
Bedienungsanleitung

Stationäres eHealth Kartenterminal

ORGA 6141 online mit

Firmware-Version 3.7.2



Vorwort

Sehr geehrte Anwenderin, sehr geehrter Anwender,

vielen Dank, dass Sie sich für ein Produkt von Ingenico Healthcare entschieden haben. Diese Bedienungsanleitung beschreibt das stationäre eHealth Kartenterminal ORGA 6141 online. Es ist für den stationären Onlinebetrieb am Konnektor entwickelt. Für diese Anwendungszwecke ist es bestens ausgestattet. Durch sein ergonomisches Design und seine für den Online-Produktivbetrieb durch die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) zugelassene Hard- und Software eignet es sich ausgezeichnet für die vielseitigen Einsatzzwecke in der heutigen und zukünftigen Online-Telematikinfrastuktur des deutschen Gesundheitswesens. Das stationäre ORGA 6141 online Terminal vereinfacht administrative Abläufe bei der Patientendatenerfassung und Übergabe an die von Ihnen verwendete Primärsystemsoftware Ihres EDV Systems.

Im Vergleich zum bisherigen ORGA 6141 mit der Firmware-Version 2.20 ist die Hard- und Software aufgrund neuer Sicherheitsanforderungen der gematik für die Arbeit mit stationären eHealth Kartenterminals im Online-Produktivbetrieb umfangreich überarbeitet worden.

Hierdurch ist z. B. ein direkter Anschluss per USB- oder LAN-Verbindung am Primärsystem in der Online-Telematikinfrastuktur nicht mehr gestattet und wird deswegen auch nicht mehr unterstützt.

In den Geräteeinstellungen lässt sich jederzeit im Menü [**Integrität \3428**] ein Integritätstest des Gerätes durchführen.



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!



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

Ihr Ingenico Healthcare Team

Ingenico Healthcare GmbH
Konrad-Zuse-Ring 1
24220 Flintbek

Tel.: 04347 90 11 111
Internet: www.ingenico.de/healthcare
E-Mail: kontakt.ihc@ingenico.com

Hinweise zur Bedienungsanleitung

Die vorliegende Bedienungsanleitung richtet sich an Leistungserbringer im Gesundheitswesen, das medizinische und pharmazeutische Personal und Administratoren.

Die Bedienungsanleitung beschreibt die Handhabung des stationären eHealth Kartenterminals ORGA 6141 online mit der für den gematik Online-Produktivbetrieb spezifizierten und zugelassenen Firmware-Version 3.7.2.

Sie vermittelt dem Administrator und Anwender notwendige Kenntnisse über Funktion, Installation, Bedienung, Wartung und Entsorgung des Gerätes.

Diese Anleitung beinhaltet alle für eine gefahrlose Benutzung erforderlichen Informationen und gibt bei auftretenden Störungen Hinweise auf mögliche Ursachen und deren Beseitigung.

Einige Menüpunkte und Funktionalitäten der Vorgängerversion (ORGA 6141 mit Firmware 2.20) sind aufgrund neuer Sicherheitsanforderungen der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) für die Arbeit mit stationären eHealth-Kartenterminals im Online-Produktivbetrieb weggefallen und andere sind zum Betreiben des Gerätes am Konnektor in der neuen Betriebsart "eHealth KT" hinzugekommen.

Der Konnektor ist die dezentrale Komponente zur sicheren Anbindung von Clientsystemen der Institutionen (AIS, AVS) und der Kartenterminals im sicheren lokalen Netz (LAN) des Anwenders.

Im LAN der Einsatzumgebung kommuniziert das Clientsystem mit dem Konnektor über dessen LAN-seitiges Ethernet-Interface. Der Konnektor ist anschließend verantwortlich für den Zugriff auf die in der Einsatzumgebung befindlichen Kartenterminals sowie Karten und protokolliert Fehlerzustände.

Der Konnektor regelt die sicheren Kommunikationsbeziehungen zwischen Clientsystem, Kartenterminals, Karten und zentralen Diensten der TI-Plattform sowie fachanwendungsspezifischen Diensten.

Die zwischen den Funktionsmerkmalen der Komponenten bestehenden Wechselwirkungen (u.a. Die Erkennung einer gesteckten Karte im Kartenterminaldienst löst eine Reaktion im Konnektor-Kartendienst aus) werden hierzu durch den Konnektor-Administrator administrativ konfiguriert und müssen zur Gewähr eines sicheren Betriebs des Kartenterminals ebenfalls zyklisch überprüft und gepflegt werden.

Die Managementschnittstelle des Konnektor ermöglicht es dem (Konnektor-) Administrator, die Liste der verwalteten und verbundenen Kartenterminals einzusehen, den jeweiligen Verbindungsstatus zu kontrollieren sowie zum Firmware-Update eine Firmware-Image Datei an die Kartenterminals zu übertragen.

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 Bedienungsanleitung 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 dazugehörigen Kurztastensequenzen finden Sie im Anhang dieser Bedienungsanleitung auf den Seiten 80 bis 84.



HINWEIS

Eine schnelle Übersicht und Einführung in die verschiedenen Funktionselemente des Gerätes finden Sie im Abschnitt 3 »Produktbeschreibung« auf Seite 35 dieser Bedienungsanleitung.

Copyrights

Copyright © 2017 Ingenico Healthcare GmbH. Alle Rechte vorbehalten.





Alle Produkte oder Dienstleistungen, die in diesem Dokument genannt werden, sind Marken, Dienstleistungsmarken, eingetragene Marken oder eingetragene Dienstleistungsmarken der entsprechenden Eigentümer.



Kein Teil dieser Veröffentlichung darf ohne schriftliche Genehmigung der Ingenico Healthcare GmbH kopiert, gesendet, übertragen, elektronisch gespeichert oder in eine andere Sprache übersetzt werden. Diese Bedienungsanleitung dient der allgemeinen Information und stellt keine technische Spezifikation dar.

Die Ingenico Healthcare GmbH behält sich das Recht auf die Änderung von Funktionen, Eigenschaften und technischen Angaben zu jeder Zeit und ohne vorherige Benachrichtigung vor.

Versionsstand / Selbstauskunft des Terminals

Sie können den Versionsstand der Firmware Ihres Gerätes wie folgt ablesen:

Verbinden Sie das Gerät mit dem beiliegenden Netzteil mit dem Stromnetz. Das Gerät startet daraufhin automatisch. Sollte das Gerät bereits mit dem Stromnetz verbunden aber ausgeschaltet sein, können Sie das Gerät durch Drücken der -Taste einschalten. Sobald der Ruhebildschirm angezeigt wird, drücken Sie auf die -Taste um ins Hauptmenü zu gelangen. Anschließend wählen Sie das Menü [**Service** \3] durch zwei Mal Drücken auf die -Taste und anschließend Betätigen der -Taste.

Verfahren Sie genau so bei der Wahl des Menüs [**Status** \32]: Einmal Drücken auf die -Taste gefolgt von einem Druck auf die -Taste.

Mit den Cursor-Tasten  und  können Sie alle Informationen über das Gerät abrufen.

Inhaltsverzeichnis

Vorwort.....	2
Hinweise zur Bedienungsanleitung.....	3
Copyrights.....	4
Versionsstand / Selbstauskunft des Terminals	5
Kapitel 1: Allgemeine Informationen vor Inbetriebnahme	11
1. Einführung.....	11
1.1. Verwendete Symbole und Signalwörter.....	11
1.2. Prüfung der sicheren Anlieferung des eHealth Terminals auf einem vertrauenswürdigen Lieferweg.....	12
1.3. Lieferumfang	12
1.4. Funktionen der verschiedene Tasten des Gerätes	13
1.5. Displaysymbole und ihre Bedeutung.....	16
1.5.1. Symbol 1 bis 4: Karten-Kontaktiereinheiten	16
1.5.2. Symbol 6: Datenverkehr zu angeschlossenen Geräten.....	17
1.5.3. Symbol 7: Interne Stützbatterie schwach	17
1.5.4. Symbol 9: Allgemeiner Gerätestatus.....	17
1.5.5. Symbol 10: Datenverwaltung.....	17
1.6. Begriffsbestimmung.....	18
2. Sicherheit	20
2.1. Gerätesicherheit.....	20
2.2. Sicherheitsmerkmale	20
2.2.1. Das Gehäusesiegel und seine Eigenschaften	20
2.2.2. Das Slotsiegel und seine Eigenschaften.....	22
2.2.3. Tägliches Prüfen der Gehäuse- und Slotsiegel	23
2.2.4. Geräteversion	24
2.2.5. Integritätsprüfung.....	24
2.2.6. Typenschild.....	24
2.3. Sicherheit bei der Inbetriebnahme.....	25
2.3.1. Aufstellungshinweise.....	25
2.3.2. Admin-PIN Eingabe bei der Inbetriebnahme	25
2.3.3. Eingabe einer Karten PIN nach Aufforderung.....	25
2.3.3.1. Der sichere PIN Eingabe Modus.....	26
2.3.3.2. Fehlerfreier Ablauf	26
2.3.3.3. Ablauf bei inkorrekt Karten PIN Eingabe.....	26
2.3.3.4. Ablauf bei Abbruch der Karten PIN Eingabe durch den Benutzer	27

2.3.3.5.	Ablauf im Fall von Zeitüberschreitung bei Eingabe der Karten PIN	27
2.4.	Logging und Änderungsprotokollierung	27
2.5.	Sicherheit bei der Außerbetriebnahme und im Reparaturfall	27
2.6.	Normen und Richtlinien	29
2.7.	Temperatur / Umgebungsbedingungen	29
2.8.	Allgemeine Regeln & Anforderungen zur Betriebssicherheit des Gerätes	30
2.9.	Sicherheit beim Anschluss an den Konnektor	33
2.10.	Reinigung und Pflege	33
2.11.	Desinfektion	33
2.12.	Entsorgung des Gerätes	34
Kapitel 2:	Bedienungsanleitung für den Benutzer	35
3.	Produktbeschreibung	35
3.1.	Die Vorderseite des ORGA 6141 online	35
3.2.	Die Rückseite des ORGA 6141 online	36
3.3.	Die Kontaktiereinheiten 3 und 4 für die SMC-Karten	36
4.	Bedienung des Gerätes	37
4.1.	Tastatur	37
4.2.	Ein- und Ausschalten des Gerätes	37
4.3.	Aufbau des Grafikdisplays	38
4.4.	Der Ruhebildschirm	38
4.5.	Menü-Navigation	39
4.6.	Das Hauptmenü	39
4.7.	Einstecken einer eGK in die Kontaktiereinheit 1	40
4.8.	Einstecken eines HBA in die Kontaktiereinheit 2	40
4.9.	Patientendatensatz einlesen	41
Kapitel 3:	Bedienungsanleitung für den Administrator	42
5.	Inbetriebnahme	42
5.1.	Das erste Einschalten des Gerätes	42
5.2.	Admin-PIN Eingabe bei der ersten Inbetriebnahme	42
5.3.	Admin-PIN Zeitsperre	43
5.4.	Neue PIN anfordern	43
5.5.	Werksvoreinstellungen	44
5.6.	Authentizitäts- und Integritätsprüfung der gSMC-KT	45
5.7.	Einsetzen einer SMC-Karte und Versiegeln der Kontaktiereinheiten 3 und 4	46
5.8.	Verbindung des Gerätes über eine LAN-Verbindung mit dem Konnektor	48
5.9.	Initiales Pairing des Terminals mit dem Konnektor	49

6.	Die Menüoptionen (direkte Managementschnittstelle) für den Administrator im Detail.....	51
6.1.	Ausschalten des Gerätes [Ausschalten \1].....	51
6.2.	Der Menüpunkt Einstellungen [Einstellungen \2].....	51
6.2.1.	Die Konfiguration im lokalen Netzwerk [LAN Parameter \21].....	51
6.2.1.1.	LAN Parameter: [Gerätename \211].....	52
6.2.1.2.	LAN Parameter: [DHCP \212].....	52
6.2.1.2.1.	DHCP: [Ein / Aus \2121].....	52
6.2.1.2.2.	DHCP: [Erw. Optionen \2122].....	52
6.2.1.3.	LAN Parameter: [IP Adresse \213].....	52
6.2.1.4.	LAN Parameter: [Subnet Mask \214].....	53
6.2.1.5.	LAN Parameter: [Gateway \215].....	53
6.2.1.6.	LAN Parameter: [TCP Port \216].....	53
6.2.1.7.	LAN Parameter: [UDP Port \217].....	53
6.2.1.8.	LAN Parameter: [NTP Server \218].....	53
6.2.1.8.1.	NTP Server: [IP Adresse \2181].....	54
6.2.1.8.2.	NTP Server: [Timeout \2182].....	54
6.2.1.8.3.	NTP Server: [Timezone \2183].....	54
6.2.1.9.	LAN Parameter: [Neustart \219].....	54
6.2.2.	Die Konfiguration der SICCT Parameter [SICCT Parameter \22].....	54
6.2.2.1.	SICCT - Grundsätzliche Funktionsweise.....	55
6.2.2.2.	SICCT Parameter: [Keep Alive \221].....	55
6.2.2.2.1.	Keep Alive: [KA Intervall \2211].....	55
6.2.2.2.2.	Keep Alive: [KA Timeout \2212].....	55
6.2.2.3.	SICCT Parameter: [Protokoll \222].....	55
6.2.2.3.1.	Protokoll: [Block read Timeout \2221].....	55
6.2.2.3.2.	Protokoll: [Message read Timeout \2222].....	55
6.2.2.3.3.	Protokoll: [Max. Protokollfehler \2223].....	56
6.2.2.3.4.	Protokoll: [SSL accept Timeout \2224].....	56
6.2.2.4.	SICCT Parameter: [TLS Einstellung \223].....	56
6.2.2.4.1.	TLS Einstellungen: [TLS Version \2231].....	56
6.2.2.4.2.	TLS Einstellungen: [TSL Liste \2232].....	56
6.2.2.5.	SICCT Parameter: [Announcement \224].....	57
6.2.2.6.	SICCT Parameter: [Pairings \225].....	57
6.2.2.7.	SICCT Parameter: [Session Admin \226] (zweite Managementschnittstelle).....	57
6.2.2.8.	SICCT Parameter: [Zugriffsrechte \227].....	58
6.2.2.8.1.	Zugriffsrechte: [Admin Session \2271].....	58

6.2.2.8.2. Zugriffsrechte: [Set Status \2272].....	58
6.2.2.8.3. Zugriffsrechte: [Download \2273]	59
6.2.2.9. SICCT Parameter: [Neustart \228].....	59
6.2.3. Einstellen der Uhrzeit [Zeit \23]	59
6.2.4. Einstellen des Datums [Datum \24]	59
6.2.5. Einstellen der Menüsprache [Sprache \25].....	60
6.2.6. Einstellen der Displayanzeige [Display \26]	60
6.2.6.1. Individueller Text im Ruhebildschirm [Freier Text \261].....	60
6.2.6.2. Einstellen der Displayhelligkeit [Helligkeit \262]	60
6.2.6.3. Einstellen der Hintergrundfarbe [Hintergrundfarbe \263]	60
6.2.7. Einstellen der Signaltöne [Töne \27]	61
6.2.8. Einstellen des akustischen PIN Schutzes [Akustischer PIN Schutz \275].....	61
6.2.9. Durchführung eines Firmware-Updates [Update \28].....	61
6.2.9.1. Firmware Update via Konnektor	62
6.2.9.2. Firmware Update per USB-Stick (Pull-Verfahren)	63
6.2.9.2.1. Voraussetzungen zur Durchführung des Update.....	64
6.2.9.2.2. Durchführung der Firmware-Aktualisierung per USB-Stick	64
6.2.9.3. Firmware Update per TFTP-Server (Pull-Verfahren)	65
6.2.9.3.1. Voraussetzungen zur Durchführung des Update.....	65
6.2.9.3.2. Durchführung der Firmwareaktualisierung via TFTP Server im Pull-Verfahren..	65
6.2.9.4. Firmware Update per Steuerfile am TFTP Server (Push Verfahren).....	66
6.2.9.4.1. Voraussetzungen zur Durchführung des Update.....	67
6.2.9.4.2. Syntax der Steuerdatei.....	67
6.2.9.4.3. Einstellmöglichkeiten über [Poll Window \284]	69
6.2.9.4.4. Durchführung der Firmware-Aktualisierung via TFTP Server im Push-Verfahren	69
6.2.9.5. Firmware-Update: [Dateiname \281]	69
6.2.9.6. Firmware-Update: [TFTP Server IP Adresse \282]	70
6.2.9.7. Firmware-Update: [Poll Status \283]	70
6.2.9.8. Firmware-Update: [Update starten \285].....	70
6.2.10. Durchführung eines Updates der Konfigurationsparameter [Update \28]	71
6.3. Der Menüpunkt Service [Service \3]	72
6.3.1. Ändern der Admin-PIN [PIN ändern \31]	72
6.3.2. Die Terminalselbstauskunft [Status \32].....	72
6.3.3. Zurücksetzen des Terminals in den Auslieferungszustand [Werkseinstellung \33]..	73
6.3.3.1. Zurücksetzen des Terminals via Admin-PIN [via Admin-PIN \331]	74
6.3.3.2. Zurücksetzen des Terminals via Reset-Code [via Admin-PIN \332]	74

6.3.4. Terminal-Funktionstests [Test \34].....	74
6.3.4.1. Test: [Gesamttest \341].....	74
6.3.4.2. Test: [Einzeltest \342].....	75
6.3.4.2.1. Einzeltest: [Buzzer \3421].....	75
6.3.4.2.2. Einzeltest: [Display \3422]	75
6.3.4.2.3. Einzeltest: [Tasten \3423].....	75
6.3.4.2.4. Einzeltest: [Slot 1 \3424].....	75
6.3.4.2.5. Einzeltest: [Slot 2 \3425].....	75
6.3.4.2.6. Einzeltest: [Slot 3 \3426] und [Slot 4 \3427]	76
6.3.4.2.7. Einzeltest: [Integrität \3428].....	76
6.3.5. Der Kiosk-Modus [Kiosk-Modus \35]	77
ANHANG:.....	78
1. Technische Daten.....	78
2. Musteranschreiben einer gSMC-KT.....	79
3. Menüstruktur für den Anwender.....	80
4. Menüstruktur für den Administrator - Teil 1: Allgemeine Einstellungen.....	81
5. Menüstruktur für den Administrator - Teil 2: LAN Parameter	82
6. Menüstruktur für den Administrator - Teil 3: SICCT Parameter	83
7. Menüstruktur für den Administrator - Teil 4: Service Einstellungen.....	84
8. Hinweise zur Problembeseitigung, Fehlererkennung, Verhalten im Fehlerfall und Fehlerbehandlung.....	85
9. Abbildungsverzeichnis.....	91
10. Tabellenverzeichnis.....	92
11. NOTIZEN.....	93

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 gekennzeichnete Text enthält nützliche Informationen und Tipps für eine sichere Anwendung des Gerätes.



HINWEIS

Wichtiger Hinweis zum Umweltschutz

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

Sie leisten als Ärztin oder Arzt bzw. Administrator einer medizinischen Betriebsstätte einen entscheidenden Beitrag zur Sicherheit der Online-Telematikinfrastruktur. In Ihrer Arbeitsumgebung in der eigenen Praxis, in einem medizinischen Versorgungszentrum oder in einer Klinik benötigt der Schutz der Patientendaten und der Komponenten der Online-TI besonderer Aufmerksamkeit und besonders hoher Schutzmaßnahmen.

Unsere sichere Lieferkette zwischen Ingenico Healthcare und Ihnen ist ein wichtiger Beitrag zur Sicherheit der gesamten Online-TI!

Um Manipulationen nicht erst während des Einsatzes der TI-Komponenten in der Arztpraxis zu verhindern ist bereits ein Schutz der Komponenten ab dem Moment der Fertigung in den Produktionsstätten notwendig. Hierzu wurde von uns eine sogenannte "Sichere Lieferkette" aufgebaut.

Unsere mobilen und stationären eHealth Terminals werden in einer versiegelten Verpackung geliefert, die Sie bei Empfang auf Unversehrtheit prüfen müssen, um Manipulationsversuche durch unerlaubtes Öffnen der Verpackung auszuschließen. Das angebrachte Siegelband verfügt über verschiedene Schutzmechanismen, die es Ihnen ermöglichen die Unversehrtheit und Echtheit der Verpackung einfach zu überprüfen.

Sie haben nach der Lieferung eines mobilen oder stationären Gesundheitskartenterminals sowie einer gSMC-KT Karte die Möglichkeit den lückenlosen Lieferweg zwischen uns und Ihnen zu überprüfen, um sicher zu stellen, dass die Ware ordnungsgemäß, sicher und frei von Manipulationsversuchen bei Ihnen in der Praxis angekommen ist. Hierzu stellen wir Ihnen auf unserer Internetseite www.ingenico.de/healthcare/sichere-lieferkette eine Liste unserer Handelspartner zur Verfügung, die sich vertraglich dazu verpflichtet haben alle Anforderungen an die sichere Lieferkette einzuhalten. Wir liefern mobile und stationäre Gesundheitskartenterminals sowie gSMC-KT Karte für die Online-TI ausschließlich zu diesen Handelspartnern oder direkt in Leistungserbringerinstitutionen (Arztpraxis, MVZ, Krankenhaus).



ACHTUNG!

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








1.3. Lieferumfang




Folgende Dinge sind im 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 verschiedene Tasten des Gerätes

Taste	Funktion
	Taste 1: <ul style="list-style-type: none">• Eingabe des Wertes 1• Bei freier Texteingabe die Schriftzeichen ! ? # \$ % & * ß oder 1
	Taste 2: <ul style="list-style-type: none">• Eingaben des Wertes 2• Bei freier Texteingabe Schriftzeichen a b c ä A B C Ä oder 2
	Taste 3: <ul style="list-style-type: none">• Eingabe des Wertes 3• Bei freier Texteingabe die Schriftzeichen d e f D E F oder 3
	Taste 4: <ul style="list-style-type: none">• Eingaben des Wertes 4• Bei freier Texteingabe die Schriftzeichen g h i G H I oder 4
	Taste 5: <ul style="list-style-type: none">• Eingabe des Wertes 5• Bei freier Texteingabe die Schriftzeichen j k l J K L oder 5
	Taste 6: <ul style="list-style-type: none">• Eingaben des Wertes 6• Bei freier Texteingabe die Schriftzeichen m n o ö M N O Ö oder 6
	Taste 7: <ul style="list-style-type: none">• Eingabe des Wertes 7• Bei freier Texteingabe die Schriftzeichen p q r s P Q R S oder 7
	Taste 8: <ul style="list-style-type: none">• Eingaben des Wertes 8• Bei freier Texteingabe die Schriftzeichen t u v ü T U V Ü oder 8
	Taste 9: <ul style="list-style-type: none">• Eingabe des Wertes 9• Bei freier Texteingabe die Schriftzeichen w x y z W X Y Z oder 9
	Taste 0: <ul style="list-style-type: none">• Eingabe des Wertes 0• Bei freier Texteingabe die Schriftzeichen / - + . , ; : , oder 0

Taste	Funktion
	<p>F1 Taste:</p> <ul style="list-style-type: none"> Bei freier Texteingabe die Schriftzeichen - oder _ (Unterstrich) Die Funktionstaste F1 (Netzwerkstatus) hat in Kombination mit den nachfolgenden Tasten die angegebene Funktion: <ul style="list-style-type: none"> ① MAC Adresse ④ <small>GHI</small> TCP Port ⑤ <small>JKL</small> UDP Port ⑥ <small>MNO</small> SICCT Terminal Name (die ersten 16 von maximal 32 Zeichen)
	<p>F2 Taste:</p> <ul style="list-style-type: none"> Bei freier Texteingabe das Schriftzeichen , (Kommazeichen) Die Funktionstaste F2 (Verbindungsstatus) hat in Kombination mit den nachfolgenden Tasten die angegebene Funktion: <ul style="list-style-type: none"> ① TLS (Verbindungsstatus) ② <small>MNO</small> SICCT Session (Verbindungsstatus) ③ <small>DEF</small> SICCT Kommando Interpreter (Status) ④ <small>GHI</small> DHCP Server (siehe Tabelle 16 auf Seite 8989 im ANHANG) ⑥ <small>MNO</small> 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)
	<p>Cursor-Taste (nach oben):</p> <ul style="list-style-type: none"> Im Menü mit dem grünen ► Cursor einen Menüpunkt nach oben springen
	<p>Cursor-Taste (nach unten):</p> <ul style="list-style-type: none"> Im Menü mit dem grünen ► Cursor einen Menüpunkt nach unten springen
	<p>Cursor-Taste (nach links):</p> <ul style="list-style-type: none"> Eine Menüebene zurückspringen
	<p>Cursor-Taste (nach rechts):</p> <ul style="list-style-type: none"> In das Untermenü springen, auf den der grünen ► Cursor gerade zeigt
	<p>STOP Taste:</p> <ul style="list-style-type: none"> Abbrechen einer Aktion Eine Menüebene zurückspringen Durch langes Drücken im Ruhebildschirm (ca. 3 Sekunden): Ausschalten des Gerätes

Taste	Funktion
	CLEAR Taste: <ul style="list-style-type: none">• Löschen eines Wertes links neben dem Eingabecursor
	MENU Taste: <ul style="list-style-type: none">• Im Ruhebildschirm: Öffnen des Hauptmenüs• Im Hauptmenü und Untermenüs: Zurück in den Ruhebildschirm
	OK Taste: <ul style="list-style-type: none">• 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 an den Symbolplätzen fünf und acht keine Symbole angezeigt werden. Die folgenden Tabellen geben einen Überblick über deren Bedeutung.




1.5.1. Symbol 1 bis 4: Karten-Kontaktiereinheiten

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


1.5.2. Symbol 6: Datenverkehr zu angeschlossenen Geräten

Symbol	Bedeutung
	Es besteht noch keine SICCT-Session über die LAN-Schnittstelle.
	Es besteht eine "SICCT Control Session" TLS Verbindung.
	Es besteht eine "SICCT Admin Session" TLS Verbindung.



1.5.3. Symbol 7: Interne Stützbatterie schwach

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

1.5.4. Symbol 9: Allgemeiner Gerätestatus

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

1.5.5. Symbol 10: Datenverwaltung

Symbol	Bedeutung
	<p>Kein Zugang zu den Menüs:</p> <ul style="list-style-type: none">• [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 (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
eGK	Elektronische Gesundheitskarte
gematik	Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
Gesicherte Umgebung (kontrollierte Einsatzumgebung)	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	Heilberufsausweis Der 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.

Begriff	Erläuterung
Primärsystem	Computer, an dem die Software PVS/AVS/KIS ausgeführt wird und mit dem Kartenterminal kommuniziert.
Primärsystemsoftware	Software, die auf dem Primärsystem installiert ist und bei Arzt / Apotheke / Krankenhaus eingesetzt wird.
PUK	Personal Unblocking Key Ein PUK ist ein elektronischer Schlüssel, der zum Entsperren einer Chipkarte dient, nachdem eine PIN mehrmals falsch eingegeben wurde.
PVS	Praxisverwaltungssystem (Primärsystemsoftware)
Reset Administrator	Der Reset Administrator ist derjenige, der in der Lage ist, das Terminal auch ohne bekannte Admin-PIN wieder in die Werkseinstellung zurück zu versetzen, falls dem Administrator die Admin-PIN nicht mehr bekannt ist. Bei ORGA eHealth Terminals ist es mit einem sogenannten Challenge-Response-Verfahren nur Ingenico Healthcare möglich, sie wieder in den Auslieferungszustand zurück zu versetzen.
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 (Transportschichtssicherheit) Ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.
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 beschriebenen Sicherheitsmerkmale zu überprüfen.

2.1. Gerätesicherheit

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

2.2. Sicherheitsmerkmale



ACHTUNG!

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

2.2.1. Das Gehäusesiegel und seine Eigenschaften

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



Abbildung 1: Unbeschädigtes Gehäusesiegel



Abbildung 2: Beschädigtes Gehäusesiegel



Abbildung 3: Fehlendes Gehäusesiegel

Unterhalb des BSI Logos ist die schwarz gedruckte, verkürzte BSI-Zulassungsnummer des Gerätes zu finden. Beim stationären ORGA eHealth Terminal lautet sie: **DSZ0519**.

Am rechten Rand der Siegel befindet sich die Siegelnummer, die bei alle drei Siegeln des Gerätes unterschiedlich ist.

Unter einer speziellen Schwarzlichtlampe (UV) wird der Schriftzug "SECURITY" mehrzeilig über die ganze Siegelfläche sichtbar. Ein gefälschtes Siegel ist an den fehlenden Sicherheitsmerkmalen zu erkennen.

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

Die genaue Position der Gehäusesiegel können Sie der Abbildung 7 auf Seite 23 entnehmen.



ACHTUNG!

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



ACHTUNG!

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



ACHTUNG!

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

2.2.2. Das Slotsiegel und seine Eigenschaften

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



Abbildung 4: Unbeschädigtes Slotsiegel



Abbildung 5: Beschädigtes Slotsiegel

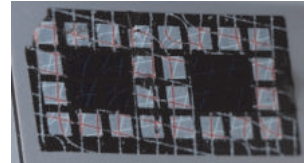


Abbildung 6: Fehlendes Slotsiegel

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.

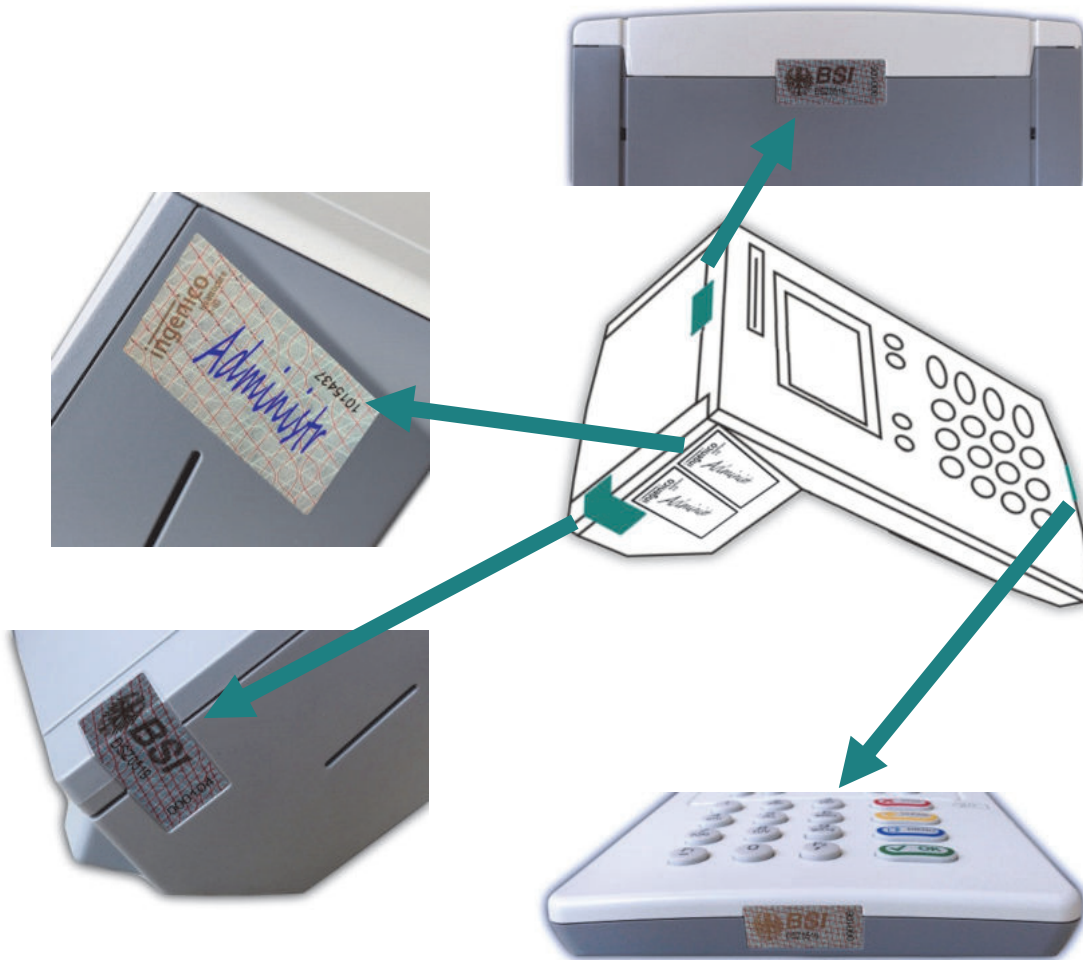


Abbildung 7: Positionen der Gehäuse- und Slotsiegel am Gehäuse des Gerätes



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 Version der Gerätesoftware, die im Menü [**Status \32**] (siehe Abschnitt »Versionsstand / Selbstauskunft des Terminals« auf Seite 5) des Gerätes angezeigt wird.

2.2.5. Integritätsprüfung

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

2.2.6. Typenschild



Abbildung 8: Typenschild mit Herstellercode HC 03000000010301

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



ACHTUNG!

Die Abbildung 8 zeigt die zulässige Position des am Gehäuse aufgeklebten Typenschilds, dessen und weitere Angaben Sie (bis auf den Herstellcode HC) über die Menüsteuerung des Gerätes (siehe Abschnitt 6.3.2 »Die Terminalselbstauskunft [Status \32]« auf Seite 72) kontrollieren können.

Bitte beachten Sie, dass aus Sicherheitsgründen außer dem Typenschild, den Geräte- und den Slotsiegeln (s. Abbildung 7) keine weiteren aufgeklebten Markierungen (Aufkleber) vorgesehen sind und nicht auf dem Gerät angebracht werden dürfen.

2.3. Sicherheit bei der Inbetriebnahme

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

2.3.1. Aufstellungshinweise



ACHTUNG!

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



ACHTUNG!

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



ACHTUNG!

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

2.3.2. Admin-PIN Eingabe bei der Inbetriebnahme

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



ACHTUNG!

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



ACHTUNG!



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

2.3.3. Eingabe einer Karten PIN nach Aufforderung

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

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

2.3.3.1. Der sichere PIN Eingabe Modus


Die Aktivierung dieser sicheren Betriebsart (Sicherer PIN Eingabemodus / secure PIN-entry mode) wird dadurch angezeigt, dass die einzugebenden PIN Ziffern durch blinkende Schlosssymbole  im Display dargestellt werden. Nur wenn diese Symbole erscheinen, ist sichergestellt, dass die eingegebene PIN ausschließlich zur gesteckten Karte übertragen wird. Die Durchführung der Signatur im Kartenterminal beginnt mit der Ausgabe des Anzeigetextes: **Bitte Geheimzahl eingeben** und in der Zeile darunter  für die Eingabe einer z. B. achtstelligen PIN.

Der sichere PIN Eingabe Modus wird zusätzlich durch ein Maskierungsgeräusch (Rauschen) zur Verhinderung akustischer Ausspähversuche während der gesamten PIN Eingabe begleitet.

Im sicheren PIN Eingabe Modus blinkt zusätzlich ein Symbol im Display. Anhand des blinkenden Symbols der entsprechenden Kontaktiereinheit kann man erkennen, für welche Karte die PIN-Eingabe angefordert wird. Wenn mehrere Gesundheitskartenterminals in einer Arztpraxis oder einem medizinischen Versorgungszentrum im Einsatz sind, befindet sich der HBA des zuständigen Arztes nicht notwendiger Weise direkt im Terminal, an dem die PIN-Eingabe für diesen HBA erfolgen muss. Bei dieser sogenannten Remote-PIN Eingabe bei der eine PIN-Eingabe für einen HBA erfolgt, der sich außerhalb des Terminals befindet, blinkt das Symbol der Kontaktiereinheit, in der sich die gSMC-KT Karte befindet



ACHTUNG!


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



ACHTUNG!

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

2.3.3.2. Fehlerfreier Ablauf

Geben Sie die Karten PIN über die Tastatur nur ein, wenn die Schlosssymbole dargestellt werden. Die abgefragte PIN (üblicherweise minimal sechs und maximal acht Ziffern) wird im Display nach der Eingabe mit einem Sternchen pro eingegebener Ziffer angezeigt. Bestätigen Sie abschließend mit der -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 inkorrektter 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 -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 -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 berechnete 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. Beide Optionen des geräteinternen (Fehler-) Loggings und der Änderungsprotokollierung werden in der aktuell vorliegenden Firmware des ORGA 6141 online nicht unterstützt und sind für spätere Firmware-Versionen geplant.

Ingenico Healthcare empfiehlt derzeit Fehler- und Änderungssituation manuell zu erfassen (z.B. das Auftreten eines Fehlerzustands mit einem Foto zu dokumentieren) und mit einem Begleittext in einem Textdokument oder einer Tabellenkalkulation (i.d.R. Betriebsdaten-änderungen) abzuspeichern.

Diese Information kann dann zur Klärung von Störungs- und Fehlermeldungen leicht an den Betreiber, Händler oder Ingenico Healthcare per E-Mail kommuniziert werden.

Dieses Logging und die Änderungsprotokollierung sollte der Administrator übernehmen.

2.5. Sicherheit bei der Außerbetriebnahme und im Reparaturfall

Das ORGA 6141 online ist ein sicherheitstechnisch sensibler Bestandteil der Telematikinfrastruktur in Ihrer Praxis. Wenn Sie das Gerät nicht mehr für die tägliche Datenerfassung verwenden, weil es defekt ist oder Sie es gegen ein anderes Gerät austauschen wollen, ist es Ihre Pflicht, bei der Außerbetriebnahme des Terminals ein paar wichtige Dinge zu beachten

und zu befolgen. Lesen Sie sich deshalb bitte folgende Hinweise aufmerksam durch und führen Sie folgende Schritte aus:

1. Vergewissern Sie sich, dass der Administrator alle wichtigen Parameter des Gerätes kennt und notiert hat.
2. Führen Sie einen Werksreset durch.

(siehe Abschnitt 6.3.3 »Zurücksetzen des Terminals in den Auslieferungszustand [Werkseinstellung \33]« auf Seite 73)



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 40) und die SMC-B und gSMC-KT Karten aus den Kontaktiereinheiten 3 und 4 (siehe Abschnitt 3.3 »Die Kontaktiereinheiten 3 und 4 für die SMC-Karten« auf Seite 36). Bewahren Sie Ihren HBA und die SMC-Karten an einem sicheren Ort auf.
4. Führen Sie je nach Grund der Außerbetriebnahme abschließend folgende Aktion aus:
 - a. Bei Einsendung des Gerätes zur Reparatur:
Verpacken Sie es sicher für den Postversand an Ihren Händler oder Ingenico Healthcare und legen Sie dem Paket eine detaillierte Fehlerbeschreibung bei.



ACHTUNG!

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

- b. Bei Einlagerung des Gerätes als Ersatzgerät:
Lagern Sie das Gerät an einem trockenen, warmen und sicheren Ort und schützen Sie das Gerät so vor unerlaubtem Zugriff von Dritten und Manipulationsversuchen.
- c. Bei der endgültigen Entsorgung des Gerätes:
Zerstören Sie die Gehäusesiegel am Gehäuse des Gerätes (siehe Abschnitt 2.2.1 »Das Gehäusesiegel und seine Eigenschaften« auf Seite 20) und beachten Sie die Entsorgungshinweise im Abschnitt 2.12 »Entsorgung des Gerätes« auf Seite 34.



ACHTUNG!

Beachten Sie bei der Wiederinbetriebnahme eines aus der Reparatur zurückkommenden Gerätes oder eines Gerätes, das Sie längere Zeit nicht benutzt haben (Ersatzgerät), dass Sie wie für ein Neugerät die allgemeinen Regeln und Anforderungen zur Betriebssicherheit des Gerätes beachten müssen (siehe Abschnitt 2.8 »Allgemeine Regeln & Anforderungen zur Betriebssicherheit des Gerätes« auf Seite 30).

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 46 beschrieben wird.

2.6. Normen und Richtlinien

Das ORGA 6141 online erfüllt die zutreffenden Normen im Geltungsbereich:

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

2.7. Temperatur / Umgebungsbedingungen

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



ACHTUNG!

Schützen Sie das Gerät vor Feuchtigkeit und Staub, da sonst die Funktion der Kartenleser beeinträchtigt werden könnte.

Fremdkörper können leicht in den Kartenschlitz der Kontaktiereinheit 1 eindringen und zu Schäden im Gerät führen.

Verwenden Sie das Gerät nur in trockener Umgebung bei Temperaturen zwischen +5 °C bis +40 °C.

2.8. Allgemeine Regeln & Anforderungen zur Betriebssicherheit des Gerätes

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



ACHTUNG!

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



ACHTUNG!

Vergewissern Sie sich vor der ersten Inbetriebnahme von der Unversehrtheit des Gerätes (Prüfen der Sicherheitsmerkmale, insbesondere der Siegel gemäß Beschreibung in Abschnitt 2.2.1 »Das Gehäusesiegel und seine Eigenschaften« auf Seite 20 und Abschnitt 2.2.2. »Das Slotsiegel und seine Eigenschaften« auf Seite 22).



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 potentiellies 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.ingenico.de/healthcare. Die zu den Firmwares zugehörigen Bestätigungen zur QES sowie die Sicherheitszertifizierung nach Common Criteria finden Sie unter www.bundesnetzagentur.de sowie unter www.bsi.bund.de



ACHTUNG!

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



ACHTUNG!

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

2.9. Sicherheit beim Anschluss an den Konnektor



ACHTUNG!

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



ACHTUNG!

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



ACHTUNG!

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



ACHTUNG!

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

2.10. Reinigung und Pflege

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

2.11. Desinfektion

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

2.12. Entsorgung des Gerätes



HINWEIS

Gemäß der EU-Richtlinie 2002/96/EG (WEEE-Richtlinie) müssen Elektro- und Elektronikgeräte, die dieses Symbol tragen, getrennt vom Hausmüll gesammelt werden, um eine ordnungsgemäße Wiederverwertung sicherzustellen.

Das Gerät beinhaltet eine interne Lithiumzelle für die Uhr und den Sicherheitsmechanismus.

Die Lithiumzelle muss an entsprechenden Sammelstationen abgegeben werden.



HINWEIS

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



ACHTUNG!

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

Kapitel 2: Bedienungsanleitung für den Benutzer

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

3. Produktbeschreibung

3.1. Die Vorderseite des ORGA 6141 online












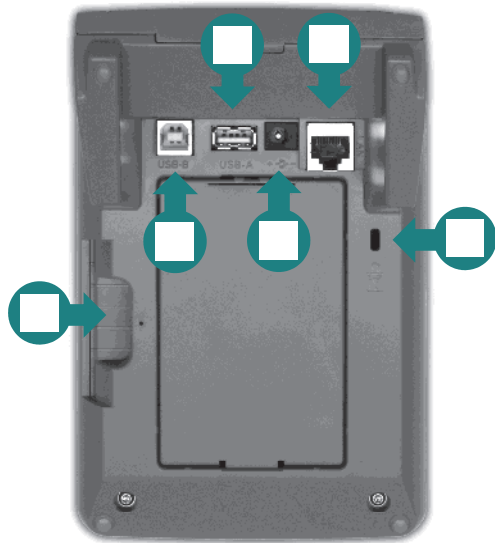
- 1: Kartenschlitz der Kontaktiereinheit 1 für die Patientenkarte (eGK)
- 2: Kartenschlitz der Kontaktiereinheit 2 für den Heilberufsausweis (HBA) am rechten Gehäuserand.
- 3: Großes Farbdisplay mit 400x240 Pixeln
- 4: Cursor-Tasten     zur Menünavigation
- 5: Ziffernblock mit Zahlentasten und Funktionstasten F1 [] und F2 []
- 6: Menütasten    

Abbildung 9: Gerätevorderseite

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 zukünftige Firmware-Updates per USB-Stick
- 3: Anschlussbuchse für Stromversorgung mit 7,5V Steckernetzteil
- 4: RJ-45 Buchse für LAN-Anschluss des Gerätes an den Konnektor
- 5: Kartenschlitz der Kontaktiereinheit 2 für den Heilberufsausweis (HBA)
- 6: Kensington-Lock Diebstahlsicherung

Abbildung 10: 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 ist mit der Gehäuseunterseite verklebt! Das Öffnen der Klappe ist nicht möglich und würde zur Beschädigung des Gerätes führen.

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



- 1 Die SMC-Karte wird mit den Kontakten der Chipkarte zur Geräte-rückseite 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 11: Die Kontaktiereinheiten 3 und 4 für die SMC-Karten

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



ACHTUNG!

Beim Einsatz des Terminals in der Online-Telematikinfrastruktur des deutschen Gesundheitswesens ist eine gSMC-KT Karten erforderlich, die sich unter einem vom Administrator unterschriebenen Slotssiegel im Gerät befinden muss.

Wenn Sie Administrator sind, lesen Sie bitte hierzu auch den Abschnitt 5.7 »Einsetzen einer SMC-Karte und Versiegeln der Kontaktiereinheiten 3 und 4« auf Seite 46.



ACHTUNG!

Wenden Sie sich an Ihren Administrator, wenn

- Sie Zweifel an der Echtheit der Siegel haben,
- sich auf dem Slotssiegel nicht die Unterschrift des Administrators befindet oder
- Ihnen sonst etwas an den Kontaktiereinheiten 3 und 4 ungewöhnlich vorkommt.

4. Bedienung des Gerätes

4.1. Tastatur



Abbildung 12: *Tastatur des Gerätes*


Das stationäre Kartenterminal ORGA 6141 online verfügt über eine Tastatur mit 20 Tasten, bestehend aus den Zifferntasten 0 bis 9 [0 1 2 3 4 5 6 7 8 9], den Funktionstasten F1 [F1] und F2 [F2], sowie den Menü-Tasten (STOP-Taste [X STOP], CLEAR-Taste [CLEAR], MENU-Taste [MENU] und OK-Taste [OK]). Die Cursor-Tasten [LEFT] [RIGHT] [UP] [DOWN] 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 13 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, nimmt es den vor der Unterbrechung vorhandenen Zustand wieder ein. Es schaltet sich automatisch ein, wenn es vorher eingeschaltet war oder bleibt ausgeschaltet, wenn es im ausgeschalteten Zustand von der Spannungsversorgung getrennt wurde. In diesem Fall schaltet es sich erst wieder ein, wenn Sie die [OK]-Taste drücken.

Das Gerät 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 -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.

Die Zeiteinstellung bleibt auch im ausgeschalteten Zustand erhalten. Im Ruhebildschirm zeigt das Display einen frei wählbaren Text (Werkseinstellung: **Willkommen!**), die Uhrzeit und das Datum an.

4.3. Aufbau des Grafikdisplays



Abbildung 13: Aufbau des Grafikdisplays

Das Gerät verfügt über ein beleuchtetes TFT-Farbdisplay mit 400x240 Pixeln, das für eine gut lesbare Darstellung der Informationen auf dem Display sorgt. Die Hauptfläche ist als Textanzeige mit maximal neun Zeilen ausgelegt. Am unteren Rand befindet sich immer eine Reihe von bis zu zehn Symbolen mit Informationen über Aktivitäten und Zustand des Gerätes. Eine ausführliche Übersicht über alle Symbole und ihre Bedeutung finden Sie im Abschnitt 1.5 »Displaysymbole und ihre Bedeutung« auf Seite 16 dieser Bedienungsanleitung.

4.4. 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 6.2.6.1 »Individueller Text im Ruhebildschirm [Freier Text \261]« auf Seite 60 dieser Bedienungsanleitung. Unter dem Begrüßungstext werden die aktuelle Uhrzeit und das aktuelle Datum angezeigt, wenn sie über einen NTP Server (siehe Abschnitt 6.2.1.8 »LAN Parameter: [NTP Server \218]« auf Seite 53) bezogen wird.



Abbildung 14: Der Ruhebildschirm

4.5. Menü-Navigation



Abbildung 15: Das Menü
[Einstellungen \2]

Durch Betätigen der MENU-Taste [MENU] gelangen Sie in das Menü des Kartenterminals. Das Menü ist in mehrere Ebenen aufgeteilt. Die Auswahl einer Ebene erfolgt entweder mit den Cursortasten ◀ ▶ und ▲ ▼, in die der Cursor bewegt werden soll und Bestätigung mit der [OK]-Taste. Das Symbol [OK] 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 Terminalselfstauskunft einsehen können, können Sie die Tastenkombination [MENU] ③ ② drücken und gelangen so ohne Umwege ins gewünschte Menü. Am oberen rechten Rand des Bildschirms wird in gelber Schrift immer die Kurztastenkombination des jeweiligen Menüs angezeigt. In diesem Beispiel (siehe Abbildung 15) [Einstellungen \2].



HINWEIS

In dieser Bedienungsanleitung 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 dazugehörigen Kurztastensequenzen finden Sie im Anhang dieser Bedienungsanleitung auf den Seiten 80 bis 84.

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 [CLEAN]-Taste können Sie fehlerhafte Eingaben korrigieren, indem Sie mit jedem [CLEAN]-Tastendruck die jeweils letzte Eingabe löschen.

4.6. Das Hauptmenü



Abbildung 16: Das Hauptmenü

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

Das Symbol [OK] 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 17: 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

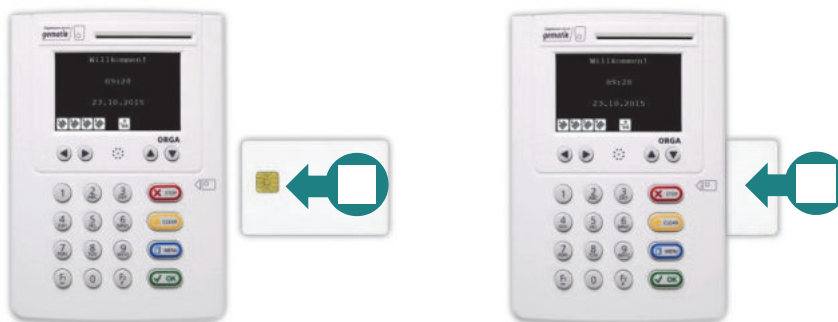


Abbildung 18: Einstecken eines HBA



Abbildung 19: Der HBA in der Kontaktiereinheit 2


Wenn Sie Ihren Heilberufsausweis (HBA) in diesem Terminal verwenden wollen, können Sie ihn auf der rechten Gehäusesseite 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. Im bestimmten Menü, 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 -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 Cursorstasten vornehmen und mit der -Taste bestätigen.

5. Inbetriebnahme

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

Nach dem Einschalten bzw. dem Anlegen der Spannung ist das Gerät betriebsbereit. Vergeben Sie bei der ersten Inbetriebnahme Ihre Administrator-PIN (Admin-PIN). Im Ruhebildschirm zeigt das Display einen frei wählbaren Text (Werkseinstellung: **Willkommen!**) an.

5.2. Admin-PIN Eingabe bei der ersten Inbetriebnahme

Bei der ersten Inbetriebnahme muss als erstes eine aus acht Ziffern bestehende Administrator-PIN (Admin-PIN) vergeben werden. Die Admin-PIN ist die gesicherte Zugangsberechtigung zu den Einstellungen Ihres Gerätes und zu den gespeicherten Daten.

Die sichere Admin-PIN Eingabe wird durch acht Schlosssymbole [#####] im Display dargestellt.



ACHTUNG!

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



ACHTUNG!

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



ACHTUNG!

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

5.3. Admin-PIN Zeitsperre

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

5.4. Neue PIN anfordern

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







5.5. Werksvoreinstellungen




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

Funktion	Menüpunkt	Einstellmöglichkeiten	Werkseinstellung
SICCT Announcement	[Announcement \224]	0 sec. (Aus) bis 3000 sec.	5 sec.
LAN Parameter DHCP	[DHCP \212]	Ein Aus	Ein
LAN Parameter TCP Port Nummer	[TCP Port \216]	0-65535	4742
LAN Parameter UDP Port Nummer	[UDP Port \217]	0-65535	4742
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]	V1.1 V1.2	V1.2
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

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

Table 2: Werksvoreinstellungen

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



ACHTUNG!

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

5.6. Authentizitäts- und Integritätsprüfung der gSMC-KT



ACHTUNG!

- Zur Integration des Terminals in die Online-Telematikinfrastruktur muss sich eine durch die gematik zugelassene gSMC-KT Karte mit gültigen Zertifikaten im Terminal befinden.
- Die gSMC-KT ist nicht im Lieferumfang des ORGA 6141 online enthalten!
- Auch wenn das Kartenterminal keine strikte Prüfung auf eine Ingenico gSMC-KT durchführt, wird der Einsatz einer Ingenico gSMC-KT empfohlen und im weiteren Textverlauf beschrieben.
- Prüfen Sie vor der Montage einer gSMC-KT Karte in einem Kartenterminal immer erst die Integrität und Authentizität der Karte.
- Führen Sie die Montage nur durch, wenn Sie sich ganz sicher sind, dass die gSMC-KT aus einer vertrauenswürdigen Quelle stammt.
- Wenden Sie sich bei Fragen oder Zweifeln bezüglich der Integrität der gSMC-KT an den Kartenherausgeber Ingenico Healthcare!



HINWEIS

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

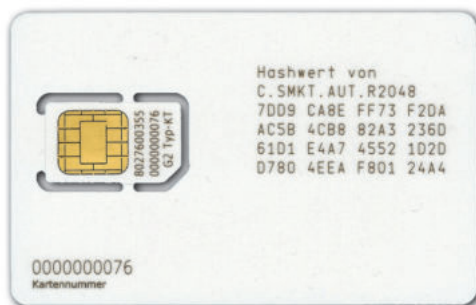


Abbildung 20: Vorderseite der gSMC-KT von Ingenico Healthcare



Abbildung 21: Rückseite der gSMC-KT von Ingenico Healthcare

In der Online-Telematikinfrastruktur werden eine Vielzahl von verschiedenen Security Module Cards (SMC) eingesetzt, um die Berechtigungen von Personen, Institutionen und Hardware-Komponenten mit dem absoluten Höchstmaß an Sicherheit zu gewährleisten. Die SMC-K (im Konnektor) und gSMC-KT (im Kartenterminal) gewährleisten die Prüfung der Berechtigungen des Zugriffs auf Patientendaten von Personen und Institutionen.

Die gSMC-KT enthält die Zertifikate und Schlüssel zum Aufbau der verschlüsselten Verbindung zum Konnektor (TLS-Verbindung) sowie zur Funktion als sogenannter Remote PIN Sender zur Durchführung eines Remote PIN - Szenarios, bei dem eine vom Konnektor aufgebaute gesicherte Verbindung zu einem Heilberufsausweis (HBA) in einem entfernten Kartenterminal genutzt wird. Die Schlüsselzertifikate einer gSMC-KT haben eine bestimmte Gültigkeitsdauer. Das Ablaufdatum der Gültigkeit ist auf dem Anschreiben zur gSMC-KT angegeben und kann in der Konfigurationsoberfläche des Konnektors nach erfolgreichem Pairing zwischen Terminal und

Konnektors abgefragt werden. Nach Ablauf der Zertifikate ist keine Datenkommunikation zwischen Terminal und Konnektor möglich und die SMC-KT muss gewechselt werden.

Das ORGA 6141 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 20 und der Rückseite in Abbildung 21 vergleichen. Die vollständige Kartenkennnummer (ICCSN) ist auf der gSMC-KT Karte neben dem Kontaktierfeld und auf dem zugehörigen Anschreiben abzulesen und muss identisch sein. Zusätzlich haben Sie zur Prüfung der Authentizität und Integrität der gSMC-KT die Möglichkeit die Vertrauenswürdigkeit der Lieferkette der Karte vom Kartenherausgeber Ingenico Healthcare bis zu Ihnen nachzuverfolgen, wenn Sie die Karte nicht direkt bei Ingenico Healthcare bestellt haben. Die Ingenico Healthcare GmbH hat hierfür auf ihrer Internetseite www.ingenico.de/healthcare/sichere-lieferkette alle Handelspartner, an die das ORGA 6141 online und die gSMC-KT geliefert werden veröffentlicht. Darüber hinaus können Sie auch über die Hotline von Ingenico Healthcare in Erfahrung bringen, wann die gSMC-KT an welche Lieferanschrift versendet wurde.

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

Die Abbildung 22 zeigt die beiden Kontaktiereinheiten 3 (unterer Kartenschlitz) und 4 (oberer Kartenschlitz), die für die Aufnahme einer Signaturkarte im im 2FF-Format (Mini-SIM) und weiterer applikationsspezifischer Smartcards vorgesehen sind. In der Online-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 (1).



Abbildung 22: Einsetzen der SMC-Karten in die Kontaktiereinheit 3 und 4



Abbildung 23: Die richtige Positionierung des Slot-siegels

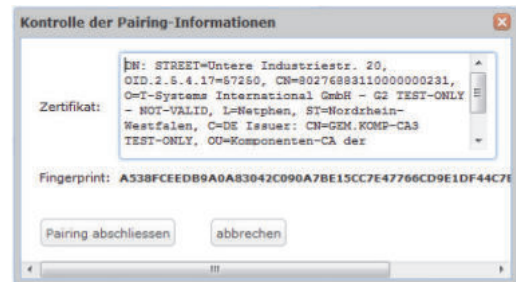
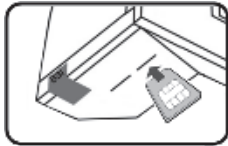


Abbildung 24: Beispiel der Angabe des gSMC-KT Fingerprints im Konfigurationsmenü eines Konnektors

Erneutes Drücken entriegelt die Karten und sie können wieder entnommen werden.

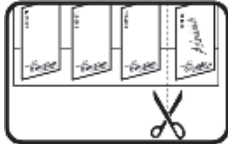
Beim Pairing Prozess muss der Administrator den Fingerprint (Hash-Wert des Authentisierungszertifikates der gSMC-KT) im Administrations-Frontend des Konnektors überprüfen. Diese Fingerprint ist direkt auf dem Kartenträger (siehe Abbildung 20) aufgedruckt. Die Abbildung 24 zeigt beispielhaft die Angabe des gSMC-KT Fingerprints im Konfigurationsmenü eines Konnektors. Weiter Details zum Fingerprint der gSMC-KT Karte entnehmen Sie bitte dem Handbuch des Konnektors.



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



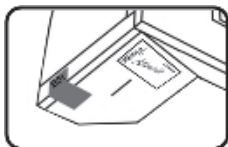
Entnehmen Sie das Trägerblatt mit den Slotsiegeln aus dem Tütchen, das sich mit der Kurzanleitung in der beiliegenden Dokumententasche befindet. Unterschreiben Sie für jede SMC-Karte, die Sie einsetzen müssen, ein Slotsiegel.



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



Die verbleibende Hälfte des Trägerblattes dient als Anfassflasche. 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 23). 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 25: Unterschreiben und richtiges Anbringen der Slotsiegel



HINWEIS!

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



HINWEIS! Anforderungen an den Siegeluntergrund:

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



ACHTUNG!

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

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

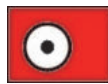
Das ORGA 6141 online wird über ein LAN-Kabel direkt mit dem Konnektor verbunden. Hierzu verwenden Sie bitte ausschließlich das beiliegende LAN-Netzwerkkabel. Zur Stromversorgung verwenden Sie bitte das beiliegende Steckernetzteil.



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



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



Hohlsteckerbuchse zur Stromversorgung über das Steckernetzteil.



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

Abbildung 26: 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 20 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 73 in Abschnitt 6.3.3 »[Werkseinstellung \33]« beschriebenen Werksreset.

ORGA
6141



Hohlstecker Buchse

Steckernetzteil



230 V Steckdose



ORGA
6141



RJ-45 Buchse

LAN-Kabel



Konnektor



RJ-45 Buchse

Abbildung 27: 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 6.2.2 »Die Konfiguration der SICCT Parameter [SICCT Parameter \22]« auf Seite 54. Schließen Sie das Gerät mit einem LAN-Kabel an den Konnektor und mit dem Steckernetzteil an eine Steckdose an, so wie es in Abbildung 27 dargestellt ist.

5.9. Initiales Pairing des Terminals mit dem Konnektor



ACHTUNG!

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



ACHTUNG!

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



ACHTUNG!

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



ACHTUNG!

Beim Anschluss des Terminals an den Konnektor (initiales Pairing) muss sich das Terminal in der organisatorischen Hoheit des Administrators befinden. Der Administrator muss gewährleisten, dass er den Pairingvorgang am Kartenterminal komplett zu Ende führt und das Prozessergebnis, dass der Konnektor eine gesicherte TLS-Verbindung zum gepairten Kartenterminal aufbauen kann, kontrolliert.

Entsprechende Anweisungen zur Kontrolle entnimmt der Administrator der Produktdokumentation des eingesetzten Konnektors.



ACHTUNG!

Im Fall eines Fehlerzustands oder bei Außerbetriebnahme müssen alle im Terminal gespeicherten Pairing-Informationen vom Administrator gelöscht werden. Dieses kann vereinfacht im Zuge eines Werksresets oder Löschen aller oder eines Pairingblocks geschehen.

Zusätzlich muss der Administrator die entsprechenden Pairing-Informationen am Konnektor löschen. Entsprechende Anweisungen zur Kontrolle entnimmt der Administrator der Produktdokumentation des eingesetzten Konnektors.



ACHTUNG!

Im Fall, dass der Pairingvorgang fehlschlug, muss der Administrator die Pairinginformation am Konnektor löschen. Entsprechende Anweisungen zur Kontrolle entnimmt der Administrator der Produktdokumentation (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 6.2.2.6 »SICCT Parameter: [Pairings \225]« auf Seite 57.

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 -Taste bestätigen Sie den Pairingvorgang und schließen den Hinweis.



HINWEIS

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

Schlägt die Durchführung fehl

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

beendet das Kartenterminal den Pairing-Vorgang und zeigt die Fehlermeldung **Abbruch** auf dem Display an. In diesem Fall hat kein Pairing mit dem Konnektor stattgefunden und muss wiederholt werden. Zur weiteren Ursachendiagnose ist dann vom Administrator das Konnektorprotokoll (Log) der Kartenterminalverwaltung im Konnektor einzusehen.



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 6.2.2.6 »SICCT Parameter: [Pairings \225]« auf Seite 57.

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 6.2.2.6 »SICCT Parameter: [Pairings \225]« auf Seite 57.






6. 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.

6.1. 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 -Taste drücken oder das Menü **[Ausschalten \1]** anwählen, mit  oder  bestätigen und durch Drücken der -Taste ausschalten. Durch Drücken der -Taste schalten Sie das Gerät wieder ein.

6.2. Der Menüpunkt Einstellungen [Einstellungen \2]

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

6.2.1. 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.

6.2.1.1. 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 Standardnamen lautet: **Terminal**

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 -Taste. Mit den Cursortasten und können Sie den blinkenden Cursor nach rechts und links bewegen und mit der -Taste können Sie den Text links neben dem blinkenden Cursor löschen.

6.2.1.2. LAN Parameter: [DHCP \212]

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

6.2.1.2.1. DHCP: [Ein / Aus \2121]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ③ [Admin PIN Eingabe] ① ② ①. Um DHCP auszuschalten, wählen Sie die ① und bestätigen mit der -Taste. Um DHCP zu aktivieren, drücken Sie die ① und bestätigen mit der -Taste.

6.2.1.2.2. 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, 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 ③ [Admin PIN Eingabe] ① ② ②. Um die erweiterten Optionen einzuschalten, wählen Sie die ① und bestätigen mit der -Taste. Um sie wieder zu deaktivieren, drücken Sie die ① und bestätigen mit der -Taste.




ACHTUNG!

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


6.2.1.3. 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 -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.


6.2.1.4. LAN Parameter: [Subnet Mask \214]

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


6.2.1.5. LAN Parameter: [Gateway \215]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [Admin PIN Eingabe] ① ⑤.
Geben Sie Ihre eigene Gateway IP Adresse ein (jeder Block dreistellig mit führenden Nullen!) und bestätigen Sie mit der -Taste. Mit den Cursorstasten ◀ und ▶ können Sie den blinkenden Cursor nach rechts und links bewegen.
Die Einstellung der IP Adresse ist nur möglich, wenn DHCP ausgeschaltet ist.

6.2.1.6. LAN Parameter: [TCP Port \216]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [Admin PIN Eingabe] ① ⑥. Geben Sie die gewünschte Port Nummer (fünfstellig mit führenden Nullen) ein und bestätigen Sie mit der -Taste. Stellen Sie jetzt die anderen Parameter der LAN-Schnittstelle ein und führen Sie dann auf jeden Fall den LAN Neustart [Neustart \219] durch!

6.2.1.7. LAN Parameter: [UDP Port \217]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [Admin PIN Eingabe] ① ⑦. Geben Sie die gewünschte UDP Port Nummer (fünfstellig mit führenden Nullen) ein und bestätigen Sie mit der -Taste. Stellen Sie jetzt die anderen Parameter der LAN-Schnittstelle ein, und führen Sie dann auf jeden Fall den auf den LAN Neustart [Neustart \219] durch!

6.2.1.8. LAN Parameter: [NTP Server \218]

Das Gerät kann über einen Network Time Protocol (NTP) Server die genaue Uhrzeit und das aktuelle Datum beziehen.

In der Werkseinstellung ist NTP deaktiviert indem der Wert [Timeout 2182] auf '00 [sec]' gesetzt ist und kann vom Administrator über diesen Menüpunkt aktiviert werden, indem ein Wert größer Null Sekunden eingestellt wird.

Ist NTP 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 NTP 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 Aktivieren von NTP im Menü [Timeout \2182] ist ein Neustart [Neustart \219] erforderlich, damit die Änderung wirksam wird.



ACHTUNG!

Das Aktivieren von NTP kann nur vom Administrator vorgenommen werden. Es wird darauf hingewiesen, dass ein aktiviertes NTP je nach Einsatzumgebung ein potenzielles Sicherheitsrisiko darstellen kann. Für den zertifizierten Betrieb darf der Administrator NTP nicht aktivieren.

6.2.1.8.1. NTP Server: [IP Adresse \2181]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern **[Admin PIN Eingabe]** und bestätigen Sie mit der **[OK]**-Taste. 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 **[Left]** und **[Right]** können Sie den blinkenden Cursor nach rechts und links bewegen. Die Einstellung der IP Adresse ist nur möglich, wenn DHCP ausgeschaltet ist.

6.2.1.8.2. NTP Server: [Timeout \2182]

Bei einem Timeout von '00 [sec]' ist der NTP Server Betrieb deaktiviert. Die Eingabe einer Zeit (maximal 60 Sekunden) startet den NTP Dienst mit dem nächsten Gerätereuestart. Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern **[Admin PIN Eingabe]** und bestätigen Sie mit der **[OK]**-Taste. Geben Sie die gewünschte Zeit in Sekunden über die Tastatur ein und bestätigen Sie Ihre Eingabe mit der **[OK]**-Taste.

6.2.1.8.3. NTP Server: [Timezone \2183]

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

6.2.1.9. 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 **[Admin PIN Eingabe]** 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.

6.2.2. 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.

6.2.2.1. 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 als zentrale Vermittlungsstelle spielt eine entscheidende Rolle. Er steuert den Datenfluss, indem er vor jeder Nutzung eine neue Verbindung (Session) herstellt. Mit jeder Verbindung wird die Gültigkeit der Verschlüsselung und des Pairing gegenseitig geprüft. Nach jeder Nutzung wird die Verbindung abgebaut.


6.2.2.2. 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.

6.2.2.2.1. 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.


6.2.2.2.2. 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 -Taste.


6.2.2.3. 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.


6.2.2.3.1. 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 -Taste.


6.2.2.3.2. 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 -Taste.

6.2.2.3.3. 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 -Taste.


6.2.2.3.4. 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 -Taste.

6.2.2.4. SICCT Parameter: [TLS Einstellung \223]


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

6.2.2.4.1. TLS Einstellungen: [TLS Version \2231]

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [Admin PIN Eingabe] ② ③ ③. 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 -Taste.

6.2.2.4.2. TLS Einstellungen: [TSL Liste \2232]

Hier können Sie die Zertifikats-Liste auswählen (Trust-Service-Statuslist), die entsprechend der Systemarbeit Anwendung finden soll. Die TSL-Listen (TSL-TU = TSL für die Testumgebung; TSL-PU = TSL für die Produktivumgebung; TSL-RU = TSL für die Referenzumgebung) sind von der gematik vorgegeben. Die TSL-LU (Laborumgebung) wurde vom Ingenico Healthcare und seinen Partnern erstellt.

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② [Admin PIN Eingabe] ② ③ ④. 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]. Bestätigen Sie Ihre Auswahl mit der -Taste.




ACHTUNG!

Die Trust-Service Status List der Laborumgebung, hier des Terminalherstellers Ingenico Healthcare [TSL-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!


6.2.2.5. 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 einstellen. Bei Eingabe des Wertes Null ist diese Funktion deaktiviert. Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② **[Admin PIN Eingabe]** ③ ④. Geben Sie anschließend den gewünschten Wert in Sekunden ein. Bestätigen Sie Ihre Eingabe mit der -Taste.

6.2.2.6. 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 -Taste.

Sie befinden sich im Hauptmenü. Drücken Sie die Ziffern ② **[Admin PIN Eingabe]** ③ ⑤ und nehmen Sie die gewünschten Einstellungen vor. Bestätigen Sie Ihre Eingabe mit der -Taste. Bei den Einstellungen ist es hilfreich sich die Menüstruktur im Anhang 6 »Menüstruktur für den Administrator - Teil 3: SICCT Parameter« auf Seite 83 anzuschauen und ggf. auch dort die Einstellungen zu notieren.

6.2.2.7. 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 Passwort 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]** ③ ⑤. Sie werden dazu aufgefordert, eine neue PIN zu vergeben. Geben Sie nun Ihre neue Session Admin PIN ein, bestätigen Sie sie mit der -Taste und wiederholen Sie die neue PIN. Bestätigen Sie erneut mit der -Taste. Bestätigen Sie Ihre Eingabe mit der -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 43).

6.2.2.8. 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.

6.2.2.8.1. 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 ③ ①. Zum deaktivieren bzw. aktivieren der Admin SICCT Session drücken Sie anschließend ③ zum Deaktivieren und ① zum Aktivieren. Bestätigen Sie Ihre Eingabe mit der -Taste.

6.2.2.8.2. 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 ④ [Admin PIN Eingabe] ② ③ ③. Wählen Sie anschließend ③ für „Aus“ und ① für „Ein“. Bestätigen Sie Ihre Eingabe mit der -Taste. Zum manuellen Ändern des Terminalnamens gehen Sie wie in Abschnitt 6.2.1.1 »LAN Parameter: [Gerätename \211]« auf Seite 52 beschrieben vor. Mit Hilfe des SICCT SET STATUS Kommandos können die Namen einzelner „Functional Units“ des Terminals gesetzt bzw. geändert werden. Im Auslieferungszustand sind die in Tabelle 3 angegebenen Werte gesetzt. Die maximale Länge für den Namen einer Functional Unit beträgt 32 Zeichen.

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

Tabelle 3: Werksvoreinstellungen der „Functional Units“ des Terminals

6.2.2.8.3. 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 6.2.2.8.1 »Zugriffsrechte: [Admin Session \2271]« auf Seite 58 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 ③ ④. Wählen Sie anschließend ① für „Aus“ und ① für „Ein“. Bestätigen Sie Ihre Eingabe mit der -Taste. Wie der manuelle Download einer Update-Datei vorgenommen wird, können Sie dem Abschnitt 6.2.9 »Durchführung eines Firmware-Updates [Update \28]« auf Seite 61 entnehmen.

6.2.2.9. 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 ③ und bestätigen Sie mit der -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.


6.2.3. Einstellen der Uhrzeit [Zeit \23]

Im Menü [Zeit \23] ist in der vorliegenden Firmware-Version 3.7.2 das manuelle Einstellen der Uhrzeit nicht möglich. Die aktuelle Uhrzeit kann aber über einen NTP Server bezogen werden (siehe Abschnitt 6.2.1.8 »LAN Parameter: [NTP Server \218]« auf Seite 53. Bei Auswahl des Menüs erscheint der Hinweis: **Funktion wird nicht unterstützt!**

6.2.4. Einstellen des Datums [Datum \24]

Im Menü [Datum \24] ist in der vorliegenden Firmware-Version 3.7.2 das manuelle Einstellen der Uhrzeit nicht möglich. Das aktuelle Datum kann aber über einen NTP Server bezogen werden (siehe Abschnitt 6.2.1.8 »LAN Parameter: [NTP Server \218]« auf Seite 53. Bei Auswahl des Menüs erscheint der Hinweis: **Funktion wird nicht unterstützt!**

6.2.5. 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] ③ und wählen anschließend die ① für Deutsch, die ② für Englisch oder die ③ für Französisch. Bestätigen Sie Ihre Eingabe mit der -Taste. Die Auswahl wird mit **Aktion erledigt** bzw. **Executed** oder **Accomplished** übernommen.

6.2.6. 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.

6.2.6.1. 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] ③ 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 verschiedene Tasten des Gerätes« auf Seite 13 und im Abschnitt 4.1 »Tastatur« auf Seite 37 dieser Bedienungsanleitung. Mit den Cursorstasten ◀ und ▶ können Sie den blinkenden Cursor nach rechts und links bewegen und mit der -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 ② [/ - + . , ; : , 0] einzugeben.




6.2.6.2. Einstellen der Displayhelligkeit [Helligkeit \262]

Um die Helligkeit des Displays auf Ihre Bedürfnisse anzupassen, drücken Sie die Ziffern ② [Admin PIN Eingabe] ③ ②. Mit den Cursorstasten ◀ und ▶ können Sie die Helligkeit individuell regeln. Beenden Sie die Einstellung mit der -Taste.

6.2.6.3. Einstellen der Hintergrundfarbe [Hintergrundfarbe \263]

Um die Hintergrundfarbe des Displays zu wählen, drücken Sie die Ziffern ② [Admin PIN Eingabe] ③ 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 -Taste.

6.2.7. Einstellen der Signaltöne [Töne \27]

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


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



ACHTUNG!

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

Das Terminal schützt alle PIN Eingaben vor einem akustischen Ausspähversuch, indem es während der PIN Eingabe ein Rauschen über den Lautsprecher abgibt, das die Eingabegeräusche während der PIN Eingabe maskiert.

Es besteht die Möglichkeit die Lautstärke des Maskierungsgeräusches anzupassen. Drücken Sie die Ziffern ② [Admin PIN Eingabe] ④ ④. Mit den Cursorstasten ◀ und ▶ können Sie die Lautstärke individuell regeln. Beenden Sie die Einstellung mit der -Taste.

6.2.9. 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 beschrieben werden.

Die Zulassung zulässiger Geräte-Software obliegt der gematik und unterliegt den gematik-Zulassungsbedingungen. Zugelassene Software-Versionen (mit Angabe der Firmware-Version) kann der Administrator der Übersicht über zugelassene TI-Komponenten („Übersicht der erteilten Zulassungen und Bestätigungen“) auf der gematik Internetseite entnehmen.

https://www.gematik.de/cms/de/zulassung/uebersicht_der_erteilten_zulassungen/zulassungsbersicht_1.jsp

Die Überprüfung, ob es sich bei der gematik zugelassenen Software auch um eine vom BSI zertifizierte Software handelt, kann der Administrator der Security Target (ST) Veröffentlichung und dem Zertifizierungsreport auf der BSI Internetseite entnehmen.

https://www.bsi.bund.de/DE/Home/home_node.html.

Die Verfahrensnummer für das ORGA 6141 online lautet: BSI-DSZ-CC-0519



ACHTUNG!

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



ACHTUNG!

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



ACHTUNG!

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



ACHTUNG!

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



ACHTUNG!

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



ACHTUNG!

Kontrollieren vor dem Update die Version der geladenen Firmware und anhand der beigegebenen Informationen (Release Notes) die neue Version, welche in das Gerät geladen werden soll.
Kontrollieren Sie nach dem erfolgten Firmware Update und Gerätereustart über die Terminalselbstauskunft, die neue Firmware-Version (siehe Abschnitt 6.3.2 »Die Terminalselbstauskunft [Status \32]« auf Seite 72).

6.2.9.1. 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 6.3.2 »Die Terminalselbstauskunft [Status \32]« auf Seite 72) kontrolliert werden. Im Fehlerfall erfolgt eine Fehlermeldung, welche angibt, dass die jeweils vorangegangene Aktion nicht durchgeführt werden konnte. Im Negativfall bleiben die vom Terminal empfangenen Daten unberücksichtigt und der vorhergehende Firmware-Stand erhalten. Nach dem Neustart arbeitet das Terminal erneut mit den zuvor eingestellten Betriebsparametern und befindet sich dann im betriebsbereiten Zustand.


Update-Verlauf	Displayanzeige
1. Initialisierung	FW Update Init DL Session Start
2. Datenübertragung	FW-Update Data DÜT-Phase
3. Übertragungsabschluss	FW Update FINISH Neustart
4. Verifikation	Überprüfung Bitte warten
5. Programmierung	Programmierung Bitte warten!
6. Abschluss	Firmware Update erfolgreich
7. Geräteneustart	Neustart

Tabelle 4: Displayanzeige während eines Firmware-Updates via Konnektor

6.2.9.2. 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 Virenschanner 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 einer Kapazität von maximal 16 GB und einem FAT32 Dateisystem.
 Kopieren Sie die Update-Datei in Stammverzeichnis des USB-Sticks und stecken Sie ihn anschließend in die USB-A Buchse auf der Unterseite des ORGA 6141 online.

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

6.2.9.2.1. Voraussetzungen zur Durchführung des Update

- Die Administrator PIN des Terminals muss bekannt sein.
- Ein USB-Stick im FAT 32 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 6.2.9.5 »Firmware-Update: [Dateiname \281]« auf Seite 69).

6.2.9.2.2. 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-Sticks in den USB-A Port auf der Unterseite des Terminals.

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

Mit den Cursorstasten **⬅** und **➡** können Sie den blinkenden Cursor nach rechts und links bewegen und mit der **↵**-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 **Ⓜ** für den Start des Updates via USB-Stick. Bestätigen Sie Ihre Eingabe mit der **✓OK**-Taste und erneut 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!

6.2.9.3. 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) abrufen.



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.

6.2.9.3.1. Voraussetzungen zur Durchführung des Update

- 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 des Firmware-Image musst dem eingestellten Namen im eHealth Terminal im Menü **[Dateiname \281]** entsprechen (siehe Abschnitt 6.2.9.5 »Firmware-Update: [Dateiname \281]< auf Seite 69) der Bedienungsanleitung zum ORGA 6141 online).
- Die IP-Adresse des TFTP-Servers ist im Terminal im Menü **[TFTP Server IP Adresse \282]** korrekt eingestellt (siehe Abschnitt 6.2.9.6 »Firmware-Update: [TFTP Server IP Adresse \282]< auf Seite 70).

6.2.9.3.2. 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 **Ⓜ [Admin PIN Eingabe] Ⓜ Ⓜ**, geben Sie den Dateinamen des Updates ein und bestätigen Sie die Eingabe mit der **✓OK**-Taste.

Mit den Cursorstasten **⏪** und **⏩** können Sie den blinkenden Cursor nach rechts und links bewegen und mit der **⌫**-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 **Ⓜ** für den Start des Updates via TFTP Server. Bestätigen Sie Ihre Eingabe mit der **✓OK**-Taste und erneut die Sicherheitsabfrage **Sind Sie sicher? [OK/STOP]** mit der **✓OK**-Taste.

Anschließend führt das Terminal alle weiteren Schritte aus, dessen Ablauf der Administrator anhand folgender Statusmeldungen verfolgt. Der erfolgreiche Fortgang (Gutfall) zeigt sich mit einem Wechsel in die nächst folgenden 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. Anforderung der Datei vom TFTP-Server	TFTP-Server: <IP-Adresse des TFTP-Servers>
2. Abruf der Datei vom TFTP-Server	TFTP-Datei: <Dateiname mit Extension „.dfu“>
3. Empfang der Datei vom TFTP-Server	TFTP-Übertragung
4. Datentransferabschluss	TFTP erfolgreich
5. Verifikation des FW-Images	Überprüfung Bitte warten!
6. Übernahme der FW in den Systemspeicher	Programmierung Bitte warten!
7. Übernahmeabschluss	Firmware Übertragung erfolgreich
8. Aktivierung des FW per Gerätereustart	Neustart


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



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

6.2.9.4. 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 abrufen. 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 Endedatum) 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.

6.2.9.4.1. Voraussetzungen zur Durchführung des Update

- 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 6.2.9.5 »Firmware-Update: [Dateiname \281]< auf Seite 69).
- Die IP-Adresse des TFTP-Servers ist im Terminal im Menü [**TFTP Server IP Adresse \282**] korrekt eingestellt (siehe Abschnitt 6.2.9.6 »Firmware-Update: [TFTP Server IP Adresse \282]< auf Seite 70).
- Das Abfragen nach einer Firmware-Image Datei wurde im Menü [**Poll Status \283**] aktiviert (siehe Abschnitt 6.2.9.7 »Firmware-Update: [Poll Status \283]< auf Seite 70).

6.2.9.4.2. Syntax der Steuerdatei

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

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

Steuerwort	Wertebereich / Format	Mandatory / Optional	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 6: Mögliche Steuerwörter der Steuerdatei für das Update via TFTP Server im Push Verfahren

6.2.9.4.3. Einstellmöglichkeiten über [Poll Window \284]

Drücken Sie die Ziffern ② [Admin PIN Eingabe] ⑧ ④. Geben Sie die den gewünschten Wert entsprechend der möglichen Parameter in Tabelle 7 für die ‚Poll Windows‘ ein und bestätigen Sie die Eingabe mit der -Taste.

Aus dem eingegeben Parameter wird eine Zufallszeitspanne zum Abruf der Steuerdatei errechnet.

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

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

6.2.9.4.4. 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!



6.2.9.5. 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 -Taste. Mit den Cursortasten  und  können Sie den blinkenden Cursor nach rechts und links bewegen und mit der -Taste können Sie

den Text links neben dem blinkenden Cursor löschen. Bestätigen Sie die Eingabe durch Drücken der -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 -Taste und erneut die Sicherheitsabfrage **Sind Sie sicher? [OK/STOP]** mit der -Taste.

6.2.9.6. 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 -Taste. Mit den Cursortasten ◀ und ▶ können Sie den blinkenden Cursor nach rechts und links bewegen und mit der -Taste können Sie den Text links neben dem blinkenden Cursor löschen.

6.2.9.7. 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 ① für „Aus“ und ② für „Ein“. Bestätigen Sie Ihre Eingabe mit der -Taste.

6.2.9.8. Firmware-Update: [Update starten \285]



ACHTUNG!


Lesen Sie sich bitte vorm Start des Firmware-Updates den gesamten Abschnitt 6.2.9 »Durchführung eines Firmware-Updates [Update \28]« ab Seite 61 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 einer Kapazität von maximal 16 GB und 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 -Taste. Anschließend werden Sie zur Sicherheit noch einmal gefragt: **Sind Sie sicher? [OK/STOP]**.

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



ACHTUNG!

Starten Sie das Update nur, wenn Sie sich ganz sicher sind, dass

- Die Installationsdatei aus einer vertrauenswürdigen Quelle stammt (z. B. Ingenico Healthcare Internetseite),
- der Dateiname Menü [**Dateiname \281**] mit dem Dateinamen der zu installierenden Update-Datei übereinstimmt und
- bei Update via. Netzwerk, die korrekte Quelle im Menü [**TFTP Server IP Adresse \282**] eingetragen wurde.



ACHTUNG!

Der Update-Vorgang kann je nach Quelle zwischen wenigen Minuten bis zu einer halben Stunde dauern.

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

6.2.10. Durchführung eines Updates der Konfigurationsparameter [Update \28]



ACHTUNG!

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



ACHTUNG!

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



ACHTUNG!

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



ACHTUNG!

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



ACHTUNG!

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

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

parameter eingespielt werden. Anstelle einer Firmware-Image Datei wird in diesem Fall eine elektronisch signierte Datei mit Konfigurationsparametern geladen. ändert dabei nicht die Firmware-Version des Terminals.

Ein Update der Konfigurationsparameter kann notwendig sein, um z.B. eine neue Version der Trusted Services List (TSL) für einen der Vertrauensräume (PU, RU, TU, LU) 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 6.3.2 »Die Terminalselbstauskunft [Status \32]« auf Seite 72) vorzunehmen.

Die einzuhaltenden Updateschritte und -vorschriften sind dieselben wie die ab dem vorherigen Abschnitt 6.2.9.2 beschriebenen. Updates sind generell nur durch autorisierte Personen (z. B. den Administrator) in gesicherten Umgebungen (z. B. Arztpraxen) erlaubt. Siehe Abschnitt 2.8 »Allgemeine Regeln & Anforderungen zur Betriebssicherheit des Gerätes« auf Seite 30.

6.3. 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.

6.3.1. 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 -Taste zu bestätigen. Geben Sie anschließend eine neue, frei wählbare achtstellige Admin-PIN ein und bestätigen Sie diese erneut mit der -Taste. Wiederholen Sie den Vorgang nach der Aufforderung und bestätigen Sie erneut mit Drücken der -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 42 dieser Bedienungsanleitung!

6.3.2. 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:
Softwareversion	3.7.2
Softwaredatum	19.10.2017
Firmware Gruppe	00010:<V3.7.2>
Hardware-Version	1.2.0
Hersteller-ID	INGHC
Produktkürzel	ORGA6100
Produktversion	3.7.2:1.2.0
Produkttyp	KT
Produkttypversion	1.2.1
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 TU g.h.i>
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 8: *Terminalselbstauskunft*



6.3.3. 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 zurück versetzen können, dabei gehen alle Einstellungen und gespeicherten Daten verloren und alle Parameter werden auf die Werksauslieferungseinträge zurückgesetzt. Auch die PIN Verwaltung wird zurückgesetzt!



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

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

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

6.3.3.2. Zurücksetzen des Terminals via Reset-Code [via Admin-PIN \332]


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





HINWEIS

Setzen Sie sich mit der Service-Hotline von Ingenico Healthcare in Verbindung, wenn Sie Ihre Admin-PIN vergessen haben. Ingenico Healthcare kann als sogenannter Reset Administrator das Terminal auch ohne Admin-PIN wieder in die Werkseinstellung zurück versetzen. 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.

6.3.4. Terminal-Funktionstests [Test \34]

Mit dieser Funktion können Sie die Hardware Ihres Gerätes 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 oder HBA, 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. 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 -Taste überspringen.

6.3.4.1. 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 -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 -Taste überspringen.



6.3.4.2. 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 ⑤ und die Ziffer für den gewünschten Test.

6.3.4.2.1. Einzeltest: [Buzzer \3421]

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


6.3.4.2.2. 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 -Taste wechselt die Farbe anschließend zu Grün und Blau, bevor Sie mit der -Taste wieder ins Ausgangsmenü gelangen.

6.3.4.2.3. 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 , 0
```

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 -Taste beendet.

6.3.4.2.4. 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
```

6.3.4.2.5. 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
```


6.3.4.2.6. 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.

6.3.4.2.7. 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 -Taste mit der Meldung **... bitte warten ...** und endet mit einer zweizeiligen Statusanzeige.

Wenn das Gerät den Integritätstest bestanden hat, wird im Display folgende Information angezeigt:

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

Die Anzeige des Status kann mit beliebiger Taste beendet werden oder schließt nach einigen Sekunden automatisch mit Ablauf des Menü Timeouts.


Wurde ein Fehler festgestellt, wird kein **ok** angezeigt. Nach einem Fehlerfall wird das Gerät mit dem nächsten Einschalten nicht mehr in den Betriebsmodus gehen. Wenden Sie sich in diesem Fall an die Service-Hotline von Ingenico Healthcare.








HINWEIS

Weitere Informationen zum Integritätstest entnehmen Sie dem Abschnitt 2.2.5 »Integritätsprüfung« auf Seite 24 dieser Bedienungsanleitung!

6.3.5. 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 -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 -Taste.

Im Kiosk-Modus, sind die ,  und -Tasten gesperrt. Sie gelangen in diesem Modus nur ins Menü, wenn Sie die -Taste fünf Sekunden lang gedrückt halten. Nach Verlassen des Menüs bleibt der Kiosk-Modus weiter aktiv, bis Sie diese Einstellung wieder im Menü **[Kiosk-Modus \35]** deaktivieren.

Folgende Einschränkungen sind im Kiosk-Modus aktiviert:


Terminalfunktion	Kiosk-Modus AUS	Kiosk-Modus EIN
Einstieg ins Menü	 -Tasten kurz drücken	 -Tasten fünf Sekunden gedrückt halten.
Ausschalten über  -Taste oder dem Menüpunkt [Ausschalten \1]	möglich (aktiviert)	nicht möglich (deaktiviert)
Quickinfo mit F1- oder F2-Taste + Zifferntaste	möglich (aktiviert)	nicht möglich (deaktiviert)
Menü-Timeout	60 Sekunden	30 Sekunden

Tabelle 9: Kiosk-Modus Eigenschaften

ANHANG:


1. Technische Daten


Spannungsversorgung:	Über USB: 500mA Netzteil: 900 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 10: Technische Daten

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


2. Musteranschreiben einer gSMC-KT









8027600355000000076



23.10.2022

Personalisierungsdaten dieser gSMC-KT:

-  Kartennummer (ICCSN)

-  Gültigkeitsdatum der Zertifikate auf der gSMC-KT


gSMC-KT Karte für stationäre Gesundheitskartenterminals

Sehr geehrte Anwenderin, sehr geehrter Anwender,

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


<https://ingenico.de/healthcare/downloads>

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




Achtung!

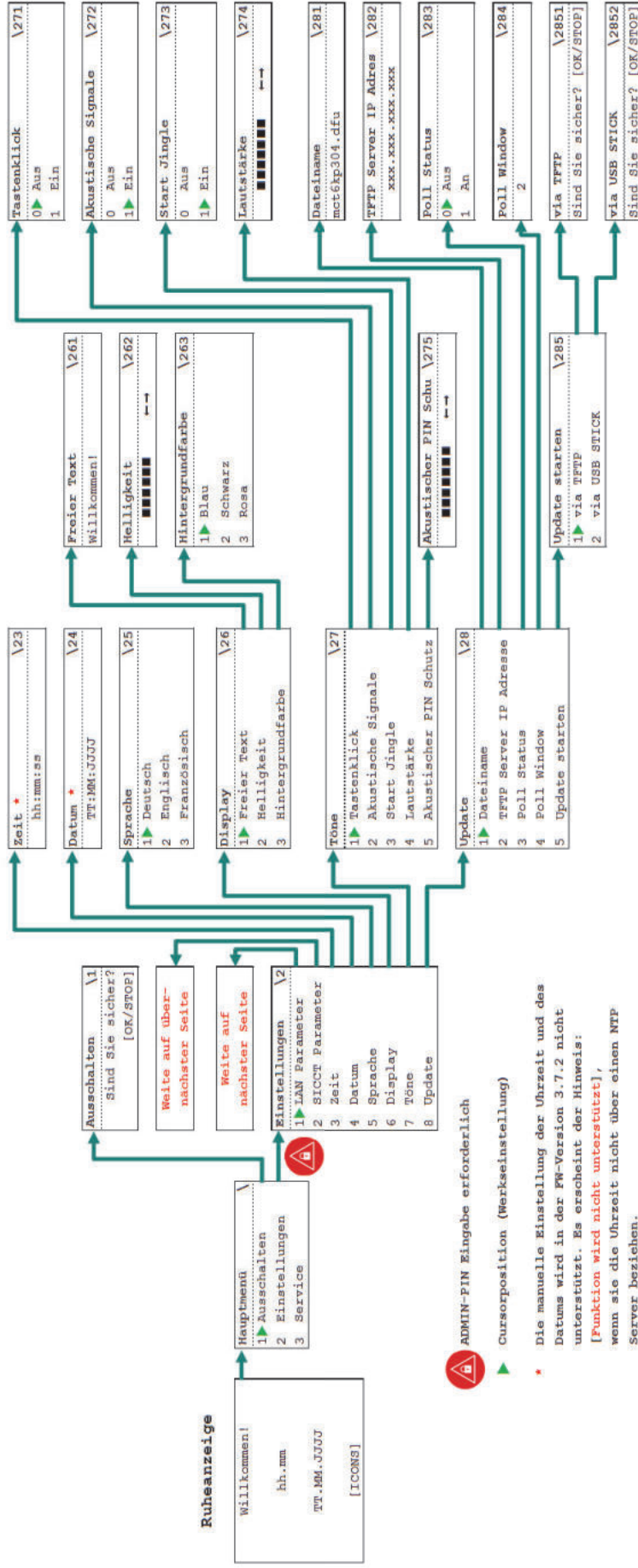
- Prüfen Sie vor der Montage einer gSMC-KT Karte in einem Kartenterminal immer erst die Integrität und Authentizität der Karte.
- Führen Sie die Montage nur durch, wenn Sie sich ganz sicher sind, dass die gSMC-KT aus einer vertrauenswürdigen Quelle stammt.
- Wenden Sie sich bei Fragen oder Zweifeln bezüglich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



www.ingenico.de/healthcare
Ingenico Healthcare GmbH · Konrad-Zuse-Ring 1 · D-24220 Flintbek · kontakt.ihc@ingenico.com
Geschäftsführer: Oliver Neufuß · Frank Hartmann
Sitz der Gesellschaft: Flintbek · HRB NR. 8903 KI · Amtsgericht Kiel · Steuer-Nr. 147/5838/2204 · Ust-ID Deutschland: DE252422299
Commerzbank AG Kiel · IBAN-Nr. DE47 2104 0010 0749 0188 00 · BIC: COBADEFFXXX
V7.7.1 / Best.-Nr. 200677

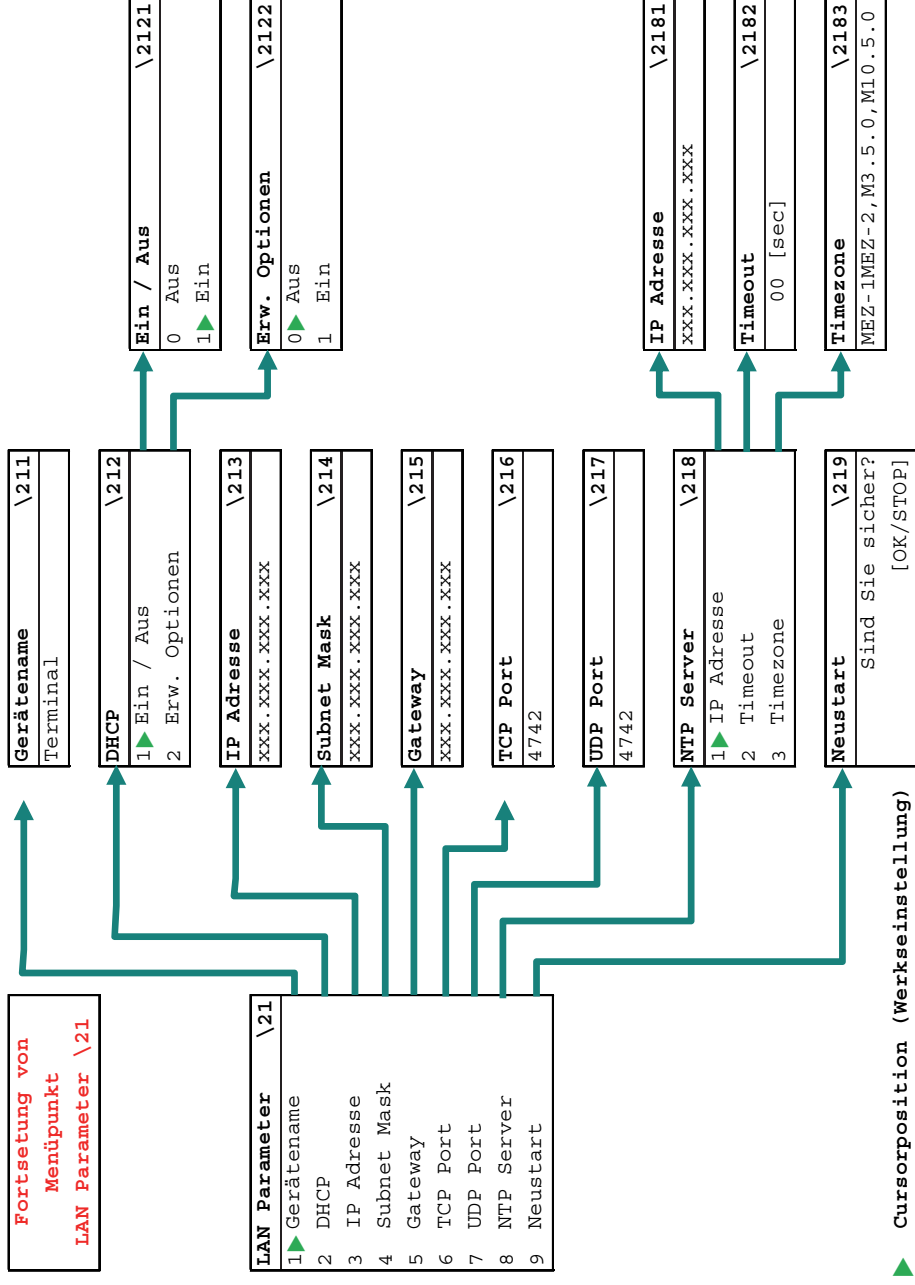


4. Menüstruktur für den Administrator - Teil 1: Allgemeine Einstellungen

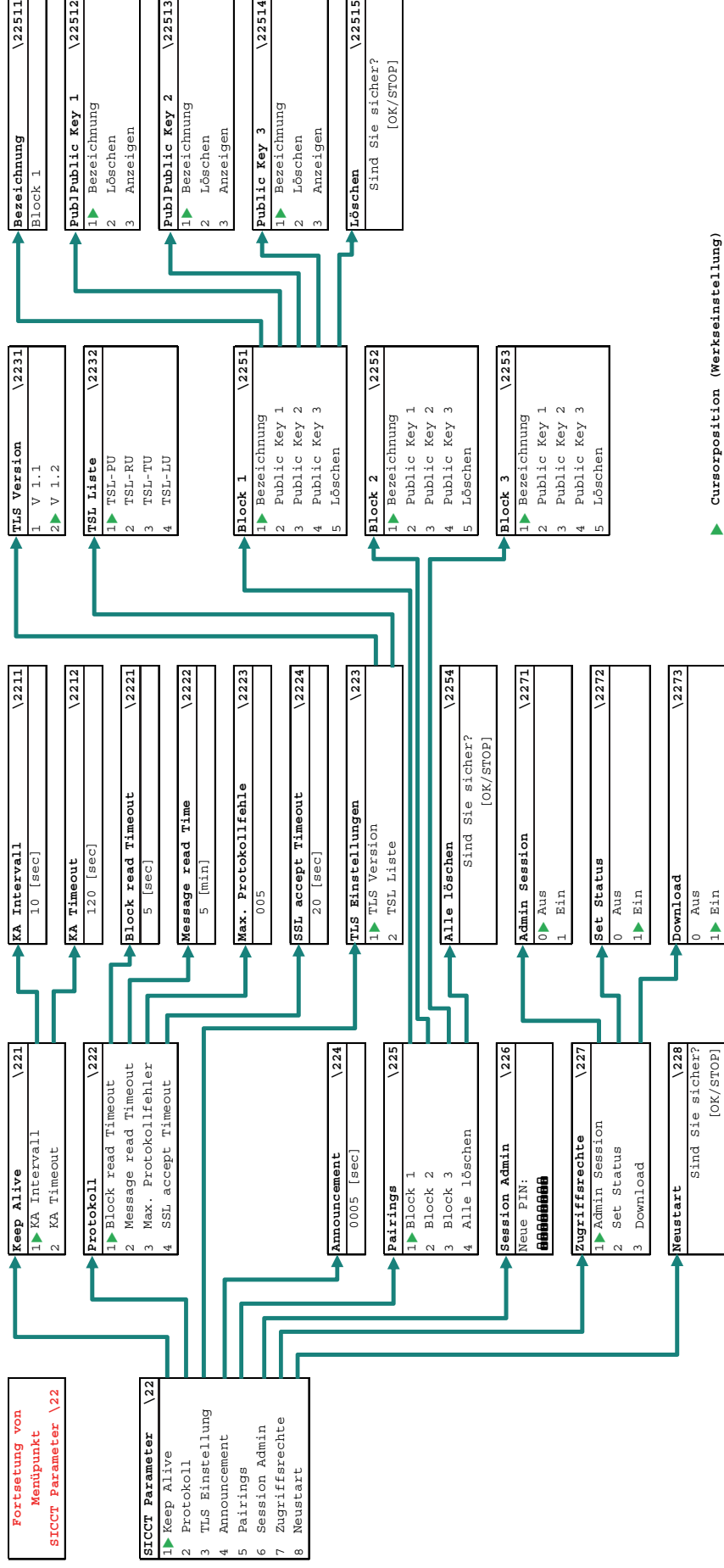


- ADMIN-PIN Eingabe erforderlich
- Cursorposition (Werkzeinstellung)
- Die manuelle Einstellung der Uhrzeit und des Datums wird in der FW-Version 3.7.2 nicht unterstützt. Es erscheint der Hinweis: [Funktion wird nicht unterstützt], wenn sie die Uhrzeit nicht über einen NTP Server beziehen.

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

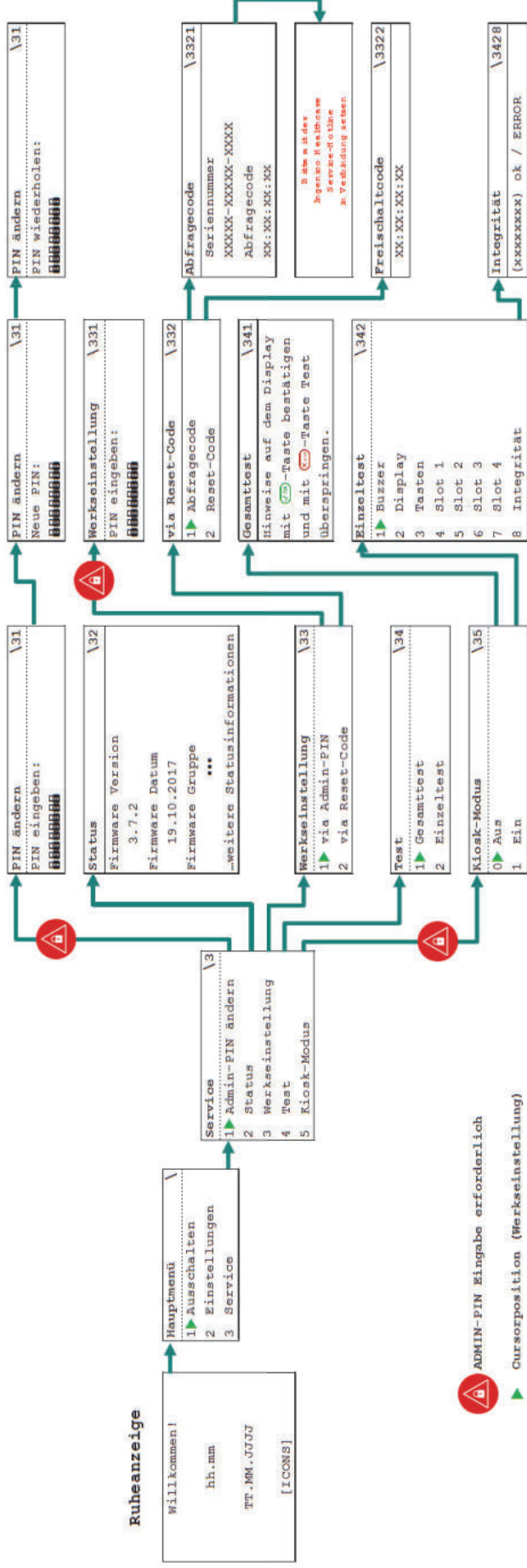


6. Menüstruktur für den Administrator - Teil 3: SICCT Parameter



▲ Cursorposition (Werkzeinstellung)

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



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

Probleme bei der Inbetriebnahme des ORGA 6141 online


Problem:	Mögliche Ursachen	Mögliche Lösungen
Die Verpackung des Neugerätes ist beschädigt und die Gehäusesiegel sehen beschädigt aus.	<ul style="list-style-type: none"> • Das Gerät wurde nicht sachgemäß zwischengelagert und transportiert • Das Gerät wurde manipuliert bzw. es wurde versucht das Gerät zu manipulieren. 	<ul style="list-style-type: none"> • Lesen Sie sich die Sicherheitshinweise im Abschnitt 2 »Sicherheit« auf Seite 20 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.	<ul style="list-style-type: none"> • Das Gerät wurde durch langes Drücken der STOP Taste im Ruhebildschirm (ca. 3 Sekunden) ausgeschaltet. • Das Gerät ist defekt 	<ul style="list-style-type: none"> • 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: ■■■■■■■■■■	<ul style="list-style-type: none"> • Das Gerät ist neu und befindet sich noch im Auslieferungszustand. • Es wurde ein Werksreset durchgeführt, aber noch keine neue Admin-PIN eingegeben. 	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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 beschriebene Problem auf. 	<ul style="list-style-type: none"> • Tritt der Fehler bei erneutem Einschalten nochmals auf, ist das Gerät einzuschicken, die Software ist defekt und eine einwandfreie Funktion unter Umständen nicht mehr gegeben.
Nach dem Einschalten des Gerätes erscheint plötzlich folgendes Symbol im Display: 	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Das Terminal muss zeitnahe gegen ein neues Gerät getauscht werden.

Tabelle 11: 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: <ul style="list-style-type: none"> • Die gesteckte eGK ist defekt • Die Kontaktiereinheit 1 ist verschlissen oder verschmutzt • Die Karte steckt falsch herum 	<ul style="list-style-type: none"> • 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 12: 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?	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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 Ingenico Healthcare.

Tabelle 13: Probleme beim Übertragen von Patientendaten zum Primärsystem

Fehlermeldungen und Ursachen - Identification & Authentication

Typ:	Mögliche Ursachen	Mögliche Lösungen
falsche PIN oder fehlerhafte Eing.	<ul style="list-style-type: none"> Eingabe einer falschen Admin-PIN 	<ul style="list-style-type: none"> Korrekte Admin-PIN eingeben
PIN Zeitsperre bitte warten...	<ul style="list-style-type: none"> PIN wurde mehrfach falsch eingegeben. Eine erneute PIN-Eingabe ist erst nach einer Wartezeit möglich. 	<ul style="list-style-type: none"> Korrekte Admin-PIN nach angegebener Zeit eingeben
kein Abfragecode generiert	<ul style="list-style-type: none"> Die Funktion „Abfragecode“ wurde über das Terminal Menü noch nicht aufgerufen. 	<ul style="list-style-type: none"> Setzen Sie sich mit der Service-Hotline von Ingenico Healthcare in Verbindung
falscher Code Fehlerzähler=X	<ul style="list-style-type: none"> Ein falscher Freischaltcode wurde eingegeben. 	<ul style="list-style-type: none"> Korrekten Freischaltcode eingeben
Abbruch	<ul style="list-style-type: none"> STOP-Taste während der PIN-Eingabe gedrückt 	<ul style="list-style-type: none"> Beginnen Sie den Vorgang erneut von vorn.

Tabelle 14: Fehlermeldungen und Ursachen - Identification & Authentication

Fehlermeldungen und Ursachen - Firmware Update

Typ:	Mögliche Ursachen	Mögliche Lösungen
Fehler bei der Datenübertragung	<ul style="list-style-type: none"> Dateisystem des USB-Sticks beschädigt Der beabsichtigte Download-Vorgang wird abgebrochen. 	<ul style="list-style-type: none"> USB-Stick neu formatieren und Firmware-Image Datei erneut kopieren.
Filesystem nicht unterstützt!	<ul style="list-style-type: none"> Falsches Dateisystem (nicht FAT 16 / FAT 32) Der beabsichtigte Download-Vorgang wird abgebrochen. 	<ul style="list-style-type: none"> USB-Stick mit dem Dateisystem FAT32 neu formatieren und Firmware-Image Datei erneut kopieren.
Ungültige Firmware	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Geeignete Firmware-Image Datei auf den USB-Stick kopieren
Ungültige Firmware	<ul style="list-style-type: none"> Firmware-Image Datei nicht für das Terminal geeignet 	<ul style="list-style-type: none"> Geeignete Firmware-Image Datei auf den TFTP-Server kopieren
Speicherfehler	<ul style="list-style-type: none"> Fehler beim Schreiben in FLASH-Speicher Programmierphase wird beendet, das Gerät geht in einen sicheren Fehlerzustand über. 	<ul style="list-style-type: none"> Service kontaktieren.
TFTP-Abbruch	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Geeignete Netzwerkverbindung herstellen
TFTP-Abbruch	<ul style="list-style-type: none"> Firmware-Image Datei liegt nicht im Root Directory des TFTP-Servers 	<ul style="list-style-type: none"> Firmware-Image Datei in das Root Directory des TFTP-Servers kopieren

<p><Timeout: ca. 3 1/2 Min.> TFTP-Abbruch</p>	<ul style="list-style-type: none"> • Kein TFTP Server unter der eingestellten IP-Adresse erreichbar 	<ul style="list-style-type: none"> • TFTP Server starten • Firewall Einstellungen kontrollieren • TFTP Server IP Adresse im Terminalmenü kontrollieren
<p>TFTP-Abbruch Menürückkehr</p>	<ul style="list-style-type: none"> • Fehler bei der TFTP-Übertragung • Übertragenes File ist zu groß. 	<ul style="list-style-type: none"> • Geeignete Firmware-Image Datei auf den TFTP-Server kopieren
<p>Ungültige Firmware</p>	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Geeignete Firmware-Image Datei auswählen
<p>Update File nicht gefunden!</p>	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Name der Firmware-Image Datei auf dem USB-Stick an erwarteten Updatenamen anpassen. • Firmware-Image Datei in das Root Directory des USB-Sticks kopieren
<p>Update File zu gross!</p>	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Geeignete Firmware-Image Datei auf den USB-Stick kopieren
<p>USB-Stick nicht gesteckt!</p>	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • USB-Stick ziehen und erneut gesteckt • Alternativen USB-Stick probieren

Tabelle 15: *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 -	<ul style="list-style-type: none"> • DHCP ist am Terminal deaktiviert. • Terminal verwendet statische Netzparameter (u.a. IP-Adresse und Subnet-Mask). 	<ul style="list-style-type: none"> • Aktivieren Sie DHCP am Terminal. (siehe Abschnitt 6.2.1.2.1 auf Seite 52)
DHCP Server PREINIT	<ul style="list-style-type: none"> • DHCP ist am Terminal aktiviert. • Terminal verwendet DHCP und versucht, eine Kommunikation zu einem DHCP-Server herzustellen. 	
DHCP Server FAIL	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Prüfen Sie die im Terminal eingegebene IP-Adresse und Subnet-Mask des DHCP Servers. • Deaktivieren Sie DHCP am Terminal. (siehe Abschnitt 6.2.1.2.1 auf Seite 52) und geben Sie anschließend die korrekte IP-Adresse und Subnet-Mask des DHCP Servers manuell ein (siehe Abschnitte 6.2.1.3 und 6.2.1.4 auf Seite 52).
DHCP Server BOUND	<ul style="list-style-type: none"> • DHCP ist am Terminal aktiviert. • Zustand nachdem der DHCP-Client des KTs vom DHCP-Server eine IP-Adresse bezogen hatte. 	
DHCP Server RENEW	<ul style="list-style-type: none"> • 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 16: Status - / Fehlermeldungen und Ursachen - DHCP

Fehlermeldungen und Ursachen - Sichere PIN-Eingabe

Typ:	Mögliche Ursachen	Mögliche Lösungen
Wiederholung ist nicht gleich	<ul style="list-style-type: none"> Die Wiederholung der initialen Admin-PIN Eingabe war fehlerhaft. 	<ul style="list-style-type: none"> Wiederholen Sie die korrekte Eingabe der neuen Admin-PIN.
Aktion erfolgreich	<ul style="list-style-type: none"> PIN erfolgreich eingegeben 	
Geheimzahl falsch / gesperrt	<ul style="list-style-type: none"> Falsche PIN eingegeben PIN ist auf der Karte bereits gesperrt. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Wiederholung der PIN fehlerhaft. 	<ul style="list-style-type: none"> Wiederholen Sie die korrekte Eingabe der neuen Karten-PIN.
Abbruch	<ul style="list-style-type: none"> STOP Taste gedrückt bei der PIN-Eingabe 	<ul style="list-style-type: none"> Beginnen Sie den Vorgang erneut von vorn.
Alte PIN nicht zulässig!	<ul style="list-style-type: none"> Eingabe einer alten PIN 	<ul style="list-style-type: none"> Wiederholen Sie die korrekte Eingabe mit einer neuen Karten-PIN.

Tabelle 17: Fehlermeldungen und Ursachen - Sichere PIN-Eingabe

Fehlermeldungen und Ursachen - Sonstige

Typ:	Mögliche Ursachen	Mögliche Lösungen
Abbruch Fehlende SMCKT	<ul style="list-style-type: none"> gSMC-KT nicht in Slot 3 oder 4 vorhanden. Die TCP Verbindung wird mit einem FIN / ACK beendet. 	<ul style="list-style-type: none"> 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 46)
Fehler Integrität	<ul style="list-style-type: none"> Die Software-Integritätsprüfung hat einen Manipulationsversuch festgestellt. 	<ul style="list-style-type: none"> Setzen Sie sich mit der Service-Hotline von Ingenico Healthcare in Verbindung
SICHERHEITSALARM Service kontaktieren!	<ul style="list-style-type: none"> Die im Terminal integrierten Schutzmaßnahmen gegen Manipulationsversuche wurden ausgelöst und das Terminal wurde deaktiviert. 	<ul style="list-style-type: none"> Setzen Sie sich mit der Service-Hotline von Ingenico Healthcare in Verbindung

Tabelle 18: Fehlermeldungen und Ursachen - Sonstige

9. Abbildungsverzeichnis

Abbildung 1: <i>Unbeschädigtes Gehäusesiegel</i>	20
Abbildung 2: <i>Beschädigtes Gehäusesiegel</i>	20
Abbildung 3: <i>Fehlendes Gehäusesiegel</i>	20
Abbildung 4: <i>Unbeschädigtes Slotssiegel</i>	22
Abbildung 5: <i>Beschädigtes Slotssiegel</i>	22
Abbildung 6: <i>Fehlendes Slotssiegel</i>	22
Abbildung 7: <i>Positionen der Gehäuse- und Slotsiegel am Gehäuse des Gerätes</i>	23
Abbildung 8: <i>Typenschild mit Herstellcode HC 03000000010301</i>	24
Abbildung 9: <i>Gerätevorderseite</i>	35
Abbildung 10: <i>Geräterückseite</i>	36
Abbildung 11: <i>Die Kontaktiereinheiten 3 und 4 für die SMC-Karten</i>	36
Abbildung 12: <i>Tastatur des Gerätes</i>	37
Abbildung 13: <i>Aufbau des Grafikdisplays</i>	38
Abbildung 14: <i>Der Ruhebildschirm</i>	38
Abbildung 15: <i>Das Menü [Einstellungen \2]</i>	39
Abbildung 16: <i>Das Hauptmenü</i>	39
Abbildung 17: <i>Einstecken einer eGK</i>	40
Abbildung 18: <i>Einstecken eines HBA</i>	40
Abbildung 19: <i>Der HBA in der Kontaktiereinheit 2</i>	40
Abbildung 20: <i>Vorderseite der gSMC-KT von Ingenico Healthcare</i>	45
Abbildung 21: <i>Rückseite der gSMC-KT von Ingenico Healthcare</i>	45
Abbildung 22: <i>Einsetzen der SMC-Karten in die Kontaktiereinheit 3 und 4</i>	46
Abbildung 23: <i>Die richtige Positionierung des Slotsiegels</i>	46
Abbildung 24: <i>Beispiel der Angabe des gSMC-KT Fingerprints im Konfigurationsmenü eines Konnektors</i>	46
Abbildung 25: <i>Unterschreiben und richtiges Anbringen der Slotsiegel</i>	47
Abbildung 26: <i>Anschlüsse auf der Unterseite des Gerätes</i>	48
Abbildung 27: <i>Anschluss mit LAN-Kabel am Konnektor</i>	48

10. Tabellenverzeichnis

Tabelle 1: <i>Begriffsbestimmung</i>	19
Tabelle 2: <i>Werksvoreinstellungen</i>	44
Tabelle 3: <i>Werksvoreinstellungen der „Functional Units“ des Terminals</i>	58
Tabelle 4: <i>Displayanzeige während eines Firmware-Updates per Konnektor</i>	63
Tabelle 5: <i>Displayanzeige während eines Firmware-Updates per TFTP Server im Pull-Verfahren</i>	66
Tabelle 6: <i>Mögliche Steuerwörter der Steuerdatei für das Update via TFTP Server im Push Verfahren</i>	68
Tabelle 7: <i>Parameter des Abfrageintervalls für das Update via TFTP Server im Push Verfahren</i>	69
Tabelle 8: <i>Terminalselbstauskunft</i>	73
Tabelle 9: <i>Kiosk-Modus Eigenschaften</i>	77
Tabelle 10: <i>Technische Daten</i>	78
Tabelle 11: <i>Probleme bei der Inbetriebnahme des ORGA 6141 online</i>	85
Tabelle 12: <i>Probleme beim Einlesen von eGK Patientendaten</i>	86
Tabelle 13: <i>Probleme beim Übertragen von Patientendaten zum Primärsystem</i>	86
Tabelle 14: <i>Fehlermeldungen und Ursachen - Identification & Authentication</i>	87
Tabelle 15: <i>Fehlermeldungen und Ursachen - Firmware Update</i>	88
Tabelle 16: <i>Status - / Fehlermeldungen und Ursachen - DHCP</i>	89
Tabelle 17: <i>Fehlermeldungen und Ursachen - Sichere PIN-Eingabe</i>	90
Tabelle 18: <i>Fehlermeldungen und Ursachen - Sonstige</i>	90

