T · · Systems ·

Produkthandbuch

T-Systems Konnektor

T-Systems International GmbH

Tabelle 1: Impressum

Herausgeber	T-Systems International GmbH Hahnstraße 43d 60528 Frankfurt am Main

Dateiname
26102018_OPB_KON_AGD_V1.16

Version	**Letztes Review**	**Status**
1.16	26.10.2018	Final

Ansprechpartner	**E-Mail**
T-Systems International	service.map@telekom.de

Kurzbeschreibung
Dieses Dokument ist das Benutzerhandbuch für den Konnektor der T-Systems

Änderungshistorie

Tabelle 2 Änderungshistorie

Version	Stand	Änderungen
1.1	24.10.2017	Produktmuster
1.2	14.11.2017	Final Produktmuster
1.3	21.02.2018	Erweitert um Feature ANLW_IA_BESTANDSNETZE
1.4	23.02.2018	Erweitert um Signaturdienst/Verschlüsselungsdienst
1.5	26.03.2018	Weitere Details / Kapitel Hinzugefügt, Sicherheit, Logistik, Inbetriebnahme, Außerbetriebnahme, Versionierung. Kleinere Anpassungen
1.6	16.04.2018	Anpassungen zur Abgabe bei gematik
1.7	23.05.2018	Anpassungen nach Review Prüfstelle
1.8	24.05.2018	Ergänzung Sicherheitshinweise
1.9	25.05.2018	Anpassung Konnektor Release Nummer, Ergänzung Information LogFile
1.10	12.06.2018	Anpassung Sicherheitshinweise InReihe/Parallel, Browser Zertifikatsimport Admin Oberfläche
1.11	13.06.2018	Qualitätssicherung / Fehler zu Referenzen Kapitel 6.2 behoben
1.12	18.06.2018	Ergänzung 7.4 Zugriffsberechtigung, Hinweis 5.1.2 Fernwartung Backend in 1.4.9 nicht aktiv, Sicherheitshinweis Zertifikatsimport 4.7.1 und 5.1
1.13	22.06.2018	Update der Versionsnummer auf 1.4.11
1.14	26.09.2018	Ergänzung und Updates in mehreren Kapiteln für Konnektor Release 1.5
1.15	22.10.2018	Update der Versionsnummer auf 1.5.1
1.16	26.10.2018	Anpassung der Firmware auf 1.4.13 mit der Basis der Handbuch Version 1.13

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Zusammenfassung

Mit der Einführung der elektronischen Gesundheitskarte betritt Deutschland neues Gebiet: Erstmals ist ein bundesweites Gesundheitsnetzwerk vorhanden, mit dessen Hilfe Krankenhäuser, Krankenkassen, Ärzte und Patienten digitale Informationen sicher austauschen können. Die Digitalisierung der medizinischen Versorgung gehört zu den anspruchsvollsten IT-Projekten weltweit. Experten rechnen mit über zehn Milliarden Datentransaktionen pro Jahr und schätzen das Datenaufkommen auf mehrere Dutzend Terabyte - und das ohne die Bilddaten, die durch moderne bildgebende Verfahren wie Computertomografie oder Magnetresonanztherapie zur Verfügung stehen.

Der T-Systems Konnektor dient dazu, dezentralen Anwendungsprogrammen auf den Systemen der Ärzte, Krankenhäuser etc. den Zugang zur zentralen Telematikinfrastruktur des Gesundheitswesens für die Nutzung der Fachdienste und der Chipkarten zu ermöglichen. Dazu stellt der T-Systems Konnektor einen sicheren Kanal zur zentralen Telematikinfrastruktur her, der für die sichere Ausführung der Anwendungsfälle genutzt wird.

1 Allgemeine Informationen zur Dokumentation

Diese Dokumentation bietet dem Anwender eine Anleitung zur Arbeit mit dem Produkt T-Systems Konnektor. Die Gesamtheit der Teilkomponenten Netzkonnektor, Anwendungskonnektor mit VSDM-Fachmodul wird als T-Systems Konnektor bezeichnet.

Für den Umfang dieser Dokumentation beziehen sich die Bezeichnungen Hersteller, Herausgeber und PKI-Betreiber auf die T-Systems International GmbH.

1.1 Hinweis zu Evaluierungen

Das vorliegende Handbuch beschreibt die Konfiguration und den Umgang mit dem Produkt T-Systems Konnektor und ist Teil der Dokumentation im Rahmen der Common Criteria Evaluierung unter der Kennung BSI-DSZ-CC-0928. Mehr Informationen zur Produktzertifizierung erhalten Sie auf den Webseiten des Bundesamts für Sicherheit in der Informationstechnik (BSI) und per E-Mail an service.map@telekom.de.

1.2 Zielgruppe der Dokumentation

Dieses Handbuch richtet sich an Anwender mit grundlegenden Kenntnissen in Netzwerkadministration und Netzwerkinfrastrukturen.

2 Bestimmungsgemäße Verwendung in der Telematikinfrastruktur (TI)

2.1 Überblick über die Telematikinfrastruktur

Der T-Systems Konnektor, im Weiteren auch Konnektor genannt, besteht aus den Teilkomponenten Netz- und Anwendungskonnektor mit VSDM-Fachmodul. Der Netzkonnektor setzt die sichere und vertrauenswürdige Kommunikation um und bietet diese Funktionalität den Fachkomponenten des Anwendungskonnektors und des VSDM-Fachmoduls an.

Diese Funktionalität ist in dem Ihnen vorliegenden Produkt Gegenstand der erfolgten sicherheitstechnischen Evaluierung gemäß Common Criteria unter der Kennung BSI-DSZ-CC-0928 und Schutzprofil PP-0047.

Andere Funktionen des Konnektors, wie die Funktionen zur Verwendung der elektronischen Signatur sind zum Zeitpunkt der Erstellung dieses Handbuchs noch nicht geprüft.

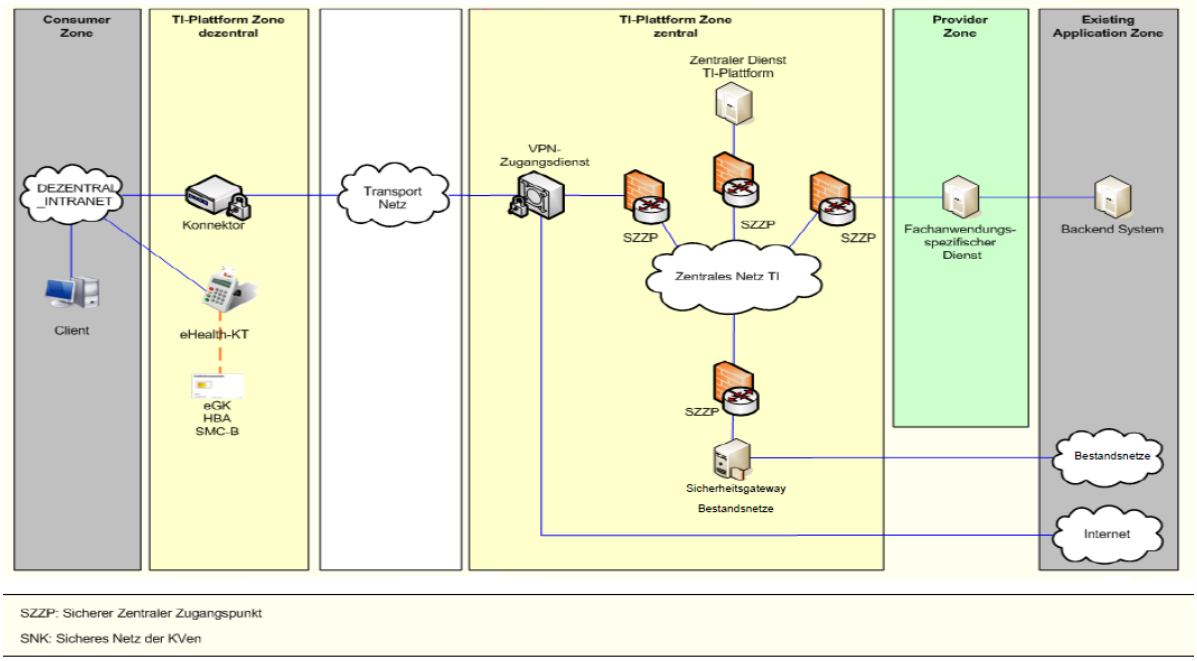


Abbildung 1 Überblick über die Telematikinfrastruktur (TI)

Der T-Systems Konnektor ist ein Gerät für den Einsatz in der Einzel- oder Gemeinschaftspraxis.

Hinweis: Teile der Funktionalität des Konnektors stehen Ihnen nur dann zur Verfügung, wenn Sie sich entscheiden, die Online-Funktionalität zu aktivieren. Die Möglichkeit zur Kommunikation mit der zentralen Telematikinfrastruktur oder die Nutzung der Online-Funktionalität des Versichertenstammdatenmanagements sind nur dann verfügbar, wenn der Konnektor die Möglichkeit hat, eine Verbindung mit dem Internet herzustellen. Wenn Sie auf die Nutzung der Online-Funktionalität verzichten, können Sie umfangreiche Funktionen des Konnektors nur in eingeschränkter Form nutzen.

Unter dem Menüpunkt Hauptmenü > Leistungsumfang können Sie den Konnektor sowohl offline als auch online konfigurieren.

Bei Fragen kontaktieren Sie uns bitte unter service.map@telekom.de.

2.2 Funktionen innerhalb der Telematikinfrastruktur

Der Konnektor dient dazu, Anwendungsprogrammen auf den Systemen der Ärzte, Krankenhäuser etc. den Zugang zur zentralen Telematikinfrastruktur des Gesundheitswesens für die Nutzung von Fachdiensten und Chipkarten zu ermöglichen. Dazu stellt der Konnektor einen sicheren Kanal zur zentralen Telematikinfrastruktur her, der für die sichere Ausführung der Anwendungsfälle genutzt wird. Darüber hinaus bietet der Konnektor Dienste für das Versichertenstammdatenmanagement und die (qualifizierte) elektronische Signatur an. Der verfügbare Leistungsumfang des Konnektors unterscheidet sich je nach Stand der eingesetzten Firmware. Der in diesem Dokument beschriebene Leistungsumfang bezieht sich auf die Firmware Version 1.4.13.

2.2.1 VPN-Zugangsdienst

Der Konnektor baut für die Kommunikation auf Transportebene mit der zentralen TI (Telematikinfrastruktur) einen verschlüsselten IPsec-Tunnel zu einem VPN-Zugangsdienst auf. Diese VPN-Verbindung wird durch den Konnektor für fachliche Anwendungsfälle mit Kommunikationsbeziehungen zu fachanwendungspezifischen Diensten sowie für Zugriffe auf die zentrale TI-Plattform im Kontext von bereitgestellten Basis-, Infrastruktur- und Netzwerkdiensten verwendet. Zusätzlich wird der IPsec-Tunnel auf Transportebene für die Kommunikation zu Bestandsnetzen genutzt.

Ein zweiter IPsec-Tunnel dient dem optionalen Zugang zum gesicherten Internetzugang (SIS - Secure Internet Service).

2.2.1.1 Zugang zur TI und SIS

Der Zugang zur TI und zum SIS (Secure Internet Service) erfolgt mit Hilfe des Konnektors und unter Verwendung eines VPN-gesicherten Tunnels. Die in diesem Zusammenhang erbrachten Sicherheitsleistungen des Konnektors sind dem Security Target für das Verfahren BSI-DSZ-CC-0928 zu entnehmen.

3 Sicherheit und Integrität

Das folgende Kapitel beinhaltet Hinweise zum sicheren Betrieb und gibt Hinweise zu den Sicherheitsfunktionen des Konnektors.

3.1 Information zum sicheren Transport und Logistik

Nach Übergabe der Sendung an den Transportdienstleister, versendet der Betreiber des Versandlagers den Lieferschein in Form einer standardisierten E-Mail an den Leistungserbringer, für den die Lieferung bestimmt ist.

Der Lieferschein enthält mindestens folgende Angaben:

- Bestellnummer der Bestellung
- Transportdienstleister
- Sendungsnummer(n) der Sendung auf der Kartonverpackung
- Geplanter Tag und Zeitspanne der Auslieferung
- Absenderadresse
- Angaben zu den Empfangsberechtigten beim Empfänger
- Lieferadresse
- Seriennummer(n) der Geräte
- Nummer der Versandtasche, in die ein Gerät (Identifikation anhand der Seriennummer) verpackt wurde
- MAC-Adresse der LAN-Schnittstellen des Geräts
- MAC-Adresse der WAN-Schnittstelle des Geräts
- Nummer des Verpackungssiegels
- Nummern aller am Gerät befindlichen Gehäusesiegel

Circa eine Stunde vor Erreichung des Fahrtziels kündigt sich der Transportdienstleister telefonisch beim Empfänger an. Ist der Mitarbeiter des Transportdienstleisters an der vorgegebenen Empfängeradresse angekommen, liefert er den Versandkarton an einen der ihm namentlich benannten Empfangsberechtigten ab. Der Empfangsberechtigte muss sich dabei durch einen Lichtbildausweis gegenüber dem Mitarbeiter des Transportdienstleisters ausweisen. Der Mitarbeiter des Transportdienstleisters weist sich unaufgefordert mit seinem Firmenausweis gegenüber dem Empfangsberechtigten aus.

Der Mitarbeiter des Transportdienstleisters darf die Sendung keiner nicht als Empfangsberechtigter benannten Person übergeben. Er fordert den Empfangsberechtigten dazu auf, unverzüglich die nachfolgend beschriebene Integritätsprüfung (Sicherheit der Geräteverpackung) durch den Leistungsempfänger durchzuführen. Der Empfangsberechtigte quittiert den Erhalt der Lieferung gegenüber dem Mitarbeiter des Transportdienstleisters. Mit der Quittierung der Übernahme geht die Verantwortung für die Geräte vom Lieferanten auf den Leistungsempfänger über.

Weiterhin kann der Leistungserbringer unter Angabe der Seriennummer sowie der beiden MAC-Adressen des Geräts beim Hersteller anfragen, ob das betreffende Gerät vom Hersteller hergestellt wurde und an wen / welches Unternehmen dieses Gerät im Rahmen der sicheren Lieferkette als direkten Empfänger ausgeliefert wurde. Der Leistungserbringer kann sich daraufhin wieder unter Angabe der Seriennummer und der beiden MAC-Adressen des Geräts an den Empfänger des Geräts wenden und erhält von dieser Auskunft darüber, an wen das Gerät im nächsten Schritt der sicheren Lieferkette ausgeliefert wurde.

Alle Akteure der sicheren Lieferkette sind verpflichtet, solche Anfragen kostenlos zu beantworten.

3.2 Sicherheit der Geräteverpackung

Nach Erhalt der Lieferung ist zu prüfen, ob die Integrität des Geräts vorhanden ist oder ob von einer Integritätsverletzung ausgegangen werden muss. Die dazu erforderlichen Prüfungen sind nachfolgend beschrieben:

- Prüfung der Bestellung: Ist die Lieferung gemäß Ihrer Bestellnummer erfolgt?
- Ist die Lieferung sowie die Geräteverpackung unbeschädigt?
    - Die Lieferung erfolgt mit einer sicheren Versandtasche, welche nicht ohne sichtbare Beschädigung geöffnet werden kann.
    - Ist an der Tasche eine sichtbare Manipulation erfolgt, ist die Annahme zu verweigern und der Hersteller davon in Kenntnis zu setzen.
    - Prüfung des Konnektor Kartons auf Manipulation (Löcher oder Risse)
    - Prüfung des Verpackungssiegels, welches über die Lasche der Öffnung geklebt ist (Siehe blauer Kreis in dem Bild). Ein Muster des Siegels ist in Kapitel 3.4.1 abgebildet.
    - Auf der Internetseite des Herstellers ist zu prüfen, ob die Siegelnummer korrekt ist.

Es ist dafür zu sorgen, dass bis zur Installation durch einen Service-Techniker der Konnektor vor unbefugten Zugriffen geschützt ist.

3.3 Sicherheitshinweise Hardware

Achtung Lebensgefahr!

- Überlastete Teile der Stromversorgung bergen ein Brand- und Stromschlagrisiko! Vermeiden Sie Überlastungen von Steckdosen durch den Anschluss des Konnektors an Verlängerungskabel und Steckdosenleisten!
- Durch unsachgemäßes Öffnen und Reparieren des Geräts kann Lebensgefahr für den Anwender entstehen! Öffnen Sie das Gehäuse nicht!
- Der T-Systems Konnektor darf nicht mit Flüssigkeit in Kontakt kommen.

3.3.1 Was tun bei Diebstahl oder erkennbarer Manipulation des Geräts?

Der Konnektor ist eine sicherheitskritische Komponente zur Anbindung einer dezentralen medizinischen Einrichtung (z.B. Arztpraxis) an die zentrale Telematikinfrastruktur. Ein möglicher Missbrauch des Geräts muss verhindert werden, sodass unbefugte Dritte über diesen freigeschalteten Konnektor keinen Zugang zur zentralen Telematikinfrastruktur erlangen können. Patientendaten sind hierdurch nicht kompromittiert, da diese nicht auf dem Konnektor hinterlegt sind! Auch die SMC-B Karte (Security Module Card Typ B) kann hiervon unbenommen weiterverwendet werden.

Hinweis: Die Entwendung des Konnektors oder ein gebrochenes Sicherheitssiegel muss umgehend gemeldet und die enthaltene gSMC-K[1] Karte gesperrt werden!

Die Meldung hat an den PKI-Betreiber zu erfolgen: T-Systems International GmbH

Die Kontaktdaten finden Sie im entsprechenden Kapitel im Anhang A.1.1.

Prüfen Sie in jedem Fall auch Ihre Einsatzumgebung auf eventuelle andere Manipulationen, sowohl bezüglich Ihrer medizinischen und verwaltungstechnischen Gegenstände, wie auch hinsichtlich Ihrer IT-Ausstattung (Server, PCs und auch Kartenterminals).

Wenden Sie sich auch bei jeglichem Zweifel an der Unversehrtheit des Konnektors oder der Unversehrtheit Ihrer Maßnahmen zum Zugriffsschutz an Ihren Systempartner oder direkt an die T-Systems International GmbH und nutzen Sie den Konnektor bis zur Klärung des Sachverhalts nicht weiter.

3.4 Sicherheitsmaßnahmen in der IT-Einsatzumgebung

Bitte berücksichtigen Sie auch die unter A.6 aufgeführten Hinweise zur Sicherheitszertifizierung des Produkts für weitere Informationen.

- Die Sicherheitsmaßnahmen in der Einsatzumgebung müssen vor dem Zugriff Unbefugter schützen.
- Sowohl während, als auch außerhalb aktiver Datenverarbeitung des Konnektors müssen die Sicherheitsmaßnahmen in der Umgebung sicherstellen, dass ein Diebstahl oder Manipulationen des Konnektors erkannt werden.
- Sichern Sie das Gerät so, dass ein unberechtigter Austausch des Geräts verhindert oder erkannt wird (z.B. verschlossener Raum).
- Es muss sichergestellt sein, dass der T-Systems Konnektor in der vorgesehenen und in diesem Handbuch beschriebenen Art und Weise administriert wird.

[1] gerätespezifische Security Module Card Konnektor

- Alle Administratoren in der zentralen Telematikinfrastruktur müssen fachkundig und vertrauenswürdig sein. Außerdem müssen die Administratoren ihre Authentisierungsinformationen und -token (z.B. PIN bzw. Passwort oder Schlüssel-Token) geheim halten bzw. dürfen diese nicht weitergeben.
- Der Konnektor kann bestimmte Arten von Manipulationsversuchen erkennen und diese an Sie melden. Achten Sie auf solche Meldungen! Achten Sie während des Betriebs des Konnektors auf Meldungen, die Sie im Kontext Ihrer Arbeit nicht erwarten würden. Diese können auf Manipulation des Geräts hindeuten.
- Halten Sie die Firmware des T-Systems Konnektors sowie die zugehörigen Administrationsprogramme stets aktuell. Verwenden Sie nur durch die gematik GmbH (www.gematik.de) zugelassene, zertifizierte und bestätigte Firmware-Versionen.
- Die Schnittstellen des T-Systems Konnektors müssen in der vorgesehenen Art und Weise verwendet werden. Es dürfen nur solche Hard- und Softwareprodukte eingesetzt werden, die diese Voraussetzungen erfüllen.
- Es wird davon ausgegangen, dass Angriffe aus dem Netz der zentralen TI-Plattform ausgeschlossen werden können. Das schließt auch Angriffe auf den Konnektor oder auf die lokalen Netze der Leistungserbringer aus weiteren Netzen ein, die mit der TI verbunden sind.
- An das lokale Netzwerk (LAN-Switches inklusive Wireless Access Points und Router) angeschlossene Systeme welches durch ein LAN-Kabel mit der LAN-Buchse des T-Systems Konnektors verbunden ist, müssen über zeitgemäße Sicherheitsmechanismen verfügen, regelmäßig aktualisiert und durch Fachpersonal administriert werden.
- Es muss ein gesicherter Zugangspunkt zum Internet vorhanden sein. Dieser Zugangspunkt muss die dahinterliegenden Netze wirksam gegen Angriffe aus dem Internet schützen.
- Die Betreiber der zentralen Telematikinfrastruktur ergreifen geeignete Maßnahmen, um Denial of Service (DoS) Angriffe aus dem Transportnetz gegen die zentrale Telematikinfrastruktur abzuwehren.
- Als Ersatzverfahren kann der Konnektor ebenfalls nach erfolgreicher Konfiguration und Verbindung mit der TI im Offline Modus genutzt werden.

Sehr viele Einträge im Sicherheitsprotokoll können ein Hinweis auf eine DoS-Attacke sein.

- Es muss sichergestellt sein, dass administrative Tätigkeiten der lokalen und entfernten Administration in Übereinstimmung mit diesem Handbuch durchgeführt werden. Insbesondere muss für diese Tätigkeiten vertrauenswürdiges und ausgebildetes Personal eingesetzt werden.
- Der Konnektor verwendet eine interne Chipkarte (gSMC-K) als Sicherheitsmodul zur Verwaltung der Geräteidentität und als Lieferant kryptografisch sicherer Zufallszahlen. Zusätzlich werden interne Zufallszahlengeneratoren des Konnektors mit Hilfe der Chipkarte initialisiert.

3.4.1 Sicherer Betrieb von Nutzeranwendungen und Nutzerkomponenten

- Setzen Sie nur Anwendungen und Komponenten ein, die nach dem aktuellen Stand der Technik entwickelt wurden und das spezifizierte Verhalten zeigen.

- Die Anwendungen und Komponenten müssen in der gleichen sicheren Art und Weise administriert werden wie der T-Systems Konnektor.
- Es muss sichergestellt sein, dass die Anwendungen und Komponenten den Konnektor in der spezifizierten Art und Weise nutzen, insbesondere die spezifizierten Konnektor-Schnittstellen korrekt nutzen.
- Es muss sichergestellt sein, dass keine Schadsoftware auf die Nutzerkomponenten oder andere IT-Systeme im LAN eingespielt wird (z.B. Einspielen von ausführbaren Dateien über lokale optische Laufwerke oder über USB-Sticks, Öffnen von E-Mail-Anhängen).
- Eine Anbindung der Client Systeme und Komponenten an potentiell unsichere Netze (z.B. Internet) sollte aufgrund des daraus entstehenden Risikos möglichst unterbunden werden und somit ausschließlich in sicherer Art und Weise erfolgen. Beim Zugang über ungeschützte oder schlecht geschützte Zugänge besteht das Risiko, dass die Vertraulichkeit und Integrität der übertragenen Daten nicht gewährleistet werden kann.
- Die Nutzung des sicheren Internet Service obliegt Ihrer Entscheidung. Die Funktionalität des Konnektors ist beschränkt auf das Routing des Datenverkehrs. Weitere Sicherheitsleistungen werden nicht angeboten. Es obliegt Ihrer Verantwortung, weitere geeignete Sicherheitsmaßnahmen zu ergreifen (Firewall, Virenscanner etc.), da auch Angriffe über den sicheren Internet Service nicht vollständig ausgeschlossen werden können.
- Im Modus Parallel (siehe auch Kapitel 4.7) ist kein Internetzugriff über den sicheren SIS-Zugang möglich. Die Internetverbindung muss also selbstständig abgesichert werden. Die Einstellung des Modus Parallel erfolgt durch die Deaktivierung des WAN-Adapters.

Hinweis: Sie sind verpflichtet, vor der ersten Inbetriebnahme, sowie in regelmäßigen Abständen die Unversehrtheit des angebrachten Sicherheitssiegels zu prüfen. Prüfen Sie also wenigstens einmal in der Woche, ob sich das Siegel noch in einem ordnungsgemäßen (originalen) Zustand befindet. Sofern Sie den Verdacht haben, dass das Gehäuse des T-Systems Konnektors geöffnet wurde (zu erkennen am gebrochenen Sicherheitssiegel), nehmen Sie das Gerät außer Betrieb und kontaktieren Ihren Servicetechniker. Weitergehende Fragen hierzu richten Sie bitte an den Herausgeber des Konnektors: T-Systems International GmbH. Die Kontaktdaten finden Sie im Anhang A.1.2.

Folgendes Bild zeigt die Positionen an denen die Siegel am Konnektor Gehäuse angebracht sind.

Muster Siegel

Jedes Siegel hat eine eindeutige Seriennummer die bei der Produktion registriert wird. Es läßt sich nicht rückstandsfrei entfernen, da es sich um ein Sicherheitssiegel handelt. Eine Manipulation ist somit jederzeit sichtbar, sollte versucht worden sein, ein Siegel zu entfernen. Es garantiert dem Leistungsempfänger ein einwandfreies Produkt.

3.5 Sicherheitsfunktionen des T-Systems Konnektors

In der folgenden Tabelle werden die geprüften Sicherheitsfunktionen des T-Systems Konnektors aufgelistet. Mit einem Neustart des Konnektors haben Sie die Möglichkeit die Integrität der Sicherheitsfunktionen zu überprüfen. Sollten die Funktionen nicht integer sein, wird dies durch eine rot leuchtende Status-LED (siehe Kapitel 4.4) sowie die Anzeige zweistelliger Fehlercodes im Display angezeigt. Weitere Informationen zur Umsetzung dieser Sicherheitsfunktionen entnehmen Sie bitte den jeweiligen Abschnitten.

Tabelle 3 Überblick über die geprüften Sicherheitsfunktionen des T-Systems Konnektors

Funktion	Beschreibung
VPN-Verbindungen	Der T-Systems Konnektor bietet die Funktion des Aufbaus einer IPsec-gesicherten Verbindung in das Netz der zentralen Telematikinfrastruktur an. Dazu beinhaltet der T-Systems Konnektor einen sogenannten VPN-Client. Nähere Erläuterungen zum VPN-Client finden Sie im Abschnitt 3.3.1
Zeitsynchronisation	Im Onlinemodus und bei bestehender VPN-Verbindung synchronisiert der T-Systems Konnektor mit Hilfe des NTP-Protokolls die interne Systemuhr. Diese Funktion bietet zwei Vorteile: die Uhrzeit des T-Systems Konnektors muss von Ihnen nicht überwacht werden, sofern Sie sich entscheiden, den T-Systems Konnektor im Online-Betrieb zu verwenden. Des Weiteren haben Sie die Möglichkeit, den T-Systems Konnektor innerhalb Ihres Netzwerks als Zeitgeber für andere Geräte zu verwenden. Mehr Informationen dazu finden Sie im Abschnitt 3.5.2.
Administration	Die Möglichkeit zur Administration des T-Systems Konnektors wird Ihnen über eine grafische Administrationsschnittstelle angeboten, die Sie über den Browser Ihres PCs oder anderer netzwerkfähiger Geräte mit der Möglichkeit zur HTML-Ausgabe verwenden können (siehe Kapitel 4). Mit Hilfe dieser Schnittstelle haben Sie zudem die Möglichkeit, die Komponenten des Anwendungskonnektors zu administrieren. Wenn Sie Hilfe bei der Einrichtung und Konfiguration des Konnektors benötigen, können Sie die Fernwartung des Systems zulassen, indem Sie über die Administrationsschnittstelle eine sogenannte Fernwartung zulassen. Mehr Einzelheiten da zur Administration finden Sie im Abschnitt 5.1.2 oder 7.13
Firewall	Der T-Systems Konnektor verfügt über eine integrierte Firewall. Diese Firewall schützt sowohl die Sicherheitsdienste des Konnektors als auch die Geräte in Ihrem Netzwerk vor unberechtigten Zugriffen. Weitere Informationen zu diesem Thema finden Sie im Abschnitt 3.5.4

In der folgenden Tabelle werden weitere nutzbare Funktionen aufgeführt.

Tabelle 4 Weitere nutzbare Funktionen

Funktion	Beschreibung
DHCP-Dienste	Der T-Systems Konnektor kann als Dienst zur Vergabe von IP-Adressen im internen Netzwerk eingesetzt werden. Bitte lesen Sie den Abschnitt 3.5.5, wenn Sie weitere Informationen dazu wünschen.
DNS-Resolver	Es besteht die Möglichkeit, den T-Systems Konnektor als DNS-Resolver zu verwenden. Weitere Informationen dazu finden Sie im Abschnitt 3.5.6

3.5.1 VPN-Client

Der VPN-Client des Konnektors handelt die kryptografischen Parameter für eine IPsec-gesicherte Verbindung mit der zentralen Telematikinfrastruktur aus. Dabei wird das Protokoll IKEv2 zur Aushandlung einer sicheren Verbindung im Tunnel-Modus verwendet. Der VPN-Client authentisiert den Einwahlpunkt in die zentrale Telematikinfrastruktur auf Grundlage eines elektronischen Zertifikats. Diese Authentisierung wird vom Konnektor durchgesetzt und kann nicht umgangen werden.

Der VPN-Client des Konnektors arbeitet ebenfalls mit einem elektronischen Zertifikat, welches auf dem internen Sicherheitsmodul (gSMC-K) abgelegt ist. Konnten die kryptografischen Parameter erfolgreich ausgehandelt werden, verbinden sich beide Kommunikationsteilnehmer unter Verwendung des Protokolls IPsec. Mit diesem gesicherten Tunnel ist es nun möglich, in sicherer Art und Weise mit der zentralen Telematikinfrastruktur zu kommunizieren.

3.5.2 Zeitsynchronisation

Die Zeitsynchronisation des T-Systems Konnektors erfolgt von einem NTP-Server, der sich in der sicheren Telematikinfrastruktur befindet. Um diese Funktion nutzen zu können, muss der Konnektor eine Verbindung in die Telematikinfrastruktur aufbauen. Dies bedeutet, dass der Konnektor im Modus Online betrieben werden muss. Die Zeitsynchronisation ist aus mehreren Gründen wichtig:

1. Der T-Systems Konnektor bietet einen sogenannten NTP-Server der Stratum-Ebene 3[2] an. Mit Hilfe dieses Dienstes können Systeme in Ihrem Netz die Zeitsynchronisation in Anspruch nehmen.
2. Der T-Systems Konnektor prüft elektronische Zertifikate. Ein elektronisches Zertifikat bestätigt die Identität der Gegenstelle (z.B. die Identität des Einwahlpunktes in die zentrale Telematikinfrastruktur) und beinhaltet Informationen über verwendete kryptografische Parameter (Algorithmen). Ein elektronisches Zertifikat ist ab einem bestimmten Zeitpunkt gültig und kann zu einem bestimmten Zeitpunkt ablaufen. Damit der T-Systems Konnektor die Gültigkeit von Zertifikaten zuverlässig überprüfen kann, ist es notwendig, dass der

[2] Stratum Ebenen bezeichnen die Entfernung (durch Anzahl benannt) des NTP-Servers von einer zeitgebenden Quelle.

Konnektor mit der korrekten Zeit konfiguriert ist. Wird der Konnektor online betrieben, erfolgt diese Zeitsynchronisation automatisch über die zentrale Telematikinfrastruktur.

3. Der T-Systems Konnektor bietet eine Sicherheitsprotokollierung an. Die Sicherheitsprotokollierung gibt Auskunft über Ereignisse, die für die Sicherheit des Systems relevant sind. Diese Einträge werden ebenso wie andere Protokollierungseinträge (z.B. zur Performance oder allgemein zu Fehlersituationen) mit einer Zeitmarke versehen. Diese Zeitmarke gibt den Zeitpunkt des Ereignisses an.

Hinweis: Im Offline-Modus erfolgt keine automatische Synchronisation der Systemzeit des Konnektors. In diesem Fall ist der Administrator für die korrekte Zeiteinstellung verantwortlich. Die Zeit muss bei der Inbetriebnahme und regelmäßig alle 3 Jahre korrekt eingestellt werden. Der lokale Administrator des Konnektors sollte daher in regelmäßigen Abständen die Richtigkeit der Uhrzeit auf dem Konnektor überprüfen.

3.5.3 Administration

Der Konnektor bietet eine Administrationsschnittstelle an, mit der die wichtigsten Funktionen konfiguriert werden können.

Hinweis: Die Administrationsoberfläche des T-Systems Konnektors ist unter https://10.10.8.15:4433 verfügbar sobald der T-Systems Konnektor gestartet ist (siehe Kapitel 5.1).

Ein Teil dieser Administrationsschnittstelle umfasst auch Funktionen, die direkt den T-Systems Konnektor betreffen. Dazu gehören unter anderem:

1. Konfiguration der Netzwerkschnittstellen
2. Konfiguration des VPN-Clients
3. Einsichtnahme in den Vertrauensraum des Konnektors
4. Import von Vertrauens- und Sperrlisten

Neben diesen Konfigurationsoptionen besteht die Möglichkeit, Funktionen des T-Systems Konnektors auszuführen. Dazu zählen unter anderem die Zeitsynchronisation, der manuelle Aufbau eines VPN-Tunnels oder das Auflösen von Domainnamen mittels eines DNS-Servers. Zur besseren Verständlichkeit werden die Konfigurationsoptionen anhand der grafischen Schnittstelle erläutert.

Nehmen Sie Änderungen an der Konfiguration nur dann vor, wenn Sie deren Bedeutung verstanden haben.

Neben der grafischen Administration über den Browser haben Sie die Möglichkeit, das System mit Hilfe eines entfernten Zugriffs konfigurieren zu lassen (Remote-Administration).

Um diese Möglichkeit zu nutzen, benötigen Sie einen Servicevertrag. Informieren Sie sich bitte bei Ihrem Lieferanten zu den angebotenen Optionen.

3.5.4 Firewall

Die Firewall des T-Systems Konnektors schützt die Kommunikation zwischen Ihrem Netzwerk und anderen Netzen. Es wird grundsätzlich sämtlicher ein- und ausgehender Datenver-

kehr auf die Einhaltung der vorgegebenen Kommunikationsregeln überprüft. Dies ist notwendig, da Sie bei Verwendung der Online-Funktionalität des Konnektors mit Kommunikationspartnern in verschiedenen Netzen verbunden sein können.

Die Firewall setzt Kommunikationsregeln sowohl für das Netz des Leistungserbringers und das WAN, als auch für den Datenverkehr innerhalb der aufgebauten VPN-Tunnel durch. Die angewandten Filterregeln sind im Security Target des Verfahrens BSI-DSZ-CC-0928 beschrieben.

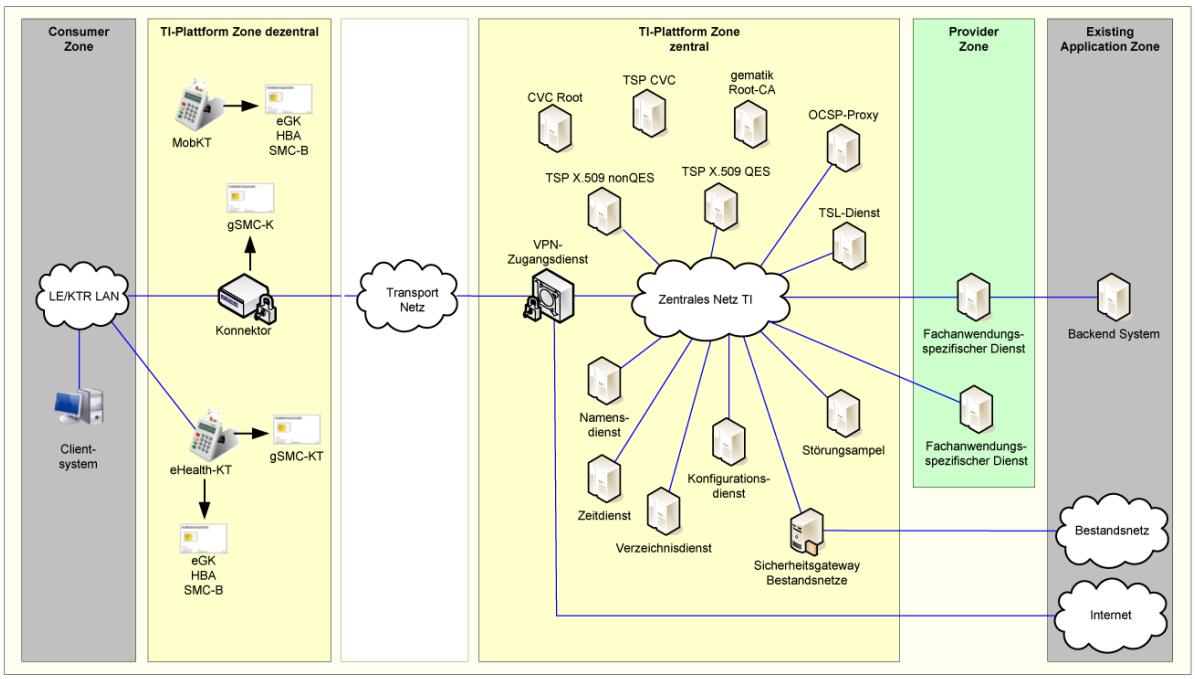


Abbildung 2 Übersicht des Gesamtsystems der TI

Die grundlegende Sicherheitsregel (policy) der T-Systems Konnektor-Firewall besteht darin, dass sämtlicher Datenverkehr, der nicht vom Konnektor initiiert wurde oder nicht an Dienste des Netz- und Anwendungskonnektors gerichtet ist, blockiert wird. Ein aktiver Zugriff auf Ihr Netzwerk über den T-Systems Konnektor ist nicht möglich. Zudem filtert die integrierte Firewall den Datenverkehr dahingehend, dass ausschließlich zulässige Protokolle und Fachdienste Zugriff auf die jeweiligen Netze erlangen.

Die Firewall ist eng mit der Sicherheitsprotokollierung verknüpft. Wird eine Regelverletzung erkannt, so wird diese im Sicherheitsprotokoll des Konnektors protokolliert. Sie können sich in Kapitel 7.10 über die Auswertung des Sicherheitsprotokolls informieren.

Der T-Systems Konnektor filtert den Datenverkehr auf Basis von fest hinterlegten Firewallregeln. Die Administration der Firewall ist nur eingeschränkt möglich. Insbesondere besteht keine Möglichkeit, die bestehenden Regeln zu deaktivieren oder die Firewall gänzlich abzuschalten. Dem Administrator ist es aber möglich, weitere Regeln zu aktivieren und somit weiteren Datenverkehr zu blockieren (siehe Kapitel 6.4).

Es können allerdings nur Firewall-Regeln definiert werden, die den ausgehenden Verkehr verbieten. Diese einschränkenden Regeln gelten auch nur, wenn der SIS für die Kommunikation verwendet wird.

Nachfolgend ist zur Übersicht das Gesamtsystem der Telematikinfrastruktur dargestellt und die für die verschiedenen Netze fest hinterlegten Firewallregeln beschrieben.

Tabelle 5 Firewallregeln für das Netz der Telematik

Telematikinfrastruktur	
Dieses Netz bietet verschiedene Sicherheits- und Fachdienste an und ist vertrauenswürdig. Die Adressen der Netzsegmente für die Sicherheits- und Fachdienste sind fest hinterlegt (siehe Abschnitt 6.5). Für die verschiedenen Netzsegmente gelten folgende Regeln:	
Netz der gesicherten Fachdienste	▪ Sicherstellung, dass alle Pakete, die für die Kommunikation mit einem Fachdienst bestimmt sind, ausschließlich über den VPN-Tunnel der TI übertragen werden. ▪ Verwerfen aller Pakete aus dem Netz des Leistungserbringers ▪ Verwerfen aller Pakete, die an den Konnektor gehen ▪ Die Verbindung ist nur vom T-Systems Konnektor und vom Fachmodul erlaubt
Netz der offenen Fachdienste	▪ Sicherstellung, dass alle Pakete, die für die Kommunikation mit einem Fachdienst bestimmt sind, ausschließlich über den VPN-Tunnel der TI übertragen werden. ▪ Verwerfen aller vom Konnektor initiierten Pakete ▪ Verwerfen aller Pakete, die an den Konnektor gehen ▪ Die Verbindung ist nur vom Netz des Leistungserbringers und vom Fachmodul erlaubt
Netz der zentralen TI	▪ Sicherstellung, dass alle Pakete, die für die Kommunikation mit einem Fachdienst bestimmt sind, ausschließlich über den VPN-Tunnel der TI übertragen werden. ▪ Verwerfen aller Pakete aus dem Netz des Leistungserbringers ▪ Verwerfen aller Pakete, die an den Konnektor gehen ▪ Die Verbindung ist nur vom T-Systems Konnektor erlaubt
Netz der dezentralen TI	▪ Verwerfen aller Pakete vom Konnektor und an den Konnektor gehend ▪ Verwerfen aller Pakete aus dem Netz des Leistungserbringers ▪ Die Kommunikation ist nur vom T-Systems Konnektor erlaubt

Tabelle 6 Firewallregeln für das Internet

Internet	
Der T-Systems Konnektor ermöglicht unter Verwendung des sicheren Internet Service (SIS) einen Zugang zum Internet. Die Adressen der Netzsegmente des SIS sind fest hinterlegt (siehe Abschnitt 6.5 , Für die verschiedenen Netzsegmente gelten folgende Regeln:	
Netz des SIS	▪ Verwerfen aller Pakete vom Konnektor und an den Konnektor gehend ▪ Verwerfen aller Pakete aus dem Netz des Leistungserbringers
Internet via SIS	▪ Verwerfen aller Pakete aus dem Netz des Leistungserbringers, wenn kein Internet-Modus SIS konfiguriert wurde (siehe Abschnitt 6.2) ▪ Umleitung aller Pakete aus dem Netz des Leistungserbringers an Hosts im Internet, wenn der Internet-Modus SIS konfiguriert wurde (siehe Abschnitt 6.2) Verwerfen aller Pakete, die an den Konnektor und an das Netz des Leistungserbringers gesendet werden

Internet	
	▪ Die Verbindung ist nur erlaubt vom Konnektor und vom Netz des Leistungserbringers, wenn der Internet-Modus SIS konfiguriert wurde
Internet via IAG (Internet Access Gateway)	▪ Beim Anbindungsmodus Parallel werden alle Pakete verworfen, die nicht an die LAN-IP-Adresse adressiert sind und nicht aus dem Netz des Leistungserbringers stammen ▪ Beim Anbindungsmodus InReihe werden alle Pakete verworfen, die nicht an die WAN-IP-Adresse adressiert sind ▪ Kommunikation ist erlaubt für das Protokoll IPsec zu den VPN-Konzentratoren der TI bzw. des SIS ▪ Kommunikation ist ausgehend erlaubt für das Protokoll HTTP und HTTPS zu den Provideradressen der CRL, des DNS Root Anchors, des Hash- & URL-Servers und des Registrierungsservers ▪ Kommunikation ist ausgehend erlaubt für das Protokoll DNS ▪ Blockieren der Kommunikation aus dem Netz des Leistungserbringers für die Fälle: ▪ Internet-Modus = Keiner (siehe Abschnitt 6.2) ▪ Internet-Modus = Verbindungsstatus zur TI = Nicht möglich (siehe Abschnitt 6.1) ▪ Internet-Modus = Leistungsumfang Logisch getrennt (siehe Abschnitt 7.2) Dieses Feature ist abgekündigt und soll nicht mehr verwendet werden. ▪ Für den Fall Internet-Modus IAG oder Keiner, werden alle Pakete aus dem Netz des Leistungserbringers, die nicht für die Netze der TI bestimmt sind, zum Default-Gateway umgeleitet ▪ Blockieren aller Pakete aus Richtung des IAG

Tabelle 7 Firewallregeln für Bestandsnetze

Bestandsnetze	
Dazu zählen Kommunikationsnetze, mit denen Sie heute bereits zum Zwecke der Kommunikation - auch medizinischer Daten - verbunden sein können. Der Begriff Bestandsnetze meint die Obermenge aller vorhandener Netzsegmente, die in Abbildung 1 Überblick über die Telematikinfrastruktur (TI) in dem Bereich Existing Application Zone aufgeführt sind. Dabei handelt es sich um Netze, die bereits heute für den Austausch medizinischer Daten verwendet werden, aber nicht originär zur Telematikinfrastruktur (TI) zählen, allerdings über den VPN-Zugang der Telematikinfrastruktur erreichbar sind. Um mit einem solchen Netzsegment zu kommunizieren, muss dieses Segment in der Konfiguration aktiviert werden (siehe Kapitel 6.5). Es wird der Untermenge Aktive Bestandsnetze zugeordnet.	
Netz der aktiven Bestandsnetze	▪ Sicherstellung, dass alle Pakete, die für die Kommunikation mit einem Fachdienst bestimmt sind, ausschließlich über den VPN-Tunnel der TI übertragen werden. ▪ Wenn der Konnektor für die logische Separation konfiguriert wurde, werden alle Pakete verworfen, die aus dem Netz des Leistungserbringers kommen. Dieses Feature ist abgekündigt und soll nicht mehr verwendet werden. ▪ Verwerfen aller Pakete an nicht freigegebene Bestandsnetze ▪ Verwerfen aller Pakete, die an den Konnektor gehen ▪ Die Verbindung ist nur erlaubt vom Konnektor für DNS und vom Netz des Leistungserbringers

Tabelle 8 Firewallregeln für das Netz des Leistungserbringers

Netz des Leistungserbringers	
Das ist das Netz der Arztpraxis oder des Krankenhauses. Hier befinden sich z.B. die Kartenterminals und Praxisverwaltungssysteme. Die gesamte Kommunikation zu den Diensten der TI und des SIS wird ausschließlich über den Konnektor geleitet.	
	Verwerfen aller Pakete, die nicht aus dem Netz des Leistungserbringers und seiner konfigurierten Netzsegmente stammen
	Kommunikation ist nur erlaubt für den Zugriff auf die Dienste, die der Konnektor selbst anbietet. Alle weitere Kommunikation wird blockiert.
	Kommunikation ist erlaubt vom Konnektor ausgehend
	Kommunikation aus einem Intranet-VPN wird blockiert
	Wenn Intranet-Routen-Modus = Block (siehe Abschnitt 6.2) konfiguriert ist, dann wird jeglicher Verkehr aus dem Netz des Leistungserbringers blockiert
	Wenn Intranet-Routen-Modus = Redirect (siehe Abschnitt 6.2) konfiguriert ist, dann wird der Datenverkehr aus dem Netz des Leistungserbringers auf das adressierte Subnetz (siehe Abschnitt 6.3) umgeleitet.

Tabelle 9 Allgemeine Firewallregeln

Allgemeine Regeln	
	▪ TCP-Port-7(Echo)-Pakete werden verworfen ▪ ICMP-EchoRequest (Typ 8) und ICMP-EchoResponse (Typ 0) ist ausschließlich für die oben aufgeführte zugelassene Kommunikation möglich ▪ DHCP-Pakete aus der TI oder dem SIS werden verworfen ▪ Verwerfen von nicht vom Konnektor initiierten IPsec-Paketen (IKE, ESP und IPsec NAT-T) ▪ Es ist nur Kommunikation der IP-Protokolle 1 (ICMP), 17 (UDP), 6 (TCP) und 50 (ESP) möglich.

Die Firewall des Konnektors bietet keinen Ersatz für einen Virenscanner und andere erforderliche Schutzmaßnahmen. Angriffe durch Viren und Trojaner kann der Konnektor nicht abwehren. Die Aufgabe des Konnektors besteht in der Sicherstellung vertrauenswürdiger Kommunikationskanäle, insbesondere in die Telematikinfrastruktur. Verwenden Sie in Ihrem Netzwerk ausschließlich vertrauenswürdige Software!

3.5.5 DHCP-Dienste

Sie haben die Möglichkeit den T-Systems Konnektor zur Vergabe von Netzwerkadressen in Ihrem Netzwerk zu verwenden. Diese Funktion wird als DHCP-Server bezeichnet und kann optional verwendet werden.

Wenn Sie bereits über ein Netzwerk verfügen, in das Sie Ihre Geräte eingebunden haben, verfügen Sie möglicherweise bereits über einen lokalen DHCP-Server. Üblicherweise wird diese Funktion von Ihrem Netzwerkrouter angeboten. Wenn Sie diese Konfiguration weiter beibehalten wollen, dann müssen Sie den DHCP-Server des Konnektors deaktivieren, da sonst Adresskonflikte zwischen den Netzwerkgeräten auftreten. Unter dem Menüpunkt DHCP-Server können Sie den Server ein- und ausschalten.

Wenn Sie den DHCP-Server des Konnektors nutzen wollen, dann müssen Sie den in Ihrem Router konfigurierten DHCP-Server deaktivieren und ihre vorhandenen Netzwerkgeräte neu konfigurieren.

Alternativ haben Sie die Möglichkeit den T-Systems Konnektor so zu konfigurieren, dass dieser den bereits vorhandenen DNS-Server verwendet oder mit einer sogenannten statischen IP-Adresse betrieben wird. Damit verwenden Sie den integrierten DNS-Client. Der DNS-Client des Konnektors in Richtung Ihres Netzwerks kann nicht gemeinsam mit dem DNS-Server in Richtung Ihres Netzwerks betrieben werden.

3.5.6 DNS-Resolver

Der T-Systems Konnektor bietet die Funktion eines DNS-Stub-Resolvers an. Das Protokoll DNS (Domain Name System) bietet die Möglichkeit, einen Domainnamen (z.B. www.gematik.de) in eine IP-Adresse zu übersetzen. Der Grund dafür besteht darin, dass die Netzwerkkommunikation ausschließlich auf Basis von IP-Adressen (v4 und v6) arbeitet und die Verwendung von Namenseinträgen der besseren Verständlichkeit dient. Die Funktion des DNS-Stub-Resolvers bedeutet, dass der T-Systems Konnektor DNS-Anfragen nicht selbst auflöst, sondern solche Anfragen an den eingestellten (konfigurierten) DNS-Server weiterleitet und dem ursprünglich anfragenden System in Ihrem Netz die Auskunft zur Verfügung stellt. Die Nutzung dieser Funktionalität ist optional.

3.5.7 Hinweise zur Verwendung des integrierten Sicherheitsmoduls

Der T-Systems Konnektor verwendet ein integriertes Sicherheitsmodul zur Speicherung kryptografischer Schlüssel. Dieses Sicherheitsmodul trägt die Bezeichnung gSMC-K. Die korrekte Arbeitsweise des Netz- und Anwendungskonnektors ist maßgeblich von diesem Sicherheitsmodul abhängig. Das Sicherheitsmodul wurde eigenständig einer Prüfung gemäß Common Criteria und zugehöriger Richtlinien unterzogen.

3.5.8 Aktivierung DNSSEC

Wird der Konnektor als DHCP-Client in der bestehenden Infrastruktur betrieben, so kann ein Fehler bei der Namensauflösung (DNS-Resolver) auftreten. Diese Situation kann u.a. entstehen, wenn die über das zugewiesene Gateway publizierten DNS-Server keine DNSSEC-Funktionalität aufweisen.

In diesem Fall muss unter Verwendung der Schaltfläche "Verwendung DHCP DNS ausschalten" der über das Gateway zugewiesene DNS-Eintrag durch einen manuell hinzuzufügenden DNS Server Eintrag ersetzt werden, welcher über DNSSEC-Funktionalität verfügt.

Dies ist erforderlich, um die VPN-Verbindung vom Konnektor zur Telematik Infrastruktur aufzubauen.

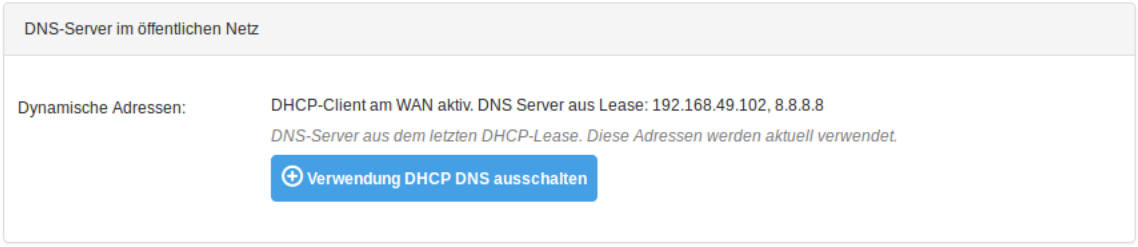


Abbildung 3 DHCP DNS ausschalten

4 In- und Außerbetriebnahme der Hardware

4.1 Bevor Sie den Konnektor anschließen

4.1.1 Lieferung des Konnektors

Bitte achten Sie in jedem Fall darauf, dass

1. die Lieferung aufgrund Ihrer Bestellung erfolgt ist (korrekte Bestellnummer),
2. die Lieferung durch einen auf der Hersteller-Webseite gelisteten Lieferanten durchgeführt wird,
3. das Informationsschreiben mit den Angaben zur Lieferung von Ihrem Vertragspartner gesendet wurde und vorliegt,
4. der Karton des T-Systems Konnektors ungeöffnet ist,
5. der Inhalt des Kartons des T-Systems Konnektors vollständig und unbeschädigt ist (siehe hierzu Abschnitt 4.2),
6. sich auf dem T-Systems Konnektor zwei Sicherheitssiegel befinden.
7. sich auf der Unterseite des Konnektors ein Typenschild nachfolgendem Muster befindet:

Wichtig: Das Typenschild zeigt das Ablaufdatum des Zertifikates und somit die maximale Nutzungsdauer des Konnektors. Es sind keine Installationsfristen oder Zeiträume einzuhalten. Durch eine spätere Inbetriebnahme verkürzt sich nur die Nutzungsdauer des Gerätes.

Im Fall von Abweichungen verweigern Sie die Annahme des Gerätes oder lassen Sie es an den Absender zurückgehen.

Bitte bewahren Sie die Übergabedokumente auf, sodass ein einfacher Austausch des Gerätes später nachweisbar ist.

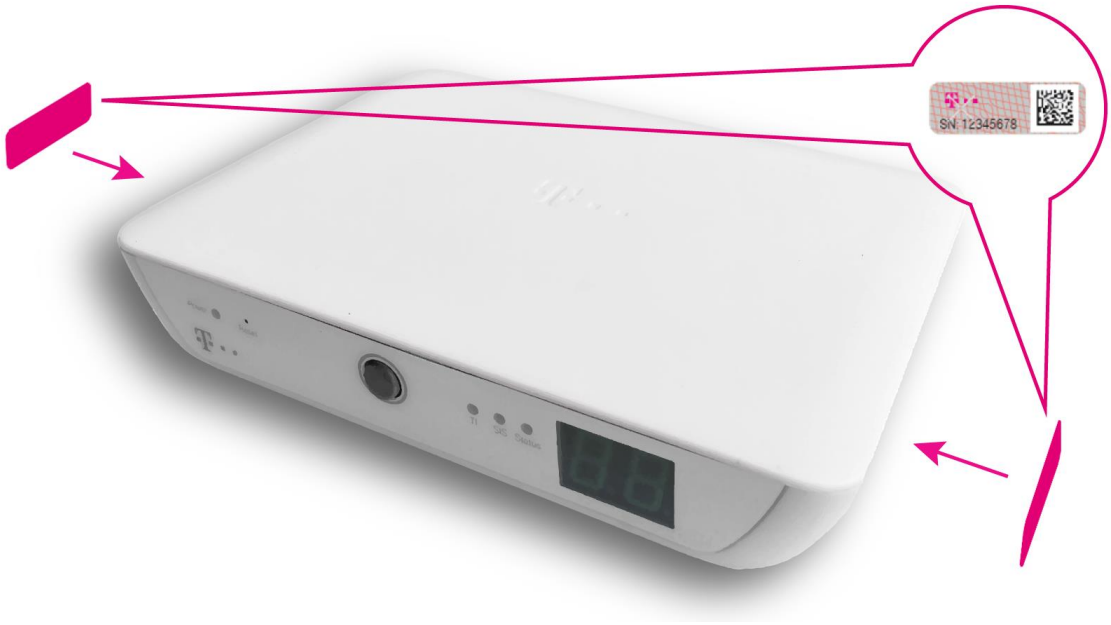


Abbildung 4 Position Sicherheitssiegel am T-Systems Konnektor

4.1.2 Einsatz des Konnektors

Bitte achten Sie in jedem Fall darauf, dass die Anforderungen an die Einsatzumgebung und den Betrieb erfüllt sind (siehe hierzu Abschnitt 4.6), bevor Sie den T-Systems Konnektor in Ihrer Infrastruktur einsetzen.

4.2 Lieferumfang

Im Lieferumfang sind folgende Komponenten enthalten:

- Hardware des T-Systems Konnektors (zugeordnete gSMC-K Karte ist intern verbaut)
- Ein Netzteil zur Stromversorgung (Verwenden Sie bitte nur das beiliegende Netzteil)
- 2 x Ethernet Kabel ca. 2m/grau/CAT5
- Wandmontagebügel
- QuickGuide/Einleger

Die Bedienungsanleitung ist mit Produktangaben beschriftet, sodass die Zugehörigkeit des Handbuchs zur ausgelieferten Hard- und Firmware geprüft werden kann.

4.3 Anschlüsse

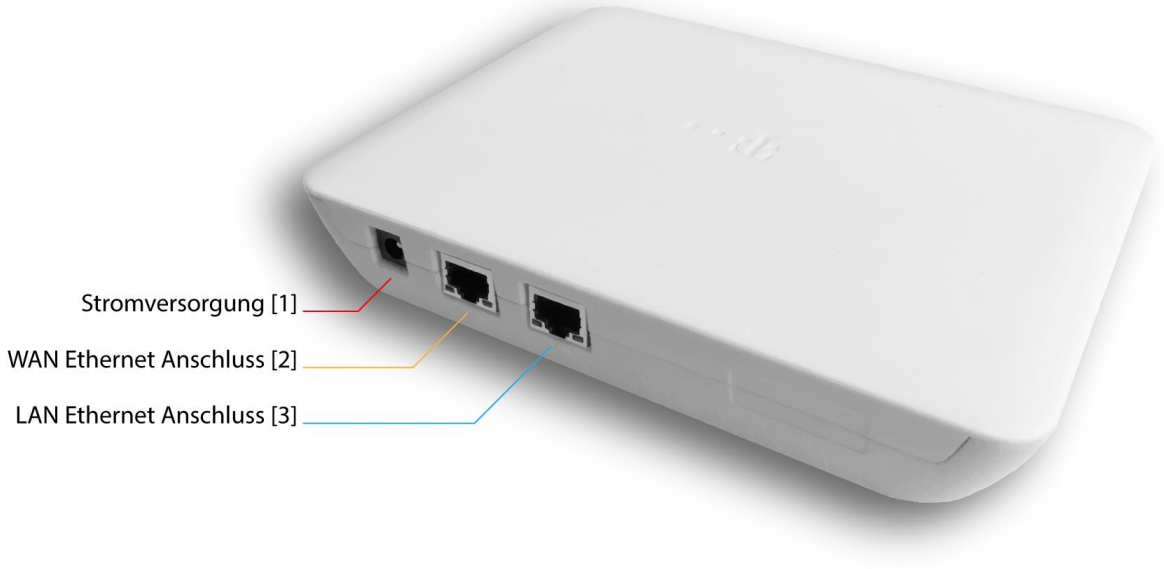


Abbildung 5 Anschlüsse des T-Systems Konnektors

Der T-Systems Konnektor verfügt über die folgenden Anschlüsse zur Verbindung Ihrer vorhandenen Infrastruktur mit der zentralen Telematikinfrastruktur.

- Anschluss für das Netzteil zur Stromversorgung [1]
- Ethernet-Anschluss zur Verbindung mit Ihrem WAN-Router (Schnittstelle zum Transportnetzwerk für den Zugang zur Telematikinfrastruktur) [2]
- Ethernet-Anschluss zur Verbindung mit Ihrem lokalen Netzwerk (LAN) [3]

4.4 Leuchtdioden

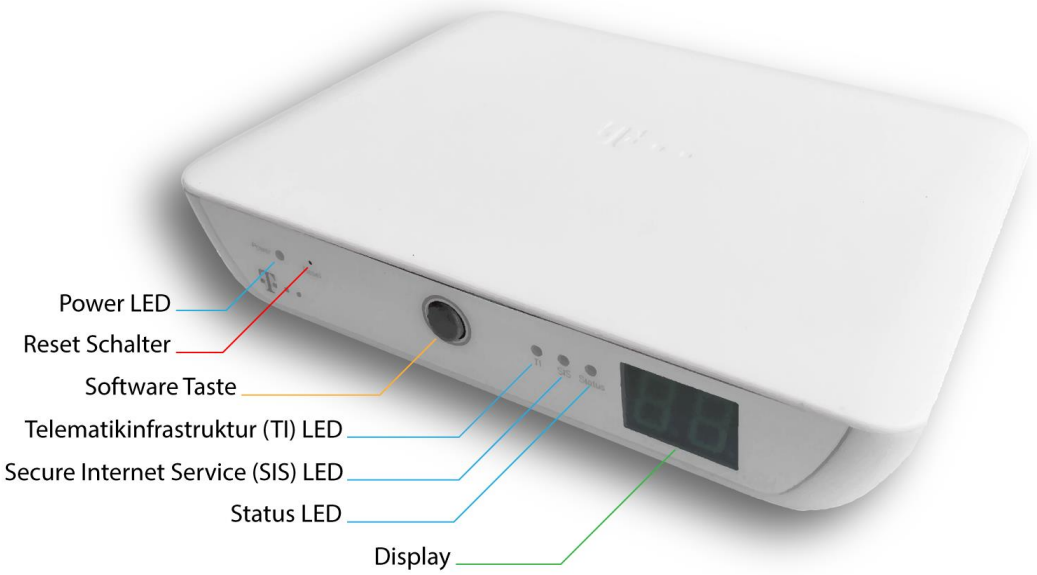


Abbildung 6 Leuchtdioden des T-Systems Konnektors

Der T-Systems Konnektor verfügt auf der Vorderseite über die folgenden LEDs:

- Power LED: Zeigt den Status der Stromversorgung
- TI LED: Zeigt den Verbindungsstatus zur Telematikinfrastruktur
- SIS LED: Zeigt den Verbindungsstatus zum sicheren Internetservice
- Status LED: Zeigt an, ob ein Fehler vorliegt

Die LEDs dienen zur Anzeige der Funktionalität der jeweiligen Leistungsmerkmale. Die LEDs können grün, orange und rot leuchten. Außerdem können unterschiedliche Zustände durch schnelles und langsames Blinken angezeigt werden.

Wie in Abbildung 6 Leuchtdioden des T-Systems Konnektors zu erkennen, verfügt der T-Systems Konnektor auch über ein zweistelliges Display, welches in einem Fehlerfall zweistellige Fehlercodes anzeigt. Wird der mittlere Dezimalpunkt angezeigt, liegen mehrere Fehler vor (siehe hierzu Tabelle 10 Anzeigestatus).

4.4.1 Anzeigenstatus

Tabelle 10 Anzeigestatus

Anzeige	Beschreibung
Die Power LED leuchtet durchgehend grün	Der Konnektor wird mit Strom versorgt.
Die Status LED blinkt grün	Im Display wechseln zweistellige Codes & der Konnektor befindet sich im Start- / Reset- / Shutdownvorgang.
Die Status LED leuchtet durchgehend grün	Der Konnektor ist betriebsbereit. Es liegen keine Fehler vor.

Anzeige	Beschreibung
Die Status LED blinkt orange & im Display blinkt 00.	Der Konnektor befindet sich im Updatevorgang.
Die Status LED leuchtet rot & im Display wird ein zweistelliger Code angezeigt	Es liegt mindestens ein Fehler vor.
Die Status LED ist aus	Es wurde noch kein Betriebszustand von der Konnektorsoftware gesetzt.
Die SIS LED blinkt grün (langsam)	Der VPN-Kanal zum SIS wird aufgebaut.
Die SIS LED blinkt orange (schnell)	Der VPN-Kanal zum SIS wird abgebaut.
Die SIS LED leuchtet durchgehend grün	Der VPN-Kanal zum SIS ist aufgebaut.
Die SIS LED ist aus	Der Konnektor befindet sich im Offline-Modus oder im Internetmodus ist IAG oder keiner festgelegt.
Die SIS LED leuchtet durchgehend rot	Der Konnektor befindet sich im Online-Modus aber der Zustand der Verbindung zum SIS ist fehlerhaft oder unbekannt.
Die TI LED blinkt grün (langsam)	Die Verbindung zur Telematikinfrastruktur wird aufgebaut.
Die TI LED blinkt orange (schnell)	Die Verbindung zur Telematikinfrastruktur wird abgebaut.
Die TI LED leuchtet durchgehend grün	Die Verbindung zur Telematikinfrastruktur ist aufgebaut.
Die TI LED ist aus	Der Konnektor befindet sich im Offline-Modus.
Die TI LED leuchtet durchgehend rot	Der Konnektor befindet sich im Online-Modus aber der Zustand der Verbindung zur Telematikinfrastruktur ist fehlerhaft oder unbekannt.
Im Display leuchtet der mittlere Dezimalpunkt dauerhaft	Es bestehen mehrere Fehler zur gleichen Zeit. Durch wiederholtes kurzes Drücken des [Software Button] werden die bestehenden Fehlercodes nacheinander angezeigt. Ist die Liste der Fehlercodes durchlaufen, wird wieder mit dem ersten Fehlercode der Liste begonnen.
Im Display wird ein zweistelliger Code angezeigt	Es besteht ein Fehler. Welcher Fehlercode für welchen Fehler kann den Abschnitten 10.1.14 und 10.1.15 entnommen werden.

Weitere Erläuterungen zu den LED Stati mit „...durchgehend rot“ können in der Liste der allgemeinen Fehlermeldungen Siehe 10.1.2 entnommen werden.

4.5 Bedienelemente

Der Konnektor verfügt über folgende Bedienelemente:

- Reset Schalter
- Software Taste

Der Reset Schalter ist zurückgesetzt montiert und nur durch eine Bohrung mit einem dünnen Gegenstand erreichbar. Die Betätigung des Reset Schalters löst unmittelbar einen Neustart der Hardware aus. Dieser Reset kann nur über die Hardware erfolgen.

Die Software Taste hat zwei Funktionen.

1. Kurzes Drücken schaltet die Anzeige der Fehlercodes im Display durch (siehe hierzu Abschnitt 4.4).
2. Langes Drücken startet die Konnektorsoftware neu.

4.6 Montage und Platzierung

Bitte beachten Sie bei der Montage bzw. Platzierung des T-Systems Konnektors, dass die Kriterien für einen sicheren Betrieb in Kapitel 3.2 innerhalb der Einsatzumgebung erfüllt werden. Außerdem achten Sie bitte auf die Einhaltung folgender Hinweise:

- Bei der Wandmontage achten Sie bitte bei geplanten Bohrstellen darauf, dass sich dort keine Elektro-, Gas- oder Wasserleitungen befinden.
- Verwenden Sie nur die mitgelieferte Wandhalterung.
- Platzieren Sie den T-Systems Konnektor nicht auf wärmeempfindlichen Flächen. Die Unterseite des Gehäuses kann sich im Betrieb erwärmen.
- Platzieren sie keine Gegenstände vor den Lüftungsschlitzen des Konnektors um eine ungehinderte Luftzirkulation zu ermöglichen.
- Vermeiden Sie, dass der T-Systems Konnektor mit Flüssigkeiten in Kontakt kommt
- Der Konnektor darf ausschließlich innerhalb von Gebäuden eingesetzt werden. Das Gerät muss in einer trockenen und staubfreien Umgebung ohne direkte Sonneneinstrahlung aufgestellt oder montiert werden.

4.7 Erstinstallation und Inbetriebnahme des Geräts in die Telematikinfrastruktur

Der T-Systems Konnektor kann in zwei verschiedenen Anbindungsmodi betrieben werden:

- Parallel: Dieser Modus wird verwendet, wenn der T-Systems Konnektor nur an das lokale Netzwerk angeschlossen wird. Hierbei wird ein bestehender Router per LAN-Kabel an die LAN-Buchse des T-Systems Konnektors verbunden. Der Konnektor kommuniziert dann mit dem Netz des Leistungserbringers und mit der Telematikinfrastruktur über die gleiche physische Schnittstelle (die LAN-Buchse).

  Alle weiteren Konfigurationsschritte, welche den „Parallel“ Modus betreffen, sind grau hinterlegt.

- InReihe: Der Modus wird verwendet, wenn der ausgehende Datenverkehr des T-Systems Konnektors, z.B. in das Netz der Telematik, über den WAN-Adapter des Konnektors gehandhabt werden soll. Das lokale Netzwerk (das Netzwerk der Praxis) ist dazu über die LAN-Buchse verbunden, während der WAN-Adapter über die WAN-Buchse beispielsweise mit einem vorhandenen DSL-Router verbunden wird.

Für die erste Inbetriebnahme benötigt der Konnektor eine Verbindung zum Internet um die Verbindung zur Telematikinfrastruktur herzustellen. Nach erfolgreicher Einrichtung kann der Konnektor später im Offline Modus betrieben werden.

Sicherheitshinweis: Im Anbindungsmodus „InReihe“ wird der gesamte Datenverkehr des LEI über den Konnektor geroutet. Damit sorgt der Konnektor für sicheren Datenverkehr.

Im Anbindungsmodus „Parallel“ ist das Netz des LEI direkt über das IAG an das Internet angeschlossen. Der LEI ist hier selbst verantwortlich für die Absicherung des Datenverkehrs. Der Konnektor sichert hier ausschließlich den Datenverkehr in die TI und durch den SIS (Sicherer Internet Service) den Datenverkehr in das Internet ab.

Details zur Darstellung und Konfiguration den Anbindungsmodi auf der Managementoberfläche können der Beschreibung des Bereichs "Allgemein > Anbindungsmodus" unter Kapitel 6.2 entnommen werden."

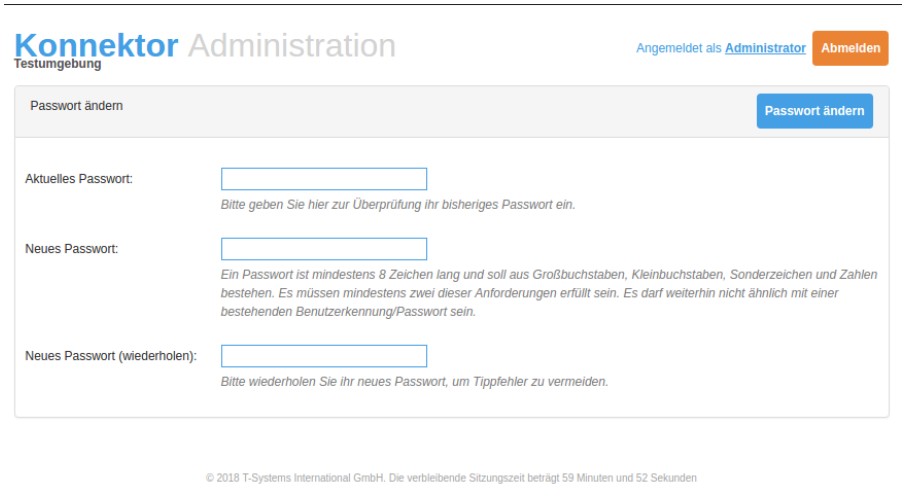
4.7.1 Erstanmeldung und Passwort ändern

Wichtig: Bitte beachten Sie bei der Erstinbetriebnahme den Sicherheitshinweis in Kapitel 5.1 Zugriff auf die Management Oberfläche

Der Konnektor verfügt auf dem LAN-Adapter über eine sogenannte Service-IP-Adresse. Die Werksseitig festgelegte IP Adresse lautet: https://10.10.8.15:4433 mit einem Subnetz 255.255.255.0 .

Sie benötigen eine Netzwerkadresse aus dem entsprechenden Netzwerksegment, um auf die Service-IP-Adresse des Konnektors zuzugreifen. Die Voraussetzungen für die Managmentoberfläche sowie der Umgang mit dem elektronischen Zertifikat wird in Kapitel 5.1 erläutert. Bei der Erstanmeldung muss das Standard-Passwort des Konnektors wie folgt geändert werden:

1. Web-Browser öffnen und in der Adresszeile die Service-IP-Adresse eingeben.
2. Die Managementoberfläche zur Anmeldung am Konnektor wird geöffnet.
3. Erstanmeldung mit den Standard-Anmeldedaten. Siehe 7.1.1 Standard.
4. Die Managementoberfläche zur Änderung des Passwortes wird geöffnet.



5. Im Eingabefeld „Aktuelles Passwort“ das aktuelle Passwort eingeben.
6. Im Eingabefeld „Neues Passwort“ ein neues Passwort eingeben.
7. Im Eingabefeld „Neues Passwort wiederholen“ das neuen Passwort wiederholt

eingeben.
8. Mit der Schaltfläche „Passwort ändern“ das neue Passwort speichern.
9. Es wird erneut die Managementoberfläche zur Anmeldung am Konnektor aufgerufen.
10. Anmeldung mit den neuen Login Daten.
11. Die Managementoberfläche für die Konnektor Administration wird angezeigt.

4.7.2 Einrichten der Infrastruktur

1. Aufruf der Seite „Infrastruktur“.
2. Im Abschnitt „Umgebungseinstellungen“ die IP-Adressen für die Netzsegmente der Telematikinfrastruktur eintragen.
3. Mit der Schaltfläche „Übernehmen“ die Änderung speichern.
4. Das „Hauptmenü“ der Managementoberfläche aufrufen.

4.7.3 Einrichten des Namensservers

Auf der Seite „Namensdienst“ können lokale sowie öffentliche DNS-Server-Adressen hinzugefügt werden.

4.7.4 IP-Adressen DNS Server

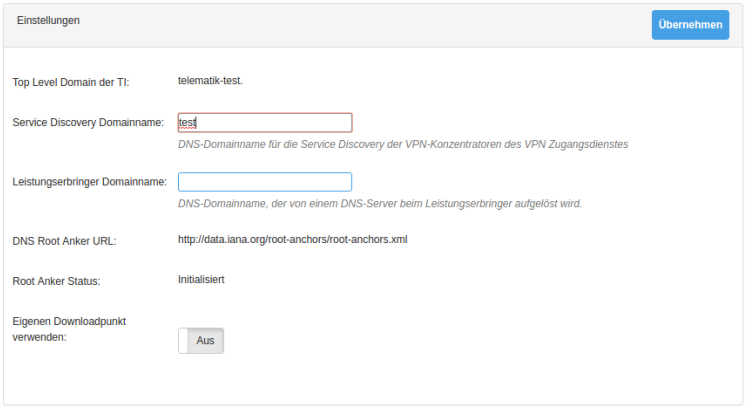
1. Aufruf der Seite „Namensdienst“.
2. Im Abschnitt „DNS-Server im öffentlichen Netz“ mit der Schaltfläche „Verwendung DHCP DNS ausschalten“ die Eingabemaske für die Eingabe der IP-Adressen öffnen.
3. Im Eingabefeld „Neuer Server“ die IP-Adresse eingeben.
4. Mit der Schaltfläche „Übernehmen“ die IP-Adresse speichern. Die IP-Adresse wird in der Liste „IP-Adresse“ angezeigt.

4.7.4.1 Abschnitt Einstellungen

Sollte in der vorhandenen Infrastruktur eigene DNS Services bereitgestellt werden so können im Abschnitt „Einstellungen“ den „Service Discovery Domainname“ und die „DNS Root Anker URL“ eintragen bzw. verändert werden.

1. Im Eingabefeld „Service Discovery Domainname“ den Service Discovery Domainname eintragen.

2. Die Schaltfläche „Eigenen Downloadpunkt verwenden“ anschalten, um das Eingabefeld „Eigene DNS Root Anker URL“ bereitzustellen. Die Schaltfläche wechselt von „Aus“ auf „An“.



3. Im Eingabefeld „Eigene DNS Root Anker URL“ die Root-Anker URL eintragen.
4. Mit der Schaltfläche „Übernehmen“ die Änderungen speichern.
5. Nach dem Speichern wird der „Root Anker Status“ als „Initialisiert“ gekennzeichnet.
6. Das „Hauptmenü“ der Managementoberfläche aufrufen.

Die Aktualisierung des **Vertrauensraums** ist im Kapitel 7.1.2 beschrieben.

4.7.5 LAN und WAN konfigurieren

Auf der Seite „LAN und WAN“ können die Einstellungen für die betreffenden Adapter mit statischen oder dynamischen IP-Adressen konfiguriert und allgemeine Routing-Einstellungen vorgenommen werden.

Bei Einstellungen auf dieser Seite muss der Netzwerkmodus, „Parallel“ oder „InReihe“ berücksichtigt werden. Siehe 4.7.

1. Aufrufen der Seite „LAN und WAN“.

4.7.5.1 WAN Segment

Standardmäßig werden die IP-Adressen dynamisch über DHCP vergeben. Ist eine Anpassung der „IAG Adresse“ erforderlich, muss das Eingabefeld „IAG Adresse“ im Segment „Allgemein“ über die DHCP Schaltfläche im „WAN“ Segment editierbar gemacht werden.

1. Die Schaltfläche „DHCP“ im „WAN“ Segment von „An“ auf „Aus“ schalten.
2. Das Eingabefeld „IAG-Adresse“ wird editierbar.
3. Die IAG-Adresse in das Eingabefeld eintragen.

Dynamische IP über DHCP im Reihen-Modus:

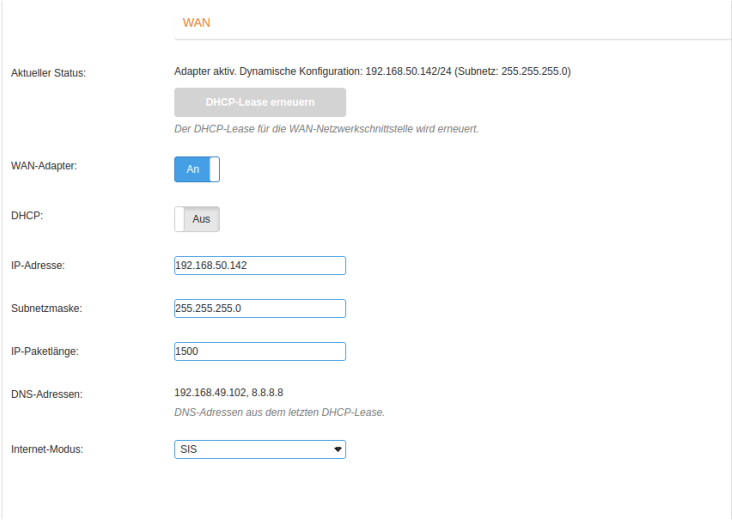
1. Die Schaltfläche „DHCP“ im „WAN“ Segment von „Aus“ wieder auf „An“ schalten.

Statische IP ohne DHCP im Reihen-Modus:

1. Im Eingabefeld „Subnetzmaske“ des „WAN“ Segmentes die Subnetzmaske eintragen.
2. Im Eingabefeld „IP-Adresse“ des „WAN“ Segmentes die IP-Adresse eintragen.

Parallel-Modus WAN Adapter ausschalten:

1. Die Schaltfläche „WAN-Adapter“ im „WAN“ Segment von „An“ auf „Aus“ schalten.



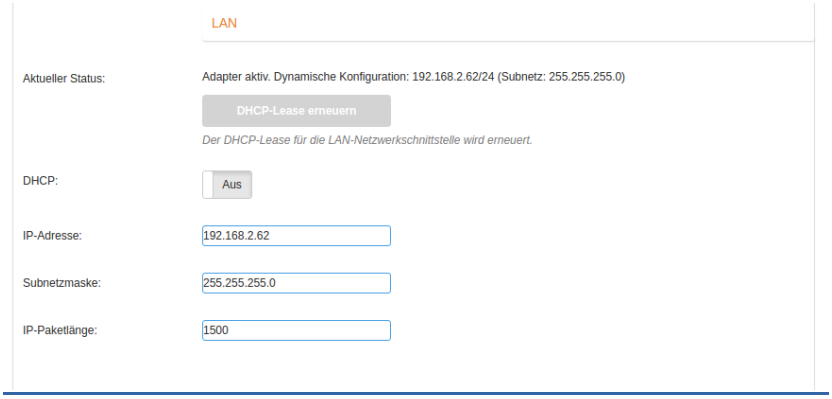
4.7.5.2 LAN Segment

Dynamische IP über DHCP im Reihen-Modus:

1. Die Schaltfläche „DHCP“ im „LAN“ Segment ist „An“ geschaltet.

Statische IP ohne DHCP im Reihen-Modus:

2. Die Schaltfläche „DHCP“ im „LAN“ Segment von „An“ auf „Aus“ schalten.
3. Im Eingabefeld „Subnetzmaske“ des „WAN“ Segmentes die Subnetzmaske eintragen.
4. Im Eingabefeld „IP-Adresse“ des „WAN“ Segmentes die IP-Adresse eintragen.
5. Mit der Schaltfläche „Übernehmen“ die Änderungen speichern.
6. Ein Hinweisfenster zeigt die laufende Konfigurationsänderung an.
7. Nach Beendigung der Konfiguration ist ein erneutes Login durchzuführen.
8. Auf der Seite „LAN und WAN“ werden die neuen Adressen angezeigt.
9. Unter „Anbindungsmodus“ im Segment „Allgemein“ wird angezeigt ob sich der Konnektor in Reihe- oder Parallel-Modus befindet.
10. Das „Hauptmenü“ der Managementoberfläche aufrufen.

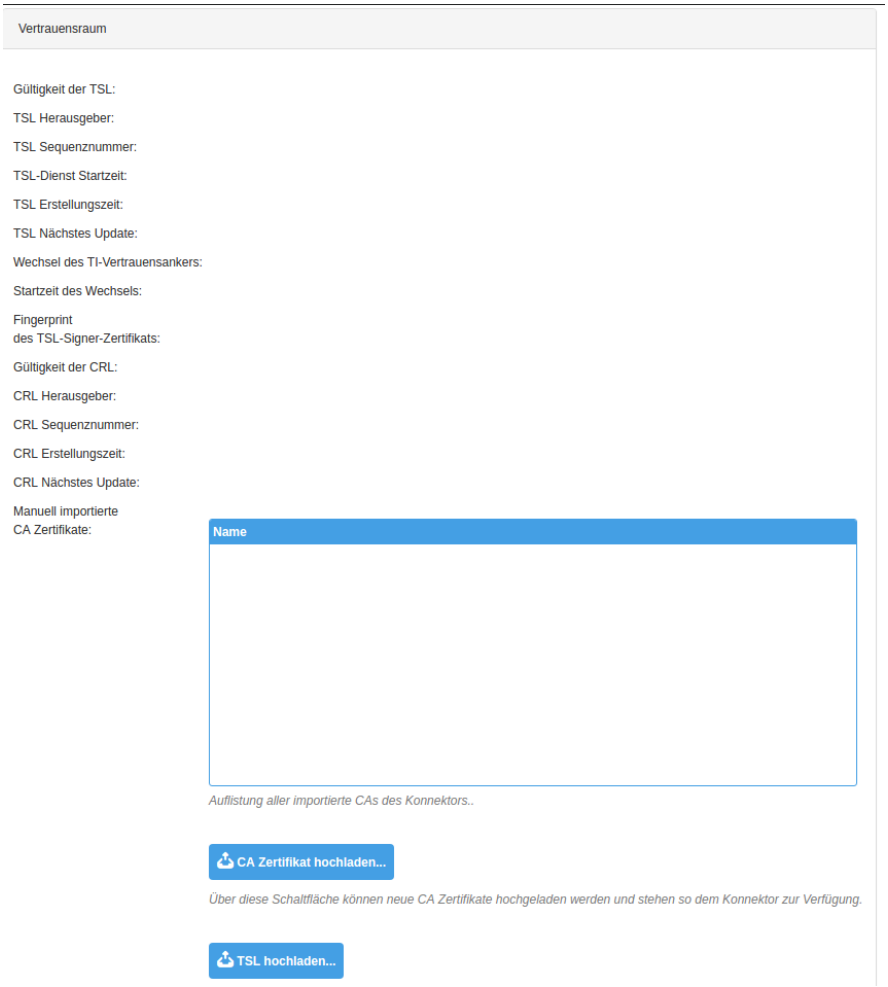


4.7.5.3 Zertifikate hochladen

Der Menüpunkt Zertifikate beinhaltet die Punkte Vertrauensraum, Vertrauensanker und Netzwerk.

Manuell können TSL Zertifikate nur im „Offline“ Modus hochgeladen werden.

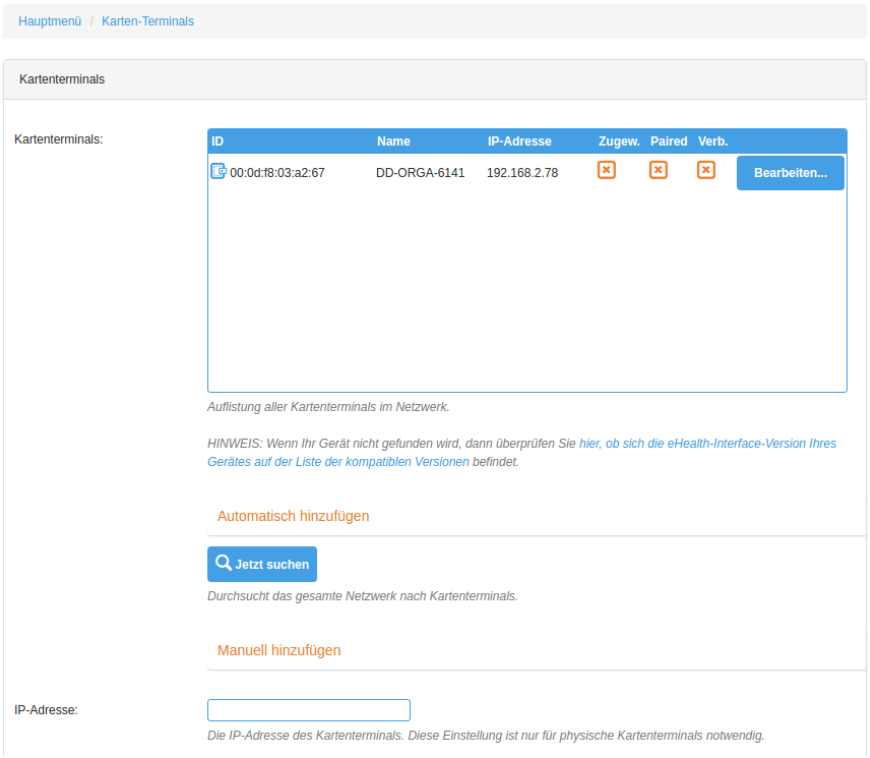
1. Aufrufen der Seite „Leistungsumfang“.
2. Im Abschnitt „Einstellungen“ die Schaltfläche „Online“ von „An“ auf „Aus“ schalten.
3. Mit der Schaltfläche „Übernehmen“ die Änderungen speichern.
4. Die Hinweismeldung mit der Schaltfläche „Fortfahren“ bestätigen.
5. Das erneute Login durchführen.
6. Aufrufen der Seite „Zertifikate“.
7. Im Abschnitt „Vertrauensraum“ mit der Schaltfläche „TSL hochladen...“ den File Upload Dialog öffnen.
8. Das TSL Zertifikat hochladen.
9. Ein Hinweisfenster zeigt an, dass die TSL aktualisiert wurde.
10. Die TSL Eigenschaften im Abschnitt „Vertrauensraum“ entsprechen denen, der hoch geladenen TSL.
11. Im Abschnitt „Vertrauensraum“ mit der Schaltfläche „CRL hochladen...“ den File Upload Dialog öffnen.
12. Die CRL hochladen.
13. Ein Hinweisfenster zeigt an, dass die CRL aktualisiert wurde.
14. Die CRL Eigenschaften im Abschnitt „Vertrauensraum“ entsprechen denen, der hoch geladenen CRL.
15. Das „Hauptmenü“ der Managementoberfläche aufrufen.
16. Aufrufen der Seite „Leistungsumfang“.
17. Im Abschnitt „Einstellungen“ die Schaltfläche „Online“ von „Aus“ auf „An“ schalten.
18. Mit der Schaltfläche „Übernehmen“ die Änderungen speichern.
19. Die Hinweismeldung mit der Schaltfläche „Fortfahren“ bestätigen.
20. Das erneute Login durchführen.



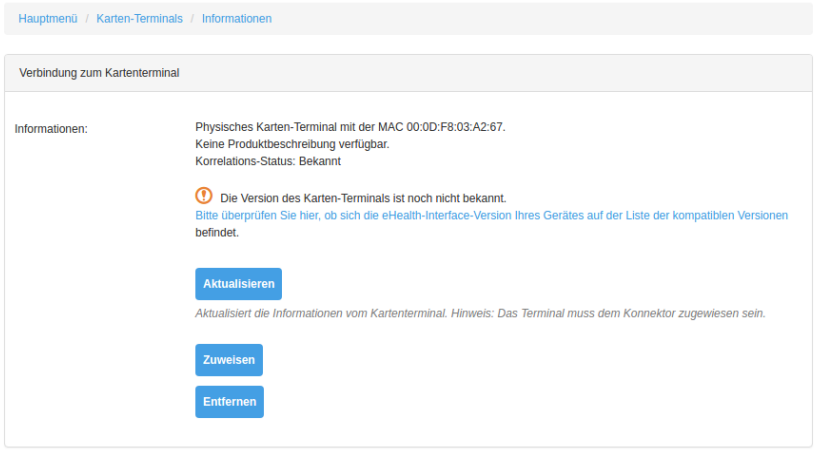
4.7.5.4 Kartenterminals konfigurieren

Wichtiger Hinweis: Das Kartenterminal muss vorkonfiguriert sein und die entsprechenden Karten (mindestens gSMC-KT) vorhanden sein müssen.

1. Aufrufen der Seite „Kartenterminals“.
2. Um verfügbare Kartenterminals anzuzeigen kann über die Schaltfläche „Jetzt suchen“ im Abschnitt „Kartenterminals“ eine Netzwerkweite Suche durchgeführt werden. Es werden alle gefunden Kartenterminals in der Liste „Kartenterminals“ hinzugefügt.
3. Mit der Eingabe der IP-Adresse eines bekannten Kartenterminals im Eingabefeld „IP-Adresse“ und der Schaltfläche „Hinzufügen“ kann ein einzelnes Kartenterminal in der Liste „Kartenterminals“ hinzugefügt werden.
4. Die verfügbaren Kartenterminals werden in der Liste „Kartenterminals“ angezeigt.



5. In der Liste „Kartenterminals“ auf die Schaltfläche „Bearbeiten“ das gewünschte Kartenterminal öffnen.
6. Die Seite „Informationen“ wird geöffnet.



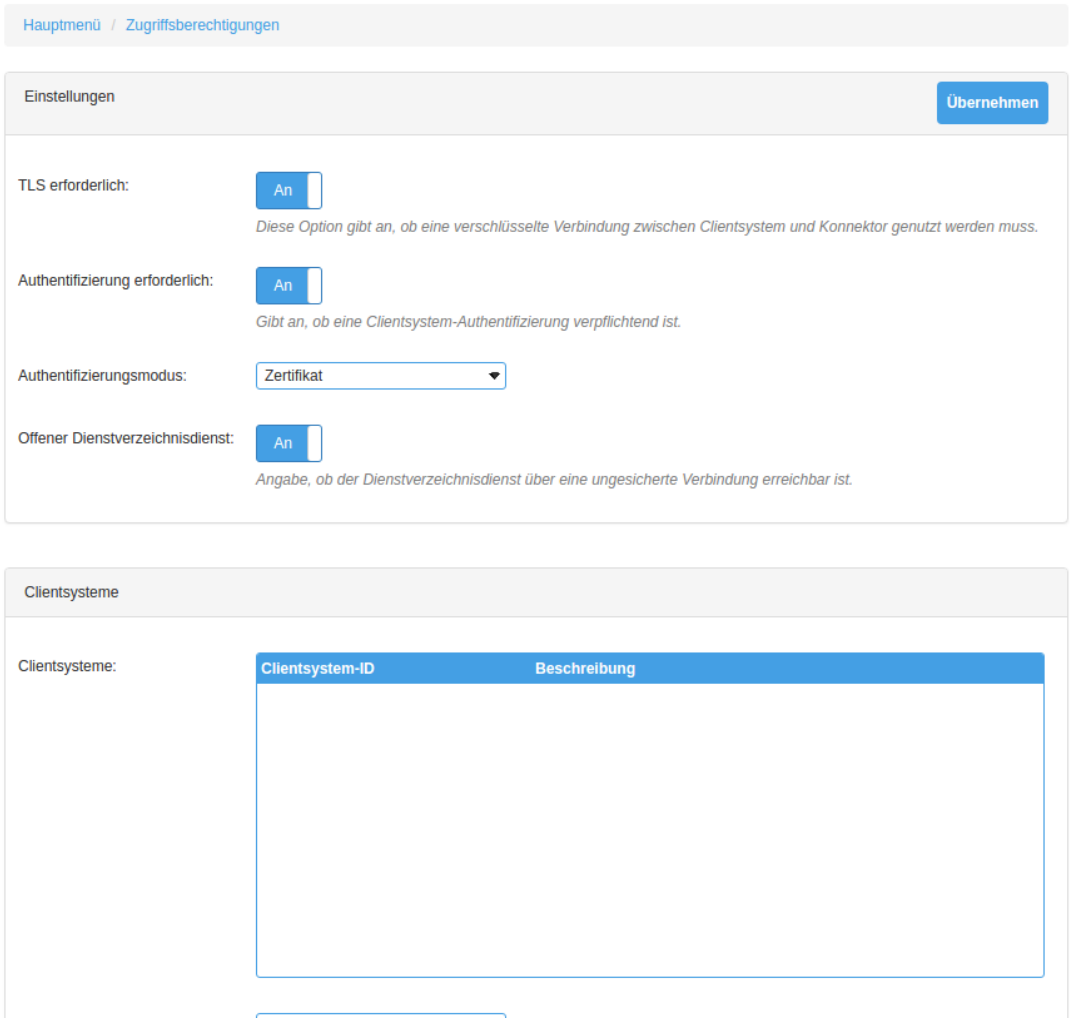
7. Im Abschnitt „Verbindung zum Kartenterminal“ auf die Schaltfläche „Zuweisen“ klicken. (Ist das Kartenterminal bereits zugewiesen, ist dieser Schritt zu überspringen.)
8. Der „Korrelations-Status“ zeigt „Zugewiesen“ und die Schaltfläche „Zuweisen“ ändert die Beschriftung zu „Zuweisung aufheben“.
9. Betätigen der Schaltfläche „Pairen“.
10. Ein Hinweisfenster zeigt das Karten-Terminal Zertifikat an.
11. Mit der Schaltfläche „Ja“ fortfahren.
12. Das Kartenterminal erwartet eine Bestätigung für das Pairen.
13. Nach dem Bestätigen werden Konnektor und das Kartenterminal gepairt und verbunden.
14. Der „Korrelations-Status“ zeigt „Aktiv“ an und das Zertifikat wird angezeigt.

15. Das „Hauptmenü“ der Managementoberfläche aufrufen.

4.7.5.5 Zugriffsberechtigungen einrichten

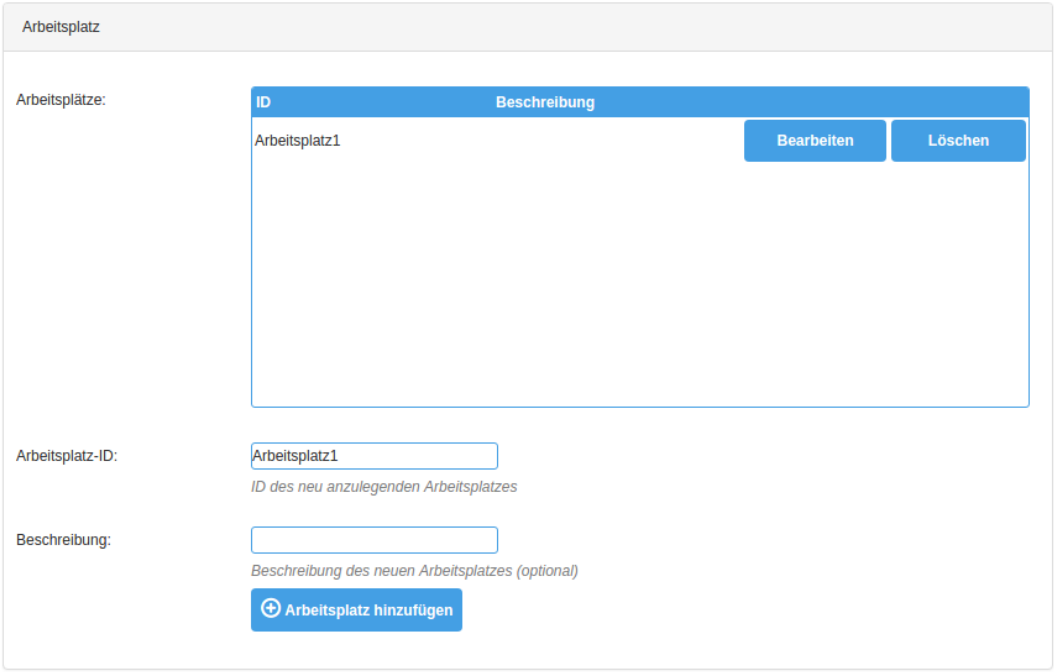
Der Menüpunkt „Zugriffsberechtigungen“ erlaubt dem Administrator, die Zugriffsberechtigungen und die dazugehörigen Einstellungen zu konfigurieren.

Im Abschnitt „Einstellungen“ wird Konfiguriert, ob eine verschlüsselte Verbindung zwischen Konnektor und Client-System genutzt werden soll. Für die Erstkonfiguration sind diese Einstellungen nicht relevant.



1. Aufrufen der Seite „Zugriffsberechtigung“.
2. Im Abschnitt „Clientsysteme“ die „Clientsystem-ID“ (Name des Clientsystems) in das Eingabefeld eintragen.
3. Mit der Schaltfläche „Clientsystem hinzufügen“ die Clientsystem-ID speichern.
4. Die Clientsystem-ID wird in der Liste „Clientsysteme“ angezeigt.
5. Im Abschnitt „Arbeitsplatz“ die „Arbeitsplatz-ID“ (Name des Arbeitsplatzes) in das Eingabefeld eintragen.
6. Mit der Schaltfläche „Arbeitsplatz hinzufügen“ die Arbeitsplatz-ID speichern.

7. Die Arbeitsplatz-ID wird in der Liste „Arbeitsplätze“ angezeigt.



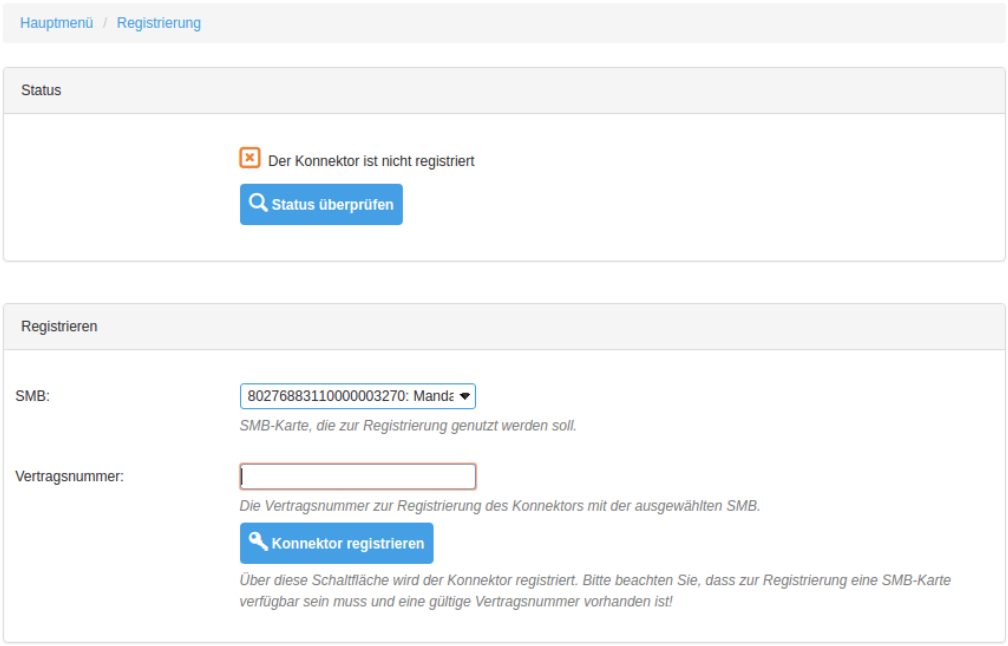
8. Die Schaltfläche „Bearbeiten“ des neu eingetragenen Arbeitsplatzes betätigen.
9. Die Seite „Arbeitsplatzrelationen“ wird angezeigt.
10. Im Abschnitt „Zugeordnete Kartenterminals“ ist das bereits konfigurierte Kartenterminal hinzuzufügen.
11. Das Kartenterminal wird in der Liste „Zuordnung“ angezeigt.
12. Aufrufen der Seite „Zugriffsberechtigungsdienst“.
13. Die Seite „Zugriffsberechtigungen“ wird angezeigt.
14. Im Abschnitt „SMB“ werden die verfügbaren SMB's angezeigt.
15. Die SMB im Menü „verfügbare SMB's“ auswählen.
16. Mit der Schaltfläche „SMB hinzufügen“ die Auswahl speichern.
17. Im Abschnitt „Mandant“ die „Mandanten-ID“ (Name des Mandanten) in das Eingabefeld eintragen.
18. Mit der Schaltfläche „Mandant hinzufügen“ die Mandanten-ID speichern.
19. Die Mandanten-ID wird in der Liste „Mandanten“ angezeigt.
20. Die Schaltfläche „Bearbeiten“ des neu eingetragenen Mandanten betätigen.
21. Die Seite „Mandantenrelationen“ wird angezeigt.
22. Im Abschnitt „Zugeordnete Kartenterminals“ das Kartenterminal aus dem Menü auswählen.
23. Mit der Schaltfläche „Zuordnung hinzufügen“ die Zuordnung speichern.
24. Das Kartenterminal wird in der Liste „Zuordnung“ angezeigt.
25. Im Abschnitt „Zugeordnete SMBs“ die SMB aus dem Menü auswählen.
26. Mit der Schaltfläche „Zuordnung hinzufügen“ die Zuordnung speichern.
27. Die SMB wird in der Liste „Zuordnung“ angezeigt.
28. Im Abschnitt „Zugeordnete Arbeitsplätze“ den Arbeitsplatz aus dem Menü auswählen.
29. Mit der Schaltfläche „Zuordnung hinzufügen“ die Zuordnung speichern.
30. Der Arbeitsplatz wird in der Liste „Zuordnung“ angezeigt.
31. Im Abschnitt „Zugeordnete Clientsysteme“ das Clientsystem aus dem Menü auswählen.
32. Mit der Schaltfläche „Zuordnung hinzufügen“ die Zuordnung speichern.
33. Das Clientsystem wird in der Liste „Zuordnung“ angezeigt.
34. Im Abschnitt „Arbeitsplätze zugeordneter Clientsysteme“ das Clientsystem und den

Arbeitsplatz aus dem Menü auswählen.
35. Mit der Schaltfläche „Zuordnung hinzufügen“ die Zuordnung speichern.
36. Die Zuordnung wird in der Liste „Zuordnung“ angezeigt.
37. Das „Hauptmenü“ der Managementoberfläche aufrufen.

4.7.5.6 Konnektor registrieren

Damit der Konnektor als Element zur sicheren Kommunikation zwischen dem Netz der Praxis oder des Krankenhauses und der Telematikinfrastruktur korrekt arbeitet, muss der Konnektor beim Anbieter des VPN-Dienstes registriert werden.

Aufrufen der Seite „Registrierung“.
Im Abschnitt „Status“ wird angezeigt, dass der Konnektor nicht registriert ist.
Im Abschnitt „Registrieren“ im Menü „SMB“ die SMB auswählen.



In das Eingabefeld „Vertragsnummer“ die Vertragsnummer eintragen.
Mit der Schaltfläche „Konnektor registrieren“ den Konnektor registrieren.
Im Kartenterminal muss die SMB Pin verifiziert werden.
Mit einem Hinweisfenster wird über die erfolgreiche Registrierung informiert, die mit der Schaltfläche „OK“ bestätigt werden muss.
Im Abschnitt „Status“ wird der Konnektor als erfolgreich registriert gekennzeichnet und das der Zugriff auf TI und SIS besteht.
Nach erfolgter Registrierung baut der Konnektor automatisch die Tunnel zu TI und SIS auf.

Damit ist die Erstinbetriebnahme abgeschlossen.

4.7.6 Installation zur Verwendung mit einem Kartenterminal

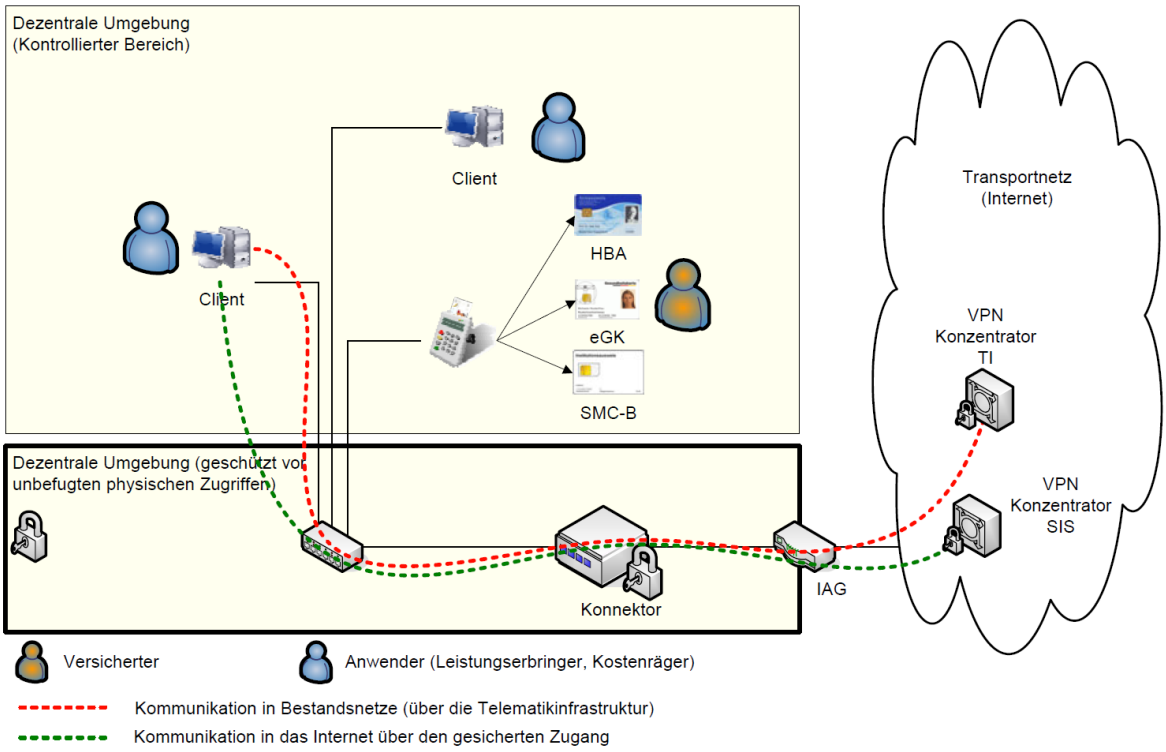


Abbildung 7 Szenario einfache Installation aus gemSpec_KON_V4.11.1, S.498

4.7.6.1 Erläuterung

In diesem Fall wird der T-Systems Konnektor als Default-Gateway für jegliche Kommunikation aus Ihrem lokalen Netzwerk in das Internet eingesetzt. Dabei übernimmt der T-Systems Konnektor das Routing der Kommunikation in das Internet und die an die Telematikinfrastruktur angeschlossenen Bestandsnetze. Durch die Ressourcenverwaltung des T-Systems Konnektors wird sichergestellt, dass bei Anwendungsfällen das Kartenterminal angesprochen wird, welches dem Arbeitsplatz zugeordnet ist, von dem aus der Anwendungsfall initiiert wurde.

4.7.6.2 Vorgehensweise

1. Stecken Sie ein Ende des LAN-Netzwerkkabel in die Buchse des T-Systems Konnektors mit der Beschriftung LAN und verbinden Sie das andere Ende mit Ihrem Switch bzw. Router Ihres lokalen Netzwerks.
2. Stecken Sie ein Ende des WAN-Netzwerkkabel in die Buchse des T-Systems Konnektors mit der Beschriftung WAN und verbinden Sie das andere Ende mit Ihrem Router oder Modem.
3. Verbinden Sie das Stromkabel mit dem T-Systems Konnektor.

4.7.7 Installation zur Verwendung mit mehreren Kartenterminals

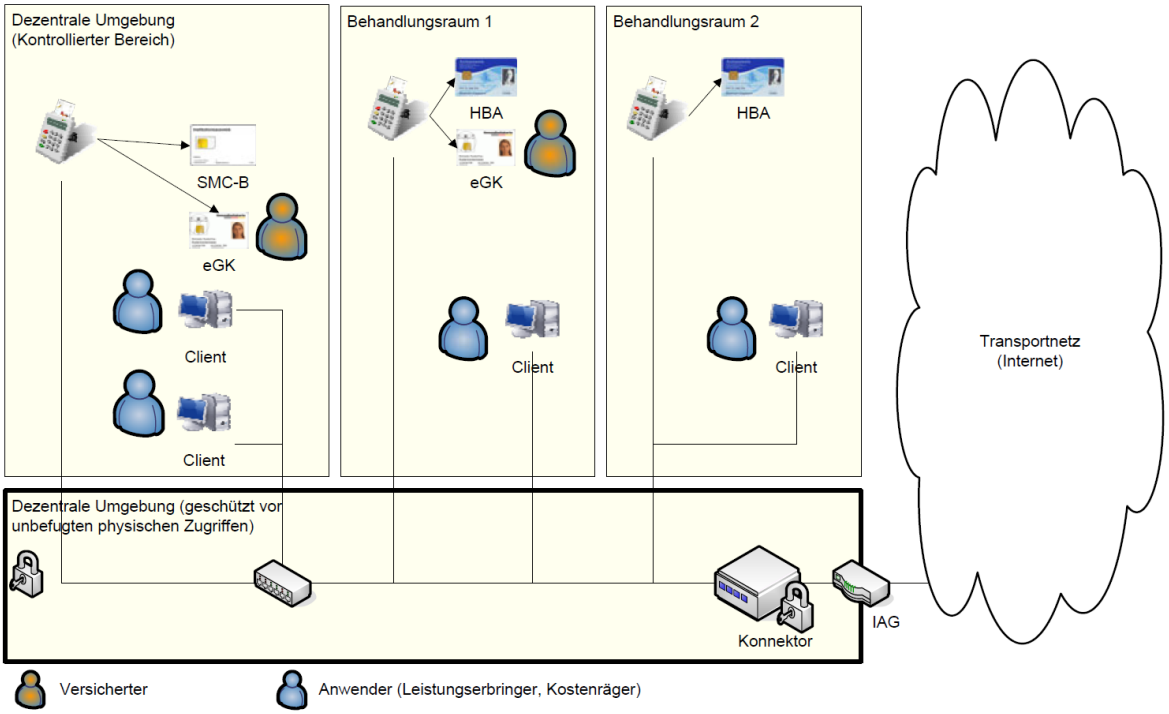


Abbildung 8 Szenario einer Installation mit mehreren Behandlungsräumen aus gemSpec_KON_V4.11.1, S.500

4.7.7.1 Erläuterung

Mit der in Szenario 1 (Abbildung 7 Szenario einfache Installation aus gemSpec_KON_V4.11.1, S.498) skizzierten Topologie kann auch ein Szenario bedient werden, bei dem mehrere Behandlungsräume unterstützt werden. Dabei ist in jedem Behandlungsraum mindestens ein Kartenterminalnötig, um die eGK einzulesen. Auf die Darstellung der Kommunikationswege in zentrale Netze wurde verzichtet, da sich hier keine Änderung gegenüber Szenario 1 ergibt. Durch die Ressourcenverwaltung des Konnektors wird sichergestellt, dass bei Anwendungsfällen diejenigen Kartenterminals angesprochen werden, welche dem jeweiligen Arbeitsplatz zugeordnet sind.

4.7.7.2 Voraussetzungen

- Anbindung der bestehenden Clientsysteme an ein zum Konnektor kompatibles LAN muss möglich sein.
- Konfiguration des Konnektors als Default-Gateway in den Clientsystemen und Einrichtung der notwendigen VPN-Tunnel im Konnektor, um in die verschiedenen Netze zu routen.
- Verfügbarkeit einer SMC-B und mehrerer Kartenterminals und Clientsysteme
- Die Clientsysteme und Kartenterminals und deren Relationen sind dem Konnektor über Konfiguration bekannt gemacht worden.

4.7.7.3 Auswirkungen

- Die Clientsysteme können über den Konnektor Anwendungsfälle der TI initiieren.
- Die Clientsysteme können über den Konnektor auf das Internet (über den SIS) und Bestandsnetze zugreifen.
- Der HBA-Inhaber muss seinen HBA mit sich führen und kann diesen in den einzelnen Kartenterminals der Behandlungsräume nutzen.

4.7.8 Installation mit speziellen Anforderungen mit mindestens einem separaten VPN-Netzwerk

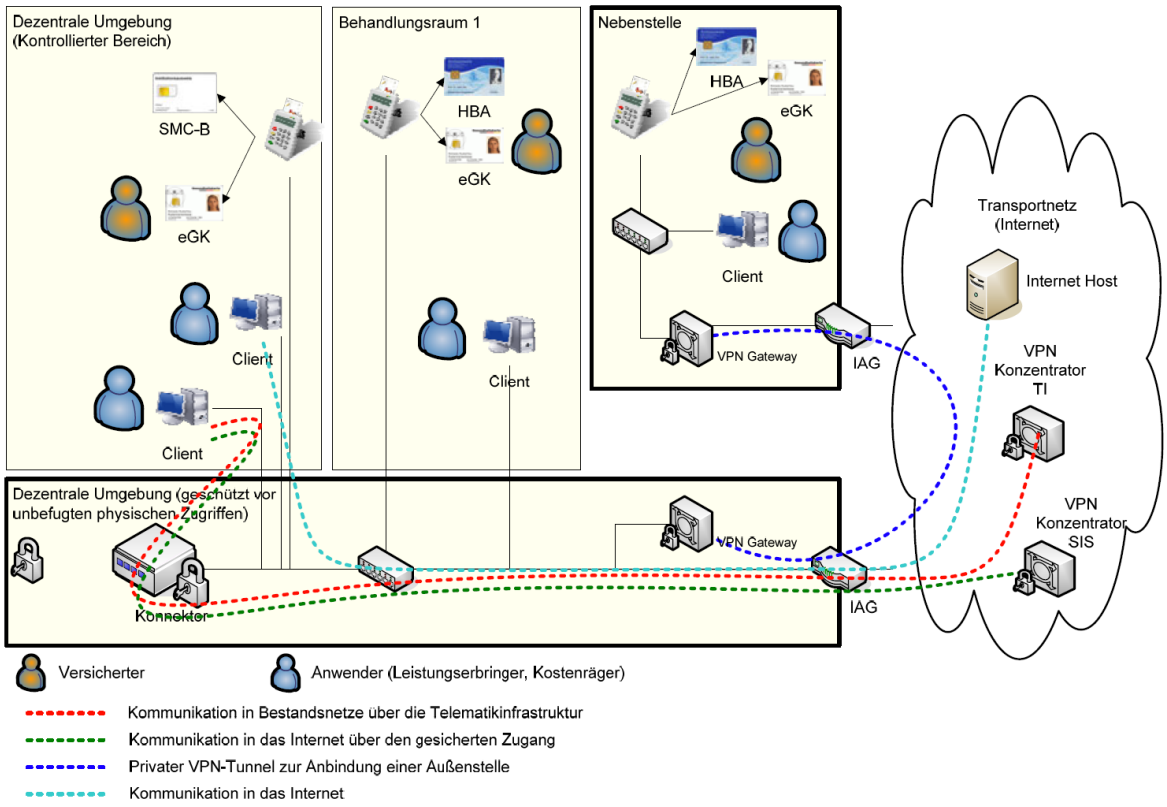


Abbildung 9 Szenario einer Integration in bestehende Infrastruktur aus gemSpec_KON_V4.11.1, S.501

4.7.8.1 Erläuterung

In diesem Fall wird der T-Systems Konnektor in Ihre vorhandene Infrastruktur eingegliedert. Produkte der Telematik können in die bestehende Infrastruktur integriert werden. Bestehende Kommunikationswege können weiter genutzt werden. Für angeschlossene Systeme kann je nach individuellem Anforderungsprofil der sichere Internetzugang über den T-Systems Konnektor genutzt werden. Auch der direkte Internetzugang über den bestehenden Internet-Router oder Modem ist möglich.

4.7.8.2 Vorgehensweise

1. Stecken Sie ein Ende des LAN-Netzwerkkabels in die Buchse des T-Systems Konnektors mit der Beschriftung LAN und verbinden Sie das andere Ende mit Ihrem Switch bzw. Router Ihres lokalen Netzwerks.
2. Stecken Sie ein Ende des WAN-Netzwerkkabels in die Buchse des T-Systems Konnektors mit der Beschriftung WAN und verbinden Sie das andere Ende ebenfalls mit Ihrem Switch bzw. Router Ihres lokalen Netzwerks.
3. Verbinden Sie das Stromkabel mit dem T-Systems Konnektor.

4.7.9 Installation mit zentralem Primärsystem als Clientsystem

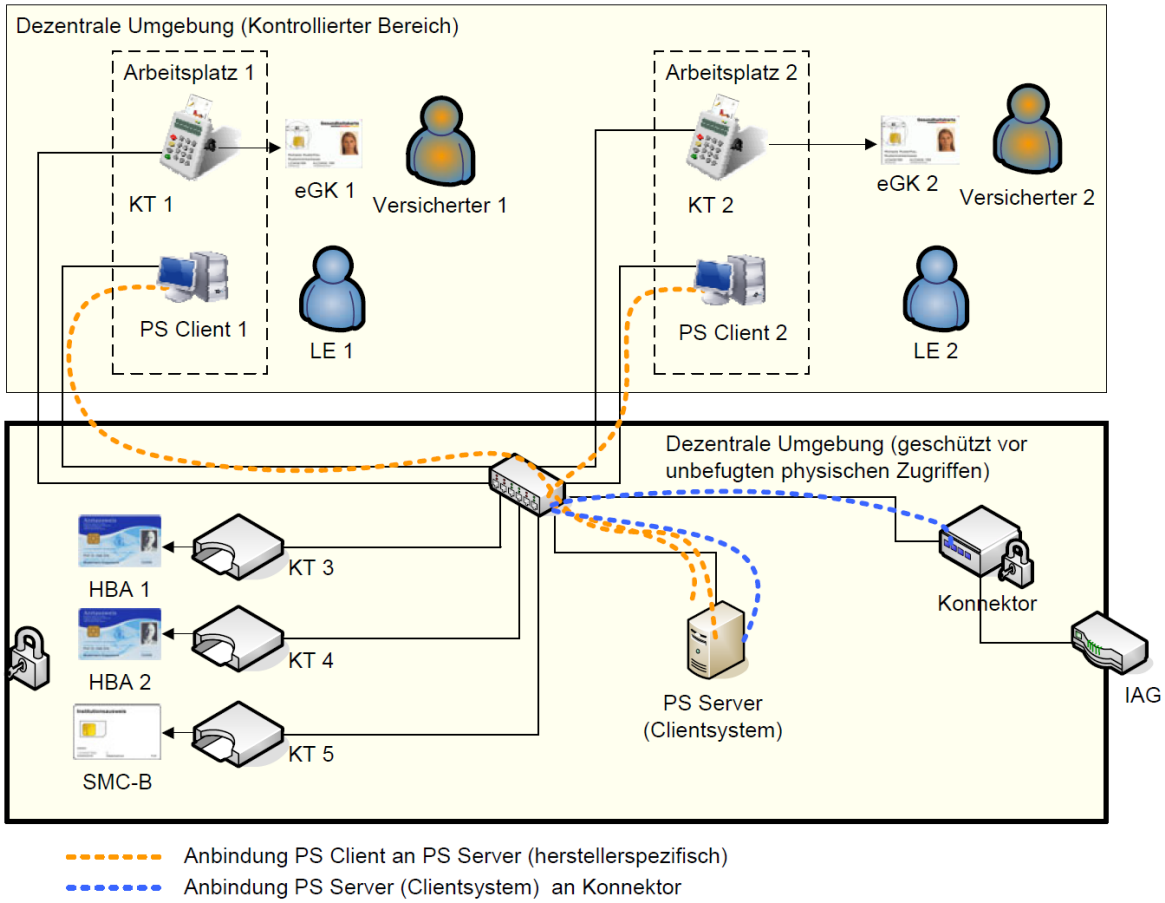


Abbildung 10 Szenario einer Installation mit zentralem Primärsystem als Clientsystem aus gemSpec_KON_V4.11.1, S.506

4.7.9.1 Erläuterung

Unter Primärsystemen werden folgende Komponenten verstanden:

- Zahnarztpraxisverwaltungssoftware (ZPVS)
- Praxisverwaltungssoftware (PVS)
- Krankenhausinformationssysteme (KIS)

Das Szenario skizziert eine dezentrale Konfiguration, bei der das Primärsystem (PS) aus einem Serveranteil PS-Server und mehreren Clientanteilen PS-Client besteht. Die Anbindung zwischen dem PS-Server und den PS-Clients ist herstellerspezifisch. Der PS-Server fungiert als ein einziges Clientsystem gegenüber der TI bzw. dem Konnektor (z.B. als Terminalserver). Die Clientsystemschnittstelle des Konnektors wird ausschließlich vom PS-Server genutzt. Der PS-Server muss bei der Kommunikation mit dem Konnektor eine Übersetzung der zugreifenden PS-Clients auf die entsprechende Entität Arbeitsplatz des Konnektors durchführen.

Beispielhaft zeigt das Szenario zwei Arbeitsplätze mit jeweils einem Kartenterminal für die eGK sowie zentral gesteckte SMC-B und HBAs. Alternativ sind auch lokal am Arbeitsplatz gesteckte HBAs möglich.

4.7.9.2 Voraussetzungen

- Netzanbindung aller Komponenten (u. a. KT, PS-Client, PS-Server, Konnektor) in der dezentralen Umgebung bis einschließlich zur Netzwerkschicht (IP-Ebene)
- Konfiguration des Primärsystems mit seinen Anteilen PS-Server und ggf. mehreren PS-Clients passend zum Informationsmodell des Konnektors (herstellerspezifisch).
- Konfiguration des Konnektors. U. a.:
- Informationsmodell: Beim Beispielszenario u.a. Entitäten Clientsystem für PS-Server, Arbeitsplatz für Arbeitsplatz 1 und Arbeitsplatz 2, Kartenterminal und KT-Slot für KT 1 – KT 5, Mandat für die vorgesehene Anzahl von Mandaten, SMB_Verwaltet sowie entsprechende Entitätenbeziehungen
- Anbindung PS-Server (ggf. über TLS)
- Pairing der Kartenterminals
- Gesteckte Karten (SMC-B, HBA, eGK)
- Anmeldung Leistungserbringer am PS-Client

4.7.9.3 Auswirkungen

- An den verschiedenen Arbeitsplätzen können für die definierten Mandanten und Nutzer Anwendungsfälle der TI initiiert werden.
- HBA-Inhaber müssen entsprechend der gewählten HBA-Deployment-Varianten
- Ihren HBA zentral stecken und über das Remote-PIN-Verfahren zugreifen
- Ihren HBA mit sich führen und lokal ins Kartenterminal der Arbeitsplätze stecken

4.8 Einsatzbereitschaft

4.8.1 Erste Inbetriebnahme: Mögliche Verletzungen der Integrität

Tabelle 11 Mögliche Fehler bei Inbetriebnahme

Fehler	Beschreibung und Maßnahme
Sie werden nicht aufgefordert das Benutzerkennwort neu zu vergeben.	Die Integrität wurde verletzt, schicken sie den Konnektor an den Hersteller zurück.
Mindestens eines der Sicherheitssiegel wurde verletzt.	Nehmen Sie das Gerät außer Betrieb und kontaktieren Ihren Servicetechniker. Weitergehende Fragen hierzu richten Sie bitte an den Herausgeber (siehe hierzu Anhang A.1 Kontakt).
Der Selbsttest schlägt fehl.	Der T-Systems Konnektor kann nicht benutzt werden. Sie haben keinen Zugriff auf die Managementoberfläche und die externen Schnittstellen. Weitere Informationen hierzu finden Sie in Kapitel 4.8.2.

4.8.2 Start des Konnektors

Der T-Systems Konnektor verfügt über einen sicheren Startmechanismus (Selbsttest). Dieser sorgt dafür, dass beim Starten eine Reihe von Sicherheitsmechanismen durchlaufen wird, die den T-Systems Konnektor in einen sicheren Betriebsmodus versetzen. Schlägt der Selbsttest fehl, kann der T-Systems Konnektor nicht benutzt werden. In diesem Fall haben Sie keinen Zugriff auf die Managementoberfläche und die externen Schnittstellen, die Status LED leuchtet rot und es wird ein Fehlercode im Display angezeigt (vgl. Kapitel 4.4).

Bitte beachten Sie, dass der T-Systems Konnektor während der Initialisierung nicht vom Strom getrennt werden darf, da sonst ein undefinierter Betriebszustand entstehen kann.

Bei der ersten Inbetriebnahme des T-Systems Konnektors wird dieser initialisiert. Es wird automatisch erkannt, dass er noch nicht initialisiert ist und die Einsatzbereitschaft wird selbstständig hergestellt. Dazu legt der T-Systems Konnektor intern neue Benutzerdaten an und erstellt einen verschlüsselten Bereich. Dort werden Betriebsanwendungen installiert, nachdem die internen Sicherheitsmechanismen durchlaufen wurden.

Im Anschluss wird sich der T-Systems Konnektor neu starten und unter Verwendung der neu angelegten Benutzerdaten kann dieser nun auf den verschlüsselten Bereich zugreifen. Die Betriebsanwendungen können nun verwendet werden.

Anschließend leuchten die LEDs durchgängig grün und signalisieren, dass die Stromversorgung und die sichere Verbindung in die Telematikinfrastruktur bestehen und der T-Systems Konnektor verwendet werden kann. Leuchten alle vier Dioden, so besteht ebenfalls die Verbindung zum sicheren Internetservice (SIS).

4.9 Betrieb

Unter welcher Adresse die Administrationsoberfläche des T-Systems Konnektors verfügbar ist, kann in Kapitel 3.5.3 eingesehen werden.

Der Konnektor kann generell in 3 unterschiedlichen Betriebsmodi eingesetzt werden:

- Offline - Keine Verbindung zur Telematikinfrastruktur möglich
- Online mit logischer Separierung in die TI - der Konnektor ist nicht als Router einsetzbar (Dieses Feature ist abgekündigt und soll nicht mehr verwendet werden.)
- Online

Überprüfen Sie den Leuchtdiodenstatus (siehe hierzu 4.4.1). Leuchten die LEDs Power, TI, SIS und Status grün können Sie ihre Fachanwendung im Zusammenhang mit dem T-Systems Konnektor verwenden.

Sollte durch Leuchten der LEDs ein Fehlerfall signalisiert werden, sehen Sie bitte ebenfalls in Kapitel 4.4.1 nach bzw. kontaktieren Sie bitte den Hersteller.

So stellen Sie den Konnektor auf Offline / Online:

1. Ausgehend von der Startseite der Administration finden Sie den Menüpunkt Leistungsumfang. Wählen Sie diesen Menüpunkt aus.
2. Auf der folgenden Seite befindet sich ein Schalter Online. Konfigurieren Sie diesen Schalter auf Aus, wenn Sie den Offline-Modus einstellen wollen.
3. Konfigurieren Sie diesen Schalter auf An, wenn Sie den Online-Modus einstellen wollen.
4. Klicken Sie danach auf die Schaltfläche Übernehmen.

Halten Sie während der Inbetriebnahme die Startreihenfolge ein. Nur mit diesem Vorgehen kann sichergestellt werden, dass die verwendete gSMC-K vertrauenswürdig ist.

4.9.1 Betriebszustände

Die aktuellen Betriebszustände des Konnektors sind anhand verschiedener Meldungen in der Softwareoberfläche unter Hauptmenü > Betriebszustände erkennbar. Die einzelnen Meldungen werden dabei unter Hauptmenü > Protokollierung archiviert. Siehe Kapitel 7.10.

(Sicherheits-)kritische Betriebszustände werden zusätzlich über die LEDs angezeigt, siehe Kapitel 4.4. Es werden verschiedene Zustände unterschieden:

1. (Sicherheits-)kritische Betriebszustände
2. Unkritische Fehlerzustände
3. Warnzustände
4. Informationen

Zu den jeweiligen Kategorien zugeordnet werden die Zustände in den folgenden Aufstellungen wiedergegeben.

4.9.1.1 (Sicherheits-)kritischer Betriebszustand

Nachfolgend werden die Meldungen aus der Protokollierung aufgelistet. Ein kritischer Betriebszustand benötigt Ihr Eingreifen. Im Regelfall handelt es sich um Zustände, die vom Konnektor nicht mehr eigenständig behandelt werden können. Kritische Betriebszustände beeinflussen das Betriebsverhalten des Konnektors und haben im Regelfall Einfluss auf die Sicherheit des Systems.

Tabelle 12 Fehlermeldungen bei kritischem Betriebszustand

Meldung	Abhilfe
EC_Software_Integrity_Check_Failed	Es wurde erkannt, dass ein Bestandteil der Software des Konnektors nicht mehr integer und damit nicht mehr vertrauenswürdig ist. Der Konnektor wird nicht gestartet und die Status LED (siehe 4.4) leuchtet rot. Senden Sie das Gerät an den Hersteller zurück.
EC_Random_Generator_Not_Reliable	Es wurde ein Problem mit dem Zufallszahlengenerator erkannt. Dieser Generator ist Teil der gSMC-K. Die gSMC-K wurde entweder aus dem Gerät entfernt oder weist einen Defekt auf. Alle vier LEDs blinken. Prüfen Sie ob die Sicherheitssiegel des Gehäuses unbeschädigt sind. Bei defektem Sicherheitssiegel oder entwendeter gSMC-K stellen Sie unverzüglich einen Sperrantrag für das Gerät beim Lieferanten. Sind keine Beschädigungsspuren erkennbar, senden Sie das Gerät an den Hersteller zurück.
EC_Security_Log_Not_Writable	Das Sicherheitsprotokoll kann nicht geschrieben werden. Sie können diese Situation nicht eigenständig beheben. Senden Sie das Gerät an den Hersteller zurück.
EC_Time_Sync_Pending_Critical	Die Uhrzeit des Geräts muss synchronisiert werden. Sie können die Uhrzeit des Systems manuell konfigurieren oder eine Zeitsynchronisation mit der Telematik Plattform vornehmen (Kapitel 6.8, 7.3 und Kapitel 3.5.2). Wenn Sie die Zeitsynchronisation nicht vornehmen, kann der Betriebszustand & EC_Time_Difference_Intolerable erreicht werden.
EC_Time_Difference_Intolerable	Die Uhrzeit des Geräts muss synchronisiert werden. Die erreichte Zeitdifferenz zu Referenzzeit kann nicht mehr toleriert werden. Nehmen Sie eine manuelle Konfiguration der Uhrzeit vor und stellen Sie anschließend die Verbindung zur sicheren Telematik Plattform her (Kapitel 6.8) Die Synchronisation der Uhrzeit erfolgt anschließend automatisch.

Meldung	Abhilfe
EC_CRL_Out_Of_Date	Die vom Konnektor verwendete Zertifikatssperrliste ist abgelaufen. Verwenden Sie die Managementoberfläche, um eine neue Zertifikatssperrliste in den Konnektor einzuspielen (Kapitel 7.1.3). Alternativ wird der Konnektor versuchen, einmal am Tag oder beim Verbindungsaufbau zur Telematikplattform eine aktuelle Zertifikatssperrliste herunterzuladen. Ist die Zertifikatssperrliste abgelaufen und kann keine neue Zertifikatssperrliste online heruntergeladen werden, so ist auch kein Aufbau eines sicheren Tunnels zur Telematik Plattform möglich. In diesem Falle muss die Zertifikatssperrliste manuell geladen und über die Managementoberfläche aktualisiert werden (siehe hierzu 7.1.3).
EC_TSL_Out_Of_Date_Beyond_Grace_Period	Der Konnektor hat erkannt, dass die Trust-Service Status List endgültig abgelaufen ist. Sie müssen die Trust-Service Status List über die Managementoberfläche des Konnektors manuell aktualisieren (Kapitel 7.1.2).
EC_TSL_Trust_Anchor_Out_Of_Date	Der Konnektor hat erkannt, dass die Gültigkeit des Vertrauensankers abgelaufen ist. Sie müssen die Trusted Service List über die Managementoberfläche des Konnektors manuell aktualisieren (Kapitel 7.1.2).
EC_Firewall_Not_Reliable	Der Konnektor hat erkannt, dass die Firewall nicht mehr zuverlässig arbeitet. Prüfen Sie die vorhandenen Einträge im Sicherheitsprotokoll (Kapitel 7.10) des Konnektors, um die Ursache zu ermitteln.
EC_Secure_KeyStore_Not_Available	Der Konnektor kann nicht mehr auf die gSMC-K zugreifen. Ergreifen Sie die gleichen Maßnahmen wie für den Zustand EC_Random_Generator_Not_Reliable.

4.9.1.2 Fehlerzustand (nicht kritisch)

Nicht kritische Fehlerzustände haben zwar Auswirkungen auf das Betriebsverhalten des Konnektors, sind aber nicht kritisch für die Sicherheit des Systems.

Tabelle 13 Fehlermeldungen bei unkritischen Betriebszustand

Meldung	Abhilfe
EC_CardTerminal_Not_Available	Das Kartenterminal mit der angegebenen Terminal-ID ist nicht verfügbar. Überprüfen Sie, ob das Terminal für den Konnektor erreichbar ist, beispielsweise unter Verwendung der Administrationsseite zu den Kartenterminals.
EC_No_VPN_TI_Connection	Der Konnektor konnte keine Verbindung zur Telematikplattform aufbauen. Führen Sie die folgenden Überprüfungen durch: Wird der Konnektor im Offline-Modus betrieben?

Meldung	Abhilfe
	Ist der Konnektor mit dem WAN verbunden und hat der Konnektor eine gültige IP-Adresse? Ist die am Konnektor eingestellte Uhrzeit korrekt? Hat der Konnektor eine aktuelle Sperrliste zur Verfügung? Ist die Trusted Service List (TSL) aktuell? Lässt Ihr Internetanbieter gesicherte VPN-Verbindungen zu? Kann das Problem nicht durch eine der angegebenen Maßnahmen behoben werden, kontaktieren Sie einen Servicetechniker oder den Hersteller zur weiteren Unterstützung.
EC_No_VPN_SIS_Connection	Der Konnektor konnte keine Verbindung zum sicheren Internet-Service herstellen. Führen Sie die gleichen Prüfungen wie beim Zustand EC_No_VPN_TI_Connection durch.
EC_No_Online_Connection	Der Konnektor konnte keine Verbindung ins WAN aufbauen. Prüfen Sie, ob der Konnektor mit dem WAN verbunden ist. Besteht die Fehlermeldung dauerhaft weiter, kontaktieren Sie einen Servicetechniker oder den Hersteller zur weiteren Unterstützung.
EC_FeatureOrTUC_Not_Available	Es wurde versucht, eine nicht vorhandene oder nicht freigeschaltete Funktion aufzurufen. Diesen Zustand können Sie nicht korrigieren, erfordert aber auch nicht ihr Eingreifen.
EC_IP_Adresses_Not_Available	Die IP-Adressen des Netzkonnektors sind nicht oder falsch gesetzt. Bitte korrigieren Sie die Netzeinstellungen im Konnektormanagement.

4.9.1.3 Warnzustand

Warnzustände werden ausgelöst, um zu signalisieren, dass ein Eingreifen in den aktuellen Betriebszustand des Konnektors erforderlich ist, um einen Fehlerzustand und damit die Beeinträchtigung der Funktionsbereitschaft zu vermeiden.

Tabelle 14 Warnmeldungen für Funktionsbereitschaft

Meldung	Abhilfe
EC_Log_Overflow	Die Anzahl der Protokolleinträge im Konnektor ist so stark angewachsen, dass auch Protokolleinträge verdrängt werden, die nicht älter sind als die konfigurierte Aufbewahrungsdauer von Protokolleinträgen. Verwenden Sie die Managementoberfläche des Konnektors, um ggf. vorhandene Protokolleinträge zu sichern und alte Protokolleinträge zu löschen.
EC_CRL_Expiring	Die im Konnektor vorhandene Zertifikatssperrliste wird bald ablaufen. Aktualisieren Sie die Sperrliste manuell oder stellen Sie eine Online-Verbindung her, sodass der Konnektor die Sperrliste eigenständig aktualisieren kann.

EC_Time_Sync_Pending_Warning	Die Uhrzeit des Geräts wurde seit mehr als 30 Tagen nicht mehr aktualisiert. Sie können die Uhrzeit des Systems manuell konfigurieren oder eine Zeitsynchronisation mit der Telematikplattform vornehmen (Kapitel 6.8, 7.3 und Kapitel 3.5.2). Wenn Sie die Zeitsynchronisation nicht vornehmen, kann der Betriebszustand EC_Time_Sync_Pending_Critical erreicht werden.
EC_TSL_Out_Of_Date_Within_Grace_Period	Die Gültigkeit der Trusted Service List ist abgelaufen. Der Konnektor akzeptiert die TSL jedoch weiterhin, da der angegebene Toleranzzeitraum noch nicht überschritten ist.
EC_CRYPTOPERATION_ALAvpnRM	Der Konnektor hat eine Häufung kryptografischer Operationen festgestellt. Prüfen Sie die Protokolldateien des Konnektors, um evtl. ungewöhnliche Zugriffe auf den Konnektor festzustellen. Der vermehrte Aufruf kryptografischer Operationen muss nicht in jedem Falle auf einen Angriff hindeuten, sondern kann auch auf eine Vielzahl an durchgeführten Prüfungen elektronischer Signaturen o.ä. zurückgeführt werden.

4.9.1.4 Infozustand

Tabelle 15 Infomeldungen zum Betriebszustand

Meldung	Abhilfe
EC_TSL_Expiring	Die Trusted Service List des Konnektors wird demnächst ablaufen. Stellen Sie eine Online-Verbindung her, um eine automatische Aktualisierung zu ermöglichen oder aktualisieren Sie die Vertrauensliste manuell (siehe Kapitel 7.1.2).
EC_TSL_Update_Not_Successful	Die Aktualisierung der Trusted Service List war nicht erfolgreich. Stellen Sie eine Online-Verbindung her, um eine automatische Aktualisierung zu ermöglichen oder aktualisieren Sie die Vertrauensliste manuell (siehe Kapitel 7.1.2).
EC_Trust_Anchor_Expiring	Der verwendete Vertrauensanker zur Prüfung der Trusted Service List wird in Kürze ablaufen. Stellen Sie eine Online-Verbindung her, um eine automatische Aktualisierung zu ermöglichen oder aktualisieren Sie die Vertrauensliste manuell.
EC_CardTerminal_Software_Out_Of_Date	Die auf dem Kartenterminal installierte Firmware ist nicht mehr länger für den produktiven Einsatz vorgesehen. Nehmen Sie Kontakt mit dem Hersteller des Kartenterminals auf und installieren Sie ein Update der Firmware.
EC_Connector_Software_Out_Of_Date	Die installierte Firmware des Konnektors ist nicht mehr länger für den produktiven Einsatz vorgesehen. Installieren Sie ein Update der Firmware. Updates können Sie von der Webseite des Herstellers beziehen.

EC_Time_Sync_Not_Successful	Die vorgenommene Zeitsynchronisation war nicht erfolgreich. Führen Sie die Synchronisation der Uhrzeit erneut durch.

4.10 Aktualisierung des T-Systems Konnektors

Die automatische Prüfung auf verfügbare Aktualisierungen ist standardmäßig eingeschaltet, wohingegen der automatische Download nicht eingeschaltet ist. Der Download wird durch den Administrator durchgeführt. Auch die Aktualisierung des T-Systems Konnektors muss durch den Administrator durchgeführt werden.

4.11 Registrierung des Konnektors

Damit der Konnektor als Element zur sicheren Kommunikation zwischen dem Netz der Praxis oder des Krankenhauses und der Telematikinfrastruktur korrekt arbeitet, muss der Konnektor beim Anbieter des VPN-Dienstes registriert werden. Dazu benötigen Sie mindestens eine personalisierte SMC-B Karte. Mit Hilfe dieser SMC-B und der zugehörigen Vertragsnummer muss der Konnektor online registriert werden unter Hauptmenü > Registrierung. Sie haben keine andere Möglichkeit, um den Konnektor zur Nutzung in der Telematikinfrastruktur zu registrieren. Zu weiteren Informationen rund um die Bedienung der Software lesen Sie bitte das entsprechende Kapitel 4.

Eine erfolgreiche Registrierung des Konnektors ist eine unbedingte Voraussetzung für eine erfolgreiche Inbetriebnahme als Online-Konnektor.

4.12 Werksreset

Die Durchführung eines Werksresets ist im Kapitel 7.16 Werksreset beschrieben. Anschließend muss ein neues Passwort vergeben werden. Siehe dazu auch Kapitel 7.16.1 Admin Passwort vergessen (Werksreset wird ausgelöst).

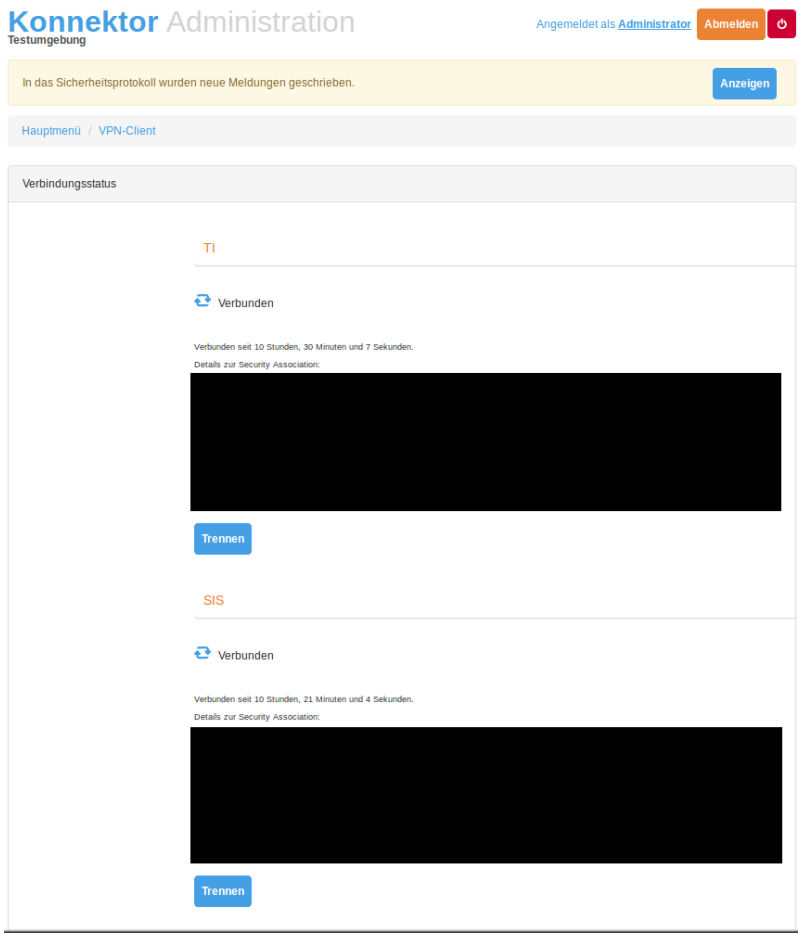
4.13 Außerbetriebnahme sowie End-of-Life (Ende des Lebenszyklus) des T-Systems Konnektors

Wenn Sie den Konnektor außer Betrieb nehmen (dauerhaft), müssen Sie den Konnektor deregistrieren und einen Werksreset durchführen. Andernfalls ist der Konnektor weiterhin auf die für Ihre Praxis oder Krankenhaus ausgestellte Praxisidentität registriert. Wird der Konnektor dauerhaft entsorgt, muss vorher die gSMC-K zerstört werden, da dort vertrauenswürdige Daten gespeichert sind.

Der T-Systems Konnektor muss bei der Außerbetriebnahme zunächst beim VPN-Zugangsdienst deregistriert werden, sodass kein weiterer Zugriff auf die zentrale TI mehr möglich ist.

1. Unter Hauptmenü > VPN-Client auswählen
2. Unter VPN Client > Verbindungsstatus TI auswählen

3. Unter Verbindungsstatus TI die Funktion „Trennen“ auswählen.



4.13.1 Deregistrierung

1. Unter Hauptmenü > Registrierung auswählen

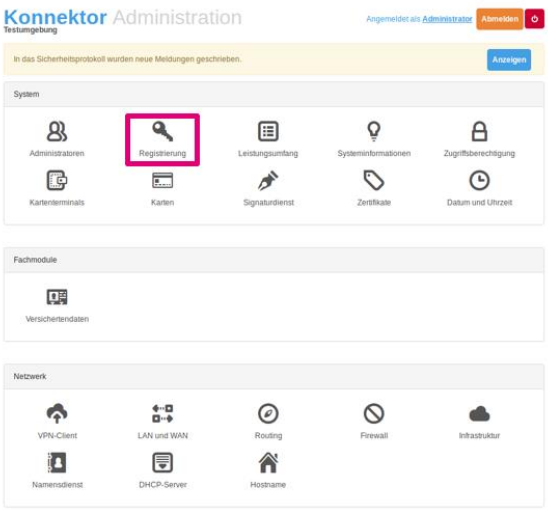


Abbildung 11 Benutzeroberfläche - Hauptmenü

2. Unter Registrierung > „Registrierung zurücknehmen“ auswählen

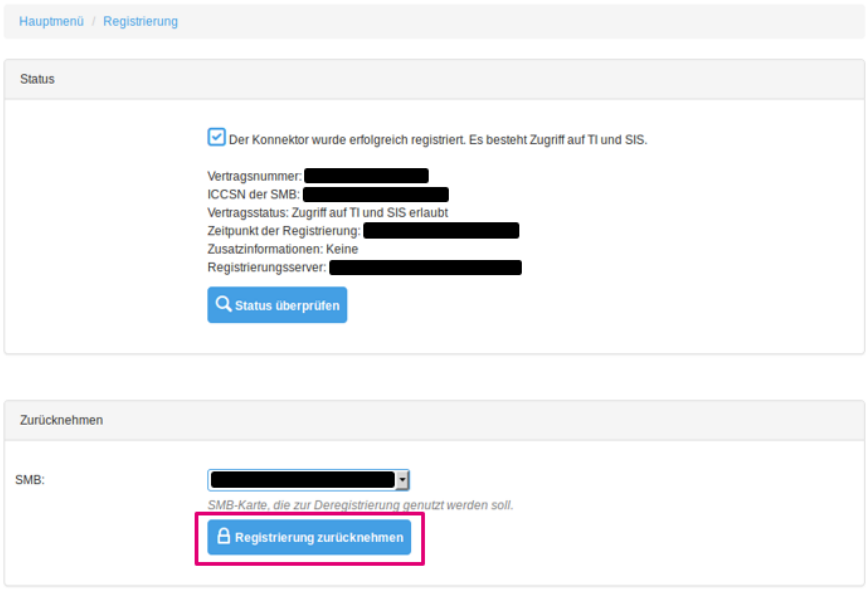


Abbildung 12 Hauptmenü>Registrierung > Registrierung zurücknehmen

4.13.2 Finale Außerbetriebnahme und Rücktransport

WICHTIG: BITTE RUFEN SIE ZWINGEND DEN HERSTELLER (Siehe A.1.3) AN. HALTEN SIE HIERZU IHRE CONTRACT-ID UND DIE ICCSN (Typenschild auf der Unterseite des Konnektors Siehe 4.1.1) BEREIT. DIES GILT INSBESONDERE FÜR DIE KONNEKTOR FIRMWARE VERSION 1.4.13 FÜR DIE EINE SPEZIELLE VORGEHENSWEISE NOTWENDIG IST!

Zur Außerbetriebnahme des Konnektors sind vom LEI einige Tätigkeiten durchzuführen um ggf. vorhandene personenbezogene Daten auf dem Konnektor vor unbefugtem Zugriff zu schützen.

Der LEI wird aufgefordert folgende Schritte zu erledigen:

- Deregistrierung des Konnektors: Dabei wird das Gerät bei T-Systems als Betreiber des vom Leistungserbringer genutzten VPN-Zugangsdienstes abgemeldet. Der Hersteller deregistriert in diesem Fall die zugehörige gSMC-K im VPN-Zugangsdienst und veranlasst die Sperrung der gSMC-K-Zertifikate.
- Werksreset: Hierbei werden Passwörter und Konfiguration auf den Auslieferungszustand zurückgesetzt.
- Zurücksendung des Konnektors über einen sicheren Lieferweg an den Hersteller: Der Hersteller wird den LEI per Telefon die Vorgehensweise erläutern um eine sichere Lieferung zu gewähren. Der Hersteller wird nach Empfang des Konnektors das Gehäuse öffnen, die im Gerät verbaute gSMC-K entfernen und diese anschließend durch Schreddern vernichten. Das verbleibende Gerät wird ebenfalls vollständig durch Schreddern vernichtet.

4.13.3 Entfernen des T-Systems Konnektors aus Infrastruktur

Nach der Außerbetriebnahme kann der T-Systems Konnektor in umgekehrter Reihenfolge als beim Anschluss aus Ihrer Infrastruktur entfernt werden.

1. Trennen Sie das Stromkabel vom T-Systems Konnektor.
2. Entfernen Sie das Ende des LAN-Netzwerkkabels aus der Buchse des T-Systems Konnektors mit der Beschriftung LAN und das andere Ende aus Ihrem Switch bzw. Router.
3. Entfernen Sie das Ende des WAN-Netzwerkkabels aus der Buchse des T-Systems Konnektors mit der Beschriftung WAN und das andere Ende aus Ihrem Switch / Router bzw. Internet-Router oder Modem.

5 Bedienung der Software

Als Anwender können Sie den T-Systems Konnektor ausschließlich unter Verwendung der Managementoberfläche konfigurieren, die Ihnen vom Anwendungskonnektor angeboten wird. Änderungen der Konnektorkonfiguration werden von diesem immer protokolliert. Dies bedeutet, dass Sie die Möglichkeit haben, erfolgte Änderungen an der Konfiguration des Konnektors mit Hilfe der Log- und Protokolldateien nachzuvollziehen.

In den beiden folgenden Kapiteln werden die Konfigurationsmöglichkeiten des Netz- und Anwendungskonnektors getrennt behandelt. Die grafische Managementoberfläche leitet die entgegengenommenen Konfigurationsparameter an den T-Systems Konnektor weiter.

5.1 Zugriff auf die Managementoberfläche

Die Administrationsschnittstelle und somit die Managementoberfläche des Konnektors sind ausschließlich unter Verwendung eines Webbrowsers mit TLS-Sicherung erreichbar. Bitte verwenden Sie hierzu einen der folgenden Browser:

Tabelle 16 Unterstützte Browser

Unterstützte Browser	
Apple Safari	Ab Version 8.0
Chromium Browser	Ab Version 34.0
Google Chrome	Ab Version 34.0
Microsoft Edge	Ab Version 1.0
Microsoft Internet Explorer	Ab Version 10.0
Mozilla Firefox	Ab Version 18.0
Opera Browser	Ab Version 15.0

Der Konnektor verwendet zur Sicherung der Kommunikation ein elektronisches Zertifikat. Falls Ihr Webbrowser beim Zugriff auf den Konnektor eine Sicherheitswarnung anzeigt, müssen Sie das Zertifikat des Konnektors als vertrauenswürdiges Zertifikat in den Vertrauensspeicher des Webbrowsers importieren bzw. eine Ausnahme einrichten. Stellen Sie hierzu sicher, dass Sie eine direkte und überprüfte Verbindung zum Konnektor haben.

Sicherheitshinweis: Der Hersteller empfiehlt aus Sicherheitsgründen eine direkte Kabel-Verbindung vom Computer des Administrators zur LAN Schnittstelle des Gerätes. Da das Gerät mit einer Service IP-Adresse ausgeliefert wird, ist hier eine manuelle Anpassung der Netzwerkschnittstelle am Computer des Administrators notwendig um die Kommunikation herzustellen (Beispielsweise 10.10.8.16 mit Subnetz 255.255.255.0 und der Konnektor IP 10.10.8.15 als Gateway).

Die Zertifikat-Import-Funktionen können je nach Betriebssystem und verwendeten Browser unterschiedlich sein.

Beispiele mit Internet Explorer und Chrome:

Bei der Nutzung von Microsoft Internet Explorer wird in der URL Leiste rechts „Zertifikatsfehler“ angezeigt.

Bei der Nutzung von Google Chrome wird in der URL Leiste links „Nicht sicher“ angezeigt.

Folgen Sie den Anweisungen und exportieren / speichern Sie das Zertifikat des Konnektors auf dem Computer von dem zukünftig die Einrichtung und Administration des Konnektors vorgenommen wird.

Bei Nutzung eines Windows Betriebssystems ist als nächster Schritt der Import des Zertifikates notwendig:

Windows-Systemsteuerung aufrufen:

Windows 10: Im Suchfeld der Windows-Taskleiste sys eingeben und wählen Sie dann "Systemsteuerung" aus.

Windows 8: Tastenkombination Windows-Taste + X und Kontextmenü "Systemsteuerung" auswählen

Windows 7: Auswahl über "Start" und dann auf "Systemsteuerung".

Auswahl rechts oben unter "Anzeige" den Eintrag "Kategorie" ( ).

Auswahl "Netzwerk und Internet" und dann auf "Internetoptionen".

Auswahl Registerkarte "Inhalte" und dann auf "Zertifikate".

Das Fenster "Zertifikate" öffnet sich

Im Fenster "Zertifikate“ die Registerkarte "Vertrauenswürdige Stammzertifizierungsstellen" auswählen.

Auswahl „Importieren...".

Das Fenster "Zertifikatimport-Assistent" öffnet sich

Auswahl im Fenster "Zertifikatimport-Assistent" auf "Weiter".

Auswahl "Durchsuchen" und die zuvor vom Browser gespeicherte Datei mit dem Zertifikat auswählen.

Auswahl „Weiter", noch einmal "Weiter" und danach "Fertig stellen".

Es öffnet sich das Fenster "Sicherheitswarnung".

Bestätigung im Fenster "Sicherheitswarnung" mit „Ja".

Auswahl zum Beenden des Zertifikatimport-Assistenten mit „OK"

Dem Zertifikat kann vertraut werden, da der Konnektor über eine sichere Lieferkette transportiert und zudem im Rahmen der Inbetriebnahme die Unversehrtheit der Siegel geprüft wurde.

Als Administrator muss man sich vor Eingabe und Anmeldung am Konnektor versichern, dass man mit der richtigen Konnektor IP-Adresse verbunden ist und das zuvor importierte Zertifikat gültig ist und keinen Fehler anzeigt.

Der Konnektor verfügt auf dem LAN-Adapter über eine sogenannte Service-IP-Adresse. Bitte verwenden Sie zur Konfiguration des Konnektors die folgenden Daten:

Tabelle 17 Standardkonfigurationsdaten

Konfigurationsdaten	
IP-Adresse	10.10.8.15
Subnetzmaske	255.255.255.0
Name	admin
Passwort	konnektor

Sie benötigen eine Netzwerkadresse aus dem entsprechenden Netzwerksegment, um auf den Konnektor unter https://10.10.8.15:4433 zuzugreifen. Dazu können Sie in der Konfiguration des Betriebssystems Ihrem Netzwerkadapter eine zweite IP-Adresse zuweisen, die sich in dem korrekten Netzwerksegment befinden muss. Weisen Sie beispielsweise Ihrem Netzwerkadapter die statische IP-Adresse 10.10.8.20 und die Subnetzmaske 255.255.255.0 zu, um auf die Managementoberfläche zuzugreifen.

5.1.1 Änderung des Benutzerkennworts

Sie werden während des erstmaligen Logins aufgefordert, das Benutzerkennwort zu ändern. Diesen Vorgang können Sie nicht umgehen. Bitte merken Sie sich das neu eingestellte Passwort.

Bei eingeschalteter dynamischer Adresszuweisung (DHCP) kann der Konnektor eine zweite IP-Adresse erhalten. Für jegliche weitere Konfiguration verwenden Sie bitte weiterhin die oben definierte IP-Adresse des Konnektors.

5.1.2 Fernwartung

Wichtiger Hinweis: Für die Gerät mit der **Firmwareversion 1.4.x** des Konnektors ist das Backend für die Fernwartungsfunktion **nicht aktiv**. Dies betrifft ebenfalls die Kapitel 5.2.4 Wartung, Kapitel 7.13 Menüpunkt Fernwartung und Kapitel 7.14 CA-Zertifikat für die Fernwartungsverbindung.

Es ist grundsätzlich möglich, den T-Systems Konnektor aus der Ferne zu administrieren. Dazu müssen Sie initial / einmalig eine Verbindung Ihres Konnektors mit dem Wartungs-Backend Ihres Service Providers, in diesem Fall die T-Systems International GmbH, herstellen.

Die Rolle des lokalen Superadministrators meldet den Konnektor per ICCSN (eindeutige 20-stellige Kartenkennnummer auf dem Typenschild an der Unterseite des Konnektors sowie über die Systeminformationen der WEB Oberfläche) beim Service Provider an. Das erfolgt

über einen sicheren Kommunikationskanal per Telefon oder verschlüsselter E-Mail. Der Service-Provider identifiziert mittels der ICCSN den Konnektor und ordnet sich diesen im Wartungs-Backend zu.

Der lokale Superadministrator des Konnektors erhält eine verschlüsselte E-Mail mit den vollständigen Zugangsdaten inkl. neu vergebenem Passwort (Die Länge des übermittelten starken Passworts beträgt 15 Zeichen). Diese Zugangsdaten sind durch den lokalen Superadministrator des Konnektors auf dem Konnektor einzutragen.

Die Einstellungen zur Konnektor-Fernwartung sind im Kapitel 7.13 beschrieben und können durch die Rolle eines Superadministrators oder eines berechtigten lokalen Administrators vorgenommen werden.

1. Setzen Sie unter Hauptmenü > Fernwartung die Option Fernwartung zulassen auf An
2. Falls erforderlich geben Sie die URL der Fernwartung sowie das Service-Provider Kennwort ein und wählen Sie anschließend Übernehmen.
3. Überprüfen Sie nun unter Hauptmenü > Fernwartung den Status. Der Status Verbunden für den Ereignis- bzw. Befehls-Kanal signalisiert eine aktive Verbindung.

Das Backend ist die dedizierte Instanz der Fernwartung und wird von der T-Systems International GmbH ausschließlich für den Zweck der Fernwartung genutzt. Es wird ausschließlich durch die T-Systems GmbH betrieben und ist nicht für Dritte freigegeben. Das Backend wird auf einen aktuellen Stand der Technik und Patchlevel gehalten.

Um eine Überprüfung von Remote Operation durch das RMS Personal nachvollziehen zu können, wird folgender Eintrag im Systemprotokoll erzeugt:

<Zeitstempel>; Event MGM/ADMINCHANGES; Operation; Info; Action=RMS_ASYNC_OPERATION; Details=Fernwartung-Operation: Asynchrone Operation-hinzufügen; User=RMS-Admin

Sollte der Konnektor so konfiguriert worden sein, das Remote Operationen erst nach lokaler Genehmigung ausgeführt werden, so ist der Log Eintrag wie folgt aufgebaut:

Zeitstempel>; Event MGM/ADMINCHANGES; Operation; Info; Action=CONFIRM; Details=Fernwartung-Operation: Asynchrone Operation genehmigen; NewVal=<Angabe von NewVal>; RefID=OPERATION_ID; User=<Benutzername des ausführenden Administrators>

Für nähere Informationen zur Fernwartung allgemein lesen Sie hierzu auch Kapitel 7.13.

Hinweis: Es ist jederzeit möglich, unter Zuhilfenahme der zuvor beschriebenen Prozedur, das Passwort zur Authentisierung des Konnektors an der Fernwartung (Wartungs-Backend) zu ändern. Eine erzwungene und regelmäßige Änderung des Passwortes ist aufgrund des hohen Aufwandes im Wartungs-Backend nicht vorgesehen.

5.1.3 Signaturdienst

Der Signaturdienst des T-Systems Konnektors umfasst die Funktionalität der nicht-qualifizierten elektronischen Signatur (nQES) mit der SM-B sowie die qualifizierte elektronische Signatur (QES) mit dem HBA und den HBA-Vorläuferkarten HBA-qSig und ZOD_2.0 (alle zusammen als HBAx bezeichnet). Es können sowohl Signaturen erstellt als auch überprüft werden.

5.1.3.1 Parallele Signatur und Gegensignatur

Neben der Erstsignatur eines noch nicht signierten Dokumentes unterstützt der T-Systems Konnektor auch parallele Signaturen (Signieren eines bereits signierten Dokumentes). Außerdem unterstützt der T-Systems Konnektor Gegensignaturen, die jeweils alle bestehenden Signaturen gegensignieren. Die angebotene Möglichkeit des Gegensignierens bezieht sich dabei auf das Signieren aller vorhandenen parallelen Signaturen. Ein Gegensignieren von Gegensignaturen wird nicht angeboten.

Zwei Arten der Gegensignatur werden unterstützt, eine dokumentinkludierende Gegensignatur, bei der das Dokument und alle Signaturen gegensigniert werden sowie eine dokumentexkludierende Gegensignatur, bei der alle Signaturen gegensigniert werden, aber nicht der fachliche Inhalt des Dokumentes selbst.

5.1.3.2 Signaturformate

Der Konnektor unterstützt folgende Signaturformate zusammen mit den angegebenen Dokumentenformaten und Signaturniveaus (nicht qualifiziert: nQES, qualifiziert: QES):

Tabelle 18 Signaturformate & Signaturniveaus

Signaturformate & Signaturniveaus					
	XML	**PDF/A**	**Text**	**TIFF**	**Binär**
XML-Signatur	QES / nQES				
CMS-Signatur	QES / nQES	QES / nQES	QES / nQES	QES / nQES	nQES
PDF-Signatur		QES / nQES			
S/MIME	nQES	nQES	nQES	nQES	nQES
PKCS#1[3]					nQES

Mit HBA-Vorläuferkarten kann nur die Signatur von Einzeldokumenten durchgeführt werden. Es werden keine Stapelsignaturen (Anzahl der Dokumente > 1) von diesen Karten unterstützt. HBA-Vorläuferkarten können nur im Einfachsignaturmodus (Konfigurationseinstellung SAK_SIMPLE_SIGNATURE_MODE aktiviert) verwendet werden. Zusätzliche Erläuterung zur SAK (Signaturanwendungskonnektor) finden Sie im Kapitel 7.3.

Die Funktionen werden an externen Systemschnittstellen des T-Systems Konnektors bereitgestellt. Um die lokale Anzeige der Signaturerstellung und Signaturprüfung für den Benutzer zu realisieren, kann der Signaturproxy verwendet werden. Herstellern von Primärsystemen ist es freigestellt, die Ansichtsfunktion selbst in ihrer Anwendung umzusetzen, und auf die Verwendung des Signaturproxys zu verzichten.

[3] Signaturerstellung (nur mit dem Authentisierungsschlüssel des HBAx und SM-B): nicht qualifiziert: Binär (nur mit bestimmten Längen)

Signaturprüfung: nicht qualifiziert: XML, PDF/A, Text, TIFF, Binär bzw. qualifiziert: XML, PDF/A, Text, TIFF

5.1.3.3 Konfigurationseinstellungen

MGM_LU_SAK: Der Administrator kann damit den „Leistungsumfang Signaturanwendungskomponente qualifizierte Signatur“ aktivieren und deaktivieren. Ist dieser Leistungsumfang deaktiviert, ist die Durchführung einer qualifizierten Signaturerstellung und Signaturprüfung nicht möglich (Fehlermeldung 4125). Die Erstellung und Prüfung einer nicht-qualifizierten Signatur ist weiterhin möglich. Standard ist Eingeschaltet.

SAK_SIMPLE_SIGNATURE_MODE: Aktivierung / Deaktivierung des „Einfachsignaturmodus“ für alle HBAx für die Durchführung von Einfachsignaturen für Dokumentenstapel der Größe 1. Ist dieser Modus aktiviert wird bei der qualifizierten Signatur eines einzelnen Dokumentes eine vereinfachte Sicherheitsumgebung angewendet (ohne gegenseitige Authentisierung der Karte und des Konnektors). Standard ist Eingeschaltet.

5.1.4 Verschlüsselungsdienst

Der Verschlüsselungsdienst bietet an seiner Systemschnittstelle Funktionen zum hybriden Ver- und Entschlüsseln von Dokumenten an, wobei folgende formaterhaltende Ver- / Entschlüsselungsmechanismen für die genannten Dokumententypen unterstützt werden:

- hybride Ver- und Entschlüsselung nach CMS-Standard von XML-, PDF/A-, Text-, TIFF-, Binär-Dokumenten
- hybride Ver- und Entschlüsselung von XML-Dokumenten
- hybride Ver- und Entschlüsselung von MIME-Dokumenten nach dem S/MIME-Standard

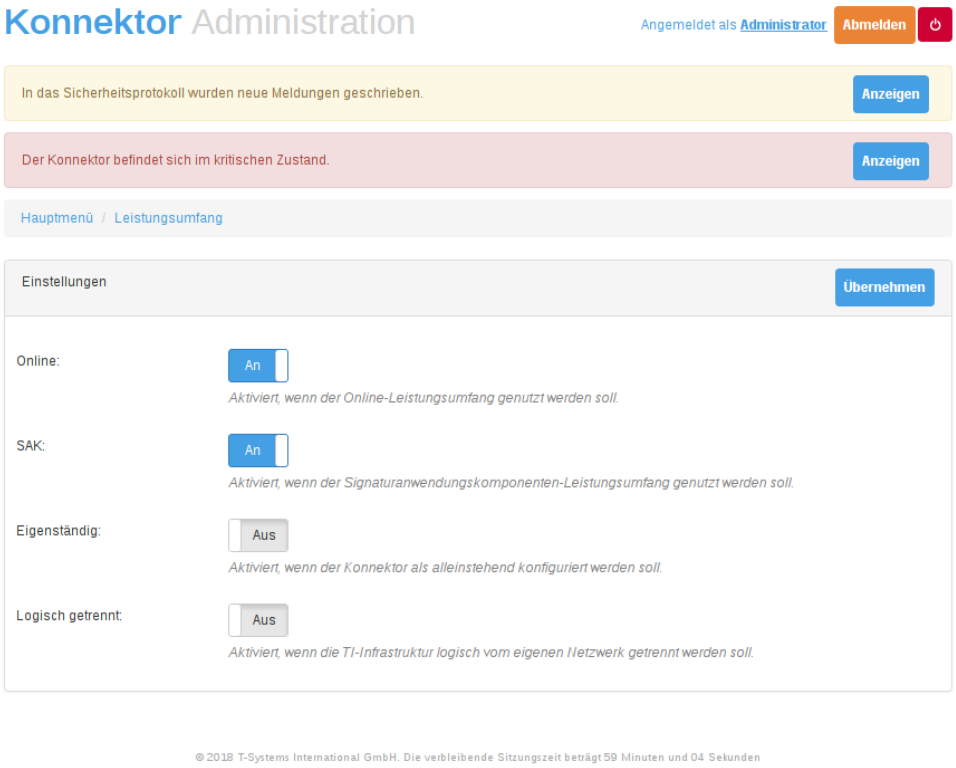
5.1.5 LDAP-Proxy

Der Konnektor ermöglicht es Clientsystemen und Fachmodulen durch Nutzung des LDAP-Proxies Daten aus dem Verzeichnisdienst der TI-Plattform (Verzeichnisdienst) abzufragen. Die Kommunikation erfolgt über das LDAPv3 Protokoll. Die Funktionalität steht nur zur Verfügung, wenn MGM_LU_ONLINE=Enabled ist.

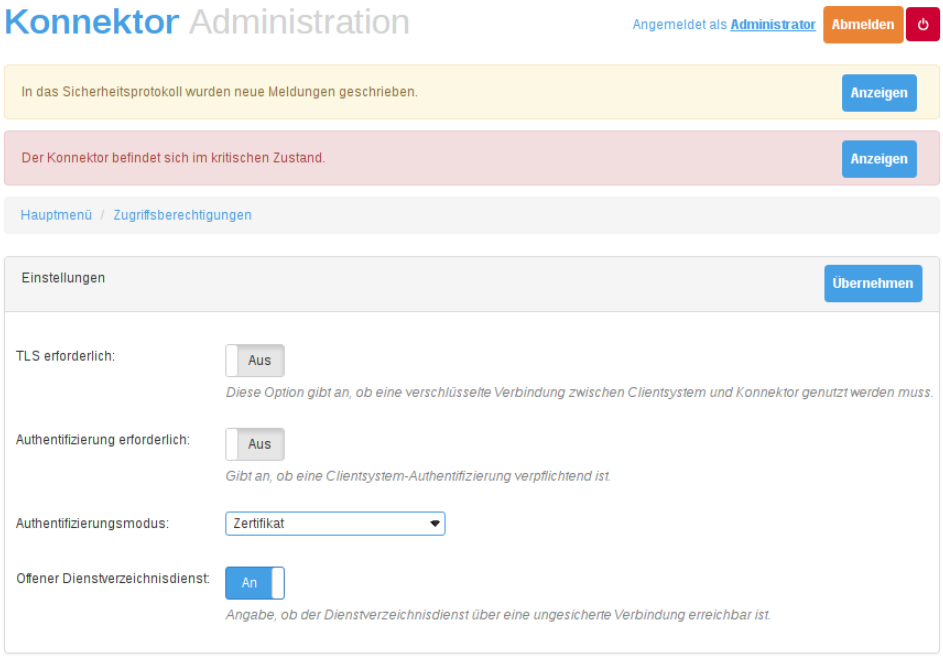
Wenn im Konnektor ANCL_TLS_MANDATORY=Enabled konfiguriert ist, kann vom Clientsystem nur über eine LDAPS-Verbindung (TCP Port 636) Daten vom Konnektor abgefragt werden. Ist Konnektor ANCL_TLS_MANDATORY=Disabled konfiguriert, können über eine LDAP-Verbindung (TCP Port 389) oder über eine LDAPS-Verbindung (TCP Port 636) Daten abgefragt werden.

Die LDAP-Proxy Einstellungen können im Menüpunkt VPN-Client vorgenommen werden.

Die Konfiguration des Parameters „MGM_LU_ONLINE“ lässt folgende Einstellungen zu:



Die Konfiguration des Parameters „ANCL_TLS_MANDATORY“ lässt folgende Einstellungen zu:



5.2 Hauptmenü

Beim Login in die Managementoberfläche wird das Hauptmenü angezeigt, welches als Ausgangspunkt für alle weiteren Aktionen in diesem Dokument immer wieder referenziert wird. Das Hauptmenü ist folgendermaßen gegliedert:

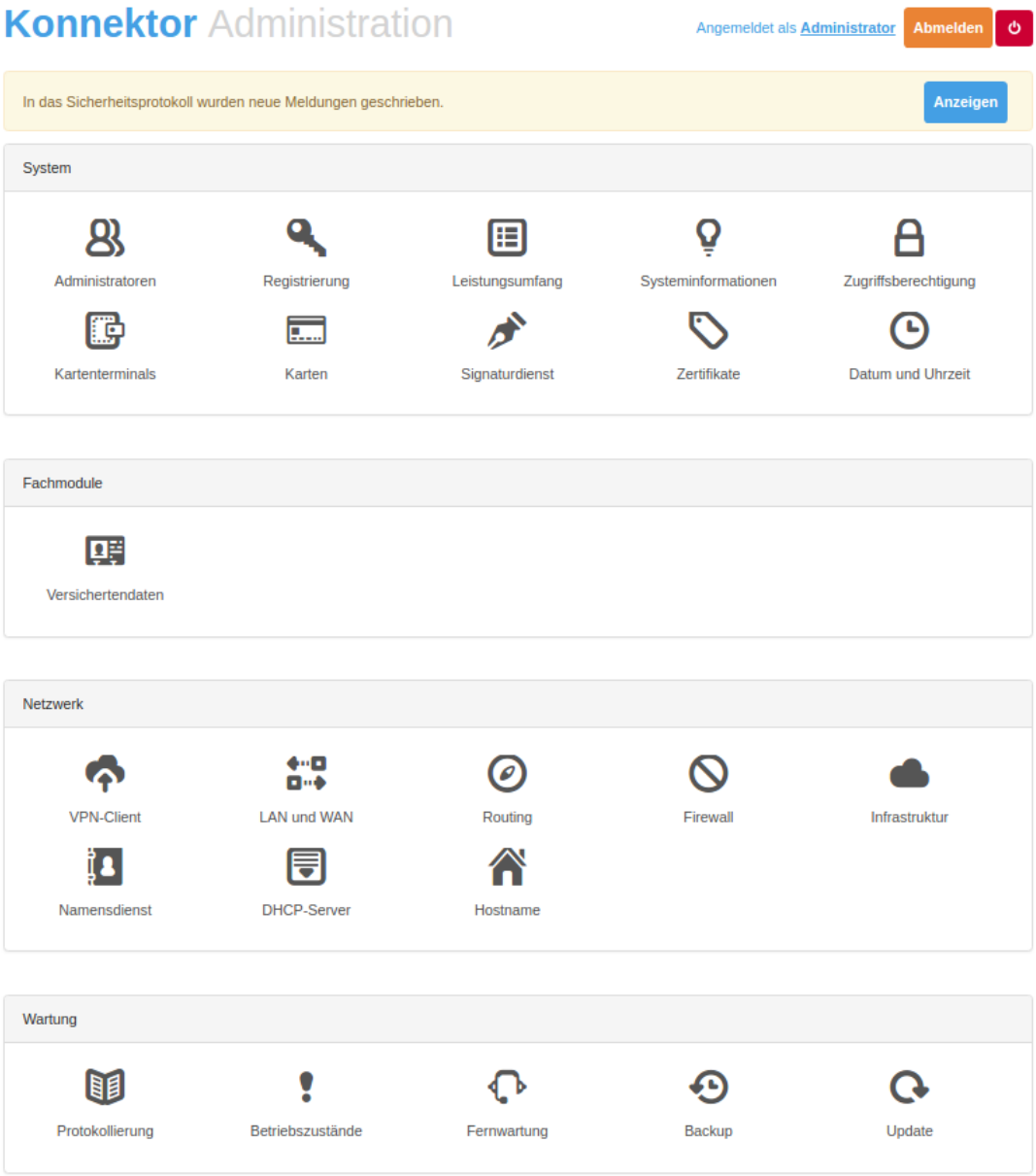


Abbildung 13 Hauptmenü

5.2.1 System

In der Sektion System werden Einstellungen und Informationen zu Diensten des Anwendungskonnektors mit Ausnahme des Fachmoduls für Versichertenstammdatenmanagement angezeigt.

Dies beinhaltet die folgenden Menüpunkte:

1. Administratoren: ermöglicht das Hinzufügen und Verwalten von Administratorenkonten.
2. Registrierung: ermöglicht die Anmeldung und Registrierung des Konnektors beim Anbieter des VPN-Dienstes.
3. Leistungsumfang: erlaubt die Einsichtnahme und Konfiguration des Leistungsumfangs des Konnektors.
4. Clientsysteme: bietet Konfigurationsinformationen und Einstellungsmöglichkeiten zu den Clientsystemen an.
5. Systeminformationen: erlaubt die Einsicht in die Versionsinformationen des Konnektors und ermöglicht die Konfiguration des Ereignisdienstes.
6. Zugriffsberechtigung: erlaubt die Konfiguration und Einsichtnahme der Zugriffsberechtigungen für Clientsysteme.
7. Kartenterminals: erlaubt die Einsichtnahme und Konfiguration zugeordneter Kartenterminals.
8. Karten: bietet eine Übersicht über vorhandene Karten in angeschlossenen Kartenterminals an.
9. Signaturdienst: ermöglicht die Konfiguration der Signaturanwendungskomponente des Konnektors.
10. Zertifikate: bietet Informationen zum aktuellen Vertrauensraum und erlaubt ebenso dessen Aktualisierung.
11. Datum und Uhrzeit: ermöglicht die Konfiguration der aktuellen Uhrzeit und des Datums.

Der Umgang mit diesen Menüpunkten wird im Abschnitt zum Anwendungskonnektor (siehe Abschnitt 7.1) erläutert.

5.2.2 Fachmodule

Im Bereich Fachmodule ermöglicht der Menüpunkt Versichertendaten die Einsichtnahme und die Konfiguration der Einstellungen für das Versichertenstammdatenmanagement (VSDM).

5.2.3 Netzwerk

Im Bereich Netzwerk können Netzwerk-Einstellungen zum T-Systems Konnektor vorgenommen werden. Die Einstellungsmöglichkeiten umfassen die im Folgenden aufgeführten Anteile.

1. VPN-Client: ermöglicht die Konfiguration zum Aufbau eines TI- und SIS-Tunnels.

2. LAN und WAN: erlaubt die Konfiguration der Einstellungen zu LAN und WAN. IP-Adressen können hier vergeben werden.
3. Routing: erlaubt die Einsichtnahme in die vorhandenen Routen und bietet die Möglichkeit neue Intranet-Routen anzulegen.
4. Firewall: ermöglicht die Einsichtnahme und Einstellung der benutzerdefinierten Firewallregeln.
5. Infrastruktur: ermöglicht die Einsichtnahme in die vorhandenen Netzsegmente und der aktivierten Bestandsnetze. Hier kann auch festgelegt werden, ob neue Bestandsnetze bei einem Update automatisch aktiviert werden sollen.
6. Namensdienst: ermöglicht die Konfiguration des DNS-Resolvers und zugeordneter DNS-Server.
7. DHCP-Server: ermöglicht die Konfiguration des integrierten DHCP-Servers
8. Hostname: ermöglicht das Setzen eines Namens für den Konnektor.

5.2.4 Wartung

Der Bereich Wartung umfasst die im Folgenden aufgeführten Anteile.

1. Protokollierung: bietet die Einsichtnahme in vorhandene Protokolleinträge an.
2. Betriebszustände: erlaubt die Einsichtnahme in den Betriebszustand des Konnektors.
3. Fernwartung: erlaubt den Start einer Fernwartung-Sitzung. Ist die Fernwartung / Remote Management Service (RMS) einmalig eingerichtet, so ist der Fernzugriff vom RMS-Backend System jederzeit möglich bis zur Deaktivierung der Fernwartung durch den lokalen Administrator
4. Backup: erlaubt den Im- und Export der Konnektoreinstellungen. Zudem besteht hier die Möglichkeit den Konnektor auf Werkseinstellung zurückzusetzen.
5. Update: erlaubt die Durchführung eines Software-Updates.

5.3 Erste Aktionen zur Inbetriebnahme des T-Systems Konnektors

Die in diesem Abschnitt beschriebenen Aktionen sind grundlegende Maßnahmen zur Inbetriebnahme des T-Systems Konnektors.

Ohne diese grundlegenden Aktionen kann der T-Systems Konnektor nicht zusammen mit ihrem Praxisverwaltungssystem verwendet werden:

- Konfiguration der Zeit
- WAN-Konfiguration
- Pairing eines Kartenterminals
- Einrichten eines Arbeitsplatzes

5.3.1 Konfiguration der Zeit

Sobald Sie Zugriff auf die Managementoberfläche des Konnektors haben, müssen Sie die Systemzeit des Konnektors einstellen. Der Konnektor weist unmittelbar nach der Inbetriebnahme nicht das korrekte Datum auf. Sie müssen das Datum und die Uhrzeit manuell auf den korrekten Wert einstellen. Bitte beachten Sie dazu die Hinweise im Abschnitt 6.8.

Eine automatische Zeitsynchronisation kann nur über die VPN-gesicherte Verbindung in die Telematik erfolgen. Damit diese Verbindung zum ersten Mal aufgebaut werden kann, muss die eingestellte Zeitangabe der aktuellen Uhrzeit entsprechen, da beim Aufbau des VPN-Tunnels Gültigkeitszeiträume elektronischer Zertifikate geprüft werden. Diese Prüfung ist im Falle einer zurückgesetzten Zeit nicht erfolgreich, demzufolge kann keine Verbindung zur TI (Telematikinfrastruktur) hergestellt werden.

Warum ist es notwendig die Systemzeit des Konnektors einzustellen?

Der Konnektor stellt die Systemzeit über einen Hardwarebaustein (RTC) ein. In der Auslieferung des Konnektors ist dieser Baustein über einen längeren Zeitraum ohne Versorgungsspannung. Beim nächsten Einschalten steht die Zeit auf der zuletzt aktiven Zeit. Danach muss die Zeit neu per Hand gestellt werden.

5.3.2 Pairing eines Kartenterminals

Bitte navigieren Sie zunächst zum Menüpunkt Kartenterminals, siehe 7.5.

Zum Pairing eines Kartenterminals müssen Sie Folgendes beachten:

Die IP-Adresse des Kartenterminals muss sich im gleichen Netzwerksegment wie die LAN-Schnittstelle des Konnektors befinden. Beachten Sie, dass der Konnektor standardmäßig mit dynamischer Adresszuweisung (DHCP) gestartet wird. Der Konnektor sollte demnach eine IP-Adresse aus Ihrem Netz zugewiesen bekommen. Sie können die vergebene IP-Adresse prüfen, indem Sie im Menüpunkt LAN/WAN unter LAN-Einstellungen die IP-Adresse ablesen. Konnte der Konnektor keine IP-Adresse beziehen, dann nimmt der Konnektor die Adresse 169.254.0.1 mit der Subnetzmaske 255.255.0.0 ein. In diesem Falle überprüfen Sie bitte Ihren DHCP-Server. Alternativ können Sie der LAN-Schnittstelle eine statische IP-Adresse zuweisen. Dazu deaktivieren Sie bitte den DHCP-Client des Konnektors und tragen die beabsichtigte statische IP-Adresse in der Konfigurationsoberfläche ein.

Der Konnektor unterstützt TLSv1.1 und TLSv1.2. Als Standardprotokoll wird TLSv1.2 verwendet. Der Konnektor erkennt automatisch, wenn das Kartenterminal TLSv1.1 verwendet. Um die TLS-Version im Terminal zu ändern (z.B. Standardversion TLSv1.2) verwenden Sie bitte das Konfigurationsmenü des Kartenterminals.

5.3.2.1 Ablauf des Pairings

Ausgehend vom Hauptmenü rufen Sie die Seite Kartenterminals auf. In der Tabelle Kartenterminals werden Ihnen alle, dem Konnektor bekannten Terminals aufgeführt. Damit ein Terminal in dieser Liste erscheint, kann eine der folgenden Aktionen durchlaufen worden sein:

1. Das Terminal hat ein Service-Announcement gesandt und der Konnektor konnte das Announcement verarbeiten.
2. Das Terminal hat auf ein vom Konnektor versendetes Service-Discovery reagiert.

3. Das Terminal wurde manuell hinzugefügt.

Für eine einfache Einbindung des Terminals prüfen Sie bitte, ob im Menü des Terminals das Senden eines Service-Announcements aktiviert ist. Nutzen Sie dazu bitte die Dokumentation des Terminalherstellers. Sind Konnektor und Terminal korrekt miteinander verbunden (IP-Adressen im gleichen Segment), sendet das Terminal nach dem Einschalten ein Service-Announcement und die IP-Adresse des Terminals wird in der Tabelle angezeigt.

Wird das Terminal nicht wie erwartet in der Tabelle aufgelistet, verwenden Sie bitte die Schaltfläche Jetzt suchen. Innerhalb eines kurzen Zeitraums (<15s) sollte das Terminal in der Tabelle aufgeführt werden.

Wurde das Terminal erkannt, wird neben dem Terminal eine Schaltfläche mit der Beschriftung Bearbeiten... eingeblendet. Klicken Sie auf diese Schaltfläche, wird die Seite Verbindung zum Kartenterminal angezeigt.

Nach Klick auf die Schaltfläche Zuweisen wird das Kartenterminal dem Konnektor zugewiesen.

1. Nachdem das Terminal zugewiesen wurde, klicken Sie auf die Schaltfläche Pairen. In diesem Prozess wird Ihnen das Zertifikat des Terminals angezeigt. Sie müssen diesen Dialog bestätigen.
2. Im weiteren Verlauf müssen Sie den Vorgang des Pairings durch betätigen der OK-Taste des Terminals bestätigen. Achten Sie bitte auf die Ausgaben im Display des Terminals.

War das Pairing erfolgreich, wird das Terminal automatisch verbunden. In der Tabelle Kartenterminals wird jetzt das Terminal mit drei Häkchen angezeigt: Zugewiesen, Paired und Verbunden.

War das Zuweisen nicht erfolgreich, überprüfen Sie unter dem Link Liste der kompatiblen Geräte, ob dieses Kartenterminal überhaupt unterstützt wird.

Wenn Sie nach der Auswahl der Schaltfläche Bearbeiten… auf Entfernen klicken, wird das Kartenterminal aus der Tabelle Verbindung zum Kartenterminal entfernt.

Achtung: Es besteht die Möglichkeit, die Verbindung zwischen Konnektor und Terminal unter Verwendung der Administrationsoberfläche manuell zu trennen. Wenn die Verbindung getrennt wird, kann auf das Terminal nicht mehr zugegriffen werden, bis die Verbindung erneut manuell hergestellt wird.

5.3.3 Einrichten eines Arbeitsplatzes

1. Ausgehend vom Hauptmenü rufen Sie die Seite Zugriffsberechtigung auf.
2. Unter der Tabelle Clientsysteme legen Sie ein neues Clientsystem an, indem Sie die entsprechende ID angeben und auf Clientsystem hinzufügen klicken. Nach erfolgreichem Hinzufügen wird das Clientsystem in der Tabelle Clientsysteme angezeigt.
3. Unter der Tabelle Arbeitsplätze legen Sie einen neuen Arbeitsplatz an, indem Sie die entsprechende ID angeben und auf Schaltfläche Arbeitsplatz hinzufügen klicken. Nach erfolgreichem Hinzufügen wird der Arbeitsplatz in der Tabelle Arbeitsplätze angezeigt. Nach Betätigen der Schaltfläche Bearbeiten wird die Seite Arbeitsplatzrelationen angezeigt. Hier haben Sie die Möglichkeit im Abschnitt Zugeordnete Kartenterminals das vorher gepairte Terminal dem ausgewählten Arbeitsplatz mit Zuordnungstyp Lokal zuzuordnen (der Zuordnungstyp Entfernt wird in Kapitel 7.1.4 näher betrachtet).

4. Unter der Tabelle SMBs werden im Auswahlmenü verfügbare SMBs die ICCSN von allen SMC-Bs angezeigt, die in einem verbundenen Kartenterminal vorhanden sind. Bei Auswahl einer ICCSN und Betätigen der Schaltfläche SMB hinzufügen wird die ausgewählte SMB in die Verwaltung übernommen und in der Tabelle SMBs angezeigt. Zusätzlich muss noch die SMC-B einem Mandanten zugeordnet werden. Dies wird im folgenden Schritt beschrieben.
5. Unter der Tabelle Mandanten legen Sie einen neuen Mandanten an, indem Sie die entsprechende ID angeben und auf Schaltfläche Mandanten hinzufügen klicken. Nach erfolgreichem Hinzufügen wird der Mandant in der Tabelle Mandanten angezeigt. Nach Betätigen der Schaltfläche Bearbeiten wird die Seite Mandantenrelationen angezeigt. Hier weisen Sie den Mandanten Relationen in folgenden Tabellen zu:

- Zugeordnete Kartenterminals
- Zugeordnete SMBs
- Zugeordnete Arbeitsplätze
- Zugeordnete Clientsysteme
- Arbeitsplätze zugeordneter Clientsysteme
- Zugeordnete Kartenterminals für Remote-PIN-Zugriff (optional: wird in Kapitel 7.1.4 näher betrachtet)
- Zugeordneter VSDM-Encryptionkey: Klicken Sie hierfür zunächst auf die Schaltfläche Generieren und tippen im nächsten Schritt den generierten Schlüssel in das Feld Neuer Schlüssel. Schließen Sie die Eingabe ab, indem Sie auf Übernehmen klicken.

Für sämtliche Konfigurationsschritte verwenden Sie die Schaltfläche Zuordnung hinzufügen. Indem Sie in der Tabelle ausgewählter Mandant auf Übernehmen klicken, werden die Information aktualisiert und der Vorgang abgeschlossen.

Die Zuordnung der SMC-B an einen Mandanten ist zwingend erforderlich, um den Konnektor in der TI zu registrieren. (siehe Kapitel 4.11)

5.3.4 Vertrauensräume

Damit der Konnektor und ein Terminal erfolgreich eine Verbindung aufbauen können, müssen die genutzten Vertrauensräume aufeinander abgestimmt sein.

5.4 Dienstverzeichnisdienst

Der Dienstverzeichnisdienst ist auf der IP-Adresse des LAN-Adapters erreichbar:

1. http-basierter Zugriff (ohne TLS-Sicherung): Port 80
   Beispiel: http://<LAN-IP-Konnektor>/connector.sds
2. Zugriff mit TLS-Sicherung: Port 443
   Beispiel: https://<LAN-IP-Konnektor>/connector.sds

In der Standardkonfiguration verlangt der Konnektor eine TLS-gesicherte Verbindung und eine Authentisierung des Clientsystems mit Zertifikat. Die Einstellungen können ausgehend von Hauptmenü > Zugriffsberechtigung > Clientsysteme angepasst werden.

Tabelle 19 Authentifizierungseinstellungen für Dienstverzeichnisdienst

Einstellungen	
TLS erforderlich	Ist dieser Schalter auf An konfiguriert, werden nur TLS-gesicherte Verbindungen akzeptiert. Bitte beachten Sie den Hinweis zum Punkt Offener Dienstverzeichnisdienst.
Authentifizierung erforderlich	Ist dieser Schalter auf An konfiguriert, muss das Clientsystem eine Authentifizierung durchführen
Authentifizierungsmodus	Das Auswahlmenü konfiguriert die Art und Weise, mit der ein Clientsystem sich gegenüber dem Konnektor authentifiziert
Offener Dienstverzeichnisdienst	Mit diesem Schalter wird geregelt, ob unabhängig vom Schalter TLS erforderlich der Dienstverzeichnisdienst ohne TLS-Sicherung erreichbar ist.

Verwenden Sie die Schaltfläche Übernehmen, um die Konfiguration zu aktivieren.

5.5 Aktualisierung der Firmware

Bevor die neue Firmware installiert werden kann, muss die Zeiteinstellung des Konnektors manuell konfiguriert werden. Das Vorgehen ist im Abschnitt 5.3.1 beschrieben. Anschließend starten Sie den Konnektor bitte neu.

Der Konnektor darf während der Installation nicht vom Stromnetz getrennt werden. Der gesamte Vorgang der Aktualisierung der Konnektorsoftware kann bis zu 45 Minuten in Anspruch nehmen.

Unter Hauptmenü > Systeminformationen oder unter Hauptmenü > Update können sie sehen, welche Firmwareversion gerade installiert ist. Möchten Sie eine Aktualisierung vornehmen, gehen Sie wie folgt vor:

Eine Aktualisierung soll nur dann erfolgen, wenn ausreichend Informationen über den Inhalt des Softwareupdates bekannt sind und eine bewusste Entscheidung bei der Freischaltung möglich ist.

Eine Aktualisierung der installierten Firmware sollte nur dann erfolgen, wenn die neue Version die Behebung eines vorhandenen Problems anzeigt oder neue Funktionen bereitgestellt werden, die für den Einsatz des Konnektors unbedingt erforderlich sind.

1. Melden Sie sich als Administrator in der Managementoberfläche an.
2. Laden Sie unter Verwendung des Menüpunkts Hauptmenü > Update > Paket-Verwaltung > Update hochladen das Firmwarepaket zur Installation. Während dieses Vorgangs zeigt die Managementoberfläche einen Fortschrittsbalken an.
3. Anschließend gehen Sie zurück in die Update-Übersicht und wählen in der Zeile des Geräts die Schaltfläche Planen. Auf der folgenden Seite stellen Sie die Option Update planen auf An.
4. Sie können nun einstellen, wann das Update ausgeführt werden soll. Wählen Sie Sofort ausführen, um die Aktualisierung direkt im Anschluss durchzuführen. Sie können auch einen anderen Zeitpunkt einstellen, um die Aktualisierung zu einem von Ihnen

festgelegten Zeitpunkt ausführen zu lassen. Nach Ihrer Einstellung klicken Sie bitte auf die Schaltfläche Übernehmen.

5. Auf der Übersichtseite der Updates wählen Sie nun Plan ausführen. Der Update-Plan ist nun aktiv, sodass die Aktualisierung nun zu dem von Ihnen angegebenen Zeitpunkt ausgeführt wird. Sobald der Aktualisierungsvorgang startet, wird dies signalisiert, indem die Status LED des Konnektors orange blinkt.

Im Anschluss an die Aktualisierung wird der T-Systems Konnektor automatisch neu gestartet und Sie können mit Hilfe der Administrationsoberfläche erneut auf das Gerät zugreifen.

Wird zu einem späteren Zeitpunkt ein Firmware Update durch einen lokalen Administrator durchgeführt, ist die korrekte Zeit auf dem Konnektor zu überprüfen und gegebenenfalls zu aktualisieren. Weicht die Zeit erheblich von der korrekten Zeit ab, kann ein Firmwareupdate aufgrund dieser Abweichung fehlschlagen.

Bitte beachten Sie die Hinweise im Kapitel 7.10.1 sollte ein Firmware Update fehlschlagen.

6 Einstellungen des Netzkonnektors

Der folgende Abschnitt erläutert die Konfiguration des Netzkonnektors. Die Konfigurationsoptionen werden dabei in tabellarischer Form dargestellt. Sie finden in der grafischen Benutzerschnittstelle den jeweiligen Konfigurationsparameter in der Spalte Option. In der Spalte Erläuterung finden Sie Hinweise zu den vorzunehmenden Einstellungen.

6.1 Menüpunkt VPN-Client

Wichtiger Hinweis: Für einen sicheren Betrieb des Konnektors ist es zwingend notwendig, dass die beiden Einstellungen „TI Sequenznummer Auswertung“ und „SIS Sequenznummer Auswertung“ aktiviert werden. Hier muss jeweils der Wert „32“ eingetragen werden. Wenn diese Option abgeschaltet ist bzw. die beiden Werte auf „0“ eingestellt sind, dann wird das Gerät nicht mehr CC-konform betrieben.

Tabelle 20 Menüpunkt VPN-Client Übersicht

VPN-Status	
Verbindungsstatus zur TI	Hier wird mit folgenden Werten angezeigt, ob ein IPsec-Tunnel zur Telematik besteht: Getrennt und Tunnel-Aufbau blockiert - Dieser Wert wird angezeigt, wenn der Netzkonnektor als Offline-Konnektor betrieben wird, d.h. keine Verbindung zum Internet besteht. In diesem Falle besteht keine Möglichkeit, eine IPsec-gesicherte Verbindung aufzubauen. Getrennt - Es besteht kein aktiver Tunnel. Dies bedeutet, dass der Netzkonnektor genutzt werden kann, um einen IPsec-gesicherten Tunnel aufzubauen, eine aktive Verbindung jedoch nicht besteht. In diesem Falle können Sie die Schaltfläche Verbinden verwenden, um eine IPsec-gesicherte Verbindung herzustellen. Verbunden - Es besteht ein aktiver VPN-Tunnel zur TI. Sie können jetzt Dienste, die sich in der Telematikinfrastruktur befinden, verwenden. Wenn Sie die Verbindung trennen wollen, verwenden Sie die Schaltfläche Trennen.
Hinweis: Je nach Verbindungszustand kann die zugeordnete Schaltfläche folgende Optionen anbieten: ▪ Verbinden - Es besteht die Möglichkeit einen VPN-Tunnel aufzubauen, da der Netzkonnektor mit dem Internet verbunden ist. Dieser Status liefert jedoch keine Aussage darüber, ob die Verbindung tatsächlich hergestellt werden kann. Auftretende Fehler während des Versuchs, einen Tunnel aufzubauen, werden in der Oberfläche mit Hilfe einer Fehlermeldung angezeigt. Um einen VPN-Tunnel zu etablieren, muss auf diese Fehlermeldungen reagiert werden. ▪ Trennen - Es wurde ein Tunnel aufgebaut. Sie können mit Hilfe der Schaltfläche den Tunnel wieder abbauen. ▪ Verbinden [deaktiviert] - Wenn Sie mit dem Mauszeiger über die Schaltfläche navigieren, wird der Mauszeiger nicht in ein Handsymbol umgewandelt. Dieser Zustand wird eingenommen, wenn der Netzkonnektor als Offline-Konnektor arbeitet und der Aufbau eines VPN-Tunnels blockiert ist.	
Hinweis: Unterhalb der Einstellung für den Tunnel in die Telematikinfrastruktur haben Sie die Möglichkeit, eine Verbindung zum sicheren Internetservice herzustellen (abgekürzt mit SIS). Diese Möglichkeit können Sie nur dann in Anspruch nehmen, wenn ein Tunnel in die Telematikinfrastruktur aufgebaut wurde. Zudem benötigen Sie ggf. einen Vertrag mit Ihrem Zugangsanbieter, um den sicheren Internetservice zu nutzen.	

VPN-Status	
Hinweis zu möglichen Fehlerursachen: Wenn der Tunnel zur Telematik nicht aufgebaut werden kann, kommen verschiedene Ursachen in Betracht. Bitte prüfen Sie folgendes: ▪ Ist das Netzwerkkabel mit dem WAN-Adapter korrekt verbunden? ▪ Stimmt die Zeitsynchronisation des Netzkonnektors? Wenn Sie das Gerät ausgeschaltet haben und nach einem längeren Zeitraum wieder in Betrieb nehmen, kann die Uhrzeit verstellt sein. In diesem Falle kann der Netzkonnektor die Gültigkeit elektronischer Zertifikate (CRL und TSL) nicht korrekt prüfen und lehnt den Aufbau einer Verbindung in die Telematikinfrastruktur ab. ▪ Ist die Vertrauensliste aktuell? Der Netzkonnektor prüft das Zertifikat der Gegenseite gegen eine Liste vertrauenswürdiger Zertifikate (Vertrauensliste). Diese Liste hat ein Ablaufdatum. Wurde das Ablaufdatum überschritten, kann keine Verbindung in die Telematikinfrastruktur hergestellt werden. ▪ Ist die Sperrliste aktuell? Der Netzkonnektor prüft das Zertifikat der Gegenseite mit Hilfe einer Sperrliste. Ist die Sperrliste abgelaufen, kann keine Verbindung in die Telematikinfrastruktur hergestellt werden. ▪ Beachten Sie in jedem Falle auf der Oberfläche angezeigte Fehlermeldungen. Zusätzlich haben Sie die Möglichkeit, das Fehlerprotokoll des Konnektors zu sichten, um Hinweise auf Fehlerursachen zu entnehmen.	
Verbindungsstatus zum SIS	In diesem Feld wird angezeigt, ob ein IPsec-Tunnel zum sicheren Internetservice besteht. Die angezeigten Statuswerte sind identisch mit dem Verbindungsstatus zur TI-Plattform.

Tabelle 21 Menüpunkt VPN-Client Einstellungen

Einstellungen	
IKE Keep-Alive Modus	Wird diese Option aktiviert, wird die Verbindung zum Konzentrator dauerhaft gehalten.
IKE Keep-Alive Intervall	Mit Hilfe dieses Eingabefelds wird der Zeitwert in Sekunden zwischen dem Versand der Keep-Alive-Pakete konfiguriert. Der Wert muss zwischen 1 und 3600 liegen, Standard ist 30 Sekunden.
IKE Keep-Alive Wiederholungen	Diese Option kann verwendet werden, um die Anzahl der Wiederholungen für den Versand der Retry-Pakete zu spezifizieren. Der Wert muss zwischen 1 und 100 liegen, Standard ist 3.
IDLE Timeout Modus	Diese Option wird aktiviert, wenn nach einem Zeitraum mit Inaktivität die Verbindung abgebaut werden soll.
IDLE Timeout	Gibt den Inaktivitätszeitraum in Sekunden an, nach dem die Verbindung abgebaut wird. Der Wert muss zwischen 1 und 3600 liegen, Standard ist 600.
NAT Keep-Alive Modus	Diese Option wird aktiviert, wenn der NAT Keep Alive verwendet werden soll.
NAT Keep-Alive Intervall	Gibt die Zeitspanne an, nach der ein neues Keep-Alive-Paket gesendet wird. Der Wert muss zwischen 1 und 3600 liegen, Standard ist 20 Sekunden.
TI MTU	Gibt die Maximum Transfer Unit (maximale Paketgröße in Byte) für die Übertragung eines Datenpakets im Tunnel der Telematikinfrastruktur an. Der Wert muss zwischen 576 und 8076 liegen, Standard ist 1418.

SIS MTU	Gibt die Maximum Transfer Unit (maximale Paketgröße in Byte) für die Übertragung eines Datenpakets im Tunnel des sicheren Internetservice an. Der Wert muss zwischen 576 und 8076 liegen, Standard ist 1418.
TI Sequenznummer Auswertung	Die Größe des Fensters für die Auswertung der Sequenznummern. Der Wert **muss** auf "32" für den konformen Betrieb gestellt werden. (Der Wert kann zwischen 1 und 32 liegen, Standard ist 0.)
SIS Sequenznummer Auswertung	Die Größe des Fensters für die Auswertung der Sequenznummern. Der Wert **muss** auf "32" aktiviert für den konformen Betrieb gestellt werden. (Der Wert kann zwischen 1 und 32 liegen, Standard ist 0.)
Hash & URL	Mit dieser Option besteht die Möglichkeit, das Hash- & URL-Verfahren zu aktivieren. Der Wert muss zwischen 0 und 32 liegen, Standard ist 0.

.

6.2 Menüpunkt LAN und WAN

Die Einstellungsseite zu LAN und WAN ermöglicht die Konfiguration der betreffenden Adapter. Der T-Systems Konnektor beinhaltet zwei physische Schnittstellen mit der Bezeichnung LAN (interne Bezeichnung eth0) und WAN (interne Bezeichnung eth1). Die Schnittstelle mit der Bezeichnung eth0 wird mit Ihrem Netzwerk (dem LAN) und die Schnittstelle mit der Bezeichnung eth1 mit dem Weitverkehrsnetz (WAN) verbunden.

Bei eingeschaltetem DHCP (dynamische Konfiguration) sind die Felder IP-Adresse und Subnetzmaske inaktiv. Nur bei ausgeschalteten DHCP können die IP-Adresse und Subnetzmaske manuell vom Administrator gesetzt werden (statische Konfiguration).

Tabelle 22 LAN-Einstellungen

LAN	
Aktueller Status	Zeigt den aktuellen Status des Adapters (aktiv / inaktiv), die eingestellte Konfiguration sowie die aktuell zugewiesene IP-Adresse und Subnetzmaske am LAN-Adapter des T-Systems Konnektors an. Außerdem kann hier über die Schaltfläche DHCP-Lease erneuern der DHCP-Lease für die LAN-Netzwerkschnittstelle erneuert werden. Die Erneuerung des DHCP-Lease kann nur bei abgebautem TI-Tunnel durchgeführt werden, andernfalls wird eine Fehlermeldung angezeigt, dass zuerst die VPN-Verbindungen getrennt werden müssen.
DHCP	Mit Hilfe dieser Schaltfläche kann eingestellt werden, ob die Adresszuweisung am LAN-Adapter unter Verwendung des DHCP-Protokolls erfolgen soll. Mit Aktivierung dieser Option wird der DHCP-Client aktiviert. Zudem kann bei Aktivierung ein neues Lease mit der Schaltfläche DHCP-Lease erneuern bezogen werden.
IP-Adresse	Die IP-Adresse des LAN-Adapters. Ist der DHCP-Client des LAN-Adapter aktiviert, wird in diesem Feld die mit den DHCP-Lease zugewiesene IP-Adresse angezeigt. Sofern der DHCP-Client deaktiviert ist, kann in diesem Feld eine statische IP-Adresse vorgegeben werden.

Subnetzmaske	Die Subnetzmaske des LAN-Adapters. Bei aktiviertem DHCP-Client wird die zugewiesene Subnetzmaske angezeigt, bei deaktiviertem DHCP-Client kann dieses Feld zur Zuweisung einer Subnetzmaske genutzt werden.
IP-Paketlänge	Dieses Feld nimmt einen numerischen Wert auf und ermöglicht die Konfiguration der sogenannten MTU, der Maximum Transfer Unit. Damit wird die Größe eines IP-Pakets in Byte angegeben. Der Wert muss zwischen 576 und 9000 liegen.

Tabelle 23 WAN-Einstellungen

WAN	
Aktueller Status	Zeigt den aktuellen Status des Adapters (aktiv / inaktiv), die eingestellte Konfiguration sowie die aktuell zugewiesene IP-Adresse und Subnetzmaske am WAN-Adapter des T-Systems Konnektors an. Außerdem kann hier über die Schaltfläche DHCP-Lease erneuern der DHCP-Lease für die WAN-Netzwerkschnittstelle erneuert werden. Die Erneuerung des DHCP-Lease kann nur bei abgebautem TI-Tunnel durchgeführt werden, andernfalls wird eine Fehlermeldung angezeigt, dass zuerst die VPN-Verbindungen getrennt werden müssen.
WAN-Adapter	Über dieses Element wird angezeigt, ob der WAN-Adapter aktiviert ist. Zudem kann über den Schalter der WAN-Adapter ein- und ausgeschaltet werden. Bitte beachten: Der WAN-Adapter kann nur im Modus InReihe und Online aktiviert sein. Die Standardeinstellung ist InReihe.
DHCP	Mit Hilfe dieses Schalters kann eingestellt werden, ob die Adresszuweisung am WAN-Adapter unter Verwendung des DHCP-Protokolls erfolgen soll. Mit Aktivierung dieser Option wird der DHCP-Client aktiviert. Zudem kann bei Aktivierung ein neues Lease mit der Schaltfläche DHCP-Lease erneuern bezogen werden.
IP-Adresse	Die IP-Adresse des WAN-Adapters. Ist der DHCP-Client des WAN-Adapters aktiviert, wird in diesem Feld die mit den DHCP-Lease zugewiesene Adresse angezeigt. Sofern der DHCP-Client deaktiviert ist, kann in diesem Feld eine statische IP-Adresse vorgegeben werden.
Subnetzmaske	Die Subnetzmaske des WAN-Adapters. Bei aktiviertem DHCP-Client wird die zugewiesene Subnetzmaske angezeigt, bei deaktiviertem DHCP-Client kann dieses Feld zur Zuweisung einer Subnetzmaske genutzt werden.
IP-Paketlänge	Dieses Feld nimmt einen numerischen Wert auf und ermöglicht die Konfiguration der sogenannten MTU, der Maximum Transfer Unit. Damit wird die Größe eines IP-Pakets in Byte angegeben. Der Wert muss zwischen 576 und 9000 liegen.
Internet-Modus	Mit diesem Element wird angezeigt, in welcher Art und Weise der Netzkonnektor eine Verbindung mit dem Internet herstellt. Zudem kann dieses Element verwendet werden, um die Art und Weise des Internetzugriffs zu konfigurieren - der Standardwert ist SIS. Die folgenden Werte können eingestellt werden: ▪ SIS - Zugriff über den sicheren Internetzugang ▪ IAG - Zugriff über den Internetprovider ▪ Keiner - Der Konnektor soll nicht auf das Internet zugreifen

Tabelle 24 Allgemeine Verbindungseinstellungen

Allgemein	
Aktuelle IAG	Aktuelle IP-Adresse des Gateways
IAG-Adresse	IP-Adresse des Gateways. Sobald der DHCP-Server eine IAG-Adresse liefert, wird diese verwendet statt der vorher konfigurierten. Die IAG-Adresse ist immer erforderlich, wenn der Netzkonnektor eine statische Konfiguration verwendet (kein DHCP). Sollte der DHCP-Server kein Gateway im DHCP-Lease mitsenden, wird die manuell hinterlegte IAG verwendet. ▪ InReihe ▪ Parallel Der Modus InReihe muss eingestellt werden, wenn über den WAN-Adapter des Konnektors der ausgehende Datenverkehr z.B. in das Netz der Telematik gehandhabt werden soll. Dies bedeutet, dass das Netz des Leistungserbringers (das Netzwerk der Praxis) mit dem LAN-Anschluss verbunden ist und der WAN-Adapter beispielsweise mit einem vorhandenen DSL-Router. Der Modus Parallel muss eingestellt werden, wenn der Konnektor ausschließlich über die LAN-Schnittstelle in das bestehende Netzwerk eingebunden werden soll. In diesem Falle kommuniziert der Netzkonnektor mit dem Netz des Leistungserbringers und mit der Telematikinfrastruktur über die gleiche physische Schnittstelle. Wie bereits im Kapitel 3.4.1beschrieben ist im Modus Parallel ist kein Internetzugriff über den sicheren SIS-Zugang möglich. Die Internetverbindung muss also selbstständig abgesichert werden. Die Einstellung des Modus Parallel erfolgt durch die Deaktivierung des WAN-Adapters. Wenn der WAN-Adapter wieder aktiviert wird, dann befindet sich der Konnektor im Modus InReihe.
Intranet-Routen-Modus	Diese Option erlaubt die Konfiguration des Intranet-Routen Modus. Die folgenden Werte sind möglich: ▪ Redirect ▪ Block Der Konfigurationswert Redirect gibt an, dass IP-Pakete innerhalb des Netzes des Leistungserbringers durch den Netzkonnektor geroutet werden sollen. Diese Option sollte nur dann aktiviert werden, wenn durch den Administrator Intranet-Routen definiert wurde. Der Konfigurationswert Block kann eingestellt werden, wenn sämtlicher IP-Verkehr zwischen Intranet-Segmenten durch den Netzkonnektor geblockt werden sollen. In beiden Fällen müssen die IP-Pakete an den Netzkonnektor gerichtet sein, damit diese Werte wirksam werden.
Service-Timeout	Zeitspanne (in Sekunden), in der eine Anfrage beantwortet werden muss, bevor ein Timeout gemeldet wird. Standard ist 0.
Übertragungsrate	Hier wird die maximale Übertragungsrate für den ausgehenden Datenverkehr in KB/s angezeigt. Der Wert muss zwischen 100 und 2147483647 liegen.

Um eine Änderung an den Einstellungen wirksam werden zu lassen, verwenden Sie den Button Übernehmen.

6.3 Menüpunkt Routing

Die Einstellungsseite zu Routing ermöglicht die Einsichtnahme in die aktuell vorhandenen Routen und bietet die Möglichkeit neue IP-Adressen hinzuzufügen.

Tabelle 25 Routing-Einstellungen

Routing-Informationen	
Routen	In dieser Übersicht werden vorhandene Routen angezeigt. Diese Tabelle dient ausschließlich der Einsichtnahme. Zu einer Route werden die folgenden Informationen angezeigt: 1. Destination/Subnetmask - Zieladresse der Route 2. Gateway - Die eingestellte Gateway-Adresse 3. Flags - Der jeweiligen Route zugeordnete Flags. Diese Flags können die folgenden Werte annehmen. a) U - Die Route ist etabliert b) G - Die Route führt zu einem Gateway. Ist dieses Flag nicht gesetzt, führt diese Route direkt zu einem Endpunkt c) H - Dieses Flag bedeutet, dass die Route zu einem Host führt d) D - Dieses Flag zeigt an, dass die Route durch eine Umleitung zustande gekommen ist e) M - Dieses Flag zeigt an, dass die Route durch eine Umleitung modifiziert wurde 4. Metric - Hier wird die Gewichtung der Route angezeigt. Diese ist immer auf 0. 5. Type - Dieser Wert kennzeichnet den Typ der Route. Der Type ist static, das bedeutet, nur die konfigurierten Routen werden erkannt. 6. Interface - Die zugeordnete physische Schnittstelle. eth1 meint dabei den für das WAN vorgesehenen Adapter, eth0 den für das LAN vorgesehen Adapter. 7. Protocol - Dieser Wert kennzeichnet das Netzwerkprotokoll

Tabelle 26 Intranet-Einstellungen

Intranet	
Intranet-Routen	In dieser Übersicht werden Informationen zu konfigurierten Intranet-Routen angezeigt. In Verbindung mit den gleichlautenden Eingabefeldern ist es möglich, eine neue Route anzulegen. Zudem können manuell hinzugefügte Routen unter Verwendung der betreffenden Schaltfläche Entfernen wieder gelöscht werden. Standardmäßig sind keine Intranet-Routen konfiguriert.
IP des Netzwerksegments	Die IP-Adresse des betreffenden Netzwerksegments, zu dem die Route gelegt werden soll.
Subnetzmaske des Segments	Die Subnetzmaske des Segments, zu dem die Route gelegt werden soll.
Next-Hop	Die IP-Adresse des sog. Next-Hop auf dem Weg zu der angegebenen IP-Adresse des Zielsegments.

6.4 Menüpunkt Firewall

Die Einstellungsseite Firewall ermöglicht die Einsichtnahme und Einstellung der benutzerdefinierten Firewallregeln für den SIS-Tunnel.

Tabelle 27 Firewallregeln

Firewallregeln	
Regeln	In dieser Übersicht werden die benutzerdefinierten Firewallregeln verwaltet. Die in Abschnitt 3.5.4 beschriebenen Firewallregeln sind fest im Netzkonnektor hinterlegt. Sie können nicht geändert werden und werden hier nicht dargestellt. 1. Quell-Netz - Die IP-Adresse des Ursprungsnetzes eines Pakets. Die Notation erfolgt in der Schreibweise IP-Adresse/Subnetzmaske. 2. Ziel-Netz - Die IP-Adresse des Zielnetzes eines Pakets. Die Notation erfolgt in der Schreibweise IP-Adresse/Subnetzmaske. 3. Protokoll - Das Protokoll, auf welches die Filterregeln angewandt werden. Es kann die Auswahl zwischen den Protokollen UDP und TCP getroffen werden. 4. Port - Der Port (Quell-Port oder Ziel-Port), für den die Filterregel zutrifft. Der Port muss als numerischer Wert angegeben werden. Entweder Quell-Port oder Ziel-Port muss definiert werden. Um eine Regel zu löschen wird der „LÖSCH“ Button wird neben dem jeweiligen Eintrag der Regeltabelle angezeigt.

6.5 Menüpunkt Infrastruktur

Die Seite Infrastruktur ermöglicht die Einsichtnahme in die vorhandenen Netzsegmente und die Bestandsnetze. Die Bestandsnetze werden hier verwaltet, d.h. Sie haben die Möglichkeit, die Netze zu aktivieren bzw. zu deaktivieren.

6.6 Menüpunkt Namensdienst

Die Einstellungsseite zu Namensdienst und DNS-Einstellungen ermöglicht Einstellungen und Einsichtnahme in die aktuelle Konfiguration.

Tabelle 28 DNS-Server im Leistungserbringernetz

DNS-Server im Leistungserbringer-Netz	
Server	In diesem Feld werden die konfigurierten DNS-Server im Netz der Leistungserbringer angezeigt.
Neuer Server	Mit Hilfe dieses Feldes kann ein neuer DNS-Server in die Konfiguration aufgenommen werden.

Tabelle 29 DNS-Server im öffentlichen Netz

DNS-Server im öffentlichen Netz	
Dynamische Adressen	Wenn der Netzkonnektor WAN-seitig eine dynamische IP-Adresse besitzt (DHCP-Client am WAN aktiv), werden in diesem Bereich dynamische DNS-Server-Adressen angezeigt. Mit der Schaltfläche Verwendung DHCP DNS ausschalten können Sie die automatische Ermittlung der DNS-Server-Adressen ausschalten und eigene DNS-Server eintragen.
Server	In diesem Feld werden die konfigurierten DNS-Server im öffentlichen Netz (Internet) angezeigt.
Neuer Server	Mit Hilfe dieses Feldes kann ein neuer DNS-Server in die Konfiguration aufgenommen werden.

Tabelle 30 DNS-Server im Netz des SIS

DNS-Server im Netz der SIS	
Server	In diesem Feld werden die konfigurierten DNS-Server im Netz des SIS angezeigt.

Tabelle 31 DNS-Server im Bestandsnetz

DNS-Server im Bestandsnetz	
Server	In diesem Feld werden die konfigurierten DNS-Server im Netz der SIS angezeigt.

Um einen DNS Eintrag zu löschen wird im Hauptmenü – Namensdienst der „LÖSCH“ Button neben dem jeweiligen Eintrag der DNS Servertabelle angezeigt.

Tabelle 32 DNS-Server im Netz der TI

DNS-Server im Netz der TI	
Server	In diesem Feld werden die konfigurierten DNS-Server im Netz der TI angezeigt.

Tabelle 33 Anzeige aktiver Bestandsnetze

Bestandsnetze	
Aktive Bestandsnetze	In diesem Feld werden die aktiven Bestandsnetze angezeigt.

Tabelle 34 Namensdienst-Einstellungen

Einstellungen	
Top Level Domain der TI	Zeigt die Top-Level-Domäne der Telematikinfrastruktur an

Service Discovery Domainname	Der Name der DNS-Domäne zur Ermittlung der VPN-Konzentratoren des VPN-Zugangsdienstes. Für den Domainnamen selbst dürfen nur alphanumerische Werte und der Unterstrich verwendet werden.
Leistungserbringer Domainname	Der Name der DNS-Domäne der Arztpraxis oder des Krankenhauses. Für den Domainnamen selbst dürfen nur alphanumerische Werte und der Unterstrich verwendet werden.
DNS-Root-Anker URL	Gibt die URL des DNS-Root-Ankers an. Dieser Eintrag wird beim automatischen Update des DNS-Root-Ankers benötigt.
Root Anker Status	Zeigt an, ob der DNS-Root-Anker initialisiert ist.
Eigenen Downloadpunkt verwenden	Mit dieser Option kann eigener DNS-Root-Anker definiert werden. Wenn diese Option eingeschaltet ist, wird darunter ein zusätzliches Eingabefeld Eigene DNS Root Anker URL angezeigt. Hier haben Sie die Möglichkeit eine URL einzutragen und mit der Schaltfläche Übernehmen zu bestätigen.

Tabelle 35 Domain Erreichbarkeitsprüfung

Erreichbarkeit des Servers prüfen	
Domainname	In diesem Feld kann die Erreichbarkeit einer Domäne geprüft werden. Tragen Sie dazu entweder den Domänen-Namen (z.B. gematik.de) oder eine IP-Adresse in der Punkt-Notation ein und verwenden Sie die Schaltfläche, um die Erreichbarkeit der eingegebenen Domäne oder IP-Adresse zu prüfen.

6.7 Menüpunkt DHCP-Server

Tabelle 36 DHCP-Server-Status

Aktueller Status	
DHCP-Server	In diesem Feld werden die aktiven Bestandsnetze angezeigt.

Tabelle 37 DHCP-Server-Einstellungen

Einstellungen	
DHCP-Server	Hier kann festgelegt werden, ob der Netzkonnektor als DHCP-Server fungiert oder nicht. Der Standardwert ist Aus. Wird der Wert auf An geändert, werden die Felder Netzwerk, Broadcast-Adresse, Erste IP-Adresse des Adress-Pools und Letzte IP-Adresse des Adress-Pools aktiv.
Netzwerk	Dieses Feld kann verwendet werden, um dem DHCP-Server eine spezifische Adresse im Netzwerk zuzuweisen. Nur sichtbar, wenn DHCP-Server aktiviert.
Broadcast-Adresse	Dieses Feld kann verwendet werden, um dem DHCP-Server eine spezifische Broadcast-Adresse zuzuweisen. Nur sichtbar, wenn DHCP-Server aktiviert.

Erste IP-Adresse des Adress-Pools	Dieses Feld kann genutzt werden, um die Start-IP-Adresse des statischen bzw. dynamischen Adress-Pools zu konfigurieren. Wurde bereits ein Wert eingestellt, so wird der zugehörige Eintrag in der Oberfläche angezeigt.
Letzte IP-Adresse des Adress-Pools	Dieses Feld kann genutzt werden, um die End-IP-Adresse des statischen bzw. dynamischen Adress-Pools zu konfigurieren. Wurde bereits ein Wert eingestellt, so wird der zugehörige Eintrag in der Oberfläche angezeigt.

Tabelle 38 DHCP-Clientgruppen

DHCP-Clientgruppen	
Clientgruppen	Diese tabellarische Übersicht zeigt die konfigurierten DHCP-Clientgruppen an. Klickt man auf Bearbeiten, öffnet sich ein neues Fenster (siehe folgende Tabelle 39 DHCP-Clientgruppen-Einstellungen)
Domainname	Dieses Feld ermöglicht die Konfiguration des Domainnamens der neu anzulegenden DHCP-Client Gruppe.

Unter Verwendung der Schaltfläche Gruppe Hinzufügen kann die neue DHCP-Clientgruppe in die Konfiguration des Netzkonnektors übernommen werden. Die Auflistung der DHCP-Clientgruppen wird in der tabellarischen Auflistung Clientgruppen angezeigt und kann bei bestehenden DHCP-Clientgruppen unter Verwendung der Schaltfläche Ändern angepasst werden. Um einen DHCP Eintrag zu löschen wird im Hauptmenü – DHCP-Server der „LÖSCH“ Button neben dem jeweiligen Eintrag der DHCP Servertabelle angezeigt

Tabelle 39 DHCP-Clientgruppen-Einstellungen

Einstellungen	
Name	Dieses Feld zeigt den Namen der DHCP-Clientgruppe an.
NTP-Server-Adresse senden	Wird der Wert auf An geändert, wird die Adresse des Konnektor-internen NTP-Servers per DHCP an die Clients gesendet.
Eigene DNS-Server verwenden	Wird der Wert auf An geändert, müssen Sie DNS-Server in die entsprechende Tabelle eingeben.
Eigenes Gateway verwenden	Wird der Wert auf An geändert, müssen Sie ein Standard-Gateway für die Gruppe definieren.
Netzmaske	Dieses Feld kann genutzt werden um der Gruppe, die neu hinzugefügt wird, eine Netzmaske zuzuweisen. Ein Beispiel für eine Netzmaske ist 255.255.255.0.
Domainname	Dieses Feld kann verwendet werden um die Clientgruppe zu benennen.

Tabelle 40 DNS-Server für DHCP-Clientgruppen

DNS-Server	
Server	Falls der Konnektor-eigene DNS-Server nicht genutzt wird, werden die hier aufgeführten Server verwendet.
Neue Adresse	Dieses Feld weist dem DNS-Server, der neu hinzugefügt wird, eine IP-Adresse zu.

Tabelle 41 Intranet-Routen für DHCP-Clientgruppen

Intranet-Routen verwenden	
Intranet-Routen	Hier können die Intranet-Routen ausgewählt werden, die in dieser Clientgruppe verwendet werden sollen. Die Intranet-Routen werden auf der Seite Routing im Abschnitt Intranet verwaltet.

Tabelle 42 Bestandsnetz für DHCP-Clientgruppen

Bestandsnetze verwenden	
Bestandsnetz	Hier können Netze gewählt werden, die in dieser Client-Gruppe verwendet werden sollen. Die Bestandsnetze werden auf der Seite Infrastruktur im Abschnitt Bestandsnetze verwaltet. Nur aktivierte Bestandsnetze können auch in der DHCP-Clientgruppe verwendet werden.

Tabelle 43 DHCP-Routing-Einstellungen

DHCP-Routing	
Routen	Dieses Feld zeigt die Routen an, die neu hinzugefügt werden.
IP-Adresse	Dieses Feld kann genutzt werden, um der Route, die neu hinzugefügt wird, eine IP-Adresse zuzuweisen.
Subnetzmaske	Dieses Feld kann genutzt werden, um der Route, die neu hinzugefügt wird, eine Subnetzmaske zuzuweisen. Ein Beispiel für eine Subnetzmaske ist 255.255.255.0.
Next-Hop	Dieses Feld kann genutzt werden, um der Route, die neu hinzugefügt wird, einen Next-Hop zuzuweisen.

6.8 Menüpunkt Datum und Uhrzeit

In diesem Kapitel werden die aktuellen Einstellungen des Netzkonnektors hinsichtlich Datum und Uhrzeit dargestellt. Bitte beachten Sie dabei, dass die korrekte Konfiguration des Datums und der Uhrzeit unabdingbar für die fehlerfreie Funktion des Konnektors ist. Wenn Sie den Konnektor als Offline-Konnektor betreiben, sind Sie dafür verantwortlich, Datum und Uhrzeit korrekt zu konfigurieren.

Tabelle 44 Zeitzone

Zeitzone
Mit diesem Element können Sie die vom Konnektor verwendete Zeitzone umstellen. Als Standard ist die mitteleuropäische Zeit einstellt (CET). Im Falle einer Synchronisation mit dem Netz der Telematikinfrastruktur wird die Zeitzone automatisch konfiguriert. Die Verwendung einer neu eingestellten Zeitzone wird über Übernehmen bestätigt.

Die Einstellungen im Bereich Datum und Uhrzeit können genutzt werden, um die Vorgaben vom Zeitserver (NTP) im Netz der Telematik zu überschreiben oder Zeit und Datum im Falle der Offline-Verwendung des Konnektors manuell zu konfigurieren. Nehmen Sie keine manuellen Änderungen an den Einstellungen vor, sofern Sie den Konnektor als Online-Konnektor verwenden (also den VPN-Tunnel in das Netz der Telematik nutzen).

Falls es dennoch erforderlich ist Zeit und Datum manuell einzustellen, beachten sie, dass die automatische Zeitsynchronisierung zunächst über NTP-Client ausschalten abgeschaltet werden muss.

Tabelle 45 Manuelle Einstellung für Datum und Zeit

Datum und Uhrzeit	
Datum	Dieses Feld erlaubt die Konfiguration der aktuellen Datumseinstellungen des Konnektors. Geben Sie das Datum bitte in der Schreibweise TT:MM: JJJJ an. Diese Einstellung wird im Falle einer Synchronisation mit der Telematikinfrastruktur automatisch konfiguriert.
Uhrzeit	Mit Hilfe dieses Feldes wird die Uhrzeit des Konnektors eingestellt. Geben Sie die Uhrzeit bitte in der Schreibweise HH:MM: SS an. Diese Einstellung wird im Falle einer Synchronisation mit dem Netz der Telematik automatisch konfiguriert.
Zeit setzen	Diese Schaltfläche ist nur aktiv, wenn die automatische Zeitsynchronisierung abgeschaltet ist. Verwenden Sie diese nach einer manuellen Änderung der Datums- und Zeitkonfiguration, um diese Änderungen wirksam werden zu lassen.
Zeit abrufen	Diese Schaltfläche ist nur aktiv, wenn die automatische Zeitsynchronisierung abgeschaltet ist. Verwenden Sie diese, um einmalig die aktuelle Zeit vom Zeitserver abzurufen und als Systemzeit zu setzen.

Im Bereich Informationen werden Angaben zur NTP-Synchronisation des Konnektors angezeigt.

Tabelle 46 Informationen zu NTP-Einstellungen

Informationen	
Primäre Adresse	Dieses Feld zeigt die IP-Adresse des primären NTP-Servers in der Telematik an.
Sekundäre Adresse	Dieses Feld zeigt die IP-Adresse des sekundären NTP-Servers in der Telematik an.

Warnungszeitraum	Nach Ablauf dieses Zeitraums wird eine Warnung über nicht erfolgte NTP Synchronisationen an das Primärsystem versandt. Ist der Wert beispielsweise auf 30 Tage eingestellt, so wird nach einer Frist von 30 Tagen (d.h. es konnte 30 Tage lang keine Zeitsynchronisation vorgenommen werden) eine Warnung an das Primärsystem versandt.
Fehlerzeitraum	Gibt die Anzahl der Tage an, nach denen der Konnektor in einen kritischen Betriebszustand wechselt. Ausgehend vom kritischen Betriebszustand erlaubt der Konnektor nur noch bestimmte Aktionen und stellt nicht mehr die volle Funktionalität zur Verfügung.
Maximale Zeitabweichung	Dieser Wert gibt die maximale Zeitabweichung an, die vom Konnektor zum Zeitpunkt der Synchronisation akzeptiert wird.

7 Einstellungen des Anwendungskonnektors

7.1 Allgemeine Informationen

Im nachfolgenden Abschnitt werden einleitende Informationen zur Administration des Anwendungskonnektors wiedergegeben.

7.1.1 Vergabe von Administrations-Accounts

Im Zuge der ersten Inbetriebnahme des T-Systems Konnektors muss ein neues Passwort erzeugt werden. Der Standard-Account des Konnektors im Auslieferungszustand lautet für den Benutzer admin und das Passwort konnektor. Im Zuge der ersten Inbetriebnahme müssen Sie die Account-Daten ändern. Dazu wird Ihnen der folgende Dialog angezeigt.

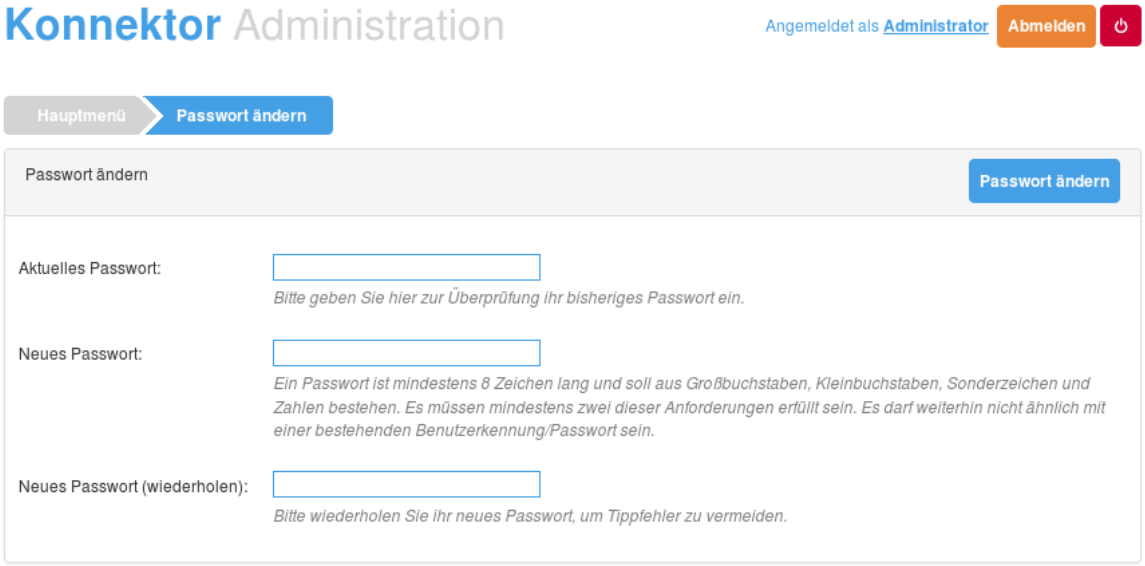


Abbildung 14 Änderung der Account-Daten

In diesem Dialog müssen Sie das bisherige Standardpasswort gegen ein neues Passwort mit den folgenden Anforderungen ersetzen:

1. Das Passwort ist mindestens 8 Zeichen lang
2. Das Passwort enthält kleine und / oder große Buchstaben
3. Das Passwort enthält mindestens eine Ziffer
4. Das Passwort enthält mindestens ein Sonderzeichen

Die Bezeichnung des Standard-Accounts (admin) bleibt in diesem Falle erhalten. Sie können zudem über die gleiche Seite neue Administrations-Accounts anlegen. Dazu ist die Seite Hauptmenü > Administratoren anzuwählen. Auf dieser Seite besteht die Möglichkeit, einen neuen Account entweder für die Rolle Administrator oder Superadministrator anzulegen. Beide Rollen unterscheiden sich dadurch, dass der Superadministrator über das Privileg verfügt, einen weiteren Administrations-Account anzulegen, während ein Account mit der Rolle

Administrator über dieses Recht nicht verfügt. Der angelegte Standard-Account ist vom Typ Superadministrator.

Warnung! Sollten Sie sich im Zuge der ersten Inbetriebnahme nicht mit dem oben genannten Standardpasswort anmelden können, so senden Sie den T-Systems Konnektor bitte unverzüglich an den Hersteller zurück. Es besteht die Wahrscheinlichkeit, dass es sich um einen potentiell gefälschten Konnektor handelt.

7.1.2 Aktualisierung des Vertrauensraums

Der Konnektor bietet Ihnen die Möglichkeit für ein manuelles Update des Vertrauensraums. Hierzu müssen Sie von der Webseite der gematik die Vertrauensliste (TSL) beziehen und diese in der Konnektorsoftware unter Zertifikate > Vertrauensraum über die Schaltfläche TSL hochladen installieren. Eine aktuelle Vertrauensliste wird benötigt, damit der Konnektor Verbindungen zur Telematikinfrastruktur aufbauen und Zertifikate der gematik korrekt prüfen kann.

Die Aktualisierung des Vertrauensraums ist eine notwendige Voraussetzung, um im Zuge der ersten Inbetriebnahme den Konnektor mit der Telematik zu verbinden. Schlägt der Aufbau der Verbindung fehl, so kann eine fehlende Aktualisierung die Ursache für dieses Verhalten sein. Falls der Verbindungsfehler durch eine abgelaufene CRL oder TSL auftritt, muss der Konnektor in den Offline-Modus geschaltet werden, um manuell eine Aktualisierung der TSL vornehmen zu können.

7.1.3 Aktualisierung der Sperrliste

Der Konnektor bietet die Möglichkeit zu einem manuellen Update der Sperrliste. In diesem Falle müssen Sie von der Seite Ihres Zugangsanbieters die betreffende Sperrliste herunterladen und im Konnektor unter Zertifikate > Vertrauensraum über die Schaltfläche CRL hochladen installieren. Eine aktuelle Sperrliste wird benötigt, damit der Konnektor Verbindungen zur Telematik aufbauen und die Zertifikate der gematik korrekt prüfen kann.

Die Aktualisierung der Sperrliste ist eine notwendige Voraussetzung, um im Zuge der ersten Inbetriebnahme den Konnektor mit der Telematik zu verbinden. Schlägt der Aufbau der Verbindung fehl, so kann eine fehlende Aktualisierung die Ursache für dieses Verhalten sein.

7.1.4 Remote-PIN-Verfahren

Damit ein HBA (Heilberufsausweis) nicht ständig durch seinen Inhaber mitgeführt werden muss oder die SMC-B (Security Module Card) nicht mehr unter ständiger Aufsicht eines Mitarbeiters der medizinischen Institution sein muss, empfiehlt es sich, das Remote-PIN-Verfahren im Konnektor einzustellen. Dabei wird der eigentliche HBA oder die SMC-B an einem sicheren Ort in ein entferntes Kartenterminal gesteckt. Der Karteninhaber greift über jeden konfigurierten Arbeitsplatz auf seine Karte zu. Die Remote-PIN-Eingabe erfolgt unter Verwendung des lokal am Arbeitsplatz vorhandenen Kartenterminals.

7.1.4.1 Voraussetzung

- 2 Terminals (1 x lokal, 1 x entfernt / zentral)

- 1 SMC-B / HBA, welcher freigeschaltet werden soll
- SMC-B / HBA muss in dem entfernten Kartenterminal gesteckt sein

7.1.4.2 Vorbereitung

1. Beide Terminals pairen. Siehe Kapitel 5.3.2.
2. Unter Zugriffsberechtigung > Mandant neuen Mandanten anlegen (wenn noch nicht vorhanden).
3. Unter Zugriffsberechtigung > Arbeitsplatz neuen Arbeitsplatz anlegen (wenn noch nicht vorhanden)
4. SMC-B (wenn vorhanden) zu Zugriffsberechtigung > SMB hinzufügen.
5. Unter Zugriffsberechtigung > Arbeitsplatz das Terminal mit eingesteckter Karte als entferntes Terminal zuordnen und das Terminal für die Remote-PIN-Eingabe als lokales Terminal zuordnen
6. Unter Zugriffsberechtigung > Schaltfläche Bearbeiten in Tabelle Mandant > Zugeordnete Kartenterminals Kartenterminals hinzufügen.
7. Unter Zugriffsberechtigung > Schaltfläche Bearbeiten in Tabelle Mandant > Zugeordnete SMBs die SMC-B (wenn verwendet) hinzufügen.
8. Unter Zugriffsberechtigung > Schaltfläche Bearbeiten in Tabelle Mandant > Zugeordnete Arbeitsplätze den zuvor angelegten Arbeitsplatz zuordnen.
9. Unter Zugriffsberechtigung > Schaltfläche Bearbeiten in Tabelle Mandant > Zugeordnete Kartenterminals für Remote-PIN-Zugriff das lokale Terminal zur PIN-Eingabe dem entsprechenden Arbeitsplatz zuordnen.

7.1.4.3 Aufruf Remote-PIN-Verfahren

Unter Karten > Infos den entsprechenden Mandanten auswählen und die gewünschte Operation Verifiziere PIN, Ändere PIN oder Entsperre PIN ausführen. Dies gilt nur für die SMC-B.

Ein HBA kann nur mit einem Soap[4]-Call über VerifyPin, ChangePin oder UnblockPin aufgerufen werden.

[4] Netzwerkprotokoll zum Austausch von Daten

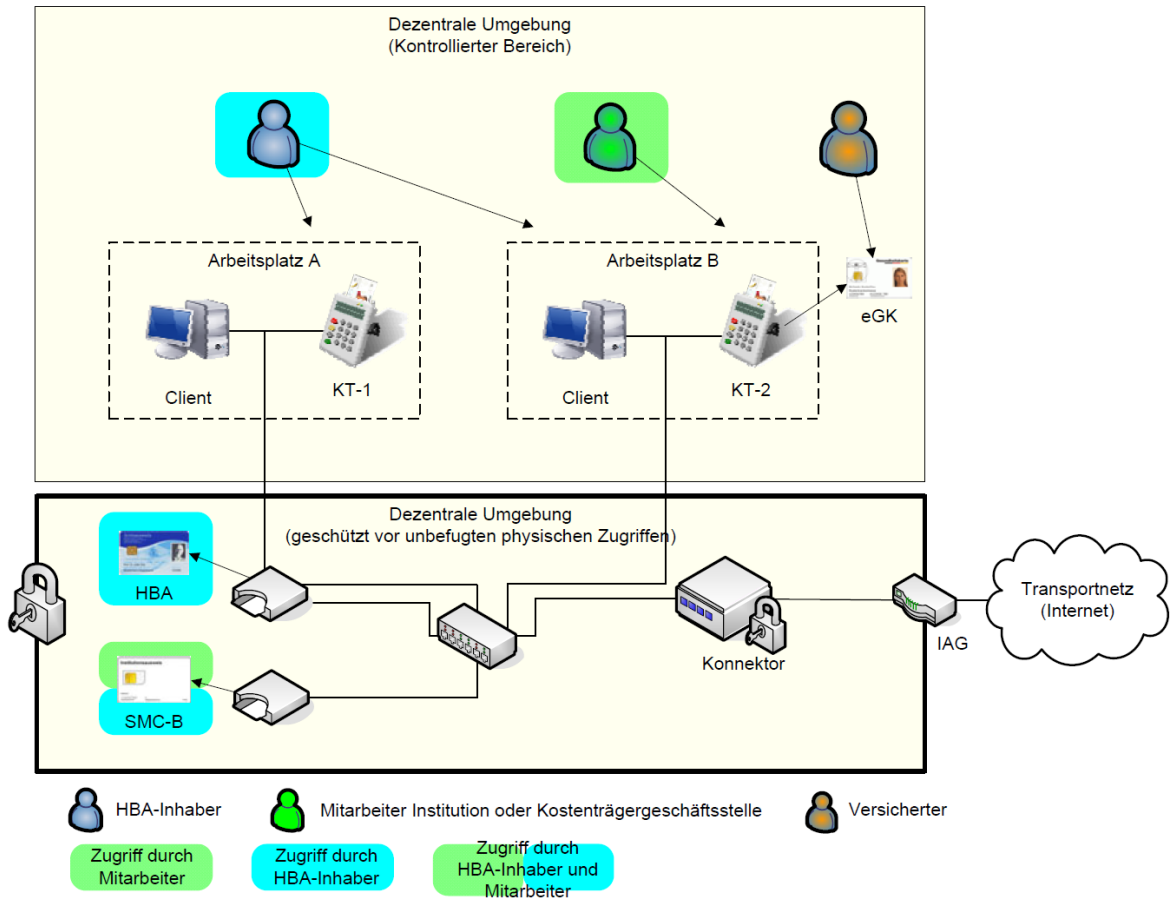


Abbildung 15 Szenario Remote-PIN-Verfahren aus gemSpec_KON_V4.11.1, S.504

7.2 Menüpunkt Administratoren

Der Menüpunkt Administratoren bietet die Möglichkeit zur Erstellung neuer Benutzeraccounts sowie zur Konfiguration des eigenen oder anderer administrativer Accounts. Beachten Sie auch die Erläuterungen im Abschnitt 7.1.1.

Tabelle 47 Verfügbare Administratoren

Verfügbare Administratoren	
Verfügbare Konten	In der tabellarischen Aufstellung werden die bestehenden administrativen Accounts angezeigt. Darüber hinaus besteht die Möglichkeit, einen weiteren Administrationsaccount anzulegen oder den eigenen Administrationsaccount zu modifizieren.

Tabelle 48 Account bearbeiten

Bearbeitung des Accounts	
Nach Auswahl der Schaltfläche Bearbeiten in der Tabelle, erscheint ein Dialog, in dem die Einstellungen angepasst werden können.	
Login-Name	Der Login-Name des Accounts. Nicht konfigurierbar.
Anzeigename	Der angezeigte Name des Administrators
E-Mail	E-Mail-Adresse des Administrators (optional)
Raum / Adresse	Der Raum oder die Adresse des Administrators (optional)
Passwort	Das Passwort zur Anmeldung am Anwendungskonnektor
Passwort (wiederholen)	Passwort-Wiederholung
Rolle	Die dem Account zugewiesene Rolle, nur für Superadministratoren änderbar.
Berechtigungen	Berechtigungstabelle des Administrators. Die Berechtigungen eines Superadministrators können nicht bearbeitet werden.

Tabelle 49 Berechtigungen einstellen

Berechtigungen eines Administrator-Kontos
Ein Superadministrator des Anwendungskonnektors kann ein administratives Konto hinsichtlich der Konfigurationsberechtigungen einschränken. Standardmäßig werden einem administrativen Konto alle Berechtigungen gegeben außer der Benutzerverwaltung. Die folgenden Berechtigungen können konfiguriert werden:

Tabelle 50 Rechtevergabe

Rechtevergabe und mögliche Einschränkungen	
Zurücksetzen auf Werkeinstellungen	Dem Administrator wird erlaubt, die vorhandene Konfiguration auf die Werkeinstellungen zurückzusetzen.
Ändern der VPN-Einstellungen	Dem Administrator wird erlaubt, die vorhandenen VPN-Einstellungen zu konfigurieren.
Ändern der LAN- / WAN-Einstellungen	Der Administrator hat die Möglichkeit, die LAN- / WAN-Einstellungen des Konnektors zu verändern. Siehe dazu Abschnitt 6.2. Ändern der DHCP-Server Einstellungen
Ändern von Datum / Uhrzeit	Erlaubt dem Administrator, die vorhandenen Datums-/ Zeiteinstellungen zu konfigurieren.
Ändern der Zugriffsberechtigungen	Erlaubt dem Administrator, die vorhandenen Zugriffsberechtigungen-Einstellungen zu konfigurieren.

Rechtevergabe und mögliche Einschränkungen	
Ändern der Clientsystem-Einstellungen	Erlaubt dem Administrator, die vorhandenen Clientsystem-Einstellungen zu konfigurieren. Das ist also ein Spezialfall der Zugriffsberechtigungen, man kann Zugriffsberechtigungen haben aber keine Clientsystemberechtigung.
Ändern der Kartenterminal-Einstellungen	Erlaubt dem Administrator, die vorhandenen Kartenterminal-Einstellungen zu konfigurieren.
Ändern der Leistungsumfänge	Erlaubt dem Administrator, die vorhandenen Leistungsumfänge-Einstellungen zu konfigurieren.
Ändern der Systeminformationen	Erlaubt dem Administrator, die vorhandenen Systeminformationen-Einstellungen zu konfigurieren.
Ändern der Signaturdienst-Einstellungen	Erlaubt dem Administrator, die vorhandenen Signaturdienst-Einstellungen zu konfigurieren.
Ändern der Zertifikats-Einstellungen	Erlaubt dem Administrator, die vorhandenen Zertifikats-Einstellungen zu konfigurieren.
Ändern der Konnektor-Einstellungen	Erlaubt dem Administrator, die folgenden Einstellungen zu konfigurieren: ▪ Neustart des Konnektors ▪ Registrieren ▪ Hostname ändern / anzeigen ▪ Einstellungen importieren, exportieren, Werksreset
Ändern der Protokollierungs-Einstellungen	Erlaubt dem Administrator, die vorhandenen Protokollierungs-Einstellungen zu konfigurieren.
Ändern der Remote-Management-Einstellungen	Erlaubt dem Administrator, die vorhandenen Remote-Management-Einstellungen zu konfigurieren. Es können alle Einträge aus der Tabelle „Berechtigungen“ geändert werden. Diese wird nur angezeigt, wenn der Button „Fernwartung zulassen“ aktiviert ist.
Ändern der Softwareaktualisierungs-Einstellungen	Erlaubt dem Administrator, die vorhandenen Update-Einstellungen zu konfigurieren.
Ändern der Namensdienst-Einstellungen	Erlaubt dem Administrator, die vorhandenen Namensdienst-Einstellungen zu konfigurieren.
Ändern der VSDM-Einstellungen	Erlaubt dem Administrator, die vorhandenen VSDM-Einstellungen zu konfigurieren.

Der Konnektor unterscheidet bei den Account-Typen zwischen Administrator und Superadministrator. Ein Superadministrator kann im Unterschied zu einem Administrator neue Accounts anlegen, verändern oder löschen. Zudem kann der Superadministrator die Berechtigungen für den jeweiligen Account anpassen.

7.2.1 Anlegen eines neuen Administrator-Kontos

Über die Schaltfläche Administrator-Konto hinzufügen unterhalb der Tabelle mit verfügbaren Konten können Sie ein neues Konto anlegen. Es öffnet sich ein neues Dialogfenster mit folgenden Konfigurationsmöglichkeiten:

Tabelle 51 Neues Administrator-Konto anlegen

Neues Administrator-Konto	
Login-Name	Der Anmelde-Name des neuen Administrators. Dieser Name muss sich von allen anderen Administratoren-Konten unterscheiden und wird für die korrekte Zuordnung der Anmeldung zum Konto benötigt.
Anzeigename	Der (reale) Name des Administrators
E-Mail	E-Mail-Adresse des Administrators (optional)
Raum / Adressen	Der Raum oder die Adresse des Administrators (optional)
Passwort	Das Passwort für die Anmeldung des Administrators am Konto. Dieses Passwort sollte nicht zu leicht zu erraten sein und sicher aufgehoben werden.
Passwort (wiederholen)	Die Eingabe des Passwortes muss wiederholt werden, damit Schreibfehler bei der Eingabe erkannt werden können.
Rolle	Die Rolle des Administrator-Kontos bestimmt den Zugriff auf den Konnektor: ein Superadministrator-Konto erlaubt einen vollständigen Zugriff. Ein Administrator-Konto hat eingeschränkten Zugriff auf das Gerät.
Berechtigungen	In dieser Tabelle werden einzelne Berechtigungen aufgelistet, die konfiguriert werden können (siehe Tabelle Berechtigungen eines Administrator-Kontos in Kapitel 7.2).

Nach Eingabe der Daten klicken Sie auf die Schaltfläche Übernehmen. Damit ist das neue Administratoren-Konto angelegt.

7.3 Menüpunkt Leistungsumfang

Mit Hilfe des Menüpunkts Leistungsumfang kann das Verhalten des Konnektors auf grundlegende Art und Weise geändert werden. So werden in diesem Bereich die Einstellungen vorgenommen, mit deren Hilfe festgelegt wird, ob der Konnektor als Online- oder Offline-Konnektor betrieben wird.

Tabelle 52 Einstellung des Betriebsmodus

Einstellungen	
Online	Ist diese Option aktiviert, dann wird der Konnektor im Online-Modus betrieben. Ist dieser Modus deaktiviert (OFFLINE), dann ist keine Kommunikation mit der Telematikinfrastruktur, d.h. keine VPN-Verbindungen, Registrierung, etc., möglich.
SAK	Diese Option muss aktiviert werden, wenn die im Konnektor integrierte Signaturanwendungskomponente (SAK) verwendet werden soll. Im gegenwärtigen Leistungsumfang des Konnektors ist die Signaturanwendungskomponente kein Bestandteil des angebotenen Leistungsumfangs.
Eigenständig	Dies bedeutet, dass der Konnektor ohne ein steuerndes Clientsystem ereignisgetrieben Fachanwendungen ausführt. Aus Fachsicht steht der Konnektor alleine, ohne Clientsysteme. Ein solcher alleinstehender Konnektor mit Zugang zur TI muss zur Durchführung der Fachanwendungen durch einen weiteren Konnektor unterstützt werden, der in direkter Verbindung zum Clientsystem steht, selbst aber keine Online-Anbindung besitzt.
Logisch getrennt	Mit dieser Option wird eine informationstechnische Trennung (Online-Bereich vs. Offline-Bereich im lokalen Netz des Leistungserbringers) durch eine logische Separation innerhalb eines Konnektors erreicht. In dieser Betriebsart ist demnach statt zwei Konnektoren (siehe Modus Eigenständig) nur ein Konnektor notwendig. Dieses Feature ist abgekündigt und soll nicht mehr verwendet werden.

7.4 Menüpunkt Zugriffsberechtigung

Die Zugriffsberechtigung definiert die erlaubten Zugriffsmöglichkeiten zu den externen Ressourcen (Kartenterminals und Kartenslots) sowie dem Client-Systemen (PVS). Um dies zu erreichen, muss der Administrator sicherstellen, dass diese Beziehungen korrekt konfiguriert sind.

Es liegt in der Verantwortung des LEI, bei Einrichtung der Verbindungen zum Primärsystem und der Zuordnung von KTs, Arbeitsplätzen, Karten, etc. gewissenhaft und fehlerfrei vorzugehen und nach der Konfiguration die hergestellten Verbindungen auf Ordnungsmäßigkeit zu prüfen.

Die Konfigurationsoptionen und deren Beschreibung sind in den nachfolgenden Tabellen und entsprechenden Unterkapiteln enthalten.

Tabelle 53 Einstellung der Zugriffsberechtigungen

Einstellungen	
TLS erforderlich	Diese Option gibt an, ob eine verschlüsselte Verbindung zwischen Clientsystem und Konnektor genutzt werden muss. Der Standardwert ist An.
Authentifizierung erforderlich	Diese Option gibt an, ob eine Clientsystem-Authentifizierung verpflichtend ist. Der Standardwert ist An.
Authentifizierungsmodus	Hier stehen zwei Möglichkeiten zur Verfügung: Zertifikat und Nutzername. Der Standardwert ist Zertifikat.
Offener Dienstverzeichnisdienst	Diese Option gibt an, ob der Dienstverzeichnisdienst über eine ungesicherte Verbindung erreichbar ist. Der Standardwert ist An.

7.4.1 Clientsysteme

In dieser tabellarischen Übersicht werden die konfigurierten Clientsysteme angezeigt. Zudem besteht die Möglichkeit, die Einstellungen eines vorhandenen Clientsystems über die Schaltfläche Bearbeiten anzupassen. Unterhalb der Tabelle finden Sie folgende Felder zum Anlegen eines neuen Clientsystems:

Unter Verwendung der Schaltfläche Clientsystem hinzufügen werden die angegeben Werte in die Konfiguration übernommen und in der Tabelle angezeigt. Beim Klick auf Schaltfläche Bearbeiten wird die Seite mit Einstellungsmöglichkeiten zum ausgewählten Clientsystem angezeigt. Änderungen werden mit der Schaltfläche Übernehmen bestätigt.

Tabelle 54 Einstellung des gewählten Clientsystems

Ausgewähltes Clientsystem	
Clientsystem-ID	Gibt die zu verwendende ID eines Clientsystems an. Dieser Wert wird benötigt, damit der Konnektor bei Operationen an der Außenschnittstelle das aufrufende Clientsystem korrekt zuordnen kann.
Beschreibung	Dieses Feld ist optional und erlaubt die Angabe einer Beschreibung des Clientsystems. Diese Einstellung dient ausschließlich zur Orientierung innerhalb der hinterlegten Konfiguration und beeinflusst nicht das Verhalten des Konnektors.

In Abhängigkeit vom eingestellten Authentifizierungsmodus (siehe folgende Kapitel 7.4.1.1 und 7.4.1.2) wird entweder bei Benutzer-Authentifizierung oder bei Zertifikats-Authentifizierung Momentan aktiv angezeigt.

7.4.1.1 Zertifikats-Authentifizierung

In diesem Bereich werden die Zertifikatsinformationen des Zertifikats angezeigt, welches bei der TLS-Authentifizierung des Clientsystems verwendet wird. Wenn noch kein Zertifikat hinterlegt ist, können Sie hier ein neues Zertifikat generieren und herunterladen oder ein X.509-Zertifikat hochladen. Ein schon vorhandenes Zertifikat kann hier mittels Schaltfläche Löschen entfernt werden.

Der Administrator übernimmt die Verantwortung für die Verlässlichkeit der importierten X.509-Zertifikate. Bei seiner Entscheidung für den Import kann er sich auf die Information der gematik stützen, welche PKI-Betreiber benennt, die die Erfüllung der Sicherheitsanforderungen der gematik erfüllen.

7.4.1.2 Benutzer-Authentifizierung

In diesem Bereich können Sie Benutzername und Passwort neu anlegen, ändern oder zurücksetzen.

Bei Änderung der Parameter im Menü Clientsysteme müssen ggf. Optionen im Praxisverwaltungssystem angepasst werden.

Die vom Praxisverwaltungs- oder Krankenhausinformationssystem verwendete Clientsystem-ID muss im Konnektor hinterlegt sein, damit dieser eingehende Anfragen mit der ausgewiesenen ID korrekt verarbeiten kann.

7.4.2 Arbeitsplätze

Die tabellarische Aufstellung zeigt die konfigurierten Arbeitsplätze an. Zudem besteht die Möglichkeit, die Einstellungen eines vorhandenen Arbeitsplatzes über die Schaltfläche Bearbeiten anzupassen. Unterhalb der Tabelle finden Sie folgende Felder zum Anlegen eines neuen Arbeitsplatzes:

Tabelle 55 Liste der konfigurierten Arbeitsplätze

Arbeitsplatz	
Arbeitsplatz hinzufügen	Unter Verwendung der Schaltfläche Arbeitsplatz hinzufügen werden die angegeben Werte in die Konfiguration übernommen und in der Tabelle angezeigt. Beim Klick auf Schaltfläche Bearbeiten wird die Seite mit Einstellungsmöglichkeiten zum ausgewählten Arbeitsplatz angezeigt.
Arbeitsplatz-ID	Die Arbeitsplatz-ID unter Ausgewählter Arbeitsplatz spezifiziert das Identifikationsmerkmal des Arbeitsplatzes. Änderungen werden mit der Schaltfläche Übernehmen bestätigt.
Beschreibung	Das Feld Beschreibung unter Ausgewählter Arbeitsplatz ist optional und erlaubt die Angabe einer Beschreibung des konfigurierten Arbeitsplatzes. Diese Einstellung dient ausschließlich zur Orientierung innerhalb der hinterlegten Konfiguration und beeinflusst nicht das Verhalten des Konnektors. Änderungen werden mit der Schaltfläche Übernehmen bestätigt.

Außerdem haben Sie hier die Möglichkeit zugeordnete Kartenterminals anzupassen oder hinzuzufügen. Folgende Felder stehen hierbei zur Verfügung:

Tabelle 56 Liste der zugeordneten Kartenterminals

Zugeordnete Kartenterminals	
Zuordnung	Hier werden die Terminals (mit den Informationen zu: Terminal-ID, Terminal-MAC, Terminal-Typ) angezeigt, die diesem Arbeitsplatz zugeordnet sind. Unterhalb der Tabelle haben Sie die Möglichkeit ein neues Terminal dem Arbeitsplatz hinzuzufügen und mittels der Schaltfläche Zuordnung hinzufügen zu bestätigen. Dabei sind folgende Einstellmöglichkeiten vorhanden:
Kartenterminal (Terminal-ID)	Dies bezeichnet das Kartenterminal, welches dem aktuell ausgewählten Arbeitsplatz neu zugeordnet wird. Wenn die Auswahlliste leer ist, dann sind dem Konnektor entweder keine Kartenterminals bekannt oder alle verfügbaren Kartenterminals sind diesem Arbeitsplatz bereits zugeordnet.

Zuordnungstyp	Typ der neuen Kartenterminal-Arbeitsplatzzuordnung. Es gibt zwei Typen zur Auswahl: lokal und entfernt. Das lokale Kartenterminal befindet sich tatsächlich lokal am Arbeitsplatz. Das entfernte Kartenterminal ist z.B. in einem anderen Raum (siehe dazu 7.1.4)

Die vom Praxisverwaltungs- oder Krankenhausinformationssystem verwendete Arbeitsplatz-ID muss im Konnektor hinterlegt sein, damit dieser eingehende Anfragen mit der ausgewiesenen ID korrekt verarbeiten kann.

7.4.3 Mandanten

Die tabellarische Aufstellung zeigt die konfigurierten Mandanten an. Zudem besteht die Möglichkeit, die Einstellungen eines vorhandenen Mandanten über die Schaltfläche Bearbeiten anzupassen. Unterhalb der Tabelle finden Sie folgende Felder zum Anlegen eines neuen Mandanten:

Tabelle 57 Liste der angelegten Mandanten

Mandant	
Mandanten-ID	Spezifiziert das Identifikationsmerkmal des Mandanten.
Beschreibung	Dieses Feld ist optional und erlaubt die Angabe einer Beschreibung des konfigurierten Mandanten. Diese Einstellung dient ausschließlich zur Orientierung innerhalb der hinterlegten Konfiguration und beeinflusst nicht das Verhalten des Konnektors.

Unter Verwendung der Schaltfläche Mandant hinzufügen werden die angegeben Werte in die Konfiguration übernommen und in der Tabelle angezeigt.

Beim Klick auf Schaltfläche Bearbeiten wird die Seite mit Einstellungsmöglichkeiten zur ausgewählten Mandanten angezeigt.

Die vom Praxisverwaltungs- oder Krankenhausinformationssystem verwendete Mandanten-ID muss im Konnektor hinterlegt sein, damit dieser eingehende Anfragen mit der ausgewiesenen ID korrekt verarbeiten kann.

Tabelle 58 Details zu ausgewähltem Mandanten

Ausgewählter Mandant	
Mandant-ID	Die Mandant-ID spezifiziert das Identifikationsmerkmal des Mandanten. Änderungen werden mit der Schaltfläche Übernehmen bestätigt.
Beschreibung	Das Feld Beschreibung unter Ausgewählter Mandant ist optional und erlaubt die Angabe einer Beschreibung des konfigurierten Mandanten. Diese Einstellung dient ausschließlich zur Orientierung innerhalb der hinterlegten Konfiguration und beeinflusst nicht das Verhalten des Konnektors. Änderungen werden mit der Schaltfläche Übernehmen bestätigt.

Hinweis: Für sämtliche weitere Konfigurationsschritte verwenden Sie die Schaltfläche Zuordnung hinzufügen.

Tabelle 59 Liste der zugeordneten Kartenterminals

Zugeordnete Kartenterminals	
Zuordnung	Hier werden die Terminals (mit den Informationen zu: (ID, Terminal-Hostname, Terminal-MAC) angezeigt, die diesem Mandant zugeordnet sind. Hier haben sie auch die Möglichkeit das Terminal zu löschen.
Kartenterminal	Hier finden Sie eine Auswahlliste mit Kartenterminals, die dem Mandanten neu zugeordnet werden können. Sollte dieses Feld nicht auswählbar sein, können keine weiteren Zuordnungen für den Mandanten hinzugefügt werden.

Tabelle 60 Liste der zugeordneten SMBs

Zugeordnete SMBs	
Zuordnung	Hier werden die SMBs (ID, ICCSN) angezeigt, die dem Mandanten zugeordnet sind. Hier haben sie auch die Möglichkeit die Zuordnung zu löschen.
Neue SMB-Zuordnung	Hier kann die ausgewählte SMB dem aktuellen Mandanten zugeordnet werden. Sollte dieses Feld nicht auswählbar sein, wurde die SMB noch nicht in die Konnektor-Verwaltung aufgenommen (siehe Kapitel 7.4.4). Es ist entweder keine SMB im Terminal vorhanden oder der Terminal ist nicht mit Konnektor verbunden (siehe Kapitel 7.5).

Tabelle 61 Liste der zugeordneten Arbeitsplätze

Zugeordnete Arbeitsplätze	
Zuordnung	Hier werden die Arbeitsplätze (Arbeitsplatz-ID, Arbeitsplatzbeschreibung) angezeigt, die dem Mandanten zugeordnet sind. Hier haben sie auch die Möglichkeit die Zuordnung zu löschen.
Arbeitsplatz	Hier finden Sie eine Auswahlliste mit Arbeitsplätzen, die dem Mandanten neu zugeordnet werden können. Sollte dieses Feld nicht auswählbar sein, können keine weiteren Zuordnungen für den Mandanten hinzugefügt werden (zum Beispiel, weil noch kein Arbeitsplatz angelegt wurde, dann siehe Kapitel 7.4.2).

Tabelle 62 Liste der zugeordneten Clientsysteme

Zugeordnete Clientsysteme	
Zuordnung	Hier werden die Clientsysteme (Clientsystem-ID, Clientsystem-Beschreibung) angezeigt, die dem Mandanten zugeordnet sind. Hier haben sie auch die Möglichkeit die Zuordnung zu löschen.

Clientsystem	Hier finden Sie eine Auswahlliste mit Clientsystemen, die dem Mandanten neu zugeordnet werden sollen. Sollte dieses Feld nicht auswählbar sein, können keine weiteren Zuordnungen für den Mandanten festgelegt werden (zum Beispiel, weil noch kein Clientsystem angelegt wurde, dann siehe Kapitel 7.4.1).

Tabelle 63 Liste der der Arbeitsplätze zugeordneter Clientsysteme

Arbeitsplätze zugeordneter Clientsysteme	
Zuordnung	Hier werden die Zuordnung Arbeitsplatz / Clientsystem (Clientsystem-ID, Clientsystem-Beschreibung, Arbeitsplatz-ID, Arbeitsplatz-Beschreibung) angezeigt, die dem Mandanten zugeordnet sind. Hier haben sie auch die Möglichkeit die Zuordnung zu löschen.
Clientsystem	Hier wird das Clientsystem angezeigt, das dem aktuell ausgewählten Mandanten und einem Arbeitsplatz neu zugeordnet ist. Eine Zuordnung von Mandant, Clientsystem und Arbeitsplatz kann nur einmal vorkommen. Für diese Zuordnung müssen Clientsysteme dem aktuellen Mandanten bereits zugeordnet worden sein.
Arbeitsplatz	Hier wird der Arbeitsplatz angezeigt, der dem aktuell ausgewählten Mandanten und einem Clientsystem neu zugeordnet wird. Eine Zuordnung von Mandant, Clientsystem und Arbeitsplatz kann nur einmal vorkommen. Für diese Zuordnung müssen Arbeitsplätze dem aktuellen Mandanten bereits zugeordnet worden sein.

Tabelle 64 Liste der zugeordneten Kartenterminals für Remote-PIN-Zugriff

Zugeordnete Kartenterminals für Remote-PIN-Zugriff	
Zuordnung	Hier werden die Terminals (Kartenterminal-ID, Kartenterminal-Hostname, Arbeitsplatz-ID, Arbeitsplatz-Beschreibung) angezeigt, die für diesen Mandanten als lokale Terminals beim Remote-Pin-Verfahren fungieren (Kapitel 7.1.4). Hier haben sie auch die Möglichkeit die Zuordnung zu löschen.
Kartenterminal	Hier wird das bzw. die Kartenterminal(s) angezeigt, das / die dem aktuell ausgewählten Mandanten und einem Arbeitsplatz neu zugeordnet ist / sind. Eine Zuordnung von Mandant, Kartenterminal und Arbeitsplatz kann nur einmal vorkommen. Für diese Zuordnung müssen Kartenterminals dem aktuellen Mandanten bereits zugeordnet worden sein.
Arbeitsplatz	Hier wird der Arbeitsplatz angezeigt, der dem aktuell ausgewählten Mandanten und einem Kartenterminal neu zugeordnet wird. Eine Zuordnung von Mandant, Kartenterminal und Arbeitsplatz kann nur einmal vorkommen. Für diese Zuordnung müssen Arbeitsplätze dem aktuellen Mandanten bereits zugeordnet worden sein.

Tabelle 65 Zugeordneter VSDM-Encryptionkey

Zugeordneter VSDM-Encryptionkey	
Encryptionkey	Dieser Schlüssel wird verwendet, um den Prüfungsnachweis mandantenspezifisch zu verschlüsseln. Er muss 16 Zeichen lang sein und kann per Hand eingegeben oder generiert werden. Bei Verwendung von mehreren Konnektoren, müssen verschiedene Schlüssel generiert werden.
Aktueller Schlüssel	Hier wird der aktuell verwendete Verschlüsselungsschlüssel angezeigt.
Generieren	Ein neuer Schlüssel wird generiert. Bitte achten Sie darauf, dass bereits vorhandene Schüssel überschrieben werden.
Neuer Schlüssel	Hier kann der neue Schlüssel manuell eingegeben werden und mit der Schaltfläche Übernehmen in die Verwaltung übernommen werden.

7.4.4 SMB

Tabelle 66 Liste der SMBs

SMB	
SMBs	In dieser Tabelle werden die SMBs (ID, ICCSN, HSM) angezeigt, die in die Konnektor-Verwaltung aufgenommen wurde. Hier haben sie auch die Möglichkeit, die Zuordnung zu löschen.
Verfügbare SMBs	Hier werden die ICCSN der verfügbaren SMBs angezeigt.

Nach Betätigen der Schaltfläche SMB hinzufügen wird die ausgewählte SMB in die Konnektor-Verwaltung aufgenommen. Sollte dieses Feld nicht auswählbar sein, ist keine SMB im Kartenterminal vorhanden oder das Terminal ist nicht mit dem Konnektor verbunden (siehe Kapitel 7.5).

7.5 Menüpunkt Kartenterminals

Der Menüpunkt Kartenterminals ermöglicht die Konfiguration von Kartenterminals. Hier können neue Kartenterminals hinzugefügt, geändert und entfernt werden. Weiterhin ist es möglich, Statusinformationen über alle verbundenen Kartenterminals einzuholen.

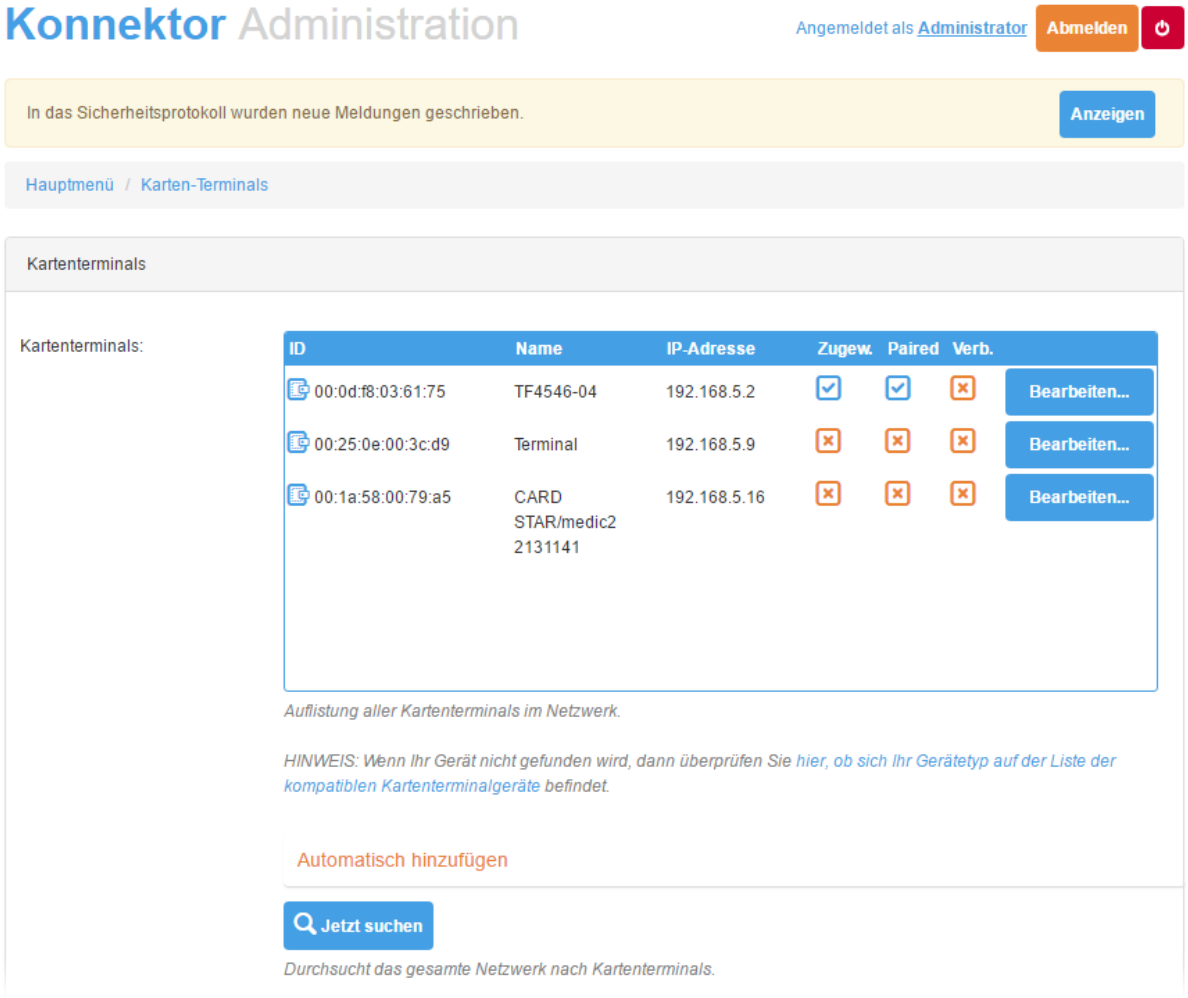


Abbildung 16 Menüpunkt Kartenterminals

Tabelle 67 Liste der Kartenterminals

Kartenterminals	
Kartenterminals	In dieser Tabelle können Sie alle momentan erkannten Kartenterminals einsehen. Neben der IP-Adresse, dem Port, dem Namen und den Statusangaben, ob das Kartenterminal zugewiesen, gepaired und / oder verbunden ist, findet sich unter der Schaltfläche Bearbeiten die Möglichkeit, das Kartenterminal aus der betreffenden Zeile zu bearbeiten. Eine nähere Erläuterung finden Sie unterhalb dieses Abschnitts. Bei Verwendung des Buttons Entfernen wird das Kartenterminal in der Zeile entfernt und steht dem Konnektor nicht mehr zu Verfügung.

Kartenterminals	
Bearbeiten	Sie können in diesem Untermenü Statusinformationen zum Kartenterminal und das zugehörige Zertifikat finden. Das Untermenü wird Ihnen nur angezeigt, wenn die Software auch mit einem Kartenterminal verbunden ist. Mit Klick auf den Button Entfernen beenden Sie die Zuordnung zu diesem Kartenterminal. Im Abschnitt Bearbeiten innerhalb des Untermenüs können Sie folgende Angaben einsehen bzw. ändern. Nach der Konfiguration klicken Sie auf Übernehmen, um die Einstellungen zu speichern. Bei Klick auf Abbrechen werden Ihre Änderungen verworfen. 5. Kartenterminal-ID - Diese Angabe zeigt dem Benutzer die ID des Kartenterminals an und ist nicht änderbar. 6. Hostname - Bezeichnung (auch: Friendly-Name) des SICCT-Terminals 7. IP-Adresse - IP-Adresse des Kartenterminals 8. TCP-Port - TCP-Port, über den das Kartenterminal kommuniziert (optional) 9. Adminname - Benutzername des Administrators 10. Adminpasswort - Passwort des Administrators, den Sie in Adminname angegeben haben
Jetzt Suchen	Mit der Schaltfläche Jetzt Suchen wird eine Suche eingeleitet, in der das gesamte Netzwerksegment nach kompatiblen Kartenterminals durchsucht wird. Konnte der Konnektor Ihr Kartenterminal nicht automatisch erkennen, können Sie das Kartenterminal manuell hinzufügen. Dazu müssen Sie die folgenden Felder vollständig ausfüllen und auf Hinzufügen klicken.
IP-Adresse	IP-Adresse des Kartenterminals
TCP-Port (optional)	TCP-Port, über den das Kartenterminal kommuniziert
Hostname (optional)	Die Bezeichnung (auch: Friendly-Name) des SICCT-Terminals
Geräte-MAC (optional)	Eindeutige Nummer zur Identifizierung Ihres Gerätes. Sie finden die Geräte-MAC am Gehäuse des Kartenterminals.

Tabelle 68 Einstellungen der Kartenterminals

Einstellungen	
Angaben unter diesem Abschnitt sind für alle Kartenterminals im Netzwerk gültig. Nach der Konfiguration klicken Sie auf Übernehmen, um die Einstellungen zu speichern.	
Discovery Port	Portnummer, über die Dienstanfragen im lokalen Netzwerk an die Kartenterminals gesendet werden sollen.
Discovery Timeout	Diese Angabe in Sekunden wartet der Konnektor auf Antworten zu Service-Discovery-Anfragen. Der Wert muss zwischen 1 und 60 liegen.
Announcement Port	Portnummer, an der der Konnektor auf Dienstbeschreibungspakete reagieren soll.
Discovery Zyklus	Angabe in Minuten, in welchem Abstand Service-Discovery-Anfragen gesendet werden sollen. Der Wert muss zwischen 0 und 140 liegen.

Einstellungen	
Keep-Alive Intervall	Angabe in Sekunden, in welchem Abstand Keep-Alive-Nachrichten gesendet werden sollen. Der Wert muss zwischen 1 und 10 liegen.
Keep-Alive Versuche	Anzahl der Fehlversuche Keep-Alive-Nachrichten erfolgreich zu versenden, bevor die Verbindung getrennt wird. Der Wert muss zwischen 3 und 10 liegen.
Handshake-Timeout	Die Dauer in Sekunden, die der Konnektor auf ein TLS-Verbindungsaufbau zum Kartenterminal wartet. Der Wert muss zwischen 1 und 60 Sekunden liegen.
Display Anzeigedauer	Dauer in Sekunden, die Meldungen auf dem Display nach Beendigung von Kommandos mit Displayausgabe angezeigt werden. Der Wert muss zwischen 1 und 30 Sekunden liegen.

7.6 Menüpunkt Karten

Im Menüpunkt Karten werden diejenigen Karten aufgeführt, die in einem mit dem Konnektor verbundenen Kartenterminal eingelegt sind. Wurden keine Karten erkannt, so werden auch keine Informationen zu diesen Karten aufgeführt.

Tabelle 69 Liste der verfügbaren Karten

Verfügbare Karten	
Karten	In dieser tabellarischen Aufstellung befindet sich die Übersicht der eingelegten Karten. Die folgenden Informationen werden in der Darstellung aufgelistet: 1. Terminal-ID: Zeigt die Bezeichnung des Terminals an, in dem die Karte eingelegt ist. Diese Bezeichnung ist identisch mit der MAC-Adresse des Terminals. 2. Slot: Gibt den Slot (Schacht) an, in dem die Karte in dem betreffenden Kartenterminal eingelegt wurde. 3. Typ: Gibt den Typ der eingelegten Karte an. Konnte der Typ der Karte nicht ermittelt werden, so wird unbekannte Karte für die eingelegte Karte angezeigt. 4. Besitzer / Info: Gibt den Karteninhaber in Kurzform sowie zusätzliche verfügbare Informationen an, wenn vorhanden. 5. Eingesteckt: Gibt den Zeitpunkt im Format Datum / Uhrzeit (DD.MM.YYYY hh:mm: ss+Zeitzone) an, zu welchem die Chipkarte in das Kartenterminal eingelegt wurde. Für jede in der Tabelle angezeigte Karte wird zusätzlich die Schaltfläche Infos angezeigt. Durch Betätigen der Schaltfläche werden die folgenden Informationen auf der Seite Informationen angezeigt: Kartenterminal, Slot, Typ, Einsteck-Zeit, Besitzer, ICCSN, Versionen und Ablaufdatum des Zertifikats. Mit Hilfe der unterhalb der Tabelle angezeigten Schaltfläche Zertifikationsinformationen anzeigen können weitere Informationen zur Gültigkeit der Kartenzertifikate angezeigt werden. Dies umfasst die Werte Besitzer/Info, Gültigkeitsende des Zertifikates, Verbl. Tage, Typ, Terminal-ID und Slot aller vorhandenen Kartenzertifikate.
Timeout	Erlaubt die Konfiguration des Zeitwerts in Sekunden (zwischen 1 und 30), nach dem eine Operation mit einem Timeout-Wert abgebrochen wird. Unter Verwendung der Schaltfläche Übernehmen wird die Einstellung für den Zeitwert übernommen.

7.7 Menüpunkt Systeminformationen

Der Menüpunkt Systeminformationen ermöglicht die Einsicht in die Versionsinformationen und erlaubt spezifische Einstellungen für die Ereignisprotokollierung vorzunehmen. Im Bereich Einstellungen wird die Konfigurationsmöglichkeit zur Einstellung der Anzahl an Wiederholungen des Ereignisversands angeboten, bis der Konnektor keine weiteren Nachrichten an ein Clientsystem versendet. Die Schnittstelle zu den Clientsystemen wird in der Konnektorspezifikation (gemSpec_KON_V4.11.1) erläutert.

Der Konnektor interagiert mit Clientsystemen unter Verwendung sogenannter Ereignisse (Events). Diese Ereignisse werden im Netzwerk des Leistungserbringers versandt. Mit dem konfigurierten Wert kann angegeben werden, wie oft der Konnektor versucht, das Ereignis an ein Clientsystem zu versenden. Wird beispielsweise der Wert 3 eingestellt, so versucht der Konnektor bis zu drei Mal ein Ereignis zu versenden. Kommt während dieser Versuche keine Verbindung mit dem Clientsystem zu Stande, wird der Konnektor die Anmeldung auf den spezifischen Ereignistyp verwerfen.

Ein Clientsystem muss die Registrierung so vornehmen, dass eine IP-Adresse oder eine per DNS auflösbare Adresse angegeben wird. Protokolle wie mDNS werden vom Konnektor nicht unterstützt.

7.8 Menüpunkt Betriebszustände

Der Menüpunkt Betriebszustände bietet einen Überblick über möglichen Betriebszustände. Zudem können die kritischen Zustände hier zurückgesetzt und der Alarmwert konfiguriert werden.

Welche Betriebszustände möglich sind, können Sie unter Kapitel 4.9.1 nachlesen.

Tabelle 70 Liste der Operationen

Operationen	
Operation	Operationsname
OK-Wert	Die Gewichtung der Operation mit positiven Ergebnis (nicht konfigurierbar)
NOK-Wert	Die Gewichtung der Operation mit negativen Ergebnis (nicht konfigurierbar)
Alarm-Wert	Der aktuell eingestellte Wert

Überschreitet der gleitende 10-Minuten-Summenwert einer der gelisteten Operationen den zugehörigen Alarmwert, so wird EC_CRYPTOPERATION_ALARM gemeldet.

7.9 Menüpunkt Zertifikate

Der Menüpunkt Zertifikate beinhaltet die Punkte Vertrauensraum, Vertrauensanker, Netzwerk sowie Einstellungen auf die im Folgenden näher eingegangen wird:

Der Vertrauensraum wird mit Hilfe einer TSL (Trusted Service List) definiert. In dieser TSL befinden sich Zertifikate, die der Konnektor als vertrauenswürdig erachtet.

Tabelle 71 Konfiguration des Vertrauensraums

Vertrauensraum	
Gültigkeit der TSL	Dieses Feld zeigt den Gültigkeitsstatus der Trusted Service List an.
TSL-Herausgeber	Dieses Feld zeigt den Herausgeber der Trusted Service List an.
TSL-Sequenznummer	Zeigt die aktuelle Version der Trusted Service List an. Die Version ist Bestandteil der TSL und wird aus dieser ermittelt.
TSL-Dienst Start-Zeit	Zeigt den Herausgabezeitpunkt der Trusted Service List an. Diese Liste ist ab diesem Zeitpunkt gültig.
TSL Erstellungszeit	Zeigt den Zeitpunkt, wann das Zertifikat erstellt wurde.
Nächstes Update	Zeigt den Zeitpunkt des nächsten notwendigen Updates an. Die Liste ist bis zu diesem Zeitpunkt gültig.
Signatur der TSL	Zeigt den Fingerabdruck der Trusted Service List an.
Gültigkeit der CRL	Dieses Feld zeigt an, ob die Certificate Revocation List (Zertifikatssperrliste) gegenüber einer vertrauenswürdigen Zertifikatsstelle auf Gültigkeit geprüft wurde.
CRL-Herausgeber	Dieses Feld zeigt an, wer die CRL erstellt hat.
CRL-Sequenznummer	Zeigt die aktuelle Version der CRL an. Die Version ist Bestandteil der CRL und wird aus dieser ermittelt.
CRL Erstellungszeit	Zeigt den Zeitpunkt, wann die CRL erstellt wurde.
Nächstes Update	Zeigt den Zeitpunkt des nächsten notwendigen Updates an. Die Liste ist bis zu diesem Zeitpunkt gültig.
Manuell importierte CA Zertifikate	Listet manuell importierte Zertifikate auf.

Über die Menüpunkte CA Zertifikat hochladen, TSL hochladen und CRL hochladen können die jeweiligen Dateien hochgeladen werden.

7.9.1 Vertrauensanker

Der Menüpunkt Vertrauensanker zeigt die Gültigkeit der Vertrauensanker TSL, sowie der Vertrauensanker gSMC-K.

Tabelle 72 Liste von Endpunkten

Netzwerk	
Primäre OCSP Forwarder-Adresse	Unter Verwendung der Schaltflächen Ping oder Test-Request kann überprüft werden, ob das primäre Rechenzentrum erreicht werden kann.

Netzwerk	
Sekundäre OCSP Forwarder-Adresse	Unter Verwendung der Schaltflächen Ping oder Test-Request kann überprüft werden, ob das sekundäre Rechenzentrum erreicht werden kann.
Port des OCSP Forwarders	Zeigt den verwendeten Port des OCSP-Forwarders.
Primäre TSL Download-Adresse	Dieses Feld zeigt die primäre Download-Adresse des TSL an.
Sekundäre TSL Download-Adresse	Dieses Feld zeigt die sekundäre Download-Adresse des TSL an.
Default HTTP-Port	Dieses Feld zeigt den Port des http-Dienstes an (Default 80).
Default HTTPs-Port	Dieses Feld zeigt den Port des https-Dienstes an (Default 443).

Tabelle 73 Einstellung zu Endpunkten

Einstellungen	
Primäre CRL Download-Adresse	Dieses Feld zeigt die primäre Download Adresse der CRL an.
Sekundäre CRL Download-Adresse	Dieses Feld zeigt die sekundäre Download Adresse der CRL an.
CRL- und TSL-Timeout	Gibt den Zeitwert in Sekunden (zwischen 1 und 3600) an, nach dem ein Download abgebrochen wird.
TSL Grace-Period	Gibt an, wie viele Tage (zwischen 1 und 30) der Konnektor mit einer zeitlich abgelaufenen TSL weiter betrieben werden kann.
OCSP Grace-Period	Standard Grace Period OCSP für nonQES[5] in Minuten (zwischen 0 und 20).
OCSP Timeout (nonQES)	Standard Timeout OCSP für nonQES-Zertifikate in Sekunden (zwischen 1 und 120).
OCSP Timeout (QES)	Standard Timeout OCSP für QES-Zertifikate in Sekunden (zwischen 1 und 120).
Warnzeit	Anzahl der Tage (zwischen 0 und 180) vor dem Ablauf des Zertifikats, bevor eine Warnung ausgegeben werden soll.
Überprüfungszeit	Anzahl der Tage (zwischen 0 und 365), nach der alle gesteckten Karten überprüft und auf den Zertifikats-Ablauf getestet werden.

Der Konnektor wird ohne eine vorkonfigurierte Trusted Service List ausgeliefert. Daher muss die Trusted Service List manuell aktualisiert werden. Diese Trusted Service List ist von der Internetseite der gematik (www.gematik.de) herunterzuladen und in den Konnektor einzuspielen. Dazu muss die Schaltfläche Hochladen im angezeigten Menü TSL hochladen verwendet werden.

[5] QES steht für qualifizierte elektronische Signatur.

7.10 Menüpunkt Protokollierung

Unter dem Menüeintrag Hauptmenü > Protokollierung sind Einsichtnahme und Export der Protokolleinträge möglich.

Hinweis: Es werden grundsätzlich weder persönliche noch medizinische Daten protokolliert. Der Hersteller T-Systems wird nur mit ausdrücklicher Genehmigung des Leistungserbringers Protokolldaten (sofern über Fernwartung bereits freigeben) an Dritte weitergeben.

Die folgenden Protokolleinträge werden unterschieden:

1. System - In diesem Bereich werden alle Einträge angezeigt, die dem System zugeordnet werden. Zudem bietet dieser Bereich den Download der Protokolldaten an.
2. Sicherheit - In diesem Bereich werden alle sicherheitskritischen Protokolleinträge verwaltet. Zudem bietet dieser Bereich den Download der Protokolldaten an (siehe Kapitel 4.9.1).

Sehr viele Einträge im Sicherheitsprotokoll können ein Hinweis auf eine DoS-Attacke sein.

3. Performance - In diesem Bereich werden alle Einträge angezeigt, die für die Performance des Konnektors von Bedeutung sind. Zudem bietet dieser Bereich den Download der Protokolldaten an.
4. VSDM Ablauf - In diesem Bereich werden alle Einträge angezeigt, die dem VSDM-Ablauf zugeordnet sind. Zudem bietet dieser Bereich den Download der Protokolldaten an.
5. VSDM Fehler - In diesem Bereich werden alle Einträge angezeigt, die VSDM-Fehlern zugeordnet sind. Zudem bietet dieser Bereich den Download der Protokolldaten an.
6. VSDM Performance - In diesem Bereich werden alle Einträge angezeigt, die der VSDM-Performance zugeordnet sind. Zudem bietet dieser Bereich den Download der Protokolldaten an.

Tabelle 74 Systemprotokolle

System	
In diesem Bereich werden vorhandene Einträge der Systemprotokollierung angezeigt.	
Download	Mit dieser Schaltfläche haben Sie die Möglichkeit, die Protokolleinträge herunterzuladen.
Löschen	Mit dieser Schaltfläche haben Sie die Möglichkeit, die Protokolleinträge zu löschen.

Tabelle 75 Sicherheitsprotokolle

Sicherheit	
In diesem Bereich werden vorhandene Einträge der Sicherheitsprotokollierung angezeigt.	
Download	Mit dieser Schaltfläche haben Sie die Möglichkeit, die Protokolleinträge herunterzuladen.

Tabelle 76 Performanceprotokolle

Performance	
In diesem Bereich werden vorhandene Einträge der Performanceprotokollierung angezeigt.	
Download	Mit dieser Schaltfläche haben Sie die Möglichkeit, die Protokolleinträge herunterzuladen.
Löschen	Mit dieser Schaltfläche haben Sie die Möglichkeit, die Protokolleinträge zu löschen.

Tabelle 77 VSDM-Ablaufprotokolle

VSDM Ablauf	
In diesem Bereich werden vorhandene Einträge der VSDM-Ablaufprotokollierung angezeigt.	
Download	Mit dieser Schaltfläche haben Sie die Möglichkeit, die Protokolleinträge herunterzuladen.

Tabelle 78 VSDM-Fehlerprotokolle

VSDM Fehler	
In diesem Bereich werden vorhandene Einträge der VSDM-Fehlerprotokollierung angezeigt.	
Download	Mit dieser Schaltfläche haben Sie die Möglichkeit, die Protokolleinträge herunterzuladen.

Tabelle 79 VSDM-Performanceprotokolle

VSDM Performance	
In diesem Bereich werden vorhandene Einträge der VSDM-Performanceprotokollierung angezeigt.	
Download	Mit dieser Schaltfläche haben Sie die Möglichkeit, die Protokolleinträge herunterzuladen.

Tabelle 80 Einstellungen zur VSDM-Performanceprotokollierung

Einstellungen	
In diesem Bereich werden vorhandene Einträge der VSDM-Performanceprotokollierung angezeigt.	
Detailgrad Systemprotokoll	Mit Hilfe dieses Elements besteht die Möglichkeit, den Detailgrad der Systemprotokollierung zu regeln. Die folgenden Möglichkeiten bestehen: 1. Info - Dieses Meldungslevel hat die höchste Granularität. Es werden sehr detaillierte Informationen über Systemzustände generiert. Verwenden Sie diese Einstellung ausschließlich zur Analyse in besonderen Fehlersituationen. 2. Warning - Beginnend ab dem Meldungslevel Warnung werden alle Systemeinträge

Einstellungen	
	3. Error - Beginnend ab dem Meldungslevel Fehler werden alle Systemeinträge protokolliert. Meldungen mit Level Warnung werden in diesem Falle nicht protokolliert. 4. Fatal - Es werden ausschließlich schwerwiegende Fehler protokolliert. Alle anderen Typen werden nicht erfasst.
Mindestspeicherdauer des Sicherheitsprotokolls	Dieses Feld zeigt die eingestellte Aufbewahrungsdauer der Protokolleinträge des Sicherheitsprotokolls an. Der Wert kann für einen Zeitraum zwischen 10 und 365 Tagen konfiguriert werden.
Mindestspeicherdauer des System- / Performance-Protokolls	Dieses Feld zeigt die eingestellte Aufbewahrungsdauer der Protokolleinträge der System- / Performance-Protokolle an. Der Wert kann für einen Zeitraum zwischen 10 und 365 Tagen konfiguriert werden.
Protokollierung von Kryptooperationen	Wird dieser Schalter aktiviert, werden alle erfolgreichen kryptografischen Operationen protokolliert.
Performance-Protokollierung	Wird dieser Schalter aktiviert, so wird das Performance-Protokoll erzeugt. Andernfalls erscheinen keine Einträge in der Performance-Protokollierung.

Die Protokollierung des Konnektors dient unter anderem zur Analyse von Fehlern aber auch möglichen Sicherheitsvorfällen. Wird zwischen dem letzten Login des aktuell angemeldeten Administrators und dem aktuellen Login ein Eintrag im Sicherheitsprotokoll erzeugt, wird in der Oberfläche des Konnektors ein diesbezüglicher Hinweis angezeigt. Somit wird jeder Administrator über Sicherheitsprotokolleinträge informiert, die während seines Logouts aufgenommen wurden.

7.10.1 Backup und Löschen der Protokollierung

Sollte ein Firmware Update des Konnektors fehlschlagen so können Sie im Menüeintrag Hauptmenü > Protokollierung die Protokollierung exportieren und anschließend löschen. Mit diesem Vorgang wird zusätzlicher Speicher für die Firmware Update zur Verfügung gestellt.

Zu löschen sind folgenden Protokollierungen:

- System
- Performance
- VSDM Ablauf
- VSDM Fehler
- VSDM Performance

7.11 Menüpunkt Backup

Nach erfolgter Kompletteinrichtung des Konnektors sollte ein erstes Backup erfolgen. Nur so können im Falle einer späteren Zurücksetzung auf Werkseinstellungen (z.B. bei vergessenem Passwort) die Bestandsdaten rückgesichert werden.

Tabelle 81 Backupsicherung erstellen

Einstellungen sichern	
SMC-B	Hier wird eine Auswahlliste mit ICCSN der SMC-B-Karten angezeigt, die zum Exportieren genutzt werden soll.
Exportieren	Über diese Schaltfläche können alle Einstellungen, die am Konnektor vorgenommen wurden, in einer Datei zusammengefasst und heruntergeladen werden.

Tabelle 82 Backupsicherung laden

Einstellungen wiederherstellen	
Importieren	Über diese Schaltfläche können vorher exportierte Einstellungs-Dateien des Konnektors hochgeladen werden.
Zurücksetzen auf Werkszustand	Die gesamten Einstellungen des Konnektors werden mit dieser Schaltfläche auf Werkseinstellung zurückgesetzt. Das Zurücksetzen dauert circa 40-45 Sekunden.

7.12 Menüpunkt Update

Im Bereich Update-Plan befindet sich die Tabelle Plan alle Geräte und die Schaltflächen zur Verwaltung von Updates. In der Tabelle Plan alle Geräte werden der Konnektor und alle angeschlossenen Terminals angezeigt. Neben der Beschreibung der aktuellen Version befinden sich hier folgende für die Durchführung einer Aktualisierung relevanten Schaltflächen.

Eine Aktualisierung soll nur dann erfolgen, wenn ausreichend Informationen über den Inhalt des Softwareupdates bekannt sind und eine bewusste Entscheidung bei der Freischaltung möglich ist.

Tabelle 83 Plan alle Geräte

Plan alle Geräte	
Plan ausführen	Diese Schaltfläche ist nur aktiv, wenn ein Update-Plan hinterlegt ist.
Planen	Diese Schaltfläche pro Zeile eines Geräts dient dazu, einen Update-Plan für das jeweilige Gerät zu hinterlegen.
Gruppen-Ansicht	Über diese Schaltfläche werden die Einträge in der Tabelle Plan alle Geräte gruppiert oder einzeln dargestellt.
Updates online suchen	Mit Hilfe dieser Schaltfläche kann die automatische Suche nach einer Software-Aktualisierung des Konnektors angestoßen werden.
Paket-Verwaltung	Mit Hilfe dieser Schaltfläche kann ein Firmware-Update manuell hochgeladen werden.

Eine Aktualisierung der installierten Firmware sollte nur dann erfolgen, wenn die neue Version die Behebung eines vorhandenen Problems anzeigt oder neue Funktionen bereitgestellt werden, die für den Einsatz des Konnektors unbedingt erforderlich sind.

Tabelle 84 Update-Einstellungen

Einstellungen	
Erprobungs-Versionen erlauben	Wenn aktiviert, werden auch Update-Pakete angeboten, die für die Erprobung gedacht sind. Diese Pakete befinden sich noch in der Qualitätssicherungsphase, daher besteht hier ein höheres Risiko auf Unvollständigkeit. Der Standardwert ist Aus.
Automatische Überprüfung	Mit Hilfe des Schalters kann die tägliche automatische Suche nach Firmware-Aktualisierungen im Internet aktiviert werden. Der Standardwert ist AN.
Automatisches Herunterladen	Ist dieser Schalter aktiviert, werden automatisch neue Firmware Aktualisierungen des Konnektors und der Kartenterminals heruntergeladen. Der Standardwert ist Aus.
URL für die Update-Anfrage	Hier wird der SOAP-Endpunkt des KSR-Dienstes[6] für Firmware-Aktualisierungsinformationen angezeigt.
URL für den Firmware-Download	Hier wird der Web-Endpunkt des KSR-Dienstes für Firmware-Downloads angezeigt.
URL für den Konfigurations-Download	Hier wird der Web-Endpunkt des KSR-Dienstes für den Download von Konfigurationsdaten angezeigt.

7.13 Menüpunkt Fernwartung

Die Möglichkeit eine Verbindung zwischen dem Konnektor und einer Fernwartung eines Service-Providers aufzubauen, muss einmalig über ein Passwort autorisiert werden. Wo und auf welchem Wege Sie das benötigte Passwort erhalten wird im Kapitel 5.1.2 beschrieben.

Damit der Service-Provider den Zustand des Konnektors verfolgen darf, muss der lokale Superadministrator eine Nutzungs- / Vertragsinformation im Feld Fernwartung zulassen bestätigen.

Der lokale Superadministrator des Konnektors erhält eine verschlüsselte E-Mail, welche die vollständigen Zugangsdaten inkl. neu vergebenem Passwort enthält. Mit diesen Zugangsdaten hat er die Möglichkeit, die Operationen der Fernwartung zu konfigurierenTabelle 85 Verbindungseinstellungen zur Fernwartung

Fernwartung	
Ereignis-Kanal	Dieses Feld ist auf Getrennt gesetzt, wenn die Fernwartung nicht zugelassen wird.

[6] Konfigurationsdienst

Befehls-Kanal	Dieses Feld ist auf Getrennt gesetzt, wenn die Fernwartung nicht zugelassen wird.
Fernwartung zulassen	Dieses Feld muss aktiviert werden, wenn eine Verbindung zur Fernwartung hergestellt werden soll. Voraussetzungen und notwendige Schritte für den Aufbau einer Verbindung mit dem Service-Provider sind in Kapitel 5.1.2 beschrieben
URL der Fernwartung	In dieses Feld wird die URL des Dienstes eingegeben, der für die Fernwartung verwendet werden soll.
Nutzername	Dieses Feld wird verwendet, um den Nutzernamen für die Anmeldung zur Fernwartung einzugeben.
Kennwort	Dieses Feld wird verwendet, um das Kennwort für die Anmeldung zur Fernwartung einzugeben.

Bei dem Ereignis- und Befehls-Kanal handelt es sich um eine Statusanzeige. Es wird keine Einstellung zugelassen die beispielspielsweise nur den Ereignis-Kanal erlaubt, der Befehls-Kanal für die Fernwartung jedoch nicht. Im laufenden Betrieb kann es zu unterschiedlichen Statusanzeigen der beiden Kanäle kommen, dies benötigt aber keinen Eingriff durch den lokalen Administrator.

Alle Berechtigungen sind per Default auf „AUSGESCHALTET“ gestellt.

Tabelle 86 Allgemeine Einstellungen zur Fernwartung

Einstellungen	
Wartungs-Intervall	Dieses Feld gibt den Zeitraum an, in den aufwendigen Operationen der Fernwartung ausgeführt werden sollen. Mögliche Optionen sind wahlweise Wartung jederzeit, Tägliche Wartung, Wöchentliche Wartung oder Monatliche Wartung. Bitte wählen Sie das gewünschte Intervall. Der Konnektor steht dann für kurze Zeit bzw. je nach geplanten Aufgaben für den Zeitraum des Wartungsintervalls nicht zur Verfügung. Sollte der Wartungsinvervall (Zeitraum) sehr kurz gewählt werden, kann eine Aufgabe über das Wartungsfenster hinaus dauern. Die Fernwartung über den Remote-Management Service erlaubt einen „Force“-Modus, der innerhalb des Wartungsintervalls Aufgaben gegenüber bereits geplanten Aufgaben vorzieht. Der kürzeste auswählbare Wartungszeitraum ist „1“ für eine Stunde.
Versand-Intervall der Diagnosedaten	In diesem Feld können Sie die Dauer in Sekunden zwischen zwei Sendevorgängen der Diagnosedaten festlegen. Mögliche Werte liegen zwischen: 10 und 540 Sekunden (9 Minuten). Die Diagnose Daten werden automatisch an die Fernwartung (Remote Management Service Backend) gesendet.

Einstellungen	
Konfigurations-Verarbeitung	In diesem Feld können Sie den Modus zur Verarbeitung von Konfigurationen der Fernwartung auswählen. Mögliche Werte sind: Zulassen, Ablehnen und Manuell genehmigen. Wird der Modus Manuell genehmigen gewählt, müssen die Operationen Neustart und / oder Firmware-Update, durch den Lokalen- bzw. den Super-Administrator, explizit genehmigt werden. Wird Zulassen ausgewählt, hat die Fernwartung jederzeit die Möglichkeit Ereignisse abzufragen bzw. Befehle an den Konnektor zu senden. Diese Remote Aktionen werden in den Konnektor Protokollen mit aufgeführt.

Tabelle 87 Berechtigungen für Fernwartung

Berechtigungen	
In diesem Feld werden alle Berechtigungen aufgelistet, die für die Fernwartung aktiviert bzw. deaktiviert werden können.	
Erlaubt das Versenden von Statusinformationen	An oder Aus
Erlaubt das Versenden der Anzeigen-Informationen	An oder Aus
Erlaubt das Versenden des System-Protokolls	**Aus** Muss aus Datenschutzgründen auf AUS stehen
Erlaubt das Versenden des Sicherheits-Protokolls	**Aus** Muss aus Datenschutzgründen auf AUS stehen
Erlaubt das Versenden des Performance-Protokolls	**Aus** Muss aus Datenschutzgründen auf AUS stehen
Erlaubt das Neustarten des Konnektors	An oder Aus
Erlaubt das Aktualisieren der Konnektor-Firmware	An oder Aus

Der Default Wert der Berechtigungen ist „Aus“. Ist der Wert auf „AN“ gestellt werden die Informationen automatisch an die Fernwartung (Remote Management Service) gesendet.

Wichtiger Hinweis: Die Berechtigung für das System-, Sicherheits- und Performance- Protokoll ist aus Datenschutzgründen zwingend auf „AUS“ zu stellen.

7.14 CA-Zertifikat für die Fernwartungsverbindung

Über diese Schaltfläche können neue CA-Zertifikate hochgeladen werden und stehen so dem T-Systems Konnektor zur Fernwartung zur Verfügung.

7.15 Logout von der Administrationsoberfläche

Von der Administrationsoberfläche kann man sich mit dem Button „Abmelden“ ausloggen.

7.16 Werksreset durchführen

Von der Administrationsoberfläche kann man den Werksreset über Hauptmenü – Backup den Button „Zurücksetzen auf Werkszustand“ klicken.

Für die Durchführung des Werksresets benötigt der Konnektor typischer Weise weniger als einer Minute.

Hinweis zum Datenschutz: Nach einem Werksreset darf das Gerät nur unter dem gleichen Vertrag weiterbetrieben oder neu konfiguriert werden.

7.16.1 Admin Passwort vergessen / Werksreset wird ausgelöst

Hinweis: Sollte das lokale Administrator Kennwort nicht mehr vorliegen, so kann über den Menüpunkt „Kennwort vergessen“ die ICCSN (Typenschild auf der Unterseite des Konnektors Siehe 4.1.1) eingegeben werden. Durch dieses Vorgehen wird ein Werksreset durchgeführt.

Für die Durchführung der Außerbetriebnahme bzw. Werksresets benötigt der Konnektor typischer Weise weniger als einer Minute

8 Einstellungen des Fachmoduls Versichertendaten

Der Bereich Versichertendaten dient der Konfiguration für das VSDM- Fachmodul des Konnektors.

Tabelle 88 VSDM-Einstellungen

Dienst	
Dienstname und -protokoll	Gibt Name und Protokoll zur Ermittlung eines Intermediärs (einer Komponente zur Ermittlung einer Kommunikationsgegenstelle im gesicherten Netz der Telematikinfrastruktur) an.
Automatische Stammdatenaktualisierung	Mit Hilfe dieses Schalters wird die automatische Stammdatenaktualisierung aktiviert / deaktiviert.
Timeout für Antwortzeiten der TI-Dienste	Gibt den Zeitwert in Sekunden an, nach dem die Verbindung zu VSDM-Diensten mit einem Timeout-Fehler abgebrochen wird. Der Standardwert ist 10. Der Minimalwert beträgt 1, während der Maximalwert 3000 Sekunden (50 Minuten) beträgt.
Maximale Bearbeitungszeit	Gibt den maximalen Zeitwert in Sekunden zur Ausführung der Operation ReadVSD an. Mit dieser Operation werden die Versichertenstammdaten aus einer elektronischen Gesundheitskarte ausgelesen. Der Minimalwert beträgt 1, während der Maximalwert 3000 Sekunden (50 Minuten) beträgt. Standard ist 30.
TI Offline Timeout	Gibt die maximal akzeptierte Zeit in Sekunden für eine fehlende Verbindung zur Telematikinfrastruktur an. Der Minimalwert beträgt 0, während der Maximalwert 3000 Sekunden (50 Minuten) beträgt.

Tabelle 89 VSDM-Protokoll

Fachmodul - VSDM-Protokoll	
Ablaufprotokollierung ab	Gibt die Mindestschwere eines generierten Protokolleintrags an, damit dieser in der Protokolldatenbank erfasst wird.
Mindestspeicherdauer des Ablaufprotokolls	Gibt die Anzahl der Tage (zwischen 10 und 365) an, nach denen Einträge aus dem Ablaufprotokoll gelöscht werden.

Tabelle 90 Performance-Protokoll

Performance-Protokoll	
Performance-Protokoll	Mit Hilfe dieses Schalters wird festgelegt, ob die Performance-Protokollierung des VSDM-Fachmoduls aktiviert sein soll oder nicht.

Tabelle 91 Mandanten-Schlüssel-Zuordnung

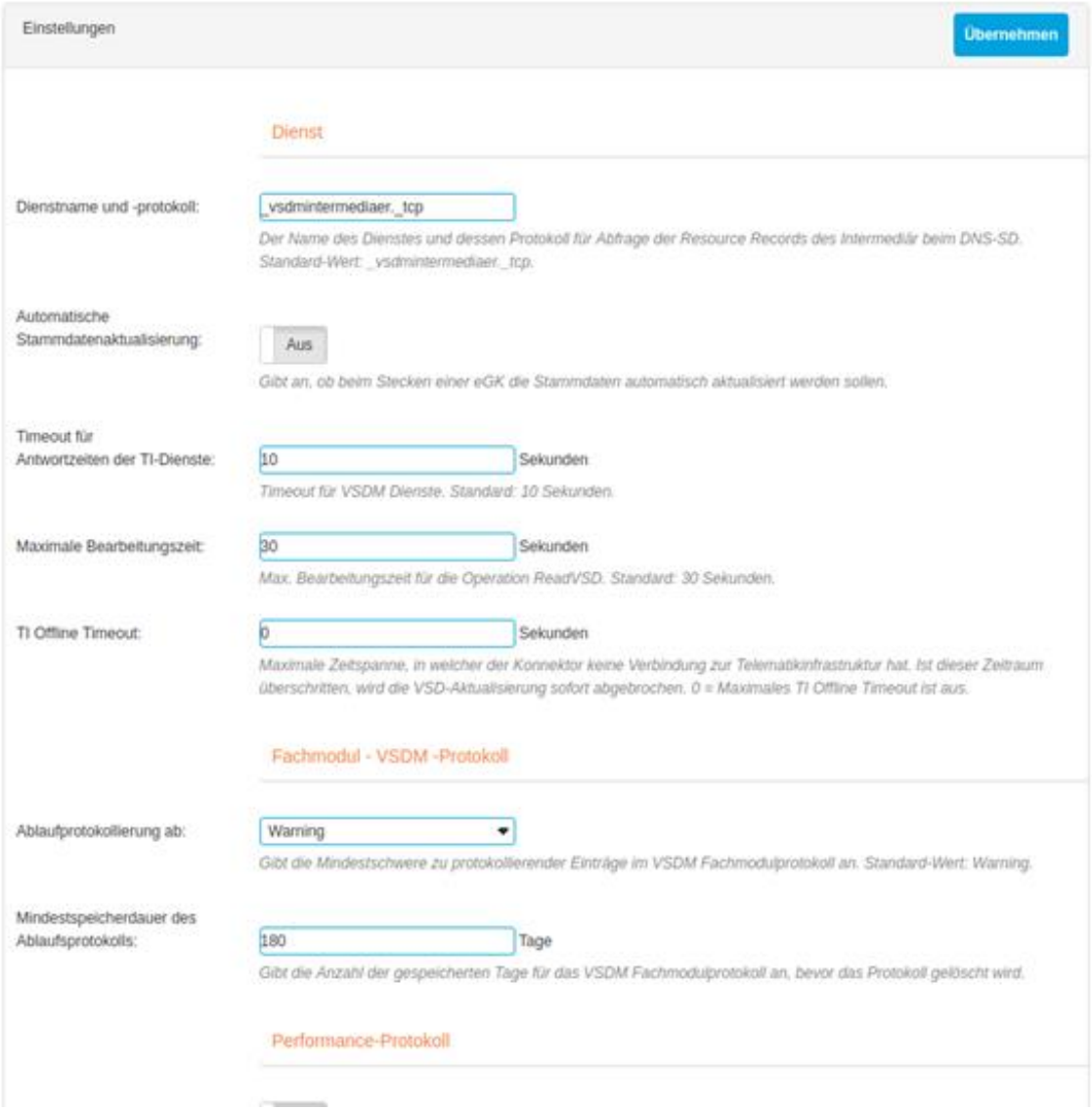
Mandanten-Schlüssel-Zuordnung	
Mandanten-Schlüssel	▪ In dieser Tabelle wird die Zuordnung zwischen einem Mandanten und einer SMB angegeben. Dies wird für den Anwendungsfall AutoUpdate-VSD und ReadVSD benötigt. ▪ Der Schlüssel für den Prüfungsnachweis muss 16 Ziffern lang sein. Er kann manuell eingegeben oder generiert werden. ▪ Zum automatischen Generieren eines Schlüssels klicken Sie zunächst auf die Schaltfläche Generieren, der generierte Schlüssel wird Ihnen dann direkt angezeigt. ▪ Falls Die den Schlüssel manuell festlegen möchten, geben Sie eine 16-stellige Ziffernkombination ein. ▪ Schließen Sie die Eingabe ab, indem Sie auf Übernehmen klicken.

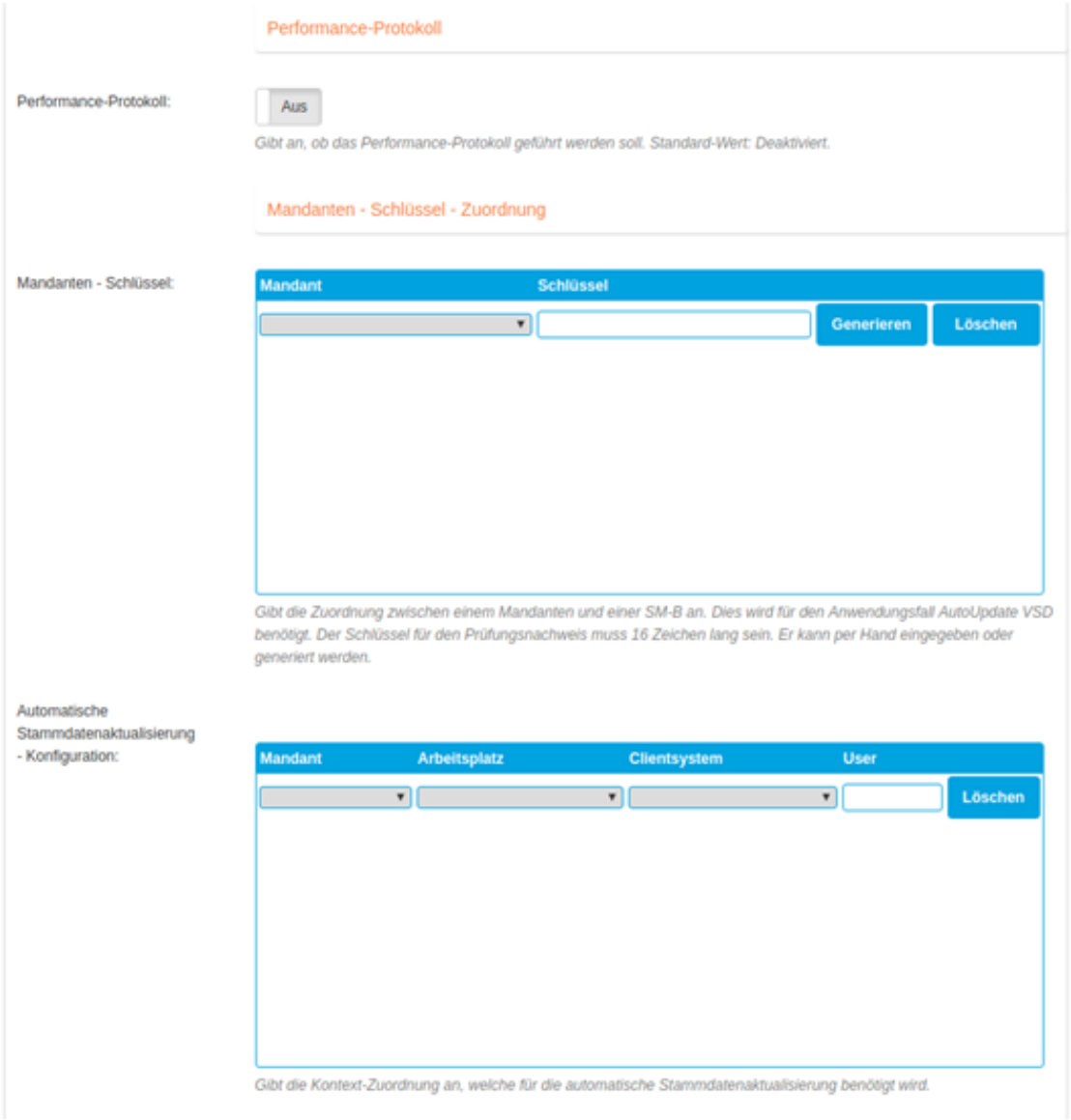
Tabelle 92 Einstellung der automatischen Stammdatenaktualisierung

Automatische Stammdatenaktualisierung – Konfiguration
Hier wird die Kontext-Zuordnung (Mandant - Arbeitsplatz - Clientsystem - User) vorgenommen, welche für die automatische Stammdatenaktualisierung benötigt wird.

Wurden Änderungen an der Konfiguration vorgenommen, können diese unter Verwendung der Schaltfläche Übernehmen zur Anwendung gebracht werden.

Übersicht der Default Einstellungen:


Einstellungen
Übernehmen
Dienst
Dienstname und -protokoll:
_vsdmintermediaer._tcp
Der Name des Dienstes und dessen Protokoll für Abfrage der Resource Records des Intermediär beim DNS-SD. Standard-Wert: _vsdmintermediaer._tcp.
Automatische Stammdatenaktualisierung:
Aus
Gibt an, ob beim Stecken einer eGK die Stammdaten automatisch aktualisiert werden sollen.
Timeout für Antwortzeiten der TI-Dienste:
10
Sekunden
Timeout für VSDM Dienste. Standard: 10 Sekunden.
Maximale Bearbeitungszeit:
30
Sekunden
Max. Bearbeitungszeit für die Operation ReadVSD. Standard: 30 Sekunden.
TI Offline Timeout:
0
Sekunden
Maximale Zeitspanne, in welcher der Konnektor keine Verbindung zur Telematikinfrastruktur hat. Ist dieser Zeitraum überschritten, wird die VSD-Aktualisierung sofort abgebrochen. 0 = Maximales TI Offline Timeout ist aus.
Fachmodul - VSDM -Protokoll
Ablaufprotokollierung ab:
Warning
Gibt die Mindestschwere zu protokollierender Einträge im VSDM Fachmodulprotokoll an. Standard-Wert: Warning.
Mindestspeicherdauer des Ablaufsprotokolls:
180
Tage
Gibt die Anzahl der gespeicherten Tage für das VSDM Fachmodulprotokoll an, bevor das Protokoll gelöscht wird.
Performance-Protokoll

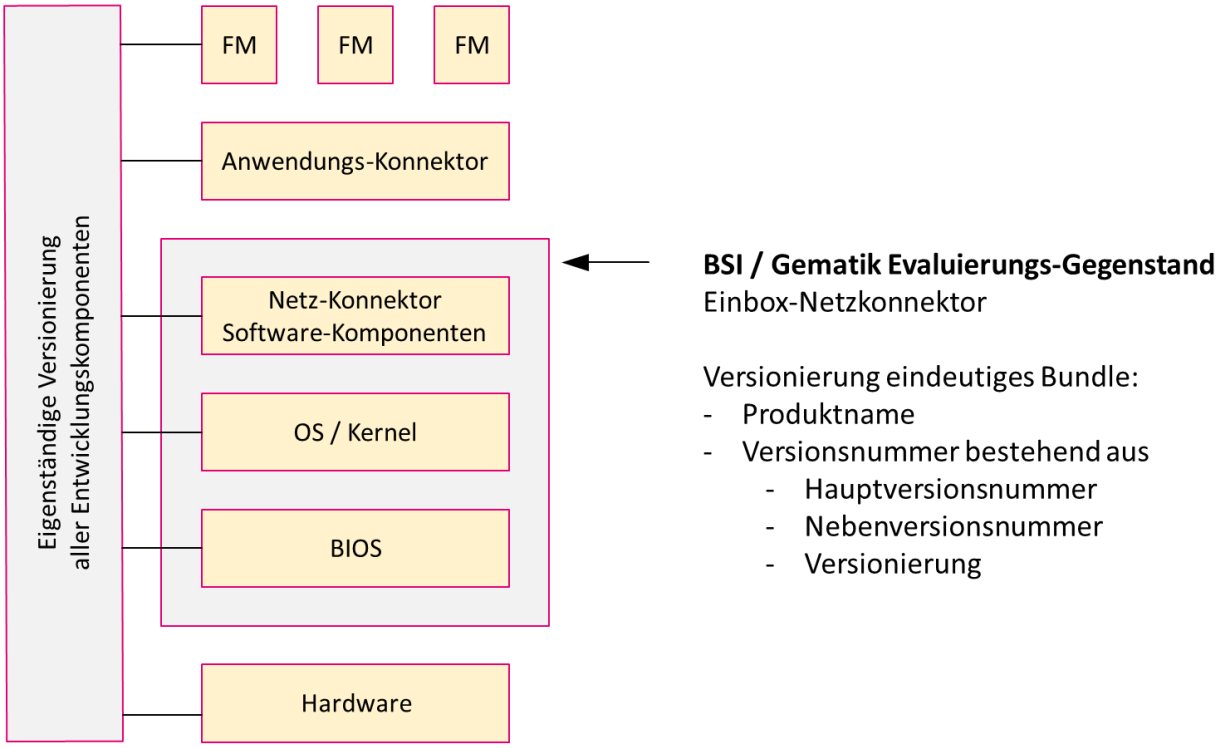

Performance-Protokoll
Performance-Protokoll:
Aus
Gibt an, ob das Performance-Protokoll geführt werden soll. Standard-Wert: Deaktiviert.
Mandanten - Schlüssel - Zuordnung
Mandanten - Schlüssel:
Mandant
Schlüssel
Generieren
Löschen
Gibt die Zuordnung zwischen einem Mandanten und einer SM-B an. Dies wird für den Anwendungsfall AutoUpdate VSD benötigt. Der Schlüssel für den Prüfungsnachweis muss 16 Zeichen lang sein. Er kann per Hand eingegeben oder generiert werden.
Automatische Stammdatenaktualisierung - Konfiguration:
Mandant
Arbeitsplatz
Clientsystem
User
Löschen
Gibt die Kontext-Zuordnung an, welche für die automatische Stammdatenaktualisierung benötigt wird.

9 Versionierung des Konnektors

In diesem Kapitel wird die Versionisierungsstrategie des Produktes "Konnektor" beschrieben. Die T-System versioniert das Produkt unabhängig von der Versionierung innerhalb der Entwicklung aus folgenden Gründen:

- Zukünftige Flexibilität für weitere Produkte
- Flexible Zusammenstellung von Einzelkomponenten zu einem Bundle
- Eineindeutige Referenzierung von Einzelkomponenten für Zertifizierungen / Zulassungen

Die Nomenklatur der Produktversion entspricht, wie unten dargestellt den Vorgaben der gematik und es wird aus der „offiziellen“ Version des Produkts-Managements eindeutig auf die Bestandteile der Komponenten aus der Entwicklung referenziert. Siehe dazu die beigefügte Tabelle im Dokument.



Im T-Systems-Entwicklungsprozess werden alle Komponenten jeweils mit eindeutiger Versionsnummer versehen. Diese Entwicklungs-Versionen stellen eine eindeutige Nachvollziehbarkeit zu einem Hard- und Softwareprodukt zu einem Entwicklungsstand und –Datum sicher.

Gegenstand der hier ausgeführten BSI-Zertifizierung sind innerhalb des T-Systems Einbox-Konnektors die Komponenten

- BIOS
- Betriebssystem / Kernel
- Software-Komponenten des Netz-Konnektors

Folgendes Beispiel verdeutlicht das oben beschriebene Konzept:

Produkt	Version	
Medical Acess Port_1BK	1.0.0	
	Unterkomponenten	Version
	Firmware	1.4.13
	Kernel	3.16.53
	Bios	S1.40.1.0

Die Kombination der o.g. Entwicklungskomponenten werden einer eindeutigen Versionsnummer im Rahmen der BSI-Zertifizierung und Zulassung zugeordnet. Die Versionsnummer setzt sich zusammen aus einem Produktnamen und einer Zahlenkombination, die GS-A_3695 konform aus den Bestandteilen Hauptversionsnummer, Nebenversionsnummer und Revisionsnummer aufgebaut ist.

Die nachfolgende Tabelle erläutert die einzelnen Bestandteile der Versionierung:

Aufbau	**Beschreibung**
Produktname	Wurde von T-Systems festgelegt: Medical Acess Port_1BK
Hauptversionsnummer	Wird erhöht, wenn signifikante Änderungen mindestens einer der Entwicklungskomponenten erfolgt sind und eine Neu-Zertifizierung erfordern.
Nebenversionsnummer	Wird erhöht, wenn kleinere Änderungen in der Funktionalität einer oder mehrerer Entwicklungskomponenten erfolgt sind und diese im Rahmen einer Re-Zertifizierung zertifiziert und zugelassen werden können.
Versionierung	Wird erhöht, wenn (notwendige) Patches oder Bugfixes erfolgt sind, die keinerlei Veränderung des nach außen sichtbaren Funktionsumfanges umfassen und insbesondere die Sicherheit und Stabilität des vorher zertifizierten und zugelassenen Konnektors sicherstellen.

Anmerkung: T-Systems ist bestrebt bereits im Vorfeld mit dem BSI ein gemeinsames Verständnis einer Versionsänderung zu gewinnen, bevor ein Sicherheitspatch oder eine Re-Zertifizierung angestoßen werden.

Die Zuordnung zwischen der Versionsnummer und den hierfür zugeordneten Entwicklungs-Versionen werden vom T-Systems Produkt-Owner verwaltet und sind für das BSI und die gematik auf Wunsch jederzeit einsehbar.

10 Fehlermeldungen

In diesem Kapitel wird ein Teil der auftretenden Fehlermeldungen und Hinweise zu deren Behebung aufgeführt.

Eine Übersicht über die gesamten Meldungen erhalten Sie in der ebenfalls mitgelieferten Schnittstellenspezifikation (17012018_OPB_KON_ThriftAPI_v1.1.pdf) des Netzkonnektors.

Die aufgeführten Meldungen können an mehreren Schnittstellen empfangen werden:

- Die Fehlermeldung kann im System- bzw. Sicherheitsprotokoll des Konnektors protokolliert werden.
- Die Fehlermeldung kann an der SOAP-Schnittstelle des Konnektors übermittelt werden.
- Die Fehlermeldungen können auf der Managementoberfläche angezeigt werden.

10.1 Fehlermeldungen des T-Systems Konnektor

10.1.1 Fehlermeldungen auf der Managementoberfläche

Tabelle 93 Fehlermeldungen auf der Managementoberfläche

Fehlermeldung & Ursache	Abhilfe
Falsche IP (Aufbau)	Bitte geben Sie eine gültige IP-Adresse ein. Beispiel: 192.168.0.12
Falsche IP (NULL-Eingabe)	Die eingegebene IP-Adresse darf nicht den Wert 0.0.0.0 haben.
Falsche Subnetzmaske	Subnetzmaske vom Nutzer ist ungültig. Bitte geben Sie eine gültige Subnetzmaske ein. Beispiel: 255.255.255.0.
Falsches IP-Netzwerk (Suffix-Schreibweise) ▪ Das Netz 0.0.0.0/0 ist nicht gültig; Wenn diese Adresse angegeben wurde. ▪ Netzwerk nicht gültig. Bitte geben Sie ein gültiges Netzwerk in Form IP-Adresse/Subnetzmaske ein. Beispiel: 192.168.1.0/24; Generell falscher Aufbau von IP-Netz	Bitte geben Sie ein gültiges Netzwerk in Form IP-Adresse / Subnetzmaske ein. Beispiel: 192.168.1.0 / 24.
Falsches IP-Netzwerk (mit ausgeschriebener Subnetzmaske)	Bitte geben Sie ein gültiges Netzwerk in Form IP-Adresse und Subnetzmaske ein. Beispiel: 192.168.1.0 und 255.255.255.0.
Start-IP-Adresse liegt nach der End-IP-Adresse (Angabe von IP-Ranges)	Die Start-IP Adresse muss vor der End-IP-Adresse sein.
Prüfung, ob eine IP-Adresse in einem Netzbereich liegt	Es kann nicht ermittelt werden, ob die gegebene IP im zulässigen IP-Bereich liegt (Der IP-Bereich muss wie folgt angegeben werden 1.2.3.4 / 24 oder 1.2.3.4 / 255.255.255.0).

Fehlermeldung & Ursache	Abhilfe
Falsche MAC-Adresse	Bitte geben Sie eine korrekte MAC-Adresse an. Beispiel: 1a:12:13:2d:23:df.
Falsche FQDN-Eingabe	Bitte geben Sie eine korrekte URL an. Bsp.: www.beispiel.de.
Falsche Eingabe in ein Textfeld	Bitte geben Sie einen Text ohne Sonderzeichen und Ziffern ein.
Falsche Eingabe eines numerischen Werts	Das Feld enthält keine Ganzzahl.
Falsche Eingabe eines positiven numerischen Werts	Das Feld enthält keine positive Ganzzahl.
Vorkommen eines nicht erlaubten Sonderzeichens in einem Textfeld	Dieses Zeichen darf nicht verwendet werden.
Eingabe eines zu kleinen numerischen Werts	Dieser Wert ist zu klein. Der Wert muss größer als (MINIMUM-WERT) sein.
Eingabe eines zu großen numerischen Werts	Dieser Wert ist zu groß. Der Wert muss kleiner als (MAX-WERT) sein.
Eingabe von numerischem Wert muss in Grenzen liegen	Dieser Wert muss zwischen (MIN) und (MAX) liegen.
Textfeldeingabe muss genaue Länge haben	Dieser Wert muss (WERT) Zeichen lang sein.

10.1.2 Allgemeine Fehlermeldungen

Tabelle 94 Allgemeine Fehlermeldungen

Code	Fehlermeldung & Ursache	Abhilfe
19803	Der angegebene Netzwerkrechner wurde mit ping nicht erreicht Der Rechner ist vom Konnektor aus nicht erreichbar. Die Ursache kann sein: keine Netzwerkroute zu anzupingendem Host (Zieladresse), der Host antwortet auf Ping-Anfragen nicht, der Host-Rechner ist einfach ausgeschaltet, etc.	Es ist keine Fehlermeldung, sondern eine negative Antwort auf die Ping-Anfrage.
19805	Informationen zu einem Netzwerk-Adapter konnten nicht ermittelt werden Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19806	Die eingegebene Adresse darf als NextHop-Adresse nicht verwendet werden Intranet-Route konnte nicht angelegt werden, weil die Next-Hop-Adresse nicht erreichbar bzw. nicht gültig ist	Überprüfen Sie die Next-Hop-Adresse der Route.
19807	Setzen der MTU für LAN fehlgeschlagen Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19809	Schwerwiegender Fehler: IP-Adressen konnten nicht gelöscht werden Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19810	Beim Setzen der Broadcast-Adresse ist ein Fehler aufgetreten Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19811	Status des VPN-Tunnels zur TI konnte nicht ermittelt werden Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19812	Status des VPN-Tunnels zum SIS konnte nicht ermittelt werden Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19813	Die IP-Adresse konnte nicht validiert werden Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19814	Subnetmaske konnte nicht ermittelt werden Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19815	IP-Adresse konnte nicht ermittelt werden Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19816	Das Netzwerk-Interface ist nicht definiert Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.

Code	Fehlermeldung & Ursache	Abhilfe
19817	Das CA Zertifikat des NK.ID nicht gefunden Interner Fehler, gSMC-K ist defekt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19818	Invalid NK.ID Zertifikat Interner Fehler, gSMC-K ist defekt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19819	Fehlerhafte Umgebungseinstellungen Interner Fehler, bei der Interpretation der Netzsegmente ist ein Fehler aufgetreten.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
4000	Syntaxfehler Fehler bei der Kommunikation mit dem Clientsystem	Kontakt zu Hersteller, siehe A.1.3.
4001	Interner Fehler Die Fehlerursache geht durch den Kontext bzw. den mitgelieferten Trace hervor	Kontakt zu Hersteller, siehe A.1.3.
4002	Der Konnektor befindet sich in einem kritischen Betriebszustand Durch den Betriebszustand können bestimmte Funktionen nicht ausgeführt werden.	Siehe 4.9.1

10.1.3 Fehlermeldungen Firewall

Tabelle 95 Fehlermeldungen Firewall

Code	Fehlermeldung & Ursache	Abhilfe
19083	Die Firewallregeln konnte nicht hinzugefügt werden. Die aktuelle Firewall-Konfiguration weist die eingegebene Regel ab. Die genaue Ursache wird der Fehlermeldung beigefügt.	Regel prüfen
19084	Das Protokoll der Firewallregeln ist nicht bekannt. Interner Fehler: Kann nur beim Ansteuern des Konnektors über Thrift-Schnittstelle vorkommen.	Kontakt zu Hersteller, siehe A.1.3.
19085	Die Option der Firewallregeln ist nicht bekannt. Interner Fehler: Kann nur beim Ansteuern des Konnektors über Thrift-Schnittstelle vorkommen.	Kontakt zu Hersteller, siehe A.1.3.
19086	Anpassung der Firewall fehlgeschlagen. Interner Fehler: Beim Aktivieren von Firewallregeln ist ein unerwarteter Fehler aufgetreten.	Kontakt zu Hersteller, siehe A.1.3.

10.1.4 Fehlermeldungen im Menü Administration und Registrierung

Tabelle 96 Fehlermeldungen im Menü Administration und Registrierung

Code	Fehlermeldung & Ursache	Abhilfe
16005 / 16006	Die Anmeldung war nicht erfolgreich. Bitte loggen Sie sich erneut ein! Software hat die Kombination aus Nutzername und Passwort nicht erkannt. Entweder nicht vorhanden oder Tippfehler.	Erneute Anmeldung mit einer gültigen Kombination aus Nutzername und Passwort am System.
16007	Die Sitzung ist nicht gültig. Bitte melden Sie sich erneut an. Es wird versucht, sich mit einer abgelaufenen Session anzumelden	Erneut am System mit Nutzernamen und Passwort anmelden.
16008	Der Administrator ist dem System nicht bekannt. Es wird versucht einen Administrator zu löschen, der im System nicht (mehr) vorhanden ist.	Da der Admin nicht mehr existiert, kann er nicht entfernt werden.
16009	Der Administrator ist bereits vorhanden. Bitte verwenden Sie eine andere Bezeichnung. Es wird versucht, einen Administrator hinzuzufügen, wobei der Nutzername für den Admin bereits verwendet wird.	Es sollte ein anderer Nutzername für den neuen Admin verwendet werden.
16010	Der Administrator ist nicht vorhanden. Es wird versucht, auf einen Admin-Account zuzugreifen, der nicht mehr existiert.	Da der Admin nicht mehr existiert, kann er nicht genutzt werden.
16011	Der letzte Superadministrator kann nicht entfernt oder zum normalen Administrator verändert werden. Es ist nur noch ein Superadmin im System vorhanden, der nicht gelöscht werden darf, da sonst keine Administrierung des Konnektors mehr möglich wäre.	Dieser Admin kann nicht gelöscht werden, bevor nicht ein anderer Superadmin im System vorhanden ist.
16012	Die beiden angegebenen neuen Passwörter stimmen nicht überein. Bei der Passwortänderung muss das neue Passwort doppelt angegeben werden (Sicherheit). Diese beiden angegebenen Passwörter stimmen nicht überein.	Angeben von zwei übereinstimmenden Passwörtern.
16013	Das neue Passwort kann nicht gesetzt werden, da es innerhalb der letzten 3 Male verwendet wurde. Das Passwort wurde für diesen Nutzer bei den letzten drei Passwortänderungen schon mal verwendet.	Es muss ein anderes Passwort eingegeben werden.
16014	Das neue Passwort ist zu kurz. Es muss mindestens 8 Zeichen besitzen.	Passwort muss mit mindestens 8 Zeichen angegeben werden.
16015	Die Zeichen eines Passworts müssen aus mindestens 3 der nachfolgenden Zeichenklassen stammen: Großbuchstaben, Kleinbuchstaben, Sonderzeichen, Ziffern	Anpassung des Passworts mit Zeichen von mindestens 3 der geforderten Zeichenklassen.

Code	Fehlermeldung & Ursache	Abhilfe
16016	Das Passwort darf nicht den Login-Namen enthalten (weder vorwärts noch rückwärts gelesen) Im Passwort wurde der Nutzername / Login-Name des Administrators angegeben	Im Passwort muss der Login-Name des zu ändernden Admins entfernt werden
16017	Das eingegebene aktuelle Passwort ist nicht korrekt.	Angabe des korrekten aktuellen Passworts
16018	Die Einstellungen konnten nicht vollständig exportiert werden. Interner Fehler	Kontakt zu Hersteller
16019	Die Einstellungen konnten nicht importiert werden. Bitte überprüfen Sie das Passwort.	Geben Sie Ihr Passwort korrekt ein.
16020	Die ausgewählten Benutzerrechte können dem ausgewählten Administrator nicht zugewiesen werden. Der Remote-Administrator hat nur eingeschränkte Rechte.	Korrigieren Sie Ihre Eingabe oder wenden Sie sich an Ihren Superadministrator
16021	Eingabefehler. Der Grund wird als Fehlertext mitgeliefert.	Korrigieren Sie die Eingabe.
16022	Die angegebene ICCSN ist nicht korrekt.	Zum Zurücksetzen der Passwörter ist die ICCSN nötig. Der Code ist in den Lieferunterlagen enthalten und befindet sich auf einem Aufkleber auf Ihrem Konnektor.

10.1.5 Fehlermeldungen im Menü Zertifikate

Tabelle 97 Fehlermeldungen im Menü Zertifikate

Code	Fehlermeldung & Ursache	Abhilfe
4127	TSL nicht gültig Import einer ungültigen TSL TSL passt nicht zum Vertrauensanker der installierten TSL	Gültige TSL importieren
4128	Der manuelle Import der TSL-Datei schlägt fehl	Gültige TSL importieren
4130	Signaturprüfung der CRL fehlgeschlagen CRL passt nicht zum installierten Vertrauensraums	Gültige CRL importieren. Überprüfung der Gültigkeit der TSL
4132	Extraktion des Ablaufdatums fehlgeschlagen Bei der Ermittlung des Ablaufdatums des Zertifikats ist ein Fehler aufgetreten.	Kontakt zu Hersteller, siehe A.1.3.
4196	Fehler bei der CV-Zertifikatsprüfung	Kontakt zu Hersteller, siehe A.1.3.

10.1.6 Fehlermeldungen im Menü VPN-Client

Tabelle 98 Fehlermeldungen im Menü VPN-Client

Code	Fehlermeldung & Ursache	Abhilfe
19001	TI: MGM_LU_ONLINE ist nicht aktiviert Konnektor befindet sich nicht im Online-Modus.	Konnektor in den Online-Modus versetzen (Konfiguration ändern).
19002	TI: Unbound ist nicht korrekt initialisiert Interner Fehler. Keine Namensauflösung möglich.	Neustart des Systems
19003	TI: Datei strongswan.conf konnte nicht erfolgreich erzeugt werden. Es konnte keine gültige Konfiguration für den VPN-Client erzeugt werden.	Kontakt zu Hersteller, siehe A.1.3.
19004	TI: Die Liste der Konzentratoren konnte nicht geladen werden. Es liegt ein Konfigurationsproblem vor. Der Konnektor konnte die Antwort des DNS-Servers nicht richtig auswerten.	Tunnelaufbau erneut versuchen
19005	TI: Keine Konzentratoren verfügbar. Es liegt ein Konfigurationsproblem vor. Der Konnektor konnte die Antwort des DNS-Servers nicht richtig auswerten.	Tunnelaufbau erneut versuchen
19006	TI: Fehler FQDN2IP Ein Namenseintrag (DNS) konnte nicht in eine IP-Adresse aufgelöst werden.	Tunnelaufbau erneut versuchen
19007	TI: Die Datei ipsec.conf konnte nicht erzeugt werden. Es konnte keine gültige Konfiguration für den VPN-Client erzeugt werden.	Kontakt zu Hersteller, siehe A.1.3.
19008	TI: Fehler VpnUP	Tunnelaufbau erneut versuchen
19011	TI: Fehler beim Erzeugen von ipsec.conf Es konnte keine gültige Konfiguration für den VPN-Client erzeugt werden.	Kontakt zu Hersteller, siehe A.1.3.
19015	Fehler beim Beenden der Verbindung zur TI. Der IPsec-Tunnel zur Telematikplattform konnte nicht richtig abgebaut werden.	Abbau erneut versuchen
19017	Fehler beim Holen des TI-Verbindungsstatus. Der Konnektor konnte den Verbindungsstatus zur Telematikplattform nicht ermitteln. Es ist nicht klar, ob der Konnektor einen aktiven Tunnel unterhält oder nicht.	Neustart des Systems

Code	Fehlermeldung & Ursache	Abhilfe
19019	VPN-Verbindung zur TI konnte nicht hergestellt werden. ▪ Die Verbindung zur Telematikplattform konnte nicht hergestellt werden. Mögliche Ursachen sind: ▪ Die Zeiteinstellungen des Konnektors sind nicht korrekt, ▪ es besteht keine Netzwerkverbindung, ▪ es sind Fehler bei den verwendeten Zertifikaten aufgetreten.	▪ Prüfung der Systemzeit, der Verbindung des Konnektors zum Netzwerk und Prüfung der System- und Sicherheitsprotokollierung. ▪ Prüfung, ob Protokolle weitere Hinweise auf die Ursache liefern, ggf. Tunnelaufbau erneut versuchen.
19020	Die Innere IP-Adresse des VPN-Tunnels zur TI konnte nicht ermittelt werden. Der Konnektor konnte eine Verbindung zur Telematikplattform herstellen, allerdings wurde die notwendige innere Tunnel-IP nicht zugewiesen. Mit diesem Fehler kann keine weitere Kommunikation mit der TI-Plattform stattfinden.	Tunnelaufbau erneut versuchen.
19021	Fehler beim Aufrufen von iptables allow TI Konzentrator Interner Fehler im Management der Firewall	Tunnelaufbau erneut versuchen.
19022	Fehler beim Aufrufen von iptables disallow TI Konzentrator Interner Fehler im Management der Firewall	Tunnelaufbau erneut versuchen.
19023	TI: Fehler beim GetAndAllowNextHashAndURLServer, keine Hash and URL Servers mehr ▪ Wenn der Konnektor so konfiguriert ist, dass das Verfahren Hash &URL verwendet werden soll, muss ein sog. Hash- &URL-Server zur Authentisierung des Endpunkts (Konzentrator) vorhanden sein. Die Fehlermeldung bedeutet, dass der betreffende Eintrag nicht vorhanden ist oder nicht gefunden wurde, sodass ein Aufbau des Tunnels zur Telematikinfrastruktur nicht möglich ist.	Tunnelaufbau erneut versuchen. Gegebenenfalls Nutzung des Verfahrens Hash &URL abschalten.
19051	SIS: Error fetching list of konzentrator Es liegt ein Konfigurationsproblem vor. Der Konnektor konnte die Antwort des DNS-Servers nicht richtig auswerten.	Tunnelaufbau erneut versuchen
19052	SIS: Fehler bei GetNamesrvAndDomainnameOfVPNServiceZone. Beim SIS-Tunnelaufbau ist ein Fehler von der Gegenseite festgestellt worden.	Kontakt zu Betreiber der TI
19053	SIS: Error FQDN2IP Ein Namenseintrag (DNS) konnte nicht in eine IP-Adresse aufgelöst werden.	Tunnelaufbau erneut versuchen.
19054	SIS: Error generating ipsec.conf Es konnte keine gültige Konfiguration für den VPN-Client erzeugt werden.	Kontakt zu Hersteller, siehe A.1.3.
19055	SIS: Error VpnUP	Kontakt zu Hersteller, siehe A.1.3.

Code	Fehlermeldung & Ursache	Abhilfe
	Interner Fehler	
19056	SIS: MGM_LU_ONLINE is not enabled Konnektor befindet sich nicht im Online-Modus.	Konnektor in den Online-Modus versetzen (Konfiguration ändern).
19057	SIS: MGM_LOGICAL_SEPARATION is NOT disabled, stopping Der Konnektor wurde zur Verwendung des Betriebsmodus logische Separation konfiguriert. Mit dieser Einstellung ist eine Verbindung zum sicheren Internetservice (SIS) nicht erlaubt.	Umkonfiguration des Konnektors oder Nutzung einer anderen Internetverbindung. Dieses Feature ist abgekündigt und soll nicht mehr verwendet werden.
19058	SIS: ANLW_INTERNET_MODUS is NOT SIS, stopping Der Konnektor ist nicht so konfiguriert, dass eine Verbindung zum sicheren Internetservice zulässig ist.	Umkonfiguration des Konnektors oder Nutzung einer anderen Internetverbindung.
19064	Error stopping connection to SIS Der IPsec-Tunnel zur Telematikplattform konnte nicht richtig abgebaut werden.	Abbau erneut versuchen.
19066	Error fetching SIS connection state Der Konnektor konnte den Verbindungsstatus zur Telematikplattform nicht ermitteln. Es ist nicht klar, ob der Konnektor einen aktiven Tunnel unterhält oder nicht.	Neustart des Systems
19072	SIS: Fehler beim GetAndAllowNextHashAndURLServer, keine Hash and URL servers mehr ▪ Wenn der Konnektor so konfiguriert ist, dass das Verfahren Hash &URL verwendet werden soll, muss ein sog. Hash- &URL-Server zur Authentisierung des Endpunkts (Konzentrator) vorhanden sein. Die Fehlermeldung bedeutet, dass der betreffende Eintrag nicht vorhanden ist oder nicht gefunden wurde, sodass ein Aufbau des Tunnels zur Telematikinfrastruktur nicht möglich ist.	Tunnelaufbau erneut versuchen. Ggf. Nutzung des Verfahrens Hash &URL abschalten.
19030	Error ipsec start Der VPN-Client konnte nicht gestartet werden.	Prüfung der VPN-Einstellungen, ggf. Neustart des Systems.
19031	Strongswan konnte nicht gestartet werden. Der VPN-Client konnte nicht gestartet werden.	Prüfung der VPN-Einstellungen, ggf. Neustart des Systems.
19032	Temporäre Datei ipsec.tmp konnte nicht gefunden und / oder gelöscht werden. Eine notwendige Konfigurationsdatei des VPN-Clients wurde nicht gefunden. Der VPN-Client kann nicht gestartet werden.	Möglicherweise verfügt das System nicht mehr über ausreichend Speicherplatz. Prüfung des verfügbaren Speicherplatzes und ggf. Löschen alter Protokolleinträge und FW-Updates zur Schaffung von Speicherplatz.
19033	Beim Ermitteln von VPN-Einstellungen ist ein Fehler aufgetreten.	Prüfung der VPN-Einstellungen auf Vollständigkeit.

Code	Fehlermeldung & Ursache	Abhilfe
	Es ist ein interner Fehler bei der Ermittlung der VPN-Einstellungen aufgetreten.	
19034	Die Initialisierung des VPN-Clients war nicht erfolgreich. Die Initialisierung des VPN-Clients ist fehlgeschlagen.	Prüfung der VPN-Einstellungen auf Vollständigkeit. Ggf. Neustart des Systems.
19035	Beim automatischen Ermitteln der URL (Hash-URL-Verfahren) schlug das Setzen der Konfigurationsparameter fehl. Der Aufbau eines VPN-Tunnels unter Verwendung des Verfahrens Hash &URL ist fehlgeschlagen.	Deaktivierung des Verfahrens Hash & URL in der Konfiguration des VPN-Clients und ggf. erneuter Versuch des Tunnelaufbaus.
19036	Das Zertifikat des Konzentrators ist im unerkannten Format Das vom VPN-Konzentrator erhaltene Zertifikat wurde vom Konnektor abgelehnt.	Kontakt zum PKI-Betreiber
19037	Das Zertifikat des TI-Konzentrators hat einen falschen FQDN Das vom VPN-Konzentrator erhaltene Zertifikat wurde vom Konnektor abgelehnt.	Kontakt zum PKI-Betreiber
19038	Das Zertifikat des TI-Konzentrators ist ungültig Das vom VPN-Konzentrator erhaltene Zertifikat wurde vom Konnektor abgelehnt.	Kontakt zum PKI-Betreiber
19039	Konzentrator meldet: authentication failed Das Zertifikat des Konnektors wurde vom VPN-Konzentrator abgelehnt.	Kontakt zu Hersteller, siehe A.1.3.
4172	Es ist keine Online-Verbindung zulässig. Die Konfiguration des Konnektors erlaubt derzeit keine Online-Verbindung.	▪ Konnektor für den Online-Betrieb konfigurieren; siehe Kapitel 4.9 ▪ Durchführen der Registrierung des Konnektors.
4173	Die CRL ist nicht mehr gültig (outdated).	Gültige CRL importieren
4174	TI-VPN-Tunnel: Verbindung konnte nicht aufgebaut werden ▪ keine gültige TSL ▪ keine Internetverbindung ▪ Konnektor ist nicht registriert ▪ Adresse des DNS-Resolvers nicht korrekt konfiguriert	▪ Überprüfen der Gültigkeit der TSL und ggf. eine gültige TSL importieren. ▪ Überprüfen der Netzwerkverbindung des Konnektors. Überprüfen der Netzwerkkonfiguration des Konnektors und ggf. korrigieren. ▪ Durchführen der Registrierung des Konnektors. ▪ Korrektur der Adresse des DNS-Resolvers.
4176	SIS-VPN-Tunnel: Verbindung konnte nicht aufgebaut werden ▪ keine gültige TSL ▪ keine Internetverbindung	▪ Überprüfen der Gültigkeit der TSL und ggf. eine gültige TSL importieren.

Code	Fehlermeldung & Ursache	Abhilfe
	▪ Konnektor ist nicht registriert oder nicht für den Sicheren Internet Service berechtigt ▪ Adresse des DNS-Resolvers nicht korrekt konfiguriert	▪ Überprüfen der Netzwerkverbindung des Konnektors. Überprüfen der Netzwerkkonfiguration des Konnektors und ggf. korrigieren. ▪ Durchführen der Registrierung des Konnektors. ▪ Korrektur der Adresse des DNS-Resolvers.

10.1.7 Fehlermeldungen im Menü LAN und WAN

Tabelle 99 Fehlermeldungen im Menü LAN und WAN

Code	Fehlermeldung & Ursache	Abhilfe
19101	Die WAN-IP-Adresse ist ungültig. Die eingegebene WAN-IP-Adresse ist nicht korrekt geschrieben oder liegt in einem nicht zugelassenen Netzwerksegment.	Überprüfung und ggf. Korrektur der eingegebenen IP-Adresse.
19109	Das Ändern des WAN-Netzes ist fehlgeschlagen. Die eingegebene WAN-IP-Adresse und/oder die Subnetzmaske ist / sind entweder syntaktisch nicht korrekt oder das WAN-Netz überschneidet sich mit einem der nicht zugelassenen Netzwerksegmente.	Überprüfung und ggf. Korrektur der eingegebenen IP-Adresse bzw. der Subnetzmaske.
19201	Die LAN-IP-Adresse ist ungültig Die eingegebene LAN-IP-Adresse ist nicht korrekt geschrieben oder liegt in einem nicht zugelassenen Netzwerksegment.	Überprüfung und ggf. Korrektur der eingegebenen IP-Adresse
19304	Die Intranet-Route konnte nicht gelöscht werden Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19306	Intranet-Route konnte weder angelegt noch geändert werden Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19309	Fehler beim Setzen der Intranet-Routen Interner Fehler. Ursache wird der Ausgabe beigefügt.	Korrektur des Routeneintrags
19313	Beim Netzwerk-Routen sind Fehler aufgetreten Das Anlegen der Netzwerk-Routen ist durchgelaufen, allerdings gab es Probleme, einige Routen anzulegen.	Routingtabelle im Abschnitt LAN / WAN kontrollieren und ggf. korrigieren.
19314	Ändern des LAN-Netzes fehlgeschlagen. Interner Fehler. Ursache wird der Ausgabe beigefügt.	Kontakt zu Hersteller, siehe A.1.3.
19315	Die IAG-Adresse ist nicht gültig Die als eingegebene Adresse des Gateways kann nicht als Gateway genutzt werden. Ursache wird der Ausgabe beigefügt.	Änderung der IAG-Adresse im Abschnitt LAN / WAN
19316	Die Routing-Adressen sind ungültig. Mehrere Ursachen möglich, z.B. fehlerhafte LAN- / WAN-Konfiguration	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19317	Der Abruf der Routing-Tabelle schlug fehl (evtl. leere Routing-Tabelle) Die Routing-Tabelle kann nicht angezeigt werden. Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.

Code	Fehlermeldung & Ursache	Abhilfe
4162	Es liegt eine fehlerhafte LAN-IP-Konfiguration vor.	1. Korrektur der LAN-IP-Konfiguration; siehe Kapitel 6.2.
4163	Es liegt eine fehlerhafte WAN-IP-Konfiguration vor.	Korrektur der WAN-IP-Konfiguration; siehe Kapitel 6.2.
4164	Beim Aktualisieren oder Aktivieren der Firewallregeln ist es zu einem Fehler gekommen.	Kontakt zu Hersteller, siehe A.1.3.
4167	CreateRoutes: Ein oder mehrere Adressen sind ungültig Beim Einrichten der Netzwerkrouten wurde eine ungültige oder eine fehlende IP-Adressen-Konfiguration festgestellt.	Korrektur der Netzwerkkonfiguration

10.1.8 Fehlermeldungen im Menü Namensdienst

Tabelle 100 Fehlermeldungen im Menü Namensdienst

Code	Fehlermeldung & Ursache	Abhilfe
19704	Die Konfigurationsdatei des DNS-Servers kann nicht geöffnet werden. Zugriffsfehler beim Versuch, die Konfigurationsdatei zum Lesen zu öffnen.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19705	Die Konfigurationsdatei des DNS-Servers kann nicht geschrieben werden. Zugriffsfehler beim Versuch, die Konfigurationsdatei zum Schreiben zu öffnen.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19707	Der Neustart des DNS-Servers schlug fehl. Starten des DNS-Servers nach der Neukonfiguration schlug fehl.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19708	Das Laden der DNS-Einstellungen ist fehlgeschlagen Beim Einlesen der DNS-Konfigurationsparameter ist ein unerwarteter Fehler aufgetreten.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19709	Der konfigurierte Trust Anchor konnte nicht heruntergeladen werden. Interner Fehler; Eventuell ist die Netzwerkverbindung gestört.	Überprüfen Sie die Netzwerkkonfiguration. Wenden Sie sich an den Hersteller, siehe A.1.3.
19710	Der DNSKEY-Eintrag konnte nicht über die konfigurierten DNS-Server beschafft werden. Interner Fehler.	Überprüfen Sie die Netzwerkkonfiguration des DNS- Servers bzw. wenden Sie sich an den Hersteller, siehe A.1.3.
19711	Bei der Verifikation der DNSKEY-Einträge gegen den Trust Anchor ist ein Fehler aufgetreten. Interner Fehler	Kontakt zu Hersteller, siehe A.1.3.
19712	Der Vertrauensraum für DNS im öffentlichen Netz ist nicht korrekt initialisiert. Interner Fehler	Kontakt zu Hersteller, siehe A.1.3.
4179	DNS: Anfrage wurde abgebrochen, da der Timeout von ANLW_SERVICE_TIMEOUT Sekunden überschritten wurde.	▪ Überprüfung Sie folgende Punkte: ▪ Netzwerkkonfiguration ▪ konfigurierte URLs ▪ Netzwerkverbindung
4180	DNS: Es ist ein Fehler bei der Namensauflösung aufgetreten	▪ Überprüfung Sie folgende Punkte: ▪ Netzwerkkonfiguration ▪ konfigurierte URLs ▪ Netzwerkverbindung

10.1.9 Fehlermeldungen im Menü Protokollierung

Tabelle 101 Fehlermeldungen im Menü Protokollierung

Code	Fehlermeldung & Ursache	Abhilfe
4150	Fehler beim Schreiben des Systemprotokolls	Kontakt zu Hersteller, siehe A.1.3.
4151	Fehler beim Schreiben eines Fachmodulprotokolls	Kontakt zu Hersteller, siehe A.1.3.
4152	Fehler beim Schreiben des Sicherheitsprotokolls	Kontakt zu Hersteller, siehe A.1.3.
4216	Fehler beim Schreiben des Konnektor Performanceprotokolls	Kontakt zu Hersteller, siehe A.1.3.
4217	Fehler beim Schreiben eines Fachmodul Performanceprotokolls	Kontakt zu Hersteller, siehe A.1.3.
4153	Zugriff auf Sicherheitsprotokoll nicht möglich	Kontakt zu Hersteller, siehe A.1.3.
4154	Zugriff auf Systemprotokoll nicht möglich	Kontakt zu Hersteller, siehe A.1.3.
4155	Zugriff auf Fachmodulprotokolle nicht möglich	Kontakt zu Hersteller, siehe A.1.3.
4218	Zugriff auf Konnektor-Performanceprotokoll nicht möglich	Kontakt zu Hersteller, siehe A.1.3.
4219	Zugriff auf Fachmodul-Performanceprotokoll nicht möglich	Kontakt zu Hersteller, siehe A.1.3.

10.1.10 Fehlermeldungen im Menü DHCP-Client

Tabelle 102 Fehlermeldungen im Menü DHCP-Client

Code	Fehlermeldung & Ursache	Abhilfe
19501	Es kam zu einem Timeout beim Zuweisen einer IP an der LAN-Schnittstelle. Es wurde eine Default-IP vergeben. Zeitüberschreitung beim Ermitteln der neuen IP über DHCP-Client (DHCP_lease)	Überprüfen Sie, ob der Konnektor an das Netzwerk des Leistungserbringers angeschlossen ist und ob in diesem Netzwerk ein DHCP-Server vorhanden ist.
19510	Es existiert bereits eine DHCP-Gruppe mit dem gleichen IP-Adressbereich. Der eingegebene Adressbereich der neuen Clientgruppe überschneidet sich mit dem Adressbereich einer bereits angelegten Clientgruppe.	Passen Sie den Adressbereich der neuen Clientgruppe so an, dass dieser mit den anderen Clientgruppen in keinem Konflikt steht.
19511	Es trat ein Fehler beim Anlegen der Client-Gruppe auf Ursache wird der Ausgabe beigefügt.	Überprüfen Sie die Parameter der neuen Clientgruppe.
19512	Der Status des DHCP-Clients konnte nicht ermittelt werden. Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
4169	Konnektor erhält keine DHCP- Informationen kein Fehler des Konnektors Fehlkonfiguration am externen DHCP-Server	Korrektur der Konfiguration des externen DHCP-Servers
4170	Konnektor besitzt identische IP-Adressen am WAN- und LAN-Interface LAN und WAN liegen im gleichen Netz die Konfiguration im Konnektor oder im externen DHCP-Server ist nicht korrekt	Korrektur der Netzwerkkonfiguration im Konnektor bzw. im externen DHCP- Servers

10.1.11 Fehlermeldungen im Menü DHCP-Server

Tabelle 103 Fehlermeldungen im Menü DHCP-Server

Code	Fehlermeldung & Ursache	Abhilfe
19605	Der DHCP-Server kann nicht gestartet werden, weil der DHCP-Client am LAN- Interface aktiv ist. Es wurde versucht, den DHCP- Server auf der LAN–Seite zu starten, während der DHCP-Client am LAN aktiv war.	Deaktivieren Sie zuerst den DHCP-Client und vergeben Sie eine statische IP-Adresse am LAN-Interface. Anschließend kann der DHCP-Server des Leistungserbringer- Netzes aktiviert werden.
19607	Der DHCP-Server konnte nicht neu gestartet werden. Bei dieser Fehlermeldung wird die Ausgabe des DHCP-Servers, welche die Ursache möglicherweise beschreibt, an die Fehlermeldung angehängt.	Überprüfen Sie die Konfiguration des DHCP-Servers und versuchen Sie erneut ihn zu starten.
4168	DHCP-Server konnte nicht gestartet werden Interner Fehler.	Kontakt zu Hersteller, siehe A.1.3.

10.1.12 Fehlermeldungen im Menü Datum und Uhrzeit

Tabelle 104 Fehlermeldungen im Menü Datum und Uhrzeit

Code	Fehlermeldung & Ursache	Abhilfe
19401	Der System-Service ntpd konnte nicht aufgerufen werden. Der NTP-Server des Konnektors konnte nicht gestartet werden. Der Konnektor stellt demzufolge kein Zeitsignal an Clients im Netz des Leistungserbringers bereit.	Neustart des Systems
19404	Der NTP-Service konnte nicht gestartet werden Der NTP-Server des Konnektors konnte nicht gestartet werden. Der Konnektor stellt demzufolge kein Zeitsignal an Clients im Netz des Leistungserbringers bereit.	Neustart des Systems
19405	Der NTP-Service konnte nicht angehalten werden Der Zeitdienst konnte nicht gestoppt werden.	Neustart des Systems
19407	Abweichung der lokalen Zeit zu der Hardware-Clock zu groß. Übergang in den kritischen Zustand Der Konnektor synchronisiert die Uhrzeit mit einem Hardware- Baustein. Die Zeitdifferenz zwischen Konnektor Uhrzeit und der von der Hardware verwalteten Uhrzeit ist zu groß und muss neu synchronisiert werden.	Manuelles Einstellen der Zeit kann das Problem beheben oder erneute Synchronisation mit dem Zeitdienst im Netz der Telematikplattform. Letzteres erfolgt automatisch bei Aufbau eines Tunnels in die Telematikinfrastruktur.
19409	Konvertierung der Hardware-Zeit des Konnektors fehlgeschlagen ▪ Die Ausgabe des Programms hw-clock kann nicht in eine gültige Zeit konvertiert werden. Mögliche Ursachen sind entweder eine fehlerhafte Systemkonfiguration (konnektor.nk.ini passt nicht zu der externen Software, wie date / hwclock etc.) oder defekte Hardware (z.B. die Uhr).	Konnektor-Update durchführen bzw. Hersteller kontaktieren, siehe A.1.3.
19411	Synchronisierung der Software- und der Hardware-Uhr des Konnektors fehlgeschlagen Die Zeitsynchronisation zwischen Hardware und Konnektorsoftware konnte nicht vorgenommen werden. Die vom Konnektor angegebene Uhr- zeit ist ggf. nicht zuverlässig.	Erneuter Versuch, die Uhrzeit zu synchronisieren.
19415	Die eingegebene Zeit kann nicht gesetzt werden Diese Meldung kann auftreten, wenn über die Managementoberfläche die Uhrzeit manuell eingestellt wird. Im Vorgang der Synchronisation ist ein Fehler aufgetreten.	Erneuter Versuch der manuellen Synchronisation
19417	Der Server für die Zeitsynchronisierung konnte nach dem Zurücksetzen der Konfiguration nicht neu gestartet werden Der NTP-Server des Konnektors konnte nicht gestartet werden. Der Konnektor stellt demzufolge kein Zeitsignal an Clients im Netz des Leistungserbringers bereit.	Neustart des Systems

Code	Fehlermeldung & Ursache	Abhilfe
19418	Die Zeitzonenangabe ist nicht gültig	Angabe einer korrekten Zeitzone
19419	Abweichung der lokalen Zeit zu der Serverzeit ist zu groß. Übergang in den kritischen Zustand Der Konnektor hat eine Zeitsynchronisierung gestartet, jedoch war die Abweichung der Konnektor Zeit von der Serverzeit größer als 60 Minuten.	Erneute Synchronisation mit dem Zeitdienst in der Telematikinfrastruktur.
19420	Synchronisierung der Zeit des Konnektors fehlgeschlagen Der Konnektor konnte seine Zeit weder mit dem ersten noch mit dem zweiten Server der TI synchronisieren.	Überprüfung der VPN-Verbindungen des Konnektors und ggf. Wiederholung des Synchronisierungsvorgangs.
19421	Fehler beim Setzen der Systemzeit Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
19422	Konfiguration des NTP-Dienstes ist fehlerhaft oder nicht vollständig Die Konfiguration des Zeitdienstes auf dem Konnektor ist fehlerhaft.	Neustart des Systems / Kontakt zu Hersteller, siehe A.1.3.
4177	Der NTP-Server des Konnektors konnte nicht synchronisiert werden.	Stellen Sie eine Verbindung zur TI her
4178	Das Fachmodul konnte die aktuelle Systemzeit des Konnektors nicht abrufen. Interner Fehler.	Kontakt zu Hersteller, siehe A.1.3.

10.1.13 Fehlermeldungen im Menü Update

Tabelle 105 Fehlermeldungen im Menü Update

Code	Fehlermeldung & Ursache	Abhilfe
4181	Integritätsprüfung UpdateInformation fehlgeschlagen.	Kontakt zu Hersteller, siehe A.1.3.
4182	Download nicht aller UpdateFiles möglich.	Kontakt zu Hersteller, siehe A.1.3.
4183	Integritätsprüfung UpdateFiles fehlgeschlagen.	Kontakt zu Hersteller, siehe A.1.3.
4184	Anwendung der UpdateFiles fehlgeschlagen.	Kontakt zu Hersteller, siehe A.1.3.
4185	Firmware-Version liegt außerhalb der gültigen Firmwaregruppe ▪ Versuch eines Firmwareupgrades mit einer Firmwareversion aus einer veralteten Firmwaregruppe	Upgrade mit aktuellem Firmwarepaket
4186	Download nicht aller UpdateFiles möglich. ▪ Netzwerkverbindung in die TI unterbrochen	Herstellung der Netzwerkverbindung und erneutes Anstoßen der Kartenterminalaktualisierung
4187	KT-Update fehlgeschlagen ▪ Netzwerkverbindung zum Kartenterminal unterbrochen ▪ Kartenterminalfehler	▪ Herstellung der Netzwerkverbindung zum Kartenterminal und erneutes Anstoßen der Kartenterminalaktualisierung ▪ Kontakt zu Hersteller des Kartenterminals
4188	Konfigurationsdienst nicht erreichbar, konfigurierte Adresse kontrollieren.	▪ Korrektur der URL des Konfigurationsdienstes in der TI ▪ Überprüfung der Netzwerkverbindung
4189	Konfigurationsdienst liefert falsches Zertifikat Interner Fehler	Kontakt zu Hersteller, siehe A.1.3.
4190	Fehler beim Beziehen der Updatelisten Interner Fehler	Kontakt zu Hersteller, siehe A.1.3.
4198	Beim Übernehmen der Bestandsnetze ist ein Fehler aufgetreten Interner Fehler	Kontakt zu Hersteller, siehe A.1.3.

10.1.14 Fehlercodes kritischer Fehler (Hardwaredisplay)

Tabelle 106 Fehlercodes kritischer Fehlern (Hardwaredisplay)

Code	Fehlermeldung & Ursache	Abhilfe
0	EC_Software_Integrity_Check_Failed	Siehe Kapitel 4.9.1.
1	EC_Random_Generator_Not_Reliable	Siehe Kapitel 4.9.1.
2	EC_Security_Log_Not_Writable	Siehe Kapitel 4.9.1.
3	EC_Time_Sync_Pending_Critical	Siehe Kapitel 4.9.1.
4	EC_Time_Difference_Intolerable	Siehe Kapitel 4.9.1.
5	EC_CRL_Out_Of_Date	Das CRL-Zertifikat ist nicht mehr gültig und muss aktualisiert werden.
6	EC_TSL_Out_Of_Date_Beyond_Grace_Period	Siehe Kapitel 4.9.1.
7	EC_TSL_Trust_Anchor_Out_Of_Date	Siehe Kapitel 4.9.1.
8	EC_Firewall_Not_Reliable	Siehe Kapitel 4.9.1.
9	EC_Secure_KeyStore_Not_Available	Siehe Kapitel 4.9.1.
20	EC_CardTerminal_Not_Available	Siehe Kapitel 4.9.1.
21	EC_No_VPN_TI_Connection	Der TI-Tunnel ist nicht aufgebaut (manuell getrennt bzw. Tunnel-Aufbau wurde abgebrochen)
22	EC_No_VPN_SIS_Connection	Der SIS-Tunnel ist nicht aufgebaut. Ein Tunnel-Aufbau nicht möglich, da der VPN-Tunnel zum SIS erst aufgebaut werden kann, wenn der VPN-Tunnel zur TI aufgebaut ist.
23	EC_No_Online_Connection	Siehe Kapitel 4.9.1.
24	EC_FeatureOrTUC_Not_Available	Siehe Kapitel 4.9.1.
25	EC_IP_Adresses_Not_Available	Siehe Kapitel 4.9.1.
40	EC_LOG_OVERFLOW	Siehe Kapitel 4.9.1.
41	EC_CRL_Expiring	Siehe Kapitel 4.9.1.
42	EC_Time_Sync_Pending_Warning	Siehe Kapitel 4.9.1.
43	EC_TSL_Out_Of_Date_Within_Grace_Period	Siehe Kapitel 4.9.1.
44	EC_CRYPTOPERATION_ALARM	Siehe Kapitel 4.9.1.
60	EC_TSL_Expiring	Siehe Kapitel 4.9.1.

Code	Fehlermeldung & Ursache	Abhilfe
61	EC_TSL_Update_Not_Successful	Siehe Kapitel 4.9.1.
62	EC_TSL_Trust_Anchor_Expiring	Siehe Kapitel 4.9.1.
63	EC_CardTerminal_Software_Out_Of_Date	Die auf dem Kartenterminal installierte Software ist nicht mehr aktuell und muss aktualisiert werden.
64	EC_Connector_Software_Out_Of_Date	Siehe Kapitel 4.9.1.
65	EC_Time_Sync_Not_Successful	Siehe Kapitel 4.9.1.

10.1.15 Fehlercodes während des Startvorgangs (Hardwaredisplay)

Tabelle 107 Fehlercodes während des Startvorgangs (Hardwaredisplay)

Code	Fehlermeldung Klartext	Fehlermeldung & Ursache	Abhilfe
90	INIT_HARDWARETEST_FAILED	Hardware Test schlug fehl	Kontakt zu Hersteller, siehe A.1.3.
91	INIT_GSMCK_NOT_AVAIL	Die gSMC-K ist nicht verfügbar	Kontakt zu Hersteller, siehe A.1.3.
92	INIT_GSMCK_DEACTIVATED	Die gSMC-K ist deaktiviert	Kontakt zu Hersteller, siehe A.1.3.
93	INIT_ACTIVATION_FAILED	Aktivierung des Konnektors schlug fehl	Kontakt zu Hersteller, siehe A.1.3.
94	BOOT_INTEGRITYTEST_FAILED	Fehlerhafter Integritätstest beim Bootvorgang	Kontakt zu Hersteller, siehe A.1.3.
95	BOOT_SERVICES_NOT_AVAIL	Boot Service steht nicht zur Verfügung	Kontakt zu Hersteller, siehe A.1.3.
96	BOOT_FATAL	Boot Fehler	Kontakt zu Hersteller, siehe A.1.3.
99	Reservierter Fehlercode für Secure-BIOS-Fehler	Reservierter Fehlercode für Secure-BIOS-Fehler	Kontakt zu Hersteller, siehe A.1.3.

Hinweis: Der Startvorgang wird bei dem ersten Fehler unterbrochen und der Fehlercode ist auf der 7-Segmentanzeige sichtbar.

A Anhang

A.1 Kontakt

A.1.1 PKI-Betreiber

Tabelle 108 Kontakt PKI-Betreiber

PKI-Betreiber	
T-Systems International GmbH	
Adresse:	Hahnstraße 43d, 60528 Frankfurt am Main
Hotline:	0800-1183307
E-Mail:	service.map@telekom.de

A.1.2 Herausgeber

Tabelle 109 Kontakt Herausgeber

Herausgeber	
T-Systems International GmbH	
Adresse:	Hahnstraße 43d, 60528 Frankfurt am Main
Hotline:	0800-1183307
E-Mail:	service.map@telekom.de

A.1.3 Hersteller

Tabelle 110 Kontakt Hersteller

Hersteller	
T-Systems International GmbH	
Adresse:	Hahnstraße 43d, 60528 Frankfurt am Main
Hotline:	0800-1183307
E-Mail:	service.map@telekom.de

A.2 Konformitätsangaben

A.2.1 CE-Zeichen

Hiermit erklärt die T-Systems International GmbH, dass der T-Systems Konnektor den Richtlinien **2014/53/EU**, **2009/125/EG** sowie **2011/65/EU** entspricht.

A.2.2 TÜV-Zertifikat

Das **TÜV Certified Green Product-Label** wird vom TÜV Rheinland vergeben und zertifiziert - neben der Produktsicherheit und der Einhaltung sozialer Standards durch den Hersteller- die wesentlichen umweltrelevanten Produkteigenschaften des Produktes. Dies sind insbesondere: Der Energieverbrauch und die Energieeffizienz, die Berücksichtigung der Treibhausgasemissionen über die Erstellung einer CO2-Bilanz, die Bewertung des Anteils recyclebarer Materialen für die Wiederverwendung und der verantwortliche Umgang mit chemischen Inhaltsstoffen.

A.3 Rücknahme von alten Geräten

Wird der Konnektor dauerhaft entsorgt, muss vorher die gSMC-K zerstört werden, da dort vertrauenswürdige Daten gespeichert sind.

Hat Ihr T-Systems Konnektor ausgedient, bringen Sie das Altgerät zur Sammelstelle Ihres kommunalen Entsorgungsträgers (z. B. Wertstoffhof). Nach dem Elektro- und Elektronikgerätegesetz sind Besitzer von Altgeräten gesetzlich gehalten, alte Elektro- und Elektronikgeräte einer getrennten Abfallerfassung zuzuführen. Helfen Sie bitte mit und leisten einen Beitrag zum Umweltschutz, indem Sie das Altgerät nicht über den Hausmüll entsorgen.

Die T-Systems International GmbH ist bei der Stiftung Elektro-Altgeräte Register unter WEEE-Reg.-Nr. DE 50478376 registriert.

Hinweis für den Entsorgungsträger: Das Datum der Herstellung bzw. des Inverkehrbringens ist auf dem Typenschild nach DIN EN 60062, Ziffer 5, angegeben.

A.4 Technische Daten

Tabelle 111 Produktdetails

Allgemein	
Modell	T-Systems Konnektor
Firmware	Version 1.4.13
Hardware	Version 2.2.4

Tabelle 112 Technische Daten

Technische Daten	
Prozessor	
CPU	INTEL Atom (E3845) Quad-Core
Taktfrequenz	1,91 GHz
Anzahl der CPUs	1
Flüchtiger Arbeitsspeicher	
Speicherkapazität	4 GByte DDR3
Nicht-Flüchtiger Speicher	
Speichertyp	Flash eMMC
Speicherkapazität	4 GByte
Durchschnittliche Lese-/Schreibgeschwindigkeit	▪ 30 MB/s Lesen ▪ 8 MB/s Schreiben
Schnittstellen	
Ethernet	2 x RJ45 / 10/100/1000 MBit
Netzteil / Versorgungsspannung	
Extern oder intern	Externes Kabelnetzteil
Spannung	230V
gSMC-K	
Chip	Infineon SLE78CLX1440P
Karte	Gem. gematik_gSMCK-G2_2016-11-24_00132

A.5 Lizenzinformationen

Dieses Produkt enthält urheberrechtlich geschützte Software. Es sind sowohl proprietäre als auch Open-Source-Programme enthalten. Bitte beachten Sie die Lizenzinformationen in der Administrations-Oberfläche unter dem Menüpunkt Systeminformationen.

Sollten Sie unvorhergesehener Weise keinen Zugriff auf die Lizenzinformationen haben, können Sie die Lizenzinformationen von service.map@telekom.de anfordern.

Herausgeber

T-Systems International GmbH

Adresse: Hahnstraße 43d, D-60528 Frankfurt am Main, Germany

A.6 Hinweise zur Sicherheitszertifizierung des Produkts

In der nachfolgenden Aufstellung werden Hinweise angegeben, die in Verbindung mit der erfolgten sicherheitstechnischen Evaluierung des Produktes nach Common Criteria stehen. Diese Hinweise sind weitgehend den Sicherheitsvorgaben des Herstellers zum Produkt T-Systems Konnektor entnommen.

A.6.1 Externer Zufallszahlengenerator

Die Umgebung stellt dem Konnektor einen externen Zufallszahlengenerator bereit, der Zufallszahlen geprüfter Güte und Qualität gemäß den Anforderungen der Klassen PTG.2 oder PTG.3 liefert. Im konkreten Einsatzfall wird dies durch die gSMC-K sichergestellt. Die gSMC-K wird als externer Zufallszahlengenerator angesteuert.

Die gSMC-K muss dem Konnektor zur Verfügung stehen. Achten Sie darauf, dass die Sicherheitssiegel des Geräts unbeschädigt sind.

A.6.2 Echtzeituhr

Der Konnektor verfügt über eine Echtzeituhr, die synchronisiert werden kann. Die Echtzeituhr erfüllt die Anforderungen zur Freilaufgenauigkeit gemäß Schutzprofil.

Sie müssen darauf achten, dass keine Manipulationen an der Hardware des Geräts erfolgen. Entsprechende Hinweise finden Sie im vorliegenden Handbuch.

A.6.3 Zeitsynchronisation

Die TI-Umgebung (die zentrale Telematikinfrastruktur-Plattform) stellt einen Dienst bereit (Zeitserver (NTP-Server), die über einen VPN-Konzentrator für den Zugang zur Telematikinfrastruktur erreichbar sind), mit dessen Hilfe der Konnektor die Echtzeituhr gemäß OE.NK.Echtzeituhr synchronisieren kann. Dieser Dienst verfügt über eine verlässliche Systemzeit und ist über einen sicheren Kanal erreichbar (Zeitserver stehen innerhalb der Telematikinfrastruktur). Um den Dienst der sicheren Zeitsynchronisation zu nutzen, muss eine Verbindung zur Telematikinfrastruktur hergestellt werden.

Sie sollten regelmäßig eine Verbindung zur Telematikplattform herstellen, um den gesicherten Zeitdienst in Anspruch zu nehmen. Erfolgt dies nicht, kann der Konnektor die Korrektheit der Zeitangaben nicht sicherstellen.

A.6.4 Sicherheitsmodul gSMC-K

Der T-Systems Konnektor hat Zugriff auf ein Sicherheitsmodul (gSMC-K), das sicher mit dem Konnektor verbunden ist. Sicher bedeutet in diesem Fall, dass die gSMC-K nicht unbemerkt vom Konnektor getrennt und dass die Kommunikation zwischen gSMC-K und Konnektor weder mitgelesen noch manipuliert werden kann. Die gSMC-K dient als Schlüsselspeicher für das Schlüsselmaterial, welches die kryptografische Identität des Konnektors repräsentiert und auch für O.NK.VPN_Auth verwendet wird. Zudem führt die gSMC-K kryptografische Operationen mit diesem Schlüsselmaterial durch (Authentisierung), ohne dass das Schlüs-

selmaterial den sicheren Schlüsselspeicher dazu verlassen muss. Die gSMC-K stellt Zufallszahlen zur Schlüsselerzeugung bereit, die von einem Zufallszahlengenerator der Klasse PTG.2 oder PTG.3 erzeugt wurden. Außerdem enthält die gSMC-K Schlüsselmaterial zur Verifikation der Authentizität des VPN-Konzentrators.

Sie müssen darauf achten, dass die gSMC-K dem Konnektor zur Verfügung steht. Achten Sie darauf, dass die Sicherheitssiegel des Geräts unbeschädigt sind.

A.6.5 Sicherer Schlüsselspeicher

Die IT-Umgebung (ein Teil des Gesamtkonnektors) stellt dem Konnektor einen sicheren Schlüsselspeicher bereit. Der sichere Schlüsselspeicher schützt sowohl die Vertraulichkeit als auch die Integrität des in ihm gespeicherten Schlüsselmaterials. Der Schlüsselspeicher wird vom T-Systems Konnektor zur Speicherung von Sitzungsschlüsseln (session keys) verwendet. Diese werden von auf der gSMC-K gespeicherten Geheimnissen (privater Schlüssel) zur Authentisierung beim Aufbau des VPN-Tunnels (kryptografische Identität des EVG, siehe FTP_ITC.1/NK.VPN_TI) abgeleitet.

Die gSMC-K muss dem Konnektor zur Verfügung stehen. Achten Sie darauf, dass die Sicherheitssiegel des Geräts unbeschädigt sind.

A.6.6 Korrekte Nutzung des T-Systems Konnektors durch den Anwendungskonnektor

Es ist sichergestellt, dass der Anwendungskonnektor zu schützende Daten der TI und der Bestandsnetze, die durch Dienste gemäß 291a SGB V [9] verarbeitet wurden, in korrekter Weise an den T-Systems Konnektor übergibt, damit der T-Systems Konnektor zu schützende Daten der TI und der Bestandsnetze über den entsprechenden VPN-Tunnel für Dienste gemäß 291a SGB V versenden kann. Dazu verwendet der Anwendungskonnektor die vom T-Systems Konnektor bereitgestellten Schnittstellen, sodass die Daten gemäß den gesetzlichen Anforderungen übertragen werden.

Sie können diesen Aspekt nicht beeinflussen. Die Software des Anwendungskonnektors und des Netzkonnektors sind Teil jeweils gesonderter Sicherheitszertifizierungen. Insbesondere die sichere Datenkommunikation mit Hilfe VPN wurde einer eingehenden Begutachtung unterzogen.

A.6.7 Korrekte Nutzung des Konnektors durch Clientsysteme (oder weitere Systeme im LAN)

Die Hersteller von Clientsystemen gestalten ihre Produkte so, dass diese den Konnektor für Dienste gemäß 291a SGB V [9] korrekt aufrufen. Aufrufe von Diensten gemäß 291a SGB V [9] müssen über den Anwendungskonnektor erfolgen.

Setzen Sie ausschließlich Praxisverwaltungs- oder Krankenhausinformationssysteme ein, die von der gematik hinsichtlich ihrer korrekten Funktions- und Arbeitsweise eine Produktzulassung erhalten haben. Nur in diesem Falle ist gewährleistet, dass das eingesetzte System sich konform zu den Anforderungen verhält.

A.6.8 Sicherer Internet Service

Die TI-Umgebung stellt einen gesicherten Zugangspunkt zum Internet bereit. Dieser Zugangspunkt schützt die dahinterliegenden Netze der Benutzer wirksam gegen Angriffe aus dem Internet.

Sie haben die Möglichkeit, einen VPN-gesicherten Zugang ins Internet zu verwenden.

A.6.9 Public-Key-Infrastruktur

PKI-Komponenten (Public-Key-Infrastruktur) sind vorhanden und werden vom T-Systems Konnektor verwendet. Diese Komponenten werden während der Erprobung durch die gematik oder einem beauftragten Unternehmen der gematik bereitgestellt.

Der T-Systems Konnektor wurde im Zuge der sicherheitstechnischen Evaluierung eingehend hinsichtlich seiner PKI-Nutzung untersucht. Die notwendigen PKI-Komponenten werden vom Konnektor automatisch verwendet.

A.7 Glossar

Tabelle 113 Glossar

Glossar	
Anwendungsentwickler	Mit Anwendungsentwicklern ist Fachpersonal gemeint, welches die programmatische Integration des T-Systems Konnektors in die lokale Infrastruktur der Einsatzumgebung vornimmt. Hierzu gehört die Initialisierung des T-Systems Konnektors, durch die Änderung des in Abschnitt 7.1.1 benannten Auslieferungszustands.
Bestandsnetz	Bestandsnetze sind bereits vorhandene Netzwerke des Gesundheitswesens, die an die Telematikinfrastruktur angeschlossen sind und über den T-Systems Konnektor erreicht werden müssen, um Anwendungsfälle zu verarbeiten.
Default-Gateway	Der Default-Gateway leitet alle nicht zu einem bestimmten (z.B. lokalen) Netz gehörenden Netzwerkanfragen in ein anderes Netz (z.B. das Internet) weiter. Kann also im lokalen Netz ein Adressat (ein Computer, Peripheriegeräte, etc.) für Datenpakete nicht gefunden werden, werden diese an das Default-Gateway geleitet.
DHCP	DHCP steht für Dynamic Host Configuration Protocol. Durch die Verwendung von DHCP kann der T-Systems Konnektor automatisch für Ihr Netzwerk konfiguriert werden, da~~. Da~~ die Funktion als DHCP-Client bei Auslieferung aktiviert ist. Ein DHCP-Server im gleichen Netzwerk übernimmt dann die Konfiguration des T-Systems Konnektors.
HBA	HBA steht für Heilberufsausweis
ICCSN	Die ICCSN ist eine eindeutige 20-stellige Kartenkennnummer zur Vermeidung von Verwechslungen. Sie setzt sich aus Ziffern zusammen, welche den Branchenhauptschlüssel, das Länderkennzeichen, den Kartenherausgeber und die Seriennummer der Karte widerspiegeln.
LAN	LAN steht für Local Area Network und ist ein lokales Netzwerk. Im Speziellen ist hiermit die lokale Infrastruktur der Einsatzumgebung gemeint.

Glossar	
MESZ	MESZ steht für Mitteleuropäische Sommerzeit und ist, unter anderen, die für deutschsprachige Länder und Gebiete gesetzlich gültige Uhrzeit. Die Differenz der MESZ zur Weltzeit (UTC) beträgt +2 Stunden, kurz UTC+2.
MEZ	MEZ steht für Mitteleuropäische Zeit und ist, unter anderen, die für deutschsprachige Länder und Gebiete gesetzlich gültige Uhrzeit. Die Differenz der MEZ zur Weltzeit (UTC) beträgt +1 Stunde, kurz UTC+1.
NTP	NTP steht für Network Time Protocol und ist ein Standard zur Synchronisierung von Uhren in Computernetzwerken und dient zur Kontrolle zeitlich relevanter Kommunikation unter Berücksichtigung der Datenpaketlaufzeit.
QES	QES steht für qualifizierte elektronische Signatur.
SIS	SIS steht für Secure Internet Service. Über den SIS kann genau festgelegt werden, wie Daten mit dem Internet ausgetauscht werden können.
SMB	Siehe Beschreibung zu SMC.
SMC	SMC steht für Security Module Card. Diese Karte dient der Identifikation einer berechtigten Institution im Gesundheitswesen. Die SMC gibt es in zwei verschiedenen Ausführungen:
	SMC-A enthält nur die Schlüssel, um auf eine Gesundheitskarte zuzugreifen sowie Mechanismen, um eine gesicherte Verbindung zwischen einem Heilberufsausweis und einer SMC herzustellen. Die SMC Typ A wird typischerweise als Plug-In-Karte im Kartenlesegerät verwendet.
	SMC-B (auch SMB) enthält neben den Funktionen des Typs A zusätzlich auch ein Zertifikat und Schlüssel für die Authentifikation der Institution in der Telematikinfrastruktur, ein Zertifikat mit Schlüssel für die Signatur von Nachrichten, die von dieser Institution versendet werden sowie ein Zertifikat und Schlüssel zur Ver- / Entschlüsselung von Nachrichten an diese Institution. Die SMC Typ B wird unter anderem vom Konnektor verwendet.
Telematikinfrastruktur	Die Telematikinfrastruktur bezeichnet die vernetzten Systeme des Gesundheitswesens. Diese kann über den hier beschriebenen T-Systems Konnektor erreicht und so die dort angebotenen Dienste genutzt werden.
UTC	UTC steht für koordinierte Weltzeit (Universal Time Coordinated) und ist die heute gültige Weltzeit.
VPN	VPN steht für Virtual Private Network. Ein VPN dient dazu, einen gesicherten und vertrauenswürdigen Kanal zwischen Netzwerken mit Hilfe kryptografischer Mittel herzustellen.
WAN	WAN steht für Wide Area Network und ist ein Netzwerk. Im Speziellen ist hiermit Transportnetz gemeint, über das der Zugang zur Telematikinfrastruktur hergestellt wird.