>• Eingaben des Wertes **8**<br>• Bei freier Texteingabe die Schriftzeichen **t u v ü T U V Ü** oder **8** |
|  | Taste 9:<br>• Eingabe des Wertes **9**<br>• Bei freier Texteingabe die Schriftzeichen **w x y z W X Y Z** oder **9** |
|  | Taste 0:<br>• Eingabe des Wertes **0**<br>• Bei freier Texteingabe die Schriftzeichen **/ - + . , ; : ,** oder **0** |

| Taste | Funktion |
|---|---|
|  | F1 Taste:<br>• Bei freier Texteingabe die Schriftzeichen **-** oder **_** (Unterstrich)<br>• Die Funktionstaste F1 (Netzwerkstatus) hat in Kombination mit den nachfolgenden Tasten die angegebene Funktion:<br>⓪ QR-Code mit allen folgenden Betriebsdaten / Status-Informationen, die über die Tasten Ⓕ1 und Ⓕ2 abgerufen werden können<br>① MAC Adresse<br>④ TCP Port<br>⑤ UDP Port<br>⑥ SICCT Terminal Name<br>• Die Funktionstaste F1 kann in folgenden Menüs gedrückt werden, um direkt einen QR-Code mit den in diesen Menüs dargestellten Parametern anzuzeigen:<br>○ [**LAN Parameter \21**] ➔ QR-Code: [**LAN-Parameter \374**]<br>○ [**SICCT Parameter \22**] ➔ QR-Code: [**SICCT-Parameter \375**]<br>○ [**Update \28**] ➔ QR-Code: [**Update Parameter \376**]<br>○ [**Service \3**] ➔ QR-Code: [**Betriebsdaten/Statistik \378**]<br>○ [**Status \32**] ➔ QR-Code: [**Status (Geräteselbstauskunft) \372**] |
|  | F2 Taste:<br>• Bei freier Texteingabe das Schriftzeichen **,** (Kommazeichen)<br>• Die Funktionstaste F2 (Verbindungsstatus) hat in Kombination mit den nachfolgenden Tasten die angegebene Funktion:<br>① TLS (Verbindungsstatus)<br>② SICCT Session (Verbindungsstatus)<br>③ SICCT Kommando Interpreter (Status)<br>④ DHCP Server (siehe Tabelle 25 auf Seite 112 im ANHANG)<br>⑤ VPN Status<br>⑥ Aktuell verwendeter Public Key-Index (Index: 1 bis 3) des aktuellen Pairing Blocks (PB-1 bis PB-3)<br>(Nur bei bestehendem Pairing und aktiver TLS Verbindung zwischen Terminal und Konnektor) |
|  | Cursor-Taste (nach oben):<br>• Im Menü mit dem grünen ▶ Cursor einen Menüpunkt nach oben springen |
|  | Cursor-Taste (nach unten):<br>• Im Menü mit dem grünen ▶ Cursor einen Menüpunkt nach unten springen |

| Taste | Funktion |
|---|---|
|  | Cursor-Taste (nach links):<br>• Eine Menüebene zurückspringen |
|  | Cursor-Taste (nach rechts):<br>• In das Untermenü springen, auf den der grünen ▶ Cursor gerade zeigt |
|  | STOP Taste:<br>• Abbrechen einer Aktion<br>• Eine Menüebene zurückspringen<br>• Durch langes Drücken im Ruhebildschirm (ca. 3 Sekunden): Ausschalten des Gerätes |
|  | CLEAR Taste:<br>• Löschen eines Wertes links neben dem Eingabecursor |
|  | MENU Taste:<br>• Im Ruhebildschirm: Öffnen des Hauptmenüs<br>• Im Hauptmenü und Untermenüs: Zurück in den Ruhebildschirm |
|  | OK Taste:<br>• Einschalten des Gerätes<br>• In das Untermenü springen, auf das der grünen ▶ Cursor gerade zeigt<br>• Eingabebestätigungen |

## 1.5. Displaysymbole und ihre Bedeutung

Die Symbolleiste unter dem Textfeld des Displays zeigt die aktuellen Zustände bzw. Aktivitäten an. Bis zu 10 Symbole können angezeigt werden, wobei in der aktuellen Version am Symbolplatz fünf keine Symbole angezeigt werden. Die folgenden Tabellen geben einen Überblick über deren Bedeutung.




### 1.5.1. Symbol 1 bis 4: Karten-Kontaktiereinheiten

| Symbol 1 für die eGK / KVK | Symbol 2 für den HBA | Symbol 3 für SMC-B / gSMC-KT | Symbol 4 für SMC-B / gSMC-KT | Bedeutung |
|---|---|---|---|---|
|  |  |  |  | Die Kontaktiereinheit ist leer |
|  |  |  |  | Es steckt eine Karte in der Kontaktiereinheit. |
|  |  |  |  | Die Karte in der Kontaktiereinheit ist aktiviert. |
|  |  |  |  | Es findet ein Datenaustausch mit der Karte in der Kontaktiereinheit statt. |
|  |  |  |  | Es ist ein Fehler aufgetreten. |
|  |  |  |  | Das Karten-Symbol blinkt bei einer sicheren PIN-Eingabe. Anhand des blinkenden Icons kann man erkennen, für welche Karte die PIN-Eingabe angefordert wird. Bei der Remote-PIN Eingabe für einen HBA, der sich außerhalb des Terminals befindet, blinkt das Symbol der Kontaktiereinheit, in der sich die gSMC-KT Karte befindet. |

### 1.5.2. Symbol 6: Datenverkehr zu angeschlossenen Geräten

| Symbol | Bedeutung |
|---|---|
|  | Es besteht noch keine SICCT-Session über die LAN-Schnittstelle. |
|  | Es besteht eine “SICCT Control Session“ TLS Verbindung. |
|  | Es besteht eine “SICCT Admin Session“ TLS Verbindung. |
|  | VPN Verbindung ist konfiguriert und aktiviert, aber noch nicht aufgebaut |
|  | VPN Verbindung ist konfiguriert und aktiviert. Ein “SICCT Control Session“ TLS Verbindung ist aktiv, aber die VPN-Verbindung besteht zurzeit nicht. |
|  | VPN Verbindung ist konfiguriert und aktiviert. Ein “SICCT Admin Session“ TLS Verbindung ist aktiv, aber die VPN-Verbindung besteht zurzeit nicht. |
|  | VPN Verbindung ist aufgebaut. Es besteht noch keine SICCT-Session |
|  | VPN Verbindung ist aufgebaut und es besteht eine “SICCT Control Session“ TLS Verbindung. |
|  | VPN Verbindung ist aufgebaut und es besteht eine “SICCT Admin Session“ TLS Verbindung. |

### 1.5.3. Symbol 7: Interne Stützbatterie schwach

| Symbol | Bedeutung |
|---|---|
|  | Die interne Stützbatterie des Terminals verfügt nur noch über eine geringe Restkapazität. Das Terminal muss zeitnahe gegen ein neues Gerät getauscht werden.<br>Das Terminal verfügt über eine interne Batterie, die auch bei ausgeschaltetem Gerät die Sicherheitsschaltungen, die das Terminal gegen Manipulationsversuche schützen mit Spannung versorgt. Die Kapazität dieser Stützbatterie ist für eine Betriebszeit von vielen Jahren ausgelegt. Wenn die Batterie verbraucht ist, wird automatisch ein Sicherheitsalarm ausgelöst und das Terminal kann nicht mehr genutzt werden. |

### 1.5.4. Symbol 8: Konfiguration als Signaturterminal außerhalb der Telematikinfrastruktur

| Symbol | Bedeutung |
|---|---|
|  | Dieses Icon zeigt an, dass das Terminal außerhalb der Telematikinfrastruktur als Signaturterminal eingesetzt wird. Es kann nicht mehr als eHealth-Terminal bei einem LEI innerhalb der Telematikinfrastruktur verwendet werden. |

### 1.5.5. Symbol 9: Allgemeiner Gerätestatus

| Symbol | Bedeutung |
|---|---|
|  | Dieses Icon zeigt an, dass Sie die Cursortasten verwenden können, um im Bildschirmmenü zu navigieren. |

### 1.5.6. Symbol 10: Datenverwaltung

| Symbol | Bedeutung |
|---|---|
|  | Kein Zugang zu den Menüs:<br>• [**Einstellungen \2**]<br>• [**Admin-PIN ändern \31**]<br>• [**Werkseinstellung via Admin-PIN \331**]<br>• [**Kiosk-Modus\35**] |
|  | Zugang mit Admin-PIN geöffnet |

## 1.6. Begriffsbestimmung

| Begriff | Erläuterung |
|---|---|
| (Stationäres) Terminal | Kartenterminal, in dem Daten von Patientenkarten gelesen werden. In dieser Bedienungsanleitung werden die Begriffe Gerät und (stationäres) Terminal gleichbedeutend mit dem Kartenterminal ‚ORGA 6141 online' verwendet. |
| Administrator (kurz: Admin) | Person, die das Kartenterminal in Betrieb nimmt, konfiguriert und ggf. die Software aktualisiert. |
| AIS | Arztinformationssystem (Primärsystemsoftware) |
| Allgemein zugänglicher Bereich | Der sogenannte allgemein zugängliche Bereich umfasst all die Orte in einer Arztpraxis, in einer Apotheke oder in einer Station eines Krankenhauses (z. B. Wartebereich), die ständig oder zeitweise ohne wirksame Aufsicht oder einfache Zugangskontrolle sind.<br>Siehe auch: Zugänglicher Bereich, Gesicherte Umgebung |
| Anwender (kurz: User) | Personen, die das Kartenterminal bedienen. |
| AVS | Apothekenverwaltungssystem (Primärsystemsoftware) |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| DHCP | Dynamic Host Configuration Protocol<br>(ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server) |
| eGK | Elektronische Gesundheitskarte |
| FAT32 | File Allocation Table 32<br>(ein von Microsoft entwickeltes Dateisystem) |
| gematik | Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH |
| Gesicherte Umgebung<br><br>(kontrollierte Einsatz-umgebung) | Als gesicherte Umgebung (auch kontrollierte Einsatzumgebung genannt) gelten vom Betreiber administrierte zugängliche Bereiche, die unter ständiger Kontrolle durch Personal sind. Kann die Kontrolle für einen Zeitpunkt nicht ausgeübt werden, ist sichergestellt, dass weitere organisatorische Schutzmaßnahmen ergriffen werden (z. B. Verschließen von Räumen oder Wegschließen von Geräten).<br>Siehe auch: Zugänglicher Bereich, Allgemein zugänglicher Bereich |
| gSMC-KT | gerätespezifische Security Module Card Kartenterminal. Die gSMC-KT dient der Identifikation des individuellen Kartenterminals. |
| HBA | Heilberufsausweis<br>Der HBA identifiziert den Heilberufler (Arzt, Apotheker, Zahnarzt, …) als berechtigte Person. |
| ICCSN | Kartenkennnummer<br>(Integrated Circuit Card Serial Number) |
| KIS | Krankenhausinformationssystem (Primärsystemsoftware) |
| Kontrollierte Einsatzumgebung | Siehe „Gesicherte Umgebung" |
| Patientenkarte | Elektronische Gesundheitskarte (eGK) |
| PIN | Persönliche Identifizierungsnummer. Mit der Eingabe dieser Geheimzahl identifiziert sich eine Person als Inhaber oder als Nutzungsberechtigter von gespeicherten Daten oder Geräte-einstellungen. |

| Begriff | Erläuterung |
|---|---|
| Primärsystem | Computer, an dem die Software PVS/AVS/KIS ausgeführt wird und mit dem Kartenterminal kommuniziert. |
| Primärsystemsoftware | Software, die auf dem Primärsystem installiert ist und bei Arzt / Apotheke / Krankenhaus eingesetzt wird. |
| PUK | Personal Unblocking Key<br>Ein PUK ist ein elektronischer Schlüssel, der zum Entsperren einer Chipkarte dient, nachdem eine PIN mehrmals falsch eingegeben wurde. |
| PVS | Praxisverwaltungssystem (Primärsystemsoftware) |
| Reset Administrator | Der Reset Administrator ist derjenige, der in der Lage ist, das Terminal auch ohne bekannte Admin-PIN wieder in die Werkseinstellung zurück zu versetzen, falls dem Administrator die Admin-PIN nicht mehr bekannt ist.<br>Bei ORGA eHealth Terminals ist es mit einem sogenannten Challenge-Response-Verfahren nur Ingenico Healthcare möglich, sie wieder in den Auslieferungszustand zurück zu versetzen. |
| SAK | Signaturanwendungskomponente |
| SICCT | Secure Interoperable ChipCard Terminal<br>Die SICCT-Spezifikation ist Grundlage des Kommunikationsstandards für die Online-Telematikinfrastruktur im deutschen Gesundheitswesen. |
| SMC | Security Module Card (siehe auch SMC-B und gSMC-KT) |
| SMC-B | Betriebsstättenkarte - die SMC-B (B = Betriebsstätte) dient der Identifikation einer berechtigten Institution im Gesundheitswesen (z. B. Arztpraxis). |
| TLS | Transport Layer Security (Transportschichtsicherheit)<br>Ein hybrides Verschlüsselungsprotokoll zur sicheren Daten-übertragung im Internet. |
| TLS-PU | TLS für die Produktionsumgebung |
| TLS-RU | TLS für die Referenzumgebung |
| TLS-TU | TLS für die Testumgebung |
| TLS-LU | TLS für die Laborumgebung<br>(dient dem alleinigen Test- und Instantsetzungsprozessen des Terminals in der Laborumgebung des Terminalherstellers) |
| TLS-SU | TLS für die Signaturumgebung<br>(nur für Einsatz mit einer Signaturanwendungskomponente) |
| IPsec VPN | Virtual Private Network mit sichererer Internet Protocol Security Kommunikation |
| Zugänglicher Bereich | Der sogenannte zugängliche Bereich umfasst all die Orte in einer Arztpraxis, in einer Apotheke oder in einer Station eines Krankenhauses (z.B. Empfangstresen), die ständig unter wirksamer Aufsicht oder einfacher Zugangskontrolle sind.<br>Siehe auch: Allgemein zugänglicher Bereich, Gesicherte Umgebung |

Tabelle 1: *Begriffsbestimmung*

# 2. Sicherheit

Dieser Abschnitt behandelt die Sicherheit beim Umgang mit dem des ORGA 6141 online und der Vorgehensweise bei der Prüfung des vertrauenswürdigen und zugelassenen Zustandes des ORGA 6141 online.

ACHTUNG!
Lesen Sie diesen Abschnitt aufmerksam durch, damit Sie jeder Zeit in der Lage sind den vertrauenswürdigen und zugelassenen Zustand des Gerätes anhand der in diesem Abschnitt beschrieben Sicherheitsmerkmale zu überprüfen.

## 2.1. Gerätesicherheit

Das stationäre Terminal ORGA 6141 online ist für den Einsatz im deutschen Gesundheitswesen vorgesehen. Es erfüllt die Anforderungen der Kassenärztlichen Bundesvereinigung (KBV) zum Lesen der Krankenversicherungskarte (KVK) und die Anforderungen der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) zur Verarbeitung der elektronischen Gesundheitskarte (eGK) und des Heilberufsausweises (HBA). Zu den Anforderungen gehört, dass der Benutzer des Gerätes sich mit dem Gebrauch vertraut macht und die einwandfreie Funktion und die Sicherheitsmerkmale am Gerät regelmäßig überprüft.

## 2.2. Sicherheitsmerkmale

ACHTUNG!
Das Gerät verfügt über mehrere Sicherheitsmerkmale, die es ihnen ermöglichen die Integrität des Gerätes zu überprüfen und sicher zu stellen, dass das Gerät nicht beschädigt, manipuliert oder anderweitig zweckentfremdet wurde.
Sie sind aus datenschutzrechtlichen Gründen verpflichtet, die Integrität des Gerätes täglich vor Inbetriebnahme zu überprüfen!

### 2.2.1. Das Gehäusesiegel und seine Eigenschaften

Das Gerät ist an drei Stellen mit einem Gehäusesiegel versiegelt, um es vor unerlaubtem Öffnen zu schützen. Der Bundesadler und rechts daneben das BSI Logo sind auf dem Siegel abgebildet. Die Farben des Siegels verändern sich je nach Betrachtungswinkel zwischen gold, ocker und grün.



Abbildung 1: *Unbeschädigtes Gehäusesiegel*


Abbildung 2: *Beschädigtes Gehäusesiegel*


Abbildung 3: *Fehlendes Gehäusesiegel*

Unterhalb des BSI Logos ist die schwarz gedruckte, verkürzte BSI-Zulassungsnummer des Gerätes zu finden. Beim stationären ORGA eHealth Terminal lautet sie: DSZ0519.
Am rechten Rand der Siegel befindet sich die Siegelnummer, die bei alle drei Siegeln des Gerätes unterschiedlich ist.
Unter einer speziellen Schwarzlichtlampe (UV) wird der Schriftzug "SECURITY" mehrzeilig über die ganze Siegelfläche sichtbar. Ein gefälschtes Siegel ist an den fehlenden Sicherheitsmerkmalen zu erkennen.

Bei einer Manipulation spalten sich die Schichten des Siegels und die sich lösende Schicht zerfällt in kleine Bruchstücke. Die Abbildung 1 links zeigt das Siegel unversehrt, die mittlere Abbildung 2 zeigt das Siegel nach einer partiellen Ablösung und dem Versuch eines deckungsgleichen Wiederaufbringens. In Abbildung 3 sind nur noch die Rückstände zu sehen, wenn das Siegel ganz entfernt wurde.
Die genaue Position der Gehäusesiegel können Sie der Abbildung 7 auf Seite 26 entnehmen.



ACHTUNG!
Wenden Sie sich an Ihren Administrator, wenn eins der Siegel beschädigt ist bzw. wenn Sie Zweifel an der Echtheit der Siegel haben.



ACHTUNG!
Notieren Sie sich am besten alle Siegelnummern Ihres eHealth Kartenterminals, um sicher zu stellen, dass sich tatsächlich die originalen und keine gefälschten Gehäusesiegel auf dem Gerät befinden.



ACHTUNG!
Verwenden Sie das Gerät so lange nicht weiter, bis zweifelsfrei die Echtheit und Unversehrtheit der Siegel geklärt ist.

### 2.2.2. Das Slotsiegel und seine Eigenschaften

Das ORGA 6141 online verfügt über zwei Karteneinschübe am linken Gehäuserand, die für die Verwendung von gSMC-KT bzw. SMC-B Karten vorgesehen sind. Wenn eine SMC-Karte vom Administrator eingesteckt wurde, hat er den Kartenschlitz anschließend mit einem von ihm signierten Slotsiegel von Ingenico Healthcare versiegelt, um eine unbemerkte Entnahme der SMC-Karte zu verhindern. Zur Identifikation befindet sich eine eindeutige Siegelnummer am Rand des Slotsiegels. Die Farben des Aufdrucks „Ingenico“ verändern sich je nach Betrachtungswinkel zwischen gold, ocker und grün.



Abbildung 4: *Unbeschädigtes Slotssiegel*



Abbildung 5: *Beschädigtes Slotssiegel*



Abbildung 6: *Fehlendes Slotssiegel*

Unter einer speziellen Schwarzlichtlampe (UV) wird der Schriftzug "SECURITY" mehrzeilig über die ganze Siegelfläche sichtbar. Ein gefälschtes Siegel ist an den fehlenden Sicherheitsmerkmalen zu erkennen.
Bei einer Manipulation spalten sich die Schichten des Siegels und die sich lösende Schicht zerfällt in kleine Bruchstücke. Die Abbildung 4 links zeigt das Siegel unversehrt, die mittlere Abbildung 5 zeigt das Siegel nach einer partiellen Ablösung und dem Versuch eines deckungsgleichen Wiederaufbringens. In Abbildung 6 sind nur noch die Rückstände zu sehen, wenn das Siegel ganz entfernt wurde.

ACHTUNG!
Wenden Sie sich an Ihren Administrator, wenn das Siegel beschädigt ist bzw. wenn Sie Zweifel an der Echtheit des Siegels haben.

ACHTUNG!
Erfassen Sie bzw. lassen Sie Ihren Administrator die Slotsiegelnummern erfassen, indem diese mit der entsprechenden Seriennummer des Kartenterminals notiert und archiviert wird.

### 2.2.3. Regelmäßiges Prüfen der Gehäuse- und Slotsiegel

Um Manipulationen am Gerät zu erkennen, ist eine regelmäßige Prüfung der Gehäuse- und Slotsiegel erforderlich. Insbesondere vor der Inbetriebnahme zu Dienstbeginn und nach Mittagspausen sowie nach längeren Abwesenheiten vom Einsatzort des Terminals, sind die Siegel auf Unversehrtheit und Echtheit zu überprüfen. Die Lage der Siegel ist in der Abbildung 7 dargestellt.

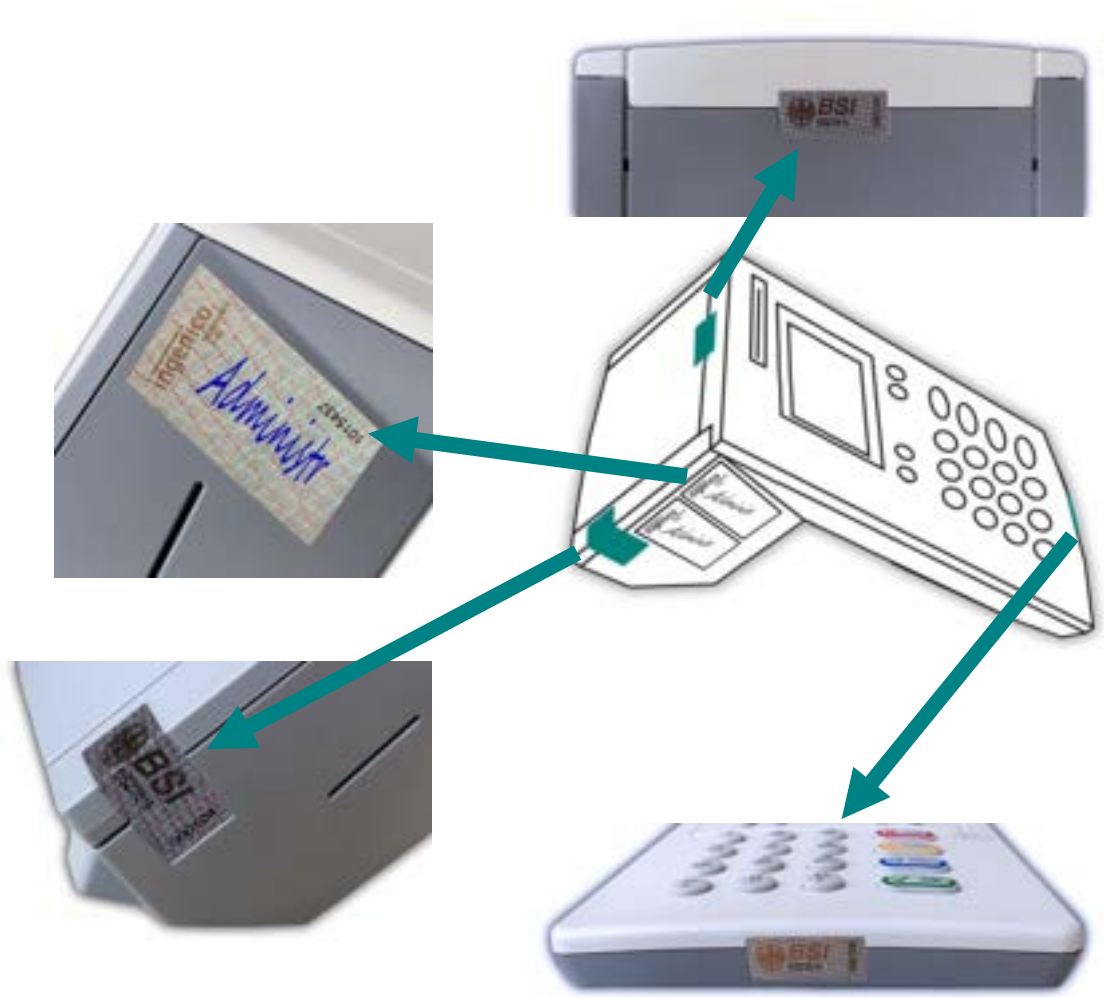


Abbildung 7: *Positionen der Gehäuse- und Slotsiegel am Gehäuse des Gerätes*

HINWEIS
Neben der Kontrolle der Signatur auf einem Slotsiegel beachten Sie die zuvor notierte Siegelnummer sowie die zugeordnete Seriennummer des Kartenterminals während der Prüfung.

HINWEIS
Berühren Sie beim Umgang mit dem Gerät möglichst nicht die Siegel bzw. behandeln Sie diese mit Vorsicht, um sie nicht zu beschädigen.

### 2.2.4. Geräteversion

Die Zertifizierung des Gerätes erfolgt nach CC = Common Criteria. Die vollständige BSI-Zertifizierungsnummer ist: BSI-DSZ-CC-0519. Auf den Gehäusesiegeln finden Sie die verkürzte Nummer: DSZ0519
Welche Geräteversion zertifiziert ist, finden Sie unter anderem im Internet auf den Seiten des BSI (Bundesamt für Sicherheit in der Informationstechnik):

http://www.bsi.bund.de

Vergleichen Sie die Angaben auf den BSI-Seiten mit der Version der Gerätesoftware, die im Menü [**Status \32**] (siehe Abschnitt »Versionsstand / Selbstauskunft des Terminals« auf Seite 5) des Gerätes angezeigt wird.

### 2.2.5. Integritätsprüfung

Das Gerät wird bei jedem Einschalten einer Hard- und Softwareprüfung unterzogen. Sollten die im Terminal integrierten Schutzmaßnahmen gegen Manipulationsversuche aktiviert worden sein (Hardwareprüfung), deutet dies auf einen unerlaubten Manipulationsversuch des Terminals hin. Im Display erscheint die Anzeige: **SICHERHEITSALARM.** Das Terminal kann nicht mehr in Betrieb genommen werden und muss zum Service beim Hersteller eingeschickt werden. Das Ergebnis der Softwareprüfung wird mit einem Vorgabewert verglichen. Ist das Ergebnis korrekt, geht das Gerät in Betrieb. Bei einem Fehler erscheint die Anzeige: **Fehler Integrität.** Tritt dieser Fehler auf, ist das Gerät ebenfalls einzuschicken, die Software ist defekt und eine einwandfreie Funktion unter Umständen nicht mehr gegeben. Die Software-Integritätsprüfung ist auch einer der Tests, die Sie im Menü [**Integrität \3428**] aufrufen können. Wird hierbei ein Fehler angezeigt, wird das Gerät mit dem nächsten Einschalten nicht mehr in den Betriebsmodus gehen.

### 2.2.6. Typenschild




Abbildung 8: *Typenschild mit zulässigem Herstellcode HC 03000000010301 oder HC 03000000020301*

Das Typenschild befindet sich auf der Geräterückseite oberhalb der Anschlüsse. Auf dem Typenschild steht unter anderem der Herstellername "Ingenico Healthcare", der Gerätename "ORGA 6141", die Information, welchen Herstellcode (HC) das Gerät hat, die einmalige Seriennummer (SN) des Gerätes und die Media-Access-Control-Adresse (MAC).

ACHTUNG!
Die Abbildung 8 zeigt die zulässige Position des am Gehäuse aufgeklebten Typenschilds, dessen und weitere Angaben Sie (bis auf den Herstellcode HC) über die Menüsteuerung des Gerätes (siehe Abschnitt 7.3.2 »Die Terminalselbstauskunft [Status \32]« auf Seite 84) kontrollieren können.
Bitte beachten Sie, dass aus Sicherheitsgründen außer dem Typenschild, den Geräte- und den Slotsiegeln (s. Abbildung 7) keine weiteren aufgeklebten Markierungen (Aufkleber) vorgesehen sind und nicht auf dem Gerät angebracht werden dürfen.

## 2.3. Sicherheit bei der Inbetriebnahme

Bei der Entwicklung des stationären Kartenterminals ORGA 6141 online haben wir größten Wert darauf gelegt, die administrativen Abläufe bei der Patientendatenerfassung so einfach wie möglich zu gestalten. Aufgrund der hohen Anforderungen an die Datensicherheit der Patientendaten ist es unsere Pflicht, Sie auch über weitere allgemeine Sicherheitshinweise beim Umgang mit einem stationären Kartenterminal zu unterrichten. Lesen Sie bitte vor der Inbetriebnahme die folgenden Sicherheitshinweise sorgfältig durch und beachten Sie sie bei Ihrer täglichen Arbeit mit dem Kartenterminal.

### 2.3.1. Aufstellungshinweise

ACHTUNG!
Aus Gründen der Datensicherheit darf das Kartenterminal bei der Verwendung nur in einer gesicherten Einsatzumgebung betrieben werden (gesicherter Bereich), in der es nie unbeaufsichtigt ist.

ACHTUNG!
Nach Dienstschluss ist das Gerät in einem verschlossenen Raum zu verwahren. Es ist sicherzustellen, dass unbefugte Personen keinen Zugang zum Gerät und angeschlossenen Systemeinheiten haben.

ACHTUNG!
Das Gerät darf nur von geschultem Personal bedient bzw. nur unter Aufsicht des geschulten Personals betrieben werden.

### 2.3.2. Admin-PIN Eingabe bei der Inbetriebnahme

Bei der ersten Inbetriebnahme muss als erstes eine aus acht Ziffern bestehende Administrator-PIN (Admin-PIN) vom Administrator vergeben werden.

ACHTUNG!
Wenn Sie nicht der Administrator sind, brechen Sie den Vorgang ab und informieren Sie Ihren Administrator, damit dieser zunächst die Konfiguration des Terminals für Sie vornimmt.

ACHTUNG!
Wenn Sie Administrator sind, lesen Sie bitte zunächst das Kapitel 3 »Bedienungsanleitung für den Administrator«, bevor Sie fortfahren.

### 2.3.3. Eingabe einer Karten PIN nach Aufforderung

Nach dem Stecken einer Karte können Sie zum Aktivieren bzw. Freischalten der Karte oder zur Durchführung bestimmter sicherheitsrelevanter Funktionen zwecks Berechtigungsprüfung zu einer Karten PIN Eingabe aufgefordert werden. Die Karten PIN hat nichts mit der Administrator-PIN des Gerätes zu tun. Sie dient der Authentisierung gegenüber der Karte. Bitte achten Sie

darauf, dass Sie, aber auch andere Benutzer, die die PIN ihrer Karte eingeben müssen, bei der Eingabe der PIN nicht beobachtet werden und ihre Karten PIN geheim halten. Die PIN Eingabe erfolgt auf der Kartenlesertastatur. In dem Hinweis zur sicheren PIN Eingabe (folgender Abschnitt) wird der Ablauf genau beschrieben.

#### 2.3.3.1. Der sichere PIN Eingabe Modus

Die Aktivierung dieser sicheren Betriebsart (Sicherer PIN Eingabemodus / secure PIN-entry mode) wird dadurch angezeigt, dass die einzugebenden PIN Ziffern durch blinkende Schlosssymbole 🔒 im Display dargestellt werden. Nur wenn diese Symbole erscheinen, ist sichergestellt, dass die eingegebene PIN ausschließlich zur gesteckten Karte übertragen wird. Die Durchführung der Signatur im Kartenterminal beginnt mit der Ausgabe des Anzeigetextes: **Bitte Geheimzahl eingeben** und in der Zeile darunter 🔒🔒🔒🔒🔒🔒🔒🔒 für die Eingabe einer z. B. achtstelligen PIN.
Der sichere PIN Eingabe Modus wird zusätzlich durch ein Maskierungsgeräusch (Rauschen) zur Verhinderung akustischer Ausspähversuche während der gesamten PIN Eingabe begleitet.
Im sicheren PIN Eingabe Modus blinkt zusätzlich ein Symbol im Display. Anhand des blinkenden Symbols der entsprechenden Kontaktiereinheit kann man erkennen, für welche Karte die PIN-Eingabe angefordert wird. Wenn mehrere Gesundheitskartenterminals in einer Arztpraxis oder einem medizinischen Versorgungszentrum im Einsatz sind, befindet sich der HBA des zuständigen Arztes nicht notwendiger Weise direkt im Terminal, an dem die PIN-Eingabe für diesen HBA erfolgen muss. Bei dieser sogenannten Remote-PIN Eingabe bei der eine PIN-Eingabe für einen HBA erfolgt, der sich außerhalb des Terminals befindet, blinkt das Symbol der Kontaktiereinheit, in der sich die gSMC-KT Karte befindet



ACHTUNG!
PINs müssen stets unbeobachtet eingegeben werden. Die Eingabe einer PIN darf nur dann erfolgen, wenn die 🔒-Symbole anzeigen, dass eine PIN Eingabe erwartet wird.



ACHTUNG!
Nur die höchstmögliche Lautstärke zehn des Maskierungsrauschens ist als ausreichend sicher gegen Ausspähversuche zu betrachten. Diese Lautstärke ist für einen zertifizierten und zugelassenen Betriebszustand zu wählen.

#### 2.3.3.2. Fehlerfreier Ablauf

Geben Sie die Karten PIN über die Tastatur nur ein, wenn die Schlosssymbole dargestellt werden. Die abgefragte PIN (üblicherweise minimal sechs und maximal acht Ziffern) wird im Display nach der Eingabe mit einem Sternchen pro eingegebener Ziffer angezeigt. Bestätigen Sie abschließend mit der OK-Taste. Anschließend wird das PIN Kontrollkommando zur Chipkarte übertragen. Bei erfolgreicher Eingabe der korrekten PIN wird im Display der Anzeigetext **Aktion erfolgreich** ausgegeben.

#### 2.3.3.3. Ablauf bei inkorrekter Karten PIN Eingabe

Der Ablauf ist derselbe wie bei der Eingabe der korrekten PIN, doch wird der Anzeigetext: **Geheimzahl falsch / gesperrt** ausgegeben.

#### 2.3.3.4. Ablauf bei Abbruch der Karten PIN Eingabe durch den Benutzer

Drückt der Benutzer vor Abschluss der PIN Eingabe die STOP-Taste, wird kein Kommando zur Chipkarte geschickt und im Display wird der Anzeigetext: **Abbruch** ausgegeben.

#### 2.3.3.5. Ablauf im Fall von Zeitüberschreitung bei Eingabe der Karten PIN

Erfolgt nach der Eingabeaufforderung nicht innerhalb von 30 Sekunden die Eingabe der ersten Ziffer oder verstreicht mehr Zeit als 30 Sekunden bis zur Eingabe der jeweils nächsten Ziffer, wird im Display der Anzeigetext **Abbruch** ausgegeben. Hat der Benutzer nur das Drücken der OK-Taste vergessen, fordert das Kartenterminal den Benutzer mit dem Anzeigetext: **Bitte Eingabe bestätigen** zur Bestätigung der eingegebenen Geheimzahl auf.
Die Funktionsabläufe nach der Konfiguration des Gerätes werden von der Verwaltungssoftware auf dem PC gesteuert. Im Alltag sind nur wenige Handgriffe zur Bedienung notwendig.

## 2.4. Logging und Änderungsprotokollierung

Ein eHealth Kartenterminal darf zur Analyse von Fehlerursachen und zur Performance-Auswertung optional vorbestimmte Zustände erfassen, strukturiert intern abspeichern und an berechtigte Anwender (i.d.R. den Administrator) ausgegeben. Dieser Vorgang wird als allgemein (Fehler-) Logging bezeichnet und verbietet explizit die Inklusion und Datenhaltung von Daten der Telematik Infrastruktur (i.d.R. zu schützende Daten der eingesetzten Karten).
Die ebenso optionale Protokollierung von Modifikationen der Betriebsdaten des Kartenterminals wird als Änderungsprotokollierung bezeichnet und unterscheidet sich vom Fehlerlogging, da hiermit (i.d.R. erfolgreiche) Veränderungen der Geräteparametrisierung z.B. der neue Versionsstand nach einem erfolgten Update der Geräte-Firmware vermerkt werden.
Das ORGA 6141 online kann mit der aktuellen Firmware 3.8.1 Betriebszustände, Fehlerereignisse und Nutzungsdaten protokollieren. Dabei werden ausschließlich Daten erfasst, die nicht zu schützende Daten der Telematikinfrastruktur sind.
Welche Betriebsdaten protokolliert und dargestellt werden, können Sie im Abschnitt 7.3.7 »Terminal Konfigurationen und Betriebszustände via QR-Codes auslesen« auf Seite 92 nachlesen.
Die Sichtung und Auswertung dieser Daten sollten durch den Administrator erfolgen. Sie helfen ihm im Falle von Fehlfunktionen des Terminals im laufenden Betrieb oder bei Problemen bei der Verbindung mit dem Konnektor die Fehlerursache schnell zu lokalisieren und zu beheben.

## 2.5. Sicherheit bei der Außerbetriebnahme und im Reparaturfall

Das ORGA 6141 online ist ein sicherheitstechnisch sensibler Bestandteil der Telematik-infrastruktur in Ihrer Praxis. Wenn Sie das Gerät nicht mehr für die tägliche Datenerfassung verwenden, weil es defekt ist oder Sie es gegen ein anderes Gerät austauschen wollen, ist es Ihre Pflicht, bei der Außerbetriebnahme des Terminals ein paar wichtige Dinge zu beachten und zu befolgen. Lesen Sie sich deshalb bitte folgende Hinweise aufmerksam durch und führen Sie folgende Schritte aus:

1. Vergewissern Sie sich, dass der Administrator alle wichtigen Parameter des Gerätes kennt und notiert hat.

2. Führen Sie einen Werksreset durch.

(siehe Abschnitt 7.3.3 »Zurücksetzen des Terminals in den Auslieferungszustand [Werkseinstellung \33]« auf Seite 85)



ACHTUNG!
Es müssen bei der Außerbetriebnahme alle im Terminal gespeicherten Pairing-Informationen gelöscht werden. Dies geschieht durch den Werksreset! Unmittelbar nach einem Werksreset muss die Admin-PIN neu vergeben werden.



ACHTUNG!
Geben Sie unmittelbar nach dem erfolgreichen Werksreset eine neue Admin-PIN ein, um das Terminal vor unerlaubtem Zugriff zu schützen.

3. Entfernen Sie den HBA aus der Kontaktiereinheit 2 (siehe Abschnitt 4.8 »Einstecken eines HBA in die Kontaktiereinheit 2« auf Seite 45) und die SMC-B und gSMC-KT Karten aus den Kontaktiereinheiten 3 und 4 (siehe Abschnitt 3.3 »Die Kontaktiereinheiten 3 und 4 für die SMC-Karten« auf Seite 40). Bewahren Sie Ihren HBA und die SMC-Karten an einem sicheren Ort auf.
4. Führen Sie je nach Grund der Außerbetriebnahme abschließend folgende Aktion aus:
    a. Bei Einsendung des Gerätes im Gewährleistungsfall:
    Trotz strenger und sorgfältiger Qualitätskontrollen bei der Auslieferung unserer Geräte, kann es in seltenen Fällen zu Verbindungsproblemen oder Funktionsstörungen der Geräte kommen. Dies kann viele Ursachen haben und nicht immer liegen diese in einer Funktionsstörung des Kartenterminals.
    Die Kartenlesegeräte für die Online-Telematikinfrastruktur wurden Ihnen über einen sicheren Versandweg in die Praxis geliefert, um die Integrität der Geräte zu gewährleisten. Ein Versand zurück zu Ihrem Lieferanten oder dem Hersteller ist aus sicherheitstechnischen Gründen nicht vorgesehen und führt unweigerlich zum Verlust der Integrität des Gerätes, da eine Manipulation des Terminals nicht mehr ausgeschlossen werden kann. Aus diesem Grund können wir keine Reparaturen an diesen Geräten vornehmen.
    Zur Inanspruchnahme berechtigter Gewährleistungsansprüche haben wir eine Checkliste mit dem Titel „Rücksendeformular / Endnutzer Checkliste bei Verbindungsproblemen mit ORGA online Geräten für den OPB1-Betrieb“ auf unserer Homepage unter „Service > Download Center“ zum Download bereitgestellt. Bitte führen Sie die in dieser Checkliste aufgeführten Funktionstests durch und füllen Sie die Checkliste vollständig aus. Setzen Sie sich vor der Einsendung des Terminals unbedingt mit Ihrem Lieferanten in Verbindung, um den Gewährleistungsanspruch und -prozess vorm Versenden des Terminals zu klären!



ACHTUNG!
Eine Reparatur von ORGA Gesundheitskartenterminals für die Online-Telematikinfrastruktur ist aus sicherheitstechnischen Gründen NICHT möglich.

HINWEIS!
Zur Inanspruchnahme berechtigter Gewährleistungsansprüche muss eine Checkliste ausgefüllt und zusammen mit dem Gesundheitskartenlesegerät eingeschickt werden. Laden Sie sich diese Checkliste von unserer Homepage aus dem Bereich „Service > Download Center“ herunter.

ACHTUNG!
Gewährleistungsansprüche sind gesetzliche Ansprüche des Endanwenders an den Verkäufer. Richten Sie Ihre Gewährleistungsforderungen an den Händler, bei dem Sie das Gesundheitskartenterminal erworben haben. Nur wenn Sie das Gerät direkt bei Ingenico Healthcare erworben haben, sind die Forderungen auch an Ingenico Healthcare zu richten!

Verpacken Sie das Terminal sicher für den Postversand an Ihren Händler oder Ingenico Healthcare und legen Sie dem Paket die vollständig ausgefüllte Checkliste bei.

ACHTUNG!
Senden Sie nur das Kartenterminal ohne Kabel oder sonstiges Zubehör ein.
Senden Sie keine HBA- bzw. SMC-Karten mit dem Gerät ein.
Notieren Sie keine Administrator-, HBA-, oder SMC-PIN auf dem Gerät oder Dokumenten, die Sie mit dem Gerät versenden.

ACHTUNG!
Führen Sie, wenn möglich einen Werksreset des Terminals durch und geben Sie unmittelbar nach dem erfolgreichen Werksreset eine neue Admin-PIN ein, um das Terminal vor unerlaubtem Zugriff zu schützen.

b. Bei Einlagerung des Gerätes als Ersatzgerät:
   Lagern Sie das Gerät an einem trockenen, warmen und sicheren Ort und schützen Sie das Gerät so vor unerlaubtem Zugriff von Dritten und Manipulationsversuchen.
c. Bei der endgültigen Entsorgung des Gerätes:
   Zerstören Sie die Gehäusesiegel am Gehäuse des Gerätes (siehe Abschnitt 2.2.1 »Das Gehäusesiegel und seine Eigenschaften« auf Seite 23) und beachten Sie die Entsorgungshinweise im Abschnitt 2.12 »Entsorgung des Gerätes« auf Seite 38.

ACHTUNG!
Beachten Sie bei der Wiederinbetriebnahme eines aus der Reparatur zurückkommenden Gerätes oder eines Gerätes, das Sie längere Zeit nicht benutzt haben (Ersatzgerät), dass Sie wie für ein Neugerät die allgemeinen Regeln und Anforderungen zur Betriebssicherheit des Gerätes beachten müssen (siehe Abschnitt 2.8 »Allgemeine Regeln & Anforderungen zur Betriebssicherheit des Gerätes« auf Seite 34).
Setzen Sie die SMC-Karten wieder in das Kartenterminal ein und versiegeln Sie die Kartenschlitze wieder, wie es im Abschnitt 5.7 »Einsetzen einer SMC-Karte und Versiegeln der Kontaktiereinheiten 3 und 4« auf Seite 52 beschrieben wird.

## 2.6. Normen und Richtlinien

Das ORGA 6141 online erfüllt die zutreffenden Normen im Geltungsbereich:

- Vibrationstest IEC 68-2-6
- Schocktest IEC 68-2-27 und 29
- Temperaturtests nach DIN EN 60068-2-1 und DIN EN 60068-2-2
- RoHS
- Elektromagnetische Verträglichkeit (siehe Konformitätserklärung)
- ISO 7816, Teil 1 - 10

## 2.7. Temperatur / Umgebungsbedingungen

Aus Gründen der Betriebssicherheit sollten das ORGA 6141 online und seine Anschlussleitungen nicht in der Nähe von HF-Störquellen oder starken Magnetfeldern (stationäre Telefone, Funkgeräte, Schaltnetzteile, Warensicherungssysteme usw.) platziert werden, da sonst die Datenübertragung gestört werden könnte.



ACHTUNG!
Schützen Sie das Gerät vor Feuchtigkeit und Staub, da sonst die Funktion der Kartenleser beeinträchtigt werden könnte.
Fremdkörper können leicht in den Kartenschlitz der Kontaktiereinheit 1 eindringen und zu Schäden im Gerät führen.
Verwenden Sie das Gerät nur in trockener Umgebung bei Temperaturen zwischen +5 °C bis +40 °C.

## 2.8. Allgemeine Regeln & Anforderungen zur Betriebssicherheit des Gerätes

Neben den Sicherheitsregeln bei der Inbetriebnahme müssen Sie eine Reihe von Maßnahmen treffen, um die Sicherheit Ihres Systems und der Patientendaten dauerhaft zu gewährleisten. Nehmen Sie das Gerät nicht in Betrieb, wenn Sie Zweifel an der Gewährleistung des sicheren Umgangs mit dem Gerät haben.



ACHTUNG!
Es dürfen nur Personen mit dem Gerät arbeiten, die die Bedienungsanleitungen gelesen haben und geübt sind im Umgang mit technischem Gerät.



ACHTUNG!
Vergewissern Sie sich vor der ersten Inbetriebnahme von der Unversehrtheit des Gerätes (Prüfen der Sicherheitsmerkmale, insbesondere der Siegel gemäß Beschreibung in Abschnitt 2.2.1 »Das Gehäusesiegel und seine Eigenschaften« auf Seite 23 und Abschnitt 2.2.2. »Das Slotsiegel und seine Eigenschaften« auf Seite 25).



ACHTUNG!
Der Anwender hat die gleiche hohe Sorgfaltspflicht im Umgang mit dem Gerät wie im Umgang mit den gespeicherten Patientendaten.



ACHTUNG!
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 10 Minuten verhindert.



ACHTUNG!
Ein Firmware-Update darf ausschließlich vom Terminal-Administrator durchgeführt werden. Der Administrator hat vor und während des Updates zu kontrollieren, dass:

- die richtige Firmware-Update Datei mit einer zugelassenen Firmware für das Update verwendet wird bzw. beim Push-Verfahren die richtige Update-Datei vom Server kopiert wird,
- beim Push-Verfahren die Datei vom richtigen PUSH SERVER (technisch TFTP-Server) bezogen wird (z.B. durch Kontrolle der IP-Adresse),
- beim Push-Verfahren der sog. PUSH SERVER (TFTP-Server) derart konfiguriert wird, dass der TFTP-Server per Logging-Funktionalität den Dateinamen, Zeitpunkt des Dateiabrufs (per TFTP-Request), Transferzeit und -dauer, Status sowie Ziel-IP-Adresse (TFTP-Request) für eine spätere Kontrolle festhält.
- Am Kartenterminal kontrolliert der Terminal-Administrator abschließend die geladene, aktive Firmware-Version.



ACHTUNG: Es besteht die Gefahr von Ausspähversuchen!
Um einen unbefugten Zugang zu vertraulichen Daten zu erhalten, ist das Ausspähen von geheimen Zugangsdaten wie z.B. der Admin- und HBA-PIN ein probates Mittel für Computerkriminelle. Diese Ausspähversuche können durch optische, elektromagnetische, akustische oder thermische Sensoren erfolgen. Beachten Sie deshalb folgende Vorsichtsmaßnahmen:

- Geben Sie eine geheime PIN nur so ein, dass die Eingabe auf dem Tastenfeld nicht von einer anderen Person oder einer im Umfeld des Terminals (ggf. versteckt) angebrachten Kamera beobachtet werden kann.
- Achten Sie auf verdächtige, technische Veränderungen im Umkreis von 10 cm um das Terminal herum oder unter dem Terminal. Sollten sich dort neue elektrische Geräte oder Installationen befinden, kontaktieren Sie umgehend den Administrator, um zu klären, ob diese technischen Veränderungen von ihm vorgenommen wurden.
- Achten Sie auch auf verdächtige Veränderungen im Umfeld des Terminals, die nicht vom Administrator vorgenommen wurden. Dies beinhaltet bspw. die Installation einer Webcam mit oder ohne eingebautes Mikrofon, Veränderungen der Sprechanlage für den Warte- und Behandlungszimmerbereich, Veränderungen der TK-Anlage, etc.
- Es sollten sich generell keine technischen Geräte mit Kamera oder Mikrofon (auch keine Mobil- oder Festnetztelefone) im Umkreis von einem Meter um das Terminal befinden.
- Im Radius von einem Meter zum Gerät darf sich keine Wand befinden, wenn sie sich nicht sicher sein können, was sich hinter dieser verbirgt (Gefahr von versteckten elektromagnetischen Sonden im Nebenraum bzw. benachbarten Wohn- oder Geschäftsräume).
- Nehmen Sie das Terminal bei Zweifeln so lange nicht in Betrieb, bis der Administrator das Umfeld um das Terminal herum auf Ausspähversuche untersucht hat.



ACHTUNG: Es besteht die Gefahr von Manipulationsversuchen!
Ein eHealth-Kartenterminal kann ein potentielles Angriffsziel von Computerkriminalität sein, die zum Ziel hat in den Besitz von vertraulichen Patientendaten zu gelangen. Deshalb sollten Sie vor jeder Benutzung das Gerät auf Manipulationen hin untersuchen:

- Prüfen Sie, ob das Gerät Veränderungen wie zum Beispiel Bohrungen aufweist, die unter Umständen mit Aufklebern verdeckt sind.
- Achten Sie auf Veränderungen am Karteneinführungsschlitz, dem Tastenfeld und insbesondere der Geräteunterseite.
- Nehmen Sie das Terminal bei Zweifeln so lange nicht in Betrieb, bis der Administrator die Installation des Terminals auf Manipulationsversuche untersucht hat.



ACHTUNG!
Überprüfen Sie regelmäßig vor der Nutzung und nach Abwesenheit die Unversehrtheit des Gerätes (Prüfen der Sicherheitsmerkmale, insbesondere der Gehäusesiegel inklusive ihrer eindeutigen Siegelnummer



ACHTUNG!
Prüfen Sie anhand der BSI-Webadresse http://www.bsi.bund.de, ob die Version der Gerätesoftware Menü [**`Status \32`**] und der Herstellcode (HC) auf dem Typenschild und die Zertifizierungsnummer auf den Siegeln mit dem zugelassenen Stand übereinstimmen.



ACHTUNG!
Überzeugen Sie sich davon, dass die Verkabelung an Ihrem eHealth Terminal im Originalzustand ist und keine zusätzlichen Teile angebracht sind. Schließen Sie das Gerät nicht an "fremde" PCs an.



ACHTUNG!
Während der Benutzung darf das Gerät niemals unbeaufsichtigt sein.
Übergeben Sie das Gerät niemals im aufgeschlossenen Zustand an andere. Verschließen Sie den Zugang, indem Sie so oft auf die STOP-Taste drücken, bis wieder der Ruhebildschirm angezeigt wird.



ACHTUNG!
PINs müssen stets unbeobachtet eingegeben werden. Die Eingabe einer PIN darf nur dann erfolgen, wenn die 🔒-Symbole anzeigen, 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.



ACHTUNG!
Notieren Sie sich die "persönlichen" Kennzeichen (Seriennummer und Gehäusesiegel Nummern) Ihres Gerätes als Identifizierungshilfe bei Ihren späteren Überprüfungen.



ACHTUNG!
Ändern Sie in regelmäßigen Abständen die Admin-PIN.
Vermeiden Sie bei Ihrer Wahl konstante oder auf-/absteigende Ziffernfolgen (00000000, 12345678 etc.), Datumswerte (Geburtstage, Jahrestage) oder Personalnummern, die leicht zu erraten sind.



ACHTUNG!
Um qualifizierte Signaturen zu erstellen, müssen Sie das Gerät mit einer bestätigten Signaturkarte (HBA) sowie einer bestätigten Signaturanwendungskomponente (Konnektor) betreiben.
(Liste der bestätigten Komponenten siehe www.bundesnetzagentur.de)



ACHTUNG!
Halten Sie die Firmware des Kartenterminals sowie die zugehörigen Treiber und Administrationsprogramme stets aktuell. Prüfen Sie dazu regelmäßig unsere Homepage unter www.ingenico.de/healthcare. Die zu den Firmwaren zugehörigen Bestätigungen zur QES sowie die Sicherheitszertifizierung nach Common Criteria finden Sie unter www.bundesnetzagentur.de sowie unter www.bsi.bund.de



ACHTUNG!
Angaben zur Version finden Sie für die Hardware auf dem Typenschild an der Unterseite des Gerätes sowie für die Firmware über die Menüsteuerung des Gerätes (siehe Abschnitt »Versionsstand / Selbstauskunft des Terminals« auf Seite 5).



ACHTUNG!
Neben der Hardware ist die Firmware ein sicherheitssensibles Element. Verwenden Sie aus diesem Grund nur zertifizierte und bestätigte Firmware-Versionen. Spielen Sie eine neue Firmware ein, so kann der Vorgang nicht abgebrochen werden. Es ist nicht möglich eine alte Vorgänger Firmware-Version, die sich nicht in der Firmware-Gruppe (Liste der zulässigen Firmware-Versionen) befindet, einzuspielen. Das Gerät prüft vor dem Anwenden der neuen Firmware, ob es sich um eine unveränderte, integre Version von Ingenico Healthcare handelt.

## 2.9. Sicherheit beim Anschluss an den Konnektor



ACHTUNG!
Verwenden Sie nur Originalzubehör und -kabel beim Anschluss des Terminals an den Konnektor.



ACHTUNG!
Überzeugen Sie sich in regelmäßigen Abständen davon, dass die Verkabelung im Originalzustand ist und keine zusätzlichen Teile angebracht sind.



ACHTUNG!
Schließen Sie das Gerät nicht an "fremde" Primärsysteme an.



ACHTUNG!
Stellen Sie sicher, dass Ihr Praxis-Netzwerk und die in Ihrem Primärsystem installierten Softwareprogramme auch durch entsprechende Maßnahmen vor dem Zugriff oder der Manipulation durch Unbefugte geschützt sind.
Wenden Sie sich umgehend an Ihren Administrator, wenn Sie sich nicht sicher sind oder Ihnen Unregelmäßigkeiten auffallen.

## 2.10. Reinigung und Pflege

Bitte reinigen Sie das Kartenterminal nur mit einem weichen, leicht feuchten Tuch. Durch die Reinigung mit einem trockenen Tuch kann das Kunststoffgehäuse elektrostatisch aufgeladen werden und zieht Staub besonders an. Vermeiden Sie den Einsatz von Putz- und Scheuermitteln sowie lösungsmittelhaltigen Stoffen.

## 2.11. Desinfektion

Sprühen Sie niemals Desinfektionsmittel direkt auf das Gerät. Es darf keine Flüssigkeit in das Gerät gelangen. Verwenden Sie am besten feuchte Desinfektionstücher. Das Gerät abzutupfen ist schonender als zu wischen. Die Siegel und die Bedruckung reagieren unter Umständen empfindlich auf zu intensiven Kontakt mit chemischen Flüssigkeiten und könnten sich im Laufe der Zeit beim Wischen ablösen bzw. unkenntlich werden.

## 2.12. Entsorgung des Gerätes



HINWEIS
Gemäß der EU-Richtlinie 2002/96/EG (WEEE-Richtlinie) müssen Elektro- und Elektronikgeräte, die dieses Symbol tragen, getrennt vom Hausmüll gesammelt werden, um eine ordnungsgemäße Wiederverwertung sicherzustellen.
Das Gerät beinhaltet eine interne Lithiumzelle für die Uhr und den Sicherheitsmechanismus.
Die Lithiumzelle muss an entsprechenden Sammelstationen abgegeben werden.



HINWEIS
Bitte treten Sie mit Ihrem Servicedienstleister in Kontakt, wenn Sie Fragen zur fachgerechten Entsorgung haben. Er hält weitere Informationen für Sie bereit.



ACHTUNG!
Lithiumbatterie niemals kurzschließen, beschädigen, erhitzen, verbrennen oder gewaltsam öffnen.

# Kapitel 2: Bedienungsanleitung für den Benutzer

Das Kapitel 2 »Bedienungsanleitung für den Benutzer« wendet sich sowohl an Administratoren wie auch an Anwender des Gerätes und enthält alle Informationen zur Handhabung und einfachen Bedienung des Gerätes in der täglichen Praxis.

## 3. Produktbeschreibung

### 3.1. Die Vorderseite des ORGA 6141 online




1: Kartenschlitz der Kontaktiereinheit 1 für die Patientenkarte (eGK)

2: Kartenschlitz der Kontaktiereinheit 2 für den Heilberufsausweis (HBA) am rechten Gehäuserand.

3: Großes Farbdisplay mit 400x240 Pixeln

4: Cursor-Tasten ◀ ▶ ▲ ▼ zur Menü-navigation

5: Ziffernblock mit Zahlentasten und Funktionstasten F1 [F1] und F2 [F2]

6: Menütasten STOP CLEAR MENU OK

Abbildung 9: *Gerätevorderseite*

HINWEIS!
Als Zubehör für Ihren Einsatzzweck bietet Ingenico Healthcare Terminalhalterungen für das ORGA 6141 online an. Diese sind sicher und robust für den komfortablen Einsatz am Point of Care konzipiert.

Die Komfort-Halterung verfügt über ein integriertes Schloss, mit dem das Kartenlesegerät schnell, zuverlässig und diebstahlsicher in der Halterung befestigt werden kann. Das Öffnen des Terminals oder das Anbringen eines Skimming-Aufsatzes werden so effektiv verhindert. Eine ungehinderte Überprüfung der Unversehrtheit der Gehäuse- und Slot-Siegel ist jederzeit gewährleistet.

## 3.2. Die Rückseite des ORGA 6141 online

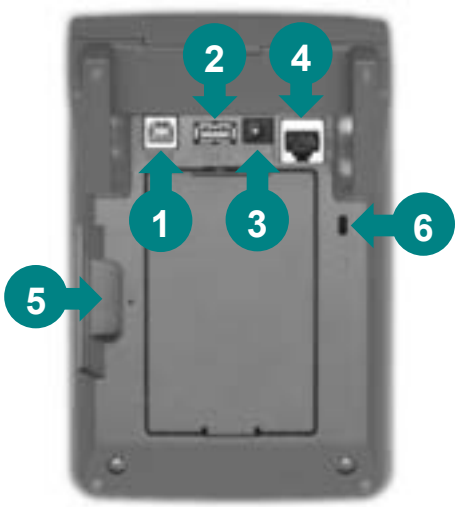



Abbildung 10: *Geräterückseite*

1: USB-B Buchse zum Anschluss eines USB-Kabels als alternative Spannungsversorgung über einen freien USB-Anschluss Ihres Primärsystems.
2: USB-A Anschluss für zukünftige Firmware-Updates per USB-Stick
3: Anschlussbuchse für Stromversorgung mit 7,5V Steckernetzteil
4: RJ-45 Buchse für LAN-Anschluss des Gerätes an den Konnektor
5: Kartenschlitz der Kontaktiereinheit 2 für den Heilberufsausweis (HBA)
6: Kensington-Lock Diebstahlsicherung

HINWEIS!
Der USB-B Anschluss kann nicht als Schnittstelle zum Anschluss ans Primärsystem verwendet werden, wie es vor dem Online-Produktivbetrieb der Telematikinfrastruktur üblich war. Als Schnittstellenverbindung steht ausschließlich die RJ-45 Buchse für einen LAN-Anschluss des Gerätes direkt am Konnektor zur Verfügung.

ACHTUNG!
Die Klappe auf der Rückseite des Gerätes bietet entgegen früherer Gerätekonfigurationen keine Erweiterungsmöglichkeit mehr für ein POE- bzw. LAN-Modul. Die darunter vorhandene Schutzfolie schützt das Gerät ausreichend vor Manipulation. Eine Verletzung der Folie löst den Sicherheitsalarm des Gerätes aus, der den Betrieb des Terminals irreversibel verhindert.
Das Terminal ist als Bestandteil der Praxis IT zu verstehen und im selben Maße zu schützen, weshalb im Bedarfsfall die Klappe mit der nötigen Vorsicht geöffnet und die Folie auf Unversehrtheit geprüft werden kann.

## 3.3. Die Kontaktiereinheiten 3 und 4 für die SMC-Karten




❶ Die SMC-Karte wird mit den Kontakten der Chipkarte zur Geräterückseite in eine der beiden Kontaktiereinheiten mit sanftem Druck eingesteckt, bis sie einrastet und vollständig im Kartenschlitz steckt
❷ Korrekt eingesteckte SMC-Karte
❸ Gehäusesiegel
❹ Slotsiegel mit individueller Nummer

Abbildung 11: *Die Kontaktiereinheiten 3 und 4 für die SMC-Karten*

Die beiden Kontaktiereinheiten 3 (unterer Kartenschlitz) und 4 (oberer Kartenschlitz) sind für die Aufnahme einer Signaturkarte im 2FF-Kartenformat (Mini-SIM) und weiterer applikationsspezifischer Smartcards vorgesehen. Im Gesundheitswesen werden dies die SMC-B und gSMC-KT sein. Die Karten können in den Kontaktiereinheiten 3 und 4 auf der linken Seite des Gerätes verwendet werden. Sie werden vom Administrator in die Kontaktiereinheiten gesteckt und mit einem Slotsiegel, das vom Administrator signiert wurde, versiegelt.

ACHTUNG!
Beim Einsatz des Terminals in der Online-Telematikinfrastruktur des deutschen Gesundheitswesens ist eine gSMC-KT Karten erforderlich, die sich unter einem vom Administrator unterschriebenen Slotssiegel im Gerät befinden muss.
**Wenn Sie Administrator sind**, lesen Sie bitte hierzu auch den Abschnitt 5.7 »Einsetzen einer SMC-Karte und Versiegeln der Kontaktiereinheiten 3 und 4« auf Seite 52.

# 4. Bedienung des Gerätes

## 4.1. Tastatur



Abbildung 12: *Tastatur des Gerätes*

Das stationäre Kartenterminal ORGA 6141 online verfügt über eine Tastatur mit 20 Tasten, bestehend aus den Zifferntasten 0 bis 9 [0 1 2 3 4 5 6 7 8 9], den Funktionstasten F1 [F1] und F2 [F2], sowie den Menü-Tasten (STOP-Taste [STOP], CLEAR-Taste [CLEAR], MENU-Taste [MENU] und OK-Taste [OK]). Die Cursor-Tasten [◀ ▶ ▲ ▼] dienen zur Auswahl von Optionen und Menüpunkten. Die Buchstaben unter den Zifferntasten zeigen eine Auswahl von Buchstaben an, die bei Freitexteingabe über die jeweilige Taste ausgewählt werden können. Eine ausführliche Übersicht über alle Funktionen der jeweiligen Tasten finden Sie im Abschnitt 1.4 »Funktionen der verschiedenen Tasten des Gerätes« auf Seite 15 dieser Bedienungsanleitung.

## 4.2. Ein- und Ausschalten des Gerätes

Wenn das ORGA 6141 online über den USB-B Eingang oder das Steckernetzteil mit Spannung versorgt wird, schaltet es sich automatisch ein. Es schaltet sich bei anliegender Spannungsversorgung nicht wieder automatisch aus. Jedoch wird der PIN-geschützte Bereich 30 Sekunden nach der letzten Aktion des Benutzers verschlossen und es wird wieder automatisch der Ruhebildschirm angezeigt. Erst beim Wegfall der externen Spannungsversorgung (z. B. Stecker ziehen oder Herunterfahren des PCs) schaltet das Gerät aus. Wenn Sie das Gerät längere Zeit nicht benutzen können Sie es auch manuell ausschalten, indem Sie im Ruhebildschirm ca. 3 Sekunden die STOP-Taste drücken.

ACHTUNG!
Bei der ersten Inbetriebnahme muss als erstes eine aus acht Ziffern bestehende Administrator-PIN (Admin-PIN) vom Administrator vergeben werden.
**Wenn Sie zur Eingabe einer neuen Admin-PIN aufgefordert werden, aber nicht der Administrator sind**, brechen Sie den Vorgang ab und informieren Sie Ihren Administrator, damit dieser zunächst die Konfiguration des Terminals für Sie vornimmt.
**Wenn Sie Administrator sind**, lesen Sie bitte zunächst das Kapitel 3 »Bedienungsanleitung für den Administrator«, bevor Sie fortfahren.

ACHTUNG!
Bei der ersten Inbetriebnahme muss als erstes eine aus acht Ziffern bestehende Administrator-PIN (Admin-PIN) vom Administrator vergeben werden.
**Wenn Sie zur Eingabe einer neuen Admin-PIN aufgefordert werden, aber nicht der Administrator sind**, brechen Sie den Vorgang ab und informieren Sie Ihren Administrator, damit dieser zunächst die Konfiguration des Terminals für Sie vornimmt.
**Wenn Sie Administrator sind**, lesen Sie bitte zunächst das Kapitel 3 »Bedienungsanleitung für den Administrator«, bevor Sie fortfahren.

HINWEIS!
Das Terminal verfügt über eine Selbstüberwachungsfunktion (Timeout-Watchdog) zur Ausfallerkennung. Im unwahrscheinlichen Falle, dass die Software des Terminals nicht mehr ordnungsgemäß arbeitet, startet das Terminal nach 15 Sekunden selbstständig neu. Der Konnektor wird nach dem Neustart die Verbindung zum gepairten Gerät selbstständig wieder aufnehmen.
Sollte das Terminal einmal nicht reagieren, warten Sie bitte mindestens 15 Sekunden, bevor Sie einen Kaltstart des Terminals durch ziehen des Netzsteckers vornehmen.

Wenn ein NTP Server eingerichtet ist, bleibt die Zeiteinstellung auch im ausgeschalteten Zustand erhalten. Im Ruhebildschirm zeigt das Display einen frei wählbaren Text (Werkseinstellung: Willkommen!) und bei funktionierender NTP Server Einstellung die Uhrzeit und das Datum an (siehe dazu den Abschnitt 7.2.1.8 »LAN Parameter: [NTP Client \218]« auf Seite 63).

## 4.3. Aufbau des Grafikdisplays




Abbildung 13: *Aufbau des Grafikdisplays*

Das Gerät verfügt über ein beleuchtetes TFT-Farbdisplay mit 400x240 Pixeln, das für eine gut lesbare Darstellung der Informationen auf dem Display sorgt. Die Hauptfläche ist als Textanzeige mit maximal neun Zeilen ausgelegt. Am unteren Rand befindet sich immer eine Reihe von bis zu zehn Symbolen mit Informationen über Aktivitäten und Zustand des Gerätes. Eine ausführliche Übersicht über alle Symbole und ihre Bedeutung finden Sie im Abschnitt 1.5 »Displaysymbole und ihre Bedeutung« auf Seite 18 dieser Bedienungsanleitung.

## 4.4. Der Ruhebildschirm




Abbildung 14: *Der Ruhebildschirm*

Im Ruhebildschirm wird im Auslieferungszustand im Display Willkommen! angezeigt. Sie können diesen Text individuell durch einen freien Text mit bis zu zwei Zeilen und jeweils 23 Zeichen ändern, um beispielsweise mehrere Geräte desselben Typs besser unterscheiden zu können. Eine genaue Anleitung, wie Sie den Text auf Ihre Bedürfnisse anpassen können, finden Sie im Abschnitt 7.2.6.1 »Individueller Text im Ruhebildschirm [Freier Text \261]« auf Seite 70 dieser Bedienungsanleitung. Unter dem Begrüßungstext werden die aktuelle Uhrzeit und das aktuelle Datum angezeigt, wenn sie über einen NTP Server (siehe Abschnitt 7.2.1.87.2.1.7.1 »LAN Parameter: [NTP Client \218]« auf Seite 63) bezogen wird.
Das Terminal informiert Sie rechtzeitig vor Ablauf der Gültigkeit der Zertifikate der eingesteckten gSMC-KT Karte. Sobald sich das Ablaufdatum eines der Zertifikate auf der gSMC-KT 42 oder weniger Tagen in der Zukunft liegt, wird dies durch eine weiße Laufschrift auf rotem Hintergrund im Ruhebildschirm angezeigt. Folgender Text erscheint im Bildschirm:

**+++ Ablauf der Zertifikatsgültigkeit der gSMC-KT in XX Tagen - Bitte kontaktieren Sie Ihren Administrator +++**

Nach Ablauf der Gültigkeit eines der Zertifikate kann das Terminal keine Verbindung mehr zum Konnektor herstellen, bis die gSMC-KT durch eine neue mit gültigen Zertifikaten ersetzt und das Terminal neu mit dem Konnektor gepairt wurde (siehe Abschnitt 5.9 »Initiales Pairing des Terminals mit dem Konnektor« auf Seite 55 bzw. Abschnitt 58 »Inbetriebnahme als Signatur-Terminal außerhalb der Telematikinfrastruktur« auf Seite 58 dieser Bedienungsanleitung).
In diesem Falle wird eine weiße Laufschrift auf rotem Hintergrund im Ruhebildschirm angezeigt. Folgender Text erscheint im Bildschirm:

**+++ Zertifikatsgültigkeit der gSMC-KT ist abgelaufen - Bitte kontaktieren Sie Ihren Administrator +++**

HINWEIS!
Das Terminal informiert Sie rechtzeitig vor Ablauf der Gültigkeit der Zertifikate der eingesteckten gSMC-KT Karte. Sobald sich das Ablaufdatum eines der Zertifikate auf der gSMC-KT 42 oder weniger Tagen in der Zukunft liegt, wird dies durch eine weiße Laufschrift auf rotem Hintergrund im Ruhebildschirm angezeigt.

Kontaktieren sie den Administrator, um rechtzeitig einen Termin zum Austausch der gSMC-KT Karte durch eine Neue zu vereinbaren.

Nach der Kenntnisnahme kann der Administrator die permanente Warnmeldungsanzeige am Gerät abschalten. Für diese Option steht der ergänzte Menüpunkt **[Display\264] gSMC-KT Warnmeldung** zur Verfügung.

Sofern diese Option genutzt wird, kann der Status der gSMC-KT Karte weiterhin über die Menüfunktion **[Test\34]** manuell abgerufen werden.

## 4.5. Menü-Navigation




Abbildung 15: *Das Menü* [**Einstellungen \2**]

Durch Betätigen der MENU-Taste [MENU] gelangen Sie in das Menü des Kartenterminals. Das Menü ist in mehrere Ebenen aufgeteilt. Die Auswahl einer Ebene erfolgt entweder mit den Cursortasten ◀ ▶ und ▲ ▼, in die der Cursor bewegt werden soll und Bestätigung mit der OK-Taste. Das Symbol ✥ in der Symbolleiste signalisiert, dass Sie mit den Cursortasten durch das Menü navigieren können.

Alternativ können Sie die Untermenüs auch direkt durch Drücken auf die entsprechende Zifferntaste erreichen.

Um beispielsweise direkt in das Untermenü zu gelangen, in dem Sie die die Terminalselbstauskunft einsehen können, können Sie die Tastenkombination MENU 3 2 drücken und gelangen so ohne Umwege ins gewünschte Menü. Am oberen rechten Rand des Bildschirms wird in gelber Schrift immer die Kurztastenkombination des jeweiligen Menüs angezeigt. In diesem Beispiel (siehe Abbildung 15) [**Einstellungen \2**].

> **HINWEIS**
> In dieser Bedienungsanweisung werden die Menüs immer mit ihren jeweiligen Kurztastenkombination dargestellt (Beispiel [**Einstellungen \2**]. Sie können so direkt mit der entsprechenden Tastenkombination ins gewünschte Menü gelangen. Dies soll Ihnen die Navigation vereinfachen und dient zur Beschleunigung der Bedienung des Gerätes in der täglichen Praxis.
> Die Menüstruktur mit den dazugehörenden Kurztastensequenzen finden Sie im Anhang dieser Bedienungsanleitung auf den Seiten 102 bis 106.

Um im Menü eine Menüebene zurückzugehen, drücken Sie die STOP- oder ◀-Taste. Um das Menü aus einer beliebigen Position heraus zu verlassen und wieder direkt zum Ruhebildschirm zu gelangen, drücken Sie die MENU-Taste. Wurden zuvor Einstellungen geändert, aber nicht bestätigt, folgt die Sicherheitsabfrage **Änderungen übernehmen?** Bestätigen Sie diese Abfrage mit OK oder verwerfen Sie die Änderungen mit der STOP-Taste. Die Übernahme einer Einstellung oder Eingabe wird mit **Aktion erledigt** und einem Signalton quittiert. Mit der CLEAR-Taste können Sie fehlerhafte Eingaben korrigieren, indem Sie mit jedem CLEAR-Tastendruck die jeweils letzte Eingabe löschen.

## 4.6. Das Hauptmenü




Abbildung 16: *Das Hauptmenü*

Aus dem Ruhebildschirm gelangen Sie mit einem Druck auf die MENU-Taste ins Hauptmenü. Von hier geht es in die weiteren Untermenüs.

Das Symbol ✥ in der Symbolleiste signalisiert, dass Sie durch Betätigen der Cursortasten den grünen Pfeil hinter den Menüpunkten durch das Auswahlmenü bewegen können. Wählen Sie einen weiterführenden Menüpunkt aus und bestätigen mit OK oder mit ▶.

## 4.7. Einstecken einer eGK in die Kontaktiereinheit 1




Von der Vorderseite des Gerätes betrachtet wird die Patientenkarte (eGK) von oben mit der Vorderseite (Bild und Chipkartenfeld) nach vorne in den Kartenschlitz der Kontaktiereinheit 1 geschoben (❶). Drücken Sie die Karte mit sanftem Druck nach unten, bis das Kartenterminal die Verbindung mit der Chipkarte herstellt.

Abbildung 17: *Einstecken einer eGK*

## 4.8. Einstecken eines HBA in die Kontaktiereinheit 2




Abbildung 18: *Einstecken eines HBA*



Abbildung 19: *Der HBA in der Kontaktiereinheit 2*

Wenn Sie Ihren Heilberufsausweis (HBA) in diesem Terminal verwenden wollen, können Sie ihn auf der rechten Gehäuseseite einstecken (❶). Dabei muss sich das Kontaktfeld der Smartcard auf dem HBA auf der Oberseite links befinden. Schieben Sie die Karte mit sanftem Druck nach links, bis sie vollständig von der Kontaktiereinheit aufgenommen und der Kontakt mit der Karte hergestellt wird (❷).

## 4.9. Patientendatensatz einlesen

Wenn Sie eine eGK in den Kartenschlitz stecken, werden die Daten in der Regel automatisch zur Software Ihres Primärsystems übertragen. Ggf. müssen Sie den Auslesevorgang aus der Software Ihres Primärsystems starten, bevor Sie die Karte stecken können und die Kommunikation mit der Smartcard auf der eGK startet. Für den genauen Ablauf des Authentifizierungsprozesses und den Ablauf der Datenübertragung lesen Sie bitte auch die Dokumentationen des Konnektors und der Primärsystemsoftware.

# Kapitel 3: Bedienungsanleitung für den Administrator

Das Kapitel 3 »Bedienungsanleitung für den Administrator« beschreibt detailliert alle Einstellungsoptionen der einzelnen Menüs und Untermenüs. In bestimmten Menüs, wie z.B. [**Einstellungen \2**] und [**Werkseinstellung \33**] ist die Eingabe der Admin PIN erforderlich. Die Eingabe der Administrator PIN öffnet alle Menüebenen, so dass Sie die PIN zur Konfiguration nur einmal eingeben müssen. Der Zugang wird erst wieder verschlossen, wenn Sie das Menü verlassen oder für 30 Sekunden keine Taste gedrückt wird. Das Gerät kehrt dann automatisch in den Ruhebildschirm zurück.
Geänderte Einstellungen werden nur übernommen, wenn sie durch Drücken der OK-Taste bestätigt werden.
In den folgenden Beschreibungen der Einstellmöglichkeiten wird die Admin PIN Eingabe nicht jedes Mal ausführlich beschrieben, da davon ausgegangen wird, dass Sie den Eingabevorgang bereits kennengelernt haben. In den weiteren Einstellungen wird dieser Eingabeprozess mit [**Admin PIN Eingabe**] abgekürzt. Ausgangspunkt der Beschreibung ist immer die Anzeige des Hauptmenüs, die Auswahl wird als Kurztastenauswahl angegeben. Alternativ können Sie natürlich die Auswahl auch mit den Cursortasten vornehmen und mit der OK-Taste bestätigen.

# 5. Inbetriebnahme als eHealth-Terminal in der Telematikinfrastruktur

Vergewissern Sie sich beim Auspacken des Gerätes, dass die Verpackung nicht beschädigt und der Packungsinhalt vollständig ist. Prüfen Sie zunächst den Inhalt der Packung auf Vollständigkeit und das stationäre Kartenterminal auf Unversehrtheit.

## 5.1. Das erste Einschalten des Gerätes




Abbildung 20: *Zugriffsrechte festlegen*

Nach dem Einschalten bzw. dem Anlegen der Spannung ist das Gerät betriebsbereit. Vergeben Sie bei der ersten Inbetriebnahme Ihre Administrator-PIN (Admin-PIN). Direkt danach können Sie entscheiden, ob Sie **SICCT Admin-Session** aktivieren wollen. Drücken Sie auf OK, wenn Sie spätere Updates des Terminals direkt über den Konnektor durchführen wollen. Drücken Sie die STOP-Taste, wenn Sie das nicht beabsichtigen. Sie könne diese Einstellung jederzeit im Menü [Admin Session \2271] verändern (siehe Abschnitt 7.2.2.8.1»Zugriffsrechte: [Admin Session \2271]« auf Seite 68). Nach erfolgter Auswahl wechselt die Anzeige in den Ruhebildschirm und Sie können mit der Konfiguration des Terminals und dem Pairing mit dem Konnektor beginnen.

## 5.2. Admin-PIN Eingabe bei der ersten Inbetriebnahme

Bei der ersten Inbetriebnahme muss als erstes eine aus acht Ziffern bestehende Administrator-PIN (Admin-PIN) vergeben werden. Die Admin-PIN ist die gesicherte Zugangsberechtigung zu den Einstellungen Ihres Gerätes und zu den gespeicherten Daten.
Die sichere Admin-PIN Eingabe wird durch acht Schlosssymbole [🔒🔒🔒🔒🔒🔒🔒🔒] im Display dargestellt.



ACHTUNG!
Vermeiden Sie bei Ihrer Wahl konstante oder auf-/absteigende Ziffernfolgen (00000000, 12345678 etc.), Datumswerte (Geburtstage, Jahrestage) oder Personalnummern, die leicht zu erraten sind.



ACHTUNG!
Notieren Sie die Admin-PIN und bewahren Sie sie unter Verschluss auf. Geben Sie Ihre PIN niemals bekannt. Achten Sie darauf, dass Sie bei der Eingabe einer PIN nicht beobachtet werden. Stellen Sie sicher, dass das Gerät jederzeit vor unbefugtem Zugriff geschützt ist!



ACHTUNG!
Werden Sie bei der ersten Inbetriebnahme nicht zur Eingabe aufgefordert, nehmen Sie das Gerät nicht in Betrieb und kontaktieren Sie Ihren Gerätelieferanten!

## 5.3. Admin-PIN Zeitsperre

Nach drei fehlerhaften Eingaben wird die Admin-PIN Eingabe für eine Minute gesperrt! Weitere Fehleingaben verlängern die Sperrzeit bis zu 24 Stunden. Sollten Sie Ihre Admin-PIN vergessen haben, können Sie eine neue Admin-PIN bei Ingenico Healthcare anfordern. Hierfür ist ein sicheres Vergabeverfahren notwendig. Bitte setzen Sie sich hierfür mit der Service-Hotline von Ingenico Healthcare in Verbindung.

## 5.4. Neue PIN anfordern

Sollten Sie Ihre Admin-PIN vergessen haben, können Sie eine neue PIN bei Ingenico Healthcare anfordern. Hierfür ist ein sicheres Vergabeverfahren notwendig. Bitte setzen Sie sich hierfür mit der Service-Hotline von Ingenico Healthcare in Verbindung.

## 5.5. Werksvoreinstellungen

Das ORGA 6141 online ist in der Werkseinstellung für den Einsatz im gematik Online-Produktivbetrieb für den direkten Anschluss an den Konnektor vorkonfiguriert. Die wichtigsten Werksvoreinstellungen für die Kommunikation mit dem Konnektor lauten wie folgt:

| Funktion | Menüpunkt | Einstell-möglichkeiten | Werksein-stellung |
|---|---|---|---|
| SICCT Announcement | [**Announcement \224**] | 0 sec. (Aus) bis 3000 sec. | 5 sec. |
| LAN Parameter DHCP | [**DHCP \2121**] | Ein<br>Aus | Ein |
| LAN Parameter TCP Port Nummer | [**TCP Port \2161**] | 0-65535 | 4742 |
| LAN Parameter UDP Port Nummer | [**UDP Port \2162**] | 0-65535 | 4742 |
| LAN Parameter NTP Client | [**NTP Client \2181**] | Ein<br>Aus | Ein |
| SICCT Protokoll SSL accept Timeout | [**SSL accept Timeout \2224**] | 1 sec. bis 30 sec. | 20 sec |
| SICCT Keep Alive Intervall | [**KA Intervall \2211**] | 1 sec. bis 10 sec. | 10 sec |
| SICCT Keep Alive Timeout | [**KA Timeout \2212**] | 120 sec. bis 300 sec. | 120 sec |
| SICCT TLS Einstellungen TLS Version | [**TLS Version \2231**] | V1.2<br>V1.3 | V1.2 |
| TSL Liste | [**TSL Liste \224**] | TSL-PU<br>TSL-RU<br>TSL-TU<br>TSL-LU<br>TSL-SU | TSL-PU |
| SICCT Zugriffsrechte Admin Session | [**Admin Session \2271**] | Ein<br>Aus | Aus |
| SICCT Zugriffsrechte* Set Status Kommandos | [**Set Status \2272**] | Ein<br>Aus | Ein |
| SICCT Zugriffsrechte* Download Kommandos | [**Download \2273**] | Ein<br>Aus | Ein |

* Nur aktiv, wenn **[Admin Session \2271]** eingeschaltet ist.

Tabelle 2: *Werksvoreinstellungen*

Um das Gerät wieder in Werkseinstellung zurück zu versetzen, drücken Sie im Ruhebildschirm auf die MENU-Taste, wählen mit den Cursor-Tasten ▲ oder ▼ den Menüpunkt 3 [**Service \3**] aus, drücken die OK-Taste, wählen erneut mit den Cursor-Tasten ▲ oder ▼ den Menüpunkt 3 [**Werkseinstellungen \33**] aus.
Anschließend wählen Sie den Menüpunkt 1 [**via Admin-PIN \331**] aus und geben nach Drücken auf OK Ihre Admin-PIN ein. Bestätigen Sie die Sicherheitsabfrage **PIN bestätigen: OK/STOP** mit der OK-Taste und nach erneutem Warnhinweis **Sind Sie sich sicher? [OK/STOP]** noch einmal mit OK. Anschließend wird das Terminal in den Auslieferungszustand zurück versetzt. Dabei gehen alle im Gerät gespeicherten Einstellungen unwiderruflich verloren.

ACHTUNG!
Beim Zurücksetzen des Gerätes in den Auslieferungszustand (Werkseinstellung) gehen alle im Gerät gespeicherten Einstellungen unwiderruflich verloren.

## 5.6. Authentizitäts- und Integritätsprüfung der gSMC-KT

ACHTUNG!

- Zur Integration des Terminals in die Online-Telematikinfrastruktur muss sich eine durch die gematik zugelassene gSMC-KT Karte mit gültigen Zertifikaten im Terminal befinden.

- Die gSMC-KT ist nicht im Lieferumfang des ORGA 6141 online enthalten!
- Auch wenn das Kartenterminal keine strikte Prüfung auf eine Ingenico gSMC-KT durchführt, wird der Einsatz einer Ingenico gSMC-KT empfohlen und im weiteren Textverlauf beschrieben.
- Prüfen Sie vor der Montage einer gSMC-KT Karte in einem Kartenterminal immer erst die Integrität und Authentizität der Karte.
- Führen Sie die Montage nur durch, wenn Sie sich ganz sicher sind, dass die gSMC-KT aus einer vertrauenswürdigen Quelle stammt.
- Wenden Sie sich bei Fragen oder Zweifeln bezüglich der Integrität der gSMC-KT an den Kartenherausgeber Ingenico Healthcare!
- Bei den in Abbildung 21 und Abbildung 22 dargestellten Vorder- und Rückseiten handelt es sich um die bei Redaktionsschluss dieser Bedienungsanleitung verwendeten gSMC-KT Karten. Es ist möglich, dass die Bedruckung von zukünftigen gSMC-KT Karten und des dazugehörigen Anschreibens (siehe »2. Musteranschreiben einer gSMC-KT« auf Seite 101 des Anhangs) von diesen durch technische Änderungen oder gesetzlichen Vorgaben abweichen können. Dies alleine stellt keinen Grund dar, die Integrität und Authentizität der Karte in Frage zu stellen. Die aktuellsten Informationen zur Funktion der gSMC-KT und der Gestaltung des Anschreibens und des Kartenkörpers erhalten Sie auf unserer Homepage unter: www.ingenico.de/healthcare/sichere-lieferkette

HINWEIS
Sollten Sie eine gSMC-KT verwenden, die nicht von Ingenico Healthcare stammt, wenden Sie sich bezüglich der Kompatibilität sowie der Integritäts- und Authentizitätsprüfung an den Kartenherausgeber Ihrer gSMC-KT.




Abbildung 21: *Vorderseite der gSMC-KT von Ingenico Healthcare*




Abbildung 22: *Rückseite der gSMC-KT von Ingenico Healthcare*

In der Online-Telematikinfrastruktur werden eine Vielzahl von verschiedenen Security Module Cards (SMC) eingesetzt, um die Berechtigungen von Personen, Institutionen und Hardware-Komponenten mit dem absoluten Höchstmaß an Sicherheit zu gewährleisten. Die SMC-K (im Konnektor) und gSMC-KT (im Kartenterminal) gewährleisten die Prüfung der Berechtigungen des Zugriffs auf Patientendaten von Personen und Institutionen.
Die gSMC-KT enthält die Zertifikate und Schlüssel zum Aufbau der verschlüsselten Verbindung zum Konnektor (TLS-Verbindung) sowie zur Funktion als sogenannter Remote PIN Sender zur Durchführung eines Remote PIN-Szenarios, bei dem eine vom Konnektor aufgebaute gesicherte Verbindung zu einem Heilberufsausweis (HBA) in einem entfernten Kartenterminal genutzt wird.
Die Schlüsselzertifikate einer gSMC-KT haben eine bestimmte Gültigkeitsdauer. Das Ablaufdatum der Gültigkeit ist auf dem Anschreiben zur gSMC-KT angegeben und kann durch einen Einzeltest des Kartenslots 1 im Menü [**Einzeltest \342**] auch ohne vorheriges Pairing des Terminals mit einem Konnektor schnell und bequem ausgelesen werden. Lesen Sie im Kapitel 7.3.4 »Terminal-Funktionstests [Test \34]« auf Seite 86 wie Sie hierfür vorzugehen haben.
Nach Ablauf der Zertifikate ist keine Datenkommunikation zwischen Terminal und Konnektor möglich und die gSMC-KT muss gewechselt werden.
Das ORGA 6141 online verfügt über zwei Slots im 2FF-Format (Mini-SIM), in die die gSMC-KT und ggf. zusätzlich eine Betriebsstättenkarte (SMC-B) bei der Erstkonfiguration einfach und bequem eingesteckt oder gewechselt werden können. Die Slots werden zum Schutz vor Missbrauch versiegelt.
Um die Authentizität (Echtheit) und Integrität (Unversehrtheit) der verwendeten gSMC-KT zu überprüfen, können Sie das, der gSMC-KT beiliegende, Anschreiben mit dem Musteranschreiben im Anhang und die Vorder- und Rückseite der gSMC-KT mit der Vorderseite der Musterkarte in Abbildung 21 und der Rückseite in Abbildung 22 vergleichen. Es ist möglich, dass die Bedruckung von zukünftigen gSMC-KT Karten und des dazugehörigen Anschreibens (siehe »2. Musteranschreiben einer gSMC-KT« auf Seite 101 des Anhangs) von diesen durch technische Änderungen oder gesetzlichen Vorgaben abweichen können. Dies alleine stellt keinen Grund dar, die Integrität und Authentizität der Karte in Frage zu stellen. Die aktuellsten Informationen zur Funktion der gSMC-KT und der Gestaltung des Anschreibens und des Kartenkörpers erhalten Sie auf unserer Homepage unter: www.ingenico.de/healthcare/sichere-lieferkette
Die vollständige Kartenkennnummer (ICCSN) ist auf der gSMC-KT Karte neben dem Kontaktierfeld und auf dem zugehörigen Anschreiben abzulesen und muss identisch sein.
Zusätzlich haben Sie zur Prüfung der Authentizität und Integrität der gSMC-KT die Möglichkeit die Vertrauenswürdigkeit der Lieferkette der Karte vom Kartenherausgeber Ingenico Healthcare bis zu Ihnen nachzuverfolgen, wenn Sie die Karte nicht direkt bei Ingenico Healthcare bestellt haben. Die Ingenico Healthcare GmbH hat hierfür auf ihrer Internetseite www.ingenico.de/healthcare/sichere-lieferkette alle Handelspartner, an die das ORGA 6141 online und die gSMC-KT geliefert werden veröffentlicht. Darüber hinaus können Sie auch über die Hotline von Ingenico Healthcare in Erfahrung bringen, wann die gSMC-KT an welche Lieferanschrift versendet wurde.

## 5.7. Einsetzen einer SMC-Karte und Versiegeln der Kontaktiereinheiten 3 und 4

Die Abbildung 23 zeigt die beiden Kontaktiereinheiten 3 (unterer Kartenschlitz) und 4 (oberer Kartenschlitz), die für die Aufnahme einer Signaturkarte im im 2FF-Format (Mini-SIM) und weiterer applikationsspezifischer Smartcards vorgesehen sind. In der Online-Telematik-infrastruktur sind dies die SMC-B und gSMC-KT. Die Karten können in den Kontaktiereinheiten 3 und 4 auf der linken Seite des Gerätes verwendet werden. Sie werden mit zur Rückwand weisender Kontaktfläche, mit der abgeschrägten Ecke zuerst eingeführt, bis sie einrasten (❶).




Abbildung 23: *Einsetzen der SMC-Karten in die Kontaktiereinheit 3 und 4*

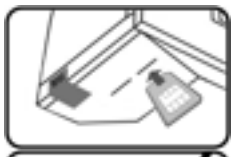



Abbildung 24: *Die richtige Positionierung des Slotsiegels*




Abbildung 25: *Beispiel der Angabe des gSMC-KT Fingerprints im Konfigurationsmenü eines Konnektors*

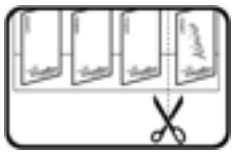
Erneutes Drücken entriegelt die Karten und sie können wieder entnommen werden.
Beim Pairing Prozess muss der Administrator den Fingerprint (Hash-Wert des Authentisierungs-zertifikates der gSMC-KT) im Administrations-Frontend des Konnektors überprüfen. Dieser Fingerprint ist direkt auf dem Kartenträger (siehe Abbildung 21) aufgedruckt. Die Abbildung 25 zeigt beispielhaft die Angabe des gSMC-KT Fingerprints im Konfigurationsmenü eines Konnektors. Weiter Details zum Fingerprint der gSMC-KT Karte entnehmen Sie bitte dem Handbuch des Konnektors.



Setzen Sie die SMC-Karten wie oben beschrieben in die Kontaktiereinheiten 3 und 4 ein. In welche Kontaktiereinheit Sie die gSMC-KT oder SMC-B Karte einsetzen, spielt keine Rolle.



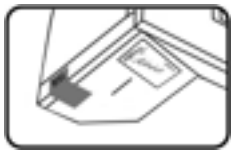
Entnehmen Sie das Trägerblatt mit den Slotsiegeln aus dem Tütchen, das sich mit der Kurzanleitung in der beiliegenden Dokumententasche befindet. Unterschreiben Sie für jede SMC-Karte, die Sie einsetzen müssen, ein Slotsiegel.



Schneiden Sie mit einer Schere das Trägerblatt so durch, dass die unterschriebenen Slotsiegel sich einzeln auf dem Trägerblatt befinden. Im Trägerblatt befindet sich eine Schlitzung, die es Ihnen ermöglicht zunächst nur eine Hälfte des Slotsiegels vom Trägerblatt zu trennen.



Die verbleibende Hälfte des Trägerblattes dient als Anfasslasche. Geben Sie darauf Acht, dass die selbstklebende Siegelunterseite nicht direkt mit Ihren Fingern oder anderen Gegenständen in Berührung kommt, da sie sehr empfindlich ist und das Slotsiegel so sehr leicht beschädigt werden kann.



Platzieren Sie das Siegel auf dem Schlitz der Kontaktiereinheit, in die Sie zuvor die SMC-Karte eingesetzt haben. Achten Sie dabei darauf, dass das Siegel den Schlitz vollständig bedeckt und die vollständige Siegelfläche auf dem Terminal haftet (siehe Abbildung 24). Legen Sie die unbenutzten Slotsiegel zurück in die Klarsichthülle und bewahren Sie sie an einem sicheren Ort zusammen mit dem Kartenträger der eingesetzten SMC-Karte auf, damit keine unsignierten Siegel in falsche Hände geraten können und Sie bei einer Neukonfiguration des Terminals oder beim Wechsel einer SMC-Karte alle Informationen zu den verbauten Karten griffbereit haben.

Abbildung 26: *Unterschreiben und richtiges Anbringen der Slotsiegel*

HINWEIS!
Eine gSMC-KT Karte enthält die Schlüssel, um auf eine Gesundheitskarte zuzugreifen, sowie Mechanismen um eine gesicherte Verbindung zwischen einem Heilberufsausweis (HBA) und einer SMC herzustellen. Die SMC macht aus dem Kartenterminal ein unverwechselbares und der Betriebsstätte, in dem es zum Einsatz kommt, eindeutig zuzuordnendes Terminal.

HINWEIS! Anforderungen an den Siegeluntergrund:
Der Untergrund muss sauber, trocken und fettfrei sein. Es dürfen keine Restsilikone oder Trennmittel auf dem Untergrund vorhanden sein, welche die Adhäsion des Sicherheitssiegels beeinträchtigen können.
Die optimale Vernetzung zwischen dem Siegel und dem Untergrund ist nach 24 Stunden gewährleistet.

ACHTUNG!
Zum Wechseln der SMC-Karte entfernen Sie das Siegel und alle Rückstände des Siegels vollständig, bevor Sie die alte durch eine neue SMC-Karte ersetzen und ein neues Siegel aufkleben.

## 5.8. Verbindung des Gerätes über eine LAN-Verbindung mit dem Konnektor

Das ORGA 6141 online wird über ein LAN-Kabel direkt mit dem Konnektor verbunden. Hierzu verwenden Sie bitte ausschließlich das beiliegende LAN-Netzwerkkabel. Zur Stromversorgung verwenden Sie bitte das beiliegende Steckernetzteil.





USB-B Buchse zum Anschluss eines USB-Kabels als alternative Spannungsversorgung über einen freien USB-Anschluss Ihres Primärsystems.



USB-A Buchse zum Einstecken eines USB-Sticks für ein Firmware-Update



Hohlsteckerbuchse zur Stromversorgung über das Steckernetzteil.



RJ-45 Buchse zum Anschluss eines LAN-Netzwerkkabels zum verbinden des Terminals mit dem Konnektor.

Abbildung 27: *Anschlüsse auf der Unterseite des Gerätes*



ACHTUNG!
Aus Gründen der Datensicherheit und zum Schutz vor Manipulation darf das Kartenterminal nur in einer gesicherten Einsatzumgebung, in der es nie unbeaufsichtigt ist, konfiguriert und mit dem Konnektor verbunden werden!



ACHTUNG!
Prüfen Sie vor jedem Pairing des Terminals mit dem Konnektor die Integrität des Gerätes, so wie in Abschnitt 2.2 »Sicherheitsmerkmale« auf Seite 23 beschrieben.



ACHTUNG!
Wenn Sie ein Kartenterminal aus dem Netzwerk dauerhaft oder temporär im Servicefall entfernen, müssen die Konfigurationsdaten umgehend gelöscht werden. Dies geschieht am schnellsten und komfortabelsten durch den auf Seite 85 in Abschnitt 7.3.3 »[Werkseinstellung \33]« beschriebenen Werksreset.




Abbildung 28: *Anschluss mit LAN-Kabel am Konnektor*

Das ORGA 6141 online kann nur per LAN-Kabel direkt am Konnektor angeschlossen werden. Ein direkter Anschluss per USB- oder LAN-Verbindung am Primärsystem ist in der Online-Telematikinfrastruktur nicht mehr gestattet und wird deswegen auch nicht mehr unterstützt. Lesen Sie zur genauen Vorgehensweise bei der Bekanntmachung des Terminals am Konnektor, dem sogenannten Pairing den Abschnitt 7.2.2 »Die Konfiguration der SICCT Parameter [SICCT Parameter \22]« auf Seite 64. Schließen Sie das Gerät mit einem LAN-Kabel an den Konnektor und mit dem Steckernetzteil an eine Steckdose an, so wie es in Abbildung 28 dargestellt ist.

## 5.9. Initiales Pairing des Terminals mit dem Konnektor



ACHTUNG!
Lesen Sie unbedingt den gesamten Abschnitt 5 »Einführung« aufmerksam bis zum Ende durch, bevor Sie mit dem Pairing des Terminals und des Konnektors beginnen, um Probleme während der Konfiguration zu vermeiden.



ACHTUNG!
Sie müssen zunächst die gSMC-KT vorschriftsmäßig ins Gerät einsetzen, bevor Sie mit dem initialen Pairing beginnen können.



ACHTUNG!
Verwenden Sie nur Originalzubehör und -kabel von Ingenico Healthcare beim Anschluss des Terminals an den Konnektor.



ACHTUNG!
Beim Anschluss des Terminals an den Konnektor (initiales Pairing) muss sich das Terminal in der organisatorischen Hoheit des Administrators befinden. Der Administrator muss gewährleisten, dass er den Pairingvorgang am Kartenterminal komplett zu Ende führt und das Prozessergebnis, dass der Konnektor eine gesicherte TLS-verbindung zum gepairten Kartenterminal aufbauen kann, kontrolliert.
Entsprechende Anweisungen zur Kontrolle entnimmt der Administrator der Produktdokumentation des eingesetzten Konnektors.



ACHTUNG!
Im Fall eines Fehlerzustands oder bei Außerbetriebnahme müssen alle im Terminal gespeicherten Pairing-Informationen vom Administrator gelöscht werden. Dieses kann vereinfacht im Zuge eines Werksresets oder Löschen aller oder eines Pairingblocks geschehen.
Zusätzlich muss der Administrator die entsprechenden Pairing-Informationen am Konnektor löschen. Entsprechende Anweisungen zur Kontrolle entnimmt der Administrator der Produktdokumentation des eingesetzten Konnektors.



ACHTUNG!
Im Fall, dass der Pairingvorgang fehlschlug, muss der Administrator die Pairinginformation am Konnektor löschen. Entsprechende Anweisungen zur Kontrolle entnimmt der Administrator der Produktdokumentation (Karten-terminalverwaltung) des eingesetzten Konnektors.

HINWEIS
Prüfen Sie als Administrator vor dem initialen Pairingvorgang, dass mindestens ein freier d.h. unbelegter Pairingblock verfügbar ist. Lesen Sie hierzu auch den Abschnitt 7.2.2.6 »SICCT Parameter: [Pairings \225]« auf Seite 67.

Bei der Installation des ORGA 6141 online in der neuen eHealth KT Betriebsart wird das Terminal direkt mit dem beiliegenden LAN-Kabel mit dem Konnektor verbunden und Sie brauchen keine Treibersoftware auf dem Primärsystem zu installieren. Der Konnektor stellt die Verbindung mit Ihrem Primärsystem und der Online-Telematikinfrastruktur her. Konfigurieren Sie das eHealth Kartenterminal und den Konnektor entsprechend der Vorgaben des Konnektors und der Netzwerkstruktur, in die das ORGA 6141 online integriert werden soll.

HINWEIS!
Ein direkter Anschluss per USB- oder LAN-Verbindung am Primärsystem ist in der Online-Telematikinfrastruktur nicht mehr gestattet und wird deswegen auch nicht mehr unterstützt.

Zur Kopplung des Kartenterminals und des Konnektors müssen beide zunächst bekannt gemacht werden. Dies geschieht beim sogenannten initialen Pairing, das vom Administrator am Konnektor initialisiert werden muss. Details hierzu finden Sie in der Bedienungsanleitung des Konnektors.
Im Zuge des initialen Pairings generiert und sendet der Konnektor eine eindeutige eHealth-Kartenterminal-Kennung (auch als Shared Secret [ShS.KT.AUT] bezeichnet) an das Kartenterminal, welches diese zusammen mit der Konnektorkennung (dem öffentlichen Schlüssel des Konnektorzertifikats) innerhalb eines freien Pairingblocks abspeichert. Der Pairingvorgang bedingt einen gesicherten Verbindungsaufbau vom Konnektor zum Kartenterminal, für den sich eine betriebsbereite gSMC-KT im Kartenterminal befinden muss.
Im Zuge des Pairings überprüft der Konnektor ebenfalls die Identität der gSMC-KT anhand des Fingerprints des gSMC-KT-Zertifikats, welches der Konnektor zusammen mit dem Terminalnamen und/oder der MAC-Adresse in die Kartenterminalverwaltung aufnimmt.
Nach dem Start des Pairings am Konnektor erscheint ein Hinweis am Kartenterminal. Es werden die MAC-Adresse des Kartenterminals und der Host-Name des Konnektors angezeigt. Mit der OK-Taste bestätigen Sie den Pairingvorgang und schließen den Hinweis.

HINWEIS
Die herstellerspezifische Zeitspanne für den Pairingvorgang beträgt fünf Minuten. In dieser Zeit muss der Pairingvorgang durch Drücken der OK-Taste abgeschlossen sein.

Schlägt die Durchführung fehl

- aufgrund eines Timeouts, oder
- brach der Administrator den Bestätigungsvorgang ab, oder
- verfügte das Kartenterminal über keinen freien Pairing-Block,

beendet das Kartenterminal den Pairing-Vorgang und zeigt die Fehlermeldung **Abbruch** auf dem Display an. In diesem Fall hat kein Pairing mit dem Konnektor stattgefunden und muss wiederholt werden. Zur weiteren Ursachendiagnose ist dann vom Administrator das Konnektorprotokoll (Log) der Kartenterminalverwaltung im Konnektor einzusehen.
Sie können die dem Kartenterminal vom Konnektor zugewiesenen Parameter jederzeit im Menü [**Pairings \225**] aufrufen und einsehen. Die eHealth-Kartenterminal-Kennung (bzw. das Shared

Secret kann hierbei nicht am Kartenterminal eingesehen werden. Lesen Sie hierzu auch den Abschnitt 7.2.2.6 »SICCT Parameter: [Pairings \225]« auf Seite 67.

## 5.10. Verbindung des Terminals mit dem Konnektor über ein Virtual Privat Network (VPN)

Das ORGA 6141 online mit der neusten Firmwareversion 3.8.1 bietet die Möglichkeit eine VPN Verbindung zwischen dem Terminal und einem VPN-Gateway aufzubauen. Damit kann z. B. eine sichere Verbindung über das Internet zwischen einem Konnektor in einem Rechenzentrum und dem Terminal in der LEI-Umgebung realisiert werden.
Zur Einrichtung der VPN-Verbindung sind folgende Voraussetzungen notwendig:

- Der Konnektor ist über einen VPN-Dienst erreichbar.
- Die IP bzw. URL des VPN-Dienstes sowie die Zugangsdaten zur Verbindung mit dem VPN-Dienst sind bekannt.
- Das X.509 CA-Zertifikate für den VPN-Zugang ist bekannt.

Mit Hilfe eines einfachen Text-Editors müssen diese Informationen in eine Textdatei geschrieben werden, um sie anschließend mit einem USB-Stick in das Terminal zu importieren.

### 5.10.1. Syntax der VPN Import-Datei

Erstellen Sie mit einem einfachen Text-Editor (z. B. Notpad) eine Textdatei mit folgendem Inhalt:

```
vpn_account_user=<BENUTZERNAME>
vpn_gateway_addr=<URL oder IP des VPN-Dienstes>
ipsec_cacert=<X.509 CA-Zertifikate für den VPN-Zugang>
```

Optional können noch weiter Parameter ergänz werden, wie z. B.:

```
ipsec_conf=<optionale Konfigurationdatei für VPN>
```



HINWEIS
Zur genauen Vorgehensweise und Syntax beim Erstellen einer Import-Datei und Bearbeitung einer Export-Datei lesen Sie bitte den Abschnitt 7.3.6 »Konfiguration via USB-Stick im- und exportieren« auf Seite 89.

Speichern Sie diese Datei mit einem Dateinamen der auf **_import.cfg** endet in das Stammverzeichnis eines USB-Sticks mit FAT32-Formatierung.
Führen Sie anschließend den Import der Daten wie im Abschnitt 7.3.6 »Konfiguration via USB-Stick im- und exportieren« auf Seite 89 beschrieben durch.
Nach erfolgreichem Import der Dateien muss noch im Menü [**Zugangsdaten \2174**] das zugehörige Passwort für den VPN Benutzernamen der Datei direkt am Terminal eingeben werden. Anschließend wird die VPN-Verbindung zum VPN-Dienst aufgebaut und in der Status-Leiste im Display erscheint das Symbol für die VPN-Verbindung an Position 6 (siehe Abschnitt 1.5.2 »Symbol 6: Datenverkehr zu angeschlossenen Geräten« auf Seite 19.

# 6. Inbetriebnahme als Signatur-Terminal außerhalb der Telematikinfrastruktur

Das ORGA 6141 online kann in der Firmwareversion 3.8.1 auch ohne ein Pairing mit einem Konnektor außerhalb der Telematikinfrastruktur des deutschen Gesundheitswesens als Signaturterminal mit LAN Anschluss betrieben werden. Hierzu besteht die Möglichkeit eine sogenannte Trust-Service Status List für die Signaturumgebung (TLS-SU) auszuwählen. Mit der Auswahl der TLS-SU wird das ORGA 6141 online unumkehrbar umkonfiguriert und verliert seine gematik-Zulassung als eHealth Terminal für die Telematikinfrastruktur.
Wenn Sie das ORGA 6141 online als Signaturterminal betreiben wollen, gehen Sie bitte wie folgt vor:

1. Folgen Sie den Anweisungen in den Abschnitten 5 »Inbetriebnahme als eHealth-Terminal in der Telematikinfrastruktur« bis zum Abschnitt 5.8 »Verbindung des Gerätes über eine LAN-Verbindung mit dem Konnektor«, die gleichermaßen für beide Betriebsarten gelten.
2. Öffnen Sie das Hauptmenü durch Drücken der MENU-Taste und wählen Sie Das Menü [**TSL Liste \2232**] durch Drücken der Ziffern ② [**Admin PIN Eingabe**] ② ③ ②.
3. Wählen Sie anschließend die ⑤ [**TSL-SU \22325**] für die vollständige Umkonfiguration des Terminals zum Signaturterminal außerhalb der Telematikinfrastruktur. Bestätigen Sie Ihre Auswahl mit der OK-Taste.
4. Bestätigen Sie anschließend die Frage **Sind Sie sicher?** mit der OK-Taste und danach den Hinweis **Auswahl ist unumkehrbar!** erneut mit der OK-Taste.
5. Anschließend wird das Terminal umkonfiguriert und führt einen Werksrest durch. Nach dem Neustart werden Sie aufgefordert eine neue Admin-PIN zu vergeben.
   In der Symbolleiste erscheint ein neues Symbol „Brief mit Siegel“ auf Position 8. Daran können Sie erkennen, dass Ihr Terminal von nun an ein Signaturterminal für den Einsatz ohne Konnektor außerhalb der Telematikinfrastruktur ist.



ACHTUNG!
Die Wahl der Trust-Service Status List der Signaturumgebung [**TLS-SU \22325**] ist unumkehrbar. Die Umkonfiguration kann weder durch einen Werksreset noch durch ein Firmware-Update rückgängig gemacht werden.
Mit der Auswahl der TSL-SU verliert das ORGA 6141 online die technische Möglichkeit, als eHealth Terminal für die Telematikinfrastruktur eingebunden zu werden
Es kann dann ausschließlich außerhalb der Telematikinfrastruktur als Signaturterminal nach einem Pairing mit einer Signaturanwendungskomponente (SAK) betrieben werden.

## 6.1. Initiales Pairing des Terminals mit einer Signaturanwendungskomponente (SAK)

Zum alternativen Betrieb des ORGA 6141 online außerhalb der Telematikinfrastruktur ist ein Pairing wie innerhalb der Telematikinfrastruktur mit einer Signaturanwendungskomponente (SAK) durchzuführen die in weiten Teilen der im Abschnitt 5.9 »Initiales Pairing des Terminals mit dem Konnektor« auf Seite 55 entspricht, wobei die SAK dabei die Rolle des Konnektors einnimmt.
Folgende Voraussetzungen der SAK sind zu erfüllen, damit das Pairing mit dem ORGA 6141 online erfolgreich durchgeführt werden kann:

- Die SAK muss immer einem sicheren Ausführungskontext ablaufen, dessen Sicherheitskontext von einem Administrator bzw. Anwender kontrolliert und unterhalten werden muss.
- Die SAK muss zum Aufbau der TLS-Verbindung ein TLS-Zertifikat im X.509-Format mit der Rolle **oid_sak** vorhalten, dessen Ausgabeinstanz (CA, Certificaton Authority) in der Trustes List TSL-SU enthalten sein muss. Dieses hat der SAK-Anbieter in der Regel mit Ingenico Healthcare entsprechend vorbereitet.
- Das ORGA 6141 online muss immer ein Sicherheitsmodul in Form einer gSMC-KT enthalten. Anderenfalls kann das Kartenterminal keine TLS-Verbindung zur SAK aufbauen.
- Die SAK muss technisch geeignet sein, erst nach einem Pairing-Prozess zum Kartenterminal, eine SICCT-Session über eine TLS-gesicherte TCP/IP-Netzwerkverbindung, einen sogenannten Trusted Channel, aufbauen zu können.
- Die SAK muss eine geeignete Terminalverwaltung vorsehen, welche vor und während des Betriebs das Pairing-Geheimnis (Shared Secret) periodisch überprüft, um festzustellen, ob die Gegenstelle noch das erwartete gepairte Kartenterminal ist oder anderenfalls eine Warnung oder Fehlermeldung an den SAK-Anwender ausgeben.

Die exakten Eigenschaften erfahren Sie von Ihrem SAK-Anbieter, der die oben genannten technischen Eigenschaften in seiner Benutzerdokumentation zur SAK beschreibt.
Ingenico Healthcare gibt Ihnen auf Anfrage Auskunft darüber, welche Anbieter von Signaturanwendungskomponenten entsprechende Produkte mit den erforderlichen Eigenschaften anbieten und deren CA-Zertifikat sich bereits in der Trusted List TSL-SU des ORGA 6141 online Terminals befinden.

# 7. Die Menüoptionen (direkte Managementschnittstelle) für den Administrator im Detail

Das Hauptmenü unterteilt sich in die drei Hauptbereiche

1. [**Ausschalten \1**]
2. [**Einstellungen \2**] und
3. [**Service \3**].

Im Menü Einstellungen können Sie das Gerät auf Ihre IT-Umgebung und das Primärsystems anpassen. Das Servicemenü bietet Ihnen die Möglichkeit, die Admin-PIN zu ändern, den Status des Gerätes zu überprüfen, das Gerät wieder in den Auslieferungszustand (Werkseinstellung) zu versetzen, ein Firmware-Update einzuspielen und die Gerätefunktionen zu überprüfen.

## 7.1. Ausschalten des Gerätes [Ausschalten \1]

Wenn Sie das Gerät längere Zeit nicht benutzen können Sie es manuell ausschalten, indem Sie im Ruhebildschirm ca. 3 Sekunden die STOP-Taste drücken oder das Menü [**Ausschalten \1**] anwählen, mit OK oder ▶ bestätigen und durch Drücken der OK-Taste ausschalten. Durch Drücken der OK-Taste schalten Sie das Gerät wieder ein.

## 7.2. Der Menüpunkt Einstellungen [Einstellungen \2]

Im Menü Einstellungen können Sie das Gerät auf Ihre IT-Umgebung und das Primärsystem anpassen.

### 7.2.1. Die Konfiguration im lokalen Netzwerk [LAN Parameter \21]

In diesem Menü haben Sie die Möglichkeit die LAN Parameter des Terminals auf die individuellen Gegebenheiten des Netzwerkes anzupassen.
Wenn Sie alle LAN-Parameter bequem auslesen und auf einem externen Gerät darstellen lassen wollen, drücken Sie die F1-Taste, um einen QR-Code darstellen zu lassen und mit einem Smartphone abzuscannen. Der QR-Code beinhaltet die Inhalte, die im Abschnitt 7.3.7.4 »QR-Code: [LAN-Parameter \374]« auf Seite 95 beschrieben werden.

#### 7.2.1.1. LAN Parameter: [Gerätename \211]

HINWEIS
Um verschiedene Geräte der gleichen Bauart besser im Netzwerk unterscheiden zu können, haben Sie die Möglichkeit, den Namen der Geräte individuell zu verändern (z. B. “ORGA-KT_Tresen“, “ORGA-KT_Raum1“, “ORGA-KT_Raum2“ usw.).
Der Standardname lautet: **ORGA6100-<Seriennummer>**

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ① ①. Anschließend können Sie über die Zifferntasten einen frei wählbaren Text eingeben. Bestätigen Sie anschließend die Eingabe mit der OK-Taste. Mit den Cursortasten ◀ und ▶ können Sie den blinkenden Cursor nach rechts und links bewegen und mit der CLEAR-Taste können Sie den Text links neben dem blinkenden Cursor löschen.

#### 7.2.1.2. LAN Parameter: [DHCP \212]

Um die Einstellungen für IP Adresse, Subnet Mask und Gateway vornehmen zu können, muss DHCP ausgeschaltet sein.

##### 7.2.1.2.1. DHCP: [Ein / Aus \2121]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ① ② ①. Um DHCP auszuschalten, wählen Sie die ⓪ und bestätigen mit der OK-Taste. Um DHCP zu aktivieren, drücken Sie die ① und bestätigen mit der OK-Taste.

##### 7.2.1.2.2. DHCP: [Erw. Optionen \2122]

Die erweiterten Optionen sind nur wirksam, wenn DHCP eingeschaltet ist! Das Gerät bezieht dann zusätzlich seinen Namen, die NTP Server IP Adresse, die Update-Server IP und den Update-Dateinamen vom DHCP Server. Daher sind bei aktivierten erweiterten Optionen diese Menü-punkte nicht editierbar.
Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ① ② ②. Um die erweiterten Optionen einzuschalten, wählen Sie die ① und bestätigen mit der OK-Taste. Um sie wieder zu deaktivieren, drücken Sie die ⓪ und bestätigen mit der OK-Taste.



ACHTUNG!
Für den zertifizierten Betrieb darf der Administrator die erweiterten DHCP Optionen nicht aktivieren. Das Aktivieren der erweiterten DHCP Optionen kann nur vom Administrator vorgenommen werden.
Eine Aktivierung je nach Einsatzumgebung stellt ein potenzielles Sicherheitsrisiko darstellt.

### 7.2.1.3. LAN Parameter: [IP Adresse \213]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ① ③.
Geben Sie Ihre eigene Geräte IP Adresse ein (jeder Block dreistellig mit führenden Nullen!) und bestätigen Sie mit der OK-Taste. Mit den Cursortasten ◀ und ▶ können Sie den blinkenden Cursor nach rechts und links bewegen.
Die Einstellung der IP Adresse ist nur möglich, wenn DHCP ausgeschaltet ist.

### 7.2.1.4. LAN Parameter: [Subnet Mask \214]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ① ④.
Geben Sie Ihre eigene Subnet Mask ein (jeder Block dreistellig mit führenden Nullen!) und bestätigen Sie mit der OK-Taste. Mit den Cursortasten ◀ und ▶ können Sie den blinkenden Cursor nach rechts und links bewegen.
Die Einstellung der IP Adresse ist nur möglich, wenn DHCP ausgeschaltet ist.

### 7.2.1.5. LAN Parameter: [Gateway/DNS \215]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ① ⑤.
Wählen Sie im Untermenü aus, welchen der beiden Parameter ① Gateway oder ② DNS Sie ändern wollen. Geben Sie Ihre eigene Gateway- bzw. DNS-IP Adresse ein (jeder Block dreistellig mit führenden Nullen!) und bestätigen Sie mit der OK-Taste. Mit den Cursortasten ◀ und ▶ können Sie den blinkenden Cursor nach rechts und links bewegen.
Die Einstellung der IP Adresse ist nur möglich, wenn DHCP ausgeschaltet ist.

### 7.2.1.6. LAN Parameter: [TCP/UDP Port \216]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ① ⑥. Wählen Sie im Untermenü aus, welchen der beiden Parameter ① TCP oder ② UDP Sie ändern wollen. Geben Sie die gewünschte Port Nummer (fünfstellig mit führenden Nullen) ein und bestätigen Sie mit der OK-Taste. Stellen Sie jetzt die anderen Parameter der LAN-Schnittstelle ein und führen Sie dann auf jeden Fall den LAN Neustart [**Neustart \219**] durch!

### 7.2.1.7. LAN Parameter: [IPsec VPN Konfiguration \217]

Das ORGA 6141 online mit der neusten Firmwareversion 3.8.1 bietet die Möglichkeit eine VPN Verbindung zwischen dem Terminal und einem VPN-Gateway aufzubauen. Damit kann z. B. eine sichere Verbindung über das Internet zwischen einem Konnektor in einem Rechenzentrum und dem Terminal in der LEI-Umgebung realisiert werden. Zur Vorgehensweise bei der Einrichtung eines VPN-Zugangs lesen Sie zunächst den Abschnitt 5.10 »Verbindung des Terminals mit dem Konnektor über ein Virtual Privat Network (VPN)« auf Seite 57.
Nach erfolgreicher Einrichtung des VPN-Zugangs können die VPN-Zugangsparameter eingesehen und bearbeitet werden.

#### 7.2.1.7.1. VPN-Parameter: [VPN-Tunnel Ein/Aus \2171]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ① ⑦ ①.
Mit dieser Funktion können Sie die VPN-Verbindung ein- oder ausschalten. Bestätigen Sie Ihre Eingabe mit der OK-Taste.

#### 7.2.1.7.2. VPN-Parameter: [VPN-Tunnel Neustart \2172]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ① ⑦ ②.
Mit dieser Funktion können Sie die VPN-Verbindung neu starten, falls die Verbindung unterbrochen wurde. Bestätigen Sie Ihre Eingabe mit der OK-Taste.

#### 7.2.1.7.3. VPN-Parameter: [VPN-Gateway Adresse \2173]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ① ⑦ ③.
Mit dieser Funktion können Sie die VPN-Gateway Adresse anschauen und ändern.
Geben Sie die VPN-Gateway Adresse mit Hilfe der Tastatur ein und bestätigen Sie die Eingabe mit der OK-Taste. Mit den Cursortasten ◀ und ▶ können Sie den blinkenden Cursor nach rechts und links bewegen und mit der CLEAR-Taste können Sie den Text links neben dem blinkenden Cursor löschen. Bestätigen Sie die Eingabe durch Drücken der OK-Taste.

#### 7.2.1.7.4. VPN-Parameter: [Zugangsdaten \2174]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ① ⑦ ④.
Mit dieser Funktion können Sie die VPN-Zugangsdaten anschauen und ändern.
Geben Sie die Benutzerkennung und das dazugehörige Passwort der Benutzerkennung mit Hilfe der Tastatur unter \21742 ein und bestätigen Sie die Eingabe mit der OK-Taste. Mit den Cursortasten ◀ und ▶ können Sie den blinkenden Cursor nach rechts und links bewegen und mit der CLEAR-Taste können Sie den Text links neben dem blinkenden Cursor löschen. Bestätigen Sie die Eingabe durch Drücken der OK-Taste. Eine Informationsmöglichkeit zu einem alternativen Verfahren via Zertitifikatimport bzw. zu den Menüpunkten \21741 und \2743 entnehmen Sie bitte den Release Notes.

#### 7.2.1.7.5. VPN-Parameter: [Status/Information \2175]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ① ⑦ ⑤.
Mit dieser Funktion können Sie die VPN-Statusinformationen anzeigen lassen. Folgende Informationen werden bei einer bestehenden VPN-Verbindung angezeigt:

- User: Benutzerkennung
- Host: Die URL-/IP-Adresse des VPN-Gateways
- IP: Die eigene IP-Adresse im VPN
- Net: Das VPN-Netzwerk
- BrC: Die ermittelte Broadcast-Adresse
- Conn: Die Dauer der Verbindung bzw. ob gerade eine Verbindung aufgebaut wird
- Encryption: Die ausgehandelten Verschlüsselungsmethoden

#### 7.2.1.7.6. VPN-Parameter: [Konfiguration löschen \2176]

Bei Veränderung der Einsatzumgebung des Terminals, bei der eine IPsec VPN Verbindung nicht mehr benötigt wird oder im Falle der Außerbetriebnahme des Terminals sollten Sie die VPN-Parameter im Gerät löschen. Dies geschieht am einfachsten, wenn Sie im Hauptmenü die Ziffern ② [**Admin PIN Eingabe**] ① ⑦ ⑥ drücken, um zum Menüpunkt [**Konfiguration löschen \2176**] zu gelangen. Bestätigen Sie die Bestätigungsabfrage **Sind Sie sicher? [OK/Stop]** mit einem Tastendruck auf die OK-Taste. Anschließend sind alle VPN-Konfigurationsdaten aus dem Terminal gelöscht. Um neue VPN-Parameter in das Terminal zu übertragen gehen Sie wie im Abschnitt 7.3.6 »Konfiguration via USB-Stick im- und exportieren« auf Seite 89 vor.

### 7.2.1.8. LAN Parameter: [NTP Client \218]

Das Gerät kann über einen Network Time Protocol (NTP) Server die genaue Uhrzeit und das aktuelle Datum beziehen.
In der Werkseinstellung ist NTP aktiviert (Menü **[Ein/Aus \2182] = Ein**) und kann vom Administrator über diesen Menüpunkt deaktiviert werden (Menü **[Ein/Aus \2182] = Aus**).
Ist der NTP Client deaktiviert oder schlägt bei einem Neustart des Gerätes der Versuch auf den NTP Server zuzugreifen fehl, wird keine Uhrzeit und kein Datum im Display angezeigt. Es gibt keine Fehlermeldung!
Wurde der NTP Client aktiviert und war der Zeitabruf vom NTP Server erfolgreich, so ist per Werkseinstellung ein Wert [**Timezone \2183**] passend für Deutschland festgelegt und die aktuelle Uhrzeit wird im Display dargestellt.



ACHTUNG!
Nach der Aktivierung bzw. Deaktivierung vom NTP Client im Menü [**Ein/Aus \2182**] ist ein Neustart [**Neustart \219**] erforderlich, damit die Änderung wirksam wird.



ACHTUNG!
Das Aktivieren bzw. Deaktivieren des NTP Client kann nur vom Administrator vorgenommen werden.

#### 7.2.1.8.1. NTP Client: [Ein/Aus \2181]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ① ⑧ ①. Aktivieren Sie den NTP Client mit der Auswahl ① [**Ein**], um die Uhrzeit und das Datum von einem NTP Server abzurufen und auf dem Display des Terminals darzustellen, oder deaktivieren Sie den NTP Client mit der Auswahl ⓪ [**Aus**], um keine Uhrzeit und Datum im Display anzeigen zu lassen. Bestätigen Sie Ihre Wahl mit der OK-Taste.

#### 7.2.1.8.2. NTP Client: [NTP Server IP Adresse \2182]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ① ⑧ ②. Geben Sie Ihre eigene NTP Server IP Adresse ein (jeder Block dreistellig mit führenden Nullen!) und bestätigen Sie mit der OK-Taste. Mit den Cursortasten ◀ und ▶ können Sie den blinkenden Cursor nach rechts und links bewegen. Die Einstellung der IP Adresse ist nur möglich, wenn DHCP ausgeschaltet ist.

#### 7.2.1.8.3. NTP Client: [Timezone \2183]

Die voreingestellten Werte gelten für ganz Deutschland und müssen nicht geändert werden.

### 7.2.1.9. LAN Parameter: [Neustart \219]



ACHTUNG!
Führen Sie nach Änderung der Einstellungen im Menü [**LAN \21**] unbedingt einen LAN Neustart durch, damit die Änderungen wirksam werden.

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ① ⑨ und bestätigen Sie mit der OK-Taste.
Führen Sie keinen Neustart durch, bleiben die Änderungen im Gerät gespeichert, werden aber nicht aktiv, bis das Gerät das nächste Mal neu gestartet wird.

## 7.2.2. Die Konfiguration der SICCT Parameter [SICCT Parameter \22]

SICCT (Secure Interoperable Chip Card Terminal) ist eine Sicherheitsspezifikation für Kartenterminals und ein wesentlicher Teil der Betriebsart „eHealth KT“. Sie sollten nur von besonders geschulten Administratoren, die die SICCT-Spezifikation kennen und anwenden können, angepasst und verwaltet werden. Die Parameter sind abhängig von den im Netzwerk verwendeten Komponenten und den Anforderungen, die sich daraus ergeben.

### 7.2.2.1. SICCT - Grundsätzliche Funktionsweise

SICCT findet nur in TCP/IP basierenden Netzwerken Anwendung. Um ein Netzwerk mit SICCT zu betreiben, müssen alle Komponenten miteinander bekannt und vertraut gemacht werden. Dies nennt man Pairing. SICCT arbeitet verschlüsselt und stellt die Information nur "vertrauten" Komponenten zur Verfügung. Dadurch wird ein sehr hoher Datenschutz erreicht. Die Verschlüsselung (TLS) benötigt ein Sicherheitsmodul (gSMC-KT in Slot 3 bzw. 4 des ORGA Kartenterminals).

Der Konnektor oder die Signaturanwendungskomponente (SAK) spielen als zentrale Vermittlungsstelle spielt eine entscheidende Rolle, denn diese steuert den Datenfluss, indem er vor jeder Nutzung eine neue Verbindung (Session) herstellt hergestellt wird. Mit jeder Verbindung wird die Gültigkeit der Verschlüsselung und des Pairings gegenseitig geprüft. Nach jeder Nutzung wird die Verbindung abgebaut.
Wenn Sie alle SICCT-Parameter bequem auslesen und auf einem externen Gerät darstellen lassen wollen, drücken Sie die F1-Taste im Menü [**SICCT Parameter \22**], um einen QR-Code darstellen zu lassen und mit einem Smartphone abzuscannen. Der QR-Code beinhaltet die Inhalte, die im Abschnitt 7.3.7.5 »QR-Code: [SICCT-Parameter \375]« auf 96 Seite beschrieben werden.

#### 7.2.2.2. SICCT Parameter: [Keep Alive \221]

Das ORGA Kartenterminal sendet nach dem Aufbau einer SICCT-Session in einem definierten Intervall „Keep Alive Ereignisse“ ("Lebenssignale"), sofern das Kartenterminal über eine eingesteckte gSMC-KT verfügt.

##### 7.2.2.2.1. Keep Alive: [KA Intervall \2211]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ② ① ①. Sie können das Intervall jetzt von einer bis zehn Sekunden einstellen.

##### 7.2.2.2.2. Keep Alive: [KA Timeout \2212]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ② ① ②. Sie können hier einstellen wie lange das Gerät auf ein Kommando vom Konnektor wartet, bevor es selbständig die Verbindung trennt. Der maximale Wert ist von 120 bis 300 Sekunden. Bestätigen Sie Ihre Eingabe mit der OK-Taste.

#### 7.2.2.3. SICCT Parameter: [Protokoll \222]

Hier stellen Sie die Wartezeit zwischen einzelnen Datenblöcken, die Maximaldauer einer Verbindung und die maximal akzeptierbare Fehleranzahl während einer Verbindung ein. Wird eine dieser Zeiten oder die Fehleranzahl überschritten, bricht das Gerät die Verbindung ab.

##### 7.2.2.3.1. Protokoll: [Block read Timeout \2221]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ② ② ①. Stellen Sie die Zeit ein, die das Gerät maximal auf den nächsten Datenblock warten darf. Der Minimalwert beträgt fünf Sekunden, der Maximalwert beträgt 60 Sekunden. Bestätigen Sie Ihre Eingabe mit der OK-Taste.

##### 7.2.2.3.2. Protokoll: [Message read Timeout \2222]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ② ② ②. Stellen Sie die Zeit ein, die das Gerät maximal eine Verbindung hält, wenn eine Information noch unvollständig und fehlerfrei ist. Der Minimalwert beträgt fünf Minuten, der Maximalwert beträgt 60 Minuten. Bestätigen Sie Ihre Eingabe mit der OK-Taste.

#### 7.2.2.3.3. Protokoll: [Max. Protokollfehler \2223]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ② ② ③. Stellen Sie die Anzahl der maximal zulässigen Protokollfehler ein. Der Minimalwert beträgt fünf Fehler, der Maximalwert beträgt 60 Fehler. Bestätigen Sie Ihre Eingabe mit der OK-Taste.

#### 7.2.2.3.4. Protokoll: [SSL accept Timeout \2224]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ② ② ④. Mit diesem Wert stellen Sie ein wie lange das Terminal nach dem Aufbau einer TCP Verbindung auf das "Client Hello" vom Konnektor (Beginn des “TLS Handshake“) wartet (SSL accepted Timeout. Bestätigen Sie Ihre Eingabe mit der OK-Taste.

### 7.2.2.4. SICCT Parameter: [TLS Einstellung \223]

Die Transport Layer Security (TLS) Einstellungen beinhalten die Art und Weise, wie die Daten verschlüsselt werden.

#### 7.2.2.4.1. TLS Einstellungen: [TLS Version \2231]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ② ③ ②. Mit dieser Funktion wählen Sie die passende TLS-Version aus. TLS V 1.2 ist die aktuell verwendete Version. Bestätigen Sie Ihre Eingabe mit der OK-Taste.

#### 7.2.2.4.2. TLS Einstellungen: [TSL Liste \2232]

Hier können Sie die Zertifikats-Liste auswählen (Trust-Service-Statuslist), die entsprechend der Systemarbeit Anwendung finden soll. Die TSL-Listen (TSL-TU = TSL für die Testumgebung; TSL-PU = TSL für die Produktivumgebung; TSL-RU = TSL für die Referenzumgebung) sind von der gematik vorgegeben. Die TSL-LU (Laborumgebung) wurde vom Ingenico Healthcare und seinen Partnern erstellt.
Die TSL-SU (Signaturumgebung) ist eine TSL-Umgebung in der das ORGA 6141 online als Signaturterminal außerhalb der Telematikinfrastruktur für ein Pairing mit einer Signaturanwendungskomponente (SAK). Die Auswahl der TLS-SU Liste [**TSL-SU \22325**] führt zu einer vollständigen Umkonfiguration des Terminals, die unumkehrbar ist. Die Umkonfiguration kann weder durch einen Werksreset noch durch ein Firmware-Update rückgängig gemacht werden.
Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ② ③ ②. Wählen Sie anschließend die ① für die Produktivumgebung (PU) für den Normalbetrieb im Praxisalltag [**TSL-PU \22321**], ② für die Referenzumgebung (RU) während der Integration der Terminals in die Netzwerkumgebung [**TSL-RU \22322**], ③ für den Testbetrieb während einer Softwareänderung [**TSL-TU \22323**] oder ⑤ für die vollständige Umkonfiguration des Terminals zum Signaturterminal außerhalb der Telematikinfrastruktur [**TSL-SU \22325**]. Bestätigen Sie Ihre Auswahl mit der OK-Taste.

ACHTUNG!
Die Trust-Service Status List der Laborumgebung, hier des Terminalherstellers Ingenico Healthcare [**TLS-LU \22324**], wird in den Release Notes zum Terminal inhaltlich beschrieben.
Dieser Menüpunkt dient den alleinigen Test und Instantsetzungsprozessen des Terminals in der Laborumgebung des Terminalherstellers und darf nur zu diesen Zwecken vom Administrator ausgewählt werden.
Die TSL-LU darf vom Administrator nicht zum Betrieb des Gerätes in der Produktivumgebung ausgewählt werden!

ACHTUNG!
Die Wahl der Trust-Service Status List der Signaturumgebung [**TLS-SU \22325**] ist unumkehrbar. Die Umkonfiguration kann weder durch einen Werksreset noch durch ein Firmware-Update rückgängig gemacht werden.
Mit der Auswahl der TSL-SU verliert das ORGA 6141 online seine gematik-Zulassung als eHealth-Terminal.
Es kann dann ausschließlich außerhalb der Telematikinfrastruktur als Signaturterminal nach einem Pairing mit einer Signaturanwendungskomponente (SAK) betrieben werden.

### 7.2.2.5. SICCT Parameter: [Announcement \224]

Das Kartenterminal kann nach einem Neustart zusätzlich einen Aufruf senden um sich "bemerkbar" zu machen. Diese Funktion ist geeignet, um neue Terminals am System zu lokalisieren und zu integrieren. In den Werkseinstellungen ist diese Funktion aktiv und der Wert auf fünf Sekunden eingestellt. Der Administrator kann das Intervall zwischen den Aufrufen auf einen Wert grösser Null und maximal 3000 Sekunden einstellt. Bei Eingabe des Wertes Null ist diese Funktion deaktiviert. Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ② ④. Geben Sie anschließend den gewünschten Wert in Sekunden ein. Bestätigen Sie Ihre Eingabe mit der OK-Taste.

### 7.2.2.6. SICCT Parameter: [Pairings \225]

Um das Kartenterminal auch in komplexeren Systemen umfangreich zu nutzen, kann es an bis zu neun Konnektoren angemeldet sein. Die Anmeldungen (Pairings) werden in der Pairingliste verwaltet. Der Administrator kann an dieser Stelle z. B. alte Pairings löschen, vorhandene Pairings ansehen und mit individuellen Namen versehen, um sie unterscheiden zu können. Jeder Pairingblock (1 bis 3) und innerhalb jedes Pairingblocks kann jeder Schlüssel (Public Key 1 bis 3) mit eigenem Namen versehen werden.
Wählen Sie den Block oder den Schlüssel aus den Sie bearbeiten wollen. Geben Sie z. B. die neue Bezeichnung ein und bestätigen Sie die Eingabe mit der OK-Taste.
Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ② ⑤ und nehmen Sie die gewünschten Einstellungen vor. Bestätigen Sie Ihre Eingabe mit der OK-Taste. Bei den Einstellungen ist es hilfreich sich die Menüstruktur im Anhang 6 »Menüstruktur für den Administrator - Teil 3: SICCT Parameter« auf Seite 105 anzuschauen und ggf. auch dort die Einstellungen zu notieren.

#### 7.2.2.7. SICCT Parameter: [Session Admin \226] (zweite Managementschnittstelle)

Zum Aufbau einer SICCT Admin-Verbindung zwischen Gerät und Konnektor muss eine "Session Admin PIN" angegeben werden. Diese kann individualisiert werden.
Der Menüpunkt [**Session Admin \226**] erlaubt dem Administrator eine vom Terminal-menüzugriff abweichende „SICCT ADMIN PIN“ zu wählen. Wird [**Session Admin \226**] nicht aufgerufen, so erhält die SICCT ADMIN PIN den Wert der Admin-PIN. Die SICCT ADMIN PIN stellt das Password beim Administratorzugriff des Konnektors auf das Terminal via SICCT Protokoll (Kommando SICCT INIT CT SESSION) dar.
Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ② ⑥. Sie werden dazu aufgefordert, eine neue PIN zu vergeben. Geben Sie nun Ihre neue Session Admin PIN ein, bestätigen Sie sie mit der OK-Taste und wiederholen Sie die neue PIN. Bestätigen Sie erneut mit der OK-Taste. Bestätigen Sie Ihre Eingabe mit der OK-Taste. Die neue Session Admin PIN ist jetzt aktiviert.
Die Direktmanagementschnittstelle, welche durch das Terminalmenü abgebildet ist, stellt die primäre Managementschnittstelle am Gerät dar.
Der Zugriff per administrativer SICCT Kommandos stellt ebenfalls eine Managementschnittstelle dar. Administrative SICCT Kommandos können nur im Kontext einer SICCT Admin Session erfolgen. Innerhalb der SICCT Admin Session sind folgende Kommandos zusätzlich erlaubt:

```
SICCT SET STATUS
SICCT CT DOWNLOAD INIT
SICCT CT DOWNLOAD DATA
SICCT CT DOWNLOAD FINISH
```

Für die SICCT ADMIN Session gelten dieselben Sperrzeiten wie für die Admin-PIN (siehe Abschnitt 5.3 »Admin-PIN Zeitsperre« auf Seite 48).

#### 7.2.2.8. SICCT Parameter: [Zugriffsrechte \227]

Im Menü Zugriffsrechte können Sie die Antwort des Terminals auf bestimmte administrative Kommandos des Konnektors aktivieren bzw. deaktivieren. In der Werkseinstellung sind bestimmte administrative Kommandos aktiviert.

##### 7.2.2.8.1. Zugriffsrechte: [Admin Session \2271]

Die Admin Session ist eine SICCT-Verbindung mit Administrator Berechtigung. Sie hat gegenüber einer SICCT Control Session den vollen Befehlsinterpreter mit den nachfolgend beschriebenen zusätzlichen SICCT Kommandos zur Verfügung.

- SICCT SET STATUS
- SICCT CT DOWNLOAD [INIT | DATA | FINISH]

Der Terminal Administrator hat hier die Möglichkeit die Administration des Terminals über den SICCT Kommandointerpreter zu verbieten (deaktiviert = Standardeinstellung) oder zu erlauben (aktivieren). Die Deaktivierung der Admin Session hat zur Folge, dass weder die Namen der Functional Units (z.B. der Terminal Name) (SICCT SET STATUS) noch die Aktualisierung der Firmware (SICCT CT DOWNLOAD …) über den Konnektor erfolgen können.

Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ② ⑦ ①. Zum deaktivieren bzw. aktivieren der Admin SICCT Session drücken Sie anschließend ⓪ zum Deaktivieren und ① zum Aktivieren. Bestätigen Sie Ihre Eingabe mit der ✓OK-Taste.

### 7.2.2.8.2. Zugriffsrechte: [Set Status \2272]

Mit dem Kommando SICCT SET STATUS vergibt der Konnektor einem neu angeschlossenen Terminal automatisch einen Terminalnamen. Wenn Sie dies unterdrücken wollen, um manuell dem Terminal einen Namen zu vergeben, gehen Sie wie folgt vor: Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ② ⑦ ②. Wählen Sie anschließend ⓪ für „Aus“ und ① für „Ein“. Bestätigen Sie Ihre Eingabe mit der ✓OK-Taste. Zum manuellen Ändern des Terminalnamens gehen Sie wie in Abschnitt 7.2.1.1 »LAN Parameter: [Gerätename \211]« auf Seite 60 beschrieben vor. Mit Hilfe des SICCT SET STATUS Kommandos können die Namen einzelner „Functional Units“ des Terminals gesetzt bzw. geändert werden. Im Auslieferungszustand sind die in Tabelle 3 angegebenen Werte gesetzt. Die maximale Länge für den Namen einer Functional Unit beträgt 32 Zeichen.

| Functional Unit | Werkseinstellung (Default Wert) |
|---|---|
| Terminal | Terminal |
| Slot 1 | ICC SLOT 1 |
| Slot 2 | ICC SLOT 2 |
| Slot 3 | ICC SLOT 3 |
| Slot 4 | ICC SLOT 4 |
| Display | Standard Display |
| Keypad | Standard Keypad |

Tabelle 3: *Werksvoreinstellungen der „Functional Units“ des Terminals*

### 7.2.2.8.3. Zugriffsrechte: [Download \2273]

Neben dem manuellen FW-Update kann der ansteuernde Konnektor innerhalb einer SICCT ADMIN Session ein Firmware-Update des Geräts über das SICCT-Protokoll initiieren. Dazu muss der Administrator zuvor die SICCT Admin Session, wie in Abschnitt 7.2.2.8.1 »Zugriffsrechte: [Admin Session \2271]« auf Seite 68 beschrieben, aktiviert haben.
Über die SICCT CT DOWNLOAD Kommandos kann der Konnektor die Firmware des Terminals aktualisieren. Dabei muss der Konnektor die maximale Größe des
SICCT Download Data Daten Objektes (SICCT DL DATA DO) berücksichtigen, welches er nach einem erfolgreichen SICCT CT DOWNLOAD INIT als Responsedaten erhält.
Diese beträgt 4092 Byte inklusive Tag und Length des SICCT DL DATA DOs.
Mit den Downloadkommandos INIT, DATA und FINISH kann der Konnektor das Terminal automatisch mit einer neuen Firmware aktualisieren.
Sobald das vom Konnektor initiierte Firmware-Update startet, wechselt das Gerät in die SICCT Download Session mit einer entsprechenden Zustandsindikation am Display. Wenn Sie dies unterdrücken wollen, um einen Download nur manuell zu starten, gehen Sie wie folgt vor:
Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ② ⑦ ③. Wählen Sie anschließend ⓪ für „Aus“ und ① für „Ein“. Bestätigen Sie Ihre Eingabe mit der ✓OK- Taste. Wie der manuelle Download einer Update-Datei vorgenommen wird, können Sie dem Abschnitt 7.2.9 »Durchführung eines Firmware-Updates [Update \28]« auf Seite 72 entnehmen.

#### 7.2.2.9. SICCT Parameter: [Neustart \228]



ACHTUNG!
Führen Sie nach Änderung der Einstellungen im Menü [**SICCT Parameter \22**] unbedingt einen SICCT Neustart durch, damit die Änderungen wirksam werden.

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ② ⑧ und bestätigen Sie mit der OK-Taste.
Führen Sie keinen Neustart durch, bleiben die Änderungen im Gerät gespeichert, werden aber nicht aktiv, bis das Gerät das nächste Mal neu gestartet wird.

### 7.2.3. Einstellen der Uhrzeit [Zeit \23]

Im Menü [**Zeit \23**] ist in der vorliegenden Firmware-Version 3.8.1 das manuelle Einstellen der Uhrzeit nicht möglich. Die aktuelle Uhrzeit kann aber über einen NTP Server bezogen werden (siehe Abschnitt 7.2.1.8 »LAN Parameter: [NTP Client \218]« auf Seite 63). Bei Auswahl des Menüs erscheint der Hinweis: **Funktion wird nicht unterstützt!**, wenn keine NTP Serverzeit bezogen wird. Ist eine NTP Serverzeit verfügbar kann diese im Menü [**Zeit \23**] eingesehen, aber nicht verändert werden.

### 7.2.4. Einstellen des Datums [Datum \24]

Im Menü [**Datum \24**] ist in der vorliegenden Firmware-Version 3.8.1 das manuelle Einstellen der Uhrzeit nicht möglich. Das aktuelle Datum kann aber über einen NTP Server bezogen werden (siehe Abschnitt 7.2.1.8 »LAN Parameter: [NTP Client \218]« auf Seite 63). Bei Auswahl des Menüs erscheint der Hinweis: **Funktion wird nicht unterstützt!**, wenn kein Datum über einen NTP Server bezogen wird. Ist das Datum über einen NTP Server verfügbar kann dieses im Menü [**Datum \24**] eingesehen, aber nicht verändert werden.

### 7.2.5. Einstellen der Menüsprache [Sprache \25]

Sie können die Sprache des Menüs von Deutsch auf Englisch oder Französisch ändern. Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ⑤ und wählen anschließend die ① für Deutsch, die ② für Englisch oder die ③ für Französisch. Bestätigen Sie Ihre Eingabe mit der OK-Taste. Die Auswahl wird mit **Aktion erledigt** bzw. **Executed** oder **Accomplished** übernommen.

### 7.2.6. Einstellen der Displayanzeige [Display \26]

Im Menü Display können Sie die Darstellung der eGK-Daten aktivieren, den Willkommenstext individualisieren, die Helligkeit des Displays und die Hintergrundfarbe einstellen.

#### 7.2.6.1. Individueller Text im Ruhebildschirm [Freier Text \261]

In diesem Menüpunkt ist es Ihnen möglich, einen Text Ihrer Wahl mit bis zu zwei Zeilen und jeweils 23 Zeichen einzugeben. Dieser Text erscheint im Display im Ruhebildschirm anstelle des

Standardtextes **Willkommen!**. Sie können zum Beispiel den Namen Ihrer Praxis als Willkommenstext eingeben.
Sie befinden sich im Hauptmenü. Ziffern ② [**Admin PIN Eingabe**] ⑥ ①. Nun können Sie den gewünschten Text eingeben. Details zur Freitexteingabe und zum Einfügen von Großbuchstaben, Umlauten und Sonderzeichen finden Sie im Abschnitt 1.4 »Funktionen der verschiedenen Tasten des Gerätes« auf Seite 15 und im Abschnitt 4.1 »Tastatur« auf Seite 41 dieser Bedienungsanleitung. Mit den Cursortasten ◀ und ▶ können Sie den blinkenden Cursor nach rechts und links bewegen und mit der CLEAR-Taste können Sie den Text links neben dem blinkenden Cursor löschen.



HINWEIS
Bei der Texteingabe ist die Eingabe von maximal 22 Zeichen pro Zeile möglich. Sonderzeichen sind mit der Taste ① [**! ? # $ & * ß 1**] und der Taste ⓪ [**/ - + . , ; : , 0**] einzugeben.

### 7.2.6.2. Einstellen der Displayhelligkeit [Helligkeit \262]

Um die Helligkeit des Displays auf Ihre Bedürfnisse anzupassen, drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ⑥ ②. Mit den Cursortasten ◀ und ▶ können Sie die Helligkeit individuell regeln. Beenden Sie die Einstellung mit der OK-Taste.

### 7.2.6.3. Einstellen der Hintergrundfarbe [Hintergrundfarbe \263]

Um die Hintergrundfarbe des Displays zu wählen, drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ⑥ ③ und wählen anschließend die ① für einen blauen, die ② für einen schwarzen oder die ③ für einen rosa Hintergrund. Bestätigen Sie Ihre Eingabe mit der OK-Taste.

## 7.2.7. Einstellen der Signaltöne [Töne \27]

Sie haben die Möglichkeit, Tastenklicks, akustische Signale und das Start Jingle einzeln an- und auszuschalten sowie die Gesamtlautstärke anzupassen. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ⑦ und wählen anschließend die ① für das Ein- bzw. Ausschalten der Tastenklicks, die ② für die akustischen Signale oder die ③ für das Start Jingle. Bestätigen Sie Ihre Auswahl mit der OK-Taste. Wählen Sie anschließend ⓪ für „Aus“ und ① für „Ein“. Bestätigen Sie Ihre Eingabe mit der OK-Taste. Um die Lautstärke der Signale auf Ihre Bedürfnisse anzupassen drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ⑦ ④. Mit den Cursortasten ◀ und ▶ können Sie die Lautstärke individuell regeln. Beenden Sie die Einstellung mit der OK-Taste.

## 7.2.8. Einstellen des akustischen PIN Schutzes [Akustischer PIN Schutz \275]



ACHTUNG!
Nur die höchstmögliche Lautstärke zehn des Maskierungsrauschens ist als ausreichend sicher gegen Ausspähversuche zu betrachten. Diese Lautstärke ist für einen zertifizierten und zugelassenen Betriebszustand zu wählen.

Das Terminal schützt alle PIN Eingaben vor einem akustischen Ausspähversuch, indem es während der PIN Eingabe ein Rauschen über den Lautsprecher abgibt, das die Eingabegeräusche während der PIN Eingabe maskiert.
Es besteht die Möglichkeit die Lautstärke des Maskierungsgeräusches anzupassen. Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ⑦ ⑤. Mit den Cursortasten ◀ und ▶ können Sie die Lautstärke individuell regeln. Beenden Sie die Einstellung mit der OK-Taste.

### 7.2.9. Durchführung eines Firmware-Updates [Update \28]

Ein Update der Geräte-Firmware bedeutet das Einspielen einer neuen zugelassenen Geräte-Software in das Kartenterminal. Dieses geschieht über einen Dateitransfer mittels einer sogenannten Firmware-Image Datei. Es stehen verschiedene Möglichkeiten des Dateitransfers zur Verfügung, die in den folgenden Abschnitten detailliert beschriebene werden.
Die Zulassung zulässiger Geräte-Software obliegt der gematik und unterliegt den gematik-Zulassungsbedingungen. Zugelassene Software-Versionen (mit Angabe der Firmware-Version) kann der Administrator der Übersicht über zugelassene TI-Komponenten („Übersicht der erteilten Zulassungen und Bestätigungen“) auf der gematik Internetseite entnehmen.
https://www.gematik.de/cms/de/zulassung/uebersicht_der_erteilten_zulassungen/zulassungsbersicht_1.jsp
Die Überprüfung, ob es sich bei der gematik zugelassenen Software auch um eine vom BSI zertifizierte Software handelt, kann der Administrator der Security Target (ST) Veröffentlichung und dem Zertifizierungsreport auf der BSI Internetseite entnehmen.
https://www.bsi.bund.de/DE/Home/home_node.html.
Die Verfahrensnummer für das ORGA 6141 online lautet: BSI-DSZ-CC-0519



ACHTUNG!
Aus Gründen der Betriebssicherheit muss der Administrator die Verfügbarkeit von aktuellen zugelassenen Firmware-Versionen organisatorisch sicherstellen, das heißt zyklisch auf verfügbare Firmware-Updates prüfen. Sofern eine zugelassene Firmware-Version verfügbar ist, muss der Administrator Sorge tragen, dass diese aktuelle Version eine vorgehende zeitnah ersetzt.



ACHTUNG!
Aus Gründen der Datensicherheit darf das Kartenterminal nur in einer gesicherten Einsatzumgebung, in der es nie unbeaufsichtigt ist, upgedatet werden!



ACHTUNG!
Schalten Sie auf gar keinen Fall während des Updatevorgangs das Gerät aus oder trennen es vom Stromnetz!



ACHTUNG!
Setzen Sie sich bei einem fehlgeschlagenen Update oder bei Zweifeln über den genauen Ablauf des Updates mit der technischen Hotline von Ingenico Healthcare in Verbindung.



ACHTUNG!
Beachten Sie, dass nach der erfolgreichen Installation von neuer Firmware die mit dieser Firmware ausgelieferte Informationen (Release Notes und ggf. eine neue Bedienungsanleitung) maßgeblich ist.



ACHTUNG!
Kontrollieren vor dem Update die Version der geladenen Firmware und anhand der beigestellten Informationen (Release Notes) die neue Version, welche in das Gerät geladen werden soll.
Kontrollieren Sie nach dem erfolgten Firmware Update und Geräteneustart über die Terminalselbstauskunft, die neue Firmware-Version (siehe Abschnitt 7.3.2 »Die Terminalselbstauskunft [Status \32]« auf Seite 84).

Wenn Sie alle Update-Parameter bequem auslesen und auf einem externen Gerät darstellen lassen wollen, drücken Sie die F1-Taste im Menü [**Update \28**], um einen QR-Code darstellen zu lassen und mit einem Smartphone abzuscannen. Der QR-Code beinhaltet die Inhalte, die im Abschnitt 7.3.7.6 »QR-Code: [Update Parameter \376]« auf Seite 96 beschrieben werden.

#### 7.2.9.1. Firmware Update via Konnektor

Sofern das Terminal nach erfolgtem Pairing mit einem Konnektor verbunden ist, kann ein Firmware-Image vom (Konnektor-) Administrator über die sogenannte Benutzerschnittstelle des Konnektors selektiert und an das Terminal gesendet werden. Der Konnektor-Administrator sorgt vorbereitend dafür, dass eine neue zugelassene Firmware-Image Datei im Konnektor abgelegt ist. Er trägt die Verantwortung dafür, dass die im Konnektor abgelegte Firmware-Update Datei aus einer vertrauenswürdigen Quelle stammt und die korrekte Firmware-Version beinhaltet.
Anschließend löst der (Konnektor-) Administrator das Firmware-Update über den Konnektor aus. Der Konnektor eröffnet daraufhin automatisch eine sogenannte SICCT Download-Session, und sendet das Firmware-Image an das verbundene Terminal unter Verwendung der SICCT-Download Kommandos, mittels welcher die Konnektor-Logik den Datentransfer phasenweise steuert, überwacht und dessen Ende-Status über Rückgabewerte vom Terminal direkt auswertet. Am Kartenterminal beobachtet der Administrator die Statusmeldungen der ausgeführten Updatephasen am Terminaldisplay, braucht mit dem Terminal aber nicht selbst zu interagieren. Der erfolgreiche Fortgang (Gutfall) zeigt sich am Terminal mit einem Wechsel in die nächste folgende Phase. Zur Sicherheit muss nach dem erfolgreichen Updatevorgang die installierte Firmware-Version noch einmal sowohl in der Benutzeroberfläche des Konnektors unter Konnektor-Services als auch in der Terminal-Selbstauskunft (siehe Abschnitt 7.3.2 »Die Terminalselbstauskunft [Status \32]« auf Seite 84) kontrolliert werden. Im Fehlerfall erfolgt eine Fehlernachricht, welche angibt, dass die jeweils vorangegangene Aktion nicht durchgeführt werden konnte. Im Negativfall bleiben die vom Terminal empfangenen Daten unberücksichtigt und der vorhergehende Firmware-Stand erhalten. Nach dem Neustart arbeitet das Terminal erneut mit den zuvor eingestellten Betriebsparametern und befindet sich dann im betriebsbereiten Zustand.

| Update-Verlauf | Displayanzeige |
|---|---|
| 1. Initialisierung | **Firmware Update *<br>Bitte warten…** |
| 2. Datenübertragung | **Signatur wird geprüft ...<br>Update wird eingelesen ...** |
| 3. Verifikation abgeschlossen | **Signatur ist gültig** |
| 4. Migration der Konfiguration | **Konfiguration wird vorbereitet... *<br>Konfiguration wird migriert...** |
| 5. Übernahme der FW in den Systemspeicher | **Update wird durchgeführt...** |
| 6. FW erfolgreich in den Systemspeicher übernommen | **Update wird abgeschlossen... *<br>Vorgang erfolgreich** |
| 7. Aktivierung der FW per Geräteneustart | **Neustart** |

* Die Meldungen erscheinen nur für einen sehr kurzen Augenblick.

Tabelle 4: *Displayanzeige während eines Firmware-Updates via Konnektor*

### 7.2.9.2. Firmware Update per USB-Stick (Pull-Verfahren)

ACHTUNG!
Der Administrator muss vor dem Kopier- und Update-Vorgang organisatorisch kontrollieren, dass die entsprechende Firmware-Image Datei aus einer sicheren Quelle bezogen wurde und eine aktuelle, zugelassene und zertifizierte Firmware-Version beinhaltet.
Des Weiteren darf der Administrator nur einen vertrauenswürdigen USB-Stick verwenden, dessen Filesystem-Inhalte er selbst kontrolliert und am besten zuvor gelöscht bzw. zusätzlich z. B. mittels Virenscanner geprüft hatte. Nach dem Update muss der Administrator den USB-Stick wieder sicher verwahren.

HINWEIS
Für die Installation mit einem USB-Stick benötigen Sie einen USB-Stick mit einem FAT32 Dateisystem.
Kopieren Sie die Update-Datei in Stammverzeichnis des USB-Sticks und stecken Sie ihn anschließend in die USB-A Buchse auf der Unterseite des ORGA 6141 online.

Es besteht die Möglichkeiten des Dateitransfers via USB-Stick am USB-A (Host) des Kartenterminals. Die Firmware-Image Datei muss dafür vom Administrator zuvor in das Root-Verzeichnis eines USB-Sticks kopiert werden.

#### 7.2.9.2.1. Voraussetzungen zur Durchführung des Updates

- Die Administrator PIN des Terminals muss bekannt sein.
- Ein USB-Stick im FAT32 Format wird für das Update benötigt.
- Die Firmware-Image Datei (*.dfu) liegt im Stammverzeichnis des USB-Sticks
- Der Dateiname des Firmware-Image muss dem eingestellten Namen im eHealth Terminal im Menü [**Dateiname \281**] entsprechen (siehe Abschnitt 7.2.9.5 »Firmware-Update: [Dateiname \281]« auf Seite 80).

### 7.2.9.2.2. Durchführung der Firmware-Aktualisierung per USB-Stick




Abbildung 29: *Informationen über die Update-Datei (1/3)*




Abbildung 30: *Informationen über die Update-Datei (2/3)*




Abbildung 31: *Informationen über die Update-Datei (3/3)*

Kopieren Sie die Firmware-Image Datei des ORGA 6141 online in das Stammverzeichnis des USB-Sticks und stecken Sie anschließend den USB-Stick in den USB-A Port auf der Unterseite des Terminals.

Drücken Sie anschließend die Ziffern ② [**Admin PIN Eingabe**] ⑧ ①, geben Sie den Dateinamen des Updates ein und bestätigen Sie die Eingabe mit der OK-Taste.

Mit den Cursortasten ◀ und ▶ können Sie den blinkenden Cursor nach rechts und links bewegen und mit der CLEAR-Taste können Sie den Text links neben dem blinkenden Cursor löschen. Bestätigen Sie die Eingabe durch Drücken der OK-Taste.

Nach der Eingabe des Dateinamens befinden Sie sich wieder im Menü [**Update \28**]. Wählen Sie anschließend den Menüpunkt [**Update starten \285**]. Wählen Sie anschließend die ② für den Start des Updates via USB-Stick. Bestätigen Sie Ihre Eingabe mit der OK-Taste.

Die Signatur der Updatedatei wird geprüft und nach erfolgreicher Prüfung vom USB-Stick in das Terminal übertragen. Ist dieser Vorgang erfolgreich abgeschlossen, wird Ihnen das im Display wie in Abbildung 32 angezeigt.

Mit den Cursortasten ◀ und ▶ können Sie sich weitere Informationen, wie in Abbildung 30 und Abbildung 31 dargestellt, zur aktuell auf dem Gerät befindlichen und zur Firmware-Version auf dem USB-Stick anzeigen lassen. Die grünen Pfeile vor den Versionsnummern der einzelnen Bestandteile der Firmware zeigt Ihnen an, welche Bestandteile der neuen Firmware aktualisiert werden.

Bestätigen Sie nach der Überprüfung die Sicherheitsabfrage **Sind Sie sicher? [OK/STOP]** mit der OK-Taste.

Nach erfolgreicher Datenübertragung startet das Terminal neu und führt den Update Vorgang selbstständig aus. Abschließend startet das Terminal nach der erfolgreichen Firmware-Aktualisierung erneut und befindet sich dann im betriebsbereiten Zustand.



ACHTUNG!
Unterbrechen Sie unter keinen Umständen während des Update-Vorgangs die Stromversorgung zum Gerät, da dies zur unvollständigen und fehlerhaften Installation der neuen Firmware führen kann und das Gerät hierdurch ggf. zerstört werden könnte!

### 7.2.9.3. Firmware Update per TFTP-Server (Pull-Verfahren)

Es besteht die Möglichkeiten des Dateitransfers via LAN bzw. TFTP-Protokoll, wobei das Kartenterminal die Firmware-Image Datei von einem TFTP-Server (im sogenannten Pull-Verfahren) abruft.



ACHTUNG!
Der Administrator muss vor dem Kopier- und Update-Vorgang organisatorisch kontrollieren, dass die entsprechende Firmware-Image Datei aus sicherer Quelle bezogen wurde und eine aktuelle, zugelassene und zertifizierte Firmware-Version beinhaltet.

#### 7.2.9.3.1. Voraussetzungen zur Durchführung des Updates

- Die Administrator PIN des Terminals muss bekannt sein.
- Ein TFTP Server ist im lokalen Netz vorhanden.
- Das Terminal und der TFTP-Server sind Teil desselben lokalen Sub-Netzwerks.
- Die Firmware-Image Datei (*.dfu) liegt im Stammverzeichnis des TFTP Servers.
- Der Dateiname der Firmware-Image Datei musst dem eingestellten Namen im eHealth Terminal im Menü [**Dateiname \281**] entsprechen (siehe Abschnitt 7.2.9.5 »Firmware-Update: [Dateiname \281]« auf Seite 80).
- Die IP-Adresse des TFTP-Servers ist im Terminal im Menü [TFTP Server IP Adresse \282] korrekt eingestellt (siehe Abschnitt 7.2.9.6 »Firmware-Update: [TFTP Server IP Adresse \282]« auf Seite 80).

#### 7.2.9.3.2. Durchführung der Firmwareaktualisierung via TFTP Server im Pull-Verfahren

Kopieren Sie die Firmware-Image Datei des ORGA 6141 online in das Stammverzeichnis des TFTP-Servers der sich im selben Netzwerk (identisches lokales Sub-Netzwerk) wie das Terminal befindet.
Drücken Sie anschließend die Ziffern ② [**Admin PIN Eingabe**] ⑧ ①, geben Sie den Dateinamen des Updates ein und bestätigen Sie die Eingabe mit der OK-Taste.
Mit den Cursortasten ◀ und ▶ können Sie den blinkenden Cursor nach rechts und links bewegen und mit der CLEAR-Taste können Sie den Text links neben dem blinkenden Cursor löschen. Bestätigen Sie die Eingabe durch Drücken der OK-Taste.
Nach der Eingabe des Dateinamens befinden Sie sich wieder im Menü [**Update \28**]. Wählen Sie anschließend den Menüpunkt [**TFTP Server IP Adresse\282**] und geben Sie die TFTP Server IP Adresse ein.
Nach der Eingabe der Server IP Adresse befinden Sie sich wieder im Menü [**Update \28**]. Wählen Sie anschließend den Menüpunkt [**Update starten \285**]. Wählen Sie anschließend die ① für den Start des Updates via TFTP Server.



HINWEIS
Sie starten den Update-Vorgang und die Überprüfung der Update-Datei wie im Abschnitt 7.2.9.2.2 »Durchführung der Firmware-Aktualisierung per USB-Stick« auf Seite 75 beschrieben. Bitte beachten Sie diese Vorgehensweise und befolgend Sie sie genau!

Anschließend führt das Terminal alle weiteren Schritte aus, dessen Ablauf der Administrator anhand folgender Statusmeldungen verfolgt. Der erfolgreiche Fortgang (Gutfall) zeigt sich mit einem Wechsel in die nächst folgende Aktion. Im Fehlerfall folgt auf eine Aktionsmeldung die generelle Fehlernachricht „TFTP-Abbruch“, welche angibt, dass die jeweils vorangegangene Aktion nicht durchgeführt werden konnte. Im Negativfall bleiben die empfangenen Daten unberücksichtigt und der zu vorige Firmware-Stand erhalten. Nach dem Neustart arbeitet das Terminal erneut mit den übernommenen Betriebsparametern und befindet sich dann im betriebsbereiten Zustand.

| Update-Verlauf | Displayanzeige |
|---|---|
| 1. Empfang der FW-Datei vom TFTP-Server und Verifikation des FW-Images | **Signatur wird geprüft ...**<br>**Update wird eingelesen ...** |
| 2. Verifikation abgeschlossen | **Signatur ist gültig** |
| 3. Benutzerdialog | **Update kann jetzt durchgeführt werden.**<br>**Sind Sie sicher? [OK/STOP]** |
| 4. Migration der Konfiguration | **Konfiguration wird vorbereitet... ***<br>**Konfiguration wird migriert...** |
| 5. Übernahme der FW in den Systemspeicher | **Update wird durchgeführt...** |
| 6. FW erfolgreich in den Systemspeicher übernommen | **Update wird abgeschlossen... ***<br>**Vorgang erfolgreich** |
| 7. Aktivierung der FW per Geräteneustart | **Neustart** |

* Die Meldungen erscheinen nur für einen sehr kurzen Augenblick.

Tabelle 5: *Displayanzeige während eines Firmware-Updates via TFTP Server im Pull-Verfahren*



ACHTUNG!
Unterbrechen Sie unter keinen Umständen während des Update-Vorgangs die Stromversorgung zum Gerät, da dies zur unvollständigen und fehlerhaften Installation der neuen Firmware führen kann und das Gerät hierdurch ggf. zerstört werden könnte!

### 7.2.9.4. Firmware Update per Steuerfile am TFTP Server (Push Verfahren)

Es besteht die Möglichkeiten des Dateitransfers via LAN bzw. TFTP-Protokoll, wobei das Kartenterminal eine Steuerdatei mit einem Hinweis auf ein an einem TFTP-Server bereitstehende Firmware-Image Datei abruft. Dadurch, dass das Steuerfile von außen modifiziert werden kann, entsteht ein (Pseudo-) Push Verfahren.



ACHTUNG!
Für den zertifizierten Betrieb darf der Administrator diesen Update-Vorgang, der standardmäßig deaktiviert ist, aus Sicherheitsgründen nicht verwenden!

Dieses Verfahren richtet sich an den erfahrenen Administrator und ist für den Betrieb im Hintergrund konzipiert. D.h. der Update-Prozess verzichtet hierbei auf Status- und Fehlerindikationen am Terminal. Alle Teilschritte erfolgen ohne Displaynachrichten wie beim interaktiven FW-Update (PULL). im Gutfall zeigt das Terminal nach erfolgreichem Update einen abschließenden „Neustart“ an. Im Fehlerfall verwirft das Terminal alle Empfangsdaten und arbeitet (ohne Neustart) unverändert weiter. Den Ausgang des Update-Prozesses erkennt der Administrator zum einen am TFTP-Server- Status (ggf. Log-File samt Abrufstatus inklusive Übertragungsstatus mit Start- und Enddatum) sowie aus einem „Vor-Nachher-Vergleich“ von Abfragedaten des Terminals (u.a. aktive Firmware-Version, Update-ID, TSL-Versionierung) entweder über den Konnektor während einer aktiven TLS-/ SICCT-Terminal-Session oder direkt über das Terminalmenü (Status).



ACHTUNG!
Der Administrator muss vor dem Kopier- und Update-Vorgang organisatorisch kontrollieren, dass die entsprechende Firmware-Image Datei aus sicherer Quelle bezogen wurde und eine aktuelle, zugelassene und zertifizierte Firmware-Version beinhaltet.

#### 7.2.9.4.1. Voraussetzungen zur Durchführung des Updates

- Die Administrator PIN des Terminals muss bekannt sein.
- Ein TFTP Server ist im lokalen Netz vorhanden.
- Das Terminal und der TFTP-Server sind Teil desselben lokalen Sub-Netzwerks.
- Die Firmware-Image Datei (*.dfu) liegt im Stammverzeichnis des TFTP Servers.
- Der Dateiname der Firmware-Image Datei musst dem eingestellten Namen im eHealth Terminal im Menü [Dateiname \281] entsprechen (siehe Abschnitt 7.2.9.5 »Firmware-Update: [Dateiname \281]« auf Seite 80).
- Die IP-Adresse des TFTP-Servers ist im Terminal im Menü [TFTP Server IP-Adresse \282] korrekt eingestellt (siehe Abschnitt 7.2.9.6 »Firmware-Update: [TFTP Server IP Adresse \282]« auf Seite 80).
- Das Abfragen nach einer Firmware-Image Datei wurde im Menü [Poll Status \283] aktiviert (siehe Abschnitt 7.2.9.7 »Firmware-Update: [Poll Status \283]« auf Seite 80).

#### 7.2.9.4.2. Syntax der Steuerdatei

Eine Steuerdatei wird durch eine Textdatei im ASCII-Format dargestellt. Der Dateiname der Steuerdatei lautet **`ctfwupdctl.txt`** (14 Zeichen inklusive Dateiextension **`.txt`**). Das Format der Steuerdatei ist ASCII, zeilenweiser Aufbau, eine Vereinbarung / Anweisung je Zeile.
Es gilt folgende Syntax:

- Der Aufbau der Textdatei erfolgt zeilenweise mit LF oder CRLF als Markierung des Zeilenendes.
- Je Zeile wird maximal eine Anweisung vereinbart.
- Jede Anweisung beginnt mit einem Steuerwort links vor dem Trennzeichen "=" dem unmittelbar eine Vereinbarung folgt.
- Eine Anweisung mit einem der in Tabelle 6 dargestellten Steuerworte darf jeweils nur einmal je Steuerdatei erfolgen.

| Steuerwort | Wertebereich / Format | Mandatory / Obtional | Beschreibung |
|---|---|---|---|
| updateid | < 1 bis 32 Zeichen lange Update – ID><br><br>Format: ASCII, alphanumerisch | M | Die <updateid> dient als eindeutiges Zuordnungskriterium, welche auch am KT erkannt bzw. vom KT abgefragt werden kann und sollte eine leicht erkennbare Datums- und Versionsinformation enthalten.<br>Es werden max. 32 Zeichen übernommen.<br>Die Angabe der <updateid> MUSS in dem Steuerfile vorhanden sein. |
| updatefile | <1 bis 32 Zeichen langer Dateiname><br><br>Format: ASCII, alphanumerisch | O | Dateiname ohne Pfadangabe.<br>Es werden max. 32 Zeichen übernommen.<br>Fehlende oder leere Angabe bedeutet, den voreingestellten Menü-Parameter zu verwenden. |
| updatewindow | <1 Zeichen lange Zahl><br><br>Wertebereich "0" - "4"<br><br>Format: ASCII, numerisch | O | Definiert einen Indexwert für die max. Wartezeit den sich ein KT als Zufallswert errechnen darf und dessen Frist bis zum Neustart und Auslösens bzw. Startens des FW – Update - Prozesses abgewartet werden muss.<br>Es wird max. 1 Zeichen übernommen.<br>Fehlende oder leere Angabe bedeutet, den voreingestellten Menü-Parameter zu verwenden. |

Tabelle 6: *Mögliche Steuerwörter der Steuerdatei für das Update via TFTP Server im Push Verfahren*

#### 7.2.9.4.3. Durchführung der Firmware-Aktualisierung via TFTP Server im Push-Verfahren

Kopieren Sie die Firmware-Updatedatei des ORGA 6141 online und die auf Ihre Bedürfnisse angepasste Steuerdatei **ctfwupdctl.txt** in das Stammverzeichnis des TFTP-Servers der sich im selben Netzwerk (identisches lokales Sub-Netzwerk) wie das Terminal befindet.
Legen Sie den Dateinamen des Firmware-Image Datei in der Steuerdatei oder im Terminal im Menü [**Dateiname \281**] fest.
Wählen Sie anschließend den Menüpunkt [**TFTP Server IP Adresse\282**] und geben Sie die TFTP Server IP Adresse ein.
Sobald das Terminal das Steuerfile übertragen und ausgewertet hat startet es neu.
Abschließend startet das Terminal nach der erfolgreichen Firmware-Aktualisierung erneut und befindet sich dann im betriebsbereiten Zustand.



ACHTUNG!
Unterbrechen Sie unter keinen Umständen während des Update-Vorgangs die Stromversorgung zum Gerät, da dies zur unvollständigen und fehlerhaften Installation der neuen Firmware führen kann und das Gerät hierdurch ggf. zerstört werden könnte!

### 7.2.9.5.Firmware-Update: [Dateiname \281]

Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ⑧ ①, geben Sie den Dateinamen des Updates ein und bestätigen Sie die Eingabe mit der OK-Taste. Mit den Cursortasten ◀ und ▶ können Sie den blinkenden Cursor nach rechts und links bewegen und mit der CLEAR-Taste können Sie den Text links neben dem blinkenden Cursor löschen. Bestätigen Sie die Eingabe durch Drücken der OK-Taste.
Nach der Eingabe des Dateinamens befinden Sie sich wieder im Menü [**Update \28**]. Wählen Sie anschließend den Menüpunkt [**Update starten \281**]. Wählen Sie anschließend die ① für ein Update via TFTP oder die ② für ein Update via USB Stick. Bestätigen Sie Ihre Eingabe mit der OK-Taste und erneut die Sicherheitsabfrage **Sind Sie sicher? [OK/STOP]** mit der OK-Taste.

### 7.2.9.6.Firmware-Update: [TFTP Server IP Adresse \282]

Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ⑧ ②, geben Sie die IP Adresse des Update Servers ein und bestätigen Sie die Eingabe mit der OK-Taste. Mit den Cursortasten ◀ und ▶ können Sie den blinkenden Cursor nach rechts und links bewegen und mit der CLEAR-Taste können Sie den Text links neben dem blinkenden Cursor löschen.

### 7.2.9.7.Firmware-Update: [Poll Status \283]

Mit dem Poll Status aktivieren bzw. deaktivieren Sie eine Abfragen nach einer Firmware-Image Datei per Steuerfile am TFTP Server.
Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ⑧ ③ und wählen Sie anschließend ⓪ für „Aus“ und ① für „Ein“. Bestätigen Sie Ihre Eingabe mit der OK-Taste.

### 7.2.9.8.Einstellmöglichkeiten über [Poll Window \284]

Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ⑧ ④. Geben Sie die den gewünschten Wert entsprechend der möglichen Parameter in Tabelle 7 für die ‚Poll Windows' ein und bestätigen Sie die Eingabe mit der OK-Taste.
Aus dem eingegeben Parameter wird eine Zufallszeitspanne zum Abruf der Steuerdatei errechnet.

| Eingestellter Indexwert | Zufallszeitspanne | Resultierende Wartezeit |
|---|---|---|
| 0 | 0 keine zus. zufällige Wartezeit | Minimale Zeitspanne = 30 Sekunden |
| 1 | 0 … 15 Sekunden | 30 bis 45 Sekunden |
| 2 | 0 … 255 Sekunden (default) | Default Zeitspanne = 30 bis 285 Sekunden (~5 Minuten) |
| 3 | 0 … 4095 Sekunden | 30 bis 4125 Sekunden (~69 Minuten = 1,15 Stunde) |
| 4 | 0 … 35535 Sekunden | 30 bis 35565 Sekunden (593 Minuten = 9,88 Stunden) |

Tabelle 7: *Parameter des Abfrageintervalls für das Update via TFTP Server im Push Verfahren*

### 7.2.9.9.Firmware-Update: [Update starten \285]



ACHTUNG!
Lesen Sie sich bitte vorm Start des Firmware-Updates den gesamten Abschnitt 7.2.9 »Durchführung eines Firmware-Updates [Update \28]« ab Seite 72 durch, bevor Sie mit dem Update beginnen.

Sie können die Quelldatei für das Firmware-Update im Netzwerk oder auf einem USB-Stick zur Verfügung stellen. Dabei ist darauf zu achten, dass die Installationsdatei im Stammverzeichnis der Netzwerkquelle (TFTP Server IP Adresse) bzw. des USB-Sticks als .dfu-Datei vorliegt.



HINWEIS
Für die Installation mit einem USB-Stick benötigen Sie einen USB-Stick mit einem FAT32 Dateisystem.
Kopieren Sie die Update-Datei in Stammverzeichnis des USB-Sticks und stecken Sie ihn anschließend in die USB-A Buchse auf der Unterseite des ORGA 6141 online.

Drücken Sie die Ziffern ② [**Admin PIN Eingabe**] ⑧ ④ und wählen Sie anschließend ① um die Installation einer .dfu-Installationsdatei im Netzwerk oder ② vom USB-Stick zu starten. Bestätigen Sie Ihre Auswahl mit der OK-Taste. Anschließend werden Sie zur Sicherheit noch einmal gefragt: **Sind Sie sicher? [OK/STOP]**.
Starten Sie das Firmware-Update mit Drücken der OK-Taste. Die Installation startet anschließend und kann nicht wieder gestoppt oder rückgängig gemacht werden! Nach erfolgreichem Update startet das Terminal selbstständig neu. Sobald der Ruhebildschirm erscheint, können Sie den USB-Stick – falls das Update per USB-Stick erfolgte – entfernen und das ORGA 6141 online wieder in Betrieb nehmen.

Brechen Sie den Vorgang mit Drücken der STOP-Taste ab, falls Sie sich nicht wirklich sicher sind, ob Sie das ORGA 6141 online mit einer neuen Firmware updaten wollen.



ACHTUNG!
Starten Sie das Update nur, wenn Sie sich ganz sicher sind, dass
- Die Installationsdatei aus einer vertrauenswürdigen Quelle stammt (z. B. Ingenico Healthcare Internetseite),
- der Dateiname Menü [**Dateiname \281**] mit dem Dateinamen der zu installierenden Update-Datei übereinstimmt und
- bei Update via. Netzwerk, die korrekte Quelle im Menü [**TFTP Server IP Adresse \282**] eingetragen wurde.



ACHTUNG!
Der Update-Vorgang kann je nach Quelle zwischen wenigen Minuten bis zu einer halben Stunde dauern.
Unterbrechen Sie unter keinen Umständen während des Update-Vorgangs die Stromversorgung zum Gerät, da dies zur unvollständigen und fehlerhaften Installation der neuen Firmware führen kann und das Gerät hierdurch ggf. zerstört werden könnte!

## 7.2.10. Durchführung eines Updates der Konfigurationsparameter [Update \28]



ACHTUNG!
Aus Gründen der Datensicherheit darf das Kartenterminal nur in einer gesicherten Einsatzumgebung, in der es nie unbeaufsichtigt ist, upgedatet werden!



ACHTUNG!
Lesen Sie vor einem Konfigurationsparameter-Update unbedingt die mit dem Update ausgelieferte Installationsanleitung und die Release Notes durch und beachten Sie genau die darin beschriebene Vorgehensweise!



ACHTUNG!
Schalten Sie auf gar keinen Fall während des Updatevorgangs das Terminal aus!
Trennen Sie auf gar keinen Fall den USB-Stick während des Updatevorgangs vom Terminal!



ACHTUNG!
Setzen Sie sich bei einem fehlgeschlagenen Update oder bei Zweifeln über den genauen Ablauf des Updates mit der technischen Hotline von Ingenico Healthcare in Verbindung.



ACHTUNG!
Die zu der jeweils aktiven Firmware gültige Bedienungsanleitung bleibt nach dem erfolgreichen Update von neuen Konfigurationsparametern gültig.

Analog zur Durchführung von Softwareupdates kann über den USB-A Port des ORGA 6141 online via USB-Stick oder die LAN-Schnittstelle ein Update der Konfigurations-

parameter eingespielt werden. Anstelle einer Firmware-Image Datei wird in diesem Fall eine elektronisch signierte Datei mit Konfigurationsparametern geladen. ändert dabei nicht die Firmware-Version des Terminals.
Ein Update der Konfigurationsparameter kann notwendig sein, um z.B. eine neue Version der Trusted Services List (TSL) für einen der Vertrauensräume (PU, RU, TU, LU, SU) in das Terminal einzuspielen.
Eine Datei mit Konfigurationsparametern wird in Form eines vom Hersteller elektronisch signierten Download-Moduls zusammen mit Release Notes und einer Installationsanweisung ausgegeben. Diese begleitenden Angaben geben Auskunft über die Inhalte der neuen Konfigurationsparameter. Z. B. über den Inhalt (u. a. Hinweise zu enthaltenen Zertifikaten) einer neuen TSL PU sowie zu Kontrollaktivitäten, um entsprechende Veränderungen am Terminal vor und nach dem Update festzustellen und zu protokollieren. Am Beispiel Update der TSL PU ist eine Kontrolle per Versionsnummer der jeweils installierten TSL PU per Aufruf der Terminalselbstauskunft (siehe Abschnitt 7.3.2 »Die Terminalselbstauskunft [Status \32]« auf Seite 84) vorzunehmen.
Die einzuhaltenden Updateschritte und -vorschriften sind dieselben wie die ab dem vorherigen Abschnitt 7.2.9.2 beschriebenen. Updates sind generell nur durch autorisierte Personen (z. B. den Administrator) in gesicherten Umgebungen (z. B. Arztpraxen) erlaubt. Siehe Abschnitt 2.8 »Allgemeine Regeln & Anforderungen zur Betriebssicherheit des Gerätes« auf Seite 34.

## 7.3. Der Menüpunkt Service [Service \3]

Das Servicemenü bietet ihnen die Möglichkeiten, die Admin-PIN zu ändern, den Status des Gerätes zu überprüfen, Sicherheitseinstellungen des Gerätes zu verändern, die Gerätefunktionen zu überprüfen und im sogenannten Kiosk-Modus den Zugriff auf das gesamte Menü zu verhindern.
Wenn Sie eine Übersicht der aktuellen Betriebsdaten und Statistiken des Terminals bequem auslesen und auf einem externen Gerät darstellen lassen wollen, drücken Sie die F1-Taste im Menü [**Service \3**], um einen QR-Code darstellen zu lassen und mit einem Smartphone abzuscannen. Der QR-Code beinhaltet die Inhalte, die im Abschnitt 967.3.7.7 »QR-Code: [Service/Einstellungen \377]« auf Seite 96 beschrieben werden.

### 7.3.1. Ändern der Admin-PIN [PIN ändern \31]

Im Menü [**Admin-PIN ändern \31**] haben Sie die Möglichkeit die Admin-PIN zu ändern. Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ③ und ①. Sie werden aufgefordert, die bisher gültige Admin-PIN einzugeben und diese mit der OK-Taste zu bestätigen. Geben Sie anschließend eine neue, frei wählbare achtstellige Admin-PIN ein und bestätigen Sie diese erneut mit der OK-Taste. Wiederholen Sie den Vorgang nach der Aufforderung und bestätigen Sie erneut mit Drücken der OK-Taste. Sie haben die PIN jetzt geändert. Notieren Sie diese und bewahren Sie sie unter Verschluss auf.



ACHTUNG!
Beachten Sie unbedingt die Sicherheitshinweise im Abschnitt 5.2 »Admin-PIN Eingabe bei der ersten Inbetriebnahme« auf Seite 47 dieser Bedienungsanleitung!

### 7.3.2. Die Terminalselbstauskunft [Status \32]

Die Statusabfrage ist eine reine Anzeigefunktion. Diese Terminalselbstauskunft zeigt neben dem Status der Soft- und Hardware-Version, die aktive FW-Gruppe, den Terminalnamen, die MAC-Adresse und aktive Werte von Konfigurationsdatenparametern (z.B. Version der geladenen TSL des Vertrauensraum PU) des Gerätes an.
Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ③ und ②. Mit den Cursortasten ▲ und ▼ können Sie, mit der Softwareversion beginnend, Informationen zu Ihrem Gerät abrufen.

Folgende Informationen werden Ihnen angezeigt:

| Status: | Wert: |
|---|---|
| Firmware Version | 3.8.1 |
| Firmware Datum | 02.12.2021 |
| Firmware Gruppe | 00017:<V3.8.1> |
| Hardware-Version | 1.2.0 |
| Hersteller-ID | INGHC |
| Produktkürzel | ORGA6100 |
| Produktversion | 3.8.1:1.2.0 |
| Produkttype | KT |
| Produkttyp Version | 1.5.0 |
| eHealth Interface Version | 1.0.0 |
| Zusätzliche Terminalangaben (Auszug) | |
| Status: | Wert: |
| SICCT Terminal Name** | Default: ORGA6100-*<Seriennummer>* |
| Seriennummer | *<Seriennummer>* |
| MAC Adresse | 00:0D:F8:*<XX>*:*<YY>*:*<ZZ>* |
| Version TSL-PU*** | *< geladene Version der TSL PU a.b.c>* |
| Version TSL-RU*** | *< geladene Version der TSL RU d.e.f>* |
| Version TSL-TU*** | *< geladene Version der TSL RU d.e.f>* |
| Version TSL-LU*** | *< geladene Version der TSL LU g.h.i>* |
| terminal_type | ORGA 6141 online |
| ** Konfigurationsparameter - am Terminal veränderlich<br>*** Konfigurationsparameter - per Konfigurationsparameter-Update veränderlich | |

Tabelle 8: *Terminalselbstauskunft*

Wenn Sie die Informationen der Terminalselbstauskunft bequem auslesen und auf einem externen Gerät darstellen lassen wollen, drücken Sie die F1-Taste im Menü [**Status \32**], um einen QR-Code darstellen zu lassen und mit einem Smartphone abzuscannen. Der QR-Code beinhaltet die Inhalte, die im Abschnitt 7.3.7.2 »QR-Code: [Status (Geräteselbstauskunft) \372]« auf Seite 94 beschrieben werden.

### 7.3.3. Zurücksetzen des Terminals in den Auslieferungszustand [Werkseinstellung \33]

Es stehen Ihnen zwei Wege zur Auswahl, auf denen Sie das Terminal in den Auslieferungszustand mit Werkseinstellungen zurückversetzen können. Dabei gehen Konfigurationseinstellungen verloren, indem diese Parameter auf entsprechenden Werksauslieferungseinträge zurückgesetzt werden. Insbesondere die PIN Verwaltung wird zurückgesetzt! Vom Terminal ermittelte Betriebsdaten/Statistik bleiben bei einem Werksreset erhalten.



ACHTUNG!
Geben Sie unmittelbar nach dem erfolgreichen Werksreset eine neue Admin-PIN ein, um das Terminal vor unerlaubtem Zugriff zu schützen.

#### 7.3.3.1. Zurücksetzen des Terminals via Admin-PIN [via Admin-PIN \331]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ③③ und ①, geben Sie die Admin-PIN ein, wenn das Gerät noch verschlossen sein sollte und bestätigen Sie diese mit der OK-Taste. Bestätigen Sie die Sicherheitshinweise erneut mit OK. Das Gerät führt einen Neustart durch und der Werksauslieferungszustand ist wiederhergestellt.

#### 7.3.3.2. Zurücksetzen des Terminals via Reset-Code [via Reset-Code \332]

Sollten Sie Ihre Admin-PIN vergessen haben, können Sie mittels eines sicheren Challenge-Response-Verfahren über den Service des Herstellers Ingenico Healthcare (Reset Administrator) einen Freischaltcode bekommen, um anschließend eine neue Admin-PIN zu vergeben. Setzen Sie sich bitte hierzu mit der Service-Hotline von Ingenico Healthcare in Verbindung.



HINWEIS
Setzen Sie sich mit der Service-Hotline von Ingenico Healthcare in Verbindung, wenn Sie Ihre Admin-PIN vergessen haben. Ingenico Healthcare kann als sogenannter Reset Administrator das Terminal auch ohne Admin-PIN wieder in die Werkseinstellung zurückversetzen. Sie erhalten dort weitere Informationen darüber, wie Sie mittels eines Reset-Codes das Terminal in den Auslieferungszustand versetzen und eine neue Admin-PIN vergeben können.

### 7.3.4. Terminal-Funktionstests [Test \34]

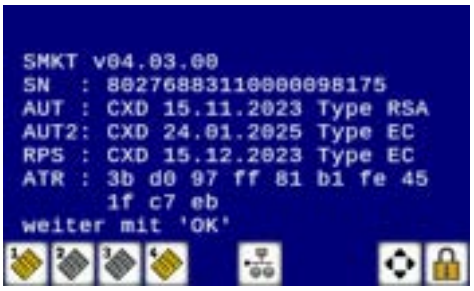



Abbildung 32: *Darstellung der Kartendetails einer gSMC-KT in Slot 4*

Mit dieser Funktion können Sie die Hardware Ihres Gerätes und die Funktionstüchtigkeit von Smartcards testen. Mit [**Gesamttest \341**] werden nacheinander alle durchführbaren Tests durchlaufen, mit dem [**Einzeltest \342**] können alle Tests einzeln aufgerufen werden. Für die Tests der Kontaktiereinheiten 1 und 2, im Test „Slot“ genannt, benötigen Sie jeweils eine im Format passende und funktionstüchtige eGK, HBA oder SMC-B, deren "Header" im Test ausgelesen werden kann. Für die Tests der Kontaktiereinheiten 3 und 4 benötigen Sie jeweils eine im Format passende und funktionstüchtige SMC-Karte, deren "Header" im Test ausgelesen werden kann. Wenn sich eine gSMC-KT im Slot 3 oder 4 befindet, werden folgende Informationen der Karte zusätzlich angezeigt:

- SMKT: Produkttypversion der gSMC-KT
- SN: Die Seriennummer (ICCSN) der Karte
- AUT: Verfallsdatum (CXD) vom EF.C.SMKT.AUT.XXXX Zertifikat
- AUT2: Verfallsdatum (CXD) vom EF.C.SMKT.AUT2.XXXX Zertifikat (falls vorhanden)
- RPS: Verfallsdatum (CXD) vom CV Zertifikat RemotePin EF.C.SMC.AUTD_RPS_CVC.E256
- ATR: Header der Karte

Der Header ist die erste Zeichenfolge, die auf der Karte gespeichert ist und benennt den Kartentyp. Die Zeichen werden im Hex-Code ausgegeben. Sollten Sie keine passende Karte bereit haben, können Sie den Test mit der STOP-Taste überspringen.

HINWEIS
Durch diesen Test ist es Ihnen möglich die Informationen einer gSMC-KT auch ohne vorheriges Pairing des Terminals mit einem Konnektor schnell und bequem auszulesen. Nutzen Sie diese Funktion auch für die Autentizitäts- und Integritätsprüfung der gSMC-KT (siehe Kapitel 5.6 »Authentizitäts- und Integritätsprüfung der gSMC-KT« auf Seite 50).

#### 7.3.4.1. Test: [Gesamttest \341]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ③ ④ ①, um alle verfügbaren Tests nacheinander durchzuführen. Jeder Test wird durch Drücken der OK-Taste abgeschlossen, um dann automatisch zum nächsten Test zu wechseln. Sollten Sie keine passende Karte für die Tests der Kontaktiereinheiten (Slots) bereit haben, können Sie diese Tests mit der STOP-Taste überspringen.

#### 7.3.4.2. Test: [Einzeltest \342]

Um eine bestimmte Funktion des Gerätes zu überprüfen, können Sie diese auch direkt anwählen. Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ③ ④ ② und die Ziffer für den gewünschten Test.

#### 7.3.4.2.1. Einzeltest: [Buzzer \3421]

Mit dieser Funktion testen Sie die Funktion des Signaltons. Der Test startet automatisch und wird nach kurzem Erklingen eines tiefen Tons automatisch beendet.

#### 7.3.4.2.2. Einzeltest: [Display \3422]

Mit dieser Funktion können Sie das Display auf Schäden überprüfen. Der Test startet automatisch mit einer Vollbildanzeige der Farbe Rot, durch Drücken der OK-Taste wechselt die Farbe anschließend zu Grün und Blau, bevor Sie mit der OK-Taste wieder ins Ausgangsmenü gelangen.

#### 7.3.4.2.3. Einzeltest: [Tasten \3423]

Mit diesem Test können Sie die Funktion aller Tasten überprüfen. Im Display werden symbolisch alle 20 Tasten des Tastenfelds dargestellt:

```
←→ ↑↓
1 2 3 X
4 5 6 ←
7 8 9 M
- 0 , O
```

Durch Drücken einer Taste beginnt das entsprechende Symbol im Display an zu blinken und wird gelb. Durch erneutes Drücken der Taste wird das Blinken beendet. Der Test wird durch Drücken der OK-Taste beendet.

#### 7.3.4.2.4. Einzeltest: [Slot 1 \3424]

Mit diesem Test können Sie die Funktion der Kontaktiereinheit 1 des oberen eGK-Kartenschlitzes testen. Wenn Sie dieses Menü anwählen, werden Sie aufgefordert, eine Karte in den oberen Kartenschlitz zu stecken. Sobald Sie eine lesbare eGK- oder HBA-Karte eingesteckt haben, wird eine Buchstabenfolge wie hier dargestellt ausgegeben:

```
ATR:
3b dd 97 ff 81 b1 fe 45
1f 03 00 64 04 05 08 03
73 96 21 d0 00 90 00 c8
```

#### 7.3.4.2.5. Einzeltest: [Slot 2 \3425]

Mit diesem Test können Sie die Funktion der Kontaktiereinheit 2 des HBA-Kartenschlitzes, der sich am rechten Gehäuserand des Gerätes befindet, testen.



HINWEIS
Bitte entnehmen Sie vor diesem Test zunächst den HBA aus dem Kartenschlitz, falls er sich in diesem Kartenschlitz befindet, und setzen ihn erst nach erfolgreichem Abschluss des Testes wieder ein!

Wenn Sie dieses Menü anwählen, werden Sie aufgefordert, eine Karte in den Kartenschlitz zu stecken. Sobald Sie eine lesbare eGK- oder HBA-Karte eingesteckt haben, wird eine Buchstabenfolge wie hier dargestellt ausgegeben:

```
ATR:
3b dd 97 ff 81 b1 fe 45
1f 03 00 64 04 05 08 03
73 96 21 d0 00 90 00 c8
```

### 7.3.4.2.6. Einzeltest: [Slot 3 \3426] und [Slot 4 \3427]

Mit diesem Test können Sie die Funktion der Kontaktiereinheit 3 bzw. 4 für die SMC-Karten testen. Wenn Sie dieses Menü anwählen, wird bei eingeschobener Karte eine Buchstabenfolge wie hier dargestellt ausgegeben:

```
ATR:
3b dd 97 ff 81 b1 fe 45
1f 03 00 64 04 05 08 03
73 96 21 d0 00 90 00 c8
```

Der Slot 3 ist der Kartenschlitz unten und Slot 4 der Kartenschlitz oben am linken Gehäuserand.

HINWEIS
Mit dem Einzeltest des Kontaktiereinheit 3 bzw. 4 können Sie prüfen, bis wann die Zertifikate auf der gSMC-KT noch gültig sind. Sobald eins der Zertifikate verfallen ist, kann das Terminal nicht mehr ordnungsgemäß Versichertenkarten, Heilberufsausweise und Institutionskarten auslesen (siehe Abschnitt 7.3.4 »Terminal-Funktionstests [Test \34]« auf Seite 86.

### 7.3.4.2.7. Einzeltest: [Integrität \3428]

Dieser Test dient zur Integritätsprüfung des Gerätes. Dabei führt das Gerät interne Berechnungen und Ergebniskontrollen zur Überprüfung der Sicherheitsfunktionen (u.a. Hash- und Kryptofunktionen, Known-Answer Tests) und des sicheren Betriebszustands durch.
Der Testdurchlauf startet unmittelbar nach dem Drücken der OK-Taste und der Eingabe des Admin-PIN mit der Meldung `... bitte warten ...` und endet mit einer zweizeiligen Statusanzeige.
Wenn das Gerät den Integritätstest bestanden hat, wird im Display folgende Information angezeigt:

```
Integrität : ok
Funktion   : ok
```

Die Anzeige des Status kann mit beliebiger Taste beendet werden oder schließt nach einigen Sekunden automatisch mit Ablauf des Menü Timeouts.
Wurde ein Fehler festgestellt, wird kein **ok** angezeigt. Nach einem Fehlerfall wird das Gerät mit dem nächsten Einschalten nicht mehr in den Betriebsmodus gehen. Wenden Sie sich in diesem Fall an die Service-Hotline von Ingenico Healthcare.

HINWEIS
Weitere Informationen zum Integritätstest entnehmen Sie dem Abschnitt 2.2.5 »Integritätsprüfung« auf Seite 27 dieser Bedienungsanleitung!

### 7.3.5. Der Kiosk-Modus [Kiosk-Modus \35]

Wenn das ORGA 6141 online in einem Kiosksystem zum Einsatz kommen soll, ist es von Vorteil, wenn der Anwender durch Drücken der MENU-Taste nicht mehr versehentlich oder absichtlich Statusabfragen vornehmen oder das Terminal ausschalten kann.
Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ③ und ⑤. Sie werden aufgefordert die Admin-PIN einzugeben. Anschließend können sie mit der Taste ⓪ den Kiosk-Modus aus- und mit der Taste ① einschalten. Bestätigen Sie Ihre Wahl mit Drücken der OK-Taste.
Im Kiosk-Modus sind die STOP, CLEAR und MENU-Tasten gesperrt. Sie gelangen in diesem Modus nur ins Menü, wenn Sie die MENU-Taste fünf Sekunden lang gedrückt halten. Nach Verlassen des Menüs bleibt der Kiosk-Modus weiter aktiv, bis Sie diese Einstellung wieder im Menü [**Kiosk-Modus \35**] deaktivieren.
Folgende Einschränkungen sind im Kiosk-Modus aktiviert:

### 7.3.6. Konfiguration via USB-Stick im- und exportieren

Das ORGA 6141 online mit der neusten Firmwareversion 3.8.1 bietet die Möglichkeit, eine Vielzahl von individuell konfigurierbaren Parametern mit Hilfe eines USB-Sticks zu im- und exportieren. Damit können z. B. VPN-Zugangsdaten in ein Terminal oder Konfigurationsdaten von einem Terminal in eine Exportdatei übertragen werden, um ggf. die Installation mehrerer Terminals im selben Netzwerk zu vereinfachen und zu beschleunigen.
Die Konfigurationsdaten werden als „Key-Value“-Paare zeilenweise in der Datei gespeichert. Als Trennzeichen wird ein Gleichheitszeichen verwenden.
Beispiel: **vpn_gateway_addr=ipsec-gw.ihcdev.de**
Von der Applikation wird die Konfigurationsdatei zeilenweise, mit max. 4KBytes pro Zeile eingelesen. Entspricht die gelesene Zeile nicht der oben beschriebenen Syntax, wird die Zeile verworfen. Hat der Wert des Parameters die Länge Null, wird der Wert entsprechend im Terminal gelöscht. Ist ein Parameter mehrfach in einer Datei enthalten, so wird er nur beim ersten Mal verarbeitet. Werte vom Typ ‚KONF‘ oder ‚CERT‘ müssen, unabhängig vom Inhalt, base64-kodiert sein.

Folgende Geräteparameter können im- bzw. exportiert werden:

| Parameter | Gruppe | Test | Beschreibung |
|---|---|---|---|
| admin_session | sicct | BOOL | Admin-Session aktiviert? Ja/Nein |
| device_name | sicct | ALPHANUM, 47 | Gerätenamen |
| dhcp_enabled | net | BOOL | DHCP oder statische IP-Konfiguration |
| domain_name_server | net | IP | DNS (statisch) |
| gateway_ip | net | IP | Gateway (statisch) |
| ip_addr | net | IP | Eigenen IP-Adresse (statisch) |
| netmask | net | IP | Netzmaske (statisch) |
| ntp_addr | net | IP | NTP Server |
| timezone | sicct | ALPHANUM, 32 | Zeitzone des Standards |
| ntp_timeout | net | NUM_NN | Timeout für NTP-Server |
| welcome_message | sicct | ALPHANUM, 32 | Text im Ruhebildschirm |
| ipsec_cacert | ipsec | CERT | X.509 CA-Zertifikate für VPN |
| ipsec_conf | ipsec | KONF | optional Konfigurationdatei für VPN |
| vpn_account_user | ipsec | ALPHANUM, 47 | Benutzerkennung |
| vpn_gateway_addr | ipsec | IP / URL | VPN-Gateway |
| import_filename | ipsec | ALPHANUM, 64 | Optional für ipsec_cacert |

Tabelle 9: *Unterstützte Parameter der Im- und Export-Dateien*

Der Parameter **`ipsec_cacerts`** hat eine Besonderheit. Es kann nur das X.509 CA-Zertifikate für den VPN-Zugang importiert werden. Beim Export wird nicht das entsprechende X.509 CA-Zertifikate des VPN-Zugangs herausgegeben. Stattdessen werden der Herausgeber, das Verfalldatum und der Fingerprint des Zertifikats, durch Komma getrennt, als Wert geschrieben. Sind, wie beim einen RSA-Schlüssel, diese Angaben nicht vorhanden, wird ein SHA2-Hash über die im Terminal gespeicherte Dateien gebildet und als Wert verwendet.

| Test | Beschreibung |
|---|---|
| ALPHA_NUM, max.Länge | Der Wert des Parameters darf nur alphanumerische Zeichen enthalten und muss kleiner gleich der angegebenen maximalen Länge sein. |
| BOOL | Der Wert des Parameters darf nur den Zeichenketten „True“ bzw. „False“ entsprechen. |
| IP | Der Wert des Parameters muss einer gültigen IP entsprechen. 4 Oktetts mit max. 3 Ziffer durch Punkte getrennt.<br>Jedes Oktett muss im Zahlenbereich 0-255 liegen. |
| IP / URL | Der Wert des Parameters kann einer gültigen IP entsprechen, siehe ‚IP‘.<br>Enthält der Wert zudem Buchstaben wird von einer URL ausgegangen. Dann muss mindestens noch ein Punkt als Domänen-Trennung enthalten sein. |
| CERT | Der Wert des Parameters muss base64 kodiert und kleiner 4080 Bytes sein. Zudem muss er eine gültige X.509 Struktur enthalten. Mittels „import_filename=xy“ vor dem Eintrag in der Konfigurationsdatei kann der Dateiname vorgegeben werden. Andernfalls wird das Zertifikat unter einem zufälligen Dateinamen abgespeichert. |
| KONF | Der Wert des Parameters muss base64 kodiert und kleiner 4080 Bytes sein. Die Konfiguration ist gemäß swanctl.conf* zu erstellen. |
| NUM_NN | Der Wert des Parameters darf nur 2-stellig, numerisch (0-99) sein. |

* Referenz: https://wiki.strongswan.org/projects/strongswan/wiki/Swanctlconf

Tabelle 10: *Tests beim Import einer Konfigurationsdatei*

Die Konfigurationsdaten werden als „Key-Value“-Paare zeilenweise in der Datei gespeichert. Als Trennzeichen wird ein Gleichheitszeichen verwenden.

Beispiel: **`vpn_gateway_addr=ipsec-gw.ihcdev.de`**

Von der Applikation wird die Konfigurationsdatei zeilenweise, mit max. 4KBytes pro Zeile eingelesen. Entspricht die gelesene Zeile nicht der oben beschriebenen Syntax, wird die Zeile verworfen. Hat der Wert des Parameters die Länge Null, wird der Wert entsprechend im Terminal gelöscht. Ist ein Parameter mehrfach in einer Datei enthalten, so wird er nur beim ersten Mal verarbeitet. Werte vom Typ ‚KONF‘ oder ‚CERT‘ müssen, unabhängig vom Inhalt, base64-kodiert sein. Entnehmen Sie der Tabelle 9 und Tabelle 10 die unterstützten Parameter der Im- und Exportdateien sowie der Tests, die beim Import der Parameter einer Konfigurationsdatei durchgeführt werden.

#### 7.3.6.1. Daten-Import: [Import von einem USB-Stick \361]

Drücken Sie die Ziffern ③ ⑧ [**`Admin PIN Eingabe`**] ①, wenn Sie Terminal-Einstellungen von einem USB-Stick im FAT32 Format importieren wollen. Bestätigen Sie Ihre Auswahl mit der OK-Taste. Sie werden aufgefordert einen USB-Stick zu stecken. Stecken Sie einen USB-Stick in die USB-A Buchse auf der Unterseite des Terminals. Anschließend sucht das Terminal nach einer Datei mit der Endung **`_import.cfg`** im Stammverzeichnis des USB-Sticks. Dabei ist zu beachten, dass sich für den erfolgreichen Import immer nur eine Datei mit der Endung **`_import.cfg`** im Stammverzeichnis des USB-Sticks befinden darf.

Ist eine passende Datei mit der Endung **`_import.cfg`** auf dem USB-Stick vorhanden, wird der Dateiname im Display angezeigt und Sie werden aufgefordert den Import-Vorgang mit Drücken der OK-Taste zu starten. Anschießend beginnt der Import der Konfigurationsdaten und der erfolgreiche Import wird mit dem Hinweis

**`Import abgeschlossen! Bitte USB-Stick entfernen`** bestätigt. Sobald Sie den USB-Stick aus dem Terminal gezogen führt das Gerät einen Neustart durch.

#### 7.3.6.2. Daten-Export: [Export auf einem USB-Stick \362]

Drücken Sie die Ziffern ③ ⑥ [**Admin PIN Eingabe**] ②, um die Terminal-Einstellungen auf einen USB-Stick im FAT32 Format zu exportieren. Bestätigen Sie Ihre Auswahl mit der OK-Taste.
Sie werden aufgefordert einen USB-Stick zu stecken. Stecken Sie einen USB-Stick in die USB-A Buchse auf der Unterseite des Terminals. Anschließend wird der USB-Stick erkannt und eine Datei mit dem Dateinamen **<Gerätename>_export.cfg** auf den USB-Stick geschrieben. Der erfolgreiche Export der Terminal-Parameter wird durch die Anzeige
**Exporterfolgreich! Bitte USB-Stick entfernen** bestätigt.
Den Textstring **<Gerätename>** richtet sich nach dem in der Werkseinstellung festgelegtem Namen, der sich auch dem Textstring **„orga6100-"** und der Seriennummer des Terminals zusammensetzt. Wenn Sie den Terminalnamen im Menü [Gerätename \211] geändert haben (siehe Abschnitt 7.2.1.1 »LAN Parameter: [Gerätename \211]« auf Seite 60), wird dieser Gerätename im Textstring **<Gerätename>** der Exportdatei verwendet.
Mit Hilfe eines einfachen Text-Editors (z. B. Notepad) können sie die Datei öffnen und die Parameter ggf. verändern, um so neue Import-Dateien für weitere Terminals zu erzeugen. Speichern Sie Ihre Änderungen unter einem Dateinamen der auf **_import.cfg** endet, wenn Sie die Datei als Import-Datei für weitere Terminals verwenden wollen.

HINWEIS
Beim Export wird nicht das entsprechende X.509 CA-Zertifikate des VPN-Zugangs (Parameter **ipsec_cacerts**) exportiert. Wenn Sie diesen Parameter für das Erzeugen einer Importdatei benötigen, müssen Sie den Wert in der Importdatei an entsprechender Stelle ergänzen.

### 7.3.7. Terminal Konfigurationen und Betriebszustände via QR-Codes auslesen

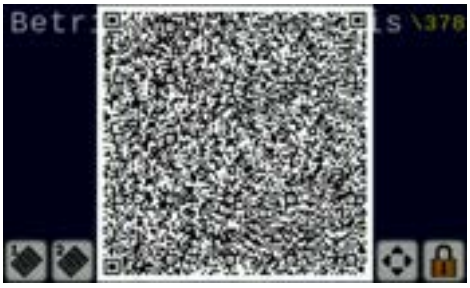


Abbildung 33: *QR-Code zum Auslesen von Terminal Konfigurationen und Betriebszuständen*

Das ORGA 6141 online kann mit Hilfe seines großen Farbdisplays 2D-Matrixcodes anzeigen. Diese können vom Konnektor oder von der SAK gesendete DataMatrix- oder QR-Codes sein, die auf dem Terminal dargestellt werden.
Die vielfältigen, individuellen Konfigurationsparameter und Betriebszustände des Terminals, lassen sich ebenfalls mit Hilfe von QR-Codes mit dynamischen Code-Inhalten schnell und bequem auf mobilen Geräten mit Kamera- und QR-Lesefunktion übertragen und darstellen. Dies erleichtert dem Administrator die Dokumentation der Installation und die Fehlersuche bei Funktionsstörungen. Bei Auswahl der folgenden Menüs wird ein QR-Code auf dem Display des Terminals dargestellt, der eine URL mit bestimmten Terminalinformationen enthält, die auf einem Webserver dargestellt oder verarbeitet werden können. Über die Nutzungsmöglichkeiten erfahren Sie mehr auf der Homepage von Ingenico Healthcare **www.ingenico.com/healthcare**.
Für die Erstellung der dynamischen QR-Codes, werden verschiedene Parameter der Geräte-Konfiguration und Betriebszustände ermittelt, zusammengefasst und eine www.w3.org konforme Informationsübergabe in der Syntax-Form „**Index=**" und „**Wert**" gewählt, um einen

möglichst hohe Datendichte zu erzielen. Und-Zeichen (&) dienen als Separatoren zwischen den einzelnen Werteangaben.
Beispielsweise wird bei der Ausgabe des QR-Codes im Menü [**Status (Geräteselbstauskunft \372**] folgender Code generiert:

**http://<Server-IP-Adresse>/orga-deviceinfo.php?index01=overview_sig_term&index02=01410000005AAC&index03=ORGA%206141%20Online&index04=1.2.1&index05=3.8.0&index06=2019-11-06&index07=13&index08=3.8.0%203.7.5%203.7.4&index09=1.2.0&index10=00%3A0D%3AF8%3A04%3A0C%3AB3&index11=ORGA6100-01410000005AAC&index12=1.18.0&index13=0.1.0**

In diesem Beispiel sind somit folgende Informationen beinhaltet:

| URL: | **http://<Server-IP-Adresse>/orga-deviceinfo.php** | |
|---|---|---|
| Index: | Bedeutung: | Wert: |
| Index01 | Bezeichnung der Zusammenfassung | overview_sig_term<br>Status (Terminalselbstauskunft) |
| Index02 | Seriennummer | 01410000005AAC |
| Index03 | Produkt Name | ORGA 6141 Online |
| Index04 | Produkt Version | 1.2.1 |
| Index05 | Firmware Version | 3.8.0 |
| Index06 | Firmware Datum | 2019-11-06 |
| Index07 | Firmware Gruppen-ID | 13 |
| Index08 | Firmware Gruppe | 3.8.0 3.7.5 3.7.4 |
| Index09 | Hardware Version | 1.2.0 |
| Index10 | MAC Adresse | 00:0D:F8:04:0C:B3 |
| Index11 | SICCT Terminal Name | ORGA6100-01410000005AAC |
| Index12 | Geladene Version der TSL-LU | 1.18.0 |
| Index13 | Geladene Version der TSL-SU | 0.1.0 |

Tabelle 11: *Beispiel der Syntax eines dynamischen QR-Code Wertes*

HINWEIS
Die in diesem Beispiel verwendeten Indizes entsprechen nicht denen der tatsächlichen Werte-Indizes. Die Tatsächlichen Indizes sind in den Tabellen in den folgenden Abschnitten tabellarisch aufgeführt.

#### 7.3.7.1. QR-Code: [Info/Service \371]

Mit dem Menüpunkt [**Info/Service \371**] rufen Sie einen QR-Code auf, der die URL der ORGA 6141 online Produktseite auf der Ingenico Healthcare Homepage enthält. Auf dieser Seite finden Sie alle wichtigen Informationen zum Terminal wie z. B. aktuelle Updates und Bedienungsanleitungen zum Gerät.

#### 7.3.7.2. QR-Code: [Status (Geräteselbstauskunft) \372]

Nach Aufruf des Menüpunkts [**Status (Geräteselbstauskunft) \372**] erscheint ein QR-Code, der Ihnen tabellarisch alle Informationen des Menüpunktes [**Status \32**] auf Ihrem Mobilgerät anzeigt.

| Index: | Bedeutung: | Beispiel/Beschreibung |
|---|---|---|
| grp | Bezeichnung der Zusammenfassung | overview_sig_term<br>Status (Terminalselbstauskunft) |
| serial | Seriennummer | 01410000005AAC |
| prod | Produkt Name | ORGA 6141 online |
| prodver | Produkt Version | 1.2.1 |
| fw | Firmware Version | 3.8.0 |
| fwdate | Firmware Datum | 2019-11-06 |
| fwgrpid | Firmware Gruppen-ID | 13 |
| fwgrp | Firmware Gruppe | 3.8.0 3.7.5 3.7.4 |
| hw | Hardware Version | 1.2.0 |
| mac | MAC Adresse | 00:0D:F8:04:0C:B3 |
| name | SICCT Terminal Name | ORGA6100-01410000005AAC |
| pu | Geladene Version der TSL-PU | 1.18.0 |
| ru | Geladene Version der TSL-RU | 0.1.0 |
| tu | Geladene Version der TSL-TU | 1.7.0 |
| lu | Geladene Version der TSL-LU | 1.18.0 |
| su | Geladene Version der TSL-SU | 1.0.0 |

Tabelle 12: *URL-Informationen des QR-Codes: [Status (Geräteselbstauskunft) \372]*

#### 7.3.7.3. QR-Code: [F1/F2 Tasten (Netzwerkstatus) \373]

Nach Aufruf des Menüpunkts [**F1/F2 Tastenstatus \373**] erscheint ein QR-Code, der alle Informationen beinhaltet, die sie über die im Abschnitt 1.4 »Funktionen der verschiedenen Tasten des Gerätes« auf Seite 15 beschriebenen Tastenkombinationen abrufen können:

| Index: | Bedeutung: | Beispiel/Beschreibung |
|---|---|---|
| grp | Bezeichnung der Zusammenfassung | status_fkeys<br>F1/F2 Tasten (Netzwerkstatus) |
| serial | Seriennummer | 01410000005AAC |
| mac | MAC Adresse | 00%3A0D%3AF8%3A04%3A0C%3AB3 |
| tcp | TCP Port | 4742 |
| udp | UDP Port | 4742 |
| name | SICCT Terminal Name | ORGA6100-01410000005AAC |
| conn | TLS Verbindungsstatus | TLS closed |
| session | SICCT Session Verbindungsstatus | close |
| sicctcmd | Status SICCT Kommando Interpreter | close |
| dhcpstat | DHCP Server | fail |
| vpnstat | VPN Status | VPN isn't active |
| pairblkno | Aktiver Pairing Block | Zum Auslesen und Darstellen dieser Parameter ist ein bestehendes Pairing und eine aktive TLS Verbindung zwischen Terminal und Konnektor erforderlich. |
| pairkeyno | Inhalt des Public key | |
| apincnt | Admin PIN Error-Counter | |
| apinlckt | Admin PIN aktuelle Sperrzeit | |
| spincnt | Session PIN Error-Counter | |
| spinlckt | Session PIN aktuelle Sperrzeit | |

Tabelle 13: *URL-Informationen des QR-Codes: [F1/F2 Tasten (Netzwerkstatus) \373]*

### 7.3.7.4. QR-Code: [LAN-Parameter \374]

Der QR-Code im Menü [**LAN-Parameter \374**] beinhaltet eine URL mit den Informationen zu folgenden LAN-Parametern des Terminals:

| Index: | Bedeutung: | Beispiel/Beschreibung |
|---|---|---|
| grp | Bezeichnung der Zusammenfassung | net |
| serial | Seriennummer | 01410000005AAC |
| name | SICCT-Terminal Name | ORGA6100-01410000005AAC |
| dhcp | DHCP | false |
| ip | IP-Adresse | 192.168.221.129 |
| ipvpn | IP-Adresse VPN | 0.0.0.0 |
| ipmask | Subnet Mask | 255.255.255.0 |
| ipgate | Gateway | 192.168.221.1 |
| dns | DNS | 0.0.0.0 |
| ucp / udp | TCP-Port / UDP-Port | 4742 / 4742 |
| vpn<br>vpngate<br>vpnuser<br>vpnstat | VPN-Tunnel<br>VPN-Gateway Adr.<br>Benutzername der Zugangsdaten<br>VPN Status | false<br>ipsec-gw.de<br>ORGA6141-DEMO<br>vpn isn't active |
| ntp<br>ipntp<br>tz | NTP Client<br>NTP Server<br>Timezone | true<br>192.168.221.1<br>MEZ-1MEZ-2,M3.5.0,M10.5.0 |

Tabelle 14: *URL-Informationen des QR-Codes: [LAN-Parameter \374]*

### 7.3.7.5. QR-Code: [SICCT-Parameter \375]

Der QR-Code im Menü [**SICCT-Parameter \375**] beinhaltet eine URL mit den Informationen zu folgenden SICCT-Parametern des Terminals:

| Index: | Bedeutung: | Beispiel/Beschreibung |
|---|---|---|
| grp | Bezeichnung der Zusammenfassung | sicct_connected<br>SICCT-Parameter |
| serial | Seriennummer | 01410000005AAC |
| waitka | Keep Alive Timeout | 120 |
| itrvlka | Keep Alive Intervall | 10 |
| waitbr | Block read Timeout | 5 |
| waitmr | Message read Timeout | 5 |
| maxperr | Max. Protokoll Fehler | 5 |
| waitacpt | SSL accept Timeout | 20 |
| tls | TLS-Version | 12 |
| ca | TSL-Liste | pu |
| announce | Announcement Interval | 5 |
| sicctstat | Set Status (Ein/Aus) | true |
| sicctdl | Download (Ein/Aus) | true |
| sicctadm | SICCT Admin Session (Ein/Aus) | true |

Tabelle 15: *URL-Informationen des QR-Codes: [SICCT-Parameter \375]*

### 7.3.7.6. QR-Code: [Update Parameter \376]

Der QR-Code im Menü [**Update Parameter \376**] beinhaltet eine URL mit den Informationen zu folgenden SICCT-Parametern des Terminals:

| Index: | Bedeutung: | Beispiel/Beschreibung |
|---|---|---|
| grp | Bezeichnung der Zusammenfassung | update |
| serial | Seriennummer | 01410000005AAC |
| dfu | Dateiname | mct6kp308.dfu (Werkseinstellung) |
| tftp | TFTP Server IP-Adresse | 192.168.1.2 (Werkseinstellung) |
| tftppoll | Poll-Status (Ein/Aus) | false |
| tftpwin | Poll-Window | 2 |
| updid | Update ID | ORGA6141_FW_V3_8_0_20191111 |

Tabelle 16: *URL-Informationen des QR-Codes: [Update Parameter \376]*

### 7.3.7.7. QR-Code: [Service/Einstellungen \377]

Der QR-Code im Menü [**Service/Einstellungen \377**] beinhaltet eine URL mit den Informationen zu folgenden SICCT-Parametern des Terminals:

| Index: | Bedeutung: | Beispiel/Beschreibung |
|---|---|---|
| grp | Bezeichnung der Zusammenfassung | Operational Service/Einstellungen |
| serial | Seriennummer | 01410000005AAC |
| kiosk | Kiosk-Modus (Ein/Aus) | false |
| s1 | Slot 1 Icon-Status | 2 |
| c1 | Slot 1 Kartentyp | 0 |
| s2 | Slot 2 Icon-Status | 2 |
| c2 | Slot 2 Kartentyp | 0 |
| s3 | Slot 3 Icon-Status | 2 |
| c3 | Slot 3 Kartentyp | 0 |
| s4 | Slot 4 Icon-Status | 1 |
| c4 | Slot 4 Kartentyp | 1 |
| ssmkt | Slot der gSMC-KT | 4 |
| smktsn | ICCSN der gSMC-KT | 80276003550000026497 |
| smktv | Version der gSMC-KT | v04.03.00 |
| autced | Aktivierungsdatum (CED) vom EF.C.SMKT.AUT.XXXX Zertifikat | 11.12.2017 |
| autcxd | Verfallsdatum (CXD) vom EF.C.SMKT.AUT.XXXX Zertifikat | 10.12.2022 |
| autt | Type von EF.C.SMKT.AUT.XXXX | 6 |
| aut2ced | Aktivierungsdatum (CED) vom EF.C.SMKT.AUT2.XXXX Zertifikat | - |
| aut2cxd | Verfallsdatum (CXD) vom EF.C.SMKT.AUT2.XXXX Zertifikat | - |
| aut2t | Type von EF.C.SMKT.AUT2.XXXX | - |

Tabelle 17: *URL-Informationen des QR-Codes: [Service/Einstellungen \377]*

### 7.3.7.8. QR-Code: [Betriebsdaten/Statistik \378]

Das ORGA 6141 online protokoliert im Laufe seiner Betriebszeit einige Betriebsdaten, die Ihnen wichtige Hinweise zum Benutzerverhalten und die quantitative Nutzung einzelner Funktionen des Terminals auflistet.
Der QR-Code im Menü [**Betriebsdaten/Statistik \378**] beinhaltet eine URL mit den Informationen zu folgenden SICCT-Parametern des Terminals:

| Index: | Bedeutung: | Wert: |
|---|---|---|
| grp | Bezeichnung der Zusammenfassung | Statistics Betriebsdaten/Statistik |
| serial | Seriennummer | 01410000005AAC |
| age | Betriebsstunden gesamt | 973h05m |
| uptime | Betriebsstunden seit Neustart | 0h60m47s |
| agefw | Betriebsstunden seit FW-Update | 973h08m |
| bt | Neustarts (Gesamtanzahl) | 165 |

| Index: | Bedeutung: | Wert: |
|---|---|---|
| btcld | Kaltstart (Spannung aus/ein) | 124 |
| btwarm | Warmstarts (Gesamtanzahl) | 41 |
| btupd | Warmstarts seit FW-Update | 0 |
| btadm | Warmstarts durch Menü initiiert | 0 |
| btdog | Warmstarts durch Watchdog | 0 |
| sicctstart | Anzahl Starts der SICCT-Applikation | 153 |
| discnt | Verbindungsabbrüche durch Terminal Gesamtanzahl | 3 |
| discntbt | Verbindungsabbrüche durch Terminal seit Neustart | 0 |
| cldiscnt | Verbindungsabbrüche durch Konnektor Gesamtanzahl | 5 |
| cldiscntbt | Verbindungsabbrüche durch Konnektor seit Neustart | 0 |
| apinok | Admin-PIN Anzahl erfolgreicher Eingaben | 12 |
| apinerr | Admin-PIN Anzahl falscher Eingaben | 1 |
| apinlck | Admin-PIN Anzahl Zeitsperren durch Falscheingabe | 0 |
| apincnt | Admin PIN - temporärer Fehlerzähler | 0 |
| apinlckt | Admin PIN - temporäre Rest-Sperrzeit in Sekunden | 0 |
| spinok | Session-PIN Anzahl erfolgreicher Eingaben | 0 |
| spinerr | Session-PIN Anzahl falscher Eingaben | 0 |
| spinlck | Session-PIN Anzahl Zeitsperren durch Falscheingabe | 0 |
| spincnt | Session PIN - temporärer Fehlerzähler | 0 |
| spinlckt | Session PIN - temporäre Rest-Sperrzeit in Sekunden | 0 |
| s1ins | Anzahl Steckzyklen Slot 1 | 5923 |
| s2ins | Anzahl Steckzyklen Slot 2 | 10 |
| s3ins | Anzahl Steckzyklen Slot 3 | 0 |
| s4ins | Anzahl Steckzyklen Slot 4 | 2 |
| s1act | Slot 1 Anzahl erfolgreicher Kartenaktivierungen | 5920 |
| s1err | Slot 1 Anzahl unlesbarer Karten | 3 |
| s1mem | Slot 1 Anzahl Memorykarten | 583 |
| s1proc | Slot 1 Anzahl Prozessorkarten | 5337 |
| s2act | Slot 2 Anzahl erfolgreicher Kartenaktivierungen | 10 |
| s2err | Slot 2 Anzahl unlesbarer Karten | 0 |
| s2mem | Slot 2 Anzahl Memorykarten | 0 |
| s2proc | Slot 2 Anzahl Prozessorkarten | 10 |
| s3act | Slot 3 Anzahl erfolgreicher Kartenaktivierungen | 0 |
| S3err | Slot 3 Anzahl Prozessorkarten | 0 |
| S3mem | Slot 3 Anzahl Memorykarten | 0 |
| s3proc | Slot 3 Anzahl Prozessorkarten | 0 |
| s4act | Slot 4 Anzahl erfolgreicher Kartenaktivierungen | 2 |
| s4err | Slot 4 Anzahl unlesbarer Karten | 0 |
| s4mem | Slot 4 Anzahl Memorykarten | 0 |
| s4proc | Slot 4 Anzahl Prozessorkarten | 2 |

| Index: | Bedeutung: | Wert: |
|---|---|---|
| s1perr | Slot 1 Protokollfehler Gesamtzahl | 0 |
| s1perrbt | Slot 1 Protokollfehler seit Neustart | 0 |
| s2perr | Slot 2 Protokollfehler Gesamtzahl | 0 |
| s2perrbt | Slot 2 Protokollfehler seit Neustart | 0 |
| s3perr | Slot 3 Protokollfehler Gesamtzahl | 0 |
| s3perrbt | Slot 3 Protokollfehler seit Neustart | 0 |
| s4perr | Slot 4 Protokollfehler Gesamtzahl | 0 |
| s4perrbt | Slot 4 Protokollfehler seit Neustart | 0 |
| vpnup | Gesamtanzahl der VPN Verbindungsaufbauten | 0 |
| vpnupbt | Seit Neustart, Anzahl der VPN Verb. Aufbauten | 0 |
| vpndn | Gesamtanzahl der VPN-Verbindungsabbauten | 0 |
| vpndnbt | Seit Neustart, Anzahl der VPN-Verbindungsabbauten | 0 |
| vpnrst | Gesamtanzahl VPN-Verb. Re-Trigger | 0 |
| vpnrstbt | Seit Neustart, Anzahl VPN-Verb. Re-Trigger | 0 |

Tabelle 18: *URL-Informationen des QR-Codes: [Betriebsdaten/Statistik \378]*

# ANHANG:

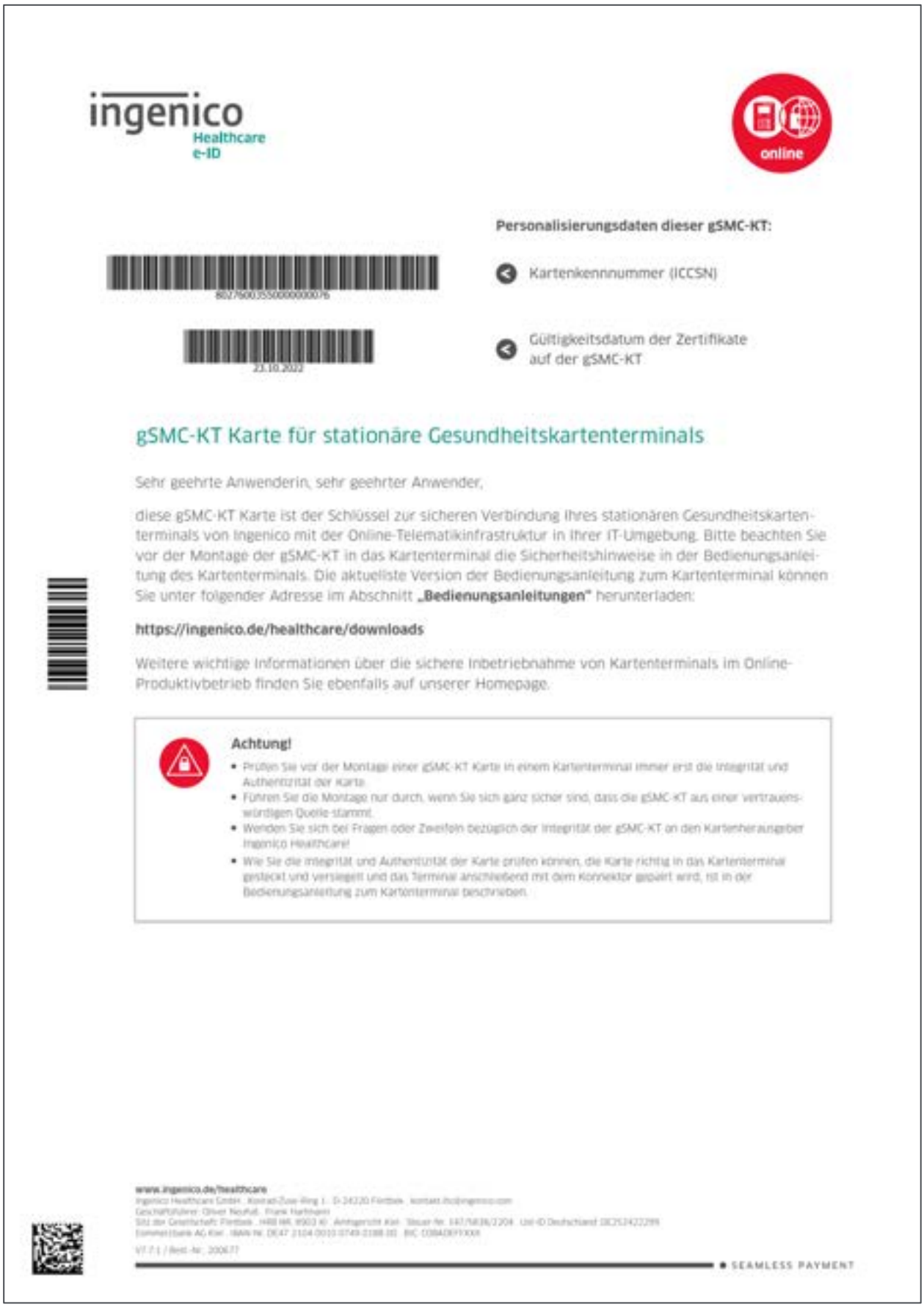
## 1. Technische Daten

| | |
|---|---|
| Spannungsversorgung: | Über USB: 500mA<br>Netzteil: 1.000 mA |
| Display | Farbdisplay mit 400x240 Pixel |
| Tastatur | Tastenmatrix 16 + 4 Tasten |
| Kartenspannung | alle Kontaktiereinheiten: A, B, C<br>A = 5V; B = 3V; C = 1,8V |
| Schnittstelle zum PC | LAN 10/100 Mb |
| Speicherausbau | 128 MB Flash / 64 MB RAM |
| Chipkartenkontaktiereinheiten | 2 Stück (Full-size PUSH-PULL ID-1)<br>2 Stück (SAM PUSH-PUSH ID-000) |
| Temperaturbereich:<br>Betriebsumgebung<br>Transport und Lagerung | <br>+5°C bis +40°C<br>-15°C bis +60°C (Nicht kondensierend) |
| Abmessungen (L x B x H) | 200 x 120 x 85 mm |
| Gewicht ohne Optionen | ca. 580 g |

Tabelle 19: *Technische Daten*

Dem Fortschritt dienende Änderungen am Design und den technischen Daten vorbehalten.

## 2. Musteranschreiben einer gSMC-KT



ingenico
Healthcare
e-ID

online

**Personalisierungsdaten dieser gSMC-KT:**

Kartenkennnummer (ICCSN)

Gültigkeitsdatum der Zertifikate auf der gSMC-KT

### gSMC-KT Karte für stationäre Gesundheitskartenterminals

Sehr geehrte Anwenderin, sehr geehrter Anwender,

diese gSMC-KT Karte ist der Schlüssel zur sicheren Verbindung Ihres stationären Gesundheitskartenterminals von Ingenico mit der Online-Telematikinfrastruktur in Ihrer IT-Umgebung. Bitte beachten Sie vor der Montage der gSMC-KT in das Kartenterminal die Sicherheitshinweise in der Bedienungsanleitung des Kartenterminals. Die aktuellste Version der Bedienungsanleitung zum Kartenterminal können Sie unter folgender Adresse im Abschnitt **„Bedienungsanleitungen"** herunterladen:

**https://ingenico.de/healthcare/downloads**

Weitere wichtige Informationen über die sichere Inbetriebnahme von Kartenterminals im Online-Produktivbetrieb finden Sie ebenfalls auf unserer Homepage.

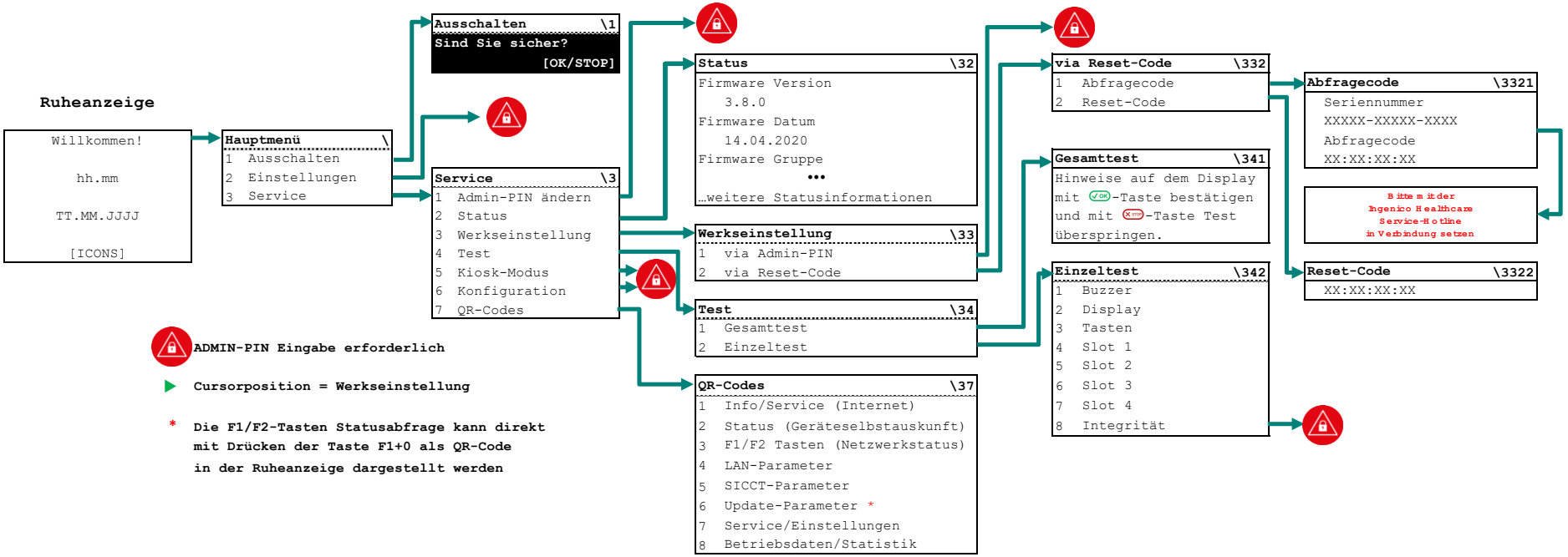
**Achtung!**

- Prüfen Sie vor der Montage einer gSMC-KT Karte in einem Kartenterminal immer erst die Integrität und Authentizität der Karte.
- Führen Sie die Montage nur durch, wenn Sie sich ganz sicher sind, dass die gSMC-KT aus einer vertrauenswürdigen Quelle stammt.
- Wenden Sie sich bei Fragen oder Zweifeln bezüglich der Integrität der gSMC-KT an den Kartenherausgeber Ingenico Healthcare!
- Wie Sie die Integrität und Authentizität der Karte prüfen können, die Karte richtig in das Kartenterminal gesteckt und versiegelt und das Terminal anschließend mit dem Konnektor gepairt wird, ist in der Bedienungsanleitung zum Kartenterminal beschrieben.

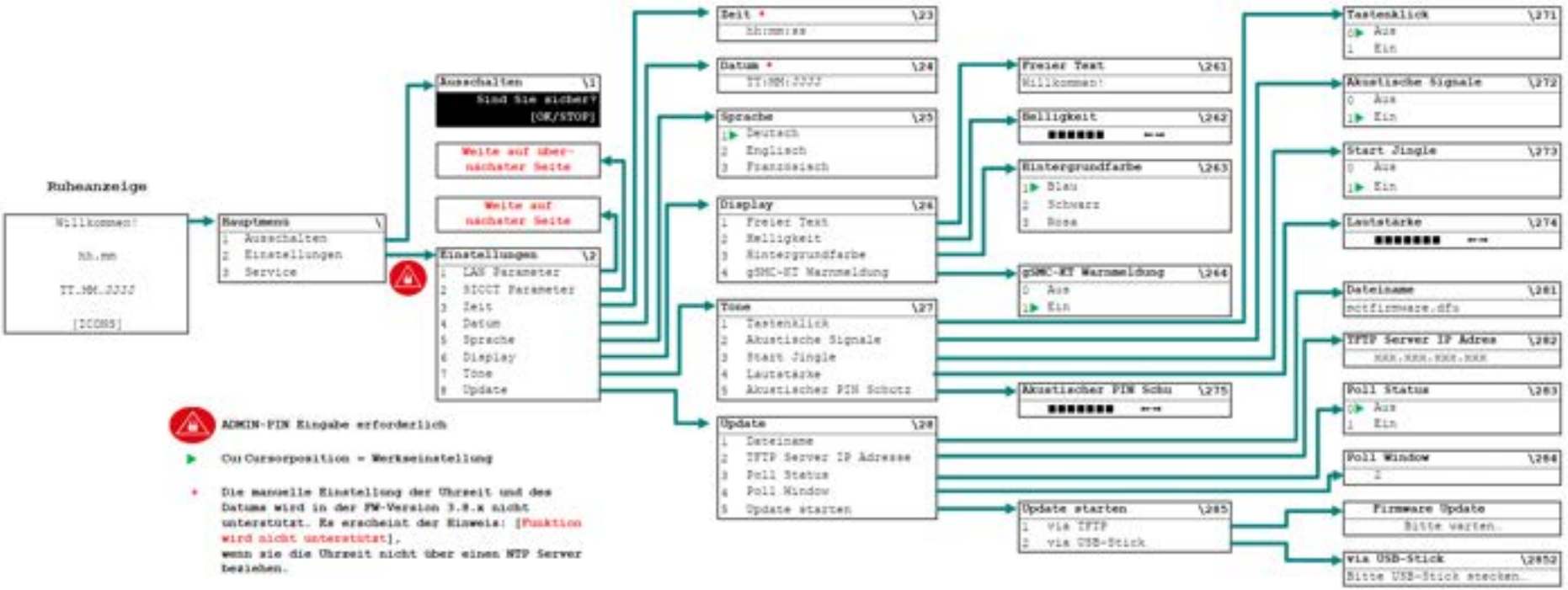
www.ingenico.de/healthcare

SEAMLESS PAYMENT

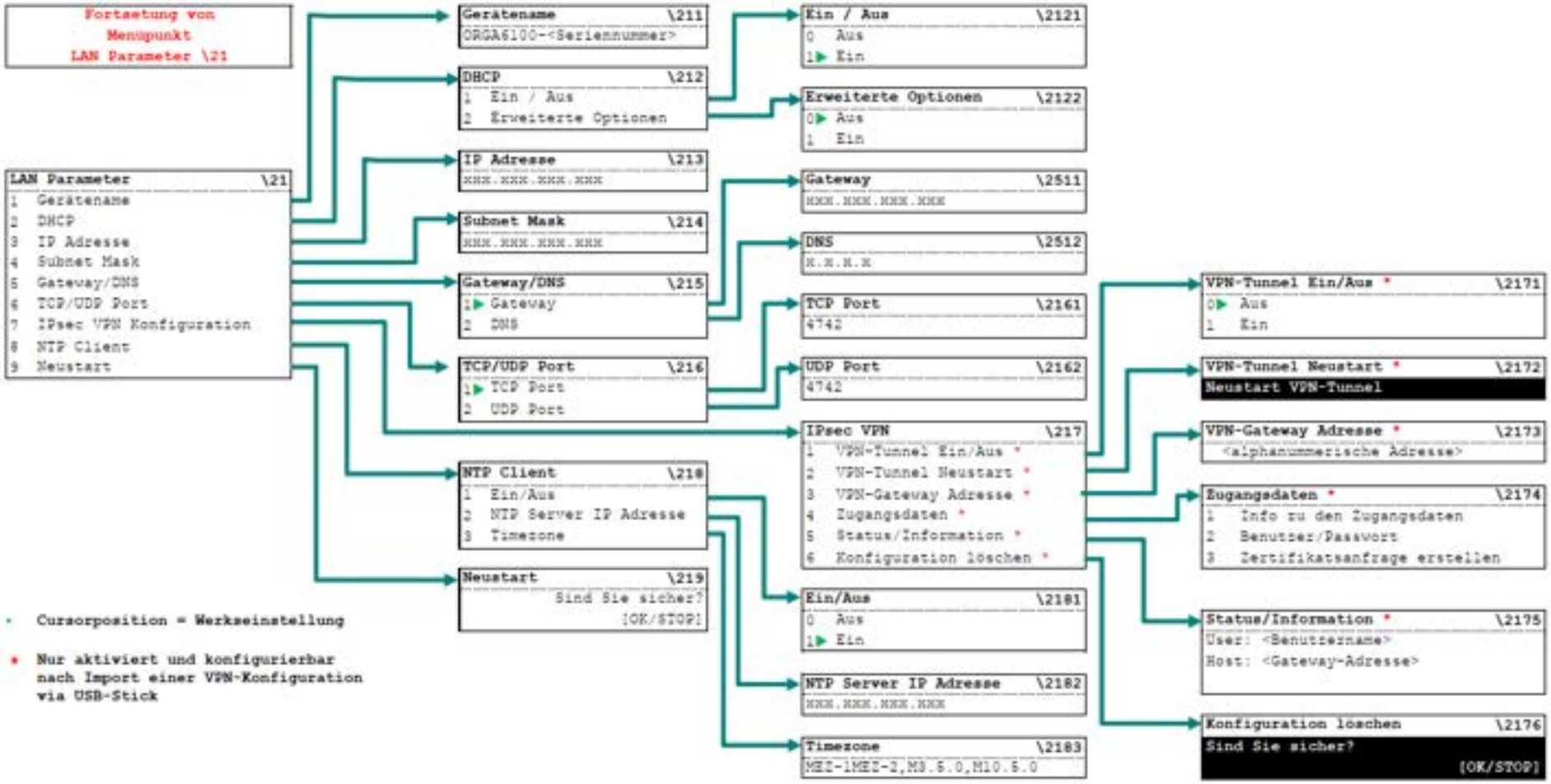
# 3. Menüstruktur für den Anwender



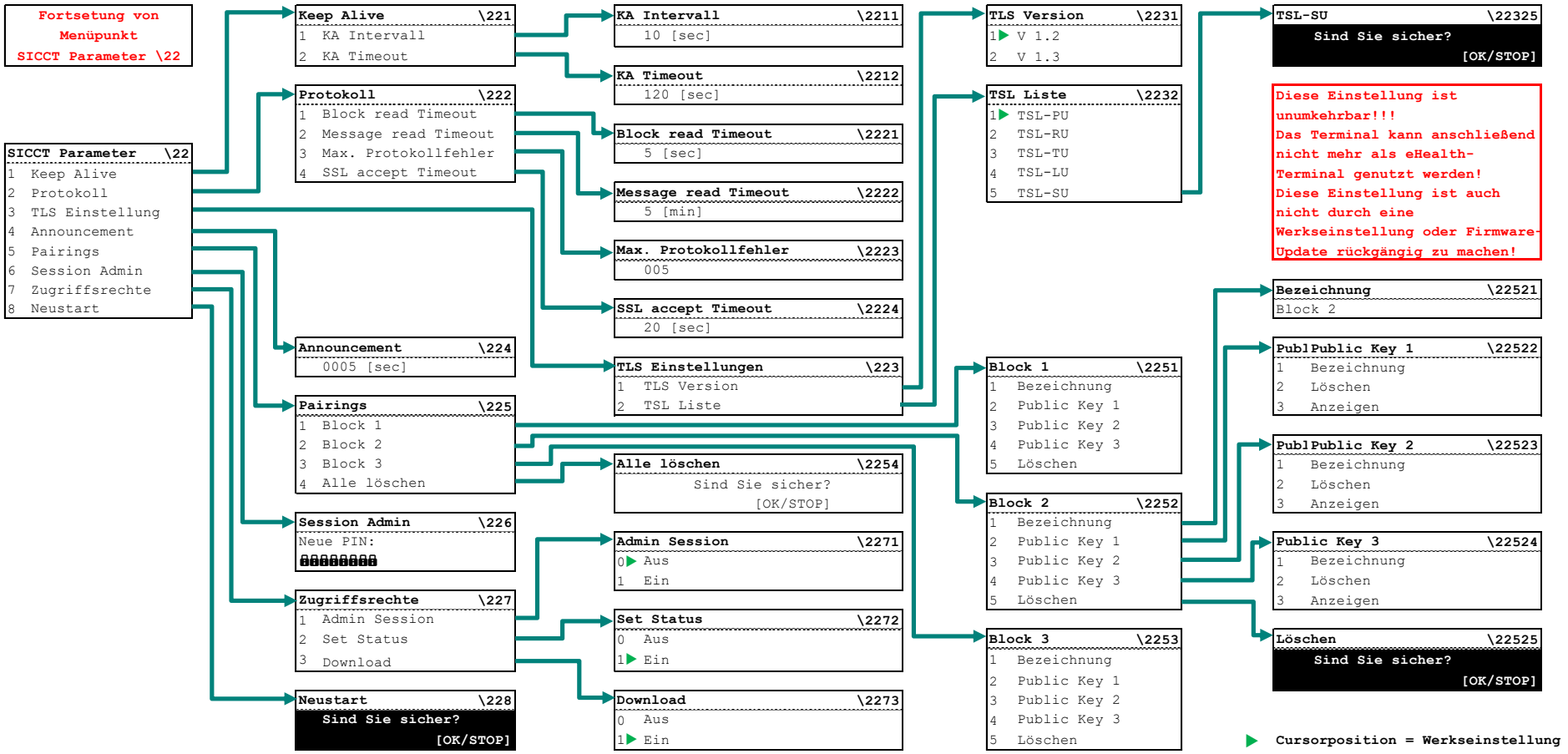
# 4. Menüstruktur für den Administrator - Teil 1: Allgemeine Einstellungen



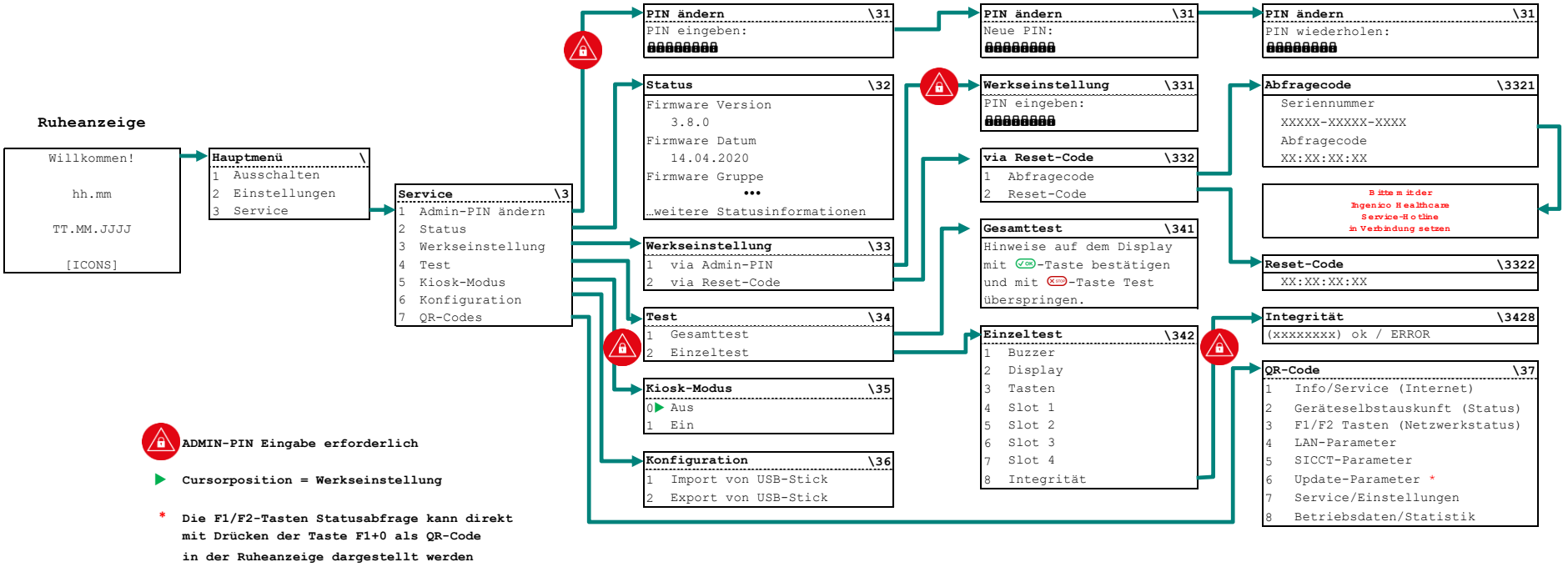
# 5. Menüstruktur für den Administrator - Teil 2: LAN Parameter



# 6. Menüstruktur für den Administrator - Teil 3: SICCT Parameter



# 7. Menüstruktur für den Administrator - Teil 4: Service Einstellungen



# 8. Hinweise zur Problembeseitigung, Fehlererkennung, Verhalten im Fehlerfall und Fehlerbehandlung

Probleme bei der Inbetriebnahme des ORGA 6141 online

| Problem: | Mögliche Ursachen | Mögliche Lösungen |
|---|---|---|
| Die Verpackung des Neugerätes ist beschädigt und die Gehäusesiegel sehen beschädigt aus. | • Das Gerät wurde nicht sachgemäß zwischengelagert und transportiert<br>• Das Gerät wurde manipuliert bzw. es wurde versucht das Gerät zu manipulieren. | • Lesen Sie sich die Sicherheitshinweise im Abschnitt 2 »Sicherheit« auf Seite 23 durch.<br>• Nehmen Sie das Gerät nicht in Betrieb und setzen Sie sich mit Ihrem Lieferanten in Verbindung.<br>• Klären Sie den Sachverhalt mit Ihrem Lieferanten und verlangen Sie den Austausch des Gerätes gegen ein neues und unbeschädigtes Gerät. |
| Das Gerät lässt sich nicht einschalten. | • Das Gerät wurde durch langes Drücken der STOP Taste im Ruhebildschirm (ca. 3 Sekunden) ausgeschaltet.<br>• Das Gerät ist defekt | • Versuchen Sie das Gerät durch langes Drücken der OK Taste einzuschalten<br>• Senden Sie das Gerät zum Service Ihres Lieferanten ein. |
| Nach dem Einschalten des Gerätes erscheint der blinkende Hinweis:<br>**Set ADMIN-PIN**<br>**Neue PIN:** | • Das Gerät ist neu und befindet sich noch im Auslieferungszustand.<br>• Es wurde ein Werksreset durchgeführt, aber noch keine neue Admin-PIN eingegeben. | • Wenden Sie sich an Ihren Administrator, wenn Sie nicht selbst der Administrator sind. Geben Sie eine neue Admin-PIN ein, wenn Sie der Administrator sind und Sie sich sicher sind, dass das Gerät neu ist oder von Ihnen per Werksreset in den Auslieferungszustand zurück gesetzt wurde. |
| Nach dem Einschalten steht im Display:<br>**Fehler Integrität.** | • Das Gerät wird bei jedem Einschalten einer Software-prüfung unterzogen. Das Ergebnis wird mit einem Vorgabewert verglichen. Ist das Ergebnis korrekt, geht das Gerät in Betrieb. Bei einem Fehler tritt das beschrieben Problem auf. | • Tritt der Fehler bei erneutem Einschalten nochmals auf, ist das Gerät einzuschicken, die Software ist defekt und eine einwandfreie Funktion unter Umständen nicht mehr gegeben. |
| Nach dem Einschalten des Gerätes erscheint plötzlich folgendes Symbol im Display:<br> | • Die interne Stützbatterie des Terminals verfügt nur noch über eine geringe Restkapazität.<br>• Wenn die Batterie verbraucht ist, wird automatisch ein Sicherheitsalarm ausgelöst und das Terminal kann nicht mehr genutzt werden. | • Das Terminal muss zeitnahe gegen ein neues Gerät getauscht werden. |

Tabelle 20: *Probleme bei der Inbetriebnahme des ORGA 6141 online*

### Probleme beim Einlesen von eGK Patientendaten

| Problem: | Mögliche Ursachen | Mögliche Lösungen |
|---|---|---|
| Nach Einstecken einer eGK erscheint der Hinweis: **Chipkarte -> nicht lesbar** | Nur bei aktivierter Karten-Anzeige:<br>• Die gesteckte eGK ist defekt<br>• Die Kontaktiereinheit 1 ist verschlissen oder verschmutzt<br>• Die Karte steckt falsch herum | • Versuchen Sie eine andere eGK auszulesen, um zu prüfen, ob die Kontaktiereinheit 1 des Gerätes funktioniert.<br>• Führen Sie den Einzeltest für den „Slot 1“ durch.<br>• Senden Sie das Gerät zum Service Ihres Lieferanten ein, falls verschieden Gesundheitskarten nur mit diesem Gerät nicht ausgelesen werden können. |

Tabelle 21: *Probleme beim Einlesen von eGK Patientendaten*

### Probleme beim Übertragen von Patientendaten zum Primärsystem

| Problem: | Mögliche Ursachen | Mögliche Lösungen |
|---|---|---|
| Ich werde in den Menüs [**Einstellungen \2**] und [**Service \3**] nach einer Admin-PIN gefragt. Diese ist mir nicht bekannt. Wie kann ich trotzdem Änderungen an den Einstellungen des Gerätes vornehmen? | • Es ist Teil des Sicherheitskonzeptes, dass gewisse Einstellungen des Gerätes nur vom Administrator vorgenommen werden können, um Manipulationen des Gerätes und versehentliche Veränderungen an den Einstellungen zu verhindern. | • Wenden Sie sich an Ihren Administrator, wenn Sie Änderungen an den Einstellungen des Kartenterminals vornehmen wollen.<br>• Wenn Sie der Administrator des Gerätes sind, aber Ihre Admin-PIN vergessen haben, können Sie mit dem sogenannten Reset-Code Verfahren das Gerät in die Werkseinstellung zurücksetzen und eine neue Admin-PIN vergeben. Dabei gehen alle Einstellungen verloren. Wenden Sie sich in diesem Fall direkt an Ingenico Healthcare. |

Tabelle 22: *Probleme beim Übertragen von Patientendaten zum Primärsystem*

Fehlermeldungen und Ursachen - Identification & Authentication

| Typ: | Mögliche Ursachen | Mögliche Lösungen |
|---|---|---|
| **falsche PIN oder fehlerhafte Eing.** | • Eingabe einer falschen Admin-PIN | • Korrekte Admin-PIN eingeben |
| **PIN Zeitsperre bitte warten…** | • PIN wurde mehrfach falsch eingegeben. Eine erneute PIN-Eingabe ist erst nach einer Wartezeit möglich. | • Korrekte Admin-PIN nach angegebener Zeit eingeben |
| **kein Abfragecode generiert** | • Die Funktion „Abfragecode“ wurde über das Terminal Menü noch nicht aufgerufen. | • Setzen Sie sich mit der Service-Hotline von Ingenico Healthcare in Verbindung |
| **falscher Code Fehlerzahler=X** | • Ein falscher Freischaltcode wurde eingegeben. | • Korrekten Freischaltcode eingeben |
| **Abbruch** | • STOP-Taste während der PIN-Eingabe gedrückt | • Beginnen Sie den Vorgang erneut von vorn. |

Tabelle 23: *Fehlermeldungen und Ursachen - Identification & Authentication*

## Fehlermeldungen und Ursachen - Firmware Update

| Typ: | Mögliche Ursachen | Mögliche Lösungen |
|---|---|---|
| **Fehler bei der Datenübertragung** | • Dateisystem des USB-Sticks beschädigt<br>• Der beabsichtigte Download-Vorgang wird abgebrochen. | • USB-Stick neu formatieren und Firmware-Image Datei erneut kopieren. |
| **Filesystem nicht unterstützt!** | • Falsches Dateisystem (nicht FAT 16 / FAT32)<br>• Der beabsichtigte Download-Vorgang wird abgebrochen. | • USB-Stick mit dem Dateisystem FAT32 neu formatieren und Firmware-Image Datei erneut kopieren. |
| **Ungültige Firmware** | • FW-Image nicht für das Terminal geeignet<br>• Fehler bei Signatur-Prüfung<br>• Nach Anzeige der Fehlermeldung verwirft das Terminal die Download-Daten (FW-Image) und startet mit der zuvor aktiven Firmware-Version. | • Geeignete Firmware-Image Datei auf den USB-Stick kopieren |
| **Ungültige Firmware** | • Firmware-Image Datei nicht für das Terminal geeignet | • Geeignete Firmware-Image Datei auf den TFTP-Server kopieren |
| **Speicherfehler** | • Fehler beim Schreiben in FLASH-Speicher<br>• Programmierphase wird beendet, das Gerät geht in einen sicheren Fehlerzustand über. | • Service kontaktieren. |
| **TFTP-Abbruch** | • Wenn der Download abgebrochen wird z.B. durch 'Stecker ziehen' (Timeout-Erkennung).<br>• Nach Anzeige der Fehlermeldung verwirft das Terminal die Download-Daten (FW-Image) und startet mit der zuvor aktiven Firmware-Version. | • Geeignete Netzwerkverbindung herstellen |
| **TFTP-Abbruch** | • Firmware-Image Datei liegt nicht im Root Directory des TFTP-Servers | • Firmware-Image Datei in das Root Directory des TFTP-Servers kopieren |
| **<Timeout: ca. 3 1/2 Min.><br>TFTP-Abbruch** | • Kein TFTP Server unter der eingestellten IP-Adresse erreichbar | • TFTP Server starten<br>• Firewall Einstellungen kontrollieren<br>• TFTP Server IP Adresse im Terminalmenü kontrollieren |
| **TFTP-Abbruch<br>Menürückkehr** | • Fehler bei der TFTP-Übertragung<br>• Übertragenes File ist zu groß. | • Geeignete Firmware-Image Datei auf den TFTP-Server kopieren |
| **Ungültige Firmware** | • Firmware-Image Datei nicht für das Terminal geeignet<br>• Version der neuen Software ist kleiner als die der Installierten.<br>• Nach Anzeige der Fehlermeldung verwirft das Terminal die Download-Daten (FW-Image) und startet mit der zuvor aktiven Firmware-Version. | • Geeignete Firmware-Image Datei auswählen |

| | | |
|---|---|---|
| **Update File nicht gefunden!** | • Dateiname des FW-Images passt nicht zum eingestellten Namen im Terminalmenü.<br>• FW-Image File liegt nicht im Root Directory des USB-Sticks.<br>• Der beabsichtigte Download-Vorgang wird abgebrochen. | • Name der Firmware-Image Datei auf dem USB-Stick an erwarteten Updatenamen anpassen.<br>• Firmware-Image Datei in das Root Directory des USB-Sticks kopieren |
| **Update File zu gross!** | • FW-Image nicht für das Terminal geeignet<br>• Nach Anzeige der Fehlermeldung verwirft das Terminal die Download-Daten (FW-Image) und belässt die zuvor aktive Firmware-Version. | • Geeignete Firmware-Image Datei auf den USB-Stick kopieren |
| **USB-Stick nicht gesteckt!** | • USB Stick wurde nicht in den USB-A Port an der Terminal Unterseite gesteckt.<br>• Der USB-Stick wurde vom Terminal nicht erkannt.<br>• Der beabsichtigte Download-Vorgang wird abgebrochen. | • USB-Stick ziehen und erneut gesteckt<br>• Alternativen USB-Stick probieren |

Tabelle 24: *Fehlermeldungen und Ursachen - Firmware Update*

Status - / Fehlermeldungen und Ursachen – DHCP

Anzeige des Status des DHCP Clients, wenn DHCP aktiv ist (DHCP = EIN).

| Typ: | Mögliche Ursachen | Mögliche Lösungen |
|---|---|---|
| **DHCP Server -** | • DHCP ist am Terminal deaktiviert.<br>• Terminal verwendet statische Netzparameter (u.a. IP-Adresse und Subnet-Mask). | • Aktivieren Sie DHCP am Terminal. (siehe Abschnitt 7.2.1.2.1 auf Seite 60) |
| **DHCP Server PREINIT** | • DHCP ist am Terminal aktiviert.<br>• Terminal verwendet DHCP und versucht, eine Kommunikation zu einem DHCP Server herzustellen. | |
| **DHCP Server FAIL** | • DHCP ist am Terminal aktiviert.<br>• Zustand nachdem der DHCP Client des KTs keinen DHCP Server erreicht hatte. Das Terminal versucht, eine Kommunikation zu einem DHCP Server herzustellen. | • Prüfen Sie die im Terminal eingegebene IP-Adresse und Subnet-Mask des DHCP Servers.<br>• Deaktivieren Sie DHCP am Terminal. (siehe Abschnitt 7.2.1.2.1 auf Seite 60) und geben Sie anschließend die korrekte IP-Adresse und Subnet-Mask des DHCP Servers manuel ein (siehe Abschnitte 7.2.1.3 und 7.2.1.4 auf Seite 61). |
| **DHCP Server BOUND** | • DHCP ist am Terminal aktiviert.<br>• Zustand nachdem der DHCP Client des KTs vom DHCP Server eine IP-Adresse bezogen hatte. | |
| **DHCP Server RENEW** | • DHCP ist am Terminal aktiviert.<br>• Zustand nachdem der DHCP Client des KTs vor Ablauf der Lease-Time vom DHCP Server eine IP-Adresse bezogen hatte. | |

Tabelle 25: *Status - / Fehlermeldungen und Ursachen – DHCP*

### Fehlermeldungen und Ursachen - Sichere PIN-Eingabe

| Typ: | Mögliche Ursachen | Mögliche Lösungen |
|---|---|---|
| **Wiederholung ist nicht gleich** | • Die Wiederholung der initialen Admin-PIN Eingabe war fehlerhaft. | • Wiederholen Sie die korrekte Eingabe der neuen Admin-PIN. |
| **Aktion erfolgreich** | • PIN erfolgreich eingegeben | |
| **Geheimzahl falsch / gesperrt** | • Falsche PIN eingegeben<br>• PIN ist auf der Karte bereits gesperrt. | • Geben Sie die PUK der Karte ein.<br>• Setzen Sie sich mit dem Kartenherausgeber in Verbindung, um die Karte wieder zu entsperren oder eine neue Karte zu beantragen. |
| **Geheimzahl nicht gleich. Abbruch** | • Wiederholung der PIN fehlerhaft. | • Wiederholen Sie die korrekte Eingabe der neuen Karten-PIN. |
| **Abbruch** | • STOP Taste gedrückt bei der PIN-Eingabe | • Beginnen Sie den Vorgang erneut von vorn. |
| **Alte PIN nicht zulässig!** | • Eingabe einer alten PIN | • Wiederholen Sie die korrekte Eingabe mit einer neuen Karten-PIN. |

Tabelle 26: *Fehlermeldungen und Ursachen - Sichere PIN-Eingabe*

### Fehlermeldungen und Ursachen – VPN-Verbindung

| Typ: | Mögliche Ursachen | Mögliche Lösungen |
|---|---|---|
| **CONNECTION FAILURE** | • Verbindungsfehler zum VPN-Gateway | • Adresse der VPN-Gateways und die Internetkonnektivität überprüfen |
| **CERTIFICATE INVALID** | • Zertifikat ungültig | • Zertifikat überprüfen. Evtl. abgelaufen |
| **AUTHENTICATION FAILURE** | • Authentisierung fehlgeschlagen | • Benutzerkennung und Passwort überprüfen |
| **NO LINK** | • kein Ethernet-Verbindung | • Kabel und Router überprüfen |
| **UNKNOWN ERROR** | • Fehler unbekannt | • Wenden Sie sich an den Administrator |

Tabelle 27: *Fehlermeldungen und Ursachen – VPN-Verbindung*

Fehlermeldungen und Ursachen - Sonstige

| Typ: | Mögliche Ursachen | Mögliche Lösungen |
|---|---|---|
| **Abbruch<br>Fehlende SMCKT** | • gSMC-KT nicht in Slot 3 oder 4 vorhanden.<br>• Die TCP Verbindung wird mit einem FIN / ACK beendet. | • Prüfen Sie, ob sich eine gSMC-KT im Slot 3 oder 4 befindet.<br>• Setzen Sie eine gSMC-KT mit gültigen Zertifikaten in den Slot 3 oder 4 ein. (siehe Abschnitt 5.7 auf Seite 52) |
| **Fehler<br>Integrität** | • Die Software-Integritätsprüfung hat einen Manipulationsversuch festgestellt. | • Setzen Sie sich mit der Service-Hotline von Ingenico Healthcare in Verbindung |
| **SICHERHEITSALARM<br>Service kontaktieren!** | • Die im Terminal integrierten Schutzmaßnahmen gegen Manipulationsversuche wurden ausgelöst und das Terminal wurde deaktiviert. | • Setzen Sie sich mit der Service-Hotline von Ingenico Healthcare in Verbindung |

Tabelle 28: *Fehlermeldungen und Ursachen - Sonstige*

# 9. Programmatische 2D-Code-Ausgaben über SICCT-Kommandos

Die nachfolgende Kurzinformation richtet sich nicht an Anwender, sondern an Konnektor- und SAK-Hersteller, welche die Ansteuerung des Kartenterminals anhand des SICCT- / eHealth KT-Kommandovorrats programmieren.



HINWEIS
Detailinformationen zur Erweiterung der Programmierung können beim Hersteller Ingenico Healthcare GmbH angefragt werden.

Die Firmware V3.8.1 beinhaltet funktionale Erweiterungen zu den SICCT-Kommandos

- **OUTPUT**: Zur Generierung und Darstellung von 2D-Codes am Terminaldisplay.
- **GET STATUS**: Zur Abfrage der Darstellungsmöglichkeiten des Terminal-Displays.

Eine Wertebereichserweiterung folgender SICCT-Datenobjekte erlaubt die 2-Code-Ausgabe sowie die Abfrage der Anzeigeeigenschaften

- [**SMTBD DO**]: Die zulässige Länge des Datenteils wurde vergrößert. Die Nutzdatenlänge beträgt ca. 1 KB.
- [**CS DO**]: Ergänzung zweier weiterer Konstanten zur Auswahl der 2D-Code-Art.
- [**DSPLC DO**]: Das Display Capabilities Datenobjekt zeigt bei der Abfrage der Functional Unit Display '40' im [**CS DO**] die Fähigkeit zur 2D-Code-Darstellung an.

Diese Erweiterungen wurden der gematik im Jahr 2019 vorgeschlagen, basieren dem SICCT-Grundkonzept zur Kodierung von Ausgabemeldungen (Messages) und gibt einer ansteuernden Instanz (Konnektor oder SAK) die technische Möglichkeit, 2D-Codes durch das Terminal generieren sowie auf dem Grafik-Display anzeigen zu lassen.
Die Nutzdaten hierzu übergibt der Konnektor bzw. die SAK via SICCT-Datenobjekt „SICCT Message To Be Displayed“ [**SMTBD DO**] und wählt die Kodierungsart (QR- oder DataMatrix-Code) via Character Set Datenobjekt [**CS_DO**] entsprechend.

Die ergänzten Werte im Character Set Data Object [**CS DO**] im [**DSPLC DO**]:

- [**'85' ,01' '30'**] = [**DSPLC DO**] mit der Indikation QR-Code
- [**'85' ,01' '40'**] = [**DSPLC DO**] mit der Indikation DataMatrix-Code

U.a. obige Rückgabewerte erhalten folgende Abfragen an die Functional Unit Display '40':

- **SICCT GET STATUS** Abfrage des [**CS DO**] (Tag '85')
- **SICCT GET STATUS** Abfrage des [**DSPLC DO**] (Tag '67')

# 10. Abbildungsverzeichnis

Abbildung 1: *Unbeschädigtes Gehäusesiegel* ..... 23
Abbildung 2: *Beschädigtes Gehäusesiegel* ..... 23
Abbildung 3: *Fehlendes Gehäusesiegel* ..... 23
Abbildung 4: *Unbeschädigtes Slotssiegel* ..... 25
Abbildung 5: *Beschädigtes Slotssiegel* ..... 25
Abbildung 6: *Fehlendes Slotssiegel* ..... 25
Abbildung 7: *Positionen der Gehäuse- und Slotsiegel am Gehäuse des Gerätes* ..... 26
Abbildung 8: *Typenschild mit zulässigem Herstellcode HC 03000000010301* ..... 27
Abbildung 9: *Gerätevorderseite* ..... 39
Abbildung 10: *Geräterückseite* ..... 40
Abbildung 11: *Die Kontaktiereinheiten 3 und 4 für die SMC-Karten* ..... 40
Abbildung 12: *Tastatur des Gerätes* ..... 41
Abbildung 13: *Aufbau des Grafikdisplays* ..... 42
Abbildung 14: *Der Ruhebildschirm* ..... 43
Abbildung 15: *Das Menü [Einstellungen \2]* ..... 44
Abbildung 16: *Das Hauptmenü* ..... 44
Abbildung 17: *Einstecken einer eGK* ..... 45
Abbildung 18: *Einstecken eines HBA* ..... 45
Abbildung 19: *Der HBA in der Kontaktiereinheit 2* ..... 45
Abbildung 20: *Zugriffsrechte festlegen* ..... 47
Abbildung 21: *Vorderseite der gSMC-KT von Ingenico Healthcare* ..... 50
Abbildung 22: *Rückseite der gSMC-KT von Ingenico Healthcare* ..... 50
Abbildung 23: *Einsetzen der SMC-Karten in die Kontaktiereinheit 3 und 4* ..... 52
Abbildung 24: *Die richtige Positionierung des Slotsiegels* ..... 52
Abbildung 25: *Beispiel der Angabe des gSMC-KT Fingerprints im Konfigurationsmenü eines Konnektors* ..... 52
Abbildung 26: *Unterschreiben und richtiges Anbringen der Slotsiegel* ..... 53
Abbildung 27: *Anschlüsse auf der Unterseite des Gerätes* ..... 54
Abbildung 28: *Anschluss mit LAN-Kabel am Konnektor* ..... 54
Abbildung 29: *Informationen über die Update-Datei (1/3)* ..... 75
Abbildung 30: *Informationen über die Update-Datei (2/3)* ..... 75
Abbildung 31: *Informationen über die Update-Datei (3/3)* ..... 75
Abbildung 32: *Darstellung der Kartendetails einer gSMC-KT in Slot 4* ..... 86
Abbildung 33: *QR-Code zum Auslesen von Terminal Konfigurationen und Betriebszuständen* 92

# 11. Tabellenverzeichnis

Tabelle 1: *Begriffsbestimmung* ..... 22
Tabelle 2*: Werksvoreinstellungen* ..... 49
Tabelle 3: *Werksvoreinstellungen der „Functional Units" des Terminals* ..... 69
Tabelle 4*: Displayanzeige während eines Firmware-Updates via Konnektor* ..... 74
Tabelle 5*: Displayanzeige während eines Firmware-Updates via TFTP Server im Pull-Verfahren* ..... 77
Tabelle 6: *Mögliche Steuerwörter der Steuerdatei für das Update via TFTP Server im Push Verfahren* ..... 79
Tabelle 7: *Parameter des Abfrageintervalls für das Update via TFTP Server im Push Verfahren* ..... 81
Tabelle 8: *Terminalselbstauskunft* ..... 84
Tabelle 9: *Unterstützte Parameter der Im- und Export-Dateien* ..... 90
Tabelle 10*: Tests beim Import einer Konfigurationsdatei* ..... 91
Tabelle 11: *Beispiel der Syntax eines dynamischen QR-Code Wertes* ..... 93
Tabelle 12: *URL-Informationen des QR-Codes: [Status (Geräteselbstauskunft) \372]* ..... 94
Tabelle 13: *URL-Informationen des QR-Codes: [F1/F2 Tasten (Netzwerkstatus) \373]* ..... 95
Tabelle 14: *URL-Informationen des QR-Codes: [LAN-Parameter \374]* ..... 96
Tabelle 15: *URL-Informationen des QR-Codes: [SICCT-Parameter \375]* ..... 96
Tabelle 16: *URL-Informationen des QR-Codes: [Update Parameter \376]* ..... 96
Tabelle 17: *URL-Informationen des QR-Codes: [Service/Einstellungen \377]* ..... 97
Tabelle 18: *URL-Informationen des QR-Codes: [Betriebsdaten/Statistik \378]* ..... 99
Tabelle 19: *Technische Daten* ..... 100
Tabelle 20: *Probleme bei der Inbetriebnahme des ORGA 6141 online* ..... 107
Tabelle 21: *Probleme beim Einlesen von eGK Patientendaten* ..... 108
Tabelle 22: *Probleme beim Übertragen von Patientendaten zum Primärsystem* ..... 108
Tabelle 23: *Fehlermeldungen und Ursachen - Identification & Authentication* ..... 109
Tabelle 24: *Fehlermeldungen und Ursachen - Firmware Update* ..... 111
Tabelle 25: *Status - / Fehlermeldungen und Ursachen – DHCP* ..... 112
Tabelle 26: *Fehlermeldungen und Ursachen - Sichere PIN-Eingabe* ..... 113
Tabelle 27: *Fehlermeldungen und Ursachen – VPN-Verbindung* ..... 113
Tabelle 28: *Fehlermeldungen und Ursachen - Sonstige* ..... 114

# 12. NOTIZEN