WORLDLINE

Bedienungsanleitung Stationäres eHealth-Kartenterminal ORGA 6141 online Hardware-Version 1.2.0 und 2.0.0 (ORGA Neo) mit Firmware-Version 3.9.0

CE

V24.5.1

Healthcare

Vorwort

Sehr geehrte Anwenderin, sehr geehrter Anwender,

vielen Dank, dass Sie sich für ein Produkt von Worldline (vormals Ingenico) Healthcare entschieden haben. Diese Bedienungsanleitung beschreibt das stationäre eHealth-Kartenterminal ORGA 6141 online.

Sie finden auf unserer Homepage www.worldline.com/de/healthcare weitere Dokumentationen zum **Remote Management Interface** inklusive dem **SMC-B Remote PIN-Verfahren** sowie einem Tutorial zur einfachen **Einrichtung einer VPN-Verbindung**. Die Firmwarestände der Version 3.9.0 sind für Bestands-kartenterminals des ORGA 6141 online ab der Firm- und Hardwareversion V3.7.4:1.2.0 als auch für Kartenterminals ab der Firm- und Hardwareversion V3.8.2:2.0.0 (ORGA Neo) vorgesehen. Somit können alle Bestands- und Neugeräte auf **derselben Firmwareversion** betrieben werden. Sie finden unter https://fachportal.gematik.de/zulassungs-bestaetigungsuebersichten den neusten Zulassungsstatus.

Das ORGA 6141 online ist ein von der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) **zugelassenes** eHealth-Kartenterminal für den stationären Online-Produktivbetrieb am Konnektor. Alternativ kann es durch einmalige Umschaltung der Betriebsdaten auch als Signaturterminal an einer **Signaturanwendungskomponente** (SAK) eingesetzt werden.

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 Bedienungsanleitung 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 Arbeiten mit Ihrem neuen eHealth-Kartenterminal, welches ab HW 2.0.0 in Farbvarianten erhältlich ist und über die Vertriebsbezeichnung ORGA Neo auf die überarbeitete Gerätegeneration hinweist.

Gerne unterstützen wir Sie bei Fragen rund um unsere Produkte, deren Installation und Bedienung. Sie erreichen uns telefonisch werktags zwischen 08:00 und 17:00 oder per E-Mail.

Ihr Worldline Healthcare Team

Worldline Healthcare GmbH
Konrad-Zuse-Ring 1
24220 Flintbek
WEEE DE 32266764

Tel.: 04347 90 11 111
Internet: www.worldline.com/de/healthcare
E-Mail: kontakt.whc@worldline.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 3.9.0.

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.

Im LAN der Einsatzumgebung kommuniziert das Primärsystem/Praxisverwaltungssystem (PVS) 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 der Karten.

Damit ist der Konnektor die dezentrale Komponente zur sicheren Anbindung von Clientsystemen der Institutionen (AIS, AVS) sowie der Kartenterminals im sicheren lokalen Netz (LAN) des Anwenders. Der Konnektor regelt auch die sicheren Kommunikationsbeziehungen zwischen Clientsystem, Kartenterminals, Karten sowie den fachanwendungsspezifischen Diensten in der TI-Infrastruktur.

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 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 103 bis 107.

HINWEIS
Eine schnelle Übersicht und Einführung in die verschiedenen Funktionselemente des Gerätes finden Sie im Abschnitt 3. Produktbeschreibung auf Seite 33 dieser Bedienungsanleitung.

Copyrights

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.

FW-Version	Änderung zur Vorgängerversion
V3.8.2	**Änderung zur Vorgängerversion V3.8.1:** • Formale Anpassungen Firmenbezeichnung, FW-Version, Release Datum und FW Gruppe (FWG) • Ergänzung der Hinweise zum optionalen Zubehör: ORGA Protect und ORGA Service APP für iOS • Anhang: gSMC-KT G2.1 Musteranschreiben • Anpassung der Internet-Links auf Worldline-Webpräsenz • Anpassung in Kapitel 2.2.6/7.3.2 - Ergänzung von Produktvarianten aufgrund von HW-Maintenance Version 2.0.0 in „Tabelle 2: *Herstellcode-Kennungen der zulässigen Produktvarianten“* und Produktversion in Tabelle 24.
V3.9.0	**Änderung zur Vorgängerversion V3.8.2:** • Formale Anpassungen Firmenbezeichnung, FW-Version, Release Datum und FW Gruppe (FWG) • Anpassungen der Herstellerangaben an Worldline (u.a. Kontakt-Mailadresse, WEEE) • Aktualisierung von Produkt- und Menüabbildungen • Menüänderungen und Erweiterungen u.a. Remote Management Interface (RMI) mit Symbolen • Ergänzung - RMI-Hinweis-Bildschirm bei Inbetriebnahme eines Neugerätes • Änderung – Symbolanzeige RMI-Status (Pos.7) low battery und Signaturterminal (Pos.8) • Ergänzung – Anzeigeplatz Datenverkehr zu RFID/NFC-Token (Pos.5) • Tabelle 3 – Werksvoreinstellungen - Ergänzungen für RMI und VPN • Tabelle 41 – Umbenennung und Ergänzung für Hinweistext auf aktive RMI-Session • VPN-Client - Ergänzung der Authentifizierungsmethoden und Zugangsdatenkonfiguration • Zubehör – Aktualisierungen • Kapitel 2.5 „Sichere Außerbetriebnahme zur Einlagerung, Verschrottung oder Rücksendung im Gewährleistungsfall“ wurde aktualisiert • Redaktionelle Anpassungen • Ergänzung in Kapitel 7.2.3.4 – Ergänzung Abbildung 35: „Statusmeldung während der Umleitung der SMC-B-PIN-Eingabe an den SMC-B-PIN-Provider“ und Ergänzung „Sicherer zertifizierter Betriebszustand“ • Ergänzung in Kapitel 7.2.3.1 – „HINWEIS: Zeitbedarf der RMI-Aktivierung“

Inhaltsverzeichnis

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 Worldline 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

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

Taste	Funktion
	**F1 Taste:** • Bei freier Texteingabe die Schriftzeichen **-** oder **_** (Unterstrich) • Die Funktionstaste F1 (Netzwerkstatus) hat in Kombination mit den nachfolgenden Tasten die angegebene Funktion: 0 QR-Code mit allen folgenden Betriebsdaten / Status-Informationen, die über die Tasten F1 und F2 abgerufen werden können 1 MAC Adresse 4 GHI TCP-Port 5 JKL UDP Port 6 MNO SICCT Terminal Name • Die Funktionstaste F1 kann in folgenden Menüs gedrückt werden, um direkt einen QR-Code mit den in diesen Menüs dargestellten Parametern anzuzeigen: ○ [**LAN Parameter \21**] ➔ QR-Code: [**LAN-Parameter \374**] ○ [**SICCT Parameter \22**] ➔ QR-Code: [**SICCT-Parameter \375**] ○ [**Update \28**] ➔ QR-Code: [**Update Parameter \376**] ○ [**Service \3**] ➔ QR-Code: [**Betriebsdaten/Statistik \378**] ○ [**Status \32**] ➔ QR-Code: [**Status (Geräteselbstauskunft) \372**]
	**F2 Taste:** • Bei freier Texteingabe das Schriftzeichen**,** (Kommazeichen) • Die Funktionstaste F2 (Verbindungsstatus) hat in Kombination mit den nachfolgenden Tasten die angegebene Funktion: 1 TLS (Verbindungsstatus) 2 ABC SICCT Session (Verbindungsstatus) 3 DEF SICCT Kommando Interpreter (Status) 4 GHI DHCP Server (siehe Tabelle 41 auf Seite 112 im ANHANG) 5 JKL VPN Status 6 MNO Aktuell verwendeter Public Key-Index (Index: 1 bis 3) des aktuellen Pairing Blocks (PB-1 bis PB-3) (Nur bei bestehendem Pairing und aktiver TLS Verbindung zwischen Terminal und Konnektor)
	**Cursor-Taste (nach oben):** • Im Menü mit dem grünen ▶ Cursor einen Menüpunkt nach oben springen
	**Cursor-Taste (nach unten):** • Im Menü mit dem grünen ▶ Cursor einen Menüpunkt nach unten springen
	**Cursor-Taste (nach links):** • Eine Menüebene zurückspringen
	**Cursor-Taste (nach rechts):** • In das Untermenü springen, auf den der grünen ▶ Cursor gerade zeigt

Taste	Funktion
	**STOP Taste:** • Abbrechen einer Aktion • Eine Menüebene zurückspringen • Durch langes Drücken im Ruhebildschirm (ca. 3 Sekunden): Ausschalten des Gerätes
	**CLEAR Taste:** • Löschen eines Wertes links neben dem Eingabecursor
	**MENU Taste:** • Im Ruhebildschirm: Öffnen des Hauptmenüs • Im Hauptmenü und Untermenüs: Zurück in den Ruhebildschirm
	**OK Taste:** • Einschalten des Gerätes • In das Untermenü springen, auf das der grünen ▶ Cursor gerade zeigt • 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 Nutzung des **Features „Remote-SMC-PIN“** blinkt das Symbol der gesteckten SMC-B bis zum Empfang der PIN-Eingabe des externen SMC-PIN-Providers via RMI. 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 5: Datenverkehr zu RFID/NFC-Token

Die Ausgabeposition 5 ist reserviert für einen optionalen RFID/NFC-Kommunikationsstatus.

Symbol	Bedeutung
	Keine aktivierte RFID-Schnittstelle / keine aktive RFID-Session.

ACHTUNG
Die RFID-Schnittstelle wird optional durch ein extern anzuschließendes Zubehör erreicht, dessen Betrieb zur RFID-Kommunikation zurzeit außerhalb des evaluierten Geräts und des sicheren Betriebs liegt.

1.5.3. Symbol 6: Datenverkehr zu angeschlossenen Geräten

An der Ausgabeposition 6 erscheinen die Zustandssymbole für das **SICCT-Session** und **VPN-Verbindung**.

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 **aufgebau**t. Es besteht noch **keine SICCT-Session**.
	**VPN-Verbindung** ist **aufgebau**t und es besteht eine "**SICCT Control Session**" TLS-Verbindung.
	**VPN-Verbindung** ist **aufgebaut** und es besteht eine "**SICCT Admin Session**" TLS-Verbindung.

1.5.4. Symbol 7: Konfiguration / Zustand der Remote Management Schnittstelle

Über Ausgabeposition 7 erfolgen die Zustandssymbole für das **Remote Management Interface (RMI).**

Symbol	Bedeutung
	Erscheint dieses Icon, zeigt es an, dass der Administrator das Remote Management Interface (RMI) in der Gerätekonfiguration aktiviert hat und zurzeit **keine RMI-Verbindung** zum Terminal besteht. **HINWEIS:** Bei diesem Zustand besteht ein exklusiver Zugriff auf die Geräteparameter via Direktmanagementschnittstelle.
	Dieses Icon zeigt an, dass zurzeit entweder eine **aktive anonyme RMI-Session** mit **Leseberechtigung** von Konfigurations- und Betriebsdaten oder eine **RMI-Session zum SMC-B-PIN-Provider** besteht.
	Dieses Icon zeigt an, dass zurzeit eine **aktive ADMIN-RMI-Session** eines entfernten Administrators **mit Lese/Schreibrechten** zur Modifikation von Konfigurations- und Betriebsdaten besteht.

1.5.5. Symbol 8: Interne Stützbatterie schwach / Konfiguration als Signaturterminal außerhalb der Telematikinfrastruktur

An der Ausgabeposition 8 können die folgenden Zustandssymbole in der Priorität der dargestellten Reihenfolge erscheinen.

Symbol	Bedeutung
	Low Battery - Die interne Stützbatterie des Terminals verfügt nur noch über eine geringe Restkapazität. **HINWEIS**: Das Terminal muss zeitnah gegen ein neues Gerät getauscht werden.
	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 vollständig verbraucht ist, wird automatisch ein Sicherheitsalarm ausgelöst und das Terminal kann nicht mehr genutzt werden.
	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.

1.5.6. Symbol 9: Allgemeiner Gerätestatus

An der Ausgabeposition 9 können die folgenden Zustandssymbole zum allgemeinen Gerätestatus erscheinen.

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

1.5.7. Symbol 10: Datenverwaltung

An der Ausgabeposition 10 können die folgenden Zustandssymbole zum Zugangsstatus zur Datenverwaltung erscheinen.

Symbol	Bedeutung
	Kein Zugang zu den Menüs: • [**Einstellungen \2**] • [**Admin-PIN ändern \31**] • [**Werkseinstellung via Admin-PIN \331**] • [**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 oder Praxisverwaltungssystem (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. *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 (ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server)
eGK	Elektronische Gesundheitskarte
FAT32	File Allocation Table 32 (ein von Microsoft entwickeltes Dateisystem)
gematik	Nationale Agentur für Digitale Medizin – gematik GmbH
Gesicherte Umgebung (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). *Siehe auch: Zugänglicher Bereich, Allgemein zugänglicher Bereich*
gSMC-KT	gerätespezifische Security Module Card Kartenterminal. Die gSMC-KT dient der Identifikation des individuellen Kartenterminals.
HBA (auch eHBA)	Heilberufsausweis Der elektronische HBA identifiziert den Heilberufler (Arzt, Apotheker, Zahnarzt, ...) als berechtigte Person.
ICCSN	Kartenkennnummer (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 Geräteeinstellungen.
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 Ein PUK ist ein elektronischer Schlüssel, der zum Entsperren einer Chipkarte dient, nachdem eine PIN mehrmals falsch eingegeben wurde.
PVS	Praxisverwaltungssystem (Primärsystemsoftware)
RPS	Remote PIN-Sender

Begriff	Erläuterung
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. Bei ORGA eHealth-Terminals ist es mit einem sogenannten Challenge-Response-Verfahren nur Worldline Healthcare möglich, sie wieder in den Auslieferungs-zustand zurück zu versetzen.
SAK	Signaturanwendungskomponente
SICCT	Secure Interoperable ChipCard Terminal 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) Ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung 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 (dient dem alleinigen Test- und Instantsetzungsprozessen des Terminals in der Laborumgebung des Terminalherstellers)
TLS-SU	TLS für die Signaturumgebung (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. 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 (eHBA). Der Benutzer des Gerätes muss sich mit dem Gebrauch vertraut machen und die einwandfreie Funktion sowie die Sicherheitsmerkmale am Gerät regelmäßig überprüfen.

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 21 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 Worldline 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 Slotsiegel

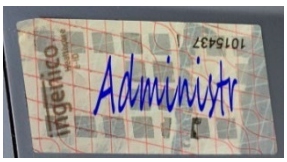


Abbildung 5:
Beschädigtes Slotsiegel

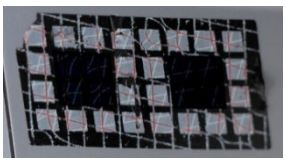


Abbildung 6:
Fehlendes Slotsiegel

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.

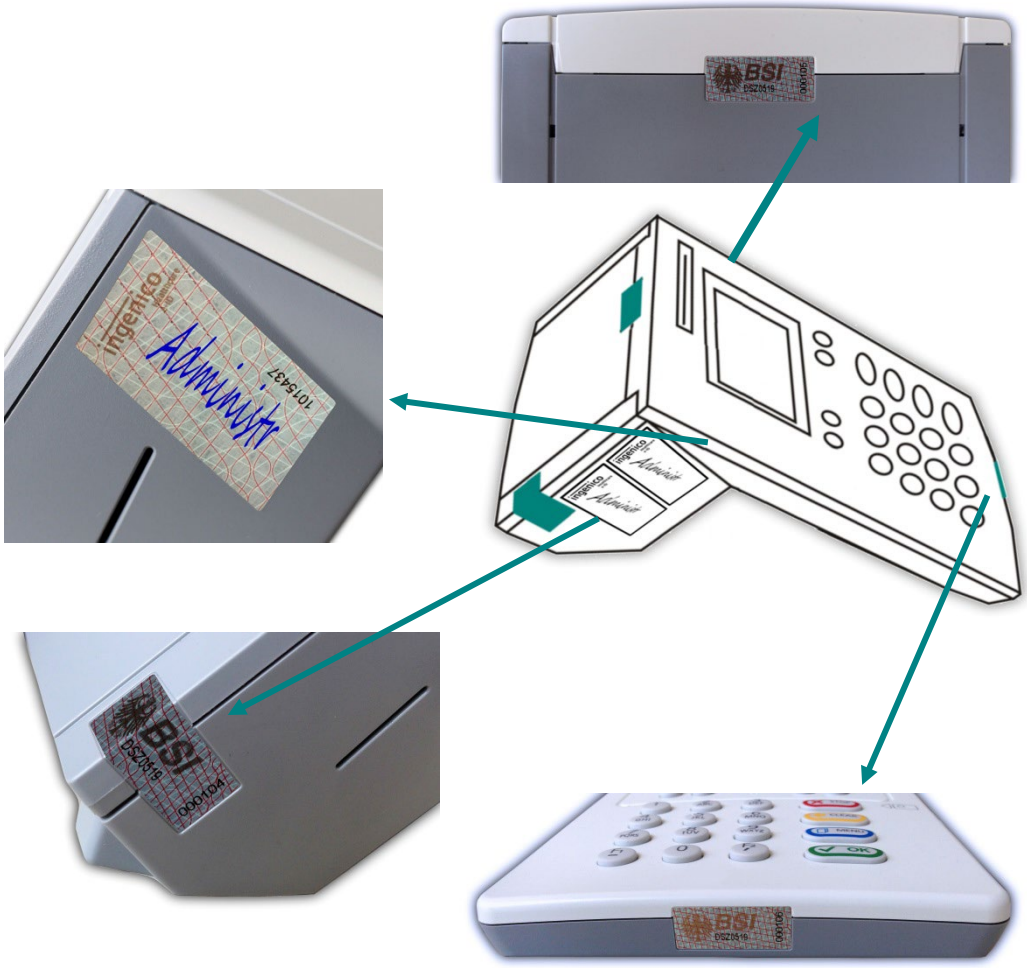


Abbildung 7: *Positionen der Gehäuse- und Slotsiegel am Gehäuse des Gerätes*

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 Produktversion der Gerätesoftware, die im Menü [**Status \32**] (siehe 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:*Beispiel - Typenschild mit zulässigem Herstellcode HC 03000000010301 oder HC 03000000020301 für V3.9.0:1.2.0*

Das Typenschild befindet sich auf der Geräterückseite oberhalb der Anschlüsse. Auf dem Typenschild steht u.a. der Herstellername, 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).

Abbildung 9: *ORGA 6141 mit Kennzeichnung „ORGA Neo“ mit HC 06000000020302*

Abbildung 10: *Beispiel – Typenschild „ORGA Neo“ mit HC 06000000020302*

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 85) 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.

Produktversion	Herstellcode	HW-Version	FW-Version	Herstellername/Attribute
3.9.0:1.2.0	HC **03**000000010301	1.2.0	3.9.0	Ingenico Healthcare, weiße Oberschale
3.9.0:1.2.0	HC **03**000000020301	1.2.0	3.9.0	Ingenico Healthcare, weiße Oberschale
3.9.0:2.0.0	HC **03**00000002030**2**	2.0.0	3.9.0	Ingenico Healthcare, weiße Oberschale
3.9.0:2.0.0	HC **04**00000002030**2**	2.0.0	3.9.0	Worldline Healthcare GmbH, weiße „Ingenico“-Oberschale mit Aufdruck „ORGA Neo“
3.9.0:2.0.0	HC **05**00000002030**2**	2.0.0	3.9.0	Worldline Healthcare GmbH, weiße Oberschale mit Aufdruck „ORGA Neo“
3.9.0:2.0.0	HC **06**00000002030**2**	2.0.0	3.9.0	Worldline Healthcare GmbH, mint farbene Oberschale mit Aufdruck „ORGA Neo“

Tabelle 2: *Herstellcode-Kennungen der zulässigen Produktvarianten*

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 diese 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.

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-Eingabe Modus / 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 ab der 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 93 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. Sichere Außerbetriebnahme zur Einlagerung, Verschrottung oder Rücksendung im Gewährleistungsfall

Das ORGA 6141 online ist ein sicherheitstechnisch sensibler Bestandteil der Telematikinfrastruktur in Ihrer Praxis. Wenn Sie das Gerät nicht mehr verwenden wollen oder können, es eingelagert, verschrottet oder im Gewährleistungsfall zurückgesendet werden soll, 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. Stellen Sie sicher, 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 86)

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 39) und die SMC-B und gSMC-KT Karten aus den Kontaktiereinheiten 3 und 4 (siehe Abschnitt
4. 3.3 Die Kontaktiereinheiten 3 und 4 für die SMC-Karten auf Seite 34).
5. Bewahren Sie Ihren HBA und die SMC-Karten an einem sicheren Ort auf.
6. 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 **„Download-Center“** zum Download bereitgestellt (https://support.worldline.com/de-de/home/healthcare/downloads/Formulare.html). 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 **vor dem 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 „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 Worldline Healthcare erworben haben, sind die Forderungen auch an Worldline Healthcare zu richten!

Verpacken Sie das Terminal sicher für den Rückversand an Ihren Händler oder Worldline 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** 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. Geben Sie unmittelbar nach dem erfolgreichen Werksreset jedoch keine neue Admin-PIN ein, sondern trennen Sie bei Aufforderung zur Eingabe einer Admin PIN das Gerät einfach von Stromnetz.

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.

ACHTUNG
Beachten Sie bei der Wiederinbetriebnahme, 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 28).
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 45 beschrieben wird.

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 19) und beachten Sie die Entsorgungshinweise im Abschnitt 2.12 Entsorgung des Gerätes auf Seite 32.

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 19 und Abschnitt 2.2.2 Das Slotsiegel und seine Eigenschaften auf Seite 20).

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 potenzielles 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 

-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.worldline.com/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 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 Worldline 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

Abbildung 11: *Gerätevorderseite*

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 Menünavigation

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

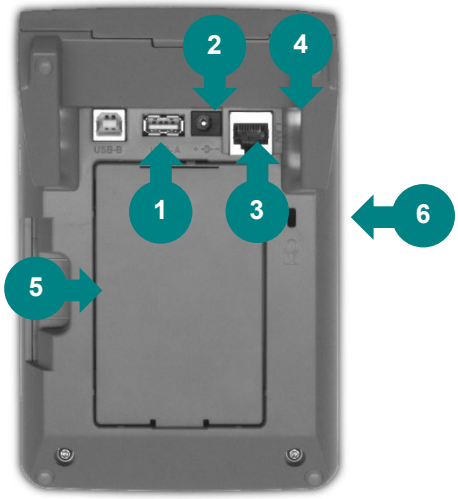
6: Menütasten STOP CLEAR MENU OK

HINWEIS

Als Zubehör für Ihren Einsatzzweck bietet Worldline 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



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

2: USB-A Anschluss für Zubehör ORGA Protect oder USB-Stick für zukünftige Firmware-Updates.

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

Abbildung 12: *Geräterückseite*

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

1: 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

2: Korrekt eingesteckte SMC-Karte

3: Gehäusesiegel

4: Slotsiegel mit individueller Nummer

Abbildung 13: *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 Slotsiegel 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 45.

4. Bedienung des Gerätes

4.1 Tastatur

Abbildung 14:
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 12 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 OK-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 58).

4.3 Aufbau des Grafikdisplays

Abbildung 15: *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 14 dieser Bedienungsanleitung.

4.4 Der Ruhebildschirm

Abbildung 16: *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 72 dieser Bedienungsanleitung. Unter dem Begrüßungstext werden die aktuelle Uhrzeit und das aktuelle Datum angezeigt, wenn diese über einen NTP-Server (siehe Abschnitt 7.2.1.8. LAN-Parameter: [NTP Client \218] auf Seite 58) bezogen wird.
Wenn das Terminal über einen NTP-Server automatisch das aktuelle Datum bezieht, dann informiert es Sie rechtzeitig über ablaufende Gültigkeiten der Zertifikate der eingesteckten gSMC-KT Karte. Hierzu muss unter [Display \264] die Anzeige dieses Hinweistextes aktiviert sein.

Sobald sich das Ablaufdatum eines der Zertifikate auf der gSMC-KT 42 oder weniger Tagen in der Zukunft liegt und der NTP-Server eingerichtet ist, 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 47 bzw. Abschnitt 6. Inbetriebnahme als Signatur-Terminal außerhalb der Telematikinfrastruktur auf Seite 50 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 17:
*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 17) [**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 103 bis 107.

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 18: *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

Abbildung 19: *Einstecken einer eGK*

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.

4.8 Einstecken eines HBA in die Kontaktiereinheit 2

Abbildung 20: *Einstecken eines HBA*

Abbildung 21:
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.

HINWEIS

Im Fall, dass zum Zeitpunkt des lokalen Admin-Zugriffs, bereits ein entfernter Admin-Zugriff über das Remote Management Interface (RMI) besteht, erhält der lokale Admin zum RMI-Status-Icon einen Hinweistext in einer PopUp-Textbox „**Remote Admin aktiv**" temporär angezeigt, welcher per Tastendruck auch sofort geschlossen werden kann.
.

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

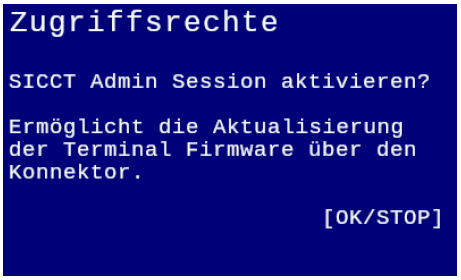


Abbildung 22: *Zugriffsrechte festlegen*

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 können diese Einstellung jederzeit im Menü [Admin Session \2271] verändern (siehe Abschnitt 7.2.2.8.1. Zugriffsrechte: [Admin Session \2271] auf Seite 63).

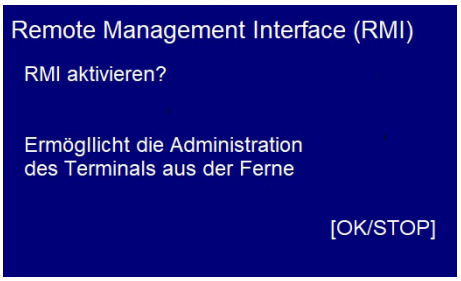


Abbildung 23: RMI aktivieren

Stereotyp folgt anschließend automatisch noch die Nachfrage „**RMI aktivieren?**“, d.h. ob mit der Bestätigung OK ebenfalls die Remote Schnittstelle (Remote Interface, RMI) aktiviert werden soll. Sie können diese Einstellung im Menü [Remote Management Interface \231] verändern (siehe 7.2.3. Remote Management Interface [Remote Management Interface \23]).

Nach erfolgter Auswahl wechselt die Anzeige in den Ruhebildschirm und Sie können mit der Konfiguration des Terminals und dem Pairing mit dem Konnektor beginnen.

Als genereller Indikator eines aktivierten RMI erscheint in der Symbolleiste das Icon  .

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 Worldline Healthcare anfordern. Hierfür ist ein sicheres Vergabeverfahren notwendig. Bitte setzen Sie sich hierfür mit der Service-Hotline von Worldline Healthcare in Verbindung.

5.4. Neue PIN anfordern

Sollten Sie Ihre Admin-PIN vergessen haben, können Sie eine neue PIN bei Worldline Healthcare anfordern. Hierfür ist ein sicheres Vergabeverfahren notwendig. Bitte setzen Sie sich hierfür mit der Service-Hotline von Worldline 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	Einstellmöglichkeiten	Werks-einstellung
SICCT Announcement	[**Announcement \224**]	0 sec. (Aus) bis 3000 sec.	5 sec.
LAN Parameter DHCP	[**DHCP \2121**]	Ein 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 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 V1.3	V1.2
TSL Liste	[**TSL Liste \224**]	TSL-PU TSL-RU TSL-TU TSL-LU TSL-SU	TSL-PU
SICCT Zugriffsrechte Admin Session	[**Admin Session \2271**]	Ein Aus	Aus
SICCT Zugriffsrechte* Set Status Kommandos	[**Set Status \2272**]	Ein Aus	Ein
SICCT Zugriffsrechte* Download Kommandos	[**Download \2273**]	Ein Aus	Ein
Remote Management Interface (RMI)**	[**Remote Management Interface \231**]	Ein Aus	Aus
Feature „Remote SMC-B PIN“	[**Remote SMC-B PIN \234**]	Ein Aus	Aus
VPN-Tunnel	[**VPN Tunnel \2171**]	Ein Aus	Aus

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

Bestandsgerät: Die neue Option RMI wird beim FW-Update auf V3.9.0 ff aktiviert, wenn zuvor [Admin Session \2271**] eingeschaltet war

Tabelle 3*: Werksvoreinstellungen*

Um das Gerät wieder in Werkseinstellung zurückzuversetzen, 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 zurückversetzt. 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. Vom Terminal ermittelte Betriebsdaten/Statistik bleiben bei einem Werksreset erhalten.

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 Worldline gSMC-KT durchführt, wird der Einsatz einer Worldline 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 Worldline Healthcare!

Bei den in Abbildung 24 und Abbildung 25 dargestellten Vorder- und Rückseiten handelt es sich um die bei Redaktionsschluss dieser Bedienungsanleitung verwendeten gSMC-KT Karten der Generation G2.1. Es ist möglich, dass die Bedruckung von zukünftigen gSMC-KT Karten und des dazugehörigen Anschreibens (siehe Musteranschreiben einer gSMC-KT auf Seite 102 des Anhangs) von diesen durch technische Änderungen oder gesetzlichen Vorgaben abweichen können. Dies allein 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:
https://support.worldline.com/de-de/home/healthcare/downloads/Sichere-Lieferkette

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

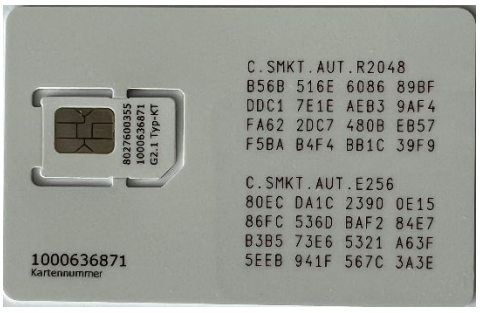


Abbildung 24:
Beispiel Vorderseite der gSMC-KT von Worldline Healthcare

Abbildung 25:
Beispiel Rückseite der gSMC-KT von Worldline 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 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 Abschnitt 7.3.4. Terminal-Funktionstests [Test \34] auf Seite 87, 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 24 und der Rückseite in Abbildung 25 vergleichen. Es ist möglich, dass die Bedruckung von zukünftigen gSMC-KT Karten und des dazugehörigen Anschreibens (siehe 0. Musteranschreiben einer gSMC-KT auf Seite 102 des Anhangs) von diesen durch technische Änderungen oder gesetzlichen Vorgaben abweichen können. Dies allein 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:

https://support.worldline.com/de-de/home/healthcare/downloads/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 Worldline Healthcare bis zu Ihnen nachzuverfolgen, wenn Sie die Karte nicht direkt bei Worldline Healthcare bestellt haben. Die Worldline Healthcare GmbH hat hierfür auf ihrer Internetseite

https://support.worldline.com/de-de/home/healthcare/downloads/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 Worldline 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 26 zeigt die beiden Kontaktiereinheiten 3 (unterer Kartenschlitz) und 4 (oberer Kartenschlitz), die für die Aufnahme einer Signaturkarte im 2FF-Format (Mini-SIM) und weiterer applikationsspezifischer Smartcards vorgesehen sind. In der Online-Telematikinfrastruktur 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). Erneutes Drücken entriegelt die Karten und sie können wieder entnommen werden.

Abbildung 26:
Einsetzen der SMC-Karten in die Kontaktiereinheit 3 und 4

Abbildung 27:
Die richtige Positionierung des Slotsiegels

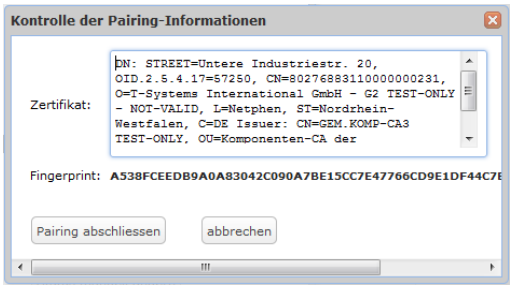
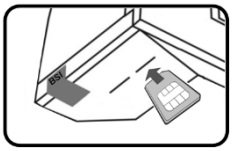


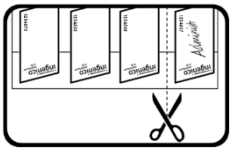
Abbildung 28:
Beispiel der Angabe des gSMC-KT Fingerprints im Konfigurationsmenü eines Konnektors

Beim Pairing Prozess muss der Administrator den Fingerprint (Hash-Wert des Authentisierungszertifikates der gSMC-KT) im Administrations-Frontend des Konnektors überprüfen. Dieser Fingerprint ist direkt auf dem Kartenträger (siehe Abbildung 24) aufgedruckt. Die Abbildung 28 zeigt beispielhaft die Angabe des gSMC-KT Fingerprints im Konfigurationsmenü eines Konnektors. Weitere Details zum Fingerprint der gSMC-KT Karte entnehmen Sie bitte dem Handbuch des Konnektors.



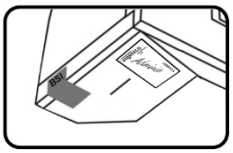
Setzen Sie die SMC-Karten wie oben beschrieben in die Kontaktiereinheiten 3 und 4 ein. In welche Kontaktiereinheit Sie die gSMC-KT oder SMC-B Karte einsetzen, spielt keine Rolle.

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 27). 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 29: *Unterschreiben und richtiges Anbringen der Slotsiegel*

HINWEIS
Empfohlen ist der Einsatz der Worldline gSMC-KT Karte, welche i.d.R. zum Gerät mit erworben wird. Die 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.

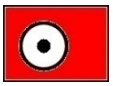
ACHTUNG
Zum Wechseln der SMC-Karte entfernen Sie das Siegel und alle Rückstände des Siegels vollständig, bevor Sie die alte durch eine neue SMC-Karte ersetzen und ein neues Siegel aufkleben.

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 Anschluss des Zubehörs ORGA Protect oder 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 30:
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 19 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 86 in Abschnitt 7.3.3. Zurücksetzen des Terminals in den Auslieferungszustand [Werkseinstellung \33]
beschriebenen Werksreset.

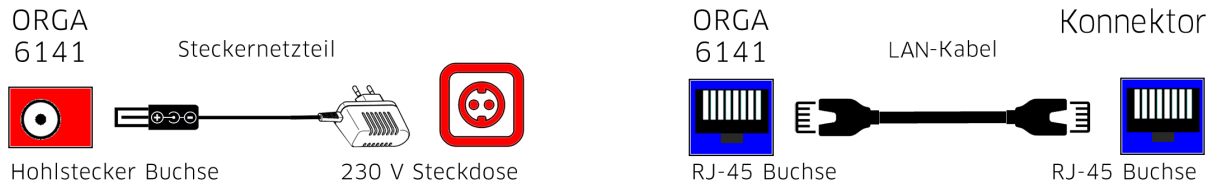


Abbildung 31: *Anschluss mit LAN-Kabel am Konnektor*

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 59. Schließen Sie das Gerät mit einem LAN-Kabel an den Konnektor und mit dem Steckernetzteil an eine Steckdose an, so wie es in Abbildung 31 dargestellt ist.

5.9. Initiales Pairing des Terminals mit dem Konnektor

ACHTUNG
Lesen Sie unbedingt den gesamten Abschnitt 1.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 Worldline 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, welcher zur Außerbetriebnahme führt, oder bei geplanter Außerbetriebnahme müssen alle im Terminal gespeicherten Pairing-Informationen vom Administrator gelöscht werden. Dieses kann vereinfacht im Zuge eines Werksreset oder durch das Löschen aller 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 Pairing-Information am Konnektor löschen. Entsprechende Anweisungen zur Kontrolle entnimmt der Administrator der Produktdokumentation (Kartenterminalverwaltung) 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 62.

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 Kartenterminal-verwaltung 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 62.

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

Das ORGA 6141 online ab 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.
Ab Firmwareversion 3.9.0 bestehen zu dem nachfolgend Beschriebenen zusätzliche Menüpunkte und alternative Optionen, um die Parameter über ein zweites Konfigurationsdateiformat zur Parametrisierung des VPN-Tunnels zu einem VPN-Gateway zu ex- und importieren. Die Beschreibungen finden Sie in der separaten Dokumentation „VPN-Tutorial für das ORGA 6141 online und das ORGA Neo ab Firmware V3.9.x“ (> V22.1) auf der Worldline Healthcare Hersteller-Webseite unter
https://worldline.com/de-de/home/main-navigation/solutions/healthcare/unser-portfolio/orga-6141-online

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-Zertifikat 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

Die folgende Vorgehensweise wird ab Firmwareversion 3.8.1 und aus Kompatibilitätsgründen weiterhin unterstützt. Die Beschreibungen eines erweiterten Formats (ab FW V3.9.0) finden Sie in der separaten Dokumentation „ORGA 6141 online VPN Tutorial“ (> V22.1) auf der Worldline Healthcare Webseite.

Erstellen Sie mit einem einfachen Text-Editor (z. B. Notepad) 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 90.

Speichern Sie diese Datei mit einem Dateinamen, der auf **_import.cfg** endet. Speichern Sie die Datei entweder in das **Stammverzeichnis** eines USB-Sticks mit FAT32-Formatierung (ab FW V3.8.1) oder alternativ in ein, nach der **14-stelligen Seriennummer** benannten, **Unterverzeichnis** (ab FW V3.9.0). Wird obige Konvention eingehalten, findet das Gerät beim Import das entsprechende Unterverzeichnis mit der vorbereiteten Konfigurationsdatei anhand der Seriennummer. Ab FW V3.9.0 haben Sie damit eine komfortable Möglichkeit, multiple Konfigurationsdateien auf dem USB-Stick nach Seriennummern geordnet vorzuhalten. Beachten Sie, dass die maximale Dateinamenlänge von maximal 32 Zeichen inklusive Dateiextension (**.cfg**) eingehalten werden muss, da im Fall des Menu-Aufrufs, das Terminal-Display nicht mehr als 32 Zeichen anzeigen kann bzw. editieren lässt.

Führen Sie anschließend den Import der Daten wie im Abschnitt 7.3.6. Konfiguration via USB-Stick im- und exportieren auf Seite 90 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 1.5.3) auf Seite 15.

6. Inbetriebnahme als Signatur-Terminal außerhalb der Telematikinfrastruktur

Das ORGA 6141 online kann auch ohne ein Pairing mit einem Konnektor außerhalb der Telematik-infrastruktur (TI) des deutschen Gesundheitswesens als **Signaturterminal mit LAN-Anschluss** betrieben werden. Hierzu besteht die Möglichkeit eine sogenannte Trust-Service Status List für die Signatur-umgebung (TLS-SU) auszuwählen. Mit der Auswahl der TLS-SU werden Betriebsdaten des ORGA 6141 online unumkehrbar umkonfiguriert, sodass es nicht weiter als eHealth-Terminal für die TI eingesetzt werden kann.

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 47 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 Worldline 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.

Worldline 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.

	Einstellungen	**\2**	*Kurzbeschreibung*
1	LAN Parameter	\21	*LAN-/Netzwerkparameterkonfiguration*
2	SICCT Parameter	\22	*Konfiguration der SICCT-Parameter und Zugriffsberechtigungen*
3	Remote Management Interface	\23	*Konfiguration der Remote Management Schnittstelle (Remote Management Interface RMI)*
4	Zeit / Datum	\24	*Kontrollfunktionen zu NTP-empfangenen Zeit- und Datumseinstellungen*
5	Sprache	\25	*Auswahl der Spracheinstellung für Menü- und Standardanzeigetexte (standard messages)*
6	Display	\26	*Konfiguraton der Display-Einstellungen*
7	Töne	\27	*Konfiguration der akustischen Signale*
8	Update	\28	*Konfiguration und manuelles Auslösen der Ladefunktion zum Update der Firmware oder der TSL-Liste.*

Tabelle 4: *Menü Einstellungen*

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 96 beschrieben werden.

	LAN Parameter	**\21**	*Kurzbeschreibung*
1	Gerätename	\211	*Konfiguration des Gerätenamens*
2	DHCP	\212	*Aktivieren/Deaktivieren und Konfiguration des DHCP-Clients*
3	IP-Adresse	\213	*Konfiguration einer statischen IP-Adresse*
4	Subnet Mask	\214	*Konfiguration der Subnet-Maske für die LAN-Zielumgebung*
5	Gateway/DNS	\215	*Konfiguration einer statischen IP-Adresse für das Internetgateway bzw. den DNS-Server*
6	TCP/UDP Port	\216	*Konfiguration der TCP-Port-Nummer für das TCP und das UDP-Protokoll*
7	IPSec VPN	\217	*Konfiguration des VPN-Clients zum Aufbau eines VPN-Tummels via IPSec-Protokoll*
8	NTP Client	\218	*Konfiguration einer statischen IP-Adresse für einen NTP-Server zum Bezug von Zeit-/ Datumseinstellungen.*
9	Neustart	\219	*Manuelles Auslösen eine Neustarts zur Übernahme geänderter LAN – oder SICCT-Parameter*

Tabelle 5: *Menü LAN Parameter*

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 Menüpunkte 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 stellt je nach Einsatzumgebung ein potenzielles Sicherheitsrisiko dar.

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]

Die 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 3.9.0 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 49.

	IPSec VPN	**\217**	*Kurzbeschreibung*
1	VPN-Tunnel Ein/Aus	\2171	Aktivieren/Deaktivieren der VPN-Tunnelkonfiguration
2	VPN-Tunnel Neustart	\2172	Neustart des konfigurierten VPN-Tunnels
3	Authentifizierungsmethode	\2173	Methodenwahl zur Authentifitierung
4	Zugangsdaten	\2174	Zugangsdatenkonfiguration zum VPN-Gateway
5	Status/Information	\2175	Anzeige von VPN-Statusinformationen
6	Konfiguration löschen	\2176	Löschen der Zugangsdatenkonfiguration zum VPN-Gateway

Tabelle 6: *Menü IPSec VPN*

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: [Authentifizierungsmethode \2173]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern 2 [Admin-PIN Eingabe] 1 7 3.
Mit dieser Funktion kontrolliert oder stellt der Administrator die gewünschte **Authentifizierungsmethode für die VPN-Verbindung** ein.

	Authentifizierungsmethode	**\2173**	*Kurzbeschreibung*
1	nicht konfiguriert	\21731	*Für die VPN-Verbindung wurde keine Authentifizierungsmethode eingestellt.*
2	PSK (PreSharedKey)	\21732	*Umschalten auf Methode PSK*
3	MSCHAPv2 (User/Passwort)	\21733	*Umschalten auf Methode MSCHAPv2*
4	PublicKey (Zertifikat)	\21734	*Umschalten auf Methode PublicKey*
5	EAP-TLS (Zertifikat)	\21735	*Umschalten auf Methode EAP-TLS*

Tabelle 7: *Menü Authentifizierungsmethode*

Von den vier angebotenen Authentifizierungsmethoden kann immer nur eine die Aktivierte sein.

Am linken Display Rand zeigt ein grüner Pfeil auf die jeweils eingestellte Authentifizierungsmethode.

Abbildung 32: *VPN-Parameter/Authentifizierungsmethode*

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.

	Zugangsdaten	**\2174**	*Kurzbeschreibung*
1	Info zu den Zugangsdaten	\21741	*Abruf der Zugangsdateninformationen*
2	VPN-Gateway Adresse	\21742	*Statische Definition der IP-Adresse des VPN-Gateways*
3	DPD-Verzögerung	\21743	*Zeitspanne für Dead Peer Detection (DPD) für die VPN/IPSec-Verbindung*
4	PreSharedKey	\21744	*Methode PSK : Konfiguration des Authentifizierungsschlüssels (authentication key) für die VPN-Verbindung*
5	EAP-MSCHAPv2	\21745	*Methode MSCHAPv2: Konfiguration von Benutzernamen und Passwort*
6	Zertifikatsanfrage erstellen	\21746	*Methode PublicKey und Methode EAP-TLS: Erzeugung eines Schlüsselpaares aus privatem (private key) und öffentlichem (public key) Schlüssel und einer Zertifizierungsanfrage (certification request) mit Darstellung als QR-Code am Display.*

Tabelle 8: *Menü Zugangsdaten*

7.2.1.7.3. VPN-Parameter: [Info Zugangsdaten \21741]

Mit dieser Funktion können Sie die Informationen zu den Zugangsdaten abrufen.

7.2.1.7.3. VPN-Parameter: [VPN-Gateway Adresse \21742]

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.

7.2.1.7.3. VPN-Parameter: [DPD-Verzögerung \21743]

Mit dieser Funktion können Sie die Dead Peer Detection-Verzögerung (DPD) in Sekunden einstellen. Als Default-Wert wurde zwanzig (20) Sekunden vorgesehen.

7.2.1.7.3. VPN-Parameter: [PreSharedKey \21744]

Mit dieser Funktion können Sie einen Pre Shared Key (16 bis 32 Zeichen) über das Menü ansehen oder eingeben.

7.2.1.7.3. VPN-Parameter: [EAP-MSCHAPv2 \21745]

Mit dieser Funktion können Sie die Parameter für EAP-MSCHAPv2 setzen. Geben Sie die Benutzerkennung und das dazugehörige Passwort der Benutzerkennung mit Hilfe der Tastatur unter \21745 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.

7.2.1.7.3. VPN-Parameter: [Zertifikatsanfrage erstellen \21746]

Mit dieser Funktion können Sie eine Zertifikatsanfrage (certificate signing request) erstellen, welche am Display als QR-Darstellung erscheint. Der dargestellte QR-Code kann z.B. mittels eines Smartphones abgescannt werden, um den certificate signing request in die eigene PKI zu übernehmen und ein signiertes Zertifikat zu erzeugen.
Das damit erzeugte und signierte Zertifikat kann via USB-Stick oder RMI in das Terminal importiert und gespeichert werden, um es entweder für die Authentifizierungsmethode PublicKey oder EAP-TLS zu aktivieren.

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 90 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.

	SICCT Parameter	**\22**	*Kurzbeschreibung*
1	Keep Alive	\221	*Definition des Intervalls für SICCT-Keep Alive Ereignisse sowie des Keep-Alive-Timeouts.*
2	Protokoll	\222	*Parameterdefintion für das SICCT-Protokoll*
3	TLS Einstellung	\223	Parameterdefintion für das Transport Layer Security-Protokoll (TLS)
4	Announcement	\224	*Aktivierung und Defintion des SICCT-Announcement-Intervalls*
5	Pairings	\225	*Pairingblock-Verwaltung zum Konnektor/SAK-Pairing*
6	Session Admin	\226	*Separate Konfiguration der Admin PIN für die SICCT ADMIN SESSION.*
7	Zugriffsrechte	\227	*Definition von Zugriffsrechten für ausgesuchte SICCT-Kommandos.*
8	Neustart	\228	*Manueller Neustart zur Aktivierung geänderter SICCT- oder LAN-Parameter*

Tabelle 9: *Menü SICCT Parameter*

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 97 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 Worldline 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 Worldline 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 Menüstruktur für den Administrator - Teil 3: SICCT Parameter auf Seite 106 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 Terminalmenüzugriff 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 41).

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 53 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 10 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 10: *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 63 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 73 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. Remote Management Interface [Remote Management Interface \23]

Das ORGA 6141 online bietet ab der Firmware Version V3.9.0 eine Remote-Management Schnittstelle (RMI) an. Über diese RMI-Schnittstelle kann anonym oder vom Administrator (ADMIN) entweder mit Hilfe der ausgelieferten **Web-Applikation** (basierend auf HTML, CSS und JavaScript) **über einen Web-browser** oder per (ggf. eigener) Remote-Management Client Applikation auf Basis des **WebSocket-Protokolls** kommuniziert werden.

Zur Kommunikation mit dem **RMI-Client** bietet das Gerät einen **internen Websocket-Server**, welcher per TCP-Port (Default 443) empfangsbereit ist, um TLS-abgesicherte HTTPS-Anfragen (Request) vom Client zu bearbeiten und mit einer entsprechenden Antwort (Response) zu beantworten.
Zum Ausweisen gegenüber dem RMI-Client verwendet der Websocket-Server ein konfigurierbares **RMI-Authentifizierungszertifikat** (TLS-Zertifikat im X.509-Format), welches die **TLS-Verbindung** per **TLS** (je nach Client-Vorgabe 1.2. oder 1.3**)** absichert. Eine Client-Authentisierung ist nicht vorgesehen.

Die Kommunikation über die RMI-Schnittstelle erfordert den Aufbau einer **RMI-Session** durch den RMI-Client. Hierzu kann sich ein anonymer Anwender (anonymous user) oder im Gerät hinterlegter Administrator mit seinen Zugangsdaten verbinden. Je nach Benutzerkennung bzw. Rolle (anonym oder ADMIN) bestehen unterschiedliche Berechtigungen.

Eine etablierte **RMI-Session** muss vom Client mittels RMI-spezifischer **Keep-Alive-Nachrichten** am Leben erhalten werden. Sobald der **interne Websocket-Server** feststellt, dass kein aktiver Datenaustausch mehr über die RMI-Schnittstelle stattfindet, beendet das Terminal die RMI-Session/ Verbindung nach einer konfigurierten **Timeout-Zeit**.

Die **RMI-Beschreibung** der per RMI-Session erreichbaren Services, Zugriffs- und Parameter-beschreibungen finden Sie in dem **separaten Dokument** „*Remote Management Interface für das ORGA 6141 online und das ORGA Neo*“ auf der Worldline Healthcare Hersteller-Webseite unter
https://worldline.com/de-de/home/main-navigation/solutions/healthcare/unser-portfolio/orga-6141-online

Abbildung 33: *Remote Management Schnittstelle (RMI)*

Die nachfolgende Beschreibung widmet sich dem **Menü zur Konfiguration und Aktivierung der RMI-Schnittstelle** durch den Administrator.
Alle weitergehenden Detailinformationen zum **RMI-Protokoll** und **RMI-Objekten** finden sich in dem **separaten Dokument** „*Remote Management Interface für das ORGA 6141 online und das ORGA Neo*“.

	Remote Management Interface	**\23**	*Kurzbeschreibung*
1	Ein/Aus	\231	*Aktivieren/Deaktivieren des RMI*
2	Timeout	\232	*Timeout-Definition für RMI-Keep-Alive*
3	Remote Admin PIN ändern	\233	*Separate Konfiguration der ADMIN PIN für das RMI*
4	Remote SMC-B PIN Ein/Aus	\234	*Aktivieren/Deaktivieren der Remote SMC-B-PIN*
5	SMC-B PIN-Provider PIN ändern	\235	*Separate Konfiguration der SMC-B PIN-Provider PIN für das Feature „Remote SMC-B PIN“*
6	Zertifikat	\236	*Verwaltung des Authentisierungszertifikats der RMI-Schnittstelle*

Tabelle 11: *Menü Remote Management Interface*

7.2.3.1 De-/Aktivieren der Remote Management Schnittstelle [Remote Management Interface \231]

Mit diesem Menüpunkt schalten Sie als ADMIN das optionale **Remote Management Interface (RMI)** ein oder aus. Per Werkseinstellung (Auslieferungszustand) ist die Option RMI ausgeschaltet (Aus).

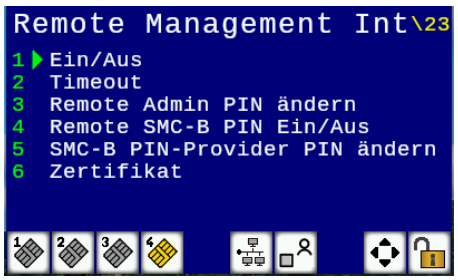


Abbildung 34: *RMI aktivieren*

Zur Indikation, dass die **Option RMI eingeschaltet** ist**,** erscheint das RMI-Status-Icon . in der Symbolleiste im Terminal-Display an der Ausgabeposition 7. Dieser Zustand bedeutet auch: **keine aktive (offene) RMI-Session**.
Im Fall, dass die **Option RMI ausgeschaltet ist,** erscheint **kein RMI-Status-Icon** an der Ausgabeposition 7 der Symbolleiste.

HINWEIS: Zeitbedarf der RMI-Aktivierung
Nach der Umschaltung erscheint das RMI-Status-Icon nach ca. 8 Sekunden, gefolgt von der Meldung "Vorgang beendet", und bevor das Terminalmenü in die Ebene „\23“ zurückwechselt.
Vom RMI-Client kann die RMI-Schnittstelle nach ca. 60 Sekunden erreicht werden.

7.2.3.2. Timeout-Parameter der Remote Management Schnittstelle (RMI) [Timeout \232]

Über diesen Menüpunkt setzen Sie als ADMIN die **Timeout-Einstellung für die RMI** in Sekunden.

Der numerische Wert bestimmt, nach welcher Timeout-Zeit das Gerät das RMI schließen wird, sofern keine RMI-Session eröffnet bzw. während einer offenen RMI-Session vom Gerät kein **Keep Alive** über den TCP-Port der RMI empfangen wurde. Per Werkseinstellung (Auslieferungszustand) ist der Timeout-Wert auf 300 Sekunden (5 Minuten) gesetzt.

7.2.3.3. Ändern der Remote Admin PIN für die RMI [Remote Admin PIN ändern \233]

Über diesen Menüpunkt setzt der ADMIN am Gerät die achtstellige **ADMIN-PIN für die Authentifizierung über die Remote Management Schnittstelle** (RMI). Im Auslieferungszustand ist die ADMIN-PIN für den Zugang über das RMI unbesetzt bzw. leer.
Nur im Fall, dass die ADMIN-PIN für das RMI leer ist, wird diese zum Zeitpunkt der Aktivierung des RMI automatisch mit dem Wert der ADMIN-PIN zum Gerätemanagement initialisiert.
Über den Aufruf des Menüpunkts Remote Admin PIN kann der ADMIN die ADMIN-PIN für das RMI separat definieren.

7.2.3.4. Remote SMC-B PIN Ein/Aus [Remote SMC-B PIN \234]

Mit diesem Menüpunkt schalten Sie als ADMIN das optionale **Feature „Remote SMC-B PIN“** ein oder aus. Die **Vorbedingung** zur Nutzung des Features „Remote SMC-B PIN“ ist**,** dass das zuvor **RMI aktiviert** und eine **SMC-B-Provider-PIN** vereinbart wurde**.** Per Werkseinstellung (Auslieferungszustand) das Feature „Remote SMC-B PIN ausgeschaltet (Aus).

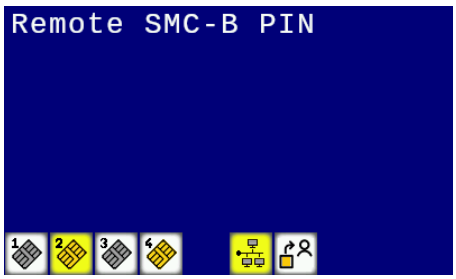


Abbildung 35: *Statusmeldung während der Umleitung der SMC-B-PIN-Eingabe an den SMC-B-PIN-Provider*

Der **SMC-PIN-Provider** ist eine Rolle einer externen Instanz, zu welcher eine lokale PIN-Eingabeaufforderung für eine gesteckte SMC-B per RMI umgeleitet werden kann. Zum Zugriff auf das Feature „Remote SMC-B PIN“ muss der externe SMC-B PIN-Provider die vereinbarte PIN via RMI nutzen. Statt den SMC-B-PIN-Eingabe-Dialog lokal am Terminal durchzuführen, wird eine Meldung am Display dargestellt, welche informiert, dass der PIN-Eingabe-Request per RMI an den externen SMC-PIN-Provider umgeleitet wurde. Das Kartenstatus-Icon für den Slot mit der gesteckten SMC-B blinkt dann wie bei einer lokalen Eingabe bis zum Empfang der PIN-Eingabe des externen PIN-Providers.

ACHTUNG: Sicherer zertifizierter Betriebszustand
Nur bei der Verwendung der sicheren PIN-Eingabe am Gerät befindet sich das Kartenterminal im sicheren zertifizierten Betriebszustand.
Der ADMIN und Nutzer/SMC-B-PIN-Provider gewährleisten, dass der Aufruf der Management-schnittstelle und die entfernte Eingabe der PIN der SMC-B ausschließlich an Clients geschieht, die dieser oder seine Organisation unter Kontrolle hat und deren Sicherheit er oder seine Organisation durchsetzen kann.

7.2.3.5. Remote SMC-B PIN Ein/Aus [PIN ändern \235]

Über diesen Menüpunkt ändert der ADMIN die achtstellige **PIN für den Remote SMC-B Provider**.
Per Werkseinstellung (Auslieferungszustand) ist die PIN des Remote SMC-B PIN Providers leer.

7.2.3.6. RMI-Zertifikatsverwaltung [Zertifikat \236]

Über diesen Menüpunkt ruft der ADMIN das Untermenü zur Verwaltung der Einstellungen des **Authentisierungszertifikats der RMI-Schnittstelle** am Gerät auf.

	Zertifikat	**\236**	*Kurzbeschreibung*
1	Anzeigen	\2361	*Anzeige von Details des RMI-Authentisierungszertifikats*
2	Neu erstellen	\2362	*Neugenerierung des RMI-Authentisierungszertifikats*
3	Zertifikatsanfrage erstellen	\2363	*Generierung eines Certificate Signing Requests (CSR) für das RMI-Authentisierungszertifikat*
4	Zertifikat importieren	\2364	*Import des signierten RMI-Authentisierungszertifikats*

Tabelle 12: *Menü Remote Management Interface/Zertifikat*

7.2.3.6.1 RMI-Zertifikat Anzeige [Anzeige \2361]

Über diesen Menüpunkt ruft der ADMIN das Untermenü zur Kontrolle der Eigenschaften des **RMI-Authentisierungszertifikats** am Gerät auf.

Abbildung 36: *RMI-Zertifikatsanzeige aufrufen*

	Anzeigen	**\2361**	*Kurzbeschreibung*
1	Zertifikatsdetails	\23611	*Anzeige von Details des RMI-Authentisierungszertifikats*
2	Zertifikatsfingerprint	\23612	*SHA-256 Hash Wert als Fingerprint des Authentisierungszertifikats der RMI-Schnittstelle*

Tabelle 13: *Menü Remote Management Interface/Zertifikat/Anzeige*

7.2.3.6.1.1 Detailanzeige des RMI-Zertifikats [Zertifikatsdetails \23611]

Über diesen Menüpunkt ruft der ADMIN **Details des konfigurierten RMI-Authentisierungszertifikats** am Geräte-Display ab. Diese umfassen die X.509-Feldinformationen u.a. den Issuer, Common Name (CN) sowie die Angaben zur zeitlichen Gültigkeit (NotBefore bzw. NotAfter).

7.2.3.6.1.2 Zertifikatsfingerprint [Zertifikatsfingerprint \23612]

Über diesen Menüpunkt ruft der ADMIN den **Fingerprint des RMI-Authentisierungszertifikats** am Gerät ab. Das RMI-Authentisierungszertifikat sichert die **TLS-Verbindung** vom **WebSocket-Server** ab.

Abbildung 37: *RMI-Zertifikatsfingerprint*

Der **RMI-Client** ermittelt ebenso den Fingerprint des empfangenen TLS-Zertifikats z.B. per Webbrowser. Unter Kenntnis des separat übermittelten Fingerprints vom Gerät ergibt sich die Prüfmöglichkeit, per Sichtkontrolle am Client feststellen, ob eine vertrauenswürdige TLS-Verbindung (ohne Man-In-The-Middle) vorliegt. Der errechnete Fingerprint des aktiven **RMI-Authentisierungszertifikats** wird hexadezimal als 32-Byte langer SHA-256 Hash Wert am Display angezeigt.

7.2.3.6.2 RMI-Zertifikaterstellung [Neu erstellen \2362]

Abbildung 38: *Neuerstellung des RMI-Zertifikats aufrufen*

Über diesen Menüpunkt ruft der ADMIN das Untermenü zur Erstellung und zum Import eines neuen **Authentisierungszertifikats für die RMI-Schnittstelle** am Gerät auf.

	Neu erstellen	**\2362**	*Kurzbeschreibung*
1	Worldline Self-Signed	\23621	*Erstellung eines self-signed RMI-Authentisierungszertifikats*
2	Parameter abfragen	\23622	*Parameterabfrage für das neue Authentisierungszertifikat der RMI-Schnittstelle*
3	Parameter Import via USB-Stick	\23623	*Import der Parameterdatei des Authentisierungszertifikats der RMI-Schnittstelle*

Tabelle 14: *Menü Remote Management Interface/Zertifikat/Neu erstellen*

7.2.3.6.2.1 Self-Signed RMI-Zertifikat [Worldline Self-Signed \23621]

Über diesen Menüpunkt erzeugt der ADMIN ein neues **selbstsigniertes (self-signed) RMI-Authentisierungszertifikat** am Gerät. Jedes Gerät enthält eine Konfiguration, welche es erlaubt, ein individuelles RMI-Zertifikat als selbst signiertes TLS-/X.509-Zertifikat zu erstellen. Die Abbildungen im nachfolgenden Kapitel zeigen die Default-Werte, welche für die einzelnen Zertifikatsfelder verwendet werden.

7.2.3.6.2.2 Parameterabfrage des RMI-Zertifikats [Parameter abfragen \23622]

Abbildung 39: *Aufruf der Parameterabfrage zur Neuerstellung des RMI-Zertifikats*

Über diesen Menüpunkt setzt der ADMIN **die Parameter des RMI-Authentisierungszertifikats** am Gerät.
Dieser Menüpunkt bietet eine Alternative zum „Worldline Self-Signed Zertifikat“, welche den ADMIN per Benutzerdialog führt, um die notwendigen Zertifikatsfeldinhalte, u.a. die Organisation, Common Name (CN) sowie die Angaben zur zeitlichen Gültigkeit (NotBefore bzw. NotAfter), am Terminal einzugeben. Abschließend generiert das Terminal ein TLS/X.509-Zertifikat.

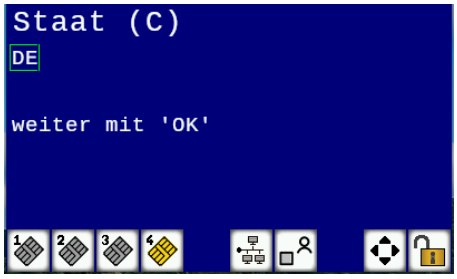


Abbildung 40: *Parameterabfrage „Staat“ (Country) zur Neuerstellung des RMI-Zertifikats (1/10)*

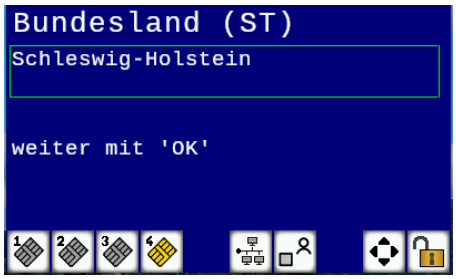


Abbildung 41: *Parameterabfrage „Bundesland“ (State) zur Neuerstellung des RMI-Zertifikats (2/10)*

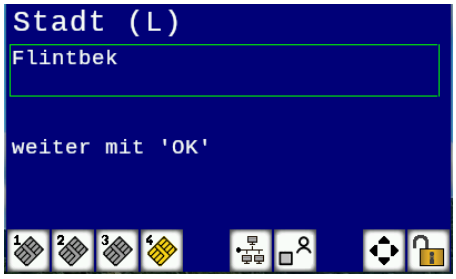


Abbildung 42: *Parameterabfrage „Stadt“ zur Neuerstellung des RMI-Zertifikats (3/10)*

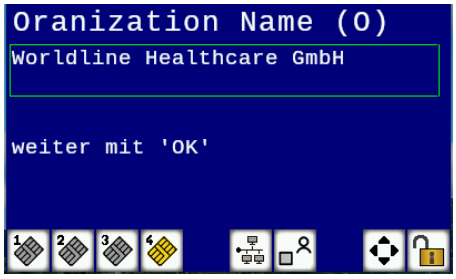


Abbildung 43: *Parameterabfrage „Organization Name“ (Organisation) zur Neuerstellung des RMI-Zertifikats(4/10)*

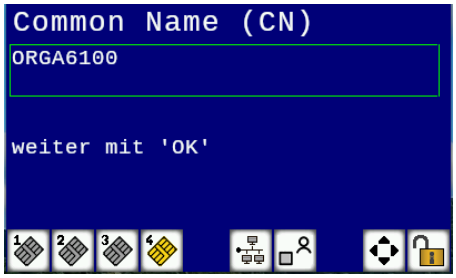


Abbildung 44: *Parameterabfrage „Common Name“ zur Neuerstellung des RMI-Zertifikats (5/10)*

Abbildung 45: *Parameterabfrage „E-mail“ (E-Mail-Adresse) zur Neuerstellung des RMI-Zertifikats (6/10)*

Abbildung 46: *Parameterabfrage „Not Before“ (Startdatum) zur Neuerstellung des RMI-Zertifikats (7/10)*

Abbildung 47: *Parameterabfrage „Not After“ (Enddatum) zur Neuerstellung des RMI-Zertifikats (8/10)*

Abbildung 48: *Prozessstatus während der Neuerstellung des RMI-Zertifikats (1/2)*

Abbildung 49: *Prozessstatus während der Neuerstellung des RMI-Zertifikats (2/2)*

7.2.3.6.2.3 RMI-Zertifikat Parameter Import [Parameter Import via USB\23623]

Über diesen Menüpunkt lädt der ADMIN eine **Konfigurationsdatei** von einem eingesteckten USB-Stick mit den **Parametern des RMI-Authentisierungszertifikats** ins Gerät. Die Konfigurationsdatei übergibt die notwendigen Zertifikatsfeldinhalte, u.a. den Issuer, Common Name (CN) sowie die Angaben zur zeitlichen Gültigkeit (NotBefore bzw. NotAfter). Abschließend generiert das Terminal ein TLS/X.509-Zertifikat.

7.2.3.6.3 CSR für RMI-Zertifikat erstellen [Zertifikatsanfrage erstellen \2363]

Über diesen Menüpunkt generiert der ADMIN einen **Certificate Signing Request (CSR) für** das RMI-**Authentisierungszertifikat** am Gerät. Der vom Terminal erstellte CSR wird als QR-Code am Terminal-Display angezeigt.
Der CSR kann dann entweder nach QR-Aufnahme oder alternativ per RMI-Abfrage in eine eigene PKI übertragen werden, um ein neu erstelltes TLS/X.509-Zertifikat zu signieren, und abschließend entweder über per USB-Stick oder via RMI in das Gerät zu importieren.

7.2.3.6.4 Import des signed RMI-Zertifikats [Zertifikat importieren \2364]

Über diesen Menüpunkt importiert der ADMIN das per externer PKI signierte **RMI-Authentisierungs-zertifikat ü**ber einen eingesteckten USB-Stick in das Gerät. Alternativ kann auch ein Import via RMI erfolgen.

7.2.4. Einstellen der Uhrzeit [Zeit \241]

	Zeit / Datum	**\24**	*Kurzbeschreibung*
1	Zeit	\241	*NTP: Anzeige der via NTP empfangenen Uhrzeit*
2	Datum	\242	*NTP: Anzeige des via NTP empfangenen Datums*

Tabelle 15: *Menü Zeit / Datum*

7.2.4.1 Einstellen der Zeit [Zeit \241]

Im Menü [**Zeit \241**] ist in der vorliegenden Firmware-Version 3.9.0 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 58). 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 \241**] eingesehen, aber nicht verändert werden.

7.2.4.2 Einstellen des Datums [Datum \242]

Im Menü [**Datum \24**] ist in der vorliegenden Firmware-Version 3.9.0 das manuelle Einstellen des Datums 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 58). 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 \242**] 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.

	Sprache	**\25**	*Kurzbeschreibung*
1	Deutsch	\251	*Umschaltung aller Standard-/Menütexte auf deutsche Sprache*
2	Englisch	\252	*Umschaltung aller Standard-/Menütexte auf englische Sprache*
3	Französisch	\253	*Umschaltung aller Standard-/Menütexte auf französische Sprache.*

Tabelle 16: *Menü Sprache*

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.

	Display	**\26**	*Kurzbeschreibung*
1	Freier Text	\261	*Konfiguration der Textmeldung für den Ruhebildschirm (idle text message)*
2	Helligkeit	\262	*Konfiguration der Display-Helligkeit*
3	Hintergrundfarbe	\263	*Konfiguration der Display-Hintergrundfarbeinstellung*
4	gSMC-KT Warnmeldung	\264	*Konfiguration der Warnmeldefunktion für den Fall einer ablaufenden gSMC-KT*

Tabelle 17: *Menü Display*

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 12 und im Abschnitt 4.1 Tastatur auf Seite 35 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.

7.2.6.4. Einstellen der Hintergrundfarbe [Hintergrundfarbe \264]

Um eine wiederkehrende Display-Warnung im Fall einer abzulaufenden gSMC-KT-Gültigkeit zu unterdrücken, kann der Administrator diese Funktion aufrufen.

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.

	Töne	**\27**	*Kurzbeschreibung*
1	Tastenklick	\271	*Aktivieren/Deaktivieren des akustischen Tastenklicksignals*
2	Akustische SIgnale	\272	*Aktivieren/Deaktivieren akustischer Signale*
3	Start Jingle	\273	*Aktivieren/Deaktivieren der Jingle-Melodie nach dem Neustart.*
4	Lautstärke	\275	*Konfiguration der Lautstärke für Signaltöne*
5	Akustischer PIN Schutz	\276	*Konfiguration der Lautstärke für das Maskierungsgeräusch der sicheren PIN-Eingabe.*

Tabelle 18: *Menü Töne*

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, dass 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.

	Update	**\28**	*Kurzbeschreibung*
1	Dateiname	\281	*Konfiguration des Dateinamens der zu ladenden Image-Datei mit Endung „.dfu“*
2	TFTP Server IP Adresse	\282	*TFTP: Konfiguration der IP-Adresse des TFTP-Servers.*
3	Poll Status	\283	*TFTP mit Steuerfile: Konfiguration für die POLL-Funktion*
4	Poll Window	\284	*TFTP mit Steuerfile: Konfiguration für die POLL-Funktion*
5	Update starten	\285	*Manuelles Auslösen des Download-Vorgangs entweder via TFTP oder vom USB-Stick*

Tabelle 19: *Menü Update*

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 Worldline 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 85).

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 97 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 85) 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
• Initialisierung	**Firmware Update * Bitte warten…**
• Datenübertragung	**Signatur wird geprüft ... Update wird eingelesen ...**
• Verifikation abgeschlossen	**Signatur ist gültig**
• Migration der Konfiguration	**Konfiguration wird vorbereitet... * Konfiguration wird migriert...**
• Übernahme der FW in den Systemspeicher	**Update wird durchgeführt...**
• FW erfolgreich in den Systemspeicher übernommen	**Update wird abgeschlossen... * Vorgang erfolgreich**
• Aktivierung der FW per Geräteneustart	**Neustart**

* Die Meldungen erscheinen nur für einen sehr kurzen Augenblick.

Tabelle 20*: 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. Entfernen Sie ggf. den USB-A-Stecker des Zubehörs ORGA Protect, um diesen nach Entfernen des USB-Sticks wieder einzustecken.

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 82).

7.2.9.2.2. Durchführung der Firmware-Aktualisierung per USB-Stick

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.

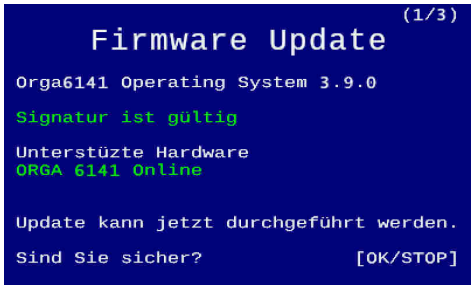
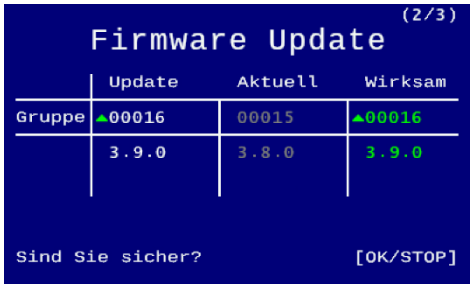
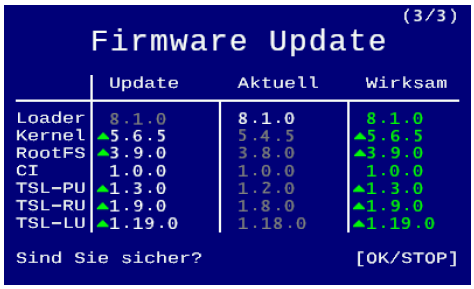


Abbildung 50: *Informationen über die Update-Datei (1/3)*



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.

Abbildung 51: *Informationen über die Update-Datei (2/3)*



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 54 angezeigt.

Abbildung 52: *Informationen über die Update-Datei (3/3)*

Mit den Cursortasten ◀ und ▶ können Sie sich weitere Informationen, wie in Abbildung 52: ***Informationen über die Update-Datei (2/3)*** und Abbildung 50 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 muss dem eingestellten Namen im eHealth-Terminal im Menü [**Dateiname \281**] entsprechen (siehe Abschnitt 7.2.9.5. Firmware-Update: [Dateiname \281] auf Seite 82).
- 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 82).

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 76 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 nächstfolgende 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 ...** **Update wird eingelesen ...**
2. Verifikation abgeschlossen	**Signatur ist gültig**
3. Benutzerdialog	**Update kann jetzt durchgeführt werden.** **Sind Sie sicher? [OK/STOP]**
4. Migration der Konfiguration	**Konfiguration wird vorbereitet... *** **Konfiguration wird migriert...**
5. Übernahme der FW in den Systemspeicher	**Update wird durchgeführt...**
6. FW erfolgreich in den Systemspeicher übernommen	**Update wird abgeschlossen... *** **Vorgang erfolgreich**
7. Aktivierung der FW per Geräteneustart	**Neustart**

* Die Meldungen erscheinen nur für einen sehr kurzen Augenblick.

Tabelle 21: *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 muss dem eingestellten Namen im eHealth-Terminal im Menü [Dateiname \281] entsprechen (siehe Abschnitt 7.2.9.5. Firmware-Update: [Dateiname \281] auf Seite 82).
- 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 82).
- 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 82).

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 22 dargestellten Steuerworte darf jeweils nur einmal je Steuerdatei erfolgen.

Steuerwort	Wertebereich / Format	Mandatory / Obtional	Beschreibung
updateid	< 1 bis 32 Zeichen lange Update – ID> 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. Es werden max. 32 Zeichen übernommen. Die Angabe der <updateid> MUSS in dem Steuerfile vorhanden sein.
updatefile	<1 bis 32 Zeichen langer Dateiname> Format: ASCII, alphanumerisch	**O**	Dateiname ohne Pfadangabe. Es werden max. 32 Zeichen übernommen. Fehlende oder leere Angabe bedeutet, den voreingestellten Menü-Parameter zu verwenden.
updatewindow	<1 Zeichen lange Zahl> Wertebereich "0" - "4" 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. Es wird max. 1 Zeichen übernommen. Fehlende oder leere Angabe bedeutet, den voreingestellten Menü-Parameter zu verwenden.

Tabelle 22: *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 23 für die ‚Poll Windows‘ ein und bestätigen Sie die Eingabe mit der ✓ OK-Taste.

Aus dem eingegebenen 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 23: *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 73 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. Worldline 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! Setzen Sie ggf. den ORGA Protect-USB-Stecker wieder ein.

ACHTUNG
Setzen Sie sich bei einem fehlgeschlagenen Update oder bei Zweifeln über den genauen Ablauf des Updates mit der technischen Hotline von Worldline 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 Konfigurationsparameter 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 85) vorzunehmen.

Die einzuhaltenden Updateschritte und -vorschriften sind dieselben wie die ab dem vorherigen Abschnitt 7.2.9.2. Firmware Update per USB-Stick (Pull-Verfahren) 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 28.

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 7.3.7.7. QR-Code: [Service/Einstellungen \377] auf Seite 98 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 41 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	3.9.0
Firmware Datum	<dd.mm.yyyy>
Firmware Gruppe	00021:<V3.9.0>
Hardware-Version	1.2.0 oder 2.0.0
Hersteller-ID	INGHC
Produktkürzel	ORGA6100
Produktversion	3.9.0:1.2.0 oder 3.9.0:2.0.0
Produkttype	KT
Produkttyp Version	1.8.0
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 *** Konfigurationsparameter - per Konfigurationsparameter-Update veränderlich	

Tabelle 24: *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 95 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 3 3 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 Worldline Healthcare (Reset Administrator) einen Freischaltcode bekommen, um anschließend eine neue Admin-PIN zu vergeben. Setzen Sie sich bitte hierzu mit der Service-Hotline von Worldline Healthcare in Verbindung.

HINWEIS
Setzen Sie sich mit der Service-Hotline von Worldline Healthcare in Verbindung, wenn Sie Ihre Admin-PIN vergessen haben. Worldline 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]

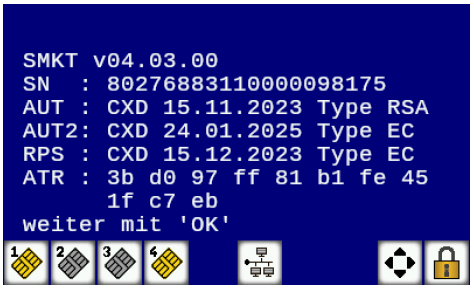


Abbildung 53:
Darstellung der Kartendetails einer gSMC-KT in Slot 4

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 Authentizität- und Integritätsprüfung der gSMC-KT (siehe Abschnitt 5.6 Authentizitäts- und Integritätsprüfung der gSMC-KT auf Seite 43).

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 87.

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 Worldline Healthcare.

HINWEIS
Weitere Informationen zum Integritätstest entnehmen Sie dem Abschnitt 2.2.5 Integritätsprüfung auf Seite 22 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.

7.3.6. Konfiguration via USB-Stick im- und exportieren

Das ORGA 6141 online mit der neusten Firmwareversion 3.9.0 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 seit der Firmware 3.8.x als „Key-Value“-Paare zeilenweise in der Datei gespeichert. Als Trennzeichen wird ein Gleichheitszeichen verwenden.

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

Dieses Format wird für den Konfigurations-Import auch weiterhin durch die Firmware 3.9.0 unterstützt. Der Datenexport erfolgt ab der FW 3.9.0 in einem neuen Format, welches auch eine umfangreiche Erweiterung des Konfigurationsimportes mit sich bringt und in der Syntax bzw. der Namensgebung der Parameter an das Remote-Management-Interface (RMI) angelehnt ist.

Beispiel: **net_vpn_server_gateway="vpngw-dev.ihcdev.de"**

Eine ausführliche Information über die erweiterten Möglichkeiten des neuen USB-Konfigurationsdaten-Imports und Exports finden Sie in Kapitel „Ablauf des USB - Import / Export“ des VPN-Tutorials bzw. in Kapitel „VPN“ der Remote-Management-Interface Beschreibung.

Entnehmen Sie der Tabelle 25 und Tabelle 26 die unterstützten Parameter der Im- und Exportdateien sowie der Tests, die beim Import der Parameter einer Konfigurationsdatei durchgeführt werden.

ACHTUNG
Wenn das Gerät über das Zubehör ORGA Protect verfügt, entfernen Sie dessen USB-Stecker vom Masseanschlusskabel aus der USB-A-Buchse.
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!
Setzen Sie, wenn vorhanden, den ORGA Protect-USB-Stecker wieder ein.

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 Konfigurationsdatei 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 25: *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. Jedes Oktett muss im Zahlenbereich 0-255 liegen.
IP / URL	Der Wert des Parameters kann einer gültigen IP entsprechen, siehe ‚IP‘. 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 26: *Tests beim Import einer Konfigurationsdatei*

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.

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

Drücken Sie die Ziffern 3 6 [**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 53), 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

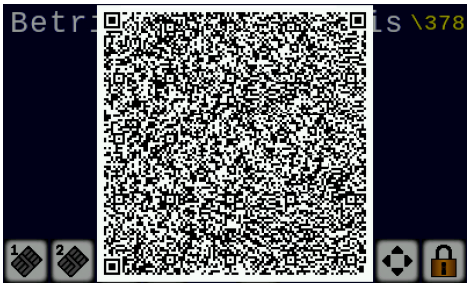


Abbildung 54:
QR-Code zum Auslesen von Terminal Konfigurationen und Betriebszuständen

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 Worldline Healthcare: www.worldline.com/de/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 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 27: *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 Worldline 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 Status (Terminalselbstauskunft)
serial	Seriennummer	01410000005AAC
prod	Produkt Name	ORGA 6141 online
prodver	Produkt Version	1.2.1
fw	Firmware Version	3.9.0
fwdate	Firmware Datum	2022-05-17
fwgrpid	Firmware Gruppen-ID	13
fwgrp	Firmware Gruppe	3.8.0 3.7.5 3.7.4
hw	Hardware Version	1.2.0 oder 2.0.0
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 28: *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 12 beschriebenen Tastenkombinationen abrufen können:

Index:	Bedeutung:	Beispiel/Beschreibung
grp	Bezeichnung der Zusammenfassung	status_fkeys 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 29: *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 vpngate vpnuser vpnstat	VPN-Tunnel VPN-Gateway Adr. Benutzername der Zugangsdaten VPN Status	false ipsec-gw.de ORGA6141-DEMO vpn isn't active
ntp ipntp tz	NTP Client NTP-Server Timezone	true 192.168.221.1 MEZ-1MEZ-2,M3.5.0,M10.5.0

Tabelle 30: *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 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 31: *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 32: *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 33: *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
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

Index:	Bedeutung:	Wert:
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
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 34: *URL-Informationen des QR-Codes: [Betriebsdaten/Statistik \378]*

ANHANG:
Technische Daten

Spannungsversorgung:	Über USB: 500mA Netzteil: 1.000 mA
Display	Farbdisplay mit 400x240 Pixel
Tastatur	Tastenmatrix 16 + 4 Tasten
Kartenspannung	alle Kontaktiereinheiten: A, B, C 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) 2 Stück (SAM PUSH-PUSH ID-000)
Temperaturbereich: Betriebsumgebung Transport und Lagerung	 +5°C bis +40°C -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 35: *Technische Daten*

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

Musteranschreiben einer gSMC-KT

WORLDLINE

Personalisierungsdaten dieser gSMC-KT (G 2.1):

- Kartenkennnummer als Barcode (ICCSN)
- Kartenkennnummer als QR-Code (ICCSN)
- Gültigkeitsdatum der Zertifikate auf der gSMC-KT (G 2.1)

gSMC-KT Karte (G 2.1)
für stationäre eHealth-Kartenterminals

online

Sehr geehrte Anwenderin, sehr geehrter Anwender,

diese gSMC-KT Karte (G 2.1) ist der Schlüssel zur sicheren Verbindung Ihres stationären Worldline (ehemals Ingenico) eHealth-Kartenterminal der Geräteserien ORGA 6141 online und ORGA Mint mit der Online-Telematik-infrastruktur in Ihrer IT-Umgebung.

Bitte prüfen Sie - vor Einsatz der gSMC-KT in das eHealth-Kartenterminal - zunächst die Aktualität der Geräte-firmware und beachten Sie die Sicherheitshinweise in der Bedienungsanleitung des Kartenterminals.

Die aktuellste Version der Bedienungsanleitung zum Kartenterminal sowie der Firmware können Sie unter folgender URL-Adresse herunterladen:

https://www.worldline.com/de/healthcare/download-center

Weitere wichtige Informationen über die sichere Inbetriebnahme Ihres eHealth-Kartenterminals im Online-Produktivbetrieb finden Sie ebenfalls auf unserer Homepage:

https://www.worldline.com/de/healthcare

Achtung!

- Prüfen Sie vor Einsatz einer gSMC-KT Karte in einem Kartenterminal immer erst die Integrität und Authentizität der Karte.
- Bitte beachten Sie für den Fall, dass Ihr Kartenterminal über eine Firmware kleiner / gleich Version 3.8.0 verfügt, das das Kartenterminal für den Gebrauch dieser gSMC-KT Karte (G 2.1) ein Update auf eine höhere Firmware-Version benötigt.
- Verwenden Sie die gSMC-KT nur, wenn Sie sich ganz sicher sind, dass sie aus einer vertrauenswürdigen Quelle stammt.
- Wenden Sie sich bei Fragen oder Zweifeln bezüglich der Integrität der gSMC-KT an den Kartenherausgeber Worldline 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.

Tipp!

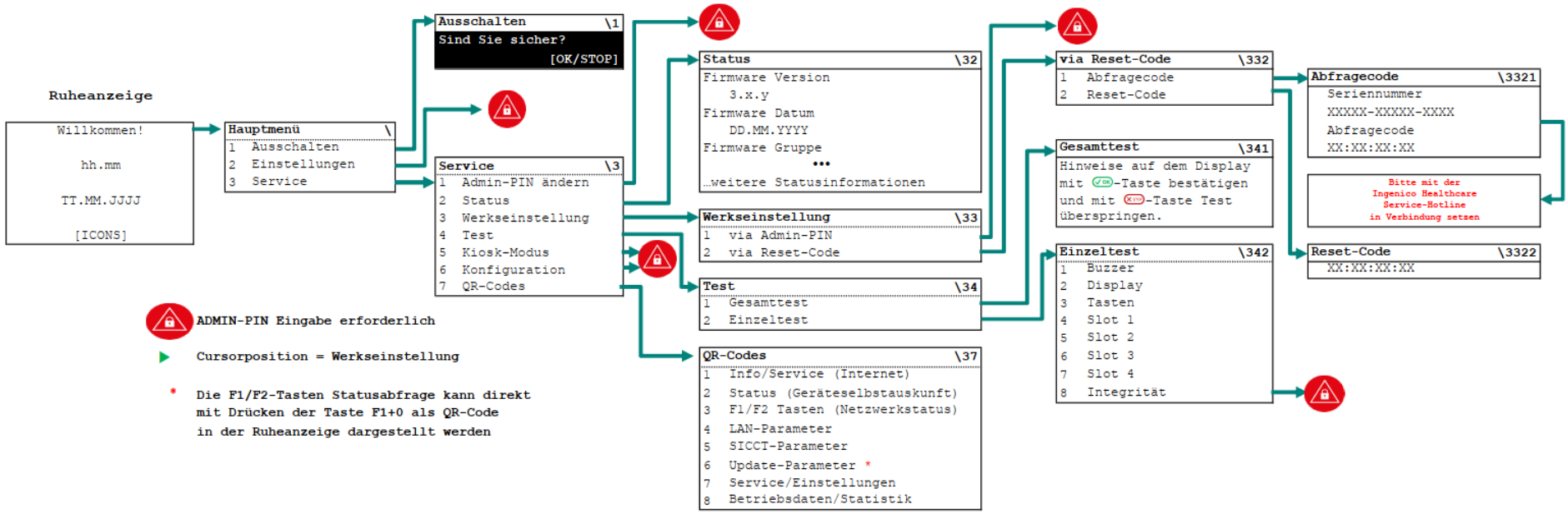
- Nutzen Sie unsere ORGA Service App auf iOS-Basis zur schnellen Dokumentation Ihrer Testergebnisse! Unsere ORGA-Kartenterminals verfügen über eine Funktionalität zur Anzeige einer Vielzahl von Konfigurations-, Ereignis-, Betriebs- und Statistikdaten, die mit Hilfe unserer Service-App sehr komfortabel über einen QR-Code ausgelesen, versendet oder auch einfach archiviert werden können.
- Die aktuelle Version der ORGA Service App für aktuelle iOS-Geräte finden Sie im Apple Store.

www.worldline.com/de/healthcare
Worldline Healthcare GmbH . Konrad-Zuse-Ring 1 . D-24220 Flintbek . Tel. +49 (0)434790 111-11
Geschäftsführer: Oliver Neufuß . Mike Uwe Petersen
Sitz der Gesellschaft: Flintbek . HRB NR. 8903 KI . Amtsgericht Kiel . Steuer-Nr. 147/5883/0713 . USt-ID Deutschland: DE252422299
Commerzbank AG Kiel . IBAN-Nr. DE47 2104 0010 0749 0188 00 . BIC: COBADEFFXXX

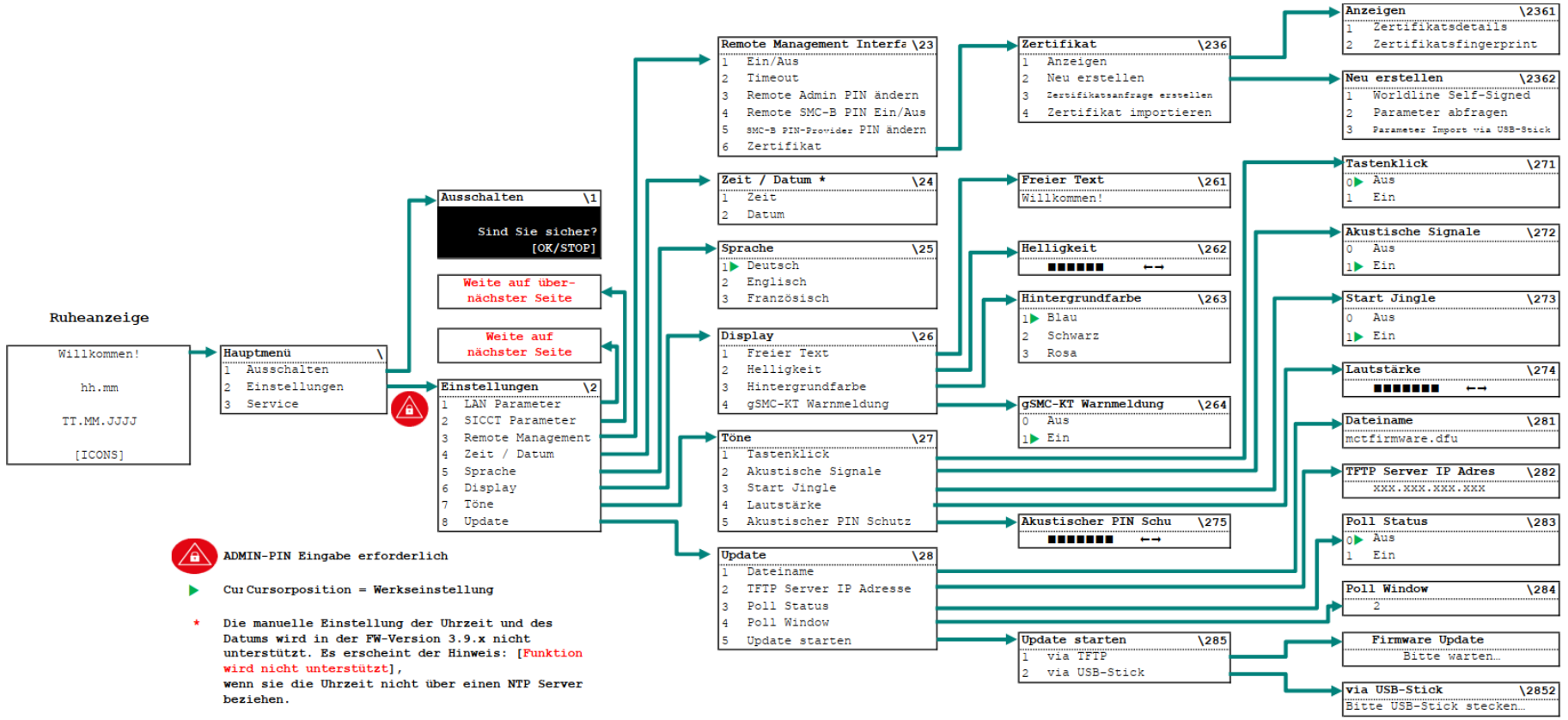
Healthcare

V22.6

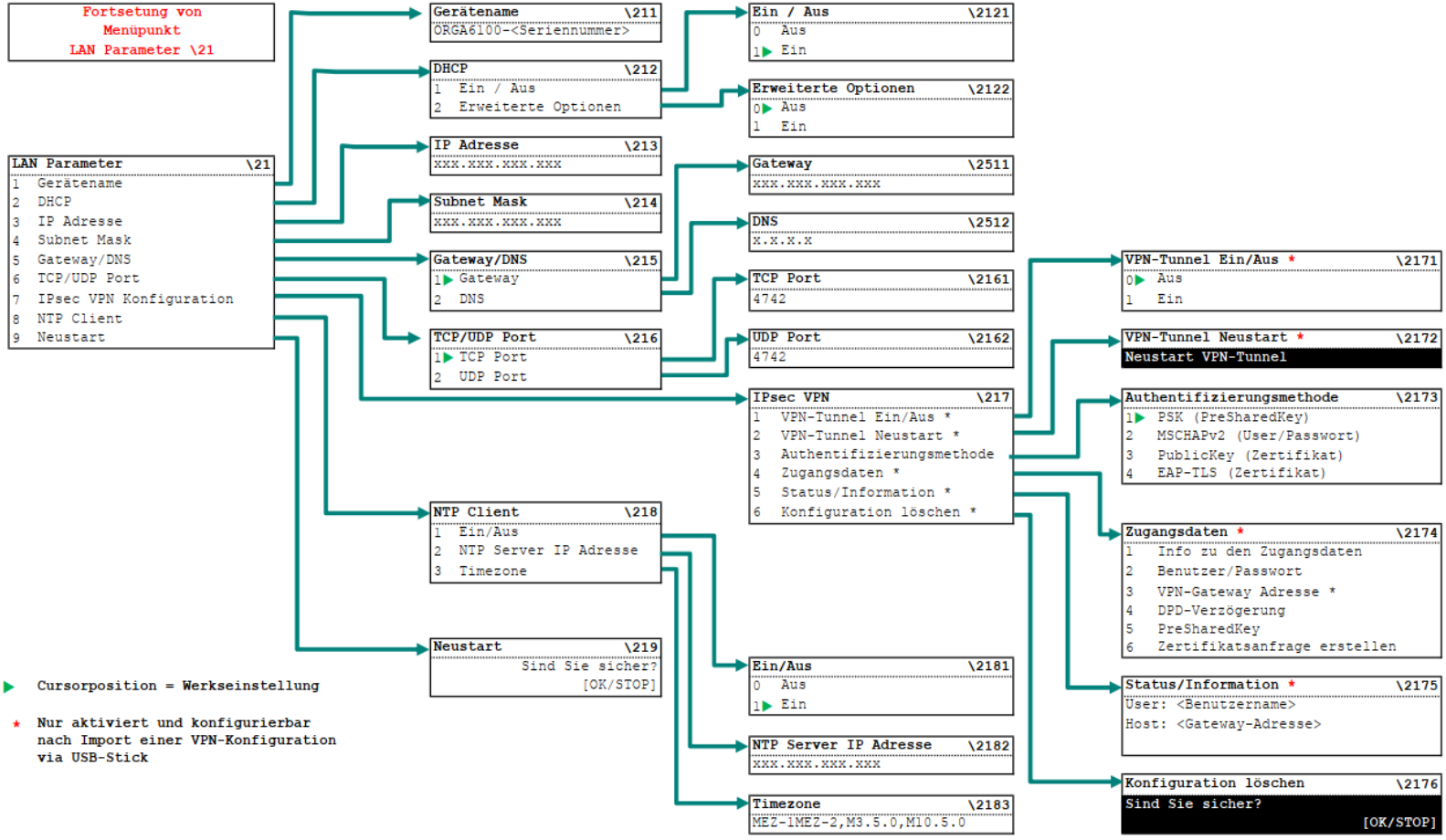
Menüstruktur für den Anwender



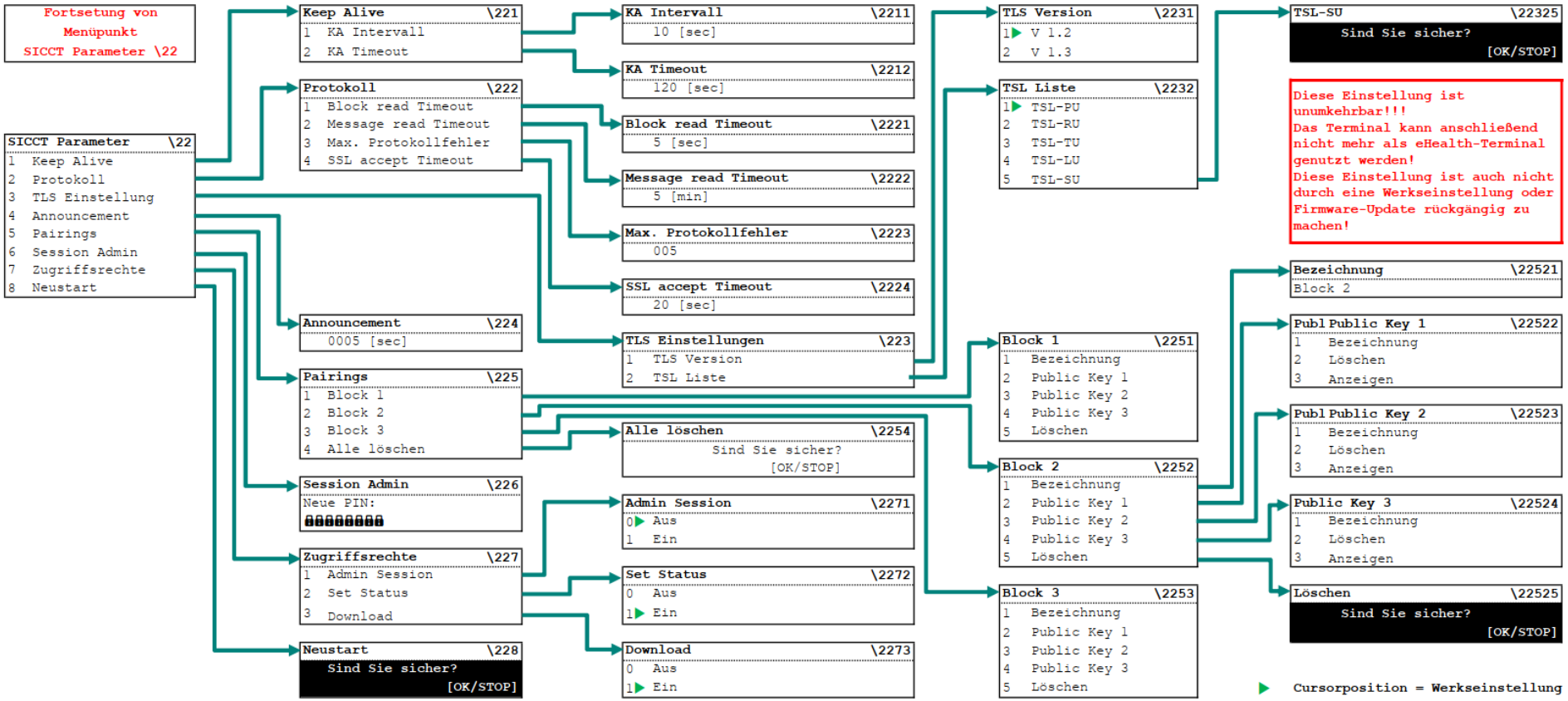
Menüstruktur für den Administrator - Teil 1: Allgemeine Einstellungen



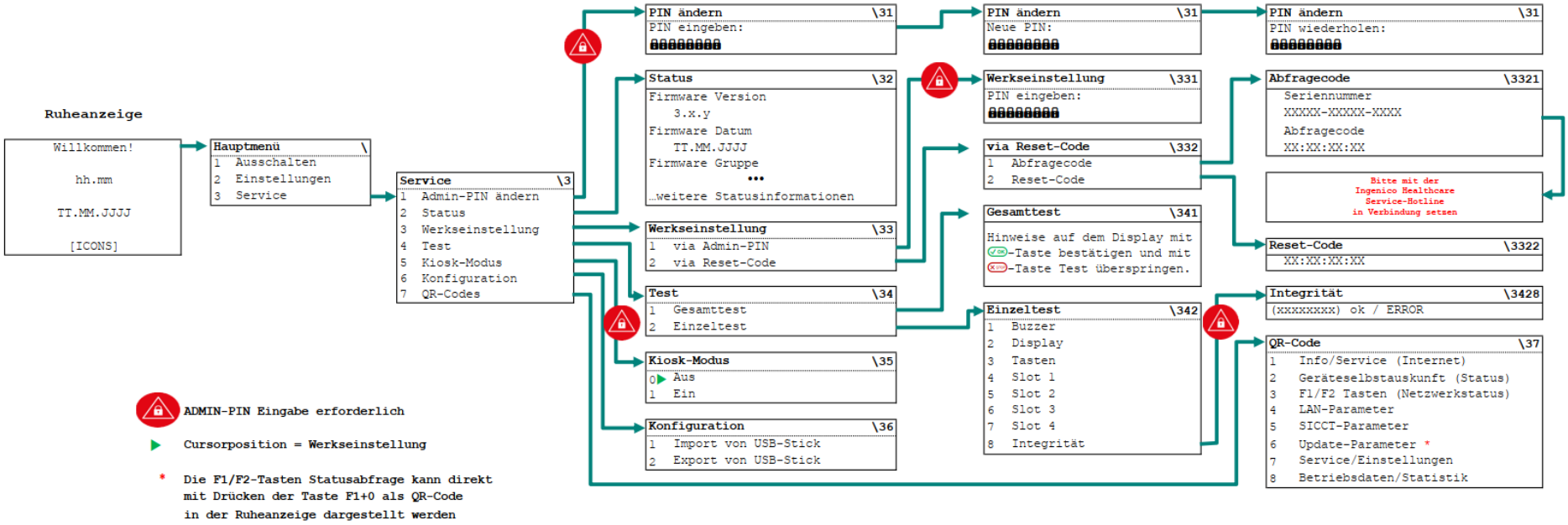
Menüstruktur für den Administrator - Teil 2: LAN Parameter



Menüstruktur für den Administrator - Teil 3: SICCT Parameter



Menüstruktur für den Administrator - Teil 4: Service Einstellungen



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. • Das Gerät wurde manipuliert bzw. es wurde versucht das Gerät zu manipulieren.	• Lesen Sie sich die Sicherheitshinweise im Abschnitt 2. Sicherheit auf Seite 19 durch. • Nehmen Sie das Gerät nicht in Betrieb und setzen Sie sich mit Ihrem Lieferanten in Verbindung. • 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. • Das Gerät ist defekt.	• Versuchen Sie das Gerät durch langes Drücken der OK-Taste einzuschalten. • Senden Sie das Gerät zum Service Ihres Lieferanten ein.
Nach dem Einschalten des Gerätes erscheint der blinkende Hinweis: **Set ADMIN-PIN** •••••••• **Neue PIN:** ••••••••	• Das Gerät ist neu und befindet sich noch im Auslieferungszustand. • 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: **Fehler Integrität.**	• Das Gerät wird bei jedem Einschalten einer Softwareprüfung 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 an Ausgabeposition 8 im Display: 	• Die interne Stützbatterie des Terminals verfügt nur noch über eine geringe Restkapazität. • Wenn die Batterie verbraucht ist, wird automatisch ein Sicherheitsalarm ausgelöst und das Terminal kann nicht mehr genutzt werden.	• Das Terminal muss zeitnah gegen ein neues Gerät getauscht werden.

Tabelle 36: *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: • Die gesteckte eGK ist defekt. • Die Kontaktiereinheit 1 ist verschlissen oder verschmutzt. • Die Karte steckt falsch herum.	• Versuchen Sie eine andere eGK auszulesen, um zu prüfen, ob die Kontaktiereinheit 1 des Gerätes funktioniert. • Führen Sie den Einzeltest für den „Slot 1“ durch. • Senden Sie das Gerät zum Service Ihres Lieferanten ein, falls verschieden Gesundheitskarten nur mit diesem Gerät nicht ausgelesen werden können.

Tabelle 37: *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. • 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 Worldline Healthcare.

Tabelle 38: *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 Worldline 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 39: *Fehlermeldungen und Ursachen - Identification & Authentication*

Fehlermeldungen und Ursachen - Firmware Update		
Typ:	**Mögliche Ursachen**	**Mögliche Lösungen**
Fehler bei der Datenübertragung	• Dateisystem des USB-Sticks beschädigt. • 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). • 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. • Fehler bei Signatur-Prüfung. • 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. • 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). • 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.> TFTP-Abbruch	• Kein TFTP-Server unter der eingestellten IP-Adresse erreichbar.	• TFTP-Server starten. • Firewall Einstellungen kontrollieren. • TFTP-Server IP-Adresse im Terminalmenü kontrollieren.
TFTP-Abbruch Menürückkehr	• Fehler bei der TFTP-Übertragung. • Übertragenes File ist zu groß.	• Geeignete Firmware-Image-Datei auf den TFTP-Server kopieren.
Ungültige Firmware	• Firmware-Image-Datei nicht für das Terminal geeignet. • Version der neuen Software ist kleiner als die der Installierten. • 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.

Fehlermeldungen und Ursachen - Firmware Update		
Typ:	**Mögliche Ursachen**	**Mögliche Lösungen**
Update File nicht gefunden!	• Dateiname des FW-Images passt nicht zum eingestellten Namen im Terminalmenü. • FW-Image File liegt nicht im Root Directory des USB-Sticks. • Der beabsichtigte Download-Vorgang wird abgebrochen.	• Name der Firmware-Image-Datei auf dem USB-Stick an erwarteten Updatenamen anpassen. • Firmware-Image-Datei in das Root Directory des USB-Sticks kopieren.
Update File zu groß!	• FW-Image nicht für das Terminal geeignet. • 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. • Der USB-Stick wurde vom Terminal nicht erkannt. • Der beabsichtigte Download-Vorgang wird abgebrochen.	• USB-Stick ziehen und erneut gesteckt. • Alternativen USB-Stick probieren.

Tabelle 40: *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. • Terminal verwendet statische Netzparameter (u.a. IP-Adresse und Subnet Mask).	• Aktivieren Sie DHCP am Terminal. (siehe Abschnitt 7.2.1.2.1. DHCP: [Ein / Aus \2121] auf Seite 53).
DHCP Server **PREINIT**	• DHCP ist am Terminal aktiviert. • Terminal verwendet DHCP und versucht, eine Kommunikation zu einem DHCP-Server herzustellen.	
DHCP Server **FAIL**	• DHCP ist am Terminal aktiviert. • 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. • Deaktivieren Sie DHCP am Terminal. (siehe Abschnitt 7.2.1.2.1. DHCP: [Ein / Aus \2121] auf Seite 53) und geben Sie anschließend die korrekte IP-Adresse und Subnet Mask des DHCP-Servers manuell ein (siehe Abschnitte 7.2.1.3. LAN-Parameter: [IP-Adresse \213] und 7.2.1.4. LAN-Parameter: [Subnet Mask \214] auf Seite 54).
DHCP Server **BOUND**	• DHCP ist am Terminal aktiviert. • Zustand, nachdem der DHCP-Client des KTs vom DHCP-Server eine IP-Adresse bezogen hatte.	
DHCP Server **RENEW**	• DHCP ist am Terminal aktiviert. • Zustand, nachdem der DHCP-Client des KTs vor Ablauf der Lease-Time vom DHCP-Server eine IP-Adresse bezogen hatte.	

Tabelle 41: *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. • PIN ist auf der Karte bereits gesperrt.	• Geben Sie die PUK der Karte ein. • 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 42: *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 43: *Fehlermeldungen und Ursachen – VPN-Verbindung*

Fehlermeldungen und Ursachen - Sonstige		
Typ:	**Mögliche Ursachen**	**Mögliche Lösungen**
Abbruch **Fehlende SMCKT**	• gSMC-KT nicht in Slot 3 oder 4 vorhanden. • Die TCP-Verbindung wird mit einem FIN / ACK beendet.	• Prüfen Sie, ob sich eine gSMC-KT im Slot 3 oder 4 befindet. • Setzen Sie eine gSMC-KT mit gültigen Zertifikaten in den Slot 3 oder 4 ein. (siehe Abschnitt 5.7 auf Seite 45)
Fehler **Integrität**	• Die Software-Integritätsprüfung hat einen Manipulationsversuch festgestellt.	• Setzen Sie sich mit der Service-Hotline von Worldline Healthcare in Verbindung.
SICHERHEITSALARM **Service kontaktieren!**	• Die im Terminal integrierten Schutzmaßnahmen gegen Manipulationsversuche wurden ausgelöst und das Terminal wurde deaktiviert.	• Setzen Sie sich mit der Service-Hotline von Worldline Healthcare in Verbindung.
Remote Admin aktiv	• Es besteht zum Zeitpunkt des Aufrufs der lokalen Admin-PIN-Eingabe ein aktiver Login eines Admins über das Remote Management Interface (RMI), d.h. via Web-Browser oder Terminal-Management-System (TMS).	• Abwarten bis die Remote-Session beendet wurde, um sich dann erneut anzumelden. • Fortsetzung des Admin-Zugriffs über die Direkt-managementschnittstelle zu Kontrollzwecken, d.h. ohne Änderungen oder Aktivierung-en lokal vorzunehmen.

Tabelle 44: *Warnung- und Fehlermeldungen und Ursachen - Sonstige*

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 Worldline Healthcare GmbH angefragt werden.

Die Firmware V3.9.0 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 auf dem SICCT-Grundkonzept zur Kodierung von Ausgabemeldungen (Messages) und gibt einer ansteuernden Instanz (Konnektor oder SAK) die technische Möglichkeit, 2D-Codes durch das Terminal zu 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')

Abbildungsverzeichnis

Tabellenverzeichnis

Originalzubehör zum ORGA 6141 online

Informationen zu allen verfügbaren Originalzubehörprodukten finden Sie entweder auf der Webseite Ihres Händlers/Anbieters oder auf der Herstellerseite:
https://worldline.com/de-de/home/main-navigation/solutions/healthcare/unser-portfolio/stationaeres-zubehoer

Zubehör ORGA Protect - Bestell-Nr. 200753 – für ORGA 6141 online mit HW V1.2.0

Zur Minimierung möglicher ESD-Effekte im Produktivumfeld, hervorgerufen durch Steckvorgänge von Dual-Interface-Karten in den oberen Kartenschlitz wird das optionale Zubehörprodukt ORGA Protect für Betreiber von Bestandsgeräten mit der älteren HW-Version V1.2.0 angeboten.

Betreiber der neuen HW-Version V2.0.0 (aka ORGA Neo) benötigen dieses Zubehör nicht.

Bei diesem Zubehörprodukt handelt es sich um einen auf der Geräteoberseite aufzuklebenden Aufsatz aus leitfähigem Kunststoff für den oberen Kartenslot (SLOT1) zur verbesserten Kartenführung und ESD-Spannungsableitung. Eine außen verlaufende und gut sichtbare Ein-Draht-Kabelverbindung verbindet Aufsatz mit dem notwendigen elektrischen Anschluss an den Masseanschluss der USB-A-Buchse an der Geräteunterseite.

Die Anwendung dieses Schutzzubehörs ist dann angezeigt, wenn das Einstecken von Karten in den oberen Kartenschlitz vermehrt zu einem Einfrieren, Neustart oder einer Beeinträchtigung der Konnektorverbindung z.B. zum fehlerhaften Zugriff auf Karten im Terminal führt.

Weitere Hinweise, Abbildungen und Schritte zur einfachen Installation und zum Betrieb finden Sie auf der Herstellerinternetseite sowie in der dem Zubehör beiliegenden Montageanleitung.
Für Wartungsaktivitäten, wie das Update der Firmware oder Konfigurationsdaten über einen USB-Stick, ist das Ableitkabel temporär von der USB-A-Buchse zu trennen.

Zubehör ORGA Service APP (für iOS)

Die optionale ORGA Service App für iOS-Smart-Devices bietet Funktionen an, um das ORGA 6141 online per QR-Code-Scan dokumentiert in Betrieb zu nehmen, Einstellungen und Betriebsdaten zu analysieren und einheitliche Reports zur Installation, zum Austausch sowie der Konfiguration zu erstellen, welche als PDF- oder CSV-Datei-Export auf dem iOS-Gerät gespeichert werden können.

Die sieben (7) unterschiedlichen QR-Codes, welche das ORGA 6141 online (ab Firmwareversion 3.8.0) generieren kann, ermöglichen es dem Anwender Informationen zu folgenden technischen Gerätedaten aufzunehmen:

- Status,
- F1/F2-Tasten,
- Lan-Parameter,
- SICCT-Parameter,
- Update-Parameter,
- Service / Einstellungen,
- Betriebsdaten / Statistiken.

Des Weiteren können die erstellten Installations-, Austausch- und Fehlerreports nach Kunden/innen und den dort installierten ORGA 6141 online angelegt und gesichert werden.
Weitere Hinweise, Abbildungen sowie den Link zur **ORGA Service App** im Appstore für iOS. finden Sie auf der Herstellerinternetseite:
https://worldline.com/de-de/home/main-navigation/solutions/healthcare/unser-portfolio/applikationen/ORGA-Service-App