



# Produkthandbuch

## T-Systems Konnektor

Firmware: 1.5.3

Hardware: 2.2.4 / 2.2.5 / 2.2.6

T-Systems International GmbH

---

Tabelle 1 Impressum

<b>Herausgeber</b>		
T-Systems International GmbH		
Hahnstraße 43d		
60528 Frankfurt am Main		
<b>Dateiname</b>		
05092019_OPB_KON_AGD_V1.30		
<b>Version</b>	<b>Letztes Review</b>	<b>Status</b>
1.30	05.09.2019	Final
<b>Ansprechpartner</b>		<b>E-Mail</b>
T-Systems International GmbH		service.map@telekom.de
<b>Kurzbeschreibung</b>		
Dieses Dokument ist das Benutzerhandbuch für den Konnektor der T-Systems.		

Im Rahmen des Zulassungsverfahrens gegenüber der gematik übermittelte Informationen zur Herstellung der Zulassungsvoraussetzungen oder notwendiger Rahmenparameter stellen Betriebs- und Geschäftsgeheimnisse des Antragsstellers bzw. Dritter dar und unterliegen der Geheimhaltung.

Eine Nutzung ist ausschließlich im Rahmen der Durchführung der Zulassung erlaubt. Eine Weitergabe an Dritte ist nur mit ausdrücklicher Genehmigung des Antragsstellers gestattet

# Änderungshistorie

Tabelle 2 Änderungshistorie

Version	Stand	Änderungen
<b>Historie gekürzt</b>		
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
1.17	29.10.2018	Anpassung der Firmware 1.4.13 mit aktualisiertem BIOS
1.18	22.11.2018	Ergänzung und Update von Werksreset und Admin-Oberfläche für Konnektor Release 1.5.1
1.19	05.12.2018	Update von Referenzen in mehreren Kapiteln und Default-Werte der Sequenznummern
1.20	04.03.2019	Anpassung der Firmware auf Version 1.5.2
1.21	21.03.2019	Ergänzung eines Fehlercodes
1.22	29.05.2019	Anpassung der Firmware auf Version 1.5.3
1.23	29.05.2019	redaktionelle Änderungen
1.24	29.05.2019	Aktualisierung der Zertifizierungs-ID
1.25	29.05.2019	Fehler bei der Hotline-Nummer (A.1) korrigiert
1.26	20.06.2019	Ergänzung von Hinweisen der Prüfstelle
1.27	24.07.2019	Ergänzung von weiteren Hinweisen der Prüfstelle
1.28	29.07.2019	Ergänzung erneuter Hinweise der Prüfstelle
1.29	30.07.2019	Fehlerkorrektur
1.30	05.09.2019	Fehlerkorrektur

# Inhaltsverzeichnis

<b>Änderungshistorie.....</b>	<b>3</b>
<b>Inhaltsverzeichnis .....</b>	<b>4</b>
<b>Abbildungsverzeichnis .....</b>	<b>9</b>
<b>Tabellenverzeichnis .....</b>	<b>11</b>
<b>1        <b>Allgemeine Informationen zur Dokumentation.....</b></b>	<b>16</b>
1.1       Hinweis zur Zulassung und deren Begrenzung .....	16
1.2       Zielgruppe der Dokumentation .....	16
<b>2        <b>Bestimmungsgemäße Verwendung in der Telematikinfrastuktur (TI).....</b></b>	<b>17</b>
2.1       Überblick über die Telematikinfrastuktur .....	17
2.2       Funktionen innerhalb der Telematikinfrastuktur .....	18
2.2.1     VPN-Zugangsdienst .....	18
<b>3        <b>Sicherheit und Integrität .....</b></b>	<b>19</b>
3.1       Information zum sicheren Transport und Logistik .....	19
3.2       Sicherheit der Geräteverpackung .....	19
3.3       Sicherheitshinweise Hardware .....	20
3.3.1     Was tun bei Diebstahl oder erkennbarer Manipulation des Geräts? .....	21
3.3.2     Rücksendung eines Gerätes .....	21
3.4       Sicherheitsmaßnahmen in der IT-Einsatzumgebung .....	22
3.4.1     Sicherer Betrieb von Nutzeranwendungen und Nutzerkomponenten.....	23
3.5       Sicherheitsfunktionen des T-Systems Konnektors.....	24
3.5.1     VPN-Client .....	25
3.5.2     Zeitsynchronisation .....	25
3.5.3     Administration .....	26
3.5.4     Firewall.....	27
3.5.5     DHCP-Dienste.....	31
3.5.6     DNS-Resolver .....	31
3.5.7     Hinweise zur Verwendung des integrierten Sicherheitsmoduls.....	32
3.5.8     Aktivierung DNSSEC.....	32
3.6       Hinweise zur Zulassung / Sicherheitszertifizierung .....	32
3.6.1     Überprüfung auf Zulassung .....	32

3.6.2	Überprüfung auf Sicherheitszertifizierung.....	33
<b>4</b>	<b>In- und Außerbetriebnahme der Hardware .....</b>	<b>34</b>
4.1	Bevor Sie den Konnektor anschließen.....	34
4.1.1	Lieferung des Konnektors.....	34
4.1.2	Einsatz des Konnektors.....	35
4.2	Lieferumfang .....	35
4.3	Anschlüsse.....	36
4.4	Leuchtdioden.....	37
4.4.1	Anzeigenstatus.....	37
4.5	Bedienelemente .....	38
4.6	Montage und Platzierung.....	39
4.7	Erstinstallation und Inbetriebnahme des Geräts in die Telematikinfrastruktur .....	39
4.7.1	Erstanmeldung und Passwort ändern.....	40
4.7.2	Einrichten der Infrastruktur .....	41
4.7.3	Einrichten des Namensservers.....	41
4.7.4	IP-Adressen DNS-Server im öffentlichen Netz .....	41
4.7.5	LAN und WAN konfigurieren .....	42
4.7.6	Installation zur Verwendung mit einem Kartenterminal .....	53
4.7.7	Installation zur Verwendung mit mehreren Kartenterminals.....	54
4.7.8	Installation mit speziellen Anforderungen mit mindestens einem separaten VPN-Netzwerk.....	55
4.7.9	Installation mit zentralem Primärsystem als Clientsystem.....	56
4.8	Einsatzbereitschaft.....	58
4.8.1	Erste Inbetriebnahme: Mögliche Verletzungen der Integrität .....	58
4.8.2	Start des Konnektors.....	58
4.9	Betrieb.....	59
4.9.1	Betriebszustände.....	59
4.10	Aktualisierung des T-Systems Konnektors .....	64
4.11	Registrierung des Konnektors .....	64
4.12	Werksreset.....	64
4.13	Außerbetriebnahme sowie End-of-Life (Ende des Lebenszyklus) des T- Systems Konnektors .....	64
4.13.1	Deregistrierung.....	66
4.13.2	Finale Außerbetriebnahme und Rücktransport .....	67
4.13.3	Entfernen des T-Systems Konnektors aus Infrastruktur.....	69

<b>5</b>	<b>Bedienung der Software .....</b>	<b>70</b>
5.1	Zugriff auf die Administrationsoberfläche.....	70
5.1.1	Verwendung von Javascript und Sitzungs-Cookies .....	72
5.1.2	Änderung des Benutzerkennworts.....	72
5.1.3	LDAP-Proxy .....	72
5.2	Hauptmenü.....	74
5.2.1	System .....	75
5.2.2	Fachmodule .....	75
5.2.3	Netzwerk .....	75
5.2.4	Wartung .....	76
5.3	Erste Aktionen zur Inbetriebnahme des T-Systems Konnektors .....	76
5.3.1	Konfiguration der Zeit .....	77
5.3.2	Pairing eines Kartenterminals.....	77
5.3.3	Einrichten eines Arbeitsplatzes.....	78
5.3.4	Vertrauensräume.....	79
5.4	Dienstverzeichnisdienst.....	79
5.5	Aktualisierung der Firmware.....	80
<b>6</b>	<b>Einstellungen des Netzkonnektors .....</b>	<b>82</b>
6.1	Menüpunkt VPN-Client.....	82
6.2	Menüpunkt LAN und WAN .....	84
6.3	Menüpunkt Routing .....	86
6.4	Menüpunkt Firewall .....	87
6.5	Menüpunkt Infrastruktur.....	88
6.6	Menüpunkt Namensdienst.....	88
6.7	Menüpunkt DHCP-Server.....	90
6.8	Menüpunkt Datum und Uhrzeit .....	92
<b>7</b>	<b>Einstellungen des Anwendungskonnektors .....</b>	<b>94</b>
7.1	Allgemeine Informationen.....	94
7.1.1	Vergabe von weiteren Administrations-Accounts.....	94
7.1.2	Aktualisierung des Vertrauensraums .....	95
7.1.3	Aktualisierung der Sperrliste.....	95
7.1.4	Remote-PIN-Verfahren.....	95
7.2	Menüpunkt Administratoren.....	97
7.2.1	Anlegen eines neuen Administrator-Kontos.....	99
7.3	Menüpunkt Leistungsumfang .....	100

7.4	Menüpunkt Zugriffsberechtigung .....	101
7.4.1	Clientsysteme.....	101
7.4.2	Arbeitsplätze .....	102
7.4.3	Mandanten .....	104
7.4.4	SMB .....	106
7.4.5	Sichere Anzeige .....	107
7.5	Menüpunkt Kartenterminals.....	108
7.6	Menüpunkt Karten .....	110
7.7	Menüpunkt Systeminformationen .....	111
7.8	Menüpunkt Betriebszustände .....	111
7.9	Menüpunkt Zertifikate.....	112
7.9.1	Vertrauensanker.....	113
7.10	Menüpunkt Protokollierung.....	114
7.10.1	Backup und Löschen der Protokollierung .....	116
7.11	Menüpunkt Backup.....	117
7.12	Menüpunkt Update .....	117
7.13	Logout von der Administrationsoberfläche.....	118
7.14	Werksreset durchführen .....	118
7.14.1	Admin Passwort vergessen / Werksreset wird ausgelöst.....	119
<b>8</b>	<b>Einstellungen des Fachmoduls Versichertendaten .....</b>	<b>120</b>
<b>9</b>	<b>Versionierung des Konnektors .....</b>	<b>124</b>
<b>10</b>	<b>Fehlermeldungen .....</b>	<b>126</b>
10.1	Fehlermeldungen des T-Systems Konnektor.....	126
10.1.1	Fehlermeldungen auf der Administrationsoberfläche.....	126
10.1.2	Allgemeine Fehlermeldungen.....	127
10.1.3	Fehlermeldungen Firewall .....	129
10.1.4	Fehlermeldungen im Menü Administration und Registrierung.....	129
10.1.5	Fehlermeldungen im Menü Zertifikate .....	131
10.1.6	Fehlermeldungen im Menü VPN-Client .....	131
10.1.7	Fehlermeldungen im Menü LAN und WAN.....	135
10.1.8	Fehlermeldungen im Menü Namensdienst .....	137
10.1.9	Fehlermeldungen im Menü Protokollierung .....	138
10.1.10	Fehlermeldungen im Menü DHCP-Client.....	138
10.1.11	Fehlermeldungen im Menü DHCP-Server .....	139
10.1.12	Fehlermeldungen im Menü Datum und Uhrzeit .....	140

10.1.13	Fehlermeldungen im Menü Update .....	141
10.1.14	Fehlercodes kritischer Fehler (Hardwaredisplay).....	142
10.1.15	Fehlercodes während des Startvorgangs (Hardwaredisplay).....	143
<b>A</b>	<b>Anhang.....</b>	<b>145</b>
A.1	Kontakt.....	145
A.1.1	PKI-Betreiber.....	145
A.1.2	Herausgeber .....	145
A.1.3	Hersteller.....	145
A.2	Konformitätsangaben .....	146
A.2.1	CE-Zeichen .....	146
A.2.2	TÜV-Zertifikat .....	146
A.3	Rücknahme von alten Geräten .....	146
A.4	Technische Daten .....	146
A.5	Lizenzinformationen .....	147
A.6	Hinweise zur Sicherheitszertifizierung des Produkts.....	148
A.6.1	Externer Zufallszahlengenerator.....	148
A.6.2	Echtzeituhr .....	148
A.6.3	Zeitsynchronisation .....	148
A.6.4	Sicherheitsmodul gSMC-K .....	148
A.6.5	Sicherer Schlüsselspeicher .....	149
A.6.6	Korrekte Nutzung des T-Systems Konnektors durch den Anwendungskonnektor .....	149
A.6.7	Korrekte Nutzung des Konnektors durch Clientsysteme (oder weitere Systeme im LAN) .....	149
A.6.8	Sicherer Internet Service .....	150
A.6.9	Public-Key-Infrastruktur .....	150
A.7	Verwendete Ports in der dezentralen Zone der TI .....	150
A.8	Glossar.....	151



## Abbildungsverzeichnis

Abbildung 1 Überblick über die Telematikinfrastruktur (TI).....	17
Abbildung 2 Konnektorverpackung .....	20
Abbildung 3 Siegel am Gehäuse des Konnektors.....	24
Abbildung 4 Muster Siegel.....	24
Abbildung 5 Übersicht des Gesamtsystems der TI .....	27
Abbildung 6 DHCP DNS ausschalten .....	32
Abbildung 7 Unterseite des Konnektors / Typenschild .....	34
Abbildung 8 Position Sicherheitssiegel am T-Systems Konnektor .....	35
Abbildung 9 Anschlüsse des T-Systems Konnektors .....	36
Abbildung 10 Leuchtdioden des T-Systems Konnektors.....	37
Abbildung 11 Administrationsoberfläche / Passwort ändern .....	40
Abbildung 12 Administrationsoberfläche / DNS Root Anker.....	42
Abbildung 13 Administrationsoberfläche / WAN Adapter ausschalten .....	43
Abbildung 14 Administrationsoberfläche / DHCP Ein-Ausschalten .....	44
Abbildung 15 Administrationsoberfläche / Online Modus Ausschalten .....	44
Abbildung 16 Administrationsoberfläche / Hinweis Offline Modus.....	45
Abbildung 17 Administrationsoberfläche / TSL Upload .....	45
Abbildung 18 Administrationsoberfläche / Online Modus Einschalten .....	46
Abbildung 19 Administrationsoberfläche / Übersicht TSL und CRL.....	47
Abbildung 20 Administrationsoberfläche / Anzeige der verbundenen Kartenterminals.....	48
Abbildung 21 Administrationsoberfläche / Verbindungsaufbau zum Kartenterminal.....	48
Abbildung 22 Administrationsoberfläche / Sichere Verbindung zum Client .....	50
Abbildung 23 Administrationsoberfläche / Anzeige verbundenen Arbeitsplätze .....	51
Abbildung 24 Administrationsoberfläche / Konnektor an TI registrieren .....	52
Abbildung 25 Szenario einfache Installation aus gemSpec_KON_V4.11.1, S.498.....	53
Abbildung 26 Szenario einer Installation mit mehreren Behandlungsräumen aus gemSpec_KON_V4.11.1, S.500 .....	54
Abbildung 27 Szenario einer Integration in bestehende Infrastruktur aus gemSpec_KON_V4.11.1, S.501 .....	55
Abbildung 28 Szenario einer Installation mit zentralem Primärsystem als Clientsystem aus gemSpec_KON_V4.11.1, S.506 .....	56
Abbildung 29 Administrationsoberfläche / Verbindung zur TI trennen.....	65
Abbildung 30 Administrationsoberfläche / Registrierung .....	66
Abbildung 31 Administrationsoberfläche / Registrierung zurücknehmen.....	66

Abbildung 32	Administrationsoberfläche / Registrierung .....	67
Abbildung 33	Administrationsoberfläche / Außerbetriebnahme.....	67
Abbildung 34	Administrationsoberfläche / Sicherheitsabfrage .....	68
Abbildung 35	Administrationsoberfläche / Eingabe der ICCSN .....	68
Abbildung 36	Administrationsoberfläche / Bestätigung „Konnektor außer Betrieb“ .....	68
Abbildung 37	Administrationsoberfläche / LDAP Proxy konfigurieren .....	73
Abbildung 38	Administrationsoberfläche / Zugriffsberechtigungen.....	73
Abbildung 39	Administrationsoberfläche / Hauptmenü.....	74
Abbildung 40	Administrationsoberfläche / Änderung der Account-Daten .....	94
Abbildung 41	Szenario Remote-PIN-Verfahren aus gemSpec_KON_V4.11.1, S.504 .....	97
Abbildung 42	Administrationsoberfläche / Kartenterminals .....	108
Abbildung 43	Administrationsoberfläche / Button „abmelden“ .....	118
Abbildung 44	Multifunktionstaste (Software Taste) .....	119
Abbildung 45	Administrationsoberfläche / Dienst.....	122
Abbildung 46	Administrationsoberfläche / Performance Protokoll .....	123
Abbildung 47	Versionierung des Konnektors .....	124
Abbildung 48	Verwendete Ports in der dezentralen Zone der TI.....	150

## Tabellenverzeichnis

Tabelle 1 Impressum .....	2
Tabelle 2 Änderungshistorie .....	3
Tabelle 3 Überblick über die geprüften Sicherheitsfunktionen des T-Systems Konnektors	24
Tabelle 4 Weitere nutzbare Funktionen .....	25
Tabelle 5 Firewall-Regeln für das Netz der Telematik.....	28
Tabelle 6 Firewall-Regeln für das Internet .....	28
Tabelle 7 Firewall-Regeln für Bestandsnetze.....	30
Tabelle 8 Firewall-Regeln für das Netz des Leistungserbringers .....	30
Tabelle 9 Allgemeine Firewall-Regeln.....	30
Tabelle 10 Anzeigestatus .....	37
Tabelle 11 Mögliche Fehler bei Inbetriebnahme .....	58
Tabelle 12 Fehlermeldungen bei kritischem Betriebszustand .....	60
Tabelle 13 Fehlermeldungen bei unkritischen Betriebszustand .....	61
Tabelle 14 Warnmeldungen für Funktionsbereitschaft .....	62
Tabelle 15 Infomeldungen zum Betriebszustand .....	63
Tabelle 16 Unterstützte Browser.....	70
Tabelle 17 Standardkonfigurationsdaten .....	71
Tabelle 18 Authentifizierungseinstellungen für Dienstverzeichnisdienst.....	80
Tabelle 19 Menüpunkt VPN-Client Übersicht.....	82
Tabelle 20 Menüpunkt VPN-Client Einstellungen .....	83
Tabelle 21 LAN-Einstellungen .....	84
Tabelle 22 WAN-Einstellungen.....	85
Tabelle 23 Allgemeine Verbindungseinstellungen .....	85
Tabelle 24 Routing-Einstellungen .....	87
Tabelle 25 Intranet-Einstellungen .....	87
Tabelle 26 Firewallregeln.....	88
Tabelle 27 DNS-Server im Leistungserbringernetz .....	88
Tabelle 28 DNS-Server im öffentlichen Netz .....	88
Tabelle 29 DNS-Server im Netz des SIS .....	89
Tabelle 30 DNS-Server im Bestandsnetz .....	89
Tabelle 31 DNS-Server im Netz der TI .....	89
Tabelle 32 Anzeige aktiver Bestandsnetze .....	89
Tabelle 33 Namensdienst-Einstellungen.....	89

Tabelle 34 Domain Erreichbarkeit prüfen.....	90
Tabelle 35 DHCP-Server-Status.....	90
Tabelle 36 DHCP-Server-Einstellungen.....	90
Tabelle 37 DHCP-Clientgruppen .....	90
Tabelle 38 DHCP-Clientgruppen-Einstellungen .....	91
Tabelle 39 Clients.....	91
Tabelle 40 DNS-Server für DHCP-Clientgruppen .....	91
Tabelle 41 Intranet-Routen für DHCP-Clientgruppen.....	92
Tabelle 42 Bestandsnetz für DHCP-Clientgruppen.....	92
Tabelle 43 DHCP-Routing-Einstellungen.....	92
Tabelle 44 Zeitzone .....	92
Tabelle 45 Manuelle Einstellung für Datum und Zeit.....	93
Tabelle 46 Informationen zu NTP-Einstellungen.....	93
Tabelle 47 Verfügbare Administratoren .....	97
Tabelle 48 Account bearbeiten .....	97
Tabelle 49 Berechtigungen einstellen.....	98
Tabelle 50 Rechtevergabe.....	98
Tabelle 51 Neues Administrator-Konto anlegen.....	100
Tabelle 52 Einstellung des Betriebsmodus .....	100
Tabelle 53 Einstellung der Zugriffsberechtigungen .....	101
Tabelle 54 Einstellung des gewählten Clientsystems.....	102
Tabelle 55 Einstellung des gewählten Arbeitsplatz .....	102
Tabelle 56 Liste der konfigurierten Arbeitsplätze .....	103
Tabelle 57 Liste der zugeordneten Kartenterminals.....	103
Tabelle 58 Liste der angelegten Mandanten.....	104
Tabelle 59 Details zu ausgewähltem Mandanten.....	104
Tabelle 60 Liste der zugeordneten Kartenterminals.....	104
Tabelle 61 Liste der zugeordneten SMBs .....	105
Tabelle 62 Liste der zugeordneten Arbeitsplätze .....	105
Tabelle 63 Liste der zugeordneten Clientsysteme .....	105
Tabelle 64 Liste der der Arbeitsplätze zugeordneter Clientsysteme.....	105
Tabelle 65 Liste der zugeordneten Kartenterminals für Remote-PIN-Zugriff .....	106
Tabelle 66 Zugeordneter VSDM-Encryptionkey.....	106
Tabelle 67 Liste der SMBs.....	106
Tabelle 68 Liste der sicheren Anzeigen (Trusted Viewer) .....	107
Tabelle 69 Liste der Kartenterminals .....	108

Tabelle 70 Einstellungen der Kartenterminals.....	109
Tabelle 71 Liste der verfügbaren Karten.....	110
Tabelle 72 Betriebszustände .....	111
Tabelle 73 Missbrauchserkennung .....	111
Tabelle 74 Konfiguration des Vertrauensraums .....	112
Tabelle 75 Liste von Endpunkten.....	113
Tabelle 76 Einstellung zu Endpunkten.....	113
Tabelle 77 Systemprotokolle .....	114
Tabelle 78 Sicherheitsprotokolle.....	114
Tabelle 79 Performanceprotokolle .....	115
Tabelle 80 VSDM-Ablaufprotokolle.....	115
Tabelle 81 VSDM-Fehlerprotokolle.....	115
Tabelle 82 VSDM-Performanceprotokolle.....	115
Tabelle 83 Einstellungen zur VSDM-Performanceprotokollierung.....	115
Tabelle 84 Backupsicherung erstellen .....	117
Tabelle 85 Backupsicherung laden.....	117
Tabelle 86 Plan alle Geräte .....	117
Tabelle 87 Update-Einstellungen.....	118
Tabelle 88 VSDM-Einstellungen .....	120
Tabelle 89 VSDM-Protokoll .....	120
Tabelle 90 Performance-Protokoll .....	120
Tabelle 91 Mandanten-Schlüssel-Zuordnung .....	121
Tabelle 92 Einstellung der automatischen Stammdatenaktualisierung .....	121
Tabelle 93 Versionierung des Konnektors .....	125
Tabelle 94 Fehlermeldungen auf der Administrationsoberfläche.....	126
Tabelle 95 Allgemeine Fehlermeldungen.....	127
Tabelle 96 Fehlermeldungen Firewall.....	129
Tabelle 97 Fehlermeldungen im Menü Administration und Registrierung .....	129
Tabelle 98 Fehlermeldungen im Menü Zertifikate .....	131
Tabelle 99 Fehlermeldungen im Menü VPN-Client .....	131
Tabelle 100 Fehlermeldungen im Menü LAN und WAN.....	135
Tabelle 101 Fehlermeldungen im Menü Namensdienst .....	137
Tabelle 102 Fehlermeldungen im Menü Protokollierung .....	138
Tabelle 103 Fehlermeldungen im Menü DHCP-Client .....	138
Tabelle 104 Fehlermeldungen im Menü DHCP-Server .....	139
Tabelle 105 Fehlermeldungen im Menü Datum und Uhrzeit .....	140

Tabelle 106 Fehlermeldungen im Menü Update .....	141
Tabelle 107 Fehlercodes kritischer Fehler (Hardwaredisplay) .....	142
Tabelle 108 Fehlercodes während des Startvorgangs (Hardwaredisplay) .....	143
Tabelle 109 Kontakt PKI-Betreiber .....	145
Tabelle 110 Kontakt Herausgeber .....	145
Tabelle 111 Kontakt Hersteller .....	145
Tabelle 112 Produktdetails .....	146
Tabelle 113 Technische Daten .....	147
Tabelle 114 Glossar .....	151

## Zusammenfassung

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 zur Zulassung und deren Begrenzung

Das vorliegende Handbuch beschreibt die Konfiguration und den Umgang mit dem Produkt T-Systems Konnektor und ist Teil der Dokumentation im Rahmen einer Re-Zertifizierung des vom BSI zertifizierten Konnektors mit der Kennung BSI-DSZ-CC-0928-V2.

Mehr Informationen zur Produktzertifizierung erhalten Sie auf den Webseiten des Bundesamts für Sicherheit in der Informationstechnik (BSI) und von ihrem Vertragspartner.

## 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 dem VSDM-Fachmodul an.

Diese Funktionalität ist in dem Ihnen vorliegenden Produkt Gegenstand der erfolgten sicherheitstechnischen Evaluierung gemäß Common Criteria unter der Kennung BSI-DSZ-CC-0928-V2 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.

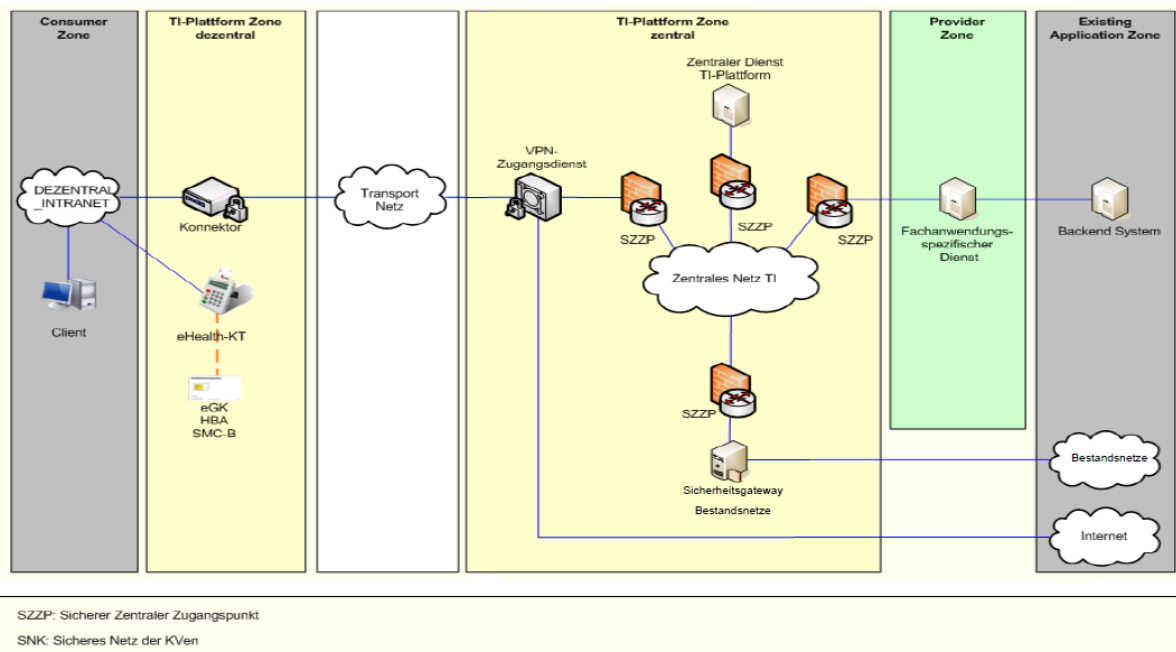


Abbildung 1 Überblick über die Telematikinfrastruktur (TI)

Der T-Systems Konnektor ist ein Gerät für den Einsatz in Praxen, Medizinischen Versorgungszentren, Krankenhäuser, Apotheken und weiteren Akteuren im Gesundheitswesen.

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.

Mit Hilfe der Administrationsoberfläche unter dem Menüpunkt **Hauptmenü > Leistungsumfang** können Sie den Konnektor sowohl offline als auch online konfigurieren.

## 2.2 Funktionen innerhalb der Telematikinfrastruktur

Der Konnektor dient dazu, Anwendungsprogrammen auf den Systemen in Praxen, Medizinischen Versorgungszentren, Krankenhäuser, Apotheken und weiteren Akteuren 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 den Dienst für das Versichertenstammdatenmanagement 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 1.5.x.

### 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 fachanwendungsspezifischen 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-V2 zu entnehmen.

## 3 Sicherheit und Integrität

Das folgende Kapitel beinhaltet Hinweise zur sicheren Lieferung sowie 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 die Lieferinformationen in Form einer standardisierten E-Mail an den Leistungserbringer, für den die Lieferung bestimmt ist.

Der Lieferinformation enthält mindestens folgende Angaben:

- Bestellnummer der Bestellung
- Transportdienstleister
- Sendungsnummer(n) der Sendung auf der Kartonverpackung
- Geplanter Tag und Zeitspanne der Auslieferung
- Angaben zum 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

Der Transportdienstleister liefert er den Versandkarton an den benannten Empfänger ab. Der Empfänger soll unverzüglich die nachfolgend beschriebene Integritätsprüfung (Sicherheit der Geräteverpackung) durchzuführen. 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?
- Sind 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 den Karton verschließt (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.



Abbildung 2 Konnektorverpackung

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<sup>1</sup> 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.

### 3.3.2 Rücksendung eines Gerätes

Geräte, deren Integrität möglicherweise verletzt worden ist, sind an den jeweiligen Hersteller des Gerätes mit Angaben zum Grund der Rücksendung zurückzusenden. Dabei genügt es einen einfachen, ungesicherten Transportweg (Postversand) zu wählen, da diese Geräte ohnehin als „unsicher“ gelten und nicht in Betrieb genommen werden dürfen.

Nach Erhalt der Meldung über eine mögliche Integritätsverletzung inkl. der Seriennummer des betroffenen Gerätes, trägt der Hersteller mindestens Seriennummern und die ICCSN der enthaltenen gSMC-K in eine Übersichtsliste ein und informiert den Helpdesk der T-Systems über den neuen / geänderten Eintrag in der Übersichtsliste. Auf Verlangen MUSS der Hersteller darüber Auskunft geben, ob eine Geräte-Seriennummer auf der Liste der Geräte mit mögl. Integritätsverletzung enthalten ist oder nicht. Der Eintrag der Seriennummer auf der Liste darf nicht gelöscht werden.

Geräte MÜSSEN vom LEI auch an den Hersteller zurückgesendet werden, wenn der Gültigkeitszeitraum der Zertifikate der im Konnektor verbauten gSMC-K abgelaufen ist oder kurz vor Ablauf steht. Der Eigentümer des Konnektors muss vor dem Versand des Konnektors auf einem beliebigen Weg, einen Werksreset durchführen, das Gerät bei T-Systems als Betreiber des vom Eigentümer genutzten VPN-Zugangsdienstes abmelden sowie deregistrieren (siehe Kapitel 4.13).

---

<sup>1</sup> gerätespezifische Security Module Card Konnektor

## 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.
- Alle Administratoren in der zentralen Telematikinfrastruktur und den damit verbundenen Konnektoren 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 stets aktuell. Verwenden Sie nur durch die gematik GmbH ([www.gematik.de](http://www.gematik.de)) zugelassene, und durch das BSI 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 zum Lesen der eGK 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 in Übereinstimmung mit diesem Handbuch durchgeführt werden. Insbesondere muss für diese Tätigkeiten vertrauenswürdige 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.
- Bitte verändern Sie nach der Installation den Standort des Gerätes nicht mehr und lassen Sie dieses dauerhaft an das Stromnetz angeschlossen sowie mit dem Internet verbunden.

### 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.
- 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, Virens Scanner etc.), da auch Angriffe über den sicheren Internet Service nicht vollständig ausgeschlossen werden können.
- Im Anbindungsmodus **Parallel** (siehe auch Kapitel 4.7) ist ebenfalls ein Internetzugriff über den sicheren SIS-Zugang möglich. Die Internetverbindung muss also selbstständig abgesichert werden. Die Einstellung des Anbindungsmodus **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.

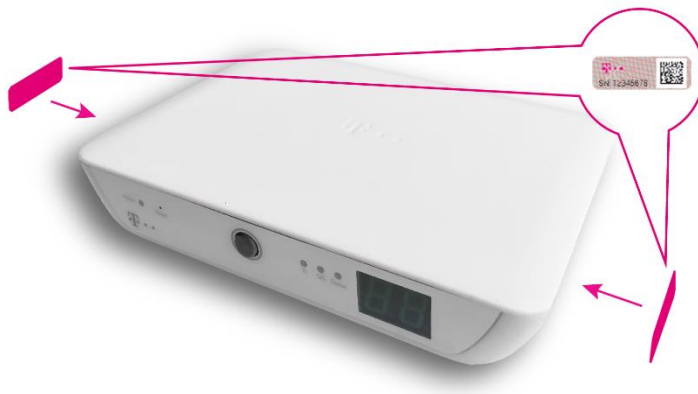


Abbildung 3 Siegel am Gehäuse des Konnektors

### Muster Siegel



Abbildung 4 Muster Siegel

Jedes Siegel hat eine eindeutige Seriennummer, die bei der Produktion des Konnektors 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 gewährleistet das Erkennen eines einwandfreien Gehäuses.

## 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 Codes 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 3.5.1
Zeitsynchronisation	Im Online-Modus 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 <a href="#">3.5.2</a> .
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. Mehr Einzelheiten zur Administration finden Sie im Abschnitt <a href="#">3.5.3</a> oder <a href="#">7.13</a>
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 <a href="#">3.5.4</a>

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 <a href="#">3.5.5</a> , 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 <a href="#">3.5.6</a>

### 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 Online-Modus betrieben werden muss. Die Zeitsynchronisation ist aus mehreren Gründen wichtig:

1. Der T-Systems Konnektor bietet einen sogenannten NTP-Server der Stratum-Ebene 3<sup>2</sup> 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 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 30 Tage korrekt eingestellt werden. Der Administrator des Konnektors sollte daher in regelmäßigen Abständen die Richtigkeit der Uhrzeit auf dem Konnektor überprüfen.

### 3.5.3 Administration

Der Konnektor bietet eine Administrationsoberfläche 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).

Über die Administrationsoberfläche können unter anderem folgende Einstellungen vorgenommen werden:

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.

---

<sup>2</sup> Stratum Ebenen bezeichnen die Entfernung (durch Anzahl benannt) des NTP-Servers von einer zeitgebenden Quelle.

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

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

Weitere Informationen zur Administration sind im Kapitel 5 beschrieben.

### 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 Datenverkehr 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-V2 beschrieben.

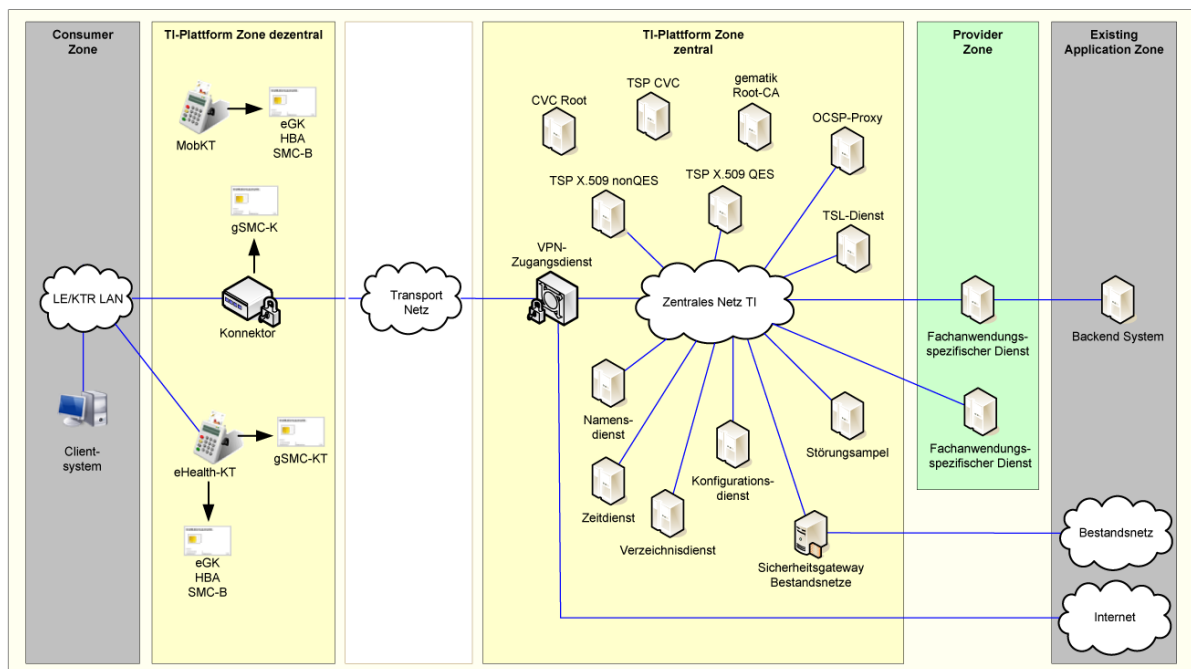


Abbildung 5 Übersicht des Gesamtsystems der TI

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 Firewall-Regeln. 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 mit tabellarischer Übersicht das Gesamtsystem der Telematikinfrastruktur dargestellt und die für die verschiedenen Netze fest hinterlegten Firewall-Regeln beschrieben.

Tabelle 5 Firewall-Regeln für das Netz der Telematik

<b>Telematikinfrastruktur</b>	
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	<ul style="list-style-type: none"> <li>▪ Sicherstellung, dass alle Pakete, die für die Kommunikation mit einem Fachdienst bestimmt sind, ausschließlich über den VPN-Tunnel der TI übertragen werden.</li> <li>▪ Verwerfen aller Pakete aus dem Netz des Leistungserbringers</li> <li>▪ Verwerfen aller Pakete, die an den Konnektor gehen</li> <li>▪ Die Verbindung ist nur vom T-Systems Konnektor und vom Fachmodul erlaubt</li> </ul>
Netz der offenen Fachdienste	<ul style="list-style-type: none"> <li>▪ Sicherstellung, dass alle Pakete, die für die Kommunikation mit einem Fachdienst bestimmt sind, ausschließlich über den VPN-Tunnel der TI übertragen werden.</li> <li>▪ Verwerfen aller vom Konnektor initiierten Pakete</li> <li>▪ Verwerfen aller Pakete, die an den Konnektor gehen</li> <li>▪ Die Verbindung ist nur vom Netz des Leistungserbringers und vom Fachmodul erlaubt</li> </ul>
Netz der zentralen TI	<ul style="list-style-type: none"> <li>▪ Sicherstellung, dass alle Pakete, die für die Kommunikation mit einem Fachdienst bestimmt sind, ausschließlich über den VPN-Tunnel der TI übertragen werden.</li> <li>▪ Verwerfen aller Pakete aus dem Netz des Leistungserbringers</li> <li>▪ Verwerfen aller Pakete, die an den Konnektor gehen</li> <li>▪ Die Verbindung ist nur vom T-Systems Konnektor erlaubt</li> </ul>
Netz der dezentralen TI	<ul style="list-style-type: none"> <li>▪ Verwerfen aller Pakete vom Konnektor und an den Konnektor gehend</li> <li>▪ Verwerfen aller Pakete aus dem Netz des Leistungserbringers</li> </ul>

Tabelle 6 Firewall-Regeln für das Internet

<b>Internet</b>
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)

---

**Internet**


---

Für die verschiedenen Netzsegmente gelten folgende Regeln:

Netz des SIS	<ul style="list-style-type: none"> <li>▪ Verwerfen aller Pakete vom Konnektor und an den Konnektor gehend</li> <li>▪ Verwerfen aller Pakete aus dem Netz des Leistungserbringers</li> </ul>
Internet via SIS	<ul style="list-style-type: none"> <li>▪ Verwerfen aller Pakete aus dem Netz des Leistungserbringers, wenn kein Internet-Modus SIS konfiguriert wurde (siehe Abschnitt 6.2)</li> <li>▪ Umleitung aller Pakete aus dem Netz des Leistungserbringers an Hosts im Internet, wenn der Internet-Modus SIS konfiguriert wurde (siehe Abschnitt 6.2)</li> <li>Verwerfen aller Pakete, die an den Konnektor und an das Netz des Leistungserbringers gesendet werden</li> <li>▪ Die Verbindung ist nur erlaubt vom Konnektor und vom Netz des Leistungserbringers, wenn der Internet-Modus SIS konfiguriert wurde</li> </ul>
Internet via IAG (Internet Access Gateway)	<ul style="list-style-type: none"> <li>▪ Beim Anbindungsmodus <b>Parallel</b> werden alle Pakete verworfen, die nicht an die LAN-IP-Adresse adressiert sind und nicht aus dem Netz des Leistungserbringers stammen</li> <li>▪ Beim Anbindungsmodus <b>InReihe</b> werden alle Pakete verworfen, die nicht an die WAN-IP-Adresse adressiert sind</li> <li>▪ Kommunikation ist erlaubt für das Protokoll IPsec zu den VPN-Konzentratoren der TI bzw. des SIS</li> <li>▪ Kommunikation ist ausgehend erlaubt für das Protokoll HTTP und HTTPS zu den Provideradressen der CRL, des DNS Root Anchors, des Hash- &amp; URL-Servers und des Registrierungsservers</li> <li>▪ Kommunikation ist ausgehend erlaubt für das Protokoll DNS</li> <li>▪ Blockieren der Kommunikation aus dem Netz des Leistungserbringers für die Fälle: <ul style="list-style-type: none"> <li>▪ Internet-Modus = Keiner (siehe Abschnitt 6.2)</li> <li>▪ Internet-Modus = Verbindungsstatus zur TI = Nicht möglich (siehe Abschnitt 6.1)</li> <li>▪ Internet-Modus = Leistungsumfang Logisch getrennt (siehe Abschnitt 7.2) <b>Dieses Feature ist abgekündigt und soll nicht mehr verwendet werden.</b></li> </ul> </li> <li>▪ 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</li> <li>▪ Blockieren aller Pakete aus Richtung des IAG</li> </ul>

---

Tabelle 7 Firewall-Regeln 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 vorhandenen Zonen, 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, ist dieses Segment in der Konfiguration aktiviert (siehe Kapitel 6.5). Es wird der Untermenge **Aktive Bestandsnetze** zugeordnet.

- 
- |                                |  |
|--------------------------------|--|
| Netz der aktiven Bestandsnetze | <ul style="list-style-type: none"> <li>▪ Sicherstellung, dass alle Pakete, die für die Kommunikation mit einem Fachdienst bestimmt sind, ausschließlich über den VPN-Tunnel der TI übertragen werden.</li> <li>▪ Wenn der Konnektor für die logische Separation konfiguriert wurde, werden alle Pakete verworfen, die aus dem Netz des Leistungserbringers kommen. <b>Dieses Feature ist abgekündigt und soll nicht mehr verwendet werden.</b></li> <li>▪ Verwerfen aller Pakete an nicht freigegebene Bestandsnetze</li> <li>▪ Verwerfen aller Pakete, die an den Konnektor gehen</li> <li>▪ Die Verbindung ist nur erlaubt vom Konnektor für DNS und vom Netz des Leistungserbringers</li> </ul> |
|--------------------------------|--|
- 

Tabelle 8 Firewall-Regeln für das Netz des Leistungserbringers

---

**Netz des Leistungserbringers**


---

Das ist das Netz der Praxen, Medizinischen Versorgungszentren, Krankenhäuser, Apotheken und weiteren Akteuren. 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 Firewall-Regeln

---

**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), 4 (IP in IP (encapsulation)), 17 (UDP), 6 (TCP) und 50 (ESP) möglich.
- 

Die Firewall des Konnektors bietet keinen Ersatz für einen Virenschanner 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 Telematikinfrastruktur aufzubauen.

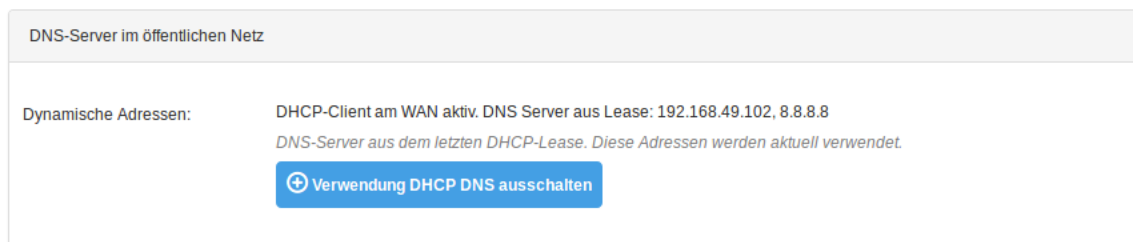


Abbildung 6 DHCP DNS ausschalten

## 3.6 Hinweise zur Zulassung / Sicherheitszertifizierung

Es kann jederzeit überprüft werden, ob die vorliegende Version des T-Systems Konnektors eine durch die gematik zugelassene und dementsprechend vom BSI sicherheitszertifizierte Produktversion ist.

### 3.6.1 Überprüfung auf Zulassung

Über die Oberfläche des T-Systems Konnektors können dessen Versionsnummern über [Hauptmenü > Systeminformationen](#) eingesehen werden.

Diese werden im Bereich [Produktversionen](#) angezeigt, siehe auch Tabelle 112 Produktdetails.

Die Versionsnummern müssen im Format [Firmware:Hardware](#) kombiniert werden, um sie mit den Produktversionen der Zulassungen für den Online-Produktivbetrieb der gematik abzugleichen.



Die gematik listet zugelassene Produkte für den Online-Produktivbetrieb auf unter:

<https://fachportal.gematik.de/zulassungen/online-produktivbetrieb/>

Es bietet sich an, die angebotenen Filter zu verwenden. Wird für Produkttyp: **Konnektor** und für Herstellername / Institution: **T-Systems International GmbH** ausgewählt, lassen sich die relevanten Versionen übersichtlich darstellen.

Die hier aufgelisteten Produkte können anhand der angezeigten Produktversion identifiziert werden. Die Produktversion setzt sich aus Firmware- und Hardwareversion zusammen. Die jeweils dreistelligen Versionsnummern werden durch einen Doppelpunkt getrennt. So steht zum Beispiel die Produktversion **1.5.3:2.2.4** für die zugelassene Produktversion des T-Systems Konnektors mit der Firmwareversion 1.5.3 und der Hardwareversion 2.2.4.

### 3.6.2 Überprüfung auf Sicherheitszertifizierung

Das BSI listet zertifizierte Produkte im Gesundheitswesen auf unter:

[https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/ZertifizierteProdukte/Gesundheitswesen/Gesundheitswesen\\_node.html](https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/ZertifizierteProdukte/Gesundheitswesen/Gesundheitswesen_node.html)

Im Bereich „Software“ ist der T-Systems Konnektor unter der Zertifizierungsnummer BSI-DSZ-CC-0928-V2 aufgelistet.

Hier sind die Zertifizierungsberichte bzw. Maintenance-Reports verfügbar und beziehen sich auf die Firmwareversion des T-Systems Konnektors.

## 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:



Abbildung 7 Unterseite des Konnektors / Typenschild

**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.



## 4.3 Anschlüsse

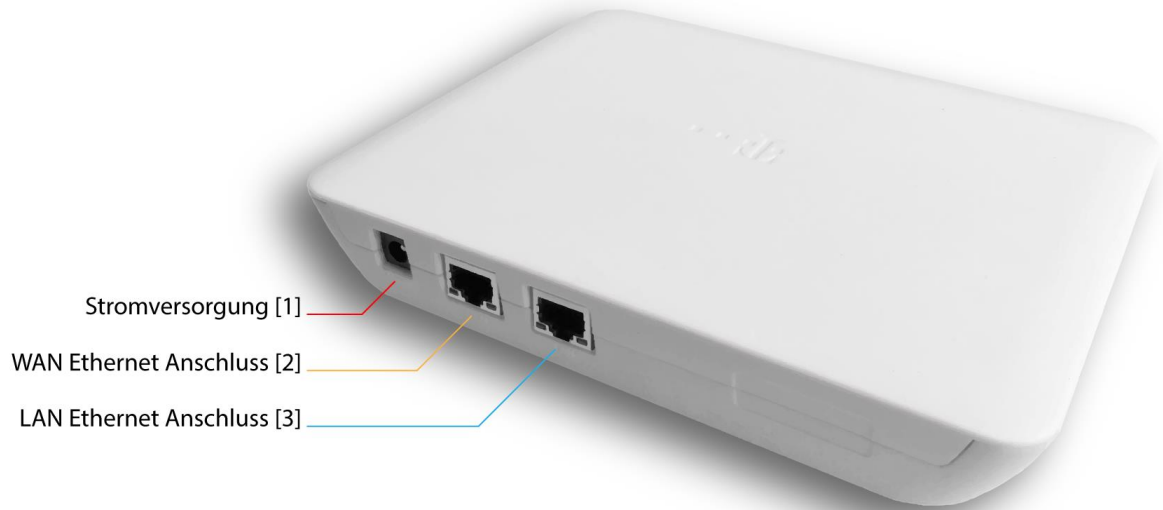


Abbildung 9 Anschlüsse des T-Systems Konnektors

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

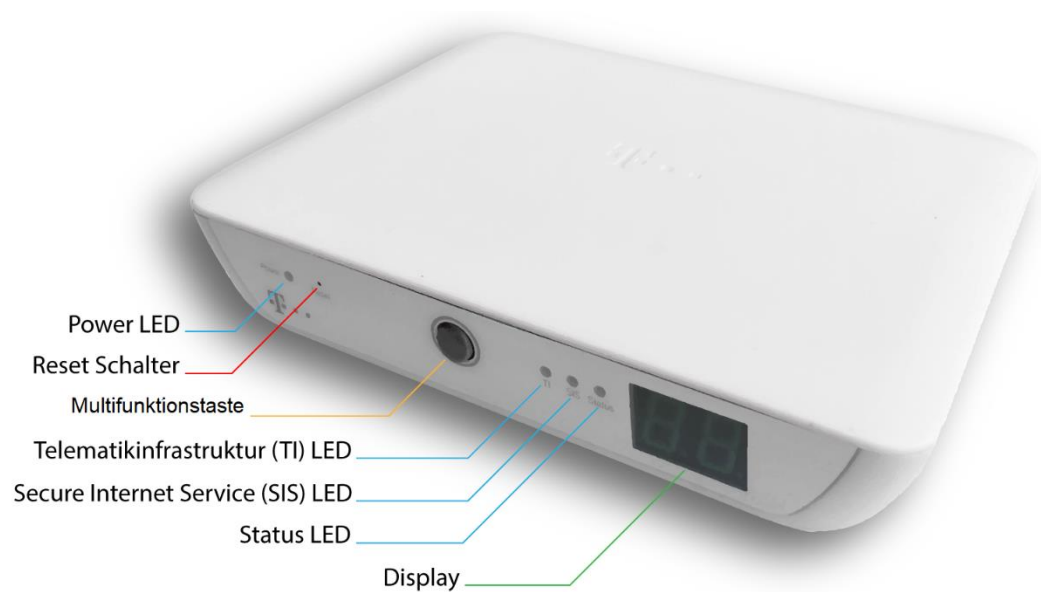


Abbildung 10 Leuchtdioden des T-Systems Konnektors

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 10 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 Anzeigestatus

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- / Shutdown-Vorgang.
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 <a href="#">10.1.14</a> und <a href="#">10.1.15</a> 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
- Multifunktionstaste

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 Multifunktionstaste (*Software Taste*) hat drei Funktionen.

1. Kurzes Drücken unter 3 Sekunden schaltet die Anzeige der Fehlercodes im Display durch (siehe hierzu Kapitel 4.4).
2. Langes Drücken über 3 Sekunden startet die Konnektorsoftware neu.
3. Doppelklick: Durch zweimaliges Drücken startet die Werksreset Routine (siehe hierzu Kapitel 7.14)

## 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:

- 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 Anbindungsmodus **Parallel** 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 Administrationsoberfläche 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 Administrationsoberfläche.

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 Administrationsoberfläche 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. Webbrowser öffnen und in der Adresszeile die Service-IP-Adresse eingeben.
2. Die Administrationsoberfläche zur Anmeldung am Konnektor wird geöffnet.
3. Erstanmeldung mit den Standard-Anmeldedaten. Siehe 5.1 Zugriff auf die Administrationsoberfläche, Tabelle 17 Standardkonfigurationsdaten.
4. Die Administrationsoberfläche zur Änderung des Passwortes wird geöffnet.

Abbildung 11 Administrationsoberfläche / Passwort ändern

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 neue Passwort wiederholt eingeben.
8. Mit der Schaltfläche „**Passwort ändern**“ das neue Passwort speichern.
9. Es wird erneut die Administrationsoberfläche zur Anmeldung am Konnektor



aufgerufen.

10. Anmeldung mit den neuen Login-Daten.
11. Die Administrationsoberfläche 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 Administrationsoberfläche 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 im öffentlichen Netz

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 „**Hinzufügen**“ die IP-Adresse speichern. Die IP-Adresse wird in der Liste „**Server**“ im Abschnitt „**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 „Eigene 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 Administrationsoberfläche aufrufen.

Abbildung 12 Administrationsoberfläche / DNS Root Anker

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 WAN-IP über DHCP **InReihe**-Modus:

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

Statische WAN-IP ohne DHCP **InReihe**-Modus:

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

Anbindungsmodus **Parallel** - WAN Adapter ausschalten:

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

The screenshot shows the WAN configuration page. At the top, it says 'WAN'. Below that, the 'Aktueller Status:' is 'Adapter aktiv. Dynamische Konfiguration: 192.168.50.142/24 (Subnetz: 255.255.255.0)'. There is a 'DHCP-Lease erneuern' button and a note: 'Der DHCP-Lease für die WAN-Netzwerkschnittstelle wird erneuert.' The 'WAN-Adapter:' is currently set to 'An'. The 'DHCP:' is set to 'Aus'. The 'IP-Adresse:' is '192.168.50.142', 'Subnetzmaske:' is '255.255.255.0', and 'IP-Paketlänge:' is '1500'. The 'DNS-Adressen:' are '192.168.49.102, 8.8.8.8' with a note 'DNS-Adressen aus dem letzten DHCP-Lease.' The 'Internet-Modus:' is set to 'SIS'.

Abbildung 13 Administrationsoberfläche / WAN Adapter ausschalten

## 4.7.5.2 LAN Segment

### Dynamische LAN-IP über DHCP im Reihen-Modus:

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

### Statische LAN-IP ohne DHCP im Reihen-Modus:

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

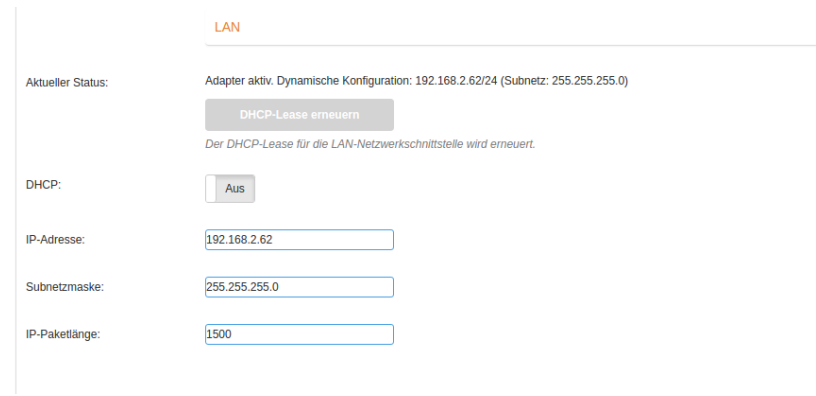


Abbildung 14 Administrationsoberfläche / DHCP Ein-Ausschalten

### 4.7.5.3 TSL hochladen / CRL hochladen

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

Manuell können TSLs nur im „Offline“ Modus hochgeladen werden. Daher ist der „Online“ Modus auszuschalten.

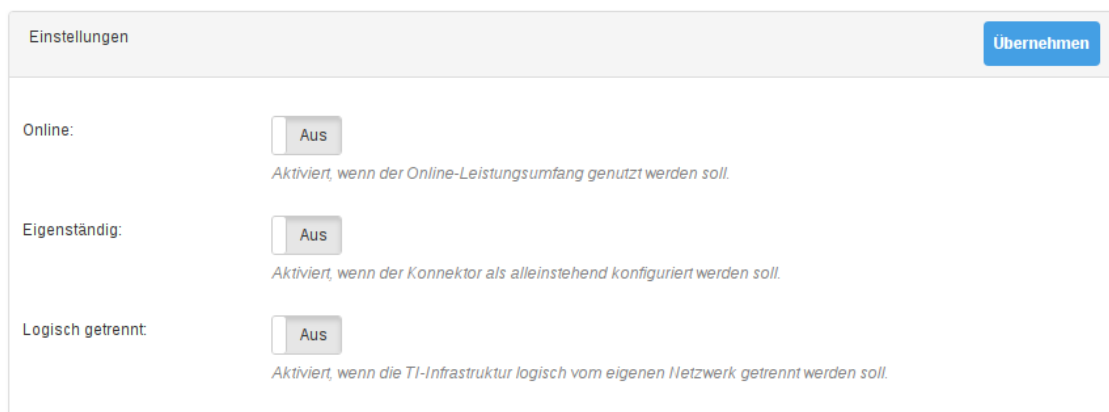


Abbildung 15 Administrationsoberfläche / Online Modus Ausschalten

Wird vom „Online“ in den „Offline“ Modus geschaltet, so erfordert dieser Wechsel einen Neustart der Netzadapter.

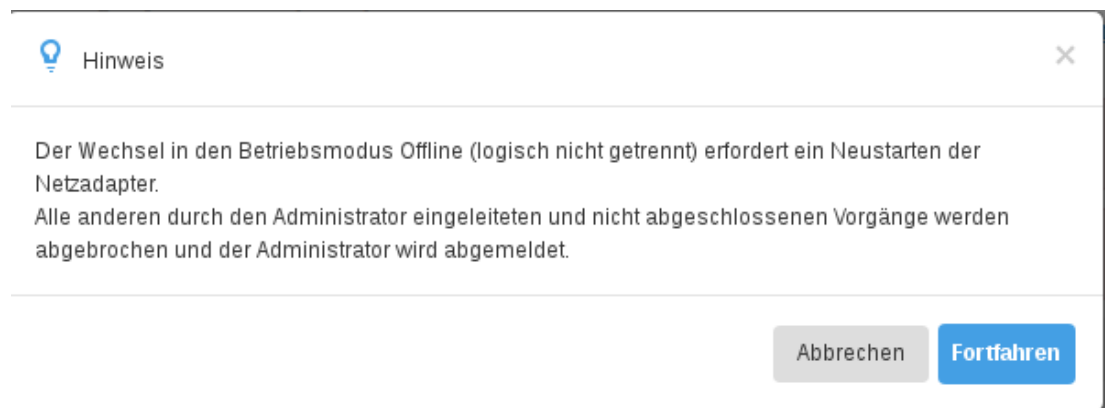


Abbildung 16 Administrationsoberfläche / Hinweis Offline Modus

#### Weitere Schritte zum Hochladen von TSLs:

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.

**Hinweis:** Bei der Erstinstallation zeigt die Administrationsoberfläche an, dass der Konnektor sich im kritischen Zustand befindet. Dies liegt daran, dass der Konnektor initial ohne TSL ausgeliefert wird.

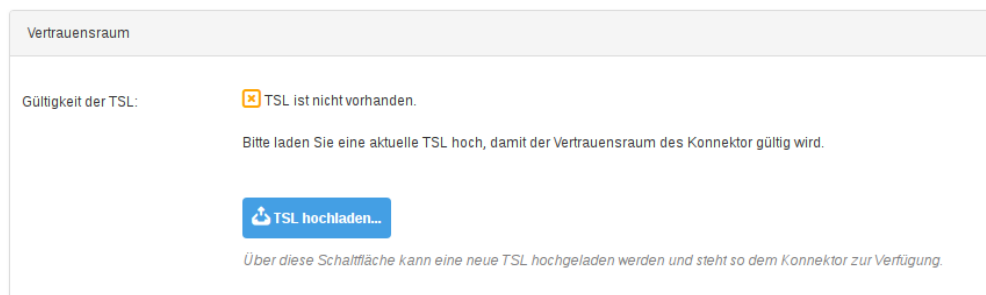


Abbildung 17 Administrationsoberfläche / TSL Upload

8. Die initiale TSL hochladen, welche unter <https://download.tsl.ti-dienste.de/TSL.xml> bereitgestellt wird.

**Hinweis:** Vor dem Import der aktuellen TSL muss ggf. je nach gSMC-K-Zertifikat des Konnektors zunächst eine TSL mit der Ankündigung des Vertrauensankerwechsels von CA3 auf CA27 importiert werden. Für den Bezug einer entsprechenden TSL wenden Sie sich bitte an den Hersteller des Konnektors (siehe A.1.3).

9. Ein Hinweisfenster zeigt an, dass die TSL aktualisiert wurde.
10. Die TSL Eigenschaften im Abschnitt „**Vertrauensraum**“ werden entsprechend der

- hochgeladenen TSL angezeigt.
11. Im Abschnitt „**Einstellungen**“ sind die CRL Download-Adressen zu finden.
  12. Nach dem Download der CRL vom angezeigten Downloadpunkt muss diese über die Schaltfläche „**CRL hochladen...**“ in den Konnektor geladen werden.
  13. Ein Hinweisenfenster zeigt an, dass die CRL aktualisiert wurde.
  14. Die CRL Eigenschaften im Abschnitt „**Vertrauensraum**“ werden entsprechend der hochgeladenen CRL angezeigt.
  15. Das „Hauptmenü“ der Administrationsoberfläche aufrufen.
  16. Aufrufen der Seite „**Leistungsumfang**“.
  17. Im Abschnitt „**Einstellungen**“ die Schaltfläche „**Online**“ von „**Aus**“ auf „**An**“ schalten.

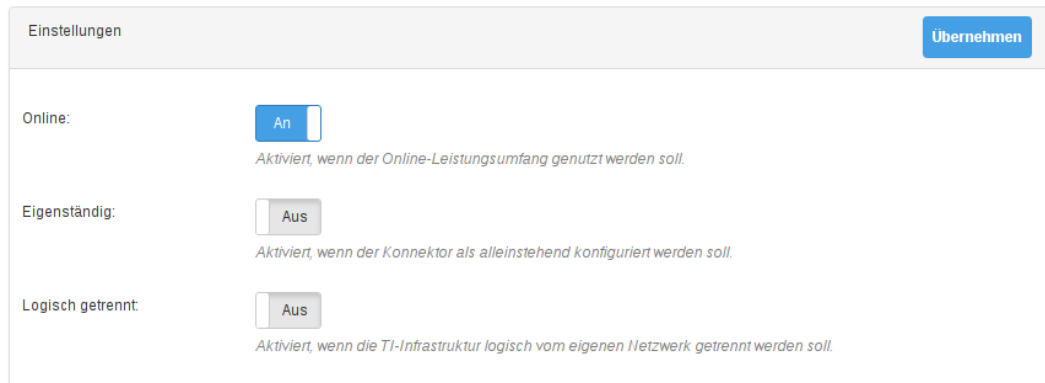


Abbildung 18 Administrationsoberfläche / Online Modus Einschalten

18. Mit der Schaltfläche „**Übernehmen**“ die Änderungen speichern.
19. Die Hinweismeldung mit der Schaltfläche „**Fortfahren**“ bestätigen.
20. Das erneute Login durchführen.

**Vertrauensraum**

Gültigkeit der TSL:  TSL ist gültig.

TSL Herausgeber: (CN=TSL Signing Unit 7 TEST-ONLY, IssuerCN=GEM.TSL-CA27 TEST-ONLY)

TSL Sequenznummer: 715

TSL-Dienst Startzeit: 28.02.2018 00:00:51+0100

TSL Erstellungszeit: 14.09.2018 01:00:00+0200

TSL Nächstes Update: 14.10.2018 01:00:00+0200

Fingerprint des TSL-Signer-Zertifikats: 443CD4A847E74BD4147E4DFD2B89057F97A2EBE8

Gültigkeit der CRL:  CRL ist gültig.

CRL Herausgeber: C=DE, O=arvato Systems GmbH NOT-VALID, CN=GEM.CRL3 TEST-ONLY

CRL Sequenznummer: 424

CRL Erstellungszeit: 25.09.2018 05:00:42+0200

CRL Nächstes Update: 02.10.2018 05:00:00+0200

[TSL hochladen...](#)

Über diese Schaltfläche kann eine neue TSL hochgeladen werden und steht so dem Konnektor zur Verfügung.

[CRL hochladen...](#)

Über diese Schaltfläche können neue Sperrlisten hochgeladen werden und stehen so dem Konnektor zur Verfügung.

Abbildung 19 Administrationsoberfläche / Übersicht TSL und CRL

**Wichtiger Hinweis:** Ist nach dem initialen Hochladen der TSL der Konnektor immer online, wird er die TSL zukünftig selbst aus der TI beziehen und aktualisieren. Die Gültigkeitsdauer der TSL wird auf der Administrationsoberfläche angezeigt. Nach Ablauf der Gültigkeit der TSL wird eine Grace Period von weiteren 30 Tagen gewährt. Ist auch diese verstrichen, dann muss vom obigen Downloadpunkt manuell eine TSL bezogen werden und über die Administrationsoberfläche in den Konnektor importiert werden.

#### 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 gefundenen 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.

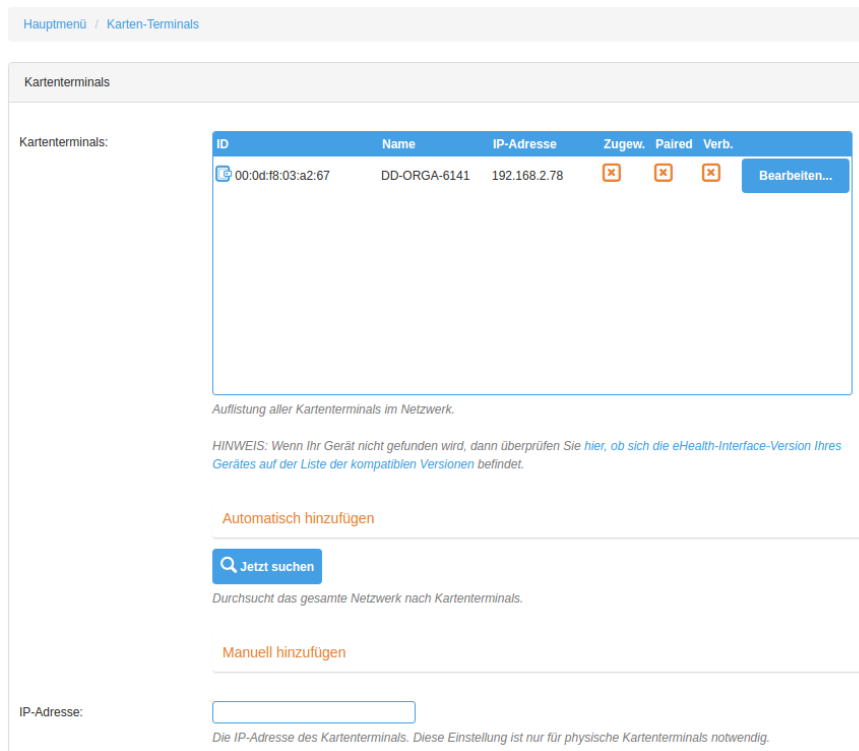


Abbildung 20 Administrationsoberfläche / Anzeige der verbundenen Kartenterminals

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

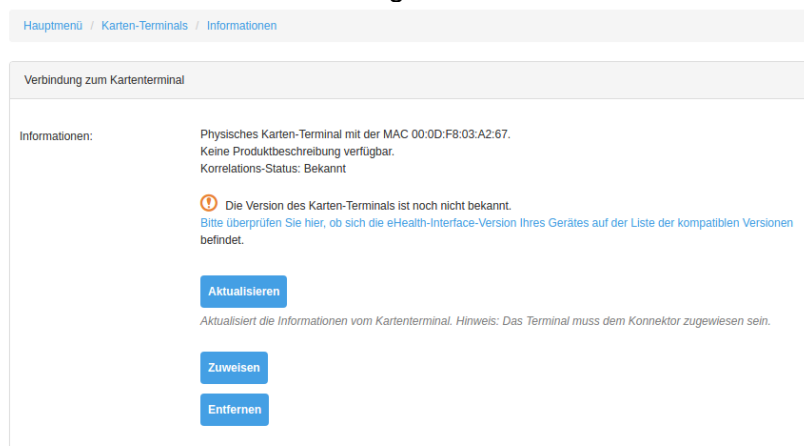


Abbildung 21 Administrationsoberfläche / Verbindungsaufbau zum Kartenterminal

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**“.
    - a. Sollten alle Pairingblöcke des Kartenterminals belegt sein, erscheint eine Hinweismeldung. In dem Fall sind die Pairingblöcke über das Kartenterminal-Menü vorher zu löschen und der Schritt zu wiederholen
  10. Ein Hinweifenster 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 Administrationsoberfläche 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.

Hauptmenü / Zugriffsberechtigungen

**Einstellungen** Übernehmen

---

TLS erforderlich:  **An**  
Diese Option gibt an, ob eine verschlüsselte Verbindung zwischen Clientsystem und Konnektor genutzt werden muss.

Authentifizierung erforderlich:  **An**  
Gibt an, ob eine Clientsystem-Authentifizierung verpflichtend ist.

Authentifizierungsmodus:  ▼

Offener Dienstverzeichnisdienst:  **An**  
Angabe, ob der Dienstverzeichnisdienst über eine ungesicherte Verbindung erreichbar ist.

**Clientsysteme**

---

Clientsysteme:

Clientssystem-ID	Beschreibung

Abbildung 22 Administrationsoberfläche / Sichere Verbindung zum Client

1. Aufrufen der Seite „**Zugriffsberechtigung**“.
2. Im Abschnitt „**Clientsysteme**“ die „**Clientssystem-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.

The screenshot shows the 'Arbeitsplatz' administration interface. At the top, there is a header 'Arbeitsplatz'. Below it, the label 'Arbeitsplätze:' is followed by a table. The table has two columns: 'ID' and 'Beschreibung'. The first row contains the value 'Arbeitsplatz1' in the 'ID' column. To the right of the table, there are two buttons: 'Bearbeiten' and 'Löschen'. Below the table, there are two input fields. The first is labeled 'Arbeitsplatz-ID:' and contains the text 'Arbeitsplatz1'. Below it is a small grey text: 'ID des neu anzulegenden Arbeitsplatzes'. The second input field is labeled 'Beschreibung:' and is empty. Below it is a small grey text: 'Beschreibung des neuen Arbeitsplatzes (optional)'. At the bottom, there is a blue button with a plus sign and the text 'Arbeitsplatz hinzufügen'.

Abbildung 23 Administrationsoberfläche / Anzeige verbundenen Arbeitsplätze

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 Administrationsoberfläche aufrufen.

#### 4.7.5.6 Konnektor registrieren

Damit der Konnektor als Element zur sicheren Kommunikation zwischen dem Netz der Praxen, Medizinischen Versorgungszentren, Krankenhäuser, Apotheken, weiteren Akteuren und der Telematikinfrastruktur korrekt arbeitet, muss der Konnektor beim Anbieter des VPN-Dienstes registriert werden.

**Hinweis:** Für eine Registrierung muss sich der Konnektor im Betriebsmodus „**Online**“ befinden.

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

The screenshot shows the 'Registrierung' (Registration) page. At the top, there is a breadcrumb 'Hauptmenü / Registrierung'. Below this, there are two main sections:

- Status:** A section with a title 'Status'. It contains a message: 'Der Konnektor ist nicht registriert' (The connector is not registered) with a red 'x' icon. Below the message is a blue button labeled 'Status überprüfen' (Check status).
- Registrieren:** A section with a title 'Registrieren'. It contains two input fields:
  - SMB:** A dropdown menu with the selected value '80276883110000003270: Mandat'. Below it is the text 'SMB-Karte, die zur Registrierung genutzt werden soll.' (SMB card to be used for registration).
  - Vertragsnummer:** An empty text input field. Below it is the text 'Die Vertragsnummer zur Registrierung des Konnektors mit der ausgewählten SMB.' (The contract number for registration of the connector with the selected SMB).
 Below these fields is a blue button labeled 'Konnektor registrieren' (Register connector). At the bottom of this section is a note: 'Über diese Schaltfläche wird der Konnektor registriert. Bitte beachten Sie, dass zur Registrierung eine SMB-Karte verfügbar sein muss und eine gültige Vertragsnummer vorhanden ist!' (Via this button the connector is registered. Please note that for registration an SMB card must be available and a valid contract number must be present!).

Abbildung 24 Administrationsoberfläche / Konnektor an TI registrieren

4. In das Eingabefeld „**Vertragsnummer**“ die Vertragsnummer eintragen.
5. Mit der Schaltfläche „**Konnektor registrieren**“ den Konnektor registrieren.
6. Im Kartenterminal muss die SMB Pin verifiziert werden.
7. 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 dass der Zugriff auf TI und gegebenenfalls auf SIS besteht ja nach Vertragsvereinbarung. 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

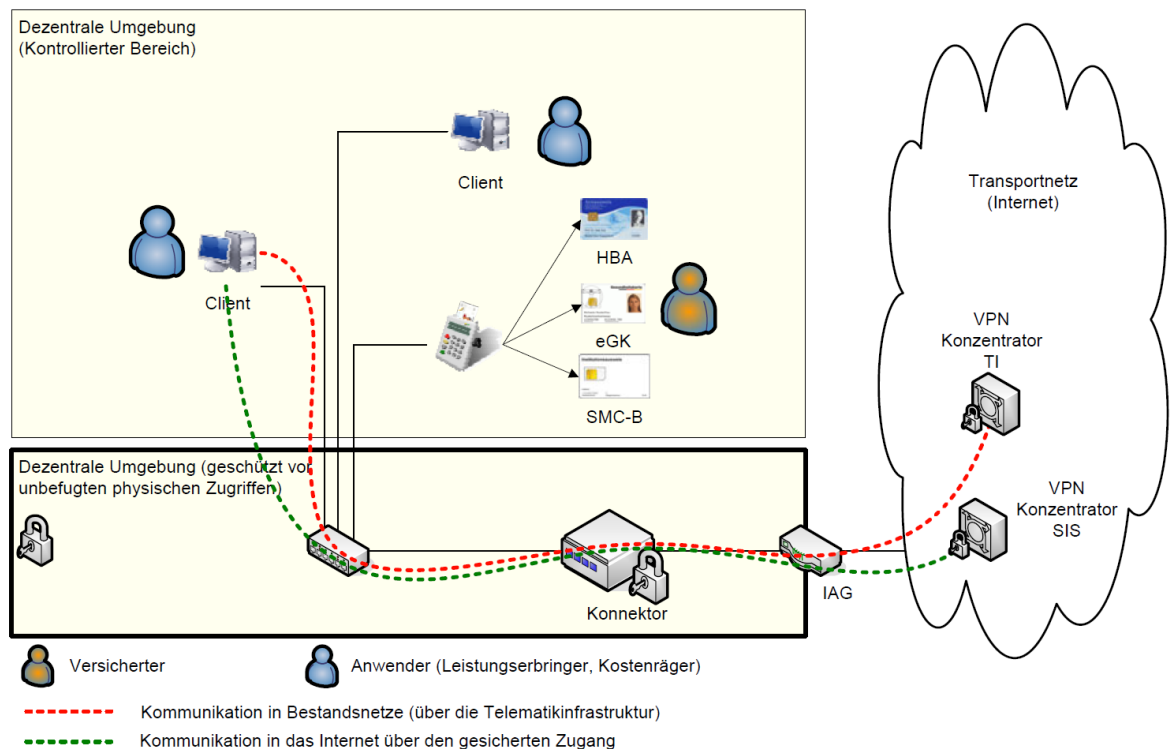


Abbildung 25 Szenario einfache Installation aus gemSpec\_KON\_V4.11.1, S.498

### 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

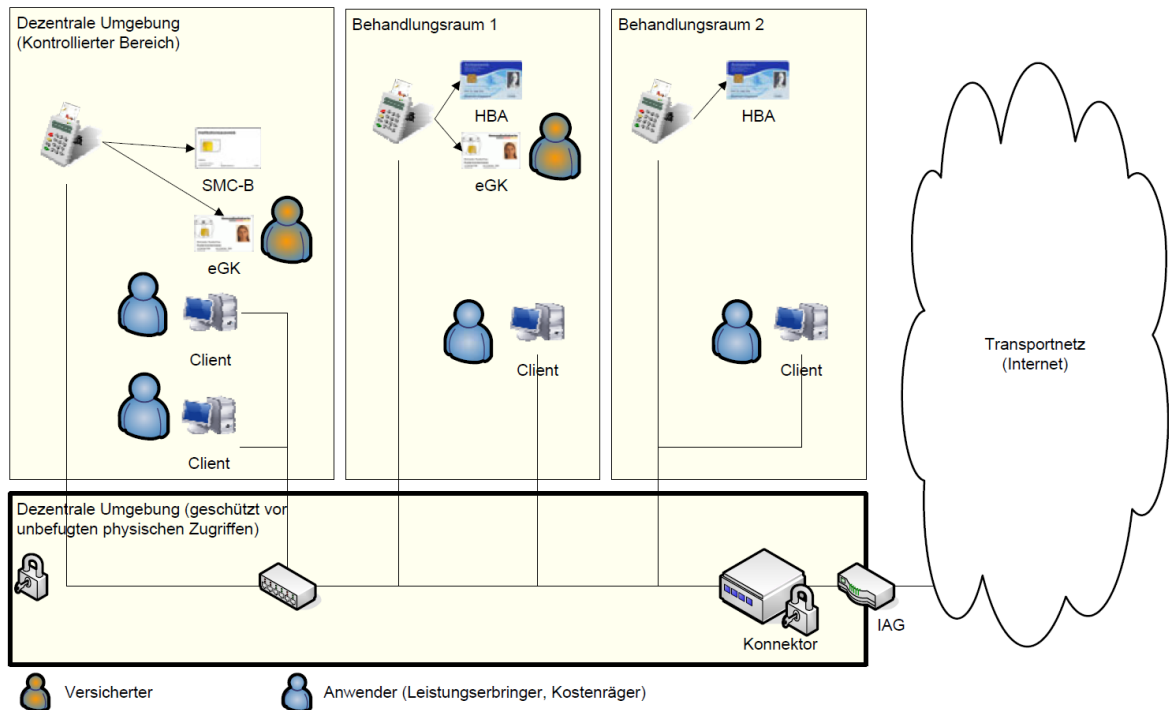


Abbildung 26 Szenario einer Installation mit mehreren Behandlungsräumen aus gemSpec\_KON\_V4.11.1, S.500

### 4.7.7.1 Erläuterung

Mit der in Szenario 1 ([Abbildung 25 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 Kartenterminal nötig, 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

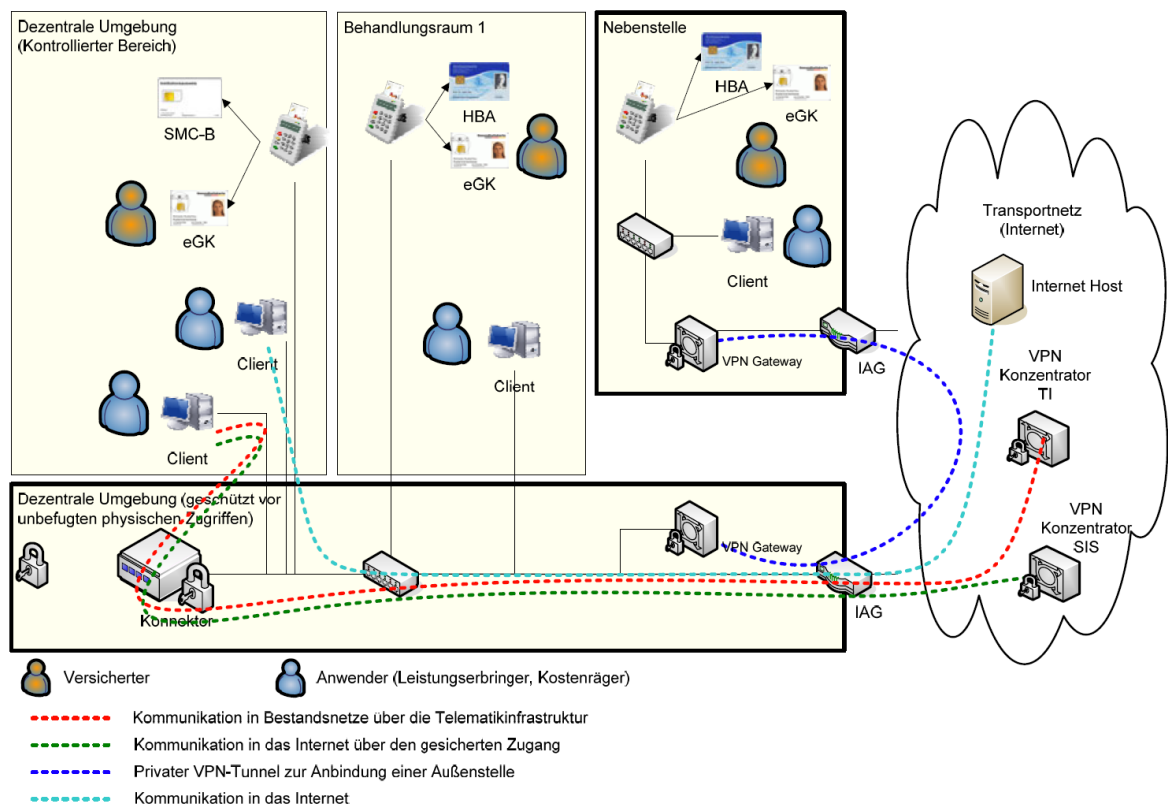


Abbildung 27 Szenario einer Integration in bestehende Infrastruktur aus gemSpec\_KON\_V4.11.1, S.501

### 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

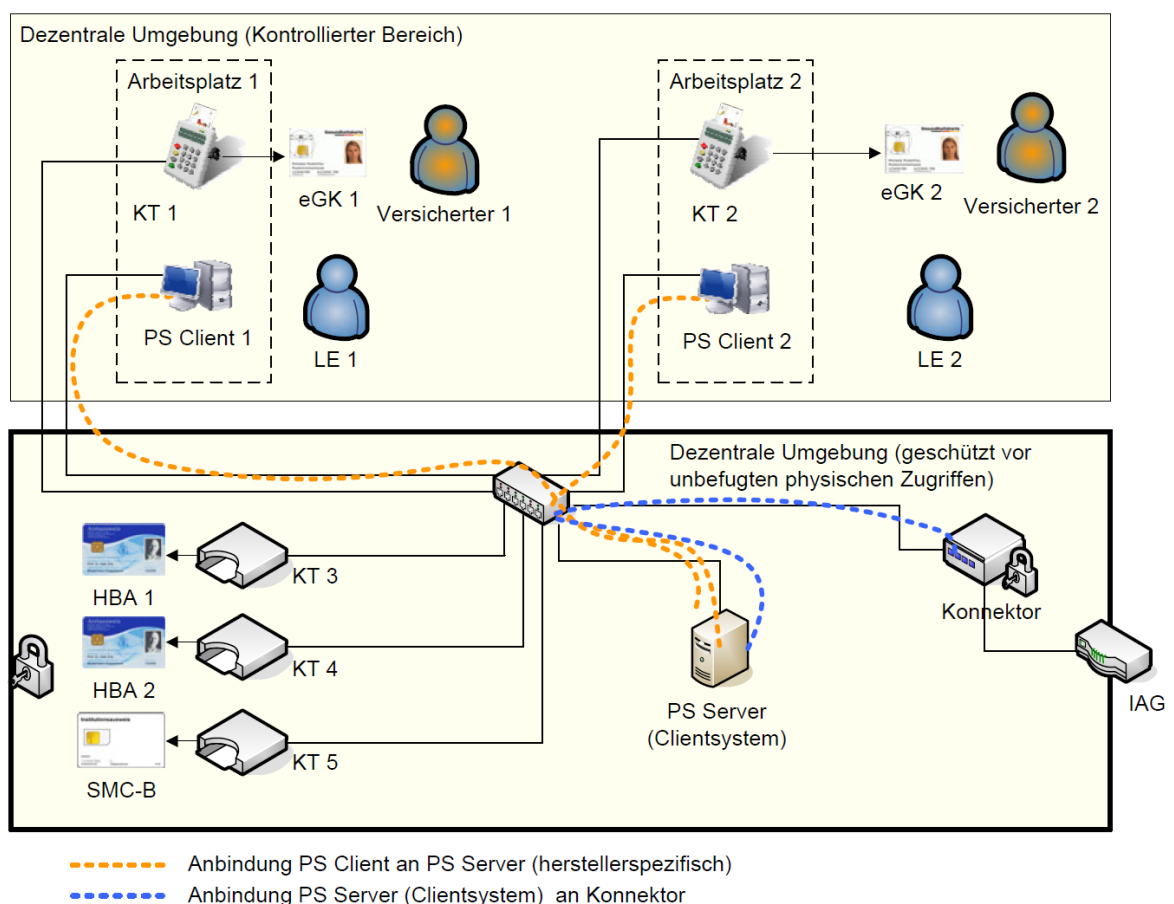


Abbildung 28 Szenario einer Installation mit zentralem Primärsystem als Clientsystem aus gemSpec\_KON\_V4.11.1, S.506

### 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 href="#">A.1 Kontakt</a> ).
Der Selbsttest schlägt fehl.	Der T-Systems Konnektor kann nicht benutzt werden. Sie haben keinen Zugriff auf die Administrationsoberfläche und die externen Schnittstellen. Weitere Informationen hierzu finden Sie in Kapitel <a href="#">4.8.2</a> .

### 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 Administrationsoberfläche 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 Administrationsoberfläche 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 Administrationsoberfläche, 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 Administrationsoberfläche 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 Administrationsoberfläche 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 Administrationsoberfläche 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
	<p>Ist der Konnektor mit dem WAN verbunden und hat der Konnektor eine gültige IP-Adresse?</p> <p>Ist die am Konnektor eingestellte Uhrzeit korrekt?</p> <p>Hat der Konnektor eine aktuelle Sperrliste zur Verfügung?</p> <p>Ist die Trusted Service List (TSL) aktuell?</p> <p>Lässt Ihr Internetanbieter gesicherte VPN-Verbindungen zu?</p> <p>Kann das Problem nicht durch eine der angegebenen Maßnahmen behoben werden, kontaktieren Sie einen Servicetechniker oder den Hersteller zur weiteren Unterstützung.</p>
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 Warmmeldungen 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 Administrationsoberfläche 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_ALARM	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 Praxen, Medizinischen Versorgungszentren, Krankenhäuser, Apotheken, weiteren Akteuren 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 [7.14 Werksreset durchführen](#) beschrieben. Anschließend muss ein neues Passwort vergeben werden. Siehe dazu auch Kapitel [7.14.1 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 Ihr Praxis, Medizinisches Versorgungszentrum, Krankenhaus, Apotheke oder weiterer Akteur 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.

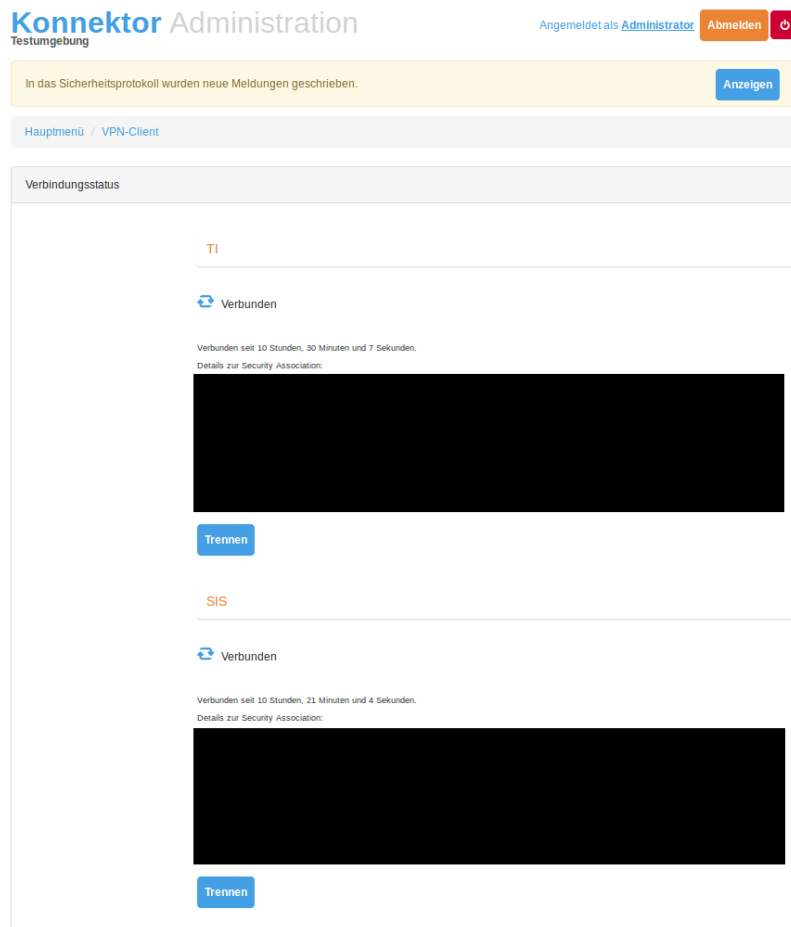


Abbildung 29 Administrationsoberfläche / Verbindung zur TI trennen

## 4.13.1 Deregistrierung

1. Unter **Hauptmenü** > **Registrierung** auswählen

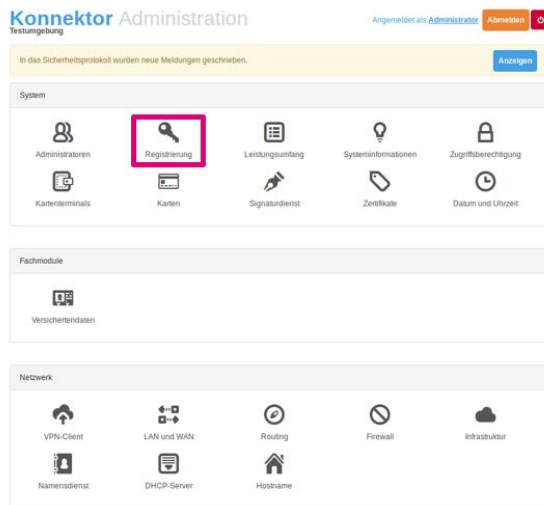


Abbildung 30 Administrationsoberfläche / Registrierung

2. Unter **Registrierung** > „**Registrierung zurücknehmen**“ auswählen

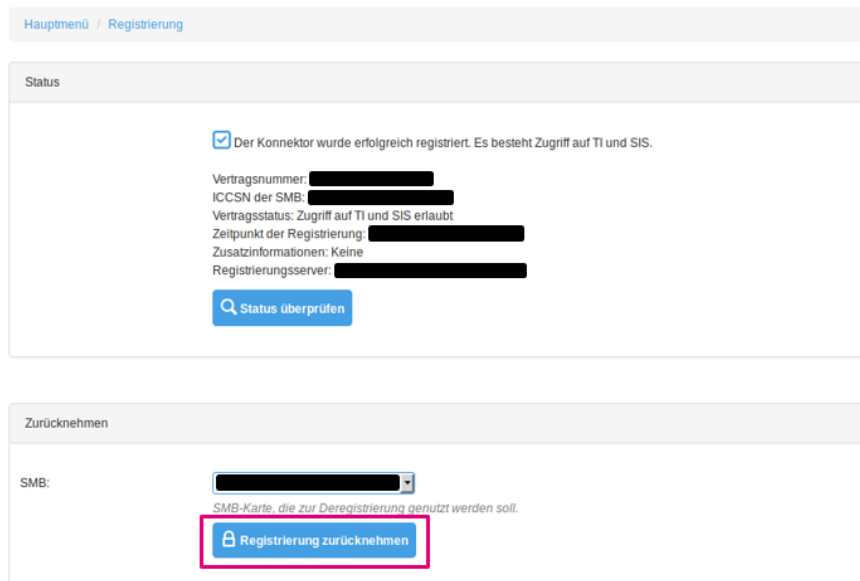


Abbildung 31 Administrationsoberfläche / Registrierung zurücknehmen

## 4.13.2 Finale Außerbetriebnahme und Rücktransport

**WICHTIG: BITTE RUFEN SIE ZWINGEND DEN HERSTELLER (Siehe A.1.3) AN. HALTEN SIE HIERZU IHRE CONTRACTID UND DIE ICCSN (Typenschild auf der Unterseite des Konnektors siehe 4.1.1) BEREIT.**

1. Unter **Hauptmenü > Registrierung** auswählen

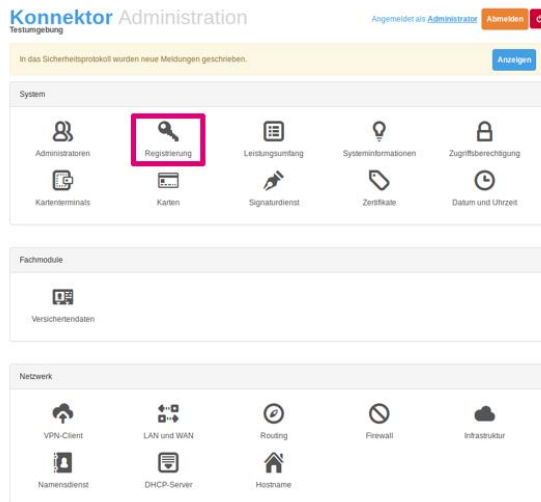


Abbildung 32 Administrationsoberfläche / Registrierung

2. Unter **Registrierung > die Funktion „Konnektor Außerbetriebnehmen“** auswählen.



Abbildung 33 Administrationsoberfläche / Außerbetriebnahme

**Achtung: Ab jetzt kann kein VPN-Tunnel zur Telematikinfrastruktur mehr aufgebaut werden!**

Sicherheitsabfrage ×

---

Wenn sie fortfahren, dann werden alle Daten gelöscht und die gSMC-K zerstört. Der Konnektor ist dann nicht mehr funktionsfähig - dies kann NICHT rückgängig gemacht werden! Bitte rufen Sie zwingend den Hersteller an, bevor sie das Gerät außer Betrieb setzen.  
Möchten Sie den Konnektor wirklich außer Betrieb nehmen?

---

Ja, ich kenne das Risiko
Abbrechen

Abbildung 34 Administrationsoberfläche / Sicherheitsabfrage

### 3. Eingabe der ICCSN (siehe Unterseite des Konnektors)

Bitte geben Sie zur Bestätigung der Außerbetriebnahme die ICCSN des Konnektors ein: ×

---

---

Abbrechen
Akzeptieren

Abbildung 35 Administrationsoberfläche / Eingabe der ICCSN

## Der Konnektor wird außer Betrieb genommen.

Das Gerät wird nun heruntergefahren, alle sicherheitsrelevanten Daten gelöscht und abschließend neu gestartet.  
Bitte beachten Sie, dass dies einige Zeit in Anspruch nehmen kann. Aktuelle Aktion:

**Der Konnektor ist nicht mehr erreichbar.**

Bitte prüfen Sie, ob nach dem automatischen Neustart auf dem Gerät der Fehlercode 93 sichtbar wird:



Dieser Code bestätigt, dass Ihre gSMC-K physisch zerstört wurde und nun das Gerät sicher entsorgt werden kann.  
Wenn dieser Fehlercode auch nach etwa 10 Minuten nicht im Display erscheint, dann kontaktieren Sie bitte die Hotline.

Abbildung 36 Administrationsoberfläche / Bestätigung „Konnektor außer Betrieb“

Der Konnektor ist nach dieser Meldung erfolgreich **außer Betrieb genommen**.

Kommt es zum Ende des Lebenszyklus des Konnektors, ist zunächst die zuvor beschriebene Außerbetriebnahme durchzuführen. Der Konnektor muss anschließend vom Leistungserbringer an den Hersteller T-Systems zurückgesendet werden, wenn der Gültigkeitszeitraum der Zertifikate (verbaute gSMC-K) abgelaufen ist oder kurz vor dem Ablauf steht. Der Leistungserbringer muss vor dem Versand des Konnektors auf einem beliebigen Weg das Gerät bei T-Systems als Betreiber des vom Leistungserbringer genutzten VPN-Zugangsdienstes abmelden. Der Betreiber deregistriert in diesem Fall die zugehörige gSMC-K im VPN-Zugangsdienst und veranlasst die Sperrung der gSMC-K-Zertifikate durch den Hersteller. Damit ist sichergestellt, dass ein solches Gerät nicht mehr mit der Telemedizininfrastruktur verbunden werden kann, sollte es während eines unsicheren Rücktransportes zum Hersteller verloren gehen oder entwendet werden. Darüber hinaus muss der Leistungserbringer einen Werks-Reset vor der Rücksendung des Geräts durchführen.

Nimmt der Endnutzer das Gerät vor Ablauf des Gültigkeitszeitraums der Zertifikate der gSMC-K vorübergehend außer Betrieb und lagert dieses ein, so muss er sicherstellen, dass das Gerät Zutrittsgeschützt (bspw. entsprechend den in der Praxis, des Medizinisches Versorgungszentrums, des Krankenhauses oder der Apotheke gelagerten Betäubungsmitteln) aufbewahrt wird.

Wird ein Konnektor am Ende seines Lebenszyklus an den Hersteller zurückgesendet oder wird eine Integritätsverletzung des Gerätes nach erfolgter Rücksendung festgestellt, so wird das Gehäuse geöffnet, die im Gerät verbaute gSMC-K entfernt und diese gSMC-K anschließend durch Schreddern vernichtet. Das verbleibende Gerät wird ebenfalls vollständig durch Schreddern vernichtet. Die Zertifikate der verbauten gSMC-K des betroffenen Geräts werden bzw. sind bereits gesperrt.

### 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-Netzkabels 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-Netzkabels 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 Administrationsoberfläche 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 Administrationsoberfläche leitet die entgegengenommenen Konfigurationsparameter an den T-Systems Konnektor weiter.

### 5.1 Zugriff auf die Administrationsoberfläche

Die Administrationsschnittstelle (Zugriff erläutert unter 4.7.1) und somit die Administrationsoberfläche 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	<a href="http://support.apple.com/de_DE/downloads/safari">support.apple.com/de_DE/downloads/safari</a>
Chromium Browser	ab Version 34.0	<a href="http://chromium.woolyss.com/download/de">chromium.woolyss.com/download/de</a>
Google Chrome	ab Version 34.0	<a href="http://www.google.de/chrome">www.google.de/chrome</a>
Microsoft Edge	ab Version 1.0	<a href="http://www.microsoft.com/de-de/windows/microsoft-edge">www.microsoft.com/de-de/windows/microsoft-edge</a>
Microsoft Internet Explorer	ab Version 10.0	<a href="http://www.microsoft.com/de-de/download/internet-explorer.aspx">www.microsoft.com/de-de/download/internet-explorer.aspx</a>
Mozilla Firefox	ab Version 18.0	<a href="http://www.mozilla.org/de/firefox/">www.mozilla.org/de/firefox/</a>
Opera Browser	ab Version 15.0	<a href="http://www.opera.com/de/download">www.opera.com/de/download</a>

Der Konnektor verwendet zur Sicherung der Kommunikation ein elektronisches Zertifikat. Ihr Webbrowser muss beim ersten Zugriff auf den Konnektor eine Sicherheitswarnung anzeigen. Sie müssen das Zertifikat des Konnektors als vertrauenswürdigen 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 Administrationsoberfläche zuzugreifen.

### 5.1.1 Verwendung von Javascript und Sitzungs-Cookies

Die Administrationsschnittstelle verwendet Javascript. Wie die Verwendung von Javascript in Ihrem Browser eingeschaltet werden kann ist unter folgendem Link beschrieben: <https://www.enable-javascript.com/de/> . Ebenfalls verwendet der Konnektor Sitzungs-Cookies. Dies muss ebenfalls in Ihrem Browser eingeschaltet werden, damit die Administrationsschnittstelle einwandfrei funktioniert. Wie Sitzungs-Cookies für die jeweiligen Browser eingerichtet werden, kann von den Hilfe-Seiten der Browser Hersteller entnommen werden.

### 5.1.2 Änderung des Benutzerkennworts

Sie werden während des erstmaligen Logins aufgefordert, das Benutzerkennwort zu ändern (Kennwortänderung erläutert unter 4.7.1). Diesen Vorgang können Sie nicht umgehen. Bitte achten Sie darauf, dass das neue Passwort mehr als 16 Zeichen lang sein und aus einer zufälligen Folge von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen muss. 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.

### 5.1.3 LDAP-Proxy

Der Konnektor ermöglicht es Clientsystemen und Fachmodulen durch Nutzung des LDAP-Proxys 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 Client-system 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:

The screenshot shows the 'Konnektor Administration' interface. At the top right, it indicates the user is logged in as 'Administrator' with 'Abmelden' and a power icon. Below this are two notification bars: a yellow one stating 'In das Sicherheitsprotokoll wurden neue Meldungen geschrieben.' and a red one stating 'Der Konnektor befindet sich im kritischen Zustand.', both with 'Anzeigen' buttons. A breadcrumb trail shows 'Hauptmenü / Leistungsumfang'. The main content area is titled 'Einstellungen' and contains four settings:

- Online:** A toggle switch set to 'An'. Description: 'Aktiviert, wenn der Online-Leistungsumfang genutzt werden soll.'
- SAK:** A toggle switch set to 'An'. Description: 'Aktiviert, wenn der Signaturanwendungskomponenten-Leistungsumfang genutzt werden soll.'
- Eigenständig:** A toggle switch set to 'Aus'. Description: 'Aktiviert, wenn der Konnektor als alleinstehend konfiguriert werden soll.'
- Logisch getrennt:** A toggle switch set to 'Aus'. Description: 'Aktiviert, wenn die TI-Infrastruktur logisch vom eigenen Netzwerk getrennt werden soll.'

At the bottom, a copyright notice reads: '© 2018 T-Systems International GmbH. Die verbleibende Sitzungszeit beträgt 59 Minuten und 04 Sekunden'.

Abbildung 37 Administrationsoberfläche / LDAP Proxy konfigurieren

Die Konfiguration des Parameters „ANCL\_TLS\_MANDATORY“ lässt folgende Einstellungen zu:

The screenshot shows the 'Konnektor Administration' interface. At the top right, it indicates the user is logged in as 'Administrator' with 'Abmelden' and a power icon. Below this are two notification bars: a yellow one stating 'In das Sicherheitsprotokoll wurden neue Meldungen geschrieben.' and a red one stating 'Der Konnektor befindet sich im kritischen Zustand.', both with 'Anzeigen' buttons. A breadcrumb trail shows 'Hauptmenü / Zugriffsberechtigungen'. The main content area is titled 'Einstellungen' and contains four settings:

- TLS erforderlich:** A toggle switch set to 'Aus'. Description: 'Diese Option gibt an, ob eine verschlüsselte Verbindung zwischen Clientsystem und Konnektor genutzt werden muss.'
- Authentifizierung erforderlich:** A toggle switch set to 'Aus'. Description: 'Gibt an, ob eine Clientsystem-Authentifizierung verpflichtend ist.'
- Authentifizierungsmodus:** A dropdown menu set to 'Zertifikat'.
- Offener Dienstverzeichnisdienst:** A toggle switch set to 'An'.

Abbildung 38 Administrationsoberfläche / Zugriffsberechtigungen

## 5.2 Hauptmenü

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

**Konnektor Administration** Angemeldet als **Administrator** [Abmelden](#)

**System**

- Administratoren
- Registrierung
- Leistungsumfang
- Systeminformationen
- Zugriffsberechtigung
- Kartenterminals
- Karten
- Zertifikate
- Datum und Uhrzeit

**Fachmodule**

- Versichertendaten

**Netzwerk**

- VPN-Client
- LAN und WAN
- Routing
- Firewall
- Infrastruktur
- Namensdienst
- DHCP-Server
- Hostname

**Wartung**

- Protokollierung
- Betriebszustände
- Backup
- Update

Abbildung 39 Administrationsoberfläche / 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. **Systeminformationen**: erlaubt die Einsicht in die Versionsinformationen des Konnektors und ermöglicht die Konfiguration des Ereignisdienstes.
5. **Zugriffsberechtigungen**: erlaubt die Konfiguration und Einsichtnahme der Zugriffsberechtigungen für Clientsysteme, Arbeitsplätze, Mandanten, SMBs.
6. **Kartenterminals**: erlaubt die Einsichtnahme und Konfiguration zugeordneter Kartenterminals.
7. **Karten**: bietet eine Übersicht über vorhandene Karten in angeschlossenen Kartenterminals an.
8. **Zertifikate**: bietet Informationen zum aktuellen Vertrauensraum und erlaubt ebenso dessen Aktualisierung.
9. **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 neben der Einsichtnahme in vorhandene Protokolleinträge folgende Funktionen.
  - a. Export von Protokollen,
  - b. Konfigurationseinstellungen wie Detailgrad Systemprotokoll, Mindestspeicherdauer etc.,
  - c. Löschen von System-, Performance-, und den VSDM-Protokollen
2. **Betriebszustände**: erlaubt die Einsichtnahme in den Betriebszustand des Konnektors.
3. **Backup**: erlaubt den Im- und Export der Konnektoreinstellungen. Zudem besteht hier die Möglichkeit den Konnektor auf Werkseinstellung zurückzusetzen.
4. **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**
- **LAN- / WAN-Konfiguration (siehe Kapitel 4.7.5)**
- **Pairing eines Kartenterminals**
- **Einrichten eines Arbeitsplatzes**

### 5.3.1 Konfiguration der Zeit

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.

Sobald Sie Zugriff auf die Administrationsoberfläche 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.

**Warum ist es notwendig die Systemzeit des Konnektors einzustellen?**

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.

### 5.3.2 Pairing eines Kartenterminals

Bitte navigieren Sie zunächst zum **Menüpunkt Kartenterminals**, siehe 7.5.

Zum Pairing eines Kartenterminals müssen Sie Folgendes beachten:

Für das erfolgreiche Pairing benötigt das KT mindestens einen freien Pairingblock, ggf. ist vor dem Pairing über das Menü des Kartenterminals mindestens ein Pairingblock freizugeben.

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 Administrationsoberfläche 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 Auswahlménü **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.

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 18 Authentifizierungseinstellungen für Dienstverzeichnisdienst

Einstellungen	
TLS erforderlich	Ist dieser Schalter auf <b>An</b> konfiguriert, werden nur TLS-gesicherte Verbindungen akzeptiert. Bitte beachten Sie den Hinweis zum Punkt Offener Dienstverzeichnisdienst.
Authentifizierung erforderlich	Ist dieser Schalter auf <b>An</b> konfiguriert, muss das Clientsystem eine Authentifizierung durchführen
Authentifizierungsmodus	Das Auswahlmü 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 <b>TLS erforderlich</b> 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:

**Grundsätzlich empfiehlt der Hersteller, Updates einzuspielen, es sei denn, es sprechen explizit bekannte Probleme dagegen.**

Melden Sie sich als Administrator in der Administrationsoberfläche an.

3. Laden Sie unter Verwendung des **Menüpunkts Hauptmenü > Update > Paket-Verwaltung > Update hochladen** das Firmwarepaket zur Installation. Während dieses Vorgangs zeigt die Administrationsoberfläche einen Fortschrittsbalken an.
4. 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**.
5. 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**.
6. 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 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:** Die Konfigurationsparameter „TI bzw. SIS Sequenznummern Auswertung“ konfigurieren den Anti-Replay-Mechanismus der jeweiligen VPN-Verbindung. Der Wert 0 deaktiviert diesen Schutzmechanismus. Werte größer 0, wobei 32 der voreingestellte Standardwert ist, legen die Größe des Sequenznummernbereichs fest, den der Schutzmechanismus analysiert.

Tabelle 19 Menüpunkt VPN-Client Übersicht

VPN-Status	
Verbindungsstatus zur TI	<p>Hier wird mit folgenden Werten angezeigt, ob ein IPsec-Tunnel zur Telematik besteht:</p> <p><b>Getrennt und Tunnel-Aufbau blockiert</b> - 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.</p> <p><b>Getrennt</b> - 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 <b>Verbinden</b> verwenden, um eine IPsec-gesicherte Verbindung herzustellen.</p> <p><b>Verbunden</b> - 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 <b>Trennen</b>.</p>
<p><b>Hinweis:</b> Je nach Verbindungszustand kann die zugeordnete Schaltfläche folgende Optionen anbieten:</p> <ul style="list-style-type: none"> <li>▪ <b>Verbinden</b> - 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 Administrationsoberfläche mit Hilfe einer Fehlermeldung angezeigt. Um einen VPN-Tunnel zu etablieren, muss auf diese Fehlermeldungen reagiert werden.</li> <li>▪ <b>Trennen</b> - Es wurde ein Tunnel aufgebaut. Sie können mit Hilfe der Schaltfläche den Tunnel wieder abbauen.</li> <li>▪ <b>Verbinden [deaktiviert]</b> - 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.</li> </ul>	
<p><b>Hinweis:</b> 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.</p>	
<p><b>Hinweis:</b> Beim Tunnelabbau kann bei einer extremen Netzlast für 2-3 Sekunden die Meldung "Der VPN TI   SIS Tunnel ist in einem unbekanntem Zustand" angezeigt werden. Diese Meldung kann ignoriert werden."</p>	

---

**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 Netzkabel 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 Administrationsoberfläche 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 20 Menüpunkt VPN-Client Einstellungen

---

<b>Einstellungen</b>	
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 <b>1</b> und <b>3600</b> liegen, Standard ist <b>30</b> 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 <b>1</b> und <b>100</b> liegen, Standard ist <b>3</b> .
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 <b>1</b> und <b>3600</b> liegen, Standard ist <b>600</b> .
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 <b>1</b> und <b>3600</b> liegen, Standard ist <b>20</b> 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 <b>576</b> und <b>8076</b> liegen, Standard ist <b>1418</b> .

---

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 <b>576</b> und <b>8076</b> liegen, Standard ist <b>1418</b> .
TI Sequenznummer Auswertung	Die Größe des Fensters für die Auswertung der Sequenznummern. Der Wert <b>muss</b> auf „ <b>32</b> “ für den konformen Betrieb gestellt werden. (Der Wert kann zwischen <b>1</b> und <b>32</b> liegen, Standard ist <b>32</b> .)
SIS Sequenznummer Auswertung	Die Größe des Fensters für die Auswertung der Sequenznummern. Der Wert <b>muss</b> auf „ <b>32</b> “ aktiviert für den konformen Betrieb gestellt werden. (Der Wert kann zwischen <b>1</b> und <b>32</b> liegen, Standard ist <b>32</b> .)
Hash & URL	Mit dieser Option besteht die Möglichkeit, das Hash- & URL-Verfahren zu aktivieren. Der Wert muss zwischen <b>0</b> und <b>32</b> liegen, Standard ist „ <b>Aus</b> “.

## 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 21 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 <b>DHCP-Lease erneuern</b> 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 <b>DHCP-Lease erneuern</b> 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 <b>576</b> und <b>9000</b> liegen.
---------------	---

Tabelle 22 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 <b>DHCP-Lease erneuern</b> 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 <b>InReihe</b> und <b>Online</b> aktiviert sein. Die Standardeinstellung ist <b>InReihe</b> .
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 <b>DHCP-Lease erneuern</b> 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 <b>576</b> und <b>9000</b> 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: <ul style="list-style-type: none"> <li>▪ <b>SIS</b> - Zugriff über den sicheren Internetzugang</li> <li>▪ <b>IAG</b> - Zugriff über den Internetprovider</li> <li>▪ <b>Keiner</b> - Der Konnektor soll nicht auf das Internet zugreifen</li> </ul>

Tabelle 23 Allgemeine Verbindungseinstellungen

Allgemein	
Aktuelle IAG	Aktuelle IP-Adresse des Gateways

---

**Allgemein**


---

IAG-Adresse	<p>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 Netzkonnetktor eine statische Konfiguration verwendet (kein DHCP). Sollte der DHCP-Server kein Gateway im DHCP-Lease mitsenden, wird die manuell hinterlegte IAG verwendet.</p> <ul style="list-style-type: none"> <li>▪ <b>InReihe</b></li> <li>▪ <b>Parallel</b></li> </ul> <p>Der Anbindungsmodus <b>InReihe</b> muss eingestellt werden, wenn über den WAN-Adapter des Konnetktors 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.</p> <p>Der Anbindungsmodus <b>Parallel</b> muss eingestellt werden, wenn der Konnetktor ausschließlich über die LAN-Schnittstelle in das bestehende Netzwerk eingebunden werden soll. In diesem Falle kommuniziert der Netzkonnetktor mit dem Netz des Leistungserbringers und mit der Telematikinfrastruktur über die gleiche physische Schnittstelle. Wie bereits im Kapitel 3.4.1 beschrieben ist im Anbindungsmodus <b>Parallel</b> ebenfalls ein Internetzugriff über den sicheren SIS-Zugang möglich. Die Einstellung des Anbindungsmodus <b>Parallel</b> erfolgt durch die Deaktivierung des WAN-Adapters. Wenn der WAN-Adapter wieder aktiviert wird, dann befindet sich der Konnetktor im Modus <b>InReihe</b>.</p>
Intranet-Routen-Modus	<p>Diese Option erlaubt die Konfiguration des Intranet-Routen Modus. Die folgenden Werte sind möglich:</p> <ul style="list-style-type: none"> <li>▪ <b>Redirect</b></li> <li>▪ <b>Block</b></li> </ul> <p>Der Konfigurationswert <b>Redirect</b> gibt an, dass IP-Pakete innerhalb des Netzes des Leistungserbringers durch den Netzkonnetktor geroutet werden sollen. Diese Option sollte nur dann aktiviert werden, wenn durch den Administrator Intranet-Routen definiert wurde. Der Konfigurationswert <b>Block</b> kann eingestellt werden, wenn sämtlicher IP-Verkehr zwischen Intranet-Segmenten durch den Netzkonnetktor geblockt werden sollen. In beiden Fällen müssen die IP-Pakete an den Netzkonnetktor gerichtet sein, damit diese Werte wirksam werden.</p>
Service-Timeout	<p>Zeitspanne (in Sekunden), in der eine Anfrage beantwortet werden muss, bevor ein Timeout gemeldet wird. Standard ist <b>60</b>. Bei <b>60</b> wird kein Timeout gemeldet.</p>
Übertragungsrate	<p>Hier wird die maximale Übertragungsrate für den ausgehenden Datenverkehr in KB/s angezeigt. Der Wert muss zwischen <b>100</b> und <b>2147483647</b> liegen.</p>

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 24 Routing-Einstellungen

Routing-Informationen	
Routen	<p>In dieser Übersicht werden vorhandene Routen angezeigt. Diese Tabelle dient ausschließlich der Einsichtnahme. Zu einer Route werden die folgenden Informationen angezeigt:</p> <ol style="list-style-type: none"> <li>1. <b>Destination/Subnetmask</b> - Zieladresse der Route</li> <li>2. <b>Gateway</b> - Die eingestellte Gateway-Adresse</li> <li>3. <b>Source</b> - Quelladresse der Route</li> <li>4. <b>Flags</b> - Der jeweiligen Route zugeordnete Flags. Diese Flags können die folgenden Werte annehmen. <ol style="list-style-type: none"> <li>a) <b>U</b> - Die Route ist etabliert</li> <li>b) <b>G</b> - Die Route führt zu einem Gateway. Ist dieses Flag nicht gesetzt, führt diese Route direkt zu einem Endpunkt</li> <li>c) <b>H</b> - Dieses Flag bedeutet, dass die Route zu einem Host führt</li> <li>d) <b>D</b> - Dieses Flag zeigt an, dass die Route durch eine Umleitung zustande gekommen ist</li> <li>e) <b>M</b> - Dieses Flag zeigt an, dass die Route durch eine Umleitung modifiziert wurde</li> </ol> </li> <li>5. <b>Metric</b> - Hier wird die Gewichtung der Route angezeigt. Diese ist immer auf <b>0</b>.</li> <li>6. <b>Interface</b> - Die zugeordnete physische Schnittstelle. eth1 meint dabei den für das WAN vorgesehenen Adapter, eth0 den für das LAN vorgesehenen Adapter.</li> <li>7. <b>Protocol</b> - Dieser Wert kennzeichnet das Netzwerkprotokoll</li> <li>8. <b>Type</b> - Dieser Wert kennzeichnet den Typ der Route. Der Type ist static, das bedeutet, nur die konfigurierten Routen werden erkannt.</li> </ol>

Tabelle 25 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 <b>Entfernen</b> 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 26 Firewallregeln

Firewallregeln	
Regeln	<p>In dieser Übersicht werden die benutzerdefinierten Firewallregeln verwaltet. Die in Abschnitt <b>3.5.4</b> beschriebenen Firewallregeln sind fest im Netzkonnektor hinterlegt. Sie können nicht geändert werden und werden hier nicht dargestellt.</p> <ol style="list-style-type: none"> <li>1. <b>Quell-Netz</b> - Die IP-Adresse des Ursprungsnetzes eines Pakets. Die Notation erfolgt in der Schreibweise IP-Adresse/Subnetzmaske.</li> <li>2. <b>Ziel-Netz</b> - Die IP-Adresse des Zielnetzes eines Pakets. Die Notation erfolgt in der Schreibweise IP-Adresse/Subnetzmaske.</li> <li>3. <b>Protokoll</b> - Das Protokoll, auf welches die Filterregeln angewandt werden. Es kann die Auswahl zwischen den Protokollen UDP und TCP getroffen werden.</li> <li>4. <b>Quell-Port</b> und <b>Ziel-Port</b> - sind die Ports für den die Filterregel zutrifft. Der Port muss als numerischer Wert angegeben werden. Entweder Quell-Port oder Ziel-Port muss definiert werden.</li> </ol> <p>Um eine Regel zu löschen wird der „LÖSCHEN“ Button neben dem jeweiligen Eintrag der Regeltabelle angezeigt.</p>

## 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 27 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 28 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 <b>Verwendung DHCP DNS ausschalten</b> 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 29 DNS-Server im Netz des SIS

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

Tabelle 30 DNS-Server im Bestandsnetz

<b>DNS-Server im Bestandsnetz</b>	
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 „Entfernen“ Button neben dem jeweiligen Eintrag der DNS Servertabelle angezeigt.

Tabelle 31 DNS-Server im Netz der TI

<b>DNS-Server im Netz der TI</b>	
Server	In diesem Feld werden die konfigurierten DNS-Server im Netz der TI angezeigt.

Tabelle 32 Anzeige aktiver Bestandsnetze

<b>Bestandsnetze</b>	
Aktive Bestandsnetze	In diesem Feld werden die aktiven Bestandsnetze angezeigt.

Tabelle 33 Namensdienst-Einstellungen

<b>Einstellungen</b>	
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 Praxis, Medizinisches Versorgungszentrum, Krankenhaus, Apotheke oder weiterer Akteur. Für den Domainnamen selbst dürfen nur alphanumerische Werte, Bindestriche sowie 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 <b>Eigene DNS Root Anker URL</b> angezeigt. Hier haben Sie die Möglichkeit eine URL einzutragen und mit der Schaltfläche <b>Übernehmen</b> zu bestätigen.

Tabelle 34 Domain Erreichbarkeit prüfen

Erreichbarkeit prüfen	
Hostname	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 „Ping an Host“, „Ping an CRL-Download Server“ oder „Ping an Konzentratoren“ um die Erreichbarkeit der eingegebenen Domäne oder IP-Adresse zu prüfen.
Status	Hier wird das Ergebnis des letzten durchgeführten Ping angezeigt.

## 6.7 Menüpunkt DHCP-Server

Tabelle 35 DHCP-Server-Status

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

Tabelle 36 DHCP-Server-Einstellungen

Einstellungen	
DHCP-Server	Hier kann festgelegt werden, ob der Netzkonnetktor als DHCP-Server fungiert oder nicht. Der Standardwert ist <b>Aus</b> . Wird der Wert auf <b>An</b> geändert, werden die Felder <b>Netzwerk</b> , <b>Broadcast-Adresse</b> , <b>Erste IP-Adresse des Adress-Pools</b> und <b>Letzte IP-Adresse des Adress-Pools</b> 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 Administrationsoberfläche 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 Administrationsoberfläche angezeigt.

Tabelle 37 DHCP-Clientgruppen

DHCP-Clientgruppen	
Clientgruppen	Diese tabellarische Übersicht zeigt die konfigurierten DHCP-Clientgruppen an. Klickt man auf <b>Bearbeiten</b> , öffnet sich ein neues Fenster (siehe folgende <b>Tabelle 38 DHCP-Clientgruppen-Einstellungen</b> )

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 „LÖSCHEN“ Button neben dem jeweiligen Eintrag der DHCP Servertabelle angezeigt

Tabelle 38 DHCP-Clientgruppen-Einstellungen

Einstellungen	
Name	Dieses Feld zeigt den Namen der DHCP-Clientgruppe an.
NTP-Server-Adresse senden	Wird der Wert auf <b>An</b> geändert, wird die Adresse des Konnektor-internen NTP-Servers per DHCP an die Clients gesendet.
Eigene DNS-Server verwenden	Wird der Wert auf <b>An</b> geändert, müssen Sie DNS-Server in die entsprechende Tabelle eingeben.
Eigenes Gateway verwenden	Wird der Wert auf <b>An</b> 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.
Lease-Dauer	Dieses Feld kann verwendet werden um die Lease-Dauer in Minuten angeben.

Tabelle 39 Clients

Clients	
Clients	Hier werden die Clients tabellarisch aufgelistet
MAC-Adresse	Hier kann die MAC-Adresse des hinzuzufügenden Clients angegeben werden.
Hostname	Hier kann der Hostname des hinzuzufügenden Clients angegeben werden.
Static-Lease	Hier kann die statische Lease-IP-Adresse des hinzuzufügenden Clients angegeben werden.

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

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

Tabelle 42 Bestandsnetz für DHCP-Clientgruppen

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

Tabelle 43 DHCP-Routing-Einstellungen

<b>DHCP-Routing</b>	
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

<b>Zeitzone</b>
Mit diesem Element können Sie die vom Konnektor verwendete Zeitzone umstellen. Als Standard ist die mitteleuropäische Zeit eingestellt (CET). Die Verwendung einer neu eingestellten Zeitzone wird über <b>Übernehmen</b> 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.JJ 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 auch aktiv, wenn keine Verbindung zur TI aufgebaut und somit 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 eine Verbindung zur TI aufgebaut und der NTP-Client ausgeschaltet ist.

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 weiteren Administrations-Accounts

Für die Administration können weitere Account-Daten hinzugefügt oder geändert werden. Dazu ist in der Administrationsoberfläche **Hauptmenü > Administratoren** anzuwählen. Dazu wird Ihnen der folgende Dialog angezeigt.

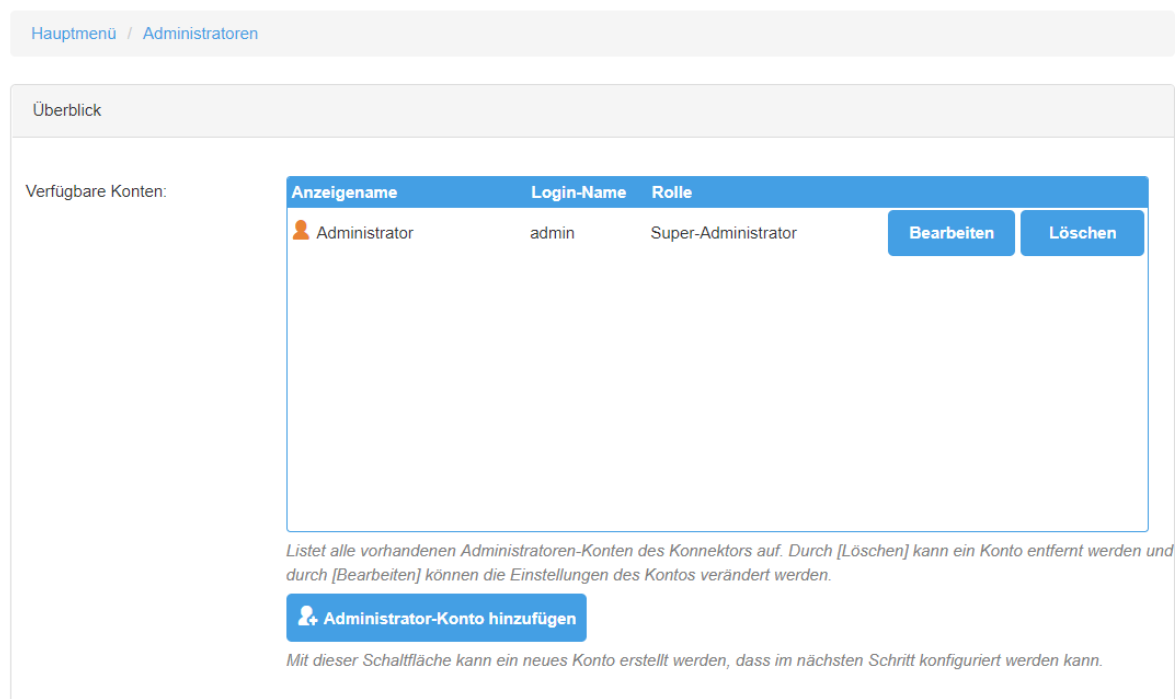


Abbildung 40 Administrationsoberfläche / Änderung der Account-Daten

Im Dialog **Administrator-Konto hinzufügen** müssen folgende Eingaben erfolgen:

1. Login-Name
2. Anzeigename
3. E-Mail
4. Raum/Adresse
5. Passwort
  - a. Das Passwort ist mehr als 16 Zeichen lang
  - b. Das Passwort enthält kleine und / oder große Buchstaben
  - c. Das Passwort enthält mindestens eine Ziffer
  - d. Das Passwort enthält mindestens ein Sonderzeichen
6. Rolle

Nachfolgend müssen noch die Einzelberechtigungen vergeben werden, welche für dieses Konto aktiviert oder deaktiviert werden können

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 Standardpasswort (5.1 Zugriff auf die Administrationsoberfläche, Tabelle 17 Standardkonfigurationsdaten) 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 (Siehe hierzu Kapitel 4.7.5.3). 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.

## 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<sup>3</sup>-Call über **VerifyPin**, **ChangePin** oder **UnblockPin** aufgerufen werden.

---

<sup>3</sup> Netzwerkprotokoll zum Austausch von Daten



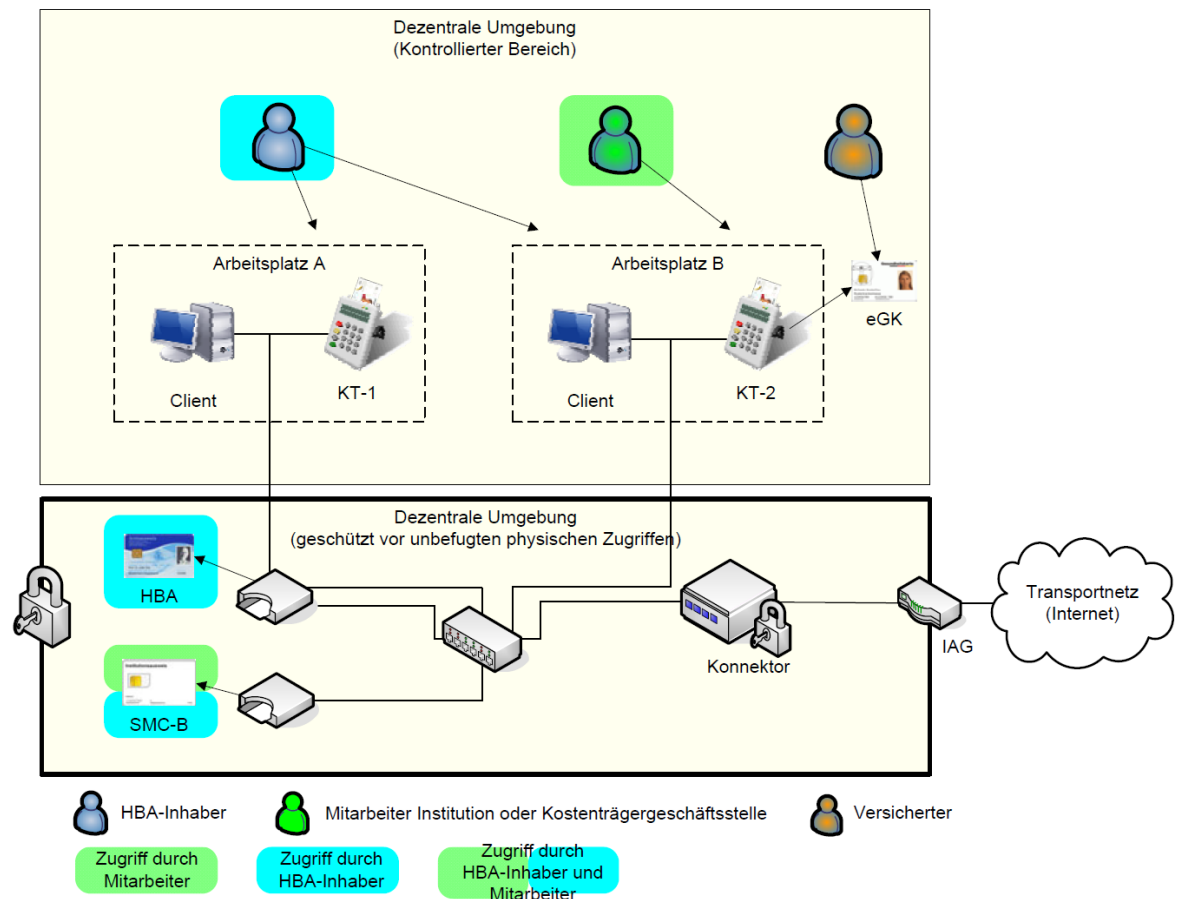


Abbildung 41 Szenario Remote-PIN-Verfahren aus gemSpec\_KON\_V4.11.1, S.504

## 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.

---

**Bearbeitung des Accounts**

Login-Name	Der Login-Name des Accounts. Nach Erstellung nicht mehr änderbar.
Anzeigename	Der angezeigte Name des Administrators
E-Mail	E-Mail-Adresse des Administrators (optional)
Raum / Adresse	Der Raum oder die Adresse des Administrators (optional)
Rolle	Die dem Account zugewiesene Rolle, nur für Superadministratoren änderbar.
Berechtigungen	Berechtigungstabelle des Administrators. Die Berechtigungen eines Superadministrators können nicht bearbeitet werden.
Passwort	Das Passwort zur Anmeldung am Anwendungskonnektor
Passwort (wiederholen)	Passwort-Wiederholung

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 <a href="#">6.2</a> .
Ändern der DHCP-Server Einstellungen	Erlaubt dem Administrator, DHCP-Einstellungen vorzunehmen
Ändern von Datum / Uhrzeit	Erlaubt dem Administrator, die vorhandenen Datums-/ Zeiteinstellungen zu konfigurieren.
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.

Rechtevergabe und mögliche Einschränkungen	
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 Zugriffsberechtigungen	Erlaubt dem Administrator, die vorhandenen Zugriffsberechtigungen-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: <ul style="list-style-type: none"> <li>▪ Neustart des Konnektors</li> <li>▪ Registrieren</li> <li>▪ Hostname ändern / anzeigen</li> <li>▪ Einstellungen importieren, exportieren, Werksreset</li> </ul>
Ändern der Protokollierungs-Einstellungen	Erlaubt dem Administrator, die vorhandenen Protokollierungs-Einstellungen zu konfigurieren.
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.
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.

---

**Einstellungen**


---

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 <b>Eigenständig</b> ) nur ein Konnektor notwendig. <b>Dieses Feature ist abgekündigt und soll nicht mehr verwendet werden.</b>
------------------	---

---

## 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 <b>An</b> .
Authentifizierung erforderlich	Diese Option gibt an, ob eine Clientsystem-Authentifizierung verpflichtend ist. Der Standardwert ist <b>An</b> .
Authentifizierungsmodus	Hier stehen zwei Möglichkeiten zur Verfügung: <b>Zertifikat</b> und <b>Nutzername</b> . Der Standardwert ist <b>Zertifikat</b> .
Offener Dienstverzeichnisdienst	Diese Option gibt an, ob der Dienstverzeichnisdienst über eine ungesicherte Verbindung erreichbar ist. Der Standardwert ist <b>An</b> .

---

### 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 angegebenen 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

Tabelle 55 Einstellung des gewählten Arbeitsplatz

Ausgewählter Arbeitsplatz	
Arbeitsplatz-ID	Gibt die zu verwendende ID eines Arbeitsplatzes an. Dieser Wert wird benötigt, damit der Konnektor bei Operationen an der Außenschnittstelle den aufrufenden Arbeitsplatz korrekt zuordnen kann.

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

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 56 Liste der konfigurierten Arbeitsplätze

Arbeitsplatz	
Arbeitsplatz hinzufügen	Unter Verwendung der Schaltfläche <b>Arbeitsplatz hinzufügen</b> werden die angegebenen Werte in die Konfiguration übernommen und in der Tabelle angezeigt. Beim Klick auf Schaltfläche <b>Bearbeiten</b> wird die Seite mit Einstellungsmöglichkeiten zum ausgewählten Arbeitsplatz angezeigt.
Arbeitsplatz-ID	Die <b>Arbeitsplatz-ID</b> unter <b>Ausgewählter Arbeitsplatz</b> spezifiziert das Identifikationsmerkmal des Arbeitsplatzes. Änderungen werden mit der Schaltfläche <b>Übernehmen</b> bestätigt.
Beschreibung	Das Feld <b>Beschreibung</b> unter <b>Ausgewählter Arbeitsplatz</b> 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 <b>Übernehmen</b> bestätigt.

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

Tabelle 57 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 <b>Zuordnung hinzufügen</b> 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: <b>lokal</b> und <b>entfernt</b> . Das lokale Kartenterminal befindet sich tatsächlich lokal am Arbeitsplatz. Das entfernte Kartenterminal ist z.B. in einem anderen Raum (siehe dazu <a href="#">7.1.4</a> )

**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 58 Liste der angelegten Mandanten

Mandant	
Mandanten-ID	Spezifiziert das Identifikationsmerkmal des Mandanten.
Beschreibung	Dieses Feld ist <b>optional</b> 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 angegebenen 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 59 Details zu ausgewähltem Mandanten

Ausgewählter Mandant	
Mandant-ID	Die <b>Mandant-ID</b> spezifiziert das Identifikationsmerkmal des Mandanten. Änderungen werden mit der Schaltfläche <b>Übernehmen</b> bestätigt.
Beschreibung	Das Feld <b>Beschreibung</b> unter <b>Ausgewählter Mandant</b> 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 <b>Übernehmen</b> bestätigt.

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

Tabelle 60 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 61 Liste der zugeordneten SMBs

<b>Zugeordnete SMBs</b>	
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 62 Liste der zugeordneten Arbeitsplätze

<b>Zugeordnete Arbeitsplätze</b>	
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 63 Liste der zugeordneten Clientsysteme

<b>Zugeordnete Clientsysteme</b>	
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 64 Liste der der Arbeitsplätze zugeordneter Clientsysteme

<b>Arbeitsplätze zugeordneter Clientsysteme</b>	
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 65 Liste der zugeordneten Kartenterminals für Remote-PIN-Zugriff

<b>Zugeordnete Kartenterminals für Remote-PIN-Zugriff</b>	
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 66 Zugeordneter VSDM-Encryptionkey

<b>Zugeordneter VSDM-Encryptionkey</b>	
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 Schlüssel überschrieben werden.
Neuer Schlüssel	Hier kann der neue Schlüssel manuell eingegeben werden und mit der Schaltfläche <b>Übernehmen</b> in die Verwaltung übernommen werden.

## 7.4.4 SMB

Tabelle 67 Liste der SMBs

<b>SMB</b>	
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).

## 7.4.5            Sichere Anzeige

Tabelle 68 Liste der sicheren Anzeigen (Trusted Viewer)

---


Sichere Anzeigen	
Sichere Anzeigen	In dieser Tabelle werden die sicheren Anzeigen aufgelistet, die in die Konnektor-Verwaltung aufgenommen wurden. Hier haben sie auch die Möglichkeit, die Zuordnung zu löschen.
Anzeige-ID	Hier wird die ID der sicheren Anzeige dargestellt.
Beschreibung	Die Beschreibung der ausgewählten sicheren Anzeige (optional).
Arbeitsplatzzuordnung	Hier kann der vorhanden Arbeitsplatz auswählen, dem die sichere Anzeige zugeordnet werden soll.

---

Nach Betätigen der Schaltfläche **Anzeige hinzufügen** kann eine neue sichere Anzeige angelegt werden.

## 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.




**Konnektor Administration** Angemeldet als [Administrator](#) [Abmelden](#) 

In das Sicherheitsprotokoll wurden neue Meldungen geschrieben. [Anzeigen](#)

[Hauptmenü](#) / [Karten-Terminals](#)

Kartenterminals

Kartenterminals:

ID	Name	IP-Adresse	Zugew.	Paired	Verb.	
 00:0d:f8:03:61:75	TF4546-04	192.168.5.2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">Bearbeiten...</a>
 00:25:0e:00:3c:d9	Terminal	192.168.5.9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Bearbeiten...</a>
 00:1a:58:00:79:a5	CARD STAR/medic2 2131141	192.168.5.16	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Bearbeiten...</a>

*Auflistung aller Kartenterminals im Netzwerk.*

*HINWEIS: Wenn Ihr Gerät nicht gefunden wird, dann überprüfen Sie hier, ob sich Ihr Gerätetyp auf der Liste der kompatiblen Kartenterminalgeräte befindet.*

[Automatisch hinzufügen](#)

[🔍 Jetzt suchen](#)

*Durchsucht das gesamte Netzwerk nach Kartenterminals.*

Abbildung 42 Administrationsoberfläche / Kartenterminals

Tabelle 69 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	<p>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.</p> <p>Mit Klick auf den Button Entfernen beenden Sie die Zuordnung zu diesem Kartenterminal. Im Abschnitt <b>Bearbeiten</b> 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.</p> <p><b>Kartenterminal-ID</b> - Diese Angabe zeigt dem Benutzer die ID des Kartenterminals an und ist nicht änderbar.</p> <p><b>Hostname</b> - Bezeichnung (auch: Friendly-Name) des SICCT-Terminals</p> <p><b>IP-Adresse</b> - IP-Adresse des Kartenterminals</p> <p><b>TCP-Port</b> - TCP-Port, über den das Kartenterminal kommuniziert (optional)</p> <p><b>Adminname</b> - Benutzername des Administrators</p> <p><b>Adminpasswort</b> - Passwort des Administrators, den Sie in Adminname angegeben haben</p>
Jetzt Suchen	<p>Mit der Schaltfläche <b>Jetzt Suchen</b> wird das gesamte Netzwerksegment nach kompatiblen Kartenterminals durchsucht.</p> <p>Konnte der Konnektor Ihr Kartenterminal nicht automatisch erkennen, können Sie das Kartenterminal manuell hinzufügen. Dazu müssen Sie die folgenden Felder vollständig ausfüllen und auf <b>Hinzufügen</b> klicken.</p>
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 70 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 <b>1</b> und <b>60</b> 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 <b>0</b> und <b>140</b> liegen.
Keep-Alive Intervall	Angabe in Sekunden, in welchem Abstand Keep-Alive-Nachrichten gesendet werden sollen. Der Wert muss zwischen <b>1</b> und <b>10</b> liegen.

---

---

**Einstellungen**

Keep-Alive Versuche	Anzahl der Fehlversuche Keep-Alive-Nachrichten erfolgreich zu versenden, bevor die Verbindung getrennt wird. Der Wert muss zwischen <b>3</b> und <b>10</b> liegen.
Handshake-Timeout	Die Dauer in Sekunden, die der Konnektor auf ein TLS-Verbindungsaufbau zum Kartenterminal wartet. Der Wert muss zwischen <b>1</b> und <b>60</b> Sekunden liegen.
Display Anzeigedauer	Dauer in Sekunden, die Meldungen auf dem Display nach Beendigung von Kommandos mit Displayausgabe angezeigt werden. Der Wert muss zwischen <b>1</b> und <b>30</b> 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 71 Liste der verfügbaren Karten

---

**Verfügbare Karten**

Karten	<p>In dieser tabellarischen Aufstellung befindet sich die Übersicht der eingelegten Karten. Die folgenden Informationen werden in der Darstellung aufgelistet:</p> <ol style="list-style-type: none"> <li><b>Terminal-ID:</b> Zeigt die Bezeichnung des Terminals an, in dem die Karte eingelegt ist. Diese Bezeichnung ist identisch mit der MAC-Adresse des Terminals.</li> <li><b>Slot:</b> Gibt den Slot (Schacht) an, in dem die Karte in dem betreffenden Kartenterminal eingelegt wurde.</li> <li><b>Typ:</b> Gibt den Typ der eingelegten Karte an. Konnte der Typ der Karte nicht ermittelt werden, so wird unbekannte Karte für die eingelegte Karte angezeigt.</li> <li><b>Besitzer / Info:</b> Gibt den Karteninhaber in Kurzform sowie zusätzliche verfügbare Informationen an, wenn vorhanden.</li> <li><b>Eingesteckt:</b> Gibt den Zeitpunkt im Format Datum / Uhrzeit (DD.MM.YYYY hh:mm:ss+Zeitzone) an, zu welchem die Chipkarte in das Kartenterminal eingelegt wurde.</li> </ol> <p>Für jede in der Tabelle angezeigte Karte wird zusätzlich die Schaltfläche Infos angezeigt. Durch Betätigen der Schaltfläche können je nach Karte die folgenden Informationen auf der Seite Informationen angezeigt werden:</p> <p>Kartenterminal, Slot, Typ, Einsteck-Zeit, Besitzer, ICCSN, Versionen und Ablaufdatum des Zertifikats.</p> <p>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.</p>
Timeout	Erlaubt die Konfiguration des Zeitwerts in Sekunden (zwischen <b>1</b> und <b>30</b> ), nach dem eine Operation mit einem Timeout-Wert abgebrochen wird. Unter Verwendung der Schaltfläche <b>Übernehmen</b> 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 72 Betriebszustände

Betriebszustände	
Kritische Fehler	Tabelle der aufgetretenen kritischen Fehler mit der Anzeige von Fehlercode, Beschreibung und dem letzten Auftreten
Warnungen	Tabelle der aufgetretenen Warnungen mit der Anzeige von Fehlercode, Beschreibung und dem letzten Auftreten

Tabelle 73 Missbrauchserkennung

Missbrauchserkennung	
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 74 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 Startzeit	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.
TSL Nächstes Update	Zeigt den Zeitpunkt des nächsten notwendigen Updates an. Die Liste ist bis zu diesem Zeitpunkt gültig.
Fingerprint des TSL-Signer-Zertifikats	Zeigt den Fingerabdruck des Signaturzertifikats 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.
CRL Nächstes Update	Zeigt den Zeitpunkt des nächsten notwendigen Updates an. Die Liste ist bis zu diesem Zeitpunkt gültig.

Über die Menüpunkte **TSL hochladen** und **CRL hochladen** können die jeweiligen Dateien in den Konnektor geladen werden.



## 7.9.1 Vertrauensanker

Der Menüpunkt **Vertrauensanker** zeigt die Gültigkeit und den Aussteller der Vertrauensanker TSL, sowie der Vertrauensanker gSMC-K.

Tabelle 75 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.
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 76 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 <sup>4</sup> 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.

<sup>4</sup> QES steht für qualifizierte elektronische Signatur.

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](http://www.gematik.de)) herunterzuladen und in den Konnektor einzuspielen. Dazu muss die Schaltfläche Hochladen im angezeigten Menü TSL hochladen verwendet werden.

## 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 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 77 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 78 Sicherheitsprotokolle

Sicherheit	
In diesem Bereich werden vorhandene Einträge der Sicherheitsprotokollierung angezeigt.	

Download	Mit dieser Schaltfläche haben Sie die Möglichkeit, die Protokolleinträge herunterzuladen.
----------	---

Tabelle 79 Performanceprotokolle

<b>Performance</b>	
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 80 VSDM-Ablaufprotokolle

<b>VSDM Ablauf</b>	
In diesem Bereich werden vorhandene Einträge der VSDM-Ablaufprotokollierung 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 81 VSDM-Fehlerprotokolle

<b>VSDM Fehler</b>	
In diesem Bereich werden vorhandene Einträge der VSDM-Fehlerprotokollierung 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 82 VSDM-Performanceprotokolle

<b>VSDM Performance</b>	
In diesem Bereich werden vorhandene Einträge der VSDM-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 83 Einstellungen zur VSDM-Performanceprotokollierung

<b>Einstellungen</b>	
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:

---

**Einstellungen**


---

	<ol style="list-style-type: none"> <li>1. <b>Info</b> - Dieses Meldungslevel hat die höchste Granularität. Es werden sehr detaillierte Informationen über Systemzustände generiert. Verwenden Sie diese Einstellung ausschließlich zur Analyse in besonderen Fehlersituationen.</li> <li>2. <b>Warning</b> - Beginnend ab dem Meldungslevel Warnung werden alle Systemeinträge</li> <li>3. <b>Error</b> - Beginnend ab dem Meldungslevel Fehler werden alle Systemeinträge protokolliert. Meldungen mit Level Warnung werden in diesem Falle nicht protokolliert.</li> <li>4. <b>Fatal</b> - Es werden ausschließlich schwerwiegende Fehler protokolliert. Alle anderen Typen werden nicht erfasst.</li> </ol>
Mindestspeicherdauer des Sicherheitsprotokolls	Dieses Feld zeigt die eingestellte Aufbewahrungsdauer der Protokolleinträge des Sicherheitsprotokolls an. Der Wert kann für einen Zeitraum zwischen <b>10</b> und <b>365</b> 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 <b>10</b> und <b>365</b> 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 Administrationsoberfläche 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 Komplett Einrichtung des Konnektors sollte ein erstes Backup erfolgen. Nur so können im Falle einer späteren Zurücksetzung auf Werkseinstellungen (z.B. bei vergesse- nem Passwort) die Bestandsdaten rückgesichert werden.

**Ab Version 1.5.3 können keine Backups aus früheren Versionen importiert werden. Wir empfehlen deshalb nach der Installation ab der Version 1.5.3 ein neues Backup zu erzeugen.**

Tabelle 84 Backupsicherung erstellen

Einstellungen sichern	
SMB	Hier wird eine Auswahlliste mit ICCSN, Mandant, Arbeitsplatz und Kartenterminal der SMB-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 85 Backupsicherung laden

Einstellungen wiederherstellen	
Importieren	Über diese Schaltfläche können vorher exportierte Einstellungs-Dateien des Konnek- tors hochgeladen werden.
Zurücksetzen auf Werkszustand	Die gesamten Einstellungen des Konnektors werden mit dieser Schaltfläche auf Werks- einstellung 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 be- finden 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 86 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 jewei- lige Gerät zu hinterlegen.
Gruppen-Ansicht	Über diese Schaltfläche werden die Einträge in der Tabelle <b>Plan alle Geräte</b> 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.

**Grundsätzlich empfiehlt der Hersteller, Updates einzuspielen, es sei denn, es sprechen explizit bekannte Probleme dagegen.**

Tabelle 87 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 <b>Aus</b> .
Automatische Überprüfung	Mit Hilfe des Schalters kann die tägliche automatische Suche nach Firmware-Aktualisierungen im Internet aktiviert werden. Der Standardwert ist <b>AN</b> .
Automatisches Herunterladen	Ist dieser Schalter aktiviert, werden automatisch neue Firmware Aktualisierungen des Konnektors und der Kartenterminals heruntergeladen. Der Standardwert ist <b>Aus</b> .
URL für die Update-Anfrage	Hier wird der SOAP-Endpunkt des KSR-Dienstes <sup>5</sup> 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 Logout von der Administrationsoberfläche

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



Abbildung 43 Administrationsoberfläche / Button „abmelden“

## 7.14 Werksreset durchführen

Der Werksreset setzt den Konnektor in den Auslieferungszustand zurück.

<sup>5</sup> Konfigurationsdienst



Abbildung 44 Multifunktionstaste (Software Taste)

Für den Werksreset müssen folgende Schritte ausgeführt werden:

#### Schritt 1 Anfordern des Werksresets:

- Durch zweimaliges schnelles Drücken der Multifunktionstaste gelangen Sie in den Bestätigungsmodus für den Werksreset.
- Der Konnektor signalisiert den erfolgreichen Doppelklick mit einem orangenen Lauflicht durch die LEDs von links nach rechts.
- Auf der 7-Segmentanzeige startet ein Countdown der von „9“ auf „0“ herunter zählt.

#### Schritt 2 Bestätigung des Werksresets:

- Um den Werksreset zu bestätigen drücken Sie bitte die Multifunktionstaste für mindestens 3 Sekunden.
- Bei erfolgreicher Bestätigung wechselt das Lauflicht auf grün und wird zu einem grünen Lauflicht.

#### Schritt 3 Ausführung des Werksresets:

- Nach Loslassen der Multifunktionstaste erlischt das Lauflicht und der Konnektor wird auf den Werkszustand zurückgesetzt.

#### Schritte 4 Erneute Anmeldung:

- Sobald der Werksreset vollständig durchlaufen wurde, können Sie sich mit der Standard Anmeldung (Name „admin“ und Passwort „konnektor“) am Konnektor anmelden.

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

Auf der Administrationsschnittstelle bleibt weiterhin der Link „Passwort vergessen?“ auf der Anmeldeseite erhalten. Wenn man darauf klickt, dann wird eine Webseite angezeigt, die das zuvor beschriebene Prozedere illustriert.

#### Zusätzliche Hinweise:

Wird während des zuvor beschriebenen Countdowns die Taste nicht gedrückt oder kürzer als 3 Sekunden, so wird an dem Konnektor nichts verändert.

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

## 7.14.1 Admin Passwort vergessen / Werksreset wird ausgelöst

Hinweis: Sollte das Administrator Kennwort nicht mehr vorliegen, so kann über den Menüpunkt „Kennwort vergessen“ ein Werksreset ausgelöst werden (siehe Kapitel zuvor 7.14).

## 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 <b>10</b> . Der Minimalwert beträgt <b>1</b> , während der Maximalwert <b>3000</b> Sekunden (50 Minuten) beträgt.
Maximale Bearbeitungszeit	Gibt den maximalen Zeitwert in Sekunden zur Ausführung der Operation <b>ReadVSD</b> an. Mit dieser Operation werden die Versichertenstammdaten aus einer elektronischen Gesundheitskarte ausgelesen. Der Minimalwert beträgt <b>1</b> , während der Maximalwert <b>3000</b> Sekunden (50 Minuten) beträgt. Standard ist <b>30</b> .
TI Offline Timeout	Gibt die maximal akzeptierte Zeit in Sekunden für eine fehlende Verbindung zur Telematikinfrastruktur an. Der Minimalwert beträgt <b>0</b> , während der Maximalwert <b>3000</b> 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 <b>10</b> und <b>365</b> ) 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

---

<b>Mandanten-Schlüssel-Zuordnung</b>	
Mandanten-Schlüssel	<ul style="list-style-type: none"><li>▪ In dieser Tabelle wird die Zuordnung zwischen einem Mandanten und einer SMB angegeben. Dies wird für den Anwendungsfall <b>AutoUpdateVSD</b> und <b>ReadVSD</b> benötigt.</li><li>▪ Der Schlüssel für den Prüfungsnachweis muss 16 Ziffern lang sein. Er kann manuell eingegeben oder generiert werden.</li><li>▪ Zum automatischen Generieren eines Schlüssels klicken Sie zunächst auf die Schaltfläche <b>Generieren</b>, der generierte Schlüssel wird Ihnen dann direkt angezeigt.</li><li>▪ Falls Sie den Schlüssel manuell festlegen möchten, geben Sie eine 16-stellige Ziffernkombination ein.</li><li>▪ Schließen Sie die Eingabe ab, indem Sie auf <b>Übernehmen</b> klicken.</li></ul>

---

Tabelle 92 Einstellung der automatischen Stammdatenaktualisierung

---

<b>Automatische Stammdatenaktualisierung – Konfiguration</b>
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:   
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:  Sekunden  
Timeout für VSDM Dienste. Standard: 10 Sekunden.

Maximale Bearbeitungszeit:  Sekunden  
Max. Bearbeitungszeit für die Operation ReadVSD. Standard: 30 Sekunden.

TI Offline Timeout:  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:   
Gibt die Mindestschwere zu protokollierender Einträge im VSDM Fachmodulprotokoll an. Standard-Wert: Warning.

Mindestspeicherdauer des Ablaufprotokolls:  Tage  
Gibt die Anzahl der gespeicherten Tage für das VSDM Fachmodulprotokoll an, bevor das Protokoll gelöscht wird.

---

**Performance-Protokoll**

Abbildung 45 Administrationsoberfläche / Dienst

**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
<input type="text"/>	<input type="text"/>		

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
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	

Gibt die Kontext-Zuordnung an, welche für die automatische Stammdatenaktualisierung benötigt wird.

Abbildung 46 Administrationsoberfläche / Performance Protokoll

## 9 Versionierung des Konnektors

In diesem Kapitel wird die Versionierungsstrategie des Produktes „Konnektor“ beschrieben. Die T-Systems 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 Produktmanagements eindeutig auf die Bestandteile der Komponenten aus der Entwicklung referenziert. Siehe dazu die beigefügte Tabelle im Dokument.

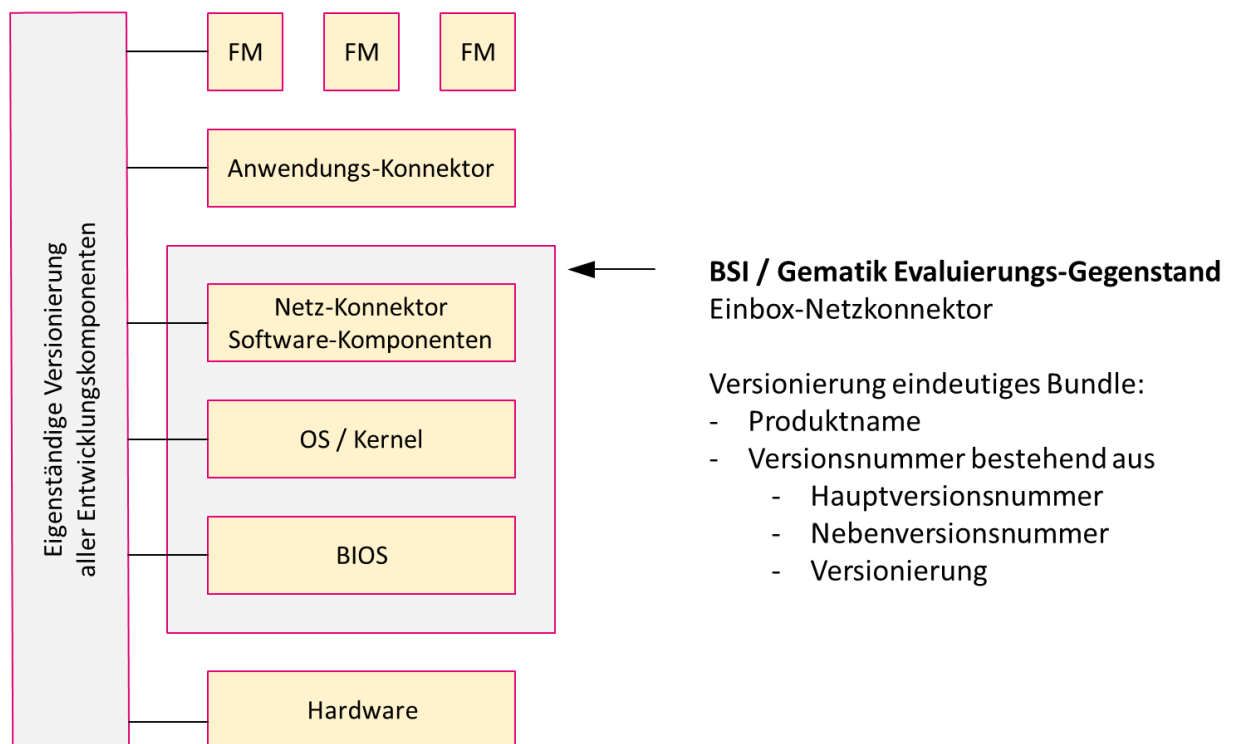


Abbildung 47 Versionierung des Konnektors

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 Inbox-Konnektors die Komponenten

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

**Folgendes Beispiel verdeutlicht das oben beschriebene Konzept:**

Produkt	Version
Medical Access Port_1BK	1.5
Unterkomponenten	Version
Firmware	1.5.3
Kernel	3.16.57
Bios	S1.40.1.1

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:

Tabelle 93 Versionierung des Konnektors

Aufbau	Beschreibung
Produktname	Wurde von T-Systems festgelegt: Medical Access 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.

Für die Beschreibung des Aufbau der Produktversion für die Auflistung der Zulassungen für den Online-Produktivbetrieb der gematik siehe Kapitel 3.6 Hinweise zur Zulassung / Sicherheitszertifizierung.

# 10 Fehlermeldungen

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

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 Administrationsoberfläche angezeigt werden.

## 10.1 Fehlermeldungen des T-Systems Konnektor

### 10.1.1 Fehlermeldungen auf der Administrationsoberfläche

Tabelle 94 Fehlermeldungen auf der Administrationsoberfläche

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) <ul style="list-style-type: none"> <li>▪ Das Netz 0.0.0.0/0 ist nicht gültig; Wenn diese Adresse angegeben wurde.</li> <li>▪ 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</li> </ul>	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).
Falsche MAC-Adresse	Bitte geben Sie eine korrekte MAC-Adresse an. Beispiel: 1a:12:13:2d:23:df.

Fehlermeldung & Ursache	Abhilfe
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 gleich als MINIMUM-WERT sein.
Eingabe eines zu großen numerischen Werts	Dieser Wert ist zu groß. Der Wert muss kleiner gleich 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 95 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 beigelegt.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
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 beigelegt.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
19809	Schwerwiegender Fehler: IP-Adressen konnten nicht gelöscht werden Interner Fehler. Ursache wird der Ausgabe beigelegt.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.

Code	Fehlermeldung & Ursache	Abhilfe
19810	Beim Setzen der Broadcast-Adresse ist ein Fehler aufgetreten Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
19811	Status des VPN-Tunnels zur TI konnte nicht ermittelt werden Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
19812	Status des VPN-Tunnels zum SIS konnte nicht ermittelt werden Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
19813	Die IP-Adresse konnte nicht validiert werden Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
19814	Subnetmaske konnte nicht ermittelt werden Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
19815	IP-Adresse konnte nicht ermittelt werden Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
19816	Das Netzwerk-Interface ist nicht definiert Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
19817	Das CA Zertifikat des NK.ID nicht gefunden Interner Fehler, gSMC-K ist defekt.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
19818	Invalid NK.ID Zertifikat Interner Fehler, gSMC-K ist defekt.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
19819	Fehlerhafte Umgebungseinstellungen Interner Fehler, bei der Interpretation der Netzsegmente ist ein Fehler aufgetreten.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
4000	Syntaxfehler Fehler bei der Kommunikation mit dem Clientsystem	Kontaktieren Sie Ihren Vertragspartner.
4001	Interner Fehler Die Fehlerursache geht durch den Kontext bzw. den mitgelieferten Trace hervor	Kontaktieren Sie Ihren Vertragspartner.
4002	Der Konnektor befindet sich in einem kritischen Betriebszustand Durch den Betriebszustand können bestimmte Funktionen nicht ausgeführt werden.	Siehe <a href="#">4.9.1</a>



## 10.1.3 Fehlermeldungen Firewall

Tabelle 96 Fehlermeldungen Firewall

Code	Fehlermeldung & Ursache	Abhilfe
19083	Die Firewallregel 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.	Kontaktieren Sie Ihren Vertragspartner.
19085	Die Option der Firewallregeln ist nicht bekannt. Interner Fehler: Kann nur beim Ansteuern des Konnektors über Thrift-Schnittstelle vorkommen.	Kontaktieren Sie Ihren Vertragspartner.
19086	Anpassung der Firewall fehlgeschlagen. Interner Fehler: Beim Aktivieren von Firewallregeln ist ein unerwarteter Fehler aufgetreten.	Kontaktieren Sie Ihren Vertragspartner.

## 10.1.4 Fehlermeldungen im Menü Administration und Registrierung

Tabelle 97 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 Nutzernamen und Passwort nicht erkannt. Entweder nicht vorhanden oder Tippfehler.	Erneute Anmeldung mit einer gültigen Kombination aus Nutzernamen 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 sollte ein anderer Nutzernamen für den neuen Admin verwendet werden.

Code	Fehlermeldung & Ursache	Abhilfe
	Es wird versucht, einen Administrator hinzuzufügen, wobei der Nutzernamen für den Admin bereits verwendet wird.	
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 Administration 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.	Angabe 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.
16016	Das Passwort darf nicht den Login-Namen enthalten (weder vorwärts noch rückwärts gelesen) Im Passwort wurde der Nutzernamen / 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.	Korrigieren Sie Ihre Eingabe oder wenden Sie sich an Ihren Superadministrator

Code	Fehlermeldung & Ursache	Abhilfe
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 98 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 Vertrauensraum	Gültige CRL importieren. Überprüfung der Gültigkeit der TSL
4132	Extraktion des Ablaufdatums fehlgeschlagen Bei der Ermittlung des Ablaufdatums des Zertifikats ist ein Fehler aufgetreten.	Kontaktieren Sie Ihren Vertragspartner.
4196	Fehler bei der CV-Zertifikatsprüfung	Kontaktieren Sie Ihren Vertragspartner.

## 10.1.6 Fehlermeldungen im Menü VPN-Client

Tabelle 99 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.	Kontaktieren Sie Ihren Vertragspartner.
19004	TI: Die Liste der Konzentratoren konnte nicht geladen werden.	Tunnelaufbau erneut versuchen

Code	Fehlermeldung & Ursache	Abhilfe
	Es liegt ein Konfigurationsproblem vor. Der Konnektor konnte die Antwort des DNS-Servers nicht richtig auswerten.	
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.	Kontaktieren Sie Ihren Vertragspartner.
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.	Kontaktieren Sie Ihren Vertragspartner.
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
19019	VPN-Verbindung zur TI konnte nicht hergestellt werden. <ul style="list-style-type: none"> <li>▪ Die Verbindung zur Telematikplattform konnte nicht hergestellt werden. Mögliche Ursachen sind:</li> <li>▪ Die Zeiteinstellungen des Konnektors sind nicht korrekt,</li> <li>▪ es besteht keine Netzwerkverbindung,</li> <li>▪ es sind Fehler bei den verwendeten Zertifikaten aufgetreten.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prüfung der Systemzeit, der Verbindung des Konnektors zum Netzwerk und Prüfung der System- und Sicherheitsprotokollierung.</li> <li>▪ Prüfung, ob Protokolle weitere Hinweise auf die Ursache liefern, ggf. Tunnelaufbau erneut versuchen.</li> </ul>
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	Tunnelaufbau erneut versuchen.

Code	Fehlermeldung & Ursache	Abhilfe
	Interner Fehler im Management der Firewall	
19023	<p>TI: Fehler beim GetAndAllowNextHashAndURLServer, keine Hash and URL Servers mehr</p> <ul style="list-style-type: none"> <li>▪ Wenn der Konnektor so konfiguriert ist, dass das Verfahren Hash &amp;URL verwendet werden soll, muss ein sog. Hash- &amp;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.</li> </ul>	Tunnelaufbau erneut versuchen. Gegebenenfalls Nutzung des Verfahrens Hash &URL abschalten.
19051	<p>SIS: Error fetching list of konzentrator</p> <p>Es liegt ein Konfigurationsproblem vor. Der Konnektor konnte die Antwort des DNS-Servers nicht richtig auswerten.</p>	Tunnelaufbau erneut versuchen
19052	<p>SIS: Fehler bei GetNamesrvAndDomainnameOfVPNServiceZone.</p> <p>Beim SIS-Tunnelaufbau ist ein Fehler von der Gegenseite festgestellt worden.</p>	Kontakt zu Betreiber der TI
19053	<p>SIS: Error FQDN2IP</p> <p>Ein Namenseintrag (DNS) konnte nicht in eine IP-Adresse aufgelöst werden.</p>	Tunnelaufbau erneut versuchen.
19054	<p>SIS: Error generating ipsec.conf</p> <p>Es konnte keine gültige Konfiguration für den VPN-Client erzeugt werden.</p>	Kontaktieren Sie Ihren Vertragspartner.
19055	<p>SIS: Error VpnUP</p> <p>Interner Fehler</p>	Kontaktieren Sie Ihren Vertragspartner.
19056	<p>SIS: MGM_LU_ONLINE is not enabled</p> <p>Konnektor befindet sich nicht im Online-Modus.</p>	Konnektor in den Online-Modus versetzen (Konfiguration ändern).
19057	<p>SIS: MGM_LOGICAL_SEPARATION is NOT disabled, stopping</p> <p>Der Konnektor wurde zur Verwendung des Betriebsmodus logische Separation konfiguriert. Mit dieser Einstellung ist eine Verbindung zum sicheren Internetservice (SIS) nicht erlaubt.</p>	<p>Umkonfiguration des Konnektors oder Nutzung einer anderen Internetverbindung.</p> <p><b>Dieses Feature ist abgekündigt und soll nicht mehr verwendet werden.</b></p>
19058	<p>SIS: ANLW_INTERNET_MODUS is NOT SIS, stopping</p> <p>Der Konnektor ist nicht so konfiguriert, dass eine Verbindung zum sicheren Internetservice zulässig ist.</p>	Umkonfiguration des Konnektors oder Nutzung einer anderen Internetverbindung.
19064	<p>Error stopping connection to SIS</p> <p>Der IPsec-Tunnel zur Telematikplattform konnte nicht richtig abgebaut werden.</p>	Abbau erneut versuchen.
19066	Error fetching SIS connection state	Neustart des Systems

Code	Fehlermeldung & Ursache	Abhilfe
	Der Konnektor konnte den Verbindungsstatus zur Telematikplattform nicht ermitteln. Es ist nicht klar, ob der Konnektor einen aktiven Tunnel unterhält oder nicht.	
19072	<p>SIS: Fehler beim GetAndAllowNextHashAndURLServer, keine Hash and URL servers mehr</p> <ul style="list-style-type: none"> <li>▪ Wenn der Konnektor so konfiguriert ist, dass das Verfahren Hash &amp;URL verwendet werden soll, muss ein sog. Hash- &amp;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.</li> </ul>	Tunnelaufbau erneut versuchen. Ggf. Nutzung des Verfahrens Hash &URL abschalten.
19030	<p>Error ipsec start</p> <p>Der VPN-Client konnte nicht gestartet werden.</p>	Prüfung der VPN-Einstellungen, ggf. Neustart des Systems.
19031	<p>Strongswan konnte nicht gestartet werden.</p> <p>Der VPN-Client konnte nicht gestartet werden.</p>	Prüfung der VPN-Einstellungen, ggf. Neustart des Systems.
19032	<p>Temporäre Datei ipsec.tmp konnte nicht gefunden und / oder gelöscht werden.</p> <p>Eine notwendige Konfigurationsdatei des VPN-Clients wurde nicht gefunden. Der VPN-Client kann nicht gestartet werden.</p>	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	<p>Beim Ermitteln von VPN-Einstellungen ist ein Fehler aufgetreten.</p> <p>Es ist ein interner Fehler bei der Ermittlung der VPN-Einstellungen aufgetreten.</p>	Prüfung der VPN-Einstellungen auf Vollständigkeit.
19034	<p>Die Initialisierung des VPN-Clients war nicht erfolgreich.</p> <p>Die Initialisierung des VPN-Clients ist fehlgeschlagen.</p>	Prüfung der VPN-Einstellungen auf Vollständigkeit. Ggf. Neustart des Systems.
19035	<p>Beim automatischen Ermitteln der URL (Hash-URL-Verfahren) schlug das Setzen der Konfigurationsparameter fehl.</p> <p>Der Aufbau eines VPN-Tunnels unter Verwendung des Verfahrens Hash &amp;URL ist fehlgeschlagen.</p>	Deaktivierung des Verfahrens Hash &URL in der Konfiguration des VPN-Clients und ggf. erneuter Versuch des Tunnelaufbaus.
19036	<p>Das Zertifikat des Konzentrators ist im unerkannten Format</p> <p>Das vom VPN-Konzentrator erhaltene Zertifikat wurde vom Konnektor abgelehnt.</p>	Kontakt zum PKI-Betreiber
19037	<p>Das Zertifikat des TI-Konzentrators hat einen falschen FQDN</p> <p>Das vom VPN-Konzentrator erhaltene Zertifikat wurde vom Konnektor abgelehnt.</p>	Kontakt zum PKI-Betreiber
19038	Das Zertifikat des TI-Konzentrators ist ungültig	Kontakt zum PKI-Betreiber

Code	Fehlermeldung & Ursache	Abhilfe
	Das vom VPN-Konzentrator erhaltene Zertifikat wurde vom Konnektor abgelehnt.	
19039	Konzentrator meldet: authentication failed Das Zertifikat des Konnektors wurde vom VPN-Konzentrator abgelehnt.	Kontaktieren Sie Ihren Vertragspartner.
4172	Es ist keine Online-Verbindung zulässig. Die Konfiguration des Konnektors erlaubt derzeit keine Online-Verbindung.	<ul style="list-style-type: none"> <li>▪ Konnektor für den Online-Betrieb konfigurieren; siehe Kapitel 4.9</li> <li>▪ Durchführen der Registrierung des Konnektors.</li> </ul>
4173	Die CRL ist nicht mehr gültig (outdated).	Gültige CRL importieren
4174	TI-VPN-Tunnel: Verbindung konnte nicht aufgebaut werden <ul style="list-style-type: none"> <li>▪ keine gültige TSL</li> <li>▪ keine Internetverbindung</li> <li>▪ Konnektor ist nicht registriert</li> <li>▪ Adresse des DNS-Resolvers nicht korrekt konfiguriert</li> </ul>	<ul style="list-style-type: none"> <li>▪ Überprüfen der Gültigkeit der TSL und ggf. eine gültige TSL importieren.</li> <li>▪ Überprüfen der Netzwerkverbindung des Konnektors. Überprüfen der Netzwerkkonfiguration des Konnektors und ggf. korrigieren.</li> <li>▪ Durchführen der Registrierung des Konnektors.</li> <li>▪ Korrektur der Adresse des DNS-Resolvers.</li> </ul>
4176	SIS-VPN-Tunnel: Verbindung konnte nicht aufgebaut werden <ul style="list-style-type: none"> <li>▪ keine gültige TSL</li> <li>▪ keine Internetverbindung</li> <li>▪ Konnektor ist nicht registriert oder nicht für den Sicheren Internet Service berechtigt</li> <li>▪ Adresse des DNS-Resolvers nicht korrekt konfiguriert</li> </ul>	<ul style="list-style-type: none"> <li>▪ Überprüfen der Gültigkeit der TSL und ggf. eine gültige TSL importieren.</li> <li>▪ Überprüfen der Netzwerkverbindung des Konnektors. Überprüfen der Netzwerkkonfiguration des Konnektors und ggf. korrigieren.</li> <li>▪ Durchführen der Registrierung des Konnektors.</li> <li>▪ Korrektur der Adresse des DNS-Resolvers.</li> </ul>

## 10.1.7 Fehlermeldungen im Menü LAN und WAN

Tabelle 100 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.

Code	Fehlermeldung & Ursache	Abhilfe
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 / Kontaktieren Sie Ihren Vertragspartner.
19306	Intranet-Route konnte weder angelegt noch geändert werden Interner Fehler. Ursache wird der Ausgabe beigefügt.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
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 <b>LAN / WAN</b> kontrollieren und ggf. korrigieren.
19314	Ändern des LAN-Netzes fehlgeschlagen. Interner Fehler. Ursache wird der Ausgabe beigefügt.	Kontaktieren Sie Ihren Vertragspartner.
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 <b>LAN / WAN</b>
19316	Die Routing-Adressen sind ungültig. Mehrere Ursachen möglich, z.B. fehlerhafte LAN- / WAN-Konfiguration	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
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 / Kontaktieren Sie Ihren Vertragspartner.
4162	Es liegt eine fehlerhafte LAN-IP-Konfiguration vor.	1. Korrektur der LAN-IP-Konfiguration; siehe Kapitel <b>6.2</b> .
4163	Es liegt eine fehlerhafte WAN-IP-Konfiguration vor.	Korrektur der WAN-IP-Konfiguration; siehe Kapitel <b>6.2</b> .
4164	Beim Aktualisieren oder Aktivieren der Firewallregeln ist es zu einem Fehler gekommen.	Kontaktieren Sie Ihren Vertragspartner.
4167	CreateRoutes: Ein oder mehrere Adressen sind ungültig Beim Einrichten der Netzwerkrouuten wurde eine ungültige oder eine fehlende IP-Adressen-Konfiguration festgestellt.	Korrektur der Netzwerkkonfiguration



## 10.1.8 Fehlermeldungen im Menü Namensdienst

Tabelle 101 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 / Kontaktieren Sie Ihren Vertragspartner.
19705	Die Konfigurationsdatei des DNS-Servers kann nicht geschrieben werden. Zugriffsfehler beim Versuch, die Konfigurationsdatei zum Schreiben zu öffnen.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
19707	Der Neustart des DNS-Servers schlug fehl. Starten des DNS-Servers nach der Neukonfiguration schlug fehl.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
19708	Das Laden der DNS-Einstellungen ist fehlgeschlagen Beim Einlesen der DNS-Konfigurationsparameter ist ein unerwarteter Fehler aufgetreten.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
19709	Der konfigurierte Trust Anchor konnte nicht heruntergeladen werden. Interner Fehler; Eventuell ist die Netzwerkverbindung gestört.	Überprüfen Sie die Netzwerkkonfiguration. Kontaktieren Sie Ihren Vertragspartner.
19710	Der DNSKEY-Eintrag konnte nicht über die konfigurierten DNS-Server beschafft werden. Interner Fehler.	Überprüfen Sie die Netzwerkkonfiguration des DNS-Servers bzw. kontaktieren Sie Ihren Vertragspartner.
19711	Bei der Verifikation der DNSKEY-Einträge gegen den Trust Anchor ist ein Fehler aufgetreten. Interner Fehler	Kontaktieren Sie Ihren Vertragspartner.
19712	Der Vertrauensraum für DNS im öffentlichen Netz ist nicht korrekt initialisiert. Interner Fehler	Kontaktieren Sie Ihren Vertragspartner.
4179	DNS: Anfrage wurde abgebrochen, da der Timeout von ANLW_SERVICE_TIMEOUT Sekunden überschritten wurde.	<ul style="list-style-type: none"> <li>▪ Überprüfung Sie folgende Punkte:</li> <li>▪ Netzwerkkonfiguration</li> <li>▪ konfigurierte URLs</li> <li>▪ Netzwerkverbindung</li> </ul>
4180	DNS: Es ist ein Fehler bei der Namensauflösung aufgetreten	<ul style="list-style-type: none"> <li>▪ Überprüfung Sie folgende Punkte:</li> <li>▪ Netzwerkkonfiguration</li> <li>▪ konfigurierte URLs</li> <li>▪ Netzwerkverbindung</li> </ul>

## 10.1.9 Fehlermeldungen im Menü Protokollierung

Tabelle 102 Fehlermeldungen im Menü Protokollierung

Code	Fehlermeldung & Ursache	Abhilfe
4150	Fehler beim Schreiben des Systemprotokolls	Kontaktieren Sie Ihren Vertragspartner.
4151	Fehler beim Schreiben eines Fachmodulprotokolls	Kontaktieren Sie Ihren Vertragspartner.
4152	Fehler beim Schreiben des Sicherheitsprotokolls	Kontaktieren Sie Ihren Vertragspartner.
4216	Fehler beim Schreiben des Konnektor Performanceprotokolls	Kontaktieren Sie Ihren Vertragspartner.
4217	Fehler beim Schreiben eines Fachmodul Performanceprotokolls	Kontaktieren Sie Ihren Vertragspartner.
4153	Zugriff auf Sicherheitsprotokoll nicht möglich	Kontaktieren Sie Ihren Vertragspartner.
4154	Zugriff auf Systemprotokoll nicht möglich	Kontaktieren Sie Ihren Vertragspartner.
4155	Zugriff auf Fachmodulprotokolle nicht möglich	Kontaktieren Sie Ihren Vertragspartner.
4218	Zugriff auf Konnektor-Performanceprotokoll nicht möglich	Kontaktieren Sie Ihren Vertragspartner.
4219	Zugriff auf Fachmodul-Performanceprotokoll nicht möglich	Kontaktieren Sie Ihren Vertragspartner.

## 10.1.10 Fehlermeldungen im Menü DHCP-Client

Tabelle 103 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.	Passen Sie den Adressbereich der neuen Clientgruppe so an, dass dieser mit den anderen Clientgruppen in keinem Konflikt steht.

Code	Fehlermeldung & Ursache	Abhilfe
	Der eingegebene Adressbereich der neuen Clientgruppe überschneidet sich mit dem Adressbereich einer bereits angelegten Clientgruppe.	
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 / Kontaktieren Sie Ihren Vertragspartner.
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 104 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.	Kontaktieren Sie Ihren Vertragspartner.

## 10.1.12 Fehlermeldungen im Menü Datum und Uhrzeit

Tabelle 105 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. kontaktieren Sie Ihren Vertragspartner.
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 Uhrzeit 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 Administrationsoberfläche 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
19418	Die Zeitzoneangabe ist nicht gültig	Angabe einer korrekten Zeitzone

Code	Fehlermeldung & Ursache	Abhilfe
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 / Kontaktieren Sie Ihren Vertragspartner.
19422	Konfiguration des NTP-Dienstes ist fehlerhaft oder nicht vollständig Die Konfiguration des Zeitdienstes auf dem Konnektor ist fehlerhaft.	Neustart des Systems / Kontaktieren Sie Ihren Vertragspartner.
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.	Kontaktieren Sie Ihren Vertragspartner.

### 10.1.13 Fehlermeldungen im Menü Update

Tabelle 106 Fehlermeldungen im Menü Update

Code	Fehlermeldung & Ursache	Abhilfe
4181	Integritätsprüfung UpdateInformation fehlgeschlagen.	Kontaktieren Sie Ihren Vertragspartner.
4182	Download nicht aller UpdateFiles möglich.	Kontaktieren Sie Ihren Vertragspartner.
4183	Integritätsprüfung UpdateFiles fehlgeschlagen.	Kontaktieren Sie Ihren Vertragspartner.
4184	Anwendung der UpdateFiles fehlgeschlagen.	Kontaktieren Sie Ihren Vertragspartner.
4185	Firmware-Version liegt außerhalb der gültigen Firmwaregruppe <ul style="list-style-type: none"> <li>▪ Versuch eines Firmwareupdates mit einer Firmwareversion aus einer veralteten Firmwaregruppe</li> </ul>	Upgrade mit aktuellem Firmwarepaket
4186	Download nicht aller UpdateFiles möglich. <ul style="list-style-type: none"> <li>▪ Netzwerkverbindung in die TI unterbrochen</li> </ul>	Herstellung der Netzwerkverbindung und erneutes Anstoßen der Kartenterminalaktualisierung

4187	KT-Update fehlgeschlagen <ul style="list-style-type: none"> <li>▪ Netzwerkverbindung zum Kartenterminal unterbrochen</li> <li>▪ Kartenterminalfehler</li> </ul>	<ul style="list-style-type: none"> <li>▪ Herstellung der Netzwerkverbindung zum Kartenterminal und erneutes Anstoßen der Kartenterminalaktualisierung</li> <li>▪ Kontakt zu Hersteller des Kartenterminals</li> </ul>
4188	Konfigurationsdienst nicht erreichbar, konfigurierte Adresse kontrollieren.	<ul style="list-style-type: none"> <li>▪ Korrektur der URL des Konfigurationsdienstes in der TI</li> <li>▪ Überprüfung der Netzwerkverbindung</li> </ul>
4189	Konfigurationsdienst liefert falsches Zertifikat Interner Fehler	Kontaktieren Sie Ihren Vertragspartner.
4190	Fehler beim Beziehen der Updatelisten Interner Fehler	Kontaktieren Sie Ihren Vertragspartner.
4198	Beim Übernehmen der Bestandsnetze ist ein Fehler aufgetreten Interner Fehler	Kontaktieren Sie Ihren Vertragspartner.

## 10.1.14 Fehlercodes kritischer Fehler (Hardwaredisplay)

Tabelle 107 Fehlercodes kritischer Fehler (Hardwaredisplay)

Code	Fehlermeldung & Ursache	Abhilfe
0	EC_Software_Integrity_Check_Failed	Siehe Kapitel <a href="#">4.9.1</a> .
1	EC_Random_Generator_Not_Reliable	Siehe Kapitel <a href="#">4.9.1</a> .
2	EC_Security_Log_Not_Writable	Siehe Kapitel <a href="#">4.9.1</a> .
3	EC_Time_Sync_Pending_Critical	Siehe Kapitel <a href="#">4.9.1</a> .
4	EC_Time_Difference_Intolerable	Siehe Kapitel <a href="#">4.9.1</a> .
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 <a href="#">4.9.1</a> .
7	EC_TSL_Trust_Anchor_Out_Of_Date	Siehe Kapitel <a href="#">4.9.1</a> .
8	EC_Firewall_Not_Reliable	Siehe Kapitel <a href="#">4.9.1</a> .
9	EC_Secure_KeyStore_Not_Available	Siehe Kapitel <a href="#">4.9.1</a> .
20	EC_CardTerminal_Not_Available	Siehe Kapitel <a href="#">4.9.1</a> .
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 ist nicht möglich, da der VPN-Tunnel zum SIS erst aufgebaut werden kann, wenn der VPN-Tunnel zur TI aufgebaut ist.

Code	Fehlermeldung & Ursache	Abhilfe
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.
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 108 Fehlercodes während des Startvorgangs (Hardwaredisplay)

Code	Fehlermeldung Klartext	Fehlermeldung & Ursache	Abhilfe
90	INIT_HARDWARETEST_FAILED	Hardware Test schlug fehl	Kontaktieren Sie Ihren Vertragspartner.
91	INIT_GSMCK_NOT_AVAIL	Die gSMC-K ist nicht verfügbar	Kontaktieren Sie Ihren Vertragspartner.
92	INIT_GSMCK_DEACTIVATED	Die gSMC-K ist deaktiviert	Kontaktieren Sie Ihren Vertragspartner.
93	INIT_ACTIVATION_FAILED	Aktivierung des Konnektors schlug fehl	Kontaktieren Sie Ihren Vertragspartner.
94	BOOT_INTEGRITYTEST_FAILED	Fehlerhafter Integritätstest beim Bootvorgang	Kontaktieren Sie Ihren Vertragspartner.

---

<b>Code</b>	<b>Fehlermeldung Klartext</b>	<b>Fehlermeldung &amp; Ursache</b>	<b>Abhilfe</b>
95	BOOT_SERVICES_NOT_AVAIL	Boot Service steht nicht zur Verfügung	Kontaktieren Sie Ihren Vertragspartner.
96	BOOT_FATAL	Boot Fehler	Kontaktieren Sie Ihren Vertragspartner.
97	INIT_RESET_INCOMPLETE	Werksreset war nicht erfolgreich	Kontaktieren Sie Ihren Vertragspartner.
99	Reservierter Fehlercode für Secure-BIOS-Fehler	Reservierter Fehlercode für Secure-BIOS-Fehler	Kontaktieren Sie Ihren Vertragspartner.

---

**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 109 Kontakt PKI-Betreiber

---

PKI-Betreiber	
T-Systems International GmbH	
Adresse:	Hahnstraße 43d, 60528 Frankfurt am Main
Hotline:	0800-1183307
E-Mail:	<a href="mailto:service.map@telekom.de">service.map@telekom.de</a>

### A.1.2 Herausgeber

Tabelle 110 Kontakt Herausgeber

---

Herausgeber	
T-Systems International GmbH	
Adresse:	Hahnstraße 43d, 60528 Frankfurt am Main
Hotline:	0800-1183307
E-Mail:	<a href="mailto:service.map@telekom.de">service.map@telekom.de</a>

### A.1.3 Hersteller

Tabelle 111 Kontakt Hersteller

---

Hersteller	
T-Systems International GmbH	
Adresse:	Hahnstraße 43d, 60528 Frankfurt am Main
Hotline:	0800-1183307
E-Mail:	<a href="mailto:service.map@telekom.de">service.map@telekom.de</a>

## 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 CO<sub>2</sub>-Bilanz, die Bewertung des Anteils recyclebarer Materialien 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 112 Produktdetails

Allgemein	
Modell	T-Systems Konnektor
Firmware	Version 1.5.3
Hardware	Versionen 2.2.4 / 2.2.5 / 2.2.6

Tabelle 113 Technische Daten

<b>Technische Daten</b>	
<b>Prozessor</b>	
CPU	INTEL Atom (E3845) Quad-Core
Taktfrequenz	1,91 GHz
Anzahl der CPUs	1
<b>Flüchtiger Arbeitsspeicher</b>	
Speicherkapazität	4 GByte DDR3
<b>Nicht-Flüchtiger Speicher</b>	
Speichertyp	Flash eMMC
Speicherkapazität	4 GByte
Durchschnittliche Lese-/Schreibgeschwindigkeit	<ul style="list-style-type: none"> <li>▪ 30 MB/s Lesen</li> <li>▪ 8 MB/s Schreiben</li> </ul>
<b>Schnittstellen</b>	
Ethernet	2 x RJ45 / 10/100/1000 MBit
<b>Netzteil / Versorgungsspannung</b>	
Extern oder intern	Externes Kabelnetzteil
Spannung	230V
<b>gSMC-K</b>	
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 Administrationsoberfläche unter dem Menüpunkt **Systeminformationen**.

Sollten Sie unvorhergesehener Weise keinen Zugriff auf die Lizenzinformationen haben, können Sie die Lizenzinformationen von [service.map@telekom.de](mailto: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.

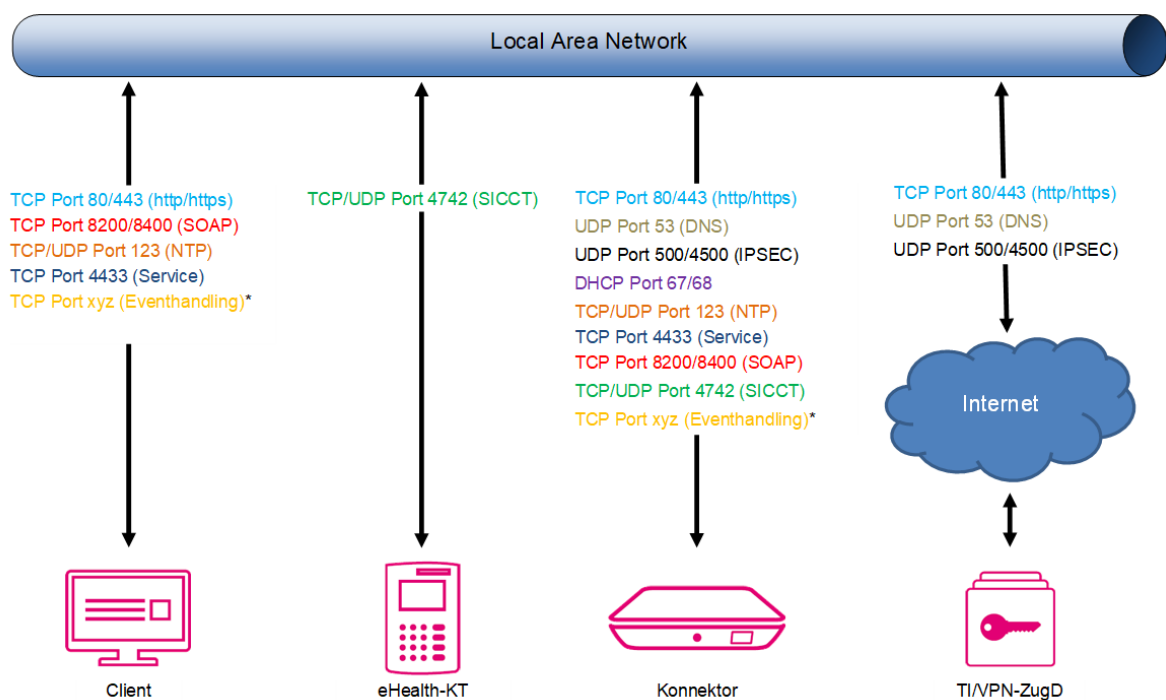
Sie haben die Möglichkeit, einen VPN-gesicherten Zugang ins Internet zu verwenden.

## 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 Verwendete Ports in der dezentralen Zone der TI



\* Diesen Port für das Eventhandling legt jeder Client selbst fest!

Hinweis: IPSEC:500/4500 wird nur ausgehend verwendet (Internet)

Abbildung 48 Verwendete Ports in der dezentralen Zone der TI

## A.8 Glossar

Tabelle 114 Glossar

Glossar	
Administrator	Mit Administrator ist Fachpersonal gemeint, welches die 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 Telemedizininfrastruktur 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 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.
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.

---

**Glossar**

---

SMC	<p>SMC steht für Security Module Card. Diese Karte dient der Identifikation einer berechtigten Institution im Gesundheitswesen. Die SMC gibt es in zwei verschiedenen Ausführungen:</p> <hr/> <p>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.</p> <hr/> <p>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.</p> <hr/>
Telematikinfrastruktur	<p>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.</p> <hr/>
UTC	<p>UTC steht für koordinierte Weltzeit (Universal Time Coordinated) und ist die heute gültige Weltzeit.</p> <hr/>
VPN	<p>VPN steht für Virtual Private Network. Ein VPN dient dazu, einen gesicherten und vertrauenswürdigen Kanal zwischen Netzwerken mit Hilfe kryptografischer Mittel herzustellen.</p> <hr/>
WAN	<p>WAN steht für Wide Area Network und ist ein Netzwerk. Im Speziellen ist hiermit Transportnetz gemeint, über das der Zugang zur Telematikinfrastruktur hergestellt wird.</p> <hr/>