secunet konnektor

Modularer Konnektor

Version 2.0.0

Bedienhandbuch

Für Administratoren und Benutzer

Version 1.04

secunet
Secunet Security Networks AG

Versionshinweise

Dieses Handbuch bezieht sich den von der gematik zugelassenen und vom BSI zertifizierten Modularen Konnektor mit Konstruktionsstand 2.0.0. Informationen über lizenzpflichtige Systemkomponenten finden Sie in Kapitel 12.5.

Dieser Konstruktionsstand legt eine Firmware- und Hardwareversion fest. Informationen zu den zugelassenen Softwareversionen sind der Webseite des Herstellers zu entnehmen (www.secunet.com), Informationen zu zugelassenen Soft- und und Hardwareversion erhalten Sie von der gematik (www.gematik.de).

Bei möglichen Fehlern im Handbuch, die erst nach der Drucklegung erkannt werden, stellt der Hersteller eine Errata zur Verfügung. Diese sowie Informationen zu möglichen Änderungen der dokumentierten Software erhalten Sie auf der Webseite von secunet (https://www.secunet.com/konnektor).

Alle Anleitungen zu Browsern in diesem Dokument beziehen sich auf den Browser Google Chrome Version 61.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Vorwort

Dieses Dokument beschreibt den Modularen Konnektor, der zur sicheren Anbindung von Clientsystemen der Institutionen und Organisationen des Gesundheitswesens an die Telematikinfrastruktur dient. Der Modulare Konnektor ist einerseits verantwortlich für den Zugriff auf die in der Einsatzumgebung befindlichen Kartenterminals sowie Karten und andererseits für die Kommunikation mit den zentralen Diensten der Telematikinfrastruktur und fachanwendungsspezifischen Diensten.

Was beinhaltet dieses Dokument

In diesem Bedienhandbuch ist die Einrichtung, Administration und Bedienung des Modularen Konnektors beschrieben.

An wen ist diese Dokumentation gerichtet

Das Bedienhandbuch richtet sich an Administratoren und Benutzer des Modularen Konnektors, die in folgenden Rollen auf das Gerät zugreifen:

- Arzt (Leistungserbringer)

  Zugriffsberechtigte Person nach § 291a Abs. 4 SGB V, die Leistungen des Gesundheitswesens für Versicherte erbringt.

- Praxispersonal

  Personen, die dezentrale Produkte der Telematikinfrastruktur, z.B. den Modularen Konnektor, im personalbedienten Bereich nutzen.

- Administrator

  Der Administrator ist für die Einrichtung, Administrierung und Bedienung des Modularen Konnektors zuständig. Die Rolle des Administrators kann auch vom Leistungserbringer oder vom Dienstleister vor Ort erfüllt werden.

- Dienstleister vor Ort (DVO)

  Der DVO unterstützt den Administrator beim Betrieb des Netzwerks mit den darin befindlichen Komponenten.

Erforderliches Vorwissen

Die Administration des Modularen Konnektors setzt Grundlagenwissen über IP-Netzwerke und deren Konfiguration im Umfeld der Telematikinfrastruktur sowie über virtuelle private Netze voraus.

Konventionen

Das Bedienhandbuch verwendet folgende typographische Konventionen:

- **Interaktive Elemente** wie **Schaltflächen** werden großgeschrieben.
- *Eingaben in die Bedienoberfläche* und hervorgehobene Eigenbezeichnungen werden kursiv dargestellt.
- Listenabsätze mit Aufzählungszeichen werden für Informationen und Aufzählungen verwendet.

▶ Handlungsanweisungen werden mit Pfeilen dargestellt.

Sicherheitssymbole

Warnung

Dieses Symbol warnt vor möglichen Sachschäden. Sachschäden können verursacht werden, wenn Sie diesen Sicherheitshinweis missachten.

Vorsicht

Dieses Symbol warnt vor möglichen Sicherheitsrisiken, z.B. durch eine fehlerhafte Konfiguration.

Tipp

Dieses Symbol weist auf Tipps zur optimalen Nutzung sowie andere nützliche Informationen hin.

1 Funktionsbeschreibung

1.1 Einsatzzweck

Der Modulare Konnektor dient dem sicheren Betrieb der IT-Systeme einer Praxis oder Praxisgemeinschaft und der Anbindung an die Telematikinfrastruktur.

Dazu stellt der Modulare Konnektor folgende Funktionen zur Verfügung:

- Anbindung an die Telematikinfrastruktur

  Der Modulare Konnektor kann eine gesicherte VPN-Verbindung (Virtual Private Network) zur zentralen Telematikinfrastruktur herstellen.

- Schutz auf Transportebene

  Der Modulare Konnektor kann sensible Daten zusätzlich auf Transportebene schützen (TLS).

- Protokollierung

  Der Modulare Konnektor protokolliert automatisch sicherheitsrelevante und operative Ereignisse.

- Anbindung an das Internet

  Der Modulare Konnektor kann das lokale Netzwerk mit dem Sicheren Internetservice (SIS) verbinden.

- Firewall

  Die am Modularen Konnektor angeschlossenen Clientsysteme und Kartenterminals im lokalen Netzwerk werden vor unberechtigtem Zugriff aus dem Internet geschützt. Der Datenverkehr wird mithilfe eines Paketfilters überwacht.

- Plattform für die Ausführung von Anwendungen (Fachmodule)

  Der Modulare Konnektor kann zur Ausführung von Fachmodulen wie z.B. dem Versichertenstammdatenmanagement (VSDM) genutzt werden und ermöglicht die gesicherte Kommunikation zwischen Fachmodulen und Anwendungsdiensten in der Telematikinfrastruktur.

- Weitere Dienste im lokalen Netzwerk

  Der Modulare Konnektor kann im lokalen Netzwerk einen NTP-, DHCP- und DNS-Server bereitstellen.

1.2 Sicherheitsfunktionen

1.2.1 Anbindung an die Telematikinfrastruktur

Die Verbindung mit der Telematikinfrastruktur (TI) nutzt den zentralen VPN-Zugangsdienst. Der VPN-Tunnel, der vom Modularen Konnektor aufgebaut wird, endet am VPN-Konzentrator, der als zentraler Verbindungspunkt des VPN-Zugangsdienstes dient.

Die Verbindung wird wie folgt aufgebaut:

1. Vor dem Aufbau der VPN-Verbindung durch den Modularen Konnektor werden die beiden Kommunikationsendpunkte authentisiert.
   - Der VPN- Zugangsdienst überprüft durch Kontrolle des Zertifikates des Modularen Konnektors, ob dieser für die Nutzung des VPN-Zugangsdienstes freigeschaltet ist.
   - Der Modulare Konnektor überprüft das Zertifikat des VPN-Zugangs-dienstes.
2. Nach erfolgreicher Authentifizierung wird die nachfolgende Kommunikation bis zur Abmeldung mit einem Sitzungsschlüssel gesichert.

Wenn vom anderen Kommunikationsendpunkt eine nicht erwartete Authentisierungsmethode verwendet wird, schlägt die Authentisierung beim Modularen Konnektor fehl. In diesem Fall wird die VPN-Verbindung nicht aufgebaut.

Die Identifizierung gegenüber der TI erfolgt mit Karten, die über die im lokalen Netzwerk angeschlossenen Kartenterminals eingelesen werden:

- Praxisausweis (Security Module Card, SMC-B)
- Heilberufsausweis (HBA)

1.2.2 Authentisierung und Vertraulichkeit externer Verbindungen

Der Modulare Konnektor erfordert die Authentisierung aller externer Kommunikationspartners (TI und SIS) und authentifiziert sich selbst gegenüber diesen Partnern. Dies erfolgt auf der Basis von IPsec und mit Hilfe von Zertifikaten nach dem Standard X.509v3.

Nach erfolgtem Verbindungsaufbau authentisiert sich der Modulare Konnektor gegenüber den Diensten der Telematikinfrastruktur mittels Schlüsselmaterial des Praxisausweises. Auf Transportschicht kann mit Hilfe von Transport Layer Security/ Secure Socket Layer (TLS/SSL) die Integrität und Vertraulichkeit der übertragenen Daten sichergestellt werden.

1.2.3 Anbindung an das Internet

Über einen von der gematik zugelassenen Sicheren Internetservice (SIS) kann die Verbindung ins Internet hergestellt werden. Dazu wird ein VPN-Tunnel zum VPN-Konzentrator des SIS aufgebaut.

Wenn außer dem Modularen Konnektor weitere Anbindungen des lokalen Netzwerks an das Internet genutzt werden, kann dies zu erheblichen Sicherheitsrisiken führen. Grundsätzlich sind auch Angriffe aus dem Internet über den SIS nicht auszuschließen. Alle Clientsysteme müssen entsprechende Sicherheitsmaßnahmen besitzen.

1.2.4 Gültigkeitsprüfung von Zertifikaten

Der Zertifikatsdienst des Modularen Konnektor überprüft die Gültigkeit von Zertifikaten. Dazu stellt der VPN-Zugangsdienst eine Trust-Service Status List (TSL) mit den Zertifikaten von zulässigen Dienstanbietern und eine Sperrliste (Certificate Revocation List, CRL) mit gesperrten Zertifikaten bereit.

Die Prüfung von Zertifikaten beinhaltet:

- Die Prüfung der Zulässigkeit des Zertifikates auf Grundlage der TSL und der CRL
- Die kryptographische Prüfung der Signatur des Zertifikates
- Die Prüfung durch den Online Certificate Status Protocol (OCSP)-Dienst der TI

1.2.5 Paketfilter

Zur Abwehr von Angriffen schränkt der Modulare Konnektor den Datenaustausch mit dem öffentlichen Transportnetz ein und unterbindet direkte Kommunikation außerhalb von VPN-Kanälen ins Transportnetz mit Ausnahme der für den VPN-Verbindungsaufbau erforderlichen Kommunikation.

Die Kommunikation mit externen Verbindungspartnern wird von einem Paketfilter (Firewall) überwacht, der den Datenfluss anhand eines Regelwerks kontrolliert. Die Regeln des Paketfilters sind werksseitig voreingestellt und können den örtlichen Erfordernissen angepasst werden.

Ein LAN-seitiger Paketfilter hindert Schadsoftware, die möglicherweise in das lokale Netzwerk gelangt ist daran, die Integrität des Modularen Konnektors zu bedrohen.

Zudem akzeptiert der Modulare Konnektor nur korrekte IP-Pakete.

1.2.6 Kryptografisch gesicherter Speicher

Der Modulare Konnektor verwendet für die Ablage von Protokolleinträgen und der für den Betrieb erforderlichen Daten einen kryptografisch gesicherten Speicher. Alle gespeicherten Daten und Schlüssel sind dadurch unter Verwendung eines geräteindividuellen Schlüssels geschützt. Der Modulare Konnektor löscht nicht mehr benötigte Schlüssel (insbesondere Sitzungsschlüssel für VPN- und TLS-Verbindungen) nach ihrer Verwendung durch aktives Überschreiben.

Die Sicherheitsprotokollierung (Security Log) wird in einem persistenten Speicher durchgeführt und steht auch nach einem Neustart zur Verfügung.

Ein internes Sicherheitsmodul (Security Module Card Konnektor, gSMC-K), beinhaltet die Identität des Modularen Konnektors, die untrennbar mit dem Gerät verbunden ist.

1.3 Weitere Dienste

1.3.1 Zeitdienst

Der Modulare Konnektor stellt im lokalen Netzwerk einen NTP-Server der Stratum-Ebene 3 für Fachmodule und Clientsysteme bereit. Dieser synchronisiert sich bei Online-Betrieb in regelmäßigen Abständen mit einem NTP-Server der Stratum-Ebene 2 in der zentralen Telematikinfrastruktur. Dabei wird eine Plausibilitätskontrolle der vom Zeitdienst übermittelten Zeitinformationen durchgeführt.

Die bereitgestellten Zeitinformationen werden für die Prüfung der Gültigkeit von Zertifikaten genutzt, und um die Einträge der Sicherheitsprotokollierung mit Zeitstempeln zu versehen.

1.3.2 DHCP-Dienst

Der Modulare Konnektor stellt im lokalen Netzwerk optional einen DHCP-Server gemäß RFC 2131 und RFC 2132 zur Verfügung.

1.3.3 DNS-Dienst

Der Modulare Konnektor stellt im lokalen Netzwerk optional einen DNS-Server zur Verfügung. Der DNS-Server unterstützt DNSSEC-Erweiterungen gemäß RFC 4035. Die für DNSSEC verwendeten Vertrauensanker werden regelmäßig aktualisiert.

1.4 Netzwerkschnittstellen

Der Modulare Konnektor besitzt zwei Netzwerkschnittstellen:

- LAN

  Die Schnittstelle zum lokalen Netzwerk und den darin befindlichen Clientsystemen und Kartenterminals.

- WAN

  Je nach Anbindungsmodus (siehe Kapitel 6.4.1.2) die Schnittstelle zum Internet Access Gateway (IAG) für die Verbindung mit der Telematikinfrastruktur.

  Der IAG bezeichnet das/die Gerät(e), die den Internetzugang ermöglichen und üblicherweise vom Internet Service Provider (ISP) zur Verfügung gestellt werden, z.B. DSL-Router und DSL-Modem.

Details zu den unterstützten Netzwerkprotokollen finden Sie in Kapitel 12.1.

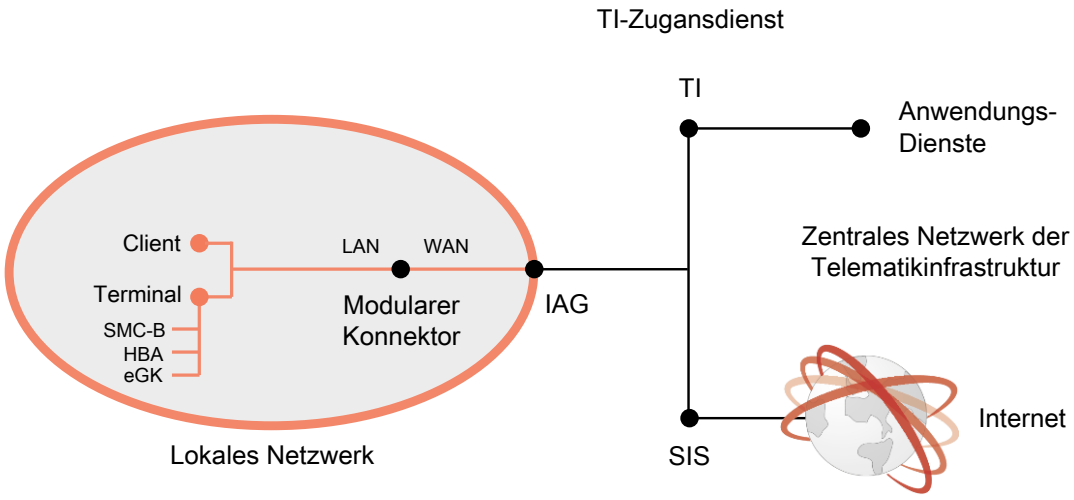


Abbildung 1: Netzwerkschnittstellen des Modularen Konnektors (Beispiel)

2 Lieferprozess

Um die Sicherheit des zugelassenen Modularen Konnektors zu gewährleisten, unterliegt der Lieferprozess definierten Anforderungen an die sichere Lieferkette. Nur Lieferanten, die diese Anforderungen an Transport und Lagerung einhalten, sind Teil der sicheren Lieferkette. Der Leistungserbringer ist als Endpunkt der sicheren Lieferkette dafür verantwortlich, dass die im Dokument "Hinweise und Prüfpunkte für Endnutzer" beschriebenen Prüfungen durchgeführt werden. Das Dokument erhalten Sie auf der Webseite von secunet (https://www.secunet.com/konnektor).

Ein Modularer Konnektor, der nicht über den Prozess der sicheren Auslieferung bezogen wurde, darf nicht in der TI in Betrieb genommen werden.

2.1 Transportverpackung prüfen

Der Modulare Konnektor wird in einer Transportverpackung geliefert. Die Transportverpackung ist mit einem Siegelband gesichert.

- Überprüfen Sie die Unversehrtheit des Siegelbands der Transportverpackung.

Bei einem Öffnungsversuch lösen sich die Schichten des Siegelbands, sodass ein Schriftzug erkennbar ist.

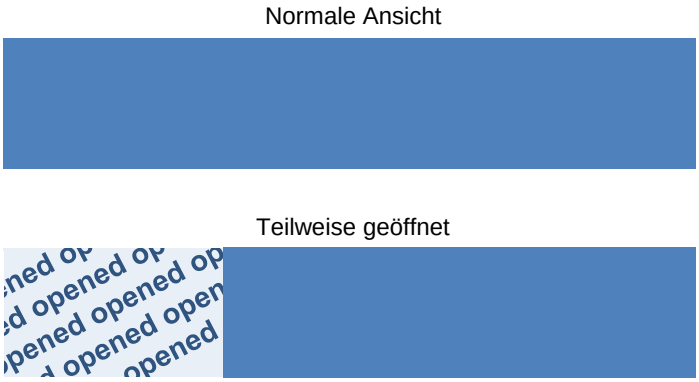


Abbildung 2: Siegelband der Transportverpackung

Wenn das Siegelband oder die Transportverpackung beschädigt sind, darf der Modulare Konnektor nicht verwendet werden. Kontaktieren Sie in diesem Fall den zuständigen DVO.

2.2 Lieferumfang

Der Lieferumfang des Modularen Konnektors umfasst folgendes Zubehör.

Komponente	Beschreibung
Modularer Konnektor	
Externes Netzteil*	AC Steckernetzteil 220V und Netzkabel
Sicherheitsbeiblätter	*Empfang und Prüfung* *Aufstellung und Inbetriebnahme*
Beiblatt	*Lizenzinformationen*
CD/DVD	Bedienhandbuch als PDF

* Zusätzlich als Ersatzteil bestellbar

Tabelle 1: Lieferumfang und Zubehör

Die Sicherheitsbeiblätter "Empfang und Prüfung" und "Aufstellung und Inbetriebnahme" enthalten Sicherheitshinweise für den Modularen Konnektors. Diese Sicherheitsbeiblätter finden Sie auch in Anhang 12.6. Verwenden Sie entweder Ausdrucke der entsprechenden Anhänge des Handbuches oder prüfen Sie, dass die beigelegten Sicherheitsbeiblätter der Gerätelieferung mit den Inhalten von Anhang 12.6 des Handbuches übereinstimmen.

Als optionales Zubehör ist eine Halterung für die Wandmontage erhältlich.

2.3 Gerät auspacken

Gehen Sie wie folgt vor:

- Entnehmen Sie den Modularen Konnektor und das mitgelieferte Zubehör vorsichtig aus der Verpackung.
- Überprüfen Sie den Lieferumfang auf Vollständigkeit.
- Beachten Sie die Sicherheitshinweise der beiden Sicherheitsbeiblätter *Empfang und Prüfung* und *Aufstellung und Inbetriebnahme*:
  - Untersuchen Sie das Gerät und das Zubehör durch Sichtkontrolle auf Schäden.
  - Prüfen sie die Sicherheitssiegel und das Gehäuse auf Manipulationen und Schäden (siehe Kapitel 2.4).
  - Notieren Sie die Seriennummern der beiden Sicherheitssiegel auf dem Sicherheitsbeiblatt *Empfang und Prüfung*.
  - Die Seriennummern sind auf den Sicherheitssiegeln in Klarschrift und als QR-Code aufgedruckt.
  - Notieren Sie die Seriennummer des Geräts auf dem Sicherheitsbeiblatt *Empfang und Prüfung*. Die Seriennummer befindet sich auf dem Typenschild und auf der Kennzeichnung auf der Verpackung.
- Bewahren Sie die Sicherheitsbeiblätter sicher und getrennt vom Modularen Konnektor auf. Unbefugte Personen dürfen keinen Zugriff auf die Sicherheitsbeiblätter haben.
- Bewahren Sie die Verpackung für eine spätere Wiederverwendung auf.

Abbildung 3: Typenschild

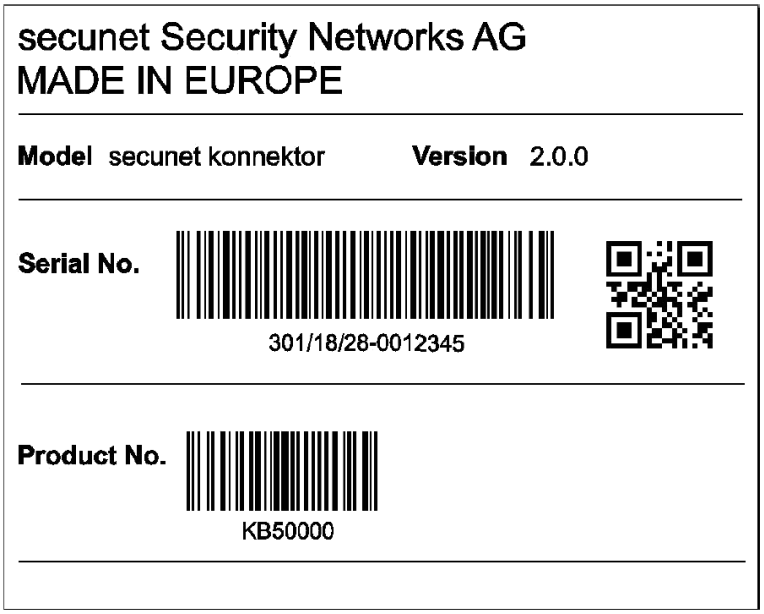


Abbildung 4: Verpackungskennzeichnung

2.4 Manipulationsversuche erkennen

2.4.1 Sicherheitssiegel

Der Modulare Konnektor ist mit zwei Sicherheitssiegeln ausgestattet, die in Vertiefungen an den beiden Gehäuseseiten angebracht sind.

Abbildung 5: Anbringungsort der Sicherheitssiegel

Achtung

- **Das Gerät darf bei beschädigten Sicherheitssiegeln auf keinen Fall in Betrieb genommen werden.**
- **Wenn während des Betriebs beschädigte Sicherheitssiegel oder ein beschädigtes Gehäuse festgestellt werden, befolgen Sie die Hinweise zur Meldung von Verlust oder Kompromittierung in Kapitel 9.**
- **Nur berechtigte Personen dürfen die Sicherheitssiegel prüfen.**

2.4.1.1 Merkmale von Sicherheitssiegeln

Die Größe der Sicherheitssiegel beträgt 30 mm x 10 mm.

Abbildung 6: Sicherheitssiegel (Beispiel)

Die Sicherheitssiegel besitzen folgende Sicherheitsmerkmale:

- Kreuzförmige Sicherheitsstanzungen
- Seriennummer (auf dem Sicherheitsbeiblatt *Empfang und Prüfung* notiert)
- Öffnungsbotschaft „GEOEFFNET OPENED“ bei Beschädigung
- Thermoreaktive Linienzüge
  Ab einer Temperatur von ca. 45 °C sind die roten Linien nicht mehr zu sehen.

Abbildung 7: Thermoreaktive Linienzüge

- UV-aktiver Schriftzug „SECURITY“
  Der Schriftzug wird unter UV-Licht von ca. 365nm sichtbar.

Abbildung 8: Sicherheitssiegel unter UV-Licht

2.4.1.2 Beschädigt Sicherheitssiegel erkennen

So erkennen Sie Beschädigungen der Sicherheitssiegel:

- Prüfen Sie, ob die Sicherheitsmerkmale beeinträchtigt sind.

Abbildung 9: Beschädigtes Sicherheitssiegel

Abbildung 10: Rückstände eines abgezogenen Sicherheitssiegels

- Prüfen Sie, ob ein Sicherheitssiegel entlang der Gehäusekanten durchschnitten oder zerkratzt ist.
- Prüfen Sie, ob ein Sicherheitssiegel eine unzureichende Verbindung zum Gehäuse besitzt und sich abheben lässt.
- Prüfen Sie, ob ein Sicherheitssiegel farblich verändert ist.
- Prüfen Sie, ob ein Sicherheitssiegel Klebereste besitzt.

Das Gerät darf bei beschädigten Sicherheitssiegeln auf keinen Fall in Betrieb genommen werden.

2.4.2 Gehäuse

Das Gehäuse bietet keinen aktiven Schutz zur Erkennung von Eindringversuchen. Es ist daher regelmäßig zu prüfen, ob Manipulationsversuche vorgenommen wurden.

2.4.2.1 Eindringversuche erkennen

Prüfen Sie das Gehäuse auf Eindringversuche (siehe Abbildung 11 auf Seite 28, Abbildung 12 auf Seite 32 und Abbildung 13 auf Seite 33):

- Prüfen Sie, ob Beschädigungen von Gehäuse und Lackierung bestehen.
- Prüfen Sie, ob Beschädigungen im Bereich der Gehäuseverbindungen bestehen.
- Prüfen Sie, ob es weitere als die in den Schnittstellen enthaltenen Öffnungen im Gehäuse gibt.
- Prüfen Sie, ob die Betriebsanzeigen (LEDs) beschädigt sind.
- Prüfen Sie, ob zusätzliche Aufkleber oder externe Anbauteile vorhanden sind.

Das Gerät darf bei beschädigtem Gehäuse oder Manipulationsverdacht auf keinen Fall in Betrieb genommen werden.

3 Gerätebeschreibung

3.1 Schnittstellen und Bedienelemente

3.1.1 Geräteoberseite

Abbildung 11: Gehäuseoberseite

Die roten Betriebsanzeigen (LEDs) signalisieren aktuelle Betriebszustände.

3.1.1.1 Anzeigen im Normalbetrieb

Der Normalbetrieb beginnt etwa drei Minuten nach dem Einschalten des Modularen Konnektors.

LED	Funktion	Signal	Erläuterung
Power	Stromversorgung	An	Eingeschaltet (Unabhängig von den weiteren Gerätefunktionen)
		Aus	Ausgeschaltet
System	Betriebszustand	An	Betriebsbereit
		Blinkt	System startet
		Aus	Nicht betriebsbereit
VPN TI	Verbindung mit TI	An	VPN-Verbindung zur TI
		Blinkt	Aufbau der VPN-Verbindung zur TI
		Aus	Keine VPN-Verbindung zur TI
VPN SIS	Verbindung mit SIS	An	VPN-Verbindung zum SIS
		Blinkt	Aufbau der VPN-Verbindung zum SIS
		Aus	Keine VPN-Verbindung zum SIS
Service	Fehler	An	Fehler / Warnung
		Blinkt	Fehler mit hoher Priorität (s. Kapitel 12.3.2)
		Aus	Kein Fehler
Update	Update	An	Update steht bereit
		Blinkt	Update wird durchgeführt
		Aus	Kein Update verfügbar oder Update erfolgreich abgeschlossen
Remote	Remote Management Schnittstelle	An	Remote Management aktiviert
		Blinkt	Remote Management wird durchgeführt
		Aus	Remote Management deaktiviert

Tabelle 2: Anzeigen im laufenden Betrieb

LED(s)	Signal	Erläuterung
Service, Update, Remote	Blinkt	Werksreset wird durchgeführt (siehe Kapitel 6.6)
Service, Update, Remote	An	Werksreset erfolgreich abgeschlossen; die Anzeigen leuchten für 15 Sekunden
Update, Remote	Blinkt	Werksreset zum Versand wird durchgeführt (s. Kapitel 6.7)
Update, Remote	An	Werksreset zum Versand erfolgreich abgeschlossen; die Anzeigen leuchten für 15 Sekunden
Remote	An	Werksreset Failsafe (feste IP) erfolgreich abgeschlossen
Service	An	Werksreset fehlgeschlagen Werksreset, Werksreset zum Versand, Werksreset Failsafe (feste IP)
Alle bis auf Power	Blinkt	System wird heruntergefahren (Dauer bis zu 3 Minuten)

Tabelle 3: Anzeigen bei besonderen Betriebszuständen

3.1.1.2 Anzeigen beim Systemstart

LED(s)	Signal	Erläuterung
Alle	An	Nacheinander kurzzeitiger Funktionstest
Alle	Fort-laufend	BIOS-Update Das Update wird automatisch installiert. Anschließend startet das System erneut. Bei einem Fehler während des BIOS-Updates leuchten alle LEDs dauerhaft.
Service, Update, Remote	An	Boot-Prozess des BIOS startet
Alle	An	Fehler beim Abarbeiten des BIOS
System	Blinkt	System startet

System, VPN TI, VPN SIS (je nach Betriebszustand)	An	System in Betrieb
Service	Blinkt	Fehler beim Systemstart, System startet neu Trennen Sie das Gerät bei mehrmaliger Wiederholung eines Systemstarts vom Stromnetz und kontaktieren Sie den DVO.

Tabelle 4: Anzeigen beim Systemstart

3.1.2 Gehäuserückseite

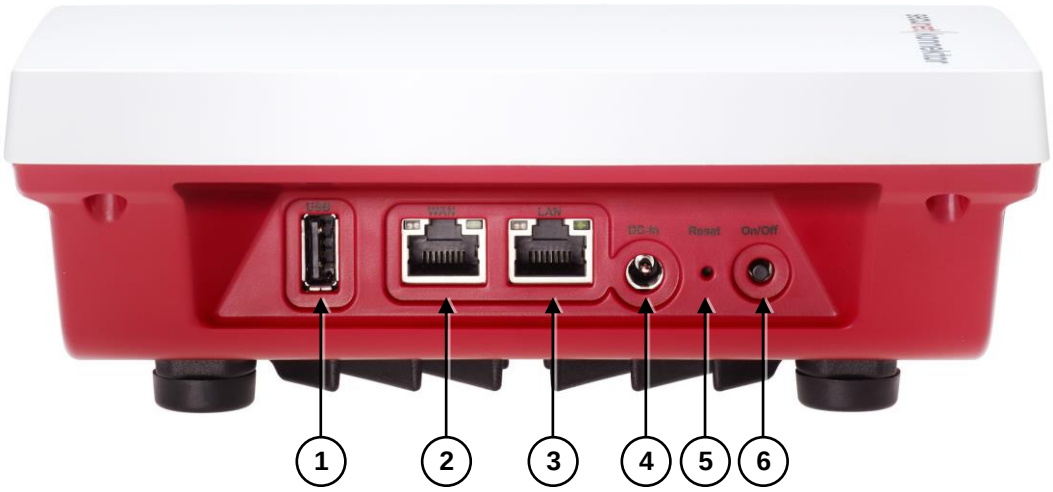


Abbildung 12: Gehäuserückseite

Position	Bezeichnung
1	Schnittstelle USB 2.0 **Die USB-Schnittstelle ist ohne Funktion und darf nicht verwendet werden.**
2	Netzwerkanschluss WAN
3	Netzwerkanschluss LAN
4	Spannungsversorgung 12 V
5	Reset-Taster für alternativen Login und Werksreset (siehe Kapitel 6.6)
6	An/Aus-Taster (Beachten sie die Hinweise in Kapitel 3.2)

Tabelle 5: Bedienelemente und Schnittstellen an der Geräterückseite

3.1.3 Gehäuseunterseite

3.1.3.1 Gehäuse ohne Wandhalterung

Abbildung 13: Gehäuseunterseite ohne Wandhalterung

Position	Bezeichnung
1	Gummifüße
2	Kühlplatte

Tabelle 6: Gehäuseunterseite

3.1.3.2 Gehäuse mit Wandhalterung (optional)

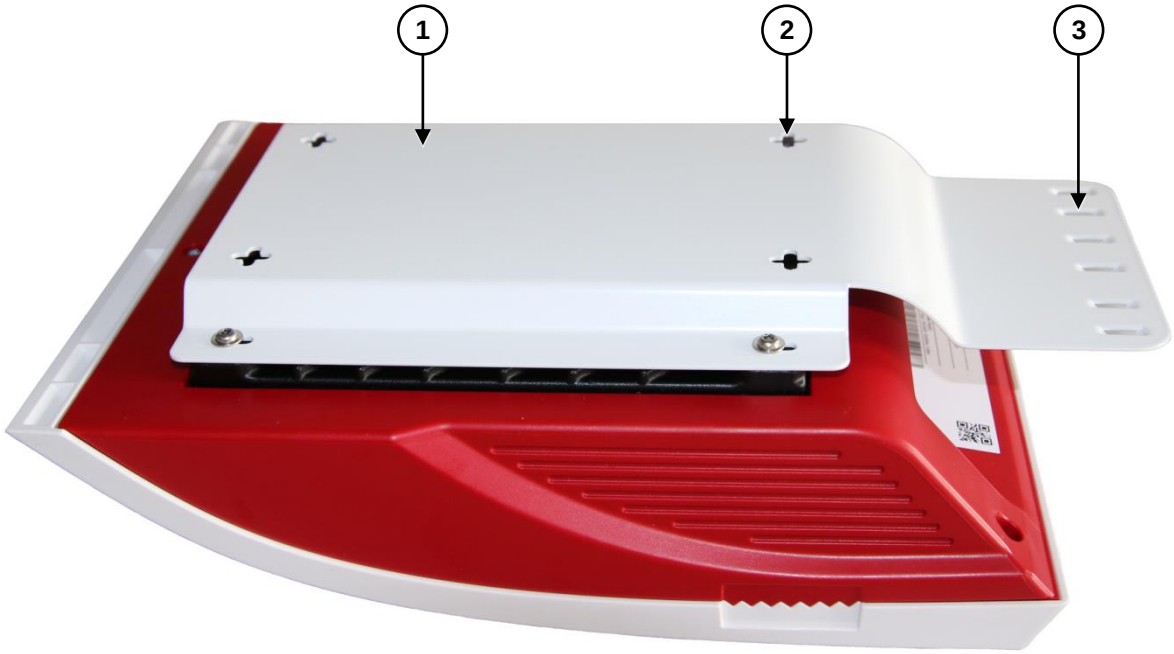


Abbildung 14: Gehäuseunterseite mit Wandhalterung

Position	Bezeichnung
1	Wandhalterung
2	Montageöffnungen
3	Kabelfixierungen

Tabelle 7: Gehäuseunterseite mit Wandhalterung

3.2 Gerät ein-/ausschalten

Der An/Aus-Taster befindet sich auf der Geräterückseite (siehe Kapitel 3.1.2).

Zwischen dem Ausschalten und dem Einschalten der Spannungsversorgung muss mindestens 30 Sekunden gewartet werden.

Einschalten:

- An/Aus-Taster kurz drücken.

  Für die Anzeigen beim Systemstart siehe Kapitel 3.1.1.2. Der Normalbetrieb beginnt etwa drei Minuten nach dem Einschalten des Modularen Konnektors.

Ausschalten:

- An/Aus-Taster innerhalb von 3 Sekunden zweimal drücken (Schutz vor unabsichtlicher Betätigung). Zwischen den beiden Taster-Betätigungen muss eine Sekunde gewartet werden. Während des Herunterfahrens blinken alle LEDs außer der Anzeige *Power*. Das Herunterfahren kann bis zu 3 Minuten dauern.

Notunterbrechung:

- An/Aus-Taster ca. 4 Sekunden lang gedrückt halten.

Schalten Sie den Modularen Konnektor stets durch die zweimalige kurze Betätigung des An/Aus-Tasters aus. Das Trennen der Spannungsversorgung oder die Notunterbrechung im laufenden Betrieb kann das Gerät irreparabel beschädigen.

Der Modulare Konnektor prüft beim Start, ob alle erforderlichen Dienste gestartet werden können. Wenn nicht alle Dienste gestartet werden können, fährt der Modulare Konnektor automatisch herunter und schaltet sich aus.

3.3 Verhalten bei Spannungsausfällen

Der Modulare Konnektor erkennt den letzten Betriebsstand (An/Aus) und stellt diesen nach einem Spannungsausfall automatisch wieder her. Dadurch startet der Modulare Konnektor nach einem Spanungsausfall automatisch, sofern der Modulare Konnektor zum Zeitpunkt des Spannungsausfalls eingeschaltet war.

3.4 Produkt- und Betriebsmerkmale

3.4.1 Produktmerkmale

Allgemein	
Abmessungen	ca. L × B × H: 250 mm × 180 mm × 70 mm
Gewicht	ca. 900 g
Schnittstellen	1 × USB 2.0 1 × WAN 1 GB Ethernet 1 × LAN 1 GB Ethernet 1 × Spannungsversorgung 12 V 1 × Werksreset 1 × Ein/Aus-Taster
Schutzklasse	2
Zertifizierungen	Hiermit erklärt die secunet Security Networks AG, dass der secunet konnektor den Richtlinien 2014/30/EU, 2014/35/EG, 2009/125/EG sowie 2011/65/EU entspricht. Die ausführliche Fassung der Erklärung zur CE-Konformität finden Sie auf der Webseite von secunet unter https://www.secunet.com/konnektor.

Interne Komponenten	
Prozessor	Intel® X86-64
Arbeitsspeicher	8 GB RAM
gSMC-K	STARCOS 3.6 Health SMCK R1
Festplatte	16 GB SSD
Netzwerk	Zwei getrennte Netzwerkcontroller für WAN/LAN

RTC	Real Time Clock, max. Drift +/- 20 ppm

Tabelle 8: Produktmerkmale

3.4.2 Betriebsmerkmale

Betriebsmerkmale	
Stromversorgung	12 V DC vom Steckernetzteil, 100 - 240 V AC 50Hz (Steckdose)
Leistungsaufnahme	7 W
Betriebsumgebung	Innenraum (Büroumgebung), maximale Einsatzhöhe 2000 m über NN
Temperatur	
In Betrieb	+5° C bis +40° C
Lagerung/Transport	-10° C bis +55° C
Luftfeuchtigkeit	
In Betrieb	10 % bis 85 %, nicht kondensierend
Lagerung/Transport	10 % bis 90 %, nicht kondensierend

Tabelle 9: Betriebsmerkmale

4 Aufbau und Betriebsumgebung

Überprüfen Sie vor der Inbetriebnahme die Unversehrtheit der Sicherheitssiegel und des Gehäuses (siehe Kapitel 2.4.1 und 2.4.2). Bei Beschädigungen darf das Gerät nicht in Betrieb genommen werden.

4.1 Sicherheitshinweise zu Aufbau und Betriebsumgebung

Der Aufstellungsort muss folgende Anforderungen erfüllen:

- **Der Modulare Konnektor darf nur in einer der folgenden Umgebungen betrieben werden:**
  - **Innerhalb eines personalbedienten Bereichs, in dem sich der Leistungserbringer regelmäßig aufhält. Dritte dürfen zum Modularen Konnektor keinen Zugriff haben.**
  - **In einem abgeschlossenen, nicht öffentlichen Betriebsraum.**
  - **In einem abgeschlossenen Schrank, der den Modularen Konnektor vor unberechtigtem Zugriff schützt.**
- **Die Einsatzumgebung des Modularen Konnektors muss diesen vor physischen Angriffen schützen.**
- **Schützen Sie den Modularen Konnektor vor Spritzwasser und direktem Sonnenlicht.**
- **Die organisatorischen Maßnahmen in der Umgebung müssen sicherstellen, dass ein Diebstahl des Modularen Konnektors oder eine Manipulation am Gerät rechtzeitig erkannt wird (siehe Kapitel 2.4.1.2 und 2.4.2).**
- **Die verwendete Steckdose muss zugänglich sein, um das Gerät bei Bedarf vom Netz trennen zu können.**
- **Schützen Sie den Modularen Konnektor im Betrieb vor Berührungen und vermeiden Sie Kontakt mit hitzeempfindlichen Gegenständen.**

Heiße Oberfläche

Verbrennungsgefahr bei Berührung im Betrieb erhitzter Gehäuseteile

Nach dem Abschalten des Geräts mindestens fünf Minuten warten, bis das Gehäuse berührt wird. Dieses gilt für den Betrieb sowohl mit wie auch ohne die optional verfügbare Wandhalterung.

4.2 Sicherheitshinweise zu Passwörtern

Ein Passwort, das für den Zugriff auf den Modularen Konnektor festgelegt wird, muss mindestens acht Zeichen lang sein und Zeichen aus drei der folgenden Zeichenarten enthalten:

- Großbuchstaben
- Kleinbuchstaben
- Sonderzeichen
- Ziffern.

Ein Passwort darf nicht den zugeordneten Benutzernamen enthalten (weder vorwärts noch rückwärts, unter Ignorieren der Groß- und Kleinschreibung). Des Weiteren darf bei einer Passwortänderung das neue Passwort keine zuvor bereits benutzten Passwörter beinhalten.

Halten Sie Passwörter stets geheim.

- **Passwörter dürfen nicht schriftlich aufbewahrt werden.**
- **Passwörter dürfen nicht an Dritte weitergegeben werden.**

4.3 Sicherheitshinweise zu Verlust oder Diebstahl

Es muss sichergestellt sein, dass für die Inbetriebnahme und Administration des Modularen Konnektors nur vertrauenswürdiges, mit der Benutzerdokumentation vertrautes, sachkundiges Personal eingesetzt wird. Wenn der Modulare Konnektor gestohlen wird oder abhandenkommt, muss der DVO informiert werden.

▶ Beachten Sie bei Verlust oder Diebstahl die Hinweise in Kapitel 9.

▶ Halten Sie das Sicherheitsbeiblatt *Empfang und Prüfung* bereit, auf dem die Seriennummer des Geräts notiert ist.

4.4 Sicherheitshinweise für die Netzwerkumgebung

Clientsysteme müssen korrekt angeschlossen werden. Der Administrator muss sich davon überzeugen, dass der Leistungserbringer das lokale Netzwerk in sicherer Weise betreibt.

Internet-Anbindung

Wenn außer durch dem Modularen Konnektor weitere Anbindungen des lokalen Netzwerks an das Internet genutzt werden, kann dies zu erheblichen Sicherheitsrisiken führen. Alle Clientsysteme müssen entsprechende Sicherheitsmaßnahmen besitzen.

Eine sichere Anbindung kann z. B. dadurch erfolgen, dass es neben dem definierten Zugang zum Transportnetz über den Modularen Konnektor keine weiteren ungeschützten oder geringer geschützten Zugänge zum Transportnetz gibt.

Verantwortung für Clientsysteme

Die Verantwortung für die Clientsysteme liegt beim Leistungserbringer. Es dürfen nur zugelassene Clientsysteme eingesetzt werden. Die Clientsysteme müssen in sicherer Art und Weise betrieben werden; auf die Clientsysteme oder andere IT-Systeme im LAN darf keine Schadsoftware aufgebracht werden.

Der Modulare Konnektor darf nur mit anderen von der gematik zugelassenen Komponenten wie z.B. zugelassenen eHealth-Kartenterminals betrieben werden. Diese müssen den Modularen Konnektor für Dienste gemäß § 291a korrekt aufrufen. Aufrufe von Diensten gemäß § 291a müssen über den Modularen Konnektor erfolgen.

Es ist dafür zu sorgen, dass administrative Tätigkeiten der lokalen und zentralen Administration in Übereinstimmung mit der Dokumentation des Modularen Konnektors durchgeführt werden. Für den Betrieb muss vertrauenswürdiges, mit der Benutzerdokumentation vertrautes, sachkundiges Personal eingesetzt werden.

Der Leistungserbringer muss sicherstellen, dass die verwendeten Komponenten, z.B. zugelassenen eHealth-Kartenterminals und Clientsystem-Anwendungen, miteinander Kompatibel sind.

4.5 Montage

Verwenden Sie für die Montage und den Betrieb des Modularen Konnektors nur das mitgelieferte Originalzubehör. Insbesondere darf nur das originale Netzteil benutzt werden, da sonst Brandgefahr besteht. Das originale Netzteil ist als Ersatzteil erhältlich.

Beachten Sie die Hinweise zur Betriebsumgebung in Kapitel 3.4.2 und 4.1. Achten Sie insbesondere auf eine ausreichende Belüftung und vermeiden Sie direkte Sonneneinstrahlung.

4.5.1 Ebene Montage

- ▶ Stellen Sie den Modularen Konnektor an einem geeigneten Ort auf.
- ▶ Stellen Sie beim Aufstellen auf einem Schreibtisch, in einem Regal oder Schrank sicher, dass das Gerät auf einer ebenen und stabilen Unterlage steht und ein Luftaustausch an der Kühlplatte unter dem Gerät möglich ist.

4.5.2 Wandmontage

Für die Wandmontage ist eine Wandhalterung verfügbar (siehe Kapitel 3.1.3.2). Der Modulare Konnektor kann mit den Kabelfixierungen nach unten oder nach rechts montiert werden.

Als Montagematerial für die Montage der Wandhalterung werden empfohlen:

- Dübel SX 4 × 20 (Fischer)
- Schraube KA30 × 20 PT-Linsenkopfschraube Stahl

Gehen Sie wie folgt vor:

- ▶ Bringen Sie zur Montage der Wandhalterung 4 Schrauben so an der Wand an, dass die Schraubenköpfe ausreichend aus der Wand hervorstehen.

Tipp

Verwenden Sie die Wandhalterung als Bohrschablone.

- ▶ Schrauben Sie die Gummifüße von der Geräteunterseite mit einem Torx-Schraubendreher Größe T10 ab und entfernen Sie die Schrauben aus den Gummifüßen.

- Befestigen Sie die Wandhalterung mittels der Schrauben aus den Gummifüßen am Gehäuse.

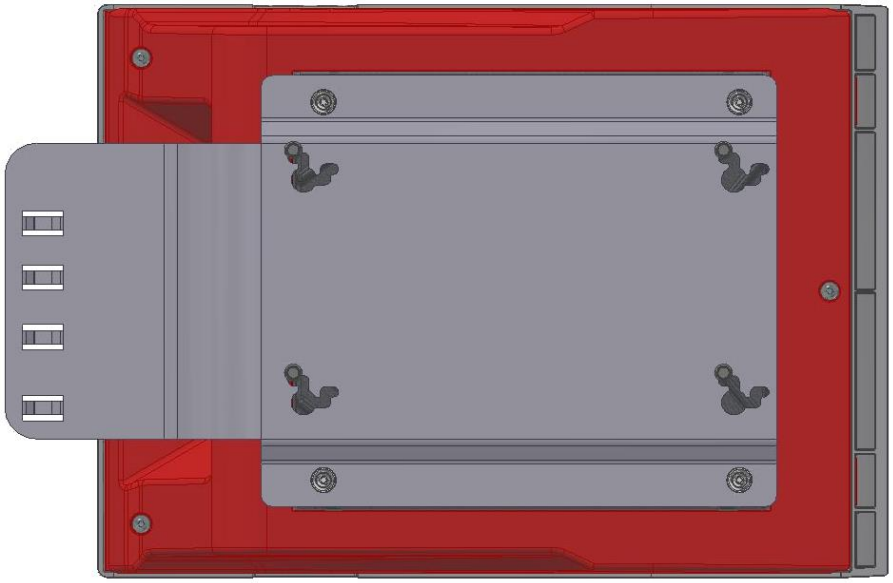


Abbildung 15: Gehäuse mit Wandhalterung

- Platzieren Sie die Montageöffnungen der Wandhalterung über den Schrauben und schieben Sie das Gerät nach unten, bis ein fester Sitz erreicht ist.

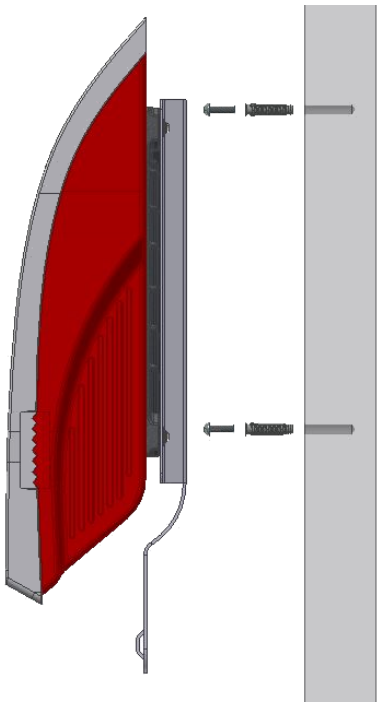


Abbildung 16: Wandmontage

4.5.3 Anschluss

- Verbinden Sie den Modularen Konnektor mit dem Netzteil und schließen Sie dieses an die Stromversorgung an (Schutzklasse 2).
- Verbinden Sie die WAN- und LAN-Anschlüsse entsprechend des geplanten Einsatzszenarios (siehe Kapitel 6.4).

Abbildung 17: Gehäuserückseite

Beachten Sie:

- **Nehmen Sie bei einer Beschädigung des Gehäuses oder des Netzteils den Modularen Konnektor bzw. das Netzteil sofort außer Betrieb.**
- **Schalten Sie den Modularen Konnektor durch die zweimalige kurze Betätigung des An/Aus-Tasters aus. Das Trennen der Spannungsversorgung im Betrieb kann das Gerät irreparabel beschädigen.**
- **Um das ausgeschaltete Gerät vom Netz zu trennen, muss der Netzstecker gezogen werden.**

Heiße Oberfläche

Verbrennungsgefahr bei Berührung im Betrieb erhitzter Gehäuseteile

Nach dem Abschalten des Geräts mindestens fünf Minuten warten, bis das Gehäuse berührt wird. Dieses gilt für den Betrieb sowohl mit wie auch ohne die optional verfügbare Wandhalterung.

5 Erstmalige Inbetriebnahme

5.1 Was Sie für die Inbetriebnahme benötigen

Stellen Sie sicher, dass für die Inbetriebnahme des Modularen Konnektors folgende Bedingungen erfüllt sind:

- Es besteht ein Internetanschluss und die erforderlichen Netzwerkkomponenten sind vorhanden (Switch).
- Wenn der Modulare Konnektor hinter einer Firewall betrieben wird, müssen folgende Ports und Protokolle freigegeben sein:
  - Ausgehend alle Ports/Protokolle
  - Eingehend UDP Port 500 und Port 4500

    Die Freigabe der eingehenden UDP Ports kann unterbleiben, wenn die Firewall des IAG die Funktion "Connection Tracking" unterstützt (siehe Kapitel 5.1.1). Dies bedeutet, dass auf Basis der vom Modularen Konnektor ausgehenden UDP Pakete die zugehörige UDP Antwort zugelassen wird. Beachten Sie die nachfolgenden Hinweise.
  - Eingehend ESP
- Eine SMC-B mit zugehöriger PIN/PUK ist vorhanden.
- Mindestens ein E-Health-Kartenterminal ist vorhanden.
- Es besteht Zugang zum VPN-Zugangsdienst (Vertragsnummer/Contract ID)
- Das Praxisverwaltungssystem ist für die Verwendung mit der TI zugelassen.
- Die aktuelle TSL und CRL zum manuellen Hochladen liegen vor.

5.1.1 Hinweise zur Verwendung der Funktion "Connection Tracking"

Wenn die Funktion "Connection Tracking" unterstützt wird, können Sie die Konfiguration auf folgende Einstellung reduzieren:

- Ausgehend alle Ports/Protokolle

Wenn Sie beabsichtigen, die Einstellungen weiter zu konkretisieren und wenn Ihr Zugangsdienstprovider die Standard Ports und Protokolle verwendet, dann kann die folgende Konfiguration angewendet werden, sofern Ihr IAG "Connection Tracking" unterstützt:

Ausgehend:

- TCPUDP: 53 (DNSSec)
- TCP: 80 (HTTP)

- TCP: 443 (HTTPS)
- UDP: 500 (IKE)
- UDP: 4500 (NAT-Traversal)
- TCP: 8443 (HTTPS)

Kann eine Verbindung nur mit der erstgenannten Konfiguration aufgebaut werden, muss ggf. noch das nachfolgende IP-Protokoll explizit freigegeben werden.

Eingehend:

- ESP

5.1.2 Empfehlungen zur Prüfung der IT-Infrastruktur

Vor der Inbetriebnahme des Modularen Konnektors ist es empfehlenswert, die Einsatzbedingungen und die vorhandene IT-Infrastruktur der Praxis zu prüfen:

- Anzahl verfügbarer Steckdosen und Netzwerksteckdosen
- Anzahl notwendiger E-Health-Kartenterminals und gSMC-KT
- Klärung von netzwerktechnischen Anforderungen und Besonderheiten im IT-Praxisbetrieb (z. B. Remote Management)
- Benötigung zusätzlicher Hardwarekomponenten
- Funktionsfähigkeit des Internetanschlusses
- Update-Status des Praxisverwaltungssystems

Um die webbasierte Bedienoberfläche des Modularen Konnektors zu benutzen, ist die Verwendung des Browsers Google Chrome ab Version 64 empfohlen. Die aktuellen Versionen für Windows-, Linux- und Mac OS-Betriebssysteme sind auf der Webseite des Herstellers verfügbar (https://www.google.de/chrome).

5.2 Geheimnis festlegen

Mithilfe des Geheimnisses kann ein alternativer Werksreset durchgeführt werden, falls das Passwort für die Anmeldung nicht mehr bekannt ist (siehe Kapitel 6.6.2).

▶ Legen Sie das Geheimnis fest. Das Geheimnis muss aus mindestens 6 Groß- oder Kleinbuchstaben bestehen.

▶ Notieren Sie das Geheimnis auf dem Sicherheitsbeiblatt *Empfang und Prüfung* und teilen Sie es dem DVO mit.

5.3 Erstanmeldung

Bei Auslieferung ist die Funktion des DHCP-Clients aktiviert, um die IP-Adresse von einem bestehenden DHCP-Server zu beziehen. Alternativ kann für den Modularen Konnektor auch eine feste IP-Adresse (192.168.210.1) mittels Werksreset Fail Safe (feste IP) vergeben werden.

Der initiale Zugriff auf die webbasierte Bedienoberfläche ist nur über die lokale Administrationsschnittstelle möglich. Die Administrationsschnittstelle wird durch eine TLS-Verbindung abgesichert und erfordert vor der Nutzung die Validierung des Zertifikats des Modularen Konnektors.

5.3.1 Erstanmeldung mit fester IP-Adresse

- Verbinden Sie den Modularen Konnektor mit dem Netzteil und schließen Sie dieses an die Stromversorgung an.
- Schließen Sie den Modularen Konnektor über einen Switch an ein Netzwerk an und verbinden Sie anschließend auch das Clientsystem mit dem Switch.
- Führen Sie einen Werksreset Fail Safe (feste IP) durch (siehe Kapitel 6.8).
- Geben Sie nach einem erfolgreich durchgeführten Werksreset Fail Safe (feste IP) am Clientsystem in der Adresszeile des Browsers folgende Adresse ein:

  ```
  https:// 192.168.210.1:8500/management
  ```

- Fahren Sie danach wie im Kapitel 5.3.2 (Erstanmeldung mittels DHCP-Server) ab dem Schritt „Validieren Sie das Zertifikat des Modularen Konnektors.“ fort.

5.3.2 Erstanmeldung mittels DHCP-Server

- Verbinden Sie den Modularen Konnektor mit dem Netzteil und schließen Sie dieses an die Stromversorgung an.
- Schließen Sie den Modularen Konnektor über einen Switch an ein Netzwerk an, das über einen DHCP-Server verfügt. Verbinden Sie anschließend auch das Clientsystem mit dem Switch.
- Schalten Sie den Modularen Konnektor ein, indem Sie die Ein/Aus-Taste kurz drücken.

  Die Betriebsanzeigen leuchten auf und das Gerät startet. Wenn die Anzeige SYSTEM dauerhaft leuchtet, ist der Modulare Konnektor betriebsbereit. Eine

Übersicht der Anzeigen beim Systemstart und möglicher Fehleranzeigen finden Sie in Kapitel 3.1.1.2.

Bei Auslieferung ist die Funktion des DHCP-Clients aktiviert, um die Adresse von einem bestehenden DHCP-Server zu beziehen. Wenn kein DHCP-Server erreichbar ist (beispielsweise wenn die LAN-Schnittstelle nicht angeschlossen ist), wird nach ca. 60 Sekunden die erste freie IP-Adresse aus dem Link Local Adressbereich `169.254.0.0/16` zugewiesen (z.B. `169.254.0.1`). Nach erfolgreich abgeschlossener Erstanmeldung können Sie dem Modularen Konnektor bei Bedarf auch eine feste IP-Adresse manuell zuweisen (siehe Kapitel 6.2.2.2)

- Geben Sie am Clientsystem in der Adresszeile des Browsers unter Verwendung der dem Modularen Konnektor zugewiesenen IP-Adresse folgende Adresse ein:

```
https://<IP-Adresse des Modularen Konnektors>:8500/management
```

- Validieren Sie das Zertifikat des Modularen Konnektors.

  Exportieren Sie dazu das Zertifikat (siehe Kapitel 5.3.3) und importieren Sie es im Browser (siehe Kapitel 5.3.4).

Vor der Validierung des Konnektor-Zertifikates dürfen keine Zugangsdaten an der Administrationsschnittstelle eingegeben werden.

- Rufen Sie die Bedienoberfläche erneut auf.

Abbildung 18: Anmeldedialog

- Melden Sie sich mit folgenden initialen Zugangsdaten an:

Benutzername:	`super`
Passwort:	`konnektor`

Sie werden aufgefordert, ein neues Passwort einzugeben.

Falls Sie bei der ersten Anmeldung nicht zum Passwortwechsel aufgefordert werden, darf der Modulare Konnektor nicht in Betrieb genommen werden. Es besteht die Gefahr einer möglichen Kompromittierung. Beachten Sie in diesem Fall die Hinweise in Kapitel 9.

- Geben Sie ein neues Passwort ein. Beachten Sie die Hinweise zu Passwörtern in Kapitel 4.2.

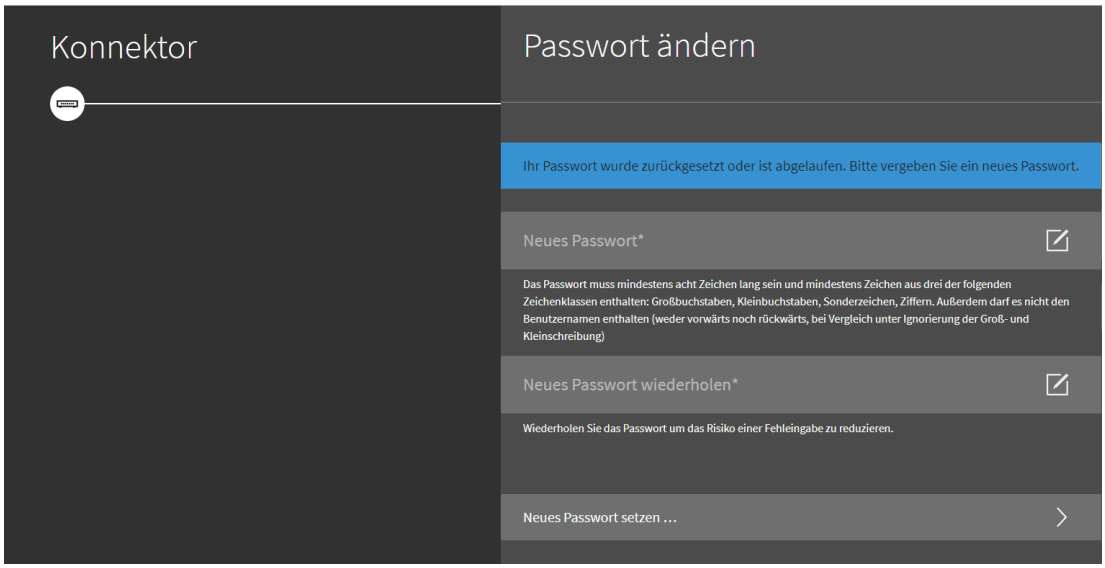


Abbildung 19: Passwort ändern

- Klicken Sie **Neues Passwort setzen**.

  Das neue Passwort wird dadurch gültig und die Ansicht **Home** wird angezeigt.

  Das initiale Benutzerkonto besitzt die Benutzerrolle *Super-Admin*. Sie haben damit Zugriff auf alle Konfigurationsdaten und Benutzerkonten.

Prüfen Sie bei der Inbetriebnahme die Systemzeit (siehe Kapitel 6.2.5.3) und passen Sie sie wenn notwendig an.

5.3.3 TLS-Zertifikat exportieren

Die Administrationsschnittstelle zum Modularen Konnektor wird über eine TLS-Verbindung abgesichert. Beim TLS-Verbindungsaufbau wird für die Authentisierung des Konnektors ein TLS-Zertifikat verwendet, das im Modularen Konnektor hinterlegt ist. Um sicherzustellen, dass bei der initialen und allen weiteren Verbindungan-fragen zum Modularen Konnektor das korrekte Zertifikat verwendet wird, muss eine Validierung des Konnektor-Zertifikates durchgeführt werden.

Erst nach der Validierung authentisiert sich der Administrator durch die Eingabe von Zugangsdaten an der Administrationsschnittstelle.

Wenn die Validierung des Konnektor-Zertifikates nicht durchgeführt wird, kann der Schutz von sensiblen Informationen wie Zugangsdaten nicht sichergestellt werden.

Gehen Sie wie folgt vor, um das TLS-Zertifikat des Modularen Konnektors zu exportieren:

- Falls nicht bereits geschehen, verbinden Sie sich wie in der Erstanmeldung beschrieben mit dem Modularen Konnektor und rufen Sie die Bedienoberfläche auf (siehe Kapitel 5.3). Es sollte nun eine entsprechende Fehlermeldung im Browser angezeigt werden:

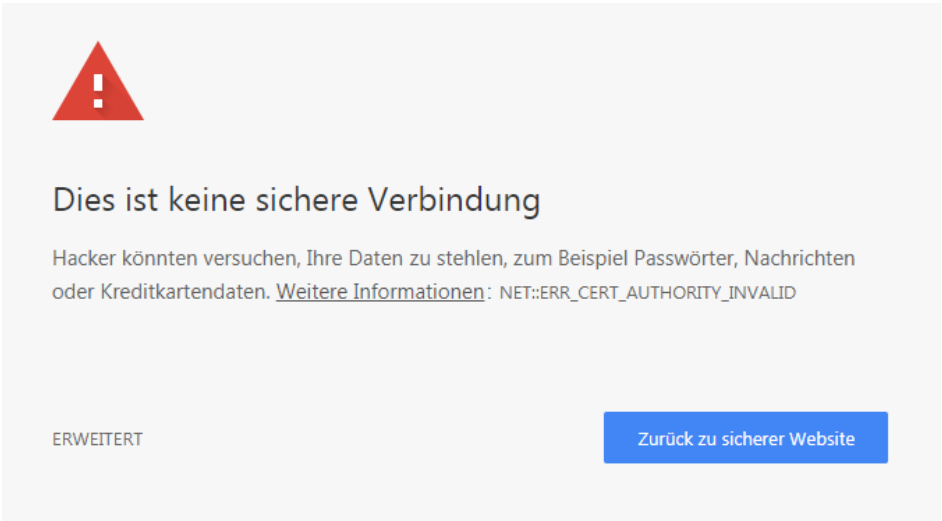


Abbildung 20: Zertifikatsfehler (Beispiel)

- Neben der Adresszeile wird ein Warnsymbol mit dem Text **Nicht sicher** angezeigt. Klicken Sie darauf, um Verbindungsinformationen einzublenden.

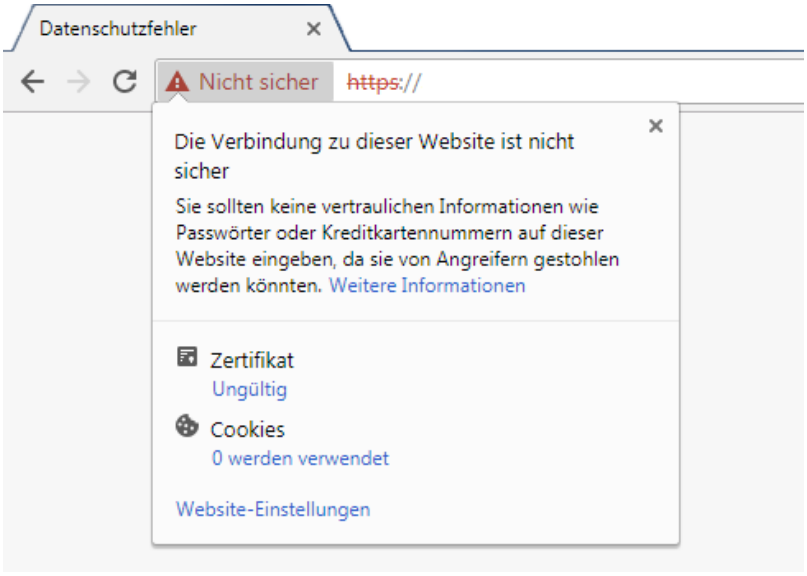


Abbildung 21: Informationen zu unsicherer Verbindung (Beispiel)

- Klicken Sie unter **Zertifikat** auf **Ungültig**, um weitere Informationen anzuzeigen.

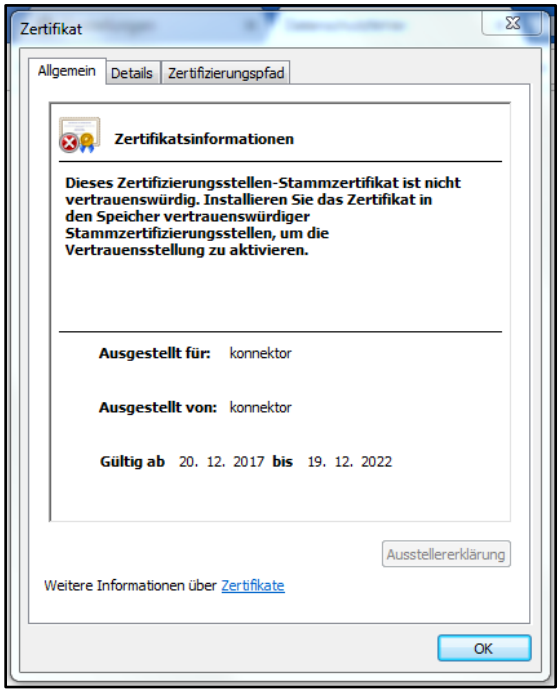


Abbildung 22: Zertifikatsinformationen

- Öffnen Sie den Reiter **Details**, um weitere Informationen über das Zertifikat wie beispielsweise den Fingerprint anzuzeigen.

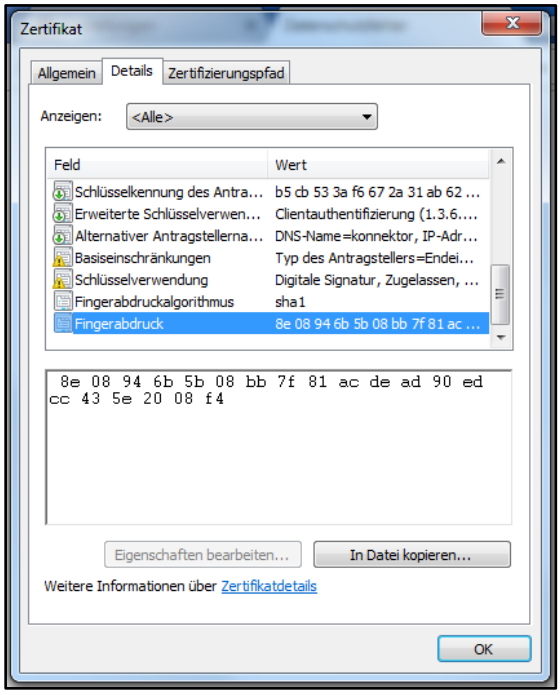


Abbildung 23: Zertifikatsdetails (Beispiel)

- Klicken Sie **In Datei kopieren …**, um das Zertifikat zu exportieren. Der Zertifikatexport-Assistent öffnet sich.

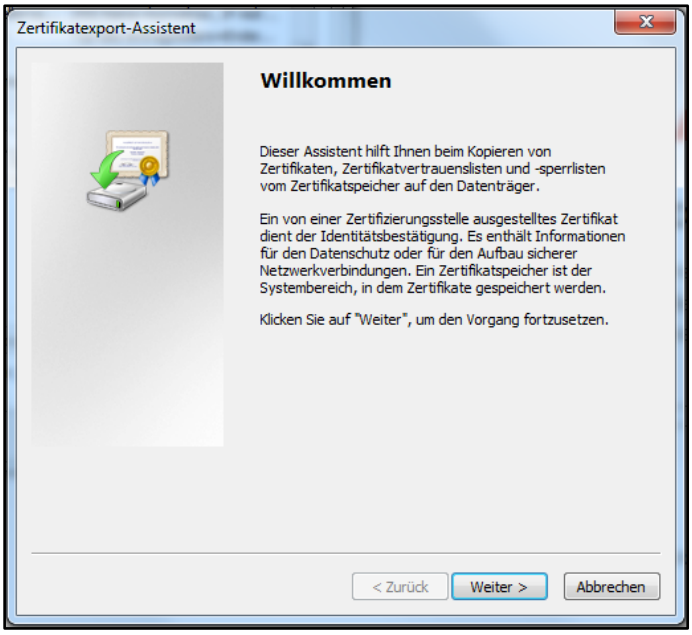


Abbildung 24: Zertifikatexport-Assistent

- Wählen Sie das Format **DER-codiert-binär X.509 (.CER)**.

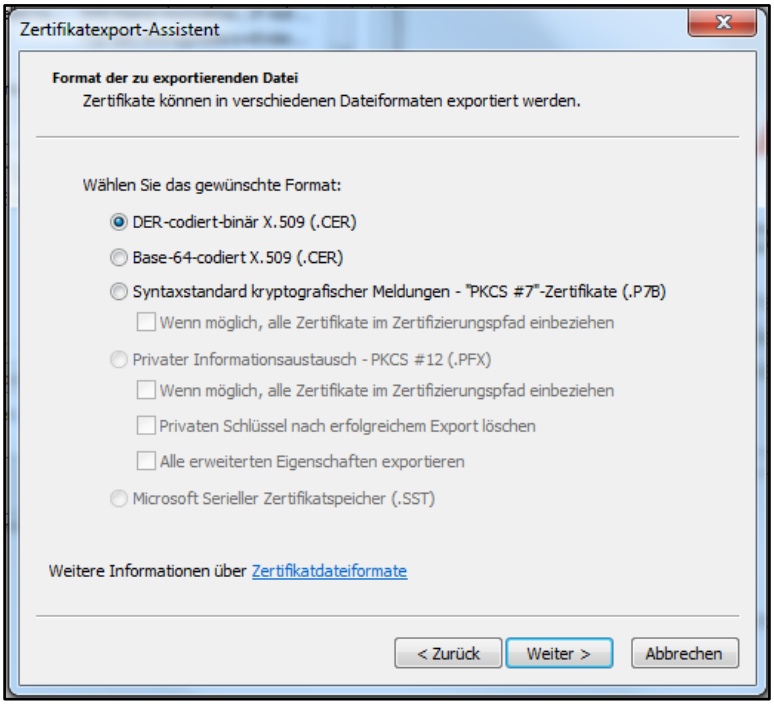


Abbildung 25: Zertifikatsformat

- Folgen Sie den Anweisungen des Zertifikatexport-Assistenten, um das Zertifikat in einer Datei abzuspeichern.

5.3.4 TLS-Zertifikat importieren und validieren

Das gespeicherte Zertifikat des Modularen Konnektors muss nun in den Browsern der Clientsysteme importiert werden.

Gehen Sie wie folgt vor, um das Zertifikat in einem Browser zu importieren:

- Klicken Sie das Menü-Symbol ⋮ rechts neben der Adressleiste, um weitere Optionen anzuzeigen.

- Klicken Sie **Einstellungen**.

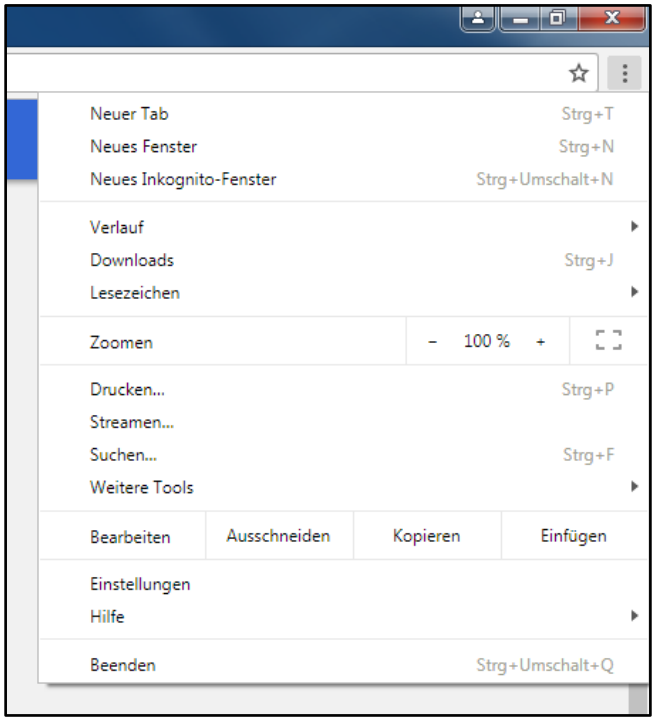


Abbildung 26: Browser-Einstellungen

- Klicken Sie am unteren Bildschirmrand **Erweitert**, um alle Einstellungen einzublenden.
- Klicken Sie **Zertifikate verwalten**.

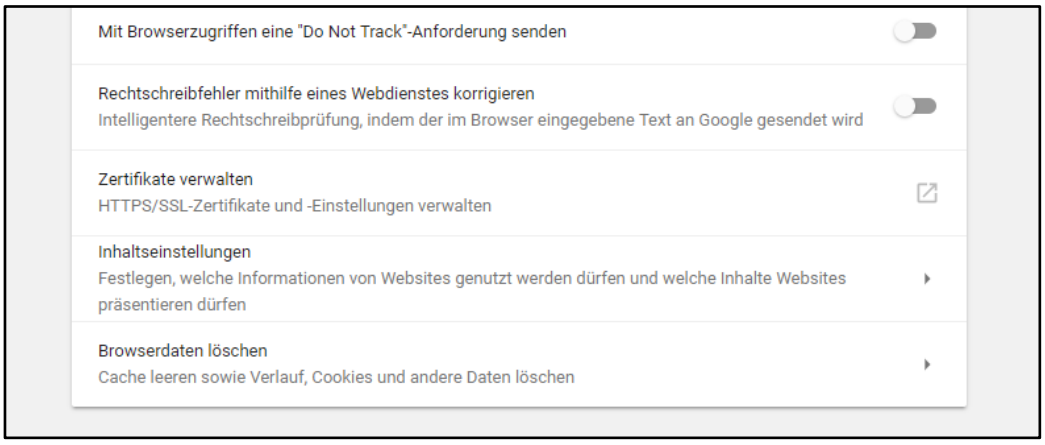


Abbildung 27: Zertifikate verwalten

Das Fenster **Zertifikate** öffnet sich, in dem alle bereits importierten Zertifikate angezeigt werden.

- Öffnen Sie den Reiter **Vertrauenswürdige Stammzertifizierungsstellen** und klicken Sie **Importieren …**

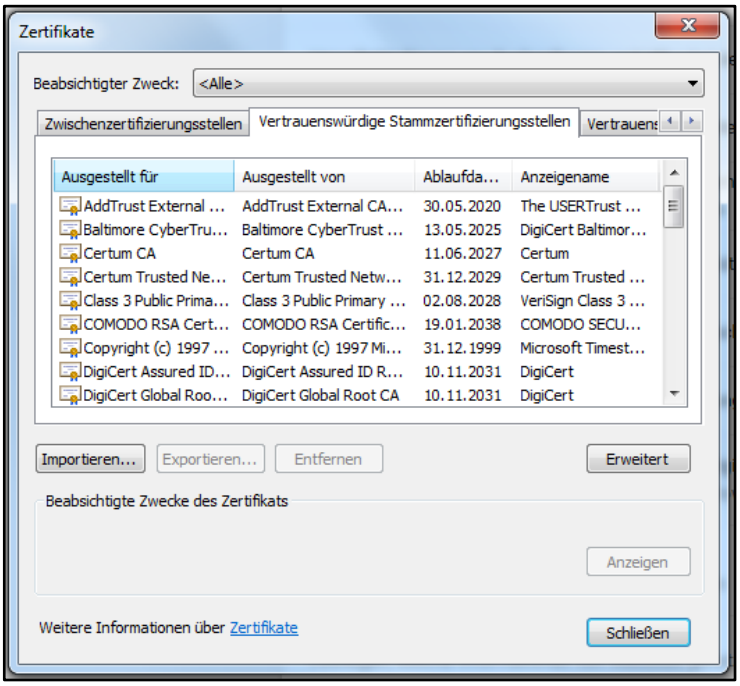


Abbildung 28: Importierte Zertifikate (Beispiel)

Der Zertifikatimport-Assistent öffnet sich:

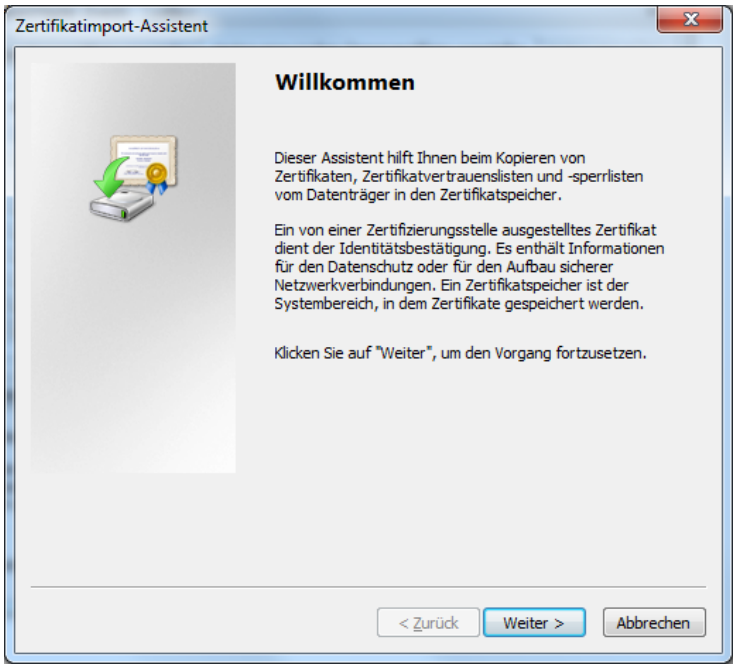


Abbildung 29: Zertifikatimport-Assistent

- Folgen Sie den Anweisungen des Zertifikatimport-Assistenten und wählen Sie die abgespeicherte Datei mit dem Zertifikat des Modularen Konnektors aus.

- Wählen Sie als Zertifikatsspeicher **Vertrauenswürdige Stammzertifizierungs-stellen** aus und schließen sie den Import ab.

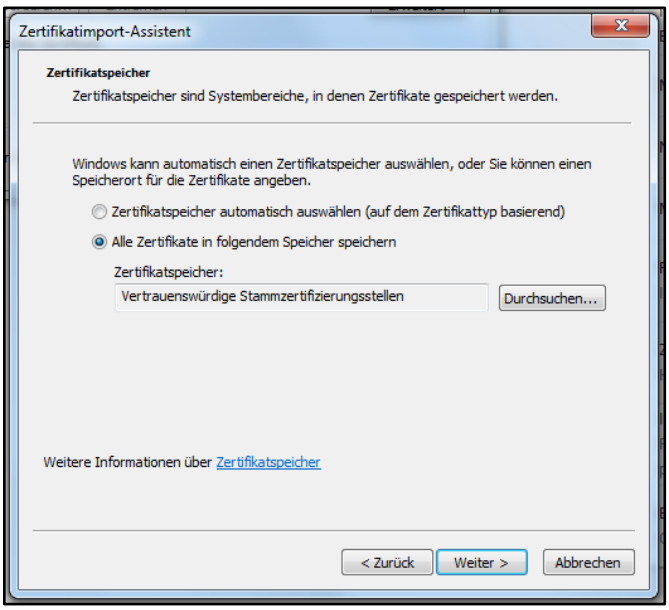


Abbildung 30: Zertifikatsspeicher

- Es wird nun eine Sicherheitswarnung angezeigt. Bestätigen Sie, dass Sie dieses Zertifikat installieren möchten.

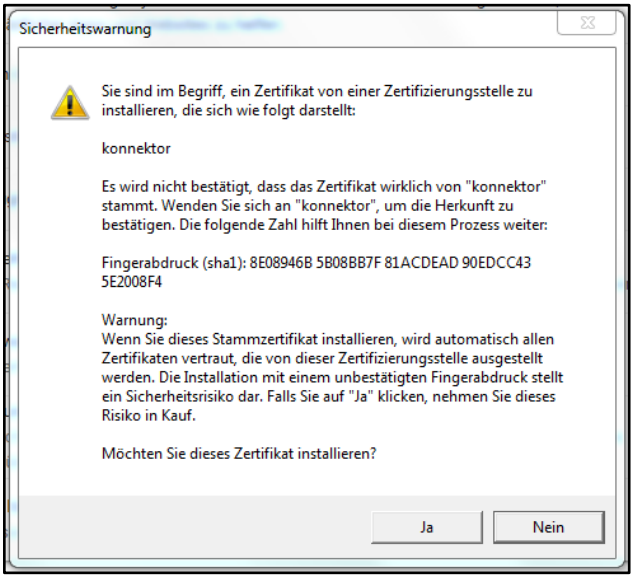


Abbildung 31: Sicherheitswarnung bei Import

- In den Browser-Einstellungen unter **Zertifikate verwalten** können Sie nun im Reiter **Vertrauenswürdige Stammzertifizierungsstellen** das Zertifikat des Modularen Konnektors einsehen.

- Wählen Sie das Zertifikat aus und klicken Sie **Anzeigen**, um weitere Informationen zum Zertifikat anzuzeigen. Hier können Sie im Reiter **Details** zum Abgleich auch den Fingerprint anzeigen (siehe nachfolgend).

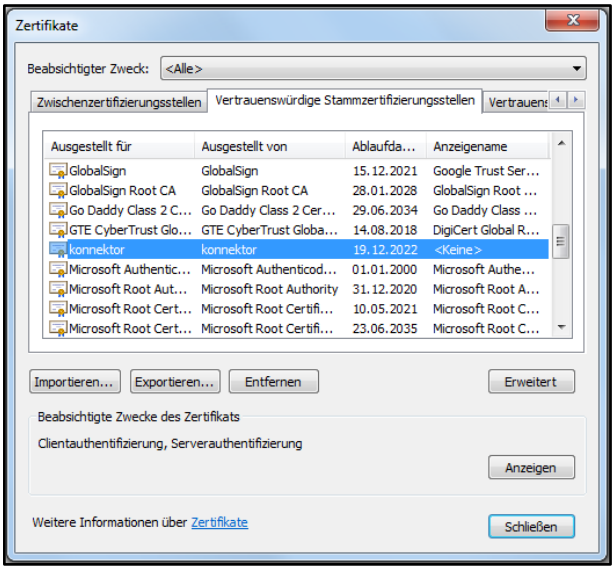


Abbildung 32: Importiertes Zertifikat des Modularen Konnektors

- Starten Sie den Browser neu.

  Das Zertifikat ist nun validiert und Sie können sich an der Bedienoberfläche des Modularen Konnektors anmelden.

Sobald Sie einmal das Zertifikat in einem Clientsystem importiert haben, können Sie die Zertifikatsvalidierung für weitere Clientsysteme im lokalen Netzwerk anhand des exportierten Zertifikats durchführen, ohne eine direkte Verbindung zwischen dem Clientsystem und dem Modularem Konnektor aufzubauen. In diesem Fall müssen Sie sicherstellen, dass das importierte Zertifikat jeweils mit dem bereits validierten Zertifikat übereinstimmt, z. B. über einen Vergleich des Fingerprints der Zertifikate.

- Führen Sie dazu für das Clientsystem die oben beschriebenen Schritte durch und vergleichen Sie den Fingerprint mit dem eines bereits validierten Zertifikats.

Falls nach der Validierung des Zertifikates des Modularen Konnektors im Browser weiterhin eine Sicherheitswarnung entsprechend Abbildung 20 angezeigt wird, vergleichen Sie wie oben beschrieben den Fingerprint des für die aktuelle Verbindung verwendeten Zertifikates mit dem eines bereits validierten Zertifikates. Wenn der Fingerprint übereinstimmt, wenden Sie

sich an den DVO.

Falls Sie Remote Management zulassen wollen, muss das Zertifikat des Modularen Konnektors im Clientsystem des Remote-Administrators importiert werden. Führen Sie dazu die oben beschriebenen Schritte im Browser des Remote Management-Systems durch und melden Sie sich dabei mit der Adresse für Remote Management an (siehe Kapitel 6.1.1).

Nach dem Import des Zertifikats des Modularen Konnektors muss der Remote-Administrator zwecks Validierung den im Browser angezeigten Fingerprint des importierten Zertifikats mit einem geeigneten Werkzeug gegenprüfen. Danach muss der Fingerprint des importierten Zertifikats mit dem eines bereits validierten Zertifikats abgeglichen werden. Dies kann zum Beispiel telefonisch zwischen Lokalem Administrator und Remote-Administrator erfolgen.

Die Remote Management Schnittstelle darf erst nach erfolgreichem Fingerprint-Abgleich verwendet werden.

5.4 Vorgehensweise bei der ersten Konfiguration

Die Konfiguration des Modularen Konnektors ist in Kapitel 6 beschrieben. Dort finden Sie auch Hinweise zum Betrieb in verschiedenen Netzwerkszenarien.

Passen Sie die Konfiguration in folgender Reihenfolge an:

1. Prüfen Sie die Systemzeit (siehe Kapitel 6.2.5.3).
2. Legen Sie im Menü **System** die grundlegenden Betriebsbedingungen fest (siehe Kapitel 6.2.5).
3. Legen Sie Benutzer für die Personen an, die den Modularen Konnektor über die Bedienoberfläche administrieren (siehe Kapitel 6.2.1).

   Falls die Administration mit Remote Management erfolgen soll, ist hierfür ein eigener Benutzer mit der Rolle **Remote-Admin** erforderlich.
4. Aktivieren Sie bei Bedarf die Remote Management-Schnittstelle (siehe Kapitel 6.2.5.1).
5. Konfigurieren Sie die Netzwerkschnittstellen und Dienste für die Anbindung an das lokale Netzwerk und nach Bedarf den IAG (siehe Kapitel 6.2.2 und 6.2.5). Die WAN-Schnittstelle ist im Auslieferungszustand deaktiviert und muss bei Bedarf manuell aktiviert werden (siehe Kapitel 6.2.2.3).
6. Verbinden Sie die Kartenterminals des lokalen Netzwerks (siehe Kapitel 6.3).
7. Legen Sie die weiteren Komponenten der Betriebsumgebung, wie Mandanten, Arbeitsplätze und Clientsysteme an (siehe Kapitel 6.2.3).

   Erstellen Sie für den Zugriff der Fachmodule auf die TI Aufrufkontexte.
8. Prüfung der bei der Produktion installierten TSL und CRL. Aufgrund der begrenzten zeitlichen Gültigkeit von TSL bzw. CRL sowie den durch Produktion und Transport gegebenen Zeiträumen kann es dazu kommen, dass die in der Produktion eingebrachten TSL und CRL nicht mehr gültig sind. Bei Bedarf können Sie eine TSL oder CRL über die Managementschnittstelle hochladen. Im Menü **System** können Sie im Bereich **Zertifikate** das jeweilige Ablaufdatum anzeigen lassen sowie eine TSL oder CRL hochladen (siehe Kapitel 6.2.5.2).

   URL für den Abruf der aktuellen TSL (Achtung: Nur bei Einsatz im Online-Rollout):

   ```
   https://download.tsl.ti-dienste.de/TSL.xml
   ```

URL für den Abruf der aktuellen CRL (Achtung: Nur bei Einsatz im Online-Rollout):

```
http://download.crl.ti-dienste.de/crl/vpnk-ca1.crl
```

9. Konfigurieren sie nach Bedarf die Verbindungen mit dem VPN-Zugangsdienst von TI und SIS (siehe Kapitel 6.2.6).

   Eine Liste der zugelassenen VPN-Zugangsdienste ist auf der Webseite der gematik verfügbar.

10. Konfigurieren Sie nach Bedarf die Fachmodule (siehe Kapitel 6.2.7).

11. Stellen Sie nach Abschluss der Konfiguration die Verkabelung des LAN-Anschlusses entsprechend des geplanten Einsatzszenarios her.

6 Die Bedienoberfläche des Modularen Konnektors

Alternativ zur Bedienoberfläche kann der Modulare Konnektor auch über die REST-Schnittstelle administriert werden. Zur sicheren Administration des Modularen Konnektors über die REST-Schnittstelle benötigen Sie eine zugehörige Spezifikation. Bitte wenden Sie sich an den Hersteller. Dieser stellt Ihnen die Spezifikation zur Verfügung.

6.1 Grundlagen zur Bedienung der Bedienoberfläche

Der Modulare Konnektor wird über eine webbasierte Bedienoberfläche konfiguriert, die Sie im Browser aufrufen können. Beachten Sie die Hinweise zu empfohlenen Browsern in Kapitel 5.1.

6.1.1 An- und Abmeldung

Sie benötigen für die Anmeldung einen unterstützten Browser.

- Geben Sie in der Adresszeile des Browsers folgende Adresse ein:

```
https://<IP-Adresse des Modularen Konnektors>:8500/management
```

- Geben Sie Ihre Zugangsdaten ein und klicken Sie **Login**.

Abbildung 33: Anmeldebildschirm

Tipp

Erstellen Sie für den wiederholten Aufruf ein Lesezeichen.

Falls Sie sich nicht anmelden können, weil das Passwort nicht mehr bekannt ist, besteht die Möglichkeit unter **Weitere Optionen anzeigen …** einen alternativen Login durchzuführen (siehe Kapitel 6.6.2).

Abmeldung

- Melden Sie sich über die Schaltfläche ⓐ im linken unteren Bildschirmbereich ab.

Bei 15-minütiger Inaktivität werden Sie automatisch abgemeldet.

Loggen Sie sich manuell über die Schaltfläche aus, wenn die Administrationstätigkeiten beendet sind.

6.1.2 Die Ansicht „Home“

Nach der Anmeldung wird die Ansicht **Home** angezeigt.

Abbildung 34: Ansicht „Home“

In der Ansicht **Home** wird im linken Fensterbereich angezeigt:

- Verbindungsstatus von TI und SIS
- Meldungen des Typs SECURITY mit dem Level FATAL anzeigen, die seit dem letzten Ausloggen des aktuellen Administrators ausgegeben wurden (siehe Kapitel 12.3).

Klicken Sie auf die mit 🔗 gekennzeichneten Schaltflächen, um weitere Informationen in den verknüpften Dialogfenstern anzuzeigen.

In den Menüs konfigurieren Sie die Einstellungen für den Betrieb und die Wartung des Modularen Konnektors. Die Namen der Menüs in der seitlichen Menüleiste können Sie über Ihre Profileinstellungen ein- und ausblenden (siehe Kapitel 6.2.1.1).

Home

Zur Ansicht **Home** zurückkehren.

Benutzer

In diesem Menü können Sie Ihr Profil einsehen, sich abmelden und die Administratoren des Modularen Konnektors verwalten (siehe Kapitel 6.2.1).

Netzwerk

In diesem Menü konfigurieren Sie die Netzwerkschnittstellen und Netzwerkdienste (siehe Kapitel 6.2.2).

Praxis

In diesem Menü verwalten Sie Clientsysteme, Mandanten, Arbeitsplätze, Karten und Terminals (siehe Kapitel 6.2.3).

Diagnose

In diesem Menü haben Sie Zugriff auf Meldungen (siehe Kapitel 6.2.4).

System

In diesem Menü treffen Sie allgemeine Einstellungen zum System und verwalten Backups (siehe Kapitel 6.2.5).

VPN

In diesem Menü konfigurieren Sie die Anbindung an die TI und den SIS (siehe Kapitel 6.2.6).

Fachmodule

In diesem Menü verwalten Sie die auf dem Modularen Konnektor betriebenen Fachanwendungen (siehe Kapitel 6.2.7).

6.1.3 In der Bedienoberfläche navigieren

In den Dialogfenstern der Bedienoberfläche navigieren Sie mit folgenden Symbolen:

Zurück

Löschen

Abbrechen (Eingabe verwerfen)

Bestätigen

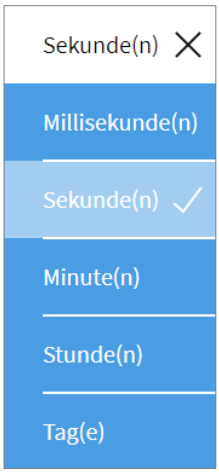
Eingabe in untergeordnetem Formular abschließen; Beachten Sie: Die Eingaben werden erst durch nochmaliges bestätigen mit ✓ gespeichert.

Hinzufügen

Eingabe (Texteingabefelder können auch direkt angeklickt werden)

Auswahlliste Expandieren

Sie können einen der angezeigten Werte wählen, wobei der aktuell gewählte Wert hervorgehoben ist (Beispiel):



···	Führt zu weiteren Einstellungen
	Verknüpfung anderem Oberflächen-Dialogfenster, beispielsweise bei Statusanzeigen in der Ansicht **Home**.

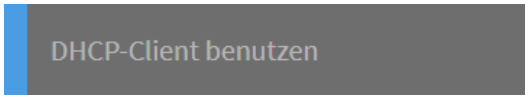
Lade-/Warteanzeigen:

	Seite lädt
	Aktion wird durchgeführt

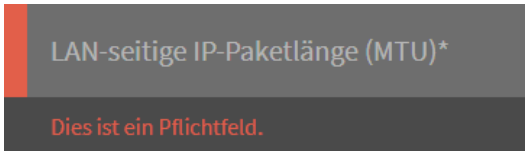
6.1.3.1 Die Prüfung von Eingaben

Wenn in einem Dialogfenster eine konfigurierte Einstellung verändert wird, wird die Validität automatisch geprüft und über Farbbalken vor dem Eingabefeld angezeigt:

Blau Eingabe gültig



Rot Eingabe nicht gültig, es wird zusätzlich ein Fehlertext angezeigt



6.1.3.2 Warnungen und Hinweise

Wenn Einstellungen vorgenommen werden, die Auswirkungen auf den Betrieb haben (z.B. Neustart oder Werksreset) oder wenn Elemente gelöscht werden (z.B. Mandanten oder Benutzer), wird ein Warnhinweis angezeigt. Bestätigen Sie diesen, um die Aktion durchzuführen.

Wichtige Informationen zum Status und aktuellen Vorgängen (z.B. eine fehlende Verbindung zur TI oder dem Herunterfahren des Modularen Konnektors) werden in einem farbigen Hinweis am oberen Bildschirmrand angezeigt.

6.2 Übersicht der Menüs und Einstellungen

Nachfolgend sind die einzelnen Einstellungen zum Konfigurieren des Modularen Konnektors beschrieben.

Standardwerte und Wertebereiche für die einzelnen Konfigurationsparameter finden sie in Kapitel 12.2.

Die Konfiguration beispielhafter Netzwerkszenarien ist in Kapitel 6.4 beschrieben.

6.2.1 Das Menü „Benutzer“

Im Menü **Benutzer** verwalten Sie die Benutzerkonten der Administratoren des Modularen Konnektors.

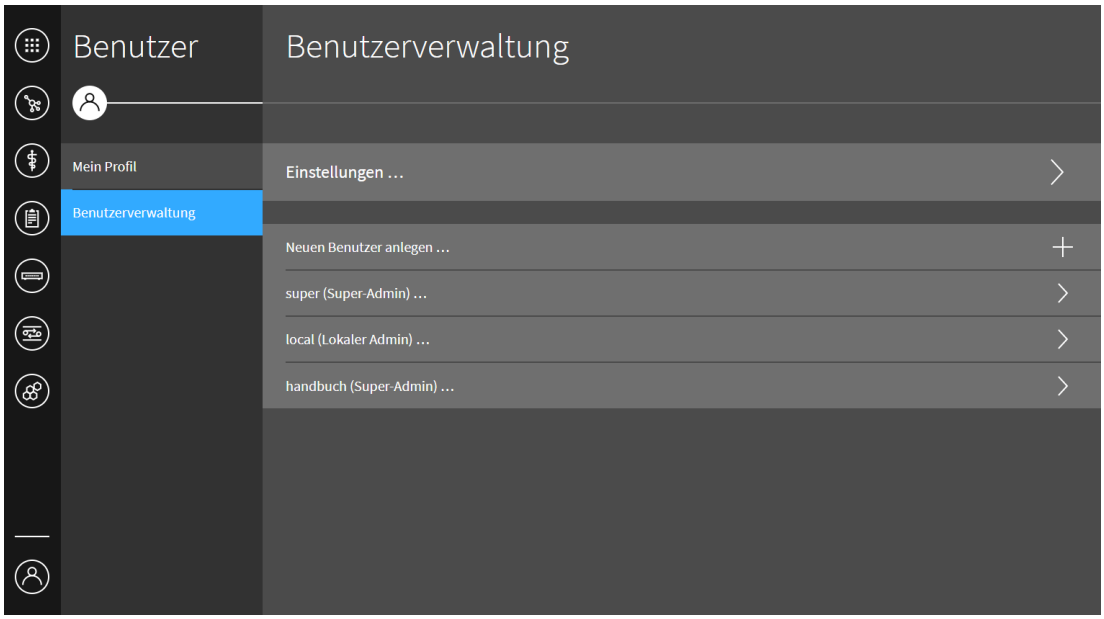


Abbildung 35: Menü „Benutzer“

6.2.1.1 Bereich „Mein Profil“

In diesem Bereich können Sie Ihre eigenen Benutzerdaten anpassen und Ihr Passwort ändern.

Mit der Einstellung **Beschrifte Apps in Seitenleiste** können Sie in der seitlichen Menüleiste die Namen der Menüs ein- und ausblenden.

6.2.1.2 Bereich „Benutzerverwaltung“

Sie haben folgende Möglichkeiten:

- Unter **Einstellungen ...** legen Sie fest, nach welchem Zeitintervall Passwörter geändert werden müssen.
- Mit **Neuen Benutzer anlegen ...** legen Sie ein Benutzerkonto an.

  Für ein neues Benutzerkonto müssen der Benutzername und das initiale Passwort eingegeben sowie eine Benutzerrolle ausgewählt werden (siehe Kapitel 6.2.1.3). Beachten sie die Hinweise zu Passwörtern in Kapitel 4.2.

Wählen Sie geeignete Benutzernamen.

Benutzernamen sind so zu wählen, dass sie im Hinblick auf die zuzuordnende Rolle nicht irreführend sind. So sollte z.B. der Benutzername nicht „Remote-Administrator“ lauten, wenn dem Benutzer die Rolle „Super-Administrator“ zugwiesen werden soll.

Optional können weitere persönliche Daten eingegeben werden:

- Vor- und Nachname
- Institution
- E-Mail-Adresse
- Telefonnummer

Halten Sie Passwörter stets geheim.

- **Passwörter dürfen nicht schriftlich aufbewahrt werden.**
- **Passwörter dürfen nicht an Dritte weitergegeben werden. Ausnahme sind die initialen Passwörter von Remote-Administratoren. Diese dürfen nur an die vom Leistungserbringer beauftragten Remote-Administratoren persönlich weitergegeben werden.**

- Wenn Sie ein bestehendes Benutzerkonto anklicken, haben Sie folgende Möglichkeiten:
  - Wählen Sie **Benutzer bearbeiten** um dessen Einstellungen zu ändern.
  - Klicken Sie auf 🗑 um das Benutzerkonto zu entfernen.

6.2.1.3 Überblick über Benutzerrollen

Die Benutzerkonten von Administratoren können folgende Rollen besitzen:

- Super-Admin
- Lokaler Admin
- Remote-Admin

Mit den Benutzerrollen sind folgende Berechtigungen verbunden:

	Super-Admin	Lokaler Admin	Remote-Admin
Lokaler Administrationszugriff (siehe Kapitel 6.1.1)	Ja	Ja	Nein
Administrationszugriff über Remote Management	Nein	Nein	Ja
Werksreset durchführen (siehe Kapitel 6.6)	Ja	Ja	Nein
Werksreset zum Versand durchführen (siehe Kapitel 6.7)	Ja	Ja	Nein
Verwaltung von Benutzerkonten (siehe Kapitel 6.2.1.2)	Ja	Nein	Nein
Passwörter zurücksetzen (siehe Kapitel 6.2.1.4)	Ja	Nein	Nein
Zeitintervall für den Passwortwechsel konfigurieren (siehe Kapitel 6.2.1.2)	Ja	Nein	Nein
Backup exportieren (siehe Kapitel 6.2.5.5)	Ja	Ja	Ja
Backup importieren (siehe Kapitel 6.2.5.5)	Ja	Nein	Nein
Remote Management initialisieren (siehe Kapitel 6.2.5.1, Einstellung „Remote-Management aktivieren“)	Ja	Ja	Nein
Remote Mangement konfigurieren (siehe Kapitel 6.2.5.1, Einstellung „Remote-Management erlauben“)	Ja	Nein	Nein
Verwaltung aller übrigen Konfigurationsdaten	Ja	Ja	Ja

Tabelle 10: Berechtigungen der Benutzerrollen

6.2.1.4 Passwort eines Benutzers zurücksetzen

- Wählen Sie im Bereich **Benutzerverwaltung** das gewünschte Konto und Klicken Sie **Benutzer bearbeiten**.
- Geben Sie in den Felder **Passwort** und **Passwort wiederholen** ein neues initiales Passwort ein. Der Benutzer wird beim nächsten Einloggen mit dem initialen Passwort automatisch aufgefordert, ein neues Passwort einzugeben.

6.2.2 Das Menü „Netzwerk“

Im Menü **Netzwerk** konfigurieren Sie die LAN- und WAN-Schnittstellen und Einstellung zur Netzwerk-Funktionalität, um den Modularen Konnektor in die Netzwerkumgebung einzubinden.

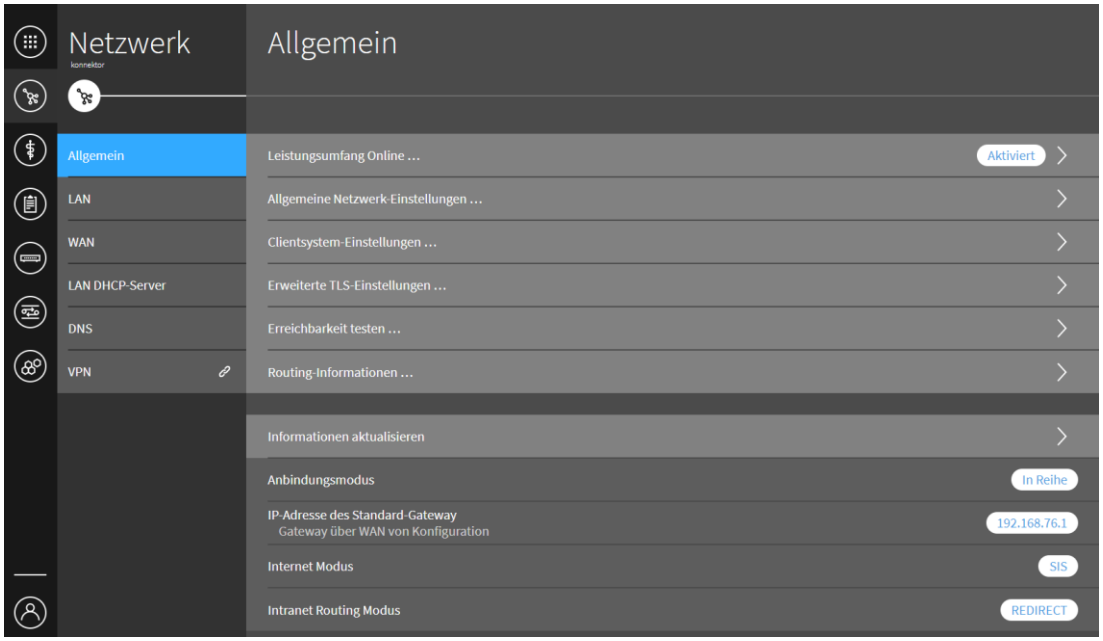


Abbildung 36: Menü „Netzwerk“

6.2.2.1 Bereich „Allgemein“

Im Bereich **Allgemein** konfigurieren Sie die Funktionalität des Modularen Konnektors im Netzwerk. Im unteren Fensterbereich werden Informationen zum Anbindungsmodus und der IP-Adresse des Standard-Gateways angezeigt.

- Unter **Leistungsumfang …** legen Sie fest, ob der Modulare Konnektor online oder offline betrieben wird (siehe Kapitel 6.4.1.1).
- Unter **Allgemeine Netzwerk-Einstellungen …** legen sie ggf. den Internetmodus (siehe Kapitel 6.4.1.3) und weitere Netzwerkeinstellungen fest.
- Unter **Clientsystem-Einstellungen …** legen Sie Einstellungen zur Verbindung mit Clientsystemen konfiguriert werden:

  Für die Kommunikation von Clientsystemen mit dem Modularen Konnektor können folgende Einstellungen konfiguriert werden:

  - Die Authentifizierungsmethode
  - Die Absicherung der Verbindung mit TLS (siehe Kapitel 6.5).
  - Der Zugriff auf den Dienstverzeichnisdienst

Für die Kommunikation vom Modularen Konnektor mit Clientsystemen können folgende Einstellungen konfiguriert werden:

- Die Authentifizierungsmethode
- Die maximale Anzahl der fehlgeschlagenen Kontaktversuche, nach der ein Clientsystem getrennt wird.

- Unter **Erweiterte TLS-Einstellungen …** konfigurieren Sie Einstellungen zum Transport Layer Security Protokoll (TLS).
- Mit **Erreichbarkeit Testen …** prüfen Sie die Verbindung zu einem System im lokalen Netzwerk.
- Unter **Routing Informationen …** werden Informationen zum Routing im lokalen Netzwerk angezeigt.

6.2.2.2 Bereich „LAN“

Im Bereich **LAN** konfigurieren sie die Schnittstelle zum lokalen Netzwerk.

Sie haben folgende Möglichkeiten:

- Unter **Einstellung …** kann die LAN-Schnittstelle konfiguriert werden.

  Bei Auslieferung ist die Funktion des DHCP-Clients aktiviert, um die Adresse von einem bestehenden DHCP-Server zu beziehen. Wenn kein DHCP-Server erreichbar ist (beispielsweise wenn das LAN-Interface nicht angeschlossen ist), wird nach ca. 60 Sekunden die erste freie IP-Adresse aus dem Link Local Adressbereich `169.254.0.0/16` zugewiesen (z.B. `169.254.0.1`). Alternativ können Sie eine IP-Adresse manuell festlegen.

  Unter **Weitere Parameter** können IP, UDP und TCP-Parameter als Schlüssel/ Wertpaare angegeben werden.

- Wenn der Modularen Konnektor im lokalen Netzwerk als DHCP-Client betrieben wird, kann mit **DHCP-Client Lease erneuern …** eine neue IP-Adresse vom DHCP-Server angefordert werden.

6.2.2.3 Bereich „WAN“

Im Bereich **WAN** konfigurieren Sie die Schnittstelle zum Internet Access Gateway (IAG) wenn der Modulare Konnektor im Anbindungsmodus *In Reihe* betrieben wird (siehe Kapitel 6.4.1.2). Die WAN-Schnittstelle ist im Auslieferungszustand deaktiviert und muss bei Bedarf manuell aktiviert werden.

Sie haben folgende Möglichkeiten:

- Unter **Einstellung …** kann die WAN-Schnittstelle konfiguriert werden.

  Legen Sie entweder eine IP-Adresse fest oder aktivieren Sie **DHCP-Client benutzen**, um die Adresse von einem externen DHCP-Server zu beziehen.

- Unter **WAN-Modus** kann die WAN-Schnittstelle aktiviert werden.

  Bei aktivierter WAN-Schnittstelle arbeitet der Modulare Konnektor im Anbindungsmodus *In Reihe*, andernfalls im Anbindungsmodus *Parallel* (siehe Kapitel 6.4.1.2).

- Wenn der Modulare Konnektor im externen Netzwerk als DHCP-Client betrieben wird, kann mit **DHCP-Client Lease erneuern …** eine neue IP-Adresse vom DHCP-Server angefordert werden.

6.2.2.4 Bereich „LAN DHCP-Server“

Der Modulare Konnektor kann einen DHCP-Server bereitstellen, um die Clientsysteme zu verwalten. Dazu werden sie in Gruppen (Clientgroups) zusammengefasst.

Sie haben folgende Möglichkeiten:

- Unter **Einstellungen ...** kann der DHCP-Server aktiviert und der Adressbereich des lokalen Netzwerks konfiguriert werden. DHCP-Server und DHCP-Client können an der LAN-Schnittstelle nicht gleichzeitig aktiv sein.

- Mit **Standard-Clientgroup wählen …** kann eine Clientgroup als Standard-Clientgroup festgelegt werden. Ihr werden neue Clientsysteme zukünftig automatisch zugeordnet.

- Unter **Clientgroup anlegen ...** legen Sie eine Clientgroup an. Legen Sie ggf. für verschiedene Organisationsbereiche jeweils eigene Clientgroups an, um die Verwaltung der Clientsysteme aufzuteilen.

  Mit **Mac / IP / Hostname – Zuordnung** werden der Clientgroup Clientsysteme zugeordnet; geben Sie dazu die MAC-Adresse und optional die IP-Adresse und den Host-Namen des Clientsystems ein.

  Für jede Clientgroup können folgende Einstellungen konfiguriert werden:

  - DNS- und NTP-Server
  - Default-Gateway
  - Netzmaske und Domain-Name
  - Lease-Dauer, nach der regelmäßig eine neue IP-Adresse angefordert wird.

- Routen
- DHCP-Optionen

6.2.2.5 Bereich „DNS“

- Unter **Einstellungen ...** können Einstellungen zum Domain Name Server (DNS) konfiguriert werden:
  - Legen Sie einen DNS-Server im Transportnetz fest und konfigurieren Sie die Einstellungen des DNS-Servers.
  - Legen Sie den DNS-Server und die DNS-Domain für den Zugangsdienst fest, um die Verbindung zur TI zu ermöglichen.

  Wenn der Modulare Konnektor als DHCP-Server betrieben wird, wird die Adresse des DNS-Servers automatisch den Clientsystemen mitgeteilt, sofern in den Clientgroups kein externer DNS-Server konfiguriert ist.
- Mit **Status aktualisieren ...** kann die Anzeige aktualisiert werden.

6.2.2.6 Verknüpfung „VPN“

Der Menüpunkt **VPN** 🔗 öffnet das verknüpfte Menü **VPN** (siehe Kapitel 6.2.6).

6.2.3 Das Menü „Praxis“

Im Menü **Praxis** verwalten Sie Karten, Terminals, Mandanten, Arbeitsplätze, Clientsysteme und Aufrufkontexte.

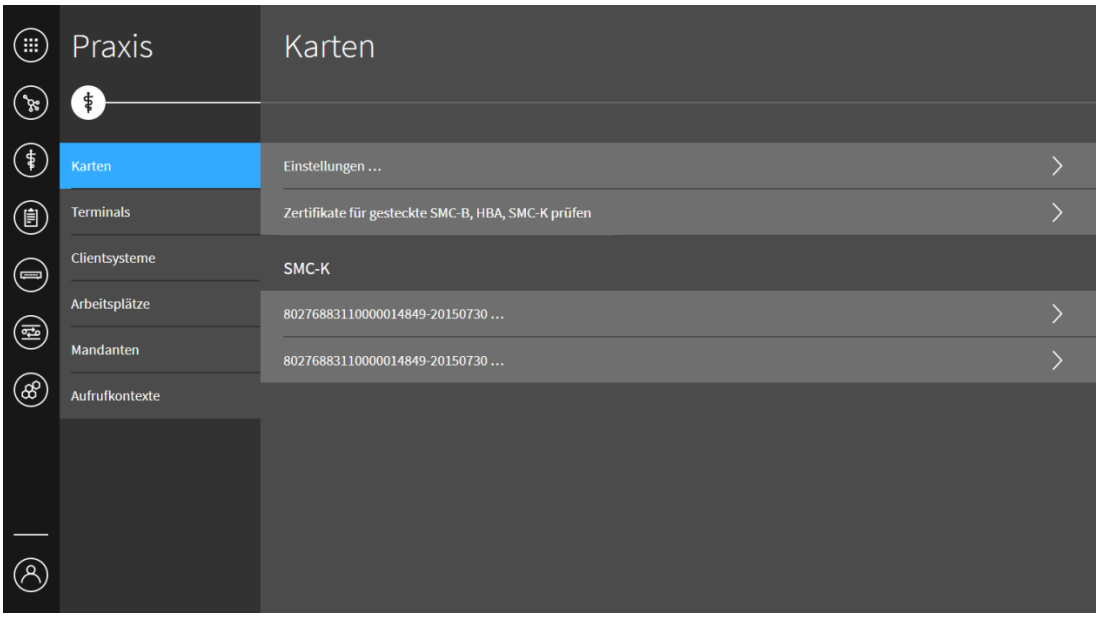


Abbildung 37: Menü „Praxis“

6.2.3.1 Bereich „Karten“

Im Bereich **Karten** werden die verwalteten Karten angezeigt.

Sie haben folgende Möglichkeiten:

- Klicken Sie auf eine Karte, um weitere Informationen und Optionen anzuzeigen. Bei SMC-Bs wird dadurch für jeden Mandanten der PIN-Status angezeigt.
- Unter **Einstellungen …** können die maximale Zeitdauer von Kartenoperationen und Einstellungen zur Zertifikatsprüfungen konfiguriert werden.
- Mit **Zertifikate für gesteckte SMC-B, HBA, SMC-K prüfen** können die Zertifikate der gesteckten Karten verifiziert werden.

6.2.3.2 Bereich „Terminals“

Im Bereich **Terminals** legen Sie Kartenterminals an und verwalten diese.

Sie haben folgende Möglichkeiten:

- Unter **Einstellungen …** können Einstellungen zum Verbindungsaufbau mit Kartenterminals konfiguriert werden.
- Mit **Liste der Kartenterminals aktualisieren** wird die angezeigte Liste der Kartenterminals aktualisiert.
- Unter **Unterstützte Versionen** wird angezeigt, welche Versionen von eHealth-Kartenterminals vom Modularen Konnektor unterstützt werden.
- Mit **Service Discovery auslösen** wird manuell die Suche nach Kartenterminals angestoßen.
- Mit **Ein neues Kartenterminal hinzufügen …** kann ein neues Terminal manuell unter Eingabe von IP-Adresse, Portnummer, MAC-Adresse und Hostname angelegt werden.

Kartenterminals verwalten

Die Anzeige der Kartenterminals ist nach Status absteigend sortiert (Aktiv und Verbunden, Bekannt etc.), bei gleichem Status alphabetisch. Klicken Sie ein Kartenterminal an, um weitere Optionen anzuzeigen:

- **Kartenterminal bearbeiten …**

  Geben Sie in den Einstellungen das am Kartenterminal festgelegte Passwort ein und aktualisieren Sie dieses ggf. bei einem Passwortwechsel.
- **Kartenterminal dem Konnektor zuweisen …**

  Bevor ein Kartenterminal genutzt werden kann, muss es dem Modularen Konnektor durch Pairing zugeordnet werden (siehe Kapitel 6.3).
- **Kartenterminal entfernen**

Kartenterminals zuordnen

Nach dem Pairing sind weitere Zuordnungen des Kartenterminals erforderlich:

- Mindestens einem Mandanten (siehe Kapitel 6.2.3.5)
- Einem Arbeitsplatz (siehe Kapitel 6.2.3.4)

Das Kartenterminal kann nur von dem zugeordneten Arbeitsplatz aus genutzt werden. Dazu kann es dem Arbeitsplatz entweder als lokales Kartenterminal zugewiesen werden (d.h. es befindet sich beim Arbeitsplatz) oder als entferntes Kartenterminal. Ein entferntes Kartenterminal befindet sich an einem beliebigen Ort im lokalen Netzwerk, die zugehörige PIN wird vom Arbeitsplatz aus über ein lokales Kartenterminal eingegeben. Ein entsprechendes Einsatzszenario ist in Kapitel 6.4.6 beschrieben.

6.2.3.3 Bereich „Clientsysteme“

Im Bereich **Clientsysteme** legen Sie Clientsysteme an, verwalten diese und konfigurieren Verbindungseinstellungen.

Sie haben folgende Möglichkeiten:

- Der Menüpunkt **Clientsystem-Einstellungen** öffnet die verknüpften Einstellungen zur Verbindung mit Clientsystemen (siehe Kapitel 6.2.2.1).
- Mit **Konnektorzertifikat …** kann für Verbindungen mit Clients über das Connector Event Transport (CEPT)-Protokoll das Zertifikat des Modularen Konnektors heruntergeladen werden. Geben Sie dazu ein Passwort ein.
- Mit **Clientsystem anlegen …** kann ein Clientsystem unter Angabe einer ID (interne Kennung) angelegt werden.

- Klicken Sie ein Clientsystem an, um weitere Optionen anzuzeigen:
  - **Clientsystem bearbeiten …**

    Ändert die ID des Clientsystems.
  - **Benutzerkennung hinzufügen …**

    Legt Benutzernamen und ein Passwort fest, mit denen sich das Clientsystem am Modularen Konnektor anmelden muss, wenn diese Authentifizierungsmethode ausgewählt wurde.
  - **Zertifikat hochladen … / Zertifikat erstellen …**

    Verwaltet TSL-Zertifikate für das Clientsystem (siehe Kapitel 6.5). Klicken Sie ein bestehendes Zertifikat an, um es herunterzuladen.

6.2.3.4 Bereich „Arbeitsplätze“

Im Bereich **Arbeitsplätze** werden die Arbeitsplätze angezeigt und verwaltet. Mit der Option **Detaillierte Ansicht** können Sie weitere Informationen zu den Arbeitsplätzen anzeigen.

Mit **Arbeitsplatz anlegen …** kann ein neuer Arbeitsplatz unter Angabe einer ID (interne Kennung) angelegt werden.

Klicken Sie einen bestehenden Arbeitsplatz an, um seine ID zu ändern oder ihm lokale und entfernte Kartenterminals zuzuweisen.

6.2.3.5 Bereich „Mandanten“

Mandanten sind Organisationseinheiten, die sich mit einer SMC-B ausweisen.

Mit der Option **Detaillierte Ansicht** können Sie weitere Informationen zu den bestehenden Mandanten anzeigen

Mit **Mandant anlegen …** kann ein Mandant unter Angabe einer ID (interne Kennung) angelegt werden. Anschließend können dem Mandanten die verwendete SMC-B sowie Kartenterminals zugewiesen werden:

- Ein lokales Kartenterminal wird am jeweiligen Arbeitsplatz benutzt, um Karten einzulesen und PINs einzugeben.
- Ein lokales Kartenterminal befindet sich lokal an einem Arbeitsplatz und kann von diesem aus genutzt werden. Hingegen ist das entfernte Kartenterminal einem entfernten oder auch – für zentral steckende Karten – keinem Arbeitsplatz fest zugewiesen. Ein lokales Kartenterminal kann als sogenanntes Remote-PIN Kartenterminals verwendet werden, um die PIN für eine in einem

entfernten Kartenterminal steckende Karte einzugeben (siehe Einsatzszenario in Kapitel 6.4.6).

- Mit **SMC-B hinzufügen (auswählen) …** können eine der verwalteten Karten auswählen um sie dem Mandanten zuzuweisen, oder unter **SMC-B hinzufügen (manuell) …** die Seriennummer der Karte manuell eingeben.

Klicken Sie einen Mandanten an, um seine Einstellungen zu bearbeiten.

6.2.3.6 Bereich „Aufrufkontexte“

Ein Aufrufkontext ist eine Kombination aus Clientsystem, Mandant und Arbeitsplatz. Aufrufkontexte werden von den Fachmodulen zur Kommunikation mit der TI benutzt (siehe Kapitel 6.2.7).

Mit der Option **Detaillierte Ansicht** können Sie weitere Informationen zu den bestehenden Aufrufkontexten anzeigen.

Mit **Aufrufkontext anlegen …** kann ein neuer Aufrufkontext erstellt werden. Wählen Sie dazu jeweils einen Mandanten, ein Clientsystem und ein Arbeitsplatz aus. Da jeder Aufrufkontext aus einer eindeutigen Kombination aus Mandant, Clientsystem und Arbeitsplatz bestehen muss, sind nicht zulässige Auswahlmöglichkeiten automatisch gesperrt und mit dem Symbol 🔒 gekennzeichnet.

Ein bestehender Aufrufkontext kann durch Anklicken gelöscht werden.

Ein Aufrufkontext kann nach dem Erstellen nicht mehr geändert, sondern nur gelöscht und ggf. neu angelegt werden.

6.2.4 Das Menü „Diagnose“

Im Menü **Diagnose** haben Sie Zugriff auf aktuelle Systeminformationen.

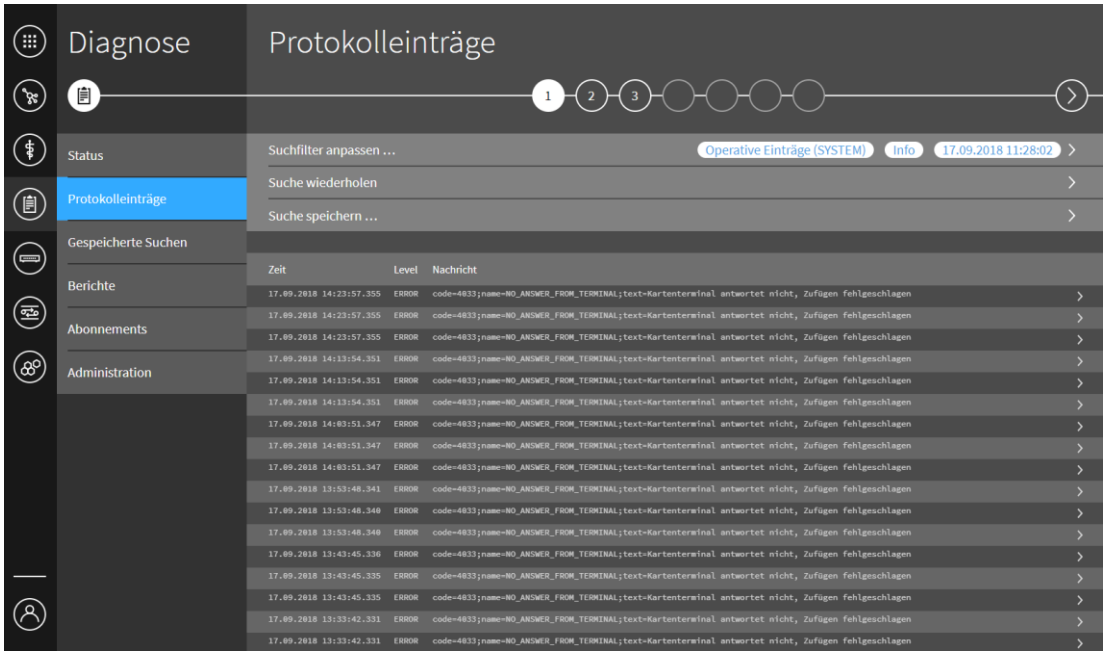


Abbildung 38: Menü „Diagnose“

6.2.4.1 Bereich „Status“

Im Bereich **Status** werden aktuelle Betriebs- und Fehlerzustände und zusätzliche Systeminformationen angezeigt.

6.2.4.2 Bereich „Protokolleinträge“

Im Bereich **Protokolleinträge** können Sie die protokollierten Meldungen durchsuchen und anzeigen. Legen Sie dazu unter **Suchfilter anpassen ...** die Suchkriterien fest. Die Suche wird daraufhin automatisch durchgeführt und die gefundenen Meldungen werden angezeigt. Eine ausführliche Beschreibung der Meldungen finden Sie im Kapitel 12.3.

Mit **Suche speichern …** können Sie die Suchfilter-Einstellungen abspeichern. Geben Sie dazu einen Namen ein und aktivieren Sie ggf. die Einstellung **Private Suche**, um den Zugriff auf die gespeicherte Suche einzuschränken; andere Benutzer können die gespeicherte Suche dann nicht verwenden oder verändern. Die Suche kann im Bereich **Gespeicherte Suchen** aufgerufen werden (siehe Kapitel 6.2.4.3).

Optional können Sie Meldungen exportieren und herunterladen:

- Mit **Download ...** werden die Meldungen als Textdatei gespeichert.
- Mit **Download komprimiert (gzip) ...** wird ein komprimiertes Archiv gespeichert.

6.2.4.3 Bereich „Gespeicherte Suchen“

Im Bereich **Gespeicherte Suchen** werden gespeicherte Suchfilter-Einstellungen angezeigt. Wenn Sie eine gespeicherte Suche aufrufen, haben Sie folgende Möglichkeiten:

- **Suche bearbeiten …**

  Ermöglicht die Anpassung der Suchfiltereinstellungen.
- **Zeitraum wählen**

  Legt den Suchzeitraum fest.
- **Ausführen und anzeigen …**

  Führt die Suche aus und zeigt die Suchergebnisse an.
- **Ausführen und herunterladen …**

  Führt die Suche aus und lädt die Suchergebnisse herunter.

6.2.4.4 Bereich „Berichte“

Im Bereich **Berichte** können Sie vom System generierte Berichte herunterladen.

6.2.4.5 Bereich „Abonnements“

Im Bereich **Abonnements** wird angezeigt, ob und mit welcher Adresse ein Clientsystem sich erfolgreich für den Systeminformationsdienst am Modularen Konnektor registriert hat.

6.2.4.6 Bereich „Administration“

Im Bereich **Administration** haben Sie folgende Möglichkeiten:

- Unter **Einstellungen …** können Sie festlegen, welche Ereignisse protokolliert werden und wie lange Protokolleinträge gespeichert bleiben.
- Bestehende Protokolleinträge können gelöscht werden.

Es können nur Protokolleinträge der Typen *System* und *Performance* gelöscht werden. Sicherheitseinträge können nicht gelöscht werden.

6.2.5 Das Menü „System“

Im Menü **System** steuern Sie grundlegende Gerätefunktionen.

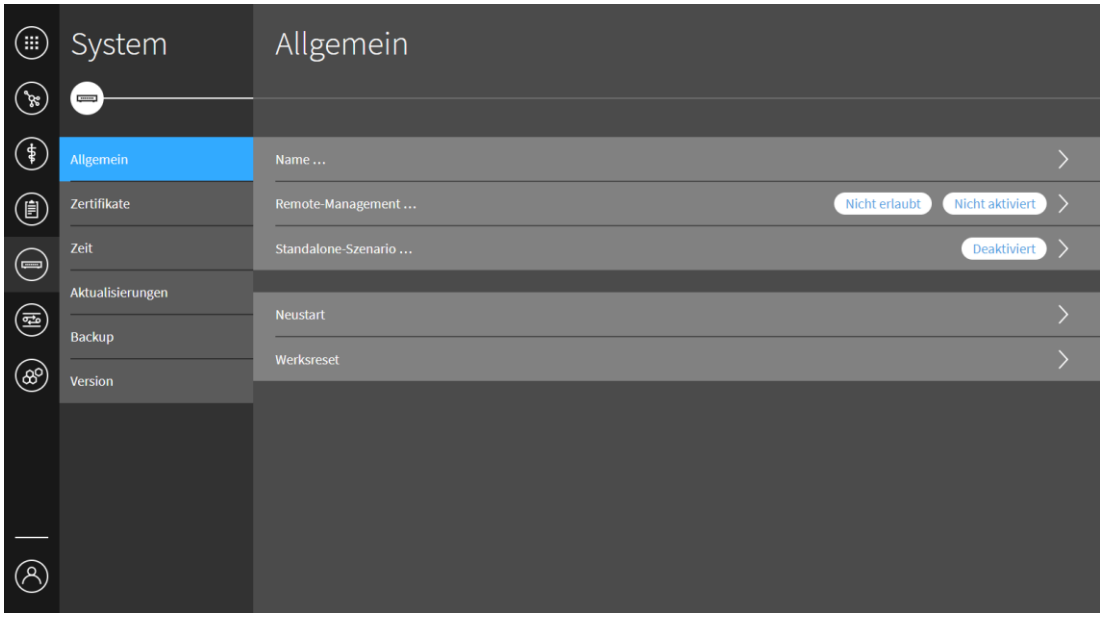


Abbildung 39: Menü „System“

6.2.5.1 Bereich „Allgemein“

In diesem Bereich konfigurieren Sie Systemeinstellungen und können einen Neustart oder Werksreset durchführen.

Sie haben folgende Möglichkeiten:

- **Name …**

  Der Name des Modularen Konnektors kann maximal 12 Zeichen lang sein und aus folgenden Zeichen bestehen:

  - Groß- und Kleinbuchstaben
  - Ziffern „0 bis 9“,
  - Zeichen „-“ (Minus)

  Nach einer Änderung des Namens ist der Neustart des Modularen Konnektors erforderlich. Dabei wird ein neues Zertifikat generiert. Dieses muss für die Benutzung der Administrationsschnittstelle erneut validiert werden, die Vorgehensweise ist analog zur Erstanmeldung (siehe Kapitel 5.3).

Vor der Validierung des Konnektor-Zertifikates dürfen keine Zugangsdaten an der Administrationsschnittstelle eingegeben werden.

- **Remote-Management …**

  Wenn Remote Management erlaubt und aktiviert ist, kann der Modulare Konnektor über das öffentliche Netzwerk administriert werden (siehe Kapitel 6.4.1.5).

- **Standalone-Szenario …**

  Wenn aktiviert, arbeitet der Modulare Konnektor ohne angeschlossene Clientsysteme (siehe Kapitel 6.4.1).

- **Neustart …**

  Startet das Gerät unter Beibehaltung der bisherigen Konfiguration neu.

- **Werksreset …**

  Führt einen Werksreset aus; beachten Sie die Hinweise in Kapitel 6.6.

- **Werksreset zum Versand …**

  Führt einen Werksreset zum Versand aus; beachten Sie die Hinweise in Kapitel 6.7.

6.2.5.2 Bereich „Zertifikate“

Der Zertifikatsdienst stellt Funktionen zur Validierung von Zertifikaten zur Verfügung (siehe Kapitel 1.2.4).

Unter **Einstellungen …** können Zeitfristen für die Aktualisierung der Trust-Service Status List (TSL) und für Abfragen über Online Certificate Status Protocol (OCSP) konfiguriert werden.

Um unerlaubte Zugriffe zu erkennen, überwacht der Modulare Konnektor die Häufigkeit bestimmter Operationen im lokalen Netzwerk.

- Unter **Missbrauch-Erkennung Einstellungen …** können die Obergrenzen für die Häufigkeit angepasst werden, ab denen ein Missbrauchs-Alarm abgegeben wird.

- Unter **Missbrauch-Erkennung Status …** werden die aktuelle Häufigkeit von Operationen und der konfigurierte Grenzwert angezeigt.

Weiterhin können Sie folgende Aktionen durchführen:

- Mit **TSL hochladen ...** und **Zertifikats-Sperrliste (CRL) hochladen ...** können aktuelle Versionen der TSL und der CRL manuell auf den Modularen Konnektor hochgeladen werden. Bei einer bestehenden Verbindung zur TI werden die TSL und die CRL normalerweise automatisch aktualisiert. Ein manuelles hochladen der TSL ist nur möglich, wenn im Modularen Konnektor die Option **Leistungsumfang Online** deaktiviert ist (siehe Kapitel 6.2.2.1).
- Mit **Erreichbarkeit der OSCP-Forwarder prüfen ...** kann geprüft werden, ob der Dienst zur automatischen Aktualisierung von TSL und CRL erreichbar ist.

6.2.5.3 Bereich „Zeit“

In diesem Bereich konfigurieren Sie die Systemzeit:

- Unter **Einstellungen …** können Zeit und Zeitzone manuell festgelegt werden.
- Mit **Zeitsynchronisierung auslösen …** kann bei Online-Betrieb die Synchronisierung der Systemzeit mit dem NTP-Server der TI durchgeführt werden.

Die angezeigten Einstellungen im Bereich **Zeitsynchronisierung** dienen der Plausibilitätskontrolle für die Zeitsynchronisierung und sind nicht veränderbar.

Beachten Sie:

- **Im Offline-Modus muss die Uhrzeit mindestens einmal jährlich synchronisiert werden.**
- **Im Online-Modus darf die im Konnektor eingestellte Zeit nicht mehr als 30 Sekunden von der in der TI gültigen Zeit abweichen, andernfalls ist eine Verbindung zur TI nicht möglich. Prüfen Sie die Zeit mindestens bei der Inbetriebnahme und passen Sie sie wenn notwendig an.**

6.2.5.4 Bereich „Aktualisierungen“

In diesem Bereich verwalten Sie Systemaktualisierungen (Updates, siehe auch Kapitel 6.7.):

- Unter **Einstellungen …** haben Sie folgende Möglichkeiten:
  - Sie können die Online-Suche nach verfügbaren Updates und für Teilnehmer von Erprobungen von Erprobungs-Updates aktivieren oder deaktivieren.
  - Sie können festlegen, ob verfügbare Updates automatisch heruntergeladen werden, um für die Installation bereitzustehen.

- Sie können festlegen, ob neue verfügbare Bestandsnetze automatisch aktiviert werden. Anderenfalls muss dies ggf. im Menü **VPN** im Bereich **Bestandsnetze** manuell geschehen.

- Unter **Einsehbare Konfigurationsparameter** werden Informationen zu den Konfigurationsdiensten zum Download von Konfigurationsdaten und Firmware angezeigt.

- Mit **Aktualisierungsinformationen aktualisieren …** kann die Anzeige aktualisiert werden.

- Unter **Geräte** werden die Komponenten angezeigt, für die Updates durchgeführt werden können. Klicken Sie ein Gerät an, um weitere Informationen und Optionen anzuzeigen:

  - Unter **Verfügbare Aktualisierungen** werden verfügbare Online-Updates angezeigt. Klicken Sie ein Update an, um es zu installieren.

  - Mit **Aktualisierung hochladen …** kann ein Update vom Clientsystem hochgeladen werden (Offline-Update).

6.2.5.5 Bereich „Backup“

In diesem Bereich können Sie Systemsicherungen (Backups) erstellen und importieren.

Um ein Backup zu erstellen, gehen Sie wie folgt vor:

▶ Klicken Sie **Backup erstellen …**

▶ Wählen Sie den Umfang der Sicherung aus:

- **Gesamtexport**

  Alle Einstellungen des Modularen Konnektors sowie alle angelegten Objekte und Benutzerkonten; damit kann die aktuelle Konfiguration zu einem späteren Zeitpunkt vollständig wiederhergestellt werden.

- **Netzkonnektor**

  Die Einstellung aus den Menüs **Netzwerk**, **Protokolle** und **VPN**, jedoch ohne die Freischaltung des Modularen Konnektors.

- **Anwendungskonnektor**

  Die Einstellungen sowie die angelegten Objekte und Benutzerkonten aus den Menüs **Praxis**, **Benutzer** und **Fachmodule**, sowie die Freischaltung des Modularen Konnektors.

- **Nur Infomodell**

  Die im Menü **Praxis** angelegten Objekte (Kartenterminals, Clientsysteme, Mandanten etc.).

- **Nur Benutzer**

  Die im Menü **Benutzer** angelegten Benutzerkonten.

▶ Geben Sie in den Feldern **Passwort** und **Passwortbestätigung** ein Passwort ein, mit dem das Backup gesichert wird. Beachten Sie die Sicherheitshinweise zu Passwörtern in Kapitel 4.2.

Nach Bestätigung wird die Backup-Datei gesichert und es werden der öffentliche Schlüssel, mit dem die gespeicherte Datei verschlüsselt wurde, und dessen Hashwert angezeigt. Damit kann später die Validität des Backups geprüft werden.

Um ein Backup zu importieren, gehen Sie wie folgt vor:

▶ Klicken Sie **Backup einspielen …**

▶ Klicken Sie **Datei auswählen** und suchen Sie die gewünschte Backup-Datei.

▶ Geben Sie unter **Passwort** das zugehörige Passwort des Backups ein.

Nach **Bestätigung** werden der öffentliche Schlüssel des Backups und dessen Hashwert angezeigt.

▶ Bestätigen Sie die Fortsetzung, wenn der öffentliche Schlüssel und der Hashwert korrekt sind.

Falls das Backup Kartenterminals beinhaltet, werden Ihnen diese für den Import zur Auswahl gestellt.

Nach Bestätigung wird das Backup importiert und das Ergebnis des Imports angezeigt.

6.2.5.6 Bereich „Version“

In diesem Bereich werden Produktdaten und Versionsangaben angezeigt.

- Unter **Firmware-Gruppendatei herunterladen …** können Sie Informationen über die zulässigen Firmware-Versionen herunterladen, beispielsweise für die Fehlersuche.
- Mit **Details …** können weitere Einzelheiten zum System angezeigt werden.

6.2.6 Das Menü „VPN“

Im Menü **VPN** konfigurieren Sie die Anbindung an den VPN-Zugangsdienst.

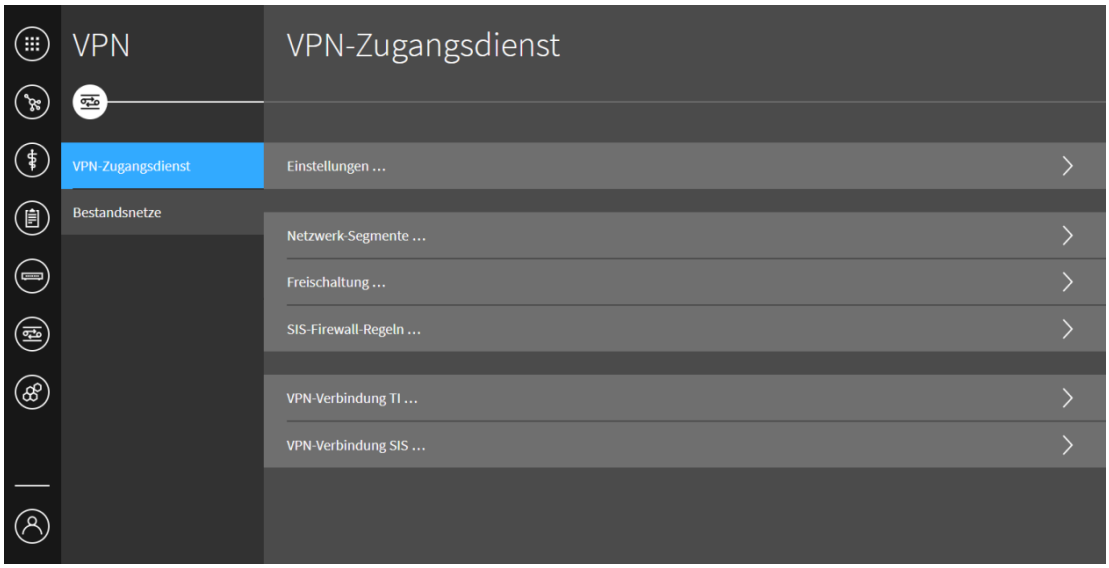


Abbildung 40: Menü „VPN“

6.2.6.1 Bereich „VPN-Zugangsdienst“

In diesem Bereich konfigurieren Sie die Anbindung an den VPN-Zugangsdienst.

Bei Verwendung von IKE ist es möglich, dass die interne IP-Adresse des Modularen Konnektor hinter dem NAT-Gateway ermittelt werden kann.

Unter **Einstellungen ...** können Netzwerkeinstellungen für den Zugang zu TI und SIS angepasst werden. Diese sind vorkonfiguriert und sollten nur bei Bedarf geändert werden:

- Aktivierung oder Deaktivierung des hash&URL-Verfahrens für den Zertifikatsaustausch
- Keep-Alive-Einstellungen für das Internet-Key-Exchange (IKE)-Protokoll
- Keep-Alive-Einstellungen für das Network Address Translation (NAT)-Protokoll
- Timeout bei Inaktivität der VPN-Verbindung
- Maximale Paketgrößen (MTU) für die Verbindungen zu TI und SIS
- Einstellungen zu Sequenznummern für das IPsec-Protokoll

Die Auswertung von IPsec-Sequenznummern kann vorübergehend deaktiviert werden. Der Modulare Konnektor arbeitet dann nicht Zertifizierungskonform.

Unter **Netzwerk-Segmente ...** werden die virtuellen privaten Netzwerke verwaltet, die über den Modularen Konnektor erreichbar sind. Die Netzwerke der TI sind vorkonfiguriert, Sie können nach Bedarf weitere Netzwerke hinzufügen.

Mit **Freischaltung ...** kann der Modulare Konnektor für einen Mandanten am VPN-Zugangsdienst der TI freigeschaltet werden. Sie benötigen dazu die Vertragsnummer (Contract ID), die Sie von Ihrem Zugangsdienst-Anbieter erhalten.

Gehen Sie wie folgt vor:

- Klicken Sie **Konnektor freischalten …**
- Wählen Sie einen Mandanten und die zu verwendende SMC-B (diese muss zum Zeitpunkt der Freischaltung an einem Kartenterminal eingesteckt sein).
- Geben Sie die zugehörige Vertragsnummer ein.

  Nach Bestätigung führt der Modulare Konnektor die Freischaltung durch und zeigt das Ergebnis an.

6.2.6.2 Regelwerk des Paketfilters konfigurieren

Der Modulare Konnektor blockiert alle Pakete, die von keiner Firewall-Regel erfasst werden. Unter **SIS-Firewall-regeln …** werden die vorhandenen Firewall-Regeln angezeigt. Sie können neue Regeln anlegen oder vorhandene durch Anklicken bearbeiten oder löschen.

Um eine Firewall-Regel zu erstellen, klicken Sie **Firewall-Regel hinzufügen …** Legen Sie anschließend für zulässige Pakete jeweils folgende Merkmale fest:

- Richtung (ein- oder ausgehend)
- Protokoll (TCP oder UDP)
- Jeweils Adresse und Port für Quelle und Ziel

Klicken Sie nach der Eingabe → und bestätigen Sie die neue Regel mit ✓ .

Durch das Anlegen zusätzlicher Filteregeln kann die Funktionsweise des SIS eingeschränkt werden. Gegebenenfalls sind durch entsprechende Einstellungen von Filterregeln bestimmte Dienste im SIS nicht mehr verfügbar. Nur erfahrene Benutzer sollten das Regelwerk des Paketfilters konfigurieren.

6.2.6.3 Verbindungen zur TI und SIS

Nach erfolgreicher Freischaltung stellt der Modulare Konnektor die Verbindungen zur TI und ggf. SIS automatisch her. Unter **VPN-Verbindung TI ...** und **VPN-Verbindung SIS ...** können Sie die Verbindungen bei Bedarf manuell trennen und wieder herstellen.

6.2.6.4 Bereich „Bestandsnetze“

Bestandsnetze sind Netzwerke, die bereits vor der Einführung der TI in Gebrauch waren und weiterhin verwendet werden.

Die Kommunikation mit den Bestandsnetzen erfolgt durch den Modularen Konnektor über den gesicherten VPN-Tunnel zur TI. Wenn sich der Adressbereich der Bestandsnetze ändert, kann dies Auswirkung auf die Kommunikation der an den Bestandsnetzen angebundenen Clientsysteme haben. Datenpakete, die an Adressen gesendet werden, die nicht mehr einem Bestandsnetz zugeordnet sind, werden vom Modularen Konnektor entsprechend der aktuellen Paketfilter-Regeln behandelt (siehe Kapitel 6.2.6.1). Je nach Anbindungsmodus des Modularen Konnektors (siehe Kapitel 6.4.1.2) können die Datenpakete an den VPN-Konzentrator des SIS oder direkt ins Internet gesendet werden. Für die Clientsysteme ist daher sicherzustellen, dass alle angebundenen Bestandsnetze auch in der aktuellen Liste des Modularen Konnektors aufgeführt werden.

Sie haben folgende Möglichkeiten:

- Durch Anklicken können Bestandsnetze angepasst werden.
- Mit **Bestandsnetze aktualisieren ...** wird die Ansicht der Bestandsnetze aktualisiert.
- Mit **Bestandsnetze aktivieren/deaktivieren** können Bestandsnetze aktiviert oder deaktiviert werden, um den Zugriff darauf zu ermöglichen oder zu unterbinden.

6.2.7 Das Menü „Fachmodule“

Im Menü **Fachmodule** werden Informationen über die auf dem Modularen Konnektor betriebenen Fachanwendungen angezeigt. Standardmäßig ist das Fachmodul Versichertenstammdatenmanagement (VSDM) installiert.

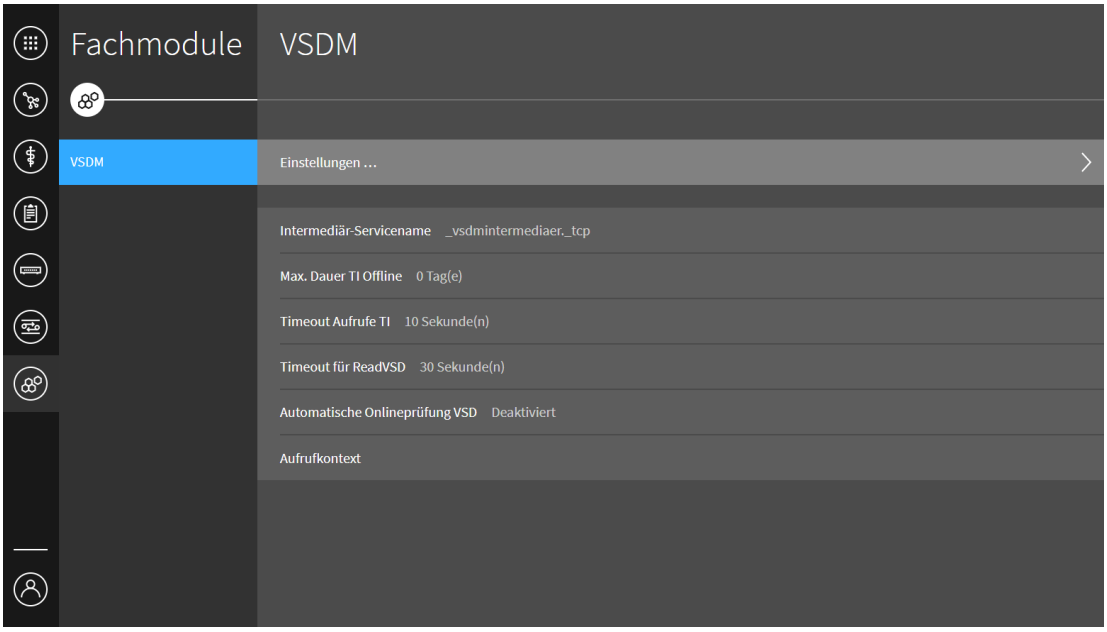


Abbildung 41: Menü „Fachmodule“

6.2.7.1 VSDM

Das Fachmodul VSDM ermöglicht den Abgleich Versichertenstammdaten.

Unter **Einstellungen …** können folgende Einstellungen des Fachmoduls VSDM konfiguriert werden:

- Intermediär-Servicename
- Maximale Dauer für den Offline-Betrieb ohne Verbindung zur TI
- Maximale Zeitdauer für Aufrufe des VSDM-Dienst in der TI
- Maximale Bearbeitungszeit für die Operation *ReadVSD*
- Automatische Online-Prüfung VSD
- Aufrufkontext für die Operation *AutoUpdateVSD*

Unter **Verschlüsselung der Prüfungsnachweise (VSDM-PNW-Key)** wird für jeden Mandanten mit Aufrufkontext eine Zeichenfolge für die Verschlüsselung von Prüfungsnachweisen benötigt. Dazu gibt es zwei Möglichkeiten:

- Eine Zeichenkette kann manuell eingegeben werden.
- Wenn das Eingabefeld gelöscht und die Eingabe bestätigt wird, generiert der Modulare Konnektor automatisch eine neue zufällige Zeichenkette.

Falls Sie mehrere Konnektorpaare (Modulare Konnektoren im Offline- und Online-Modus) innerhalb derselben Praxis administrieren, konfigurieren Sie jeweils unterschiedliche Zeichenketten für die Verschlüsselung von Prüfungsnachweisen.

6.3 Kartenterminals anbinden und benutzen

6.3.1 Kartenterminal verbinden (Pairing)

Beim Pairing wird ein Kartenterminal dem Modularen Konnektor zugeordnet und eine gesicherte Verbindung über das lokale Netzwerk eingerichtet.

- Schließen Sie das Kartenterminal an das Netzwerk an und nehmen Sie es in Betrieb.
- Notieren Sie ggf. den Fingerprint der zugehörigen Gerätekarte (gSMC-KT) und stecken Sie diese in das Kartenterminal ein. Beachten Sie die Anleitung des Herstellers.

  Der Fingerprint ist eine aus 16 Zahlenblöcken bestehende Prüfzeichenfolge.
- Öffnen Sie im Menü **Praxis** den Bereich **Terminals** und klicken Sie **Ein neues Kartenterminal hinzufügen ...**
- Klicken Sie **Service Discovery auslösen**.

  Der Modulare Konnektor erkennt das neue Kartenterminal normalerweise automatisch und zeigt es mit dem Status *Bekannt* an. Alternativ klicken Sie **Kartenterminal manuell hinzufügen** und legen Sie das Kartenterminal unter Angabe der IP-Adresse manuell an.
- Klicken Sie das neu hinzugefügte Kartenterminal an, um weitere Optionen anzuzeigen.
- Klicken Sie **Terminal dem Konnektor zuweisen**.

  Das Kartenterminal besitzt nun den Status *Zugewiesen*.
- Klicken Sie **Terminal pairen und aktivieren**.

  Der Fingerprint der am Kartenterminal gesteckten Gerätekarte wird angezeigt.
- Vergleichen Sie den Fingerprint und klicken Sie bei Übereinstimmung **Fingerprint ist identisch**.
- Bestätigen Sie am Kartenterminal das Pairing durch Drücken der Bestätigungs-Taste. Dies muss innerhalb einer geräteabhängigen Zeitspanne erfolgen (maximal 10 Minuten).

  Im Display des Kartenterminals wird der Hostname des Modularen Konnektors angezeigt und in der Bedienoberfläche des Modularen Konnektors wird das Kartenterminal nun mit dem Status *Aktiv* angezeigt.

Bei Remote-Administration muss der Remote-Administrator für den vorgenannten Vergleich und die Bestätigung durch den Leistungserbringer oder das Praxispersonal vor Ort unterstützt werden.

6.3.2 Kartenterminal außer Betrieb nehmen

Bei der Außerbetriebnahme eines Kartenterminals müssen alle Pairing-Daten im Kartenterminal gelöscht werden. Beachten Sie die Anleitung des Herstellers.

- Entfernen Sie das Kartenterminal im Modularen Konnektor aus der Liste der Kartenterminals (siehe Kapitel 6.2.3).

6.4 Netzwerkszenarien

6.4.1 Übersicht der Betriebsmodi

Hinsichtlich der Einsatzumgebung können folgende Betriebsmodi des Modularen Konnektors unterschieden werden:

- Online/Offline-Modus

  Normalerweise wird der Modulare Konnektor online mit Netzwerkanbindung betrieben, jedoch ist auch ein Offline-Betrieb möglich (siehe Kapitel 6.4.1.1)

- Anbindungsmodus (siehe Kapitel 6.4.1.2)

  Der Modulare Konnektor kann am Übergangspunkt zum IAG oder innerhalb des lokalen Netzwerks betrieben werden.

- Internetmodus (siehe Kapitel 6.4.1.3)

  Für das Internet bestimmte Datenpakete von Clientsystemen können vom Modularen Konnektor weitergeleitet, vom IAG weitergeleitet, oder blockiert werden.

- Standalone-Modus (Betrieb ohne lokaler Clientsysteme, siehe Kapitel 6.4.1.4)
- Art der Administration (Lokal oder Remote, siehe Kapitel 6.4.1.5)

6.4.1.1 Online/Offline-Modus

Der Modulare Konnektor ist für den Online-Betrieb mit Anbindung an die TI und optional SIS ausgelegt, kann jedoch auch offline betrieben werden. Es werden dann keine Verbindungen zu TI oder SIS aufgebaut; der Modulare Konnektor stellt jedoch weiterhin lokal nutzbare Funktionen zur Verfügung, wie z.B. die Ausführung von Fachmodulen.

Im Offline-Modus muss die Uhrzeit mindestens einmal jährlich synchronisiert werden (siehe Kapitel 6.2.5.3).

6.4.1.2 Anbindungsmodus

Für die Einbindung des Modularen Konnektors in die lokale Netzwerktopologie bestehen folgende Optionen:

- **In Reihe**

  Der Modulare Konnektor befindet sich am Übergangspunkt zwischen dem lokalen Netzwerk und dem Internet Access Gateway (IAG).

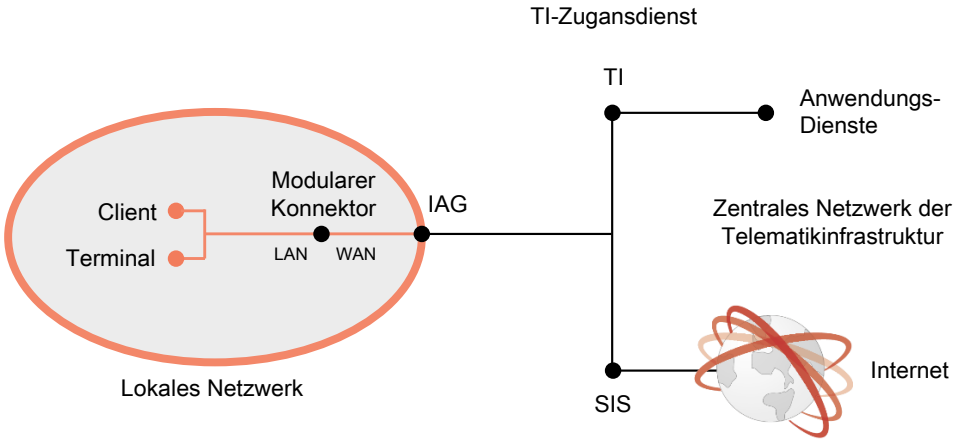


Abbildung 42: Anbindungsmodus In Reihe

- **Parallel**

  Die WAN-Schnittstelle wird nicht benutzt, die Verbindung zum IAG geschieht ggf. über das lokale Netzwerk. Bei Verwendung einer Firewall müssen die erforderlichen Ports und Protokolle für den Betrieb des Modularen Konnektors freigegeben sein (siehe Kapitel 5.1).

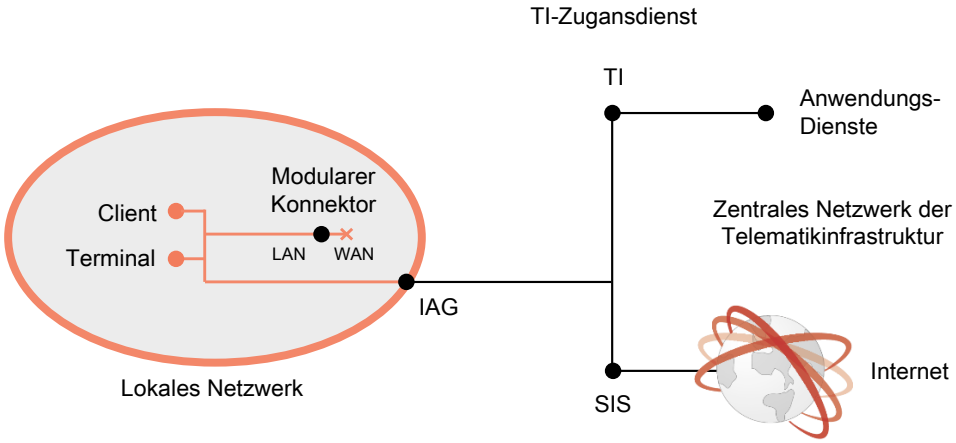


Abbildung 43: Anbindungsmodus Parallel

Wenn eine Infrastruktur im dezentralen Bereich bereits vorhanden ist, können die Produkte der TI, insbesondere der Konnektor, so in die Infrastruktur integriert werden, dass Bestandsanwendungen bereits erprobte Kommunikationswege weiter nutzen können.

Im Beispiel in Kapitel 6.4.4 existiert bereits eine Infrastruktur, die einen Internetzugang für die Arbeitsplätze ermöglicht. In diesem Fall wird der Konnektor als zusätzliches Gerät an das bestehende Netzwerk angeschlossen und nutzt den bereits vorhandenen Internetanschluss zur Kommunikation in die TI.

Beim Anbindungsmodus *Parallel* erfolgt kein Schutz des lokalen Netzwerks durch die Sicherheitsfunktionen des Modularen Konnektors. Der Leistungserbringer ist in jedem Anbindungsmodus für den Schutz des lokalen Netzwerks verantwortlich.

Übersicht der Anbindungsmodi

	In Reihe	**Parallel**
Schutz durch Sicherheitsfunktionen des Modularen Konnektors	Ja	Nein
Zugang zum SIS	Ja	Ja
Nutzung von Internetdiensten außerhalb des SIS	Nein	Ja
Einrichtungs- und Administrationsaufwand	Mittel	Niedrig

6.4.1.3 Internetmodus

Der Internetmodus legt fest, wie für das Internet bestimmten Datenpakete von Clientsystemen behandelt werden, die den Modularen Konnektor als Default Gateway verwenden:

- **SIS**

  Der Modulare Konnektor leitet alle für das Internet bestimmten Datenpakete an den SIS weiter.

- **IAG**

  Für das Internet bestimmte Datenpakete werden an das Internet Access Gateway umgeleitet (nur im Anbindungsmodus *Parallel* möglich).

- **Ohne**

  Der Modulare Konnektor verwirft alle für das Internet bestimmten Datenpakete.

Der Internetmodus muss entsprechend der Einsatzumgebung konfiguriert werden, abhängig vom Anbindungsmodus gibt es dazu folgende Möglichkeiten:

Anbindungsmodus	Reihe	Parallel
Online	SIS	SIS, IAG
Offline	Ohne	Ohne

Tabelle 11: Internetmodus

6.4.1.4 Standalone-Modus

Im Standalone-Modus wird der Modulare Konnektor ohne Anbindung lokaler Clientsysteme betrieben. In diesem Fall werden zwei Modulare Konnektoren eingesetzt (Online/Offline). Die Fachmodule werden direkt auf dem Modularen Konnektor ausgeführt und sind über den VPN-Zugangsdienst an die TI angebunden.

6.4.1.5 Administration

Der Modulare Konnektor kann über eine webbasierte Bedienoberfläche administriert werden. Dazu können folgende Bedienschnittstellen verwendet werden:

- **Lokal**

  Die Administrierung des Modularen Konnektors erfolgt über das lokale Netzwerk.

- **Remote Management**

  Die Administrierung des Modularen Konnektors erfolgt über den SIS. Hierbei erfolgt der Verbindungsaufbau immer vom Modularen Konnektor aus.

Der Modulare Konnektor kann zudem Updates (Firmware-Aktualisierungen) erhalten. Updates werden vom KSR (Konfigurations- und Software-Repository) über die WAN-Schnittstelle oder über ein Clientsystem bereitgestellt (siehe Kapitel 6.7). Der Modulare Konnektor überprüft die Signatur aller Updatepakete. Wenn die Signatur nicht korrekt ist, wird das Update nicht eingespielt und die Software verbleibt auf dem bisherigen Stand.

6.4.2 Szenario 1: Keine bestehende Infrastruktur, keine speziellen Anforderungen

6.4.2.1 Beschreibung

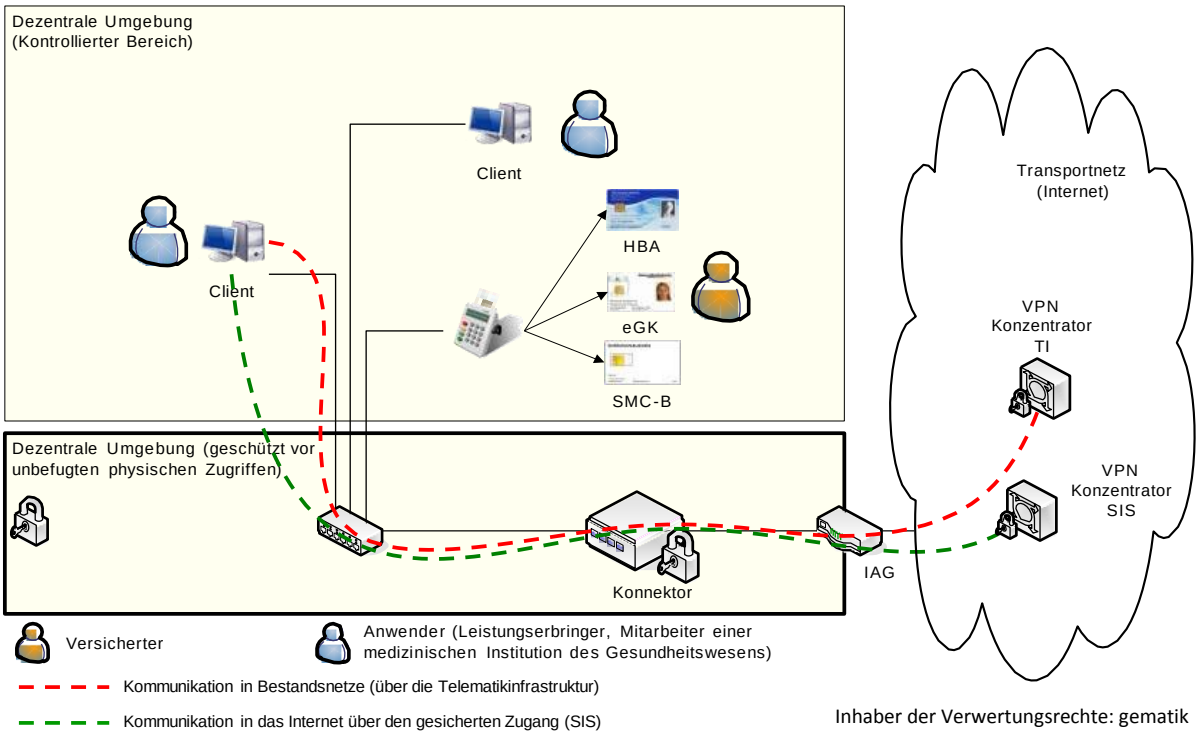


Abbildung 44: Szenario einer einfachen Installation

In diesem einfachen Netzwerkszenario wird der Modulare Konnektor als Default-Gateway für jegliche IP-Kommunikation aus dem lokalen Netzwerk eingesetzt. Dabei übernimmt der Modulare Konnektor das Routing der Kommunikation über den IAG zum SIS und in die an die TI angeschlossenen Bestandsnetze.

Ein oder mehrere Clientsysteme können über den Modularen Konnektor Anwendungsfälle der Telematikinfrastruktur initiieren und über den Modularen Konnektor und die zentrale TI-Plattform in Bestandsnetze kommunizieren. Dabei ist die Nutzung der Anwendungsfälle der TI je nach Konfiguration des Modularen Konnektors entweder nur authentifizierten oder beliebigen Clientsystemen möglich.

In diesem Beispiel werden über ein einziges Kartenterminal die SMC-B, der HBA und auch die eGK des Versicherten gelesen, es können dazu jedoch auch mehrere Kartenterminals genutzt werden.

Darüber hinaus können die Clientsysteme über den SIS auf das Internet zugreifen.

6.4.2.2 Voraussetzung

Folgende Voraussetzungen müssen vor dem weiteren Vorgehen erfüllt sein:

- Die bestehenden Clientsysteme können in ein lokales Netzwerk eingebunden werden, das zum Modularen Konnektor kompatibel ist.
- Eine SMC-B ist verfügbar.
- Der Kartenleser befindet sich in einem kontrollierten Bereich, der vom Praxispersonal überwacht wird.

6.4.2.3 Vorgehensweise

So richten Sie dieses Szenario ein:

▶ Konfigurieren Sie den Modularen Konnektor in den Clientsystemen als Default-Gateway.

▶ Konfigurieren Sie die LAN-Schnittstelle entsprechend der lokalen Netzwerkumgebung und die WAN-Schnittstelle für die Verbindung mit dem IAG (siehe Kapitel 6.2.2).

Die notwendigen Einstellungen für die WAN-Schnittstelle erhalten Sie vom Internet Service Provider (ISP).

▶ Legen Sie die erforderlichen Mandanten, Clientsysteme und einen Arbeitsplatz mit zugewiesenem Kartenterminal an (siehe Kapitel 6.2.3).

▶ Richten Sie die Verbindung zum VPN-Zugangsdienst ein (siehe Kapitel 6.2.6).

▶ Führen Sie die Freischaltung des Modularen Konnektors durch und aktivieren Sie die Verbindungen mit TI und SIS (siehe Kapitel 6.2.6.1).

6.4.2.4 Ergebnis

Nach der Installation sind folgende Ergebnisse erreicht:

- Die Clientsysteme können über den Modularen Konnektor Anwendungsfälle der TI initiieren.
- Die Clientsysteme können über den Modularen Konnektor auf das Internet und auf Bestandsnetze zugreifen.

6.4.3 Szenario 2: Mehrere Behandlungsräume

6.4.3.1 Beschreibung

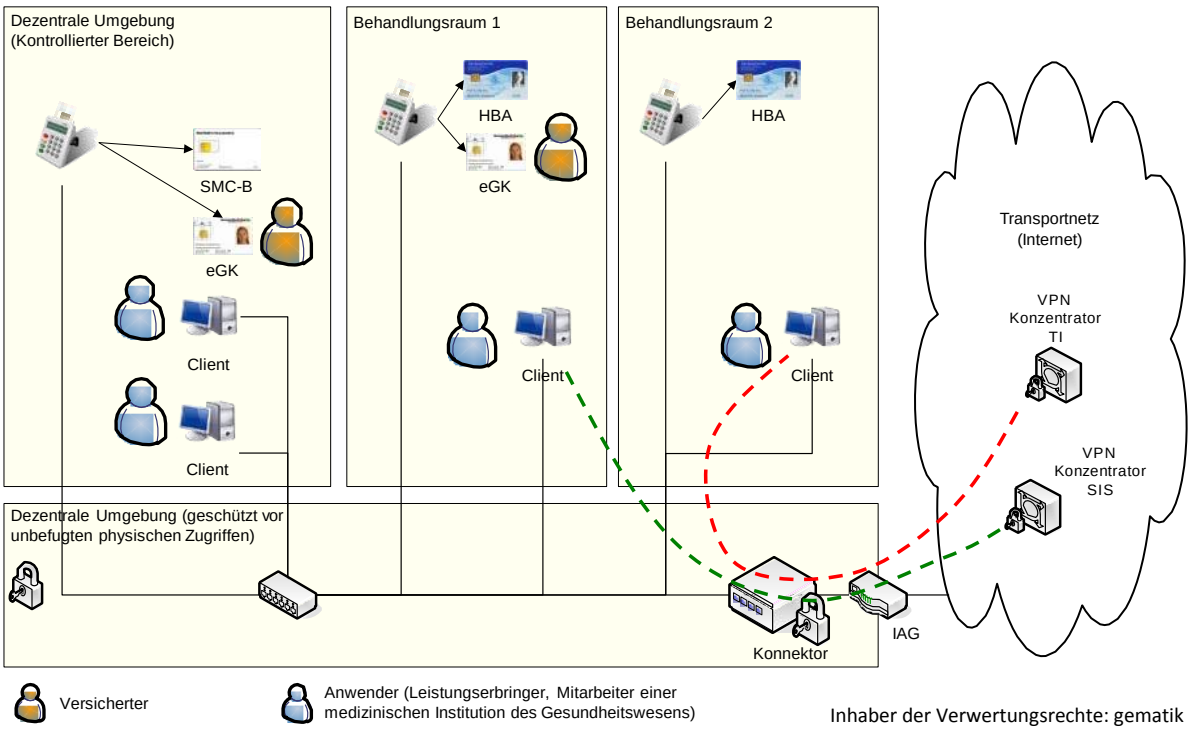


Abbildung 45: Szenario einer Installation mit mehreren Behandlungsräumen

Mit dieser Netzwerk-Topologie werden mehrere Behandlungsräume unterstützt. Dabei ist in jedem Behandlungsraum mindestens ein Kartenterminal zum Lesen von eGKs vorzusehen. Die Kommunikationswege in zentrale Netzwerke entsprechen denen in Szenario 1.

Durch die Ressourcenverwaltung des Modularen Konnektors wird sichergestellt, dass bei Anwendungsfällen die Kartenterminals angesprochen werden, die dem jeweiligen Arbeitsplatz zugeordnet sind, von dem aus der Anwendungsfall initiiert wurde.

6.4.3.2 Voraussetzung

Folgende Voraussetzungen müssen vor dem weiteren Vorgehen erfüllt sein:

- Die bestehenden Clientsysteme können in ein lokales Netzwerk eingebunden werden, das zum Modularen Konnektor kompatibel ist.
- Eine SMC-B, mehrere Kartenterminals und Clientsysteme sind verfügbar.
- Der Kartenleser, der zum Auslesen der SMC-B verwendet wird, befindet sich in einem kontrollierten Bereich, der vom Praxispersonal überwacht wird.

6.4.3.3 Vorgehensweise

So richten Sie dieses Szenario ein:

- ▶ Konfigurieren Sie den Modularen Konnektor in den Clientsystemen als Default-Gateway.
- ▶ Legen Sie die erforderlichen Mandanten, Clientsysteme und Arbeitsplätze mit zugewiesenen Kartenterminals an (siehe Kapitel 6.2.3). Achten Sie darauf, jedem Arbeitsplatz das entsprechende Kartenterminal zuzuweisen
- ▶ Konfigurieren Sie die LAN-Schnittstelle entsprechend der lokalen Netzwerkumgebung und die WAN-Schnittstelle für die Verbindung mit dem IAG (siehe Kapitel 6.2.2).

  Die notwendigen Einstellungen für die WAN-Schnittstelle erhalten Sie vom ISP.
- ▶ Richten Sie die Verbindung zum VPN-Zugangsdienst ein (siehe Kapitel 6.2.6).
- ▶ Führen Sie die Freischaltung des Modularen Konnektors durch und aktivieren Sie die Verbindungen mit TI und SIS (siehe Kapitel 6.2.6.1).

6.4.3.4 Ergebnis

Nach der Installation sind folgende Ergebnisse erreicht:

- Die Clientsysteme können über den Modularen Konnektor Anwendungsfälle der TI initiieren.
- Die Clientsysteme können über den Modularen Konnektor auf das Internet und auf Bestandsnetze zugreifen.
- Der HBA-Inhaber muss seinen HBA mit sich führen und kann diesen in den einzelnen Kartenterminals der Behandlungsräume nutzen.
- Die SMC-B muss im kontrollierten Bereich verwendet werden.

6.4.4 Szenario 3: Bestehende Infrastruktur ohne Netzsegmentierung

6.4.4.1 Beschreibung

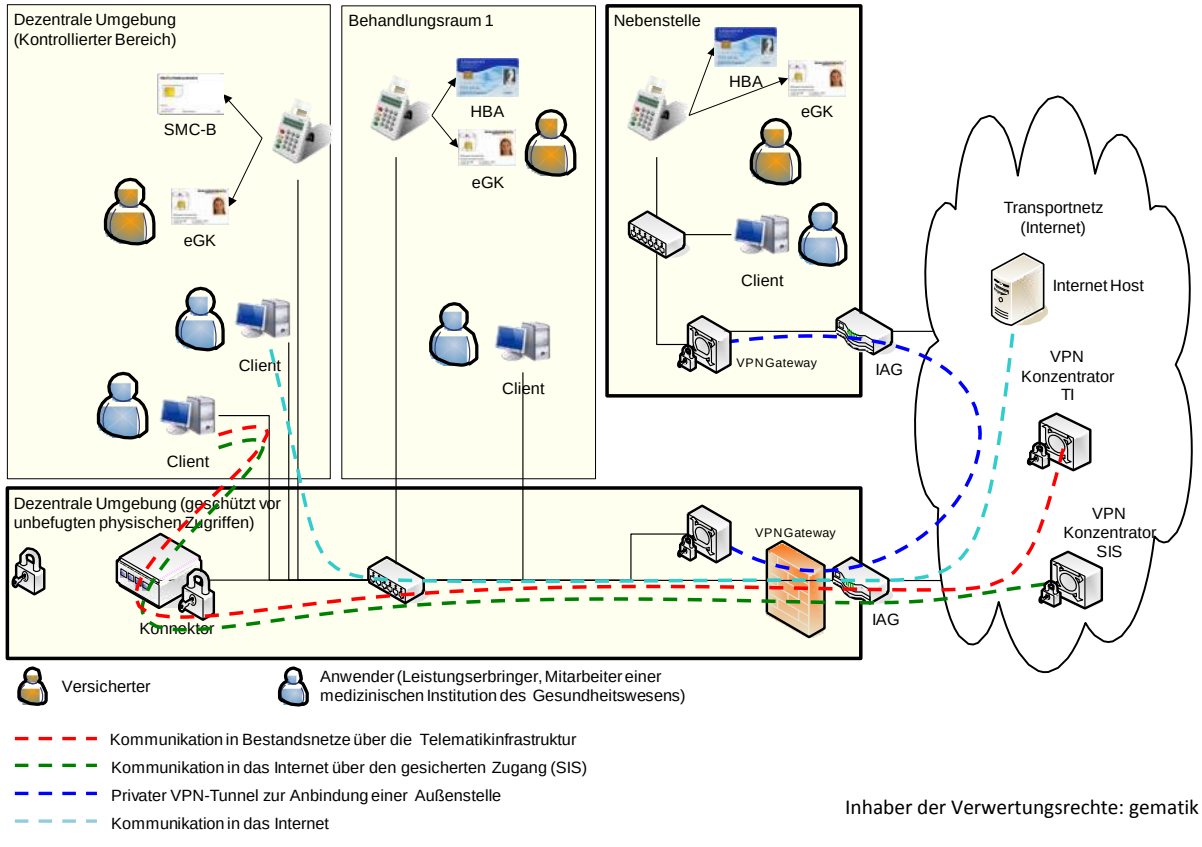


Abbildung 46: Szenario einer Integration in eine bestehende Infrastruktur

Wenn eine Infrastruktur im dezentralen Bereich bereits vorhanden ist, können die Produkte der TI, insbesondere der Modulare Konnektor, so in die Infrastruktur integriert werden, dass Bestandsanwendungen bereits erprobte Kommunikationswege weiter nutzen können.

Im dargestellten Beispiel existiert bereits eine Infrastruktur, die sowohl einen Internetzugang für die Arbeitsplätze ermöglicht, als auch eine Nebenstelle über VPN anbindet. In diesem Fall wird der Modulare Konnektor als zusätzliches Gerät an das bestehende Netzwerk angeschlossen und nutzt den bereits vorhandenen Internetanschluss zur Kommunikation mit der TI.

Hierzu wird der Anbindungsmodus *In Reihe* genutzt (siehe Kapitel 6.4.1.2).

Für die Clientsysteme muss in diesem Szenario je nach individuellem Anforderungsprofil entschieden werden, ob das jeweilige Clientsystem über die Telematikinfrastruktur kommunizieren können soll und den gesicherten Internetzugang (SIS) nutzen soll.

Wenn außer durch dem Modularen Konnektor weitere Anbindungen des lokalen Netzwerks an das Internet genutzt werden, kann dies zu erheblichen Sicherheitsrisiken führen. Alle Clientsysteme müssen entsprechende Sicherheitsmaßnahmen besitzen.

Wenn ein Clientsystem nicht über die Telematikinfrastruktur kommuniziert, bleibt der IAG als Default-Gateway dieses Clientsystems konfiguriert. In diesem Fall routet der IAG die eingehenden Pakete mit öffentlichen Zieladressen weiter in das Internet.

Wenn ein Clientsystem über die Telematikinfrastruktur kommunizieren oder den gesicherten Internetzugang (SIS) nutzen soll, muss der Modulare Konnektor als default-Gateway konfiguriert werden. In diesem Fall routet der Modulare Konnektor die eingehenden Pakete, die nicht für ihn bestimmt sind, entweder durch den VPN-Tunnel der TI über die Telematikinfrastruktur in ein angeschlossenes Bestandsnetz, oder durch den VPN-Tunnel zum SIS in das Internet. Falls kein sicherer Internetzugang konfiguriert ist, verwirft der Konnektor eingehende Pakete mit öffentlichen Zieladressen und schlägt ggf. per ICMP dem Clientsystem eine anderes Gateway (IAG) vor. Alternativ können die von den Clients benötigten Routing-Informationen manuell oder per DHCP konfiguriert werden.

6.4.4.2 Voraussetzung

Folgende Voraussetzungen müssen vor dem weiteren Vorgehen erfüllt sein:

- Der Modulare Konnektor ist kompatibel zur bestehenden Netzwerk-Infrastruktur.
- Die bestehende Infrastruktur verfügt über einen Internetzugang.
- An der Firewall sind die erforderlichen Ports und Protokolle für den Betrieb des Modularen Konnektors freigegeben (siehe Kapitel 5.1).
- Eine SMC-B und mehrere Kartenterminals sind verfügbar.

6.4.4.3 Vorgehensweise

So richten Sie dieses Szenario ein:

- Legen Sie die erforderlichen Mandanten und bestehenden Systeme des bestehenden Netzwerks an (siehe Kapitel 6.2.3).
- Konfigurieren Sie die Netzwerkeinstellungen (siehe Kapitel 6.2.2):
  - Konfigurieren Sie die LAN-Schnittstelle entsprechend dem bestehenden Netzwerk.

    Wenn ein DHCP-Server vorhanden ist, aktivieren Sie in den LAN-Einstellungen die Option **DHCP-Client benutzen**.
  - Deaktivieren Sie in den WAN-Einstellungen die Option **WAN-Schnittstelle Aktiv**.
  - Falls der sichere Internetzugang über den bestehenden IAG erfolgen soll, wählen Sie in den Internet-Modus **IAG**.
- Richten Sie die Verbindung zum VPN-Zugangsdienst ein (siehe Kapitel 6.2.6).
- Führen Sie die Freischaltung des Modularen Konnektors durch und aktivieren Sie die Verbindungen mit TI und gegebenenfalls SIS (siehe Kapitel 6.2.6.1).

6.4.4.4 Ergebnis

Nach der Installation sind folgende Ergebnisse erreicht:

- Die Produkte der Telematik sind mit geringstmöglichem Änderungsaufwand in die bestehende Netzwerk-Infrastruktur integriert. Bestehende Kommunikationswege können weiter genutzt werden.
- Für Clientsysteme kann je nach individuellen Anforderungsprofil entweder der sichere Internetzugang über den Modularen Konnektor genutzt werden oder der direkte Internetzugang über den bestehenden IAG.

6.4.5 Szenario 4: Bestehende Infrastruktur mit Netzsegmentierung

6.4.5.1 Beschreibung des Szenarios

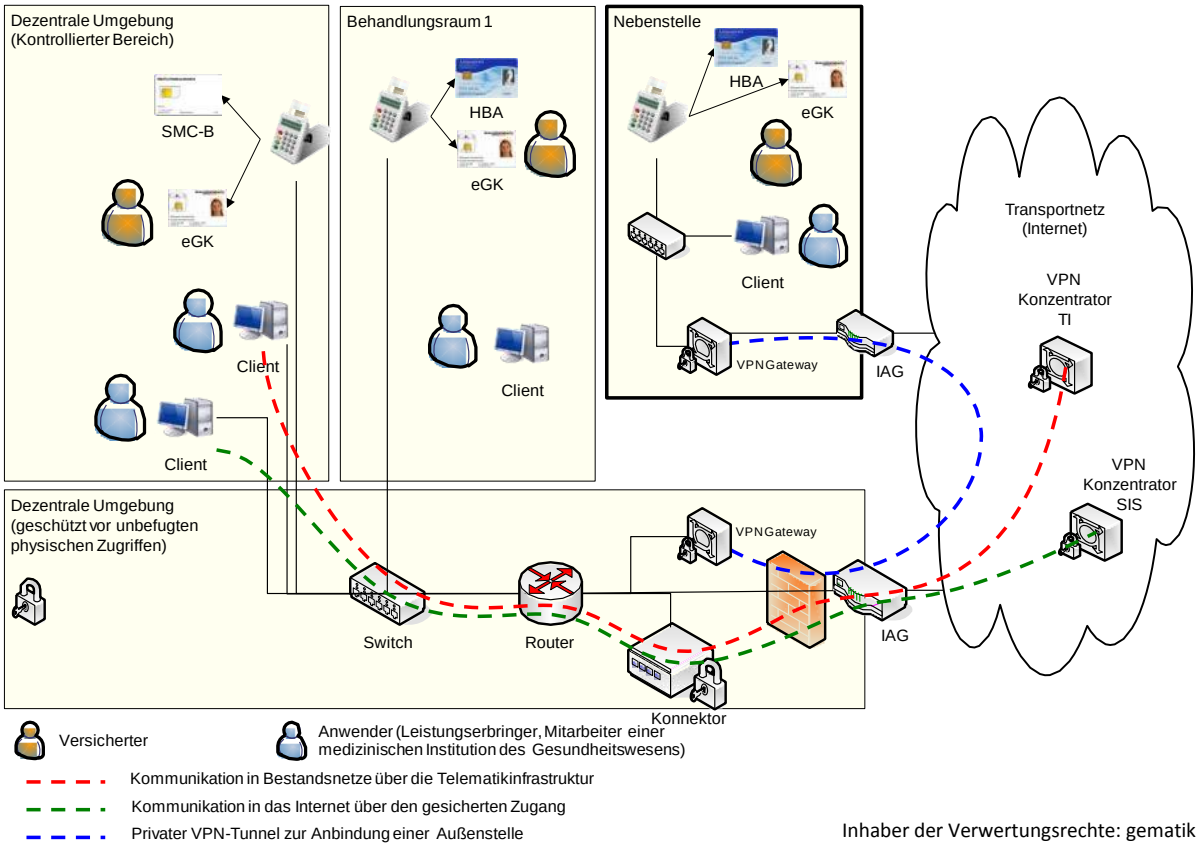


Abbildung 47: Szenario einer Integration in eine bestehende Infrastruktur mit existierendem Router

In diesem Szenario ist das bestehende Netzwerk, in das der Modulare Konnektor integriert werden soll, segmentiert und es wird ein dedizierte Router als Default-Gateway für die Clientsysteme genutzt.

In diesem Fall kann die Konfiguration der Clientsysteme unverändert bleiben und der Modulare Konnektor wird als zusätzliches Gerät in das Netzwerk integriert. Der Modulare Konnektor wird dem Router als Gateway für den sicheren Internetzugang und für den Zugang zu den an die TI angeschlossenen Bestandsnetzen bekanntgemacht.

Hierzu wird der Anbindungsmodus *In Reihe* genutzt (siehe Kapitel 6.4.1.2).

6.4.5.2 Voraussetzung

Folgende Voraussetzungen müssen vor dem weiteren Vorgehen erfüllt sein:

- Der Modulare Konnektor ist kompatibel zur bestehenden Netzwerk-Infrastruktur.
- An der Firewall sind die erforderlichen Ports und Protokolle für den Betrieb des Modularen Konnektors freigegeben (siehe Kapitel 5.1).
- Eine SMC-B und mehrere Kartenterminals sind verfügbar.

6.4.5.3 Vorgehensweise

So richten Sie dieses Szenario ein:

▶ Konfigurieren Sie im bestehenden Router den Modularen Konnektor als Gateway für den Internetzugang.

▶ Legen Sie die erforderlichen Mandanten und bestehenden Systeme des bestehenden Netzwerks an (siehe Kapitel 6.2.3).

▶ Konfigurieren Sie die Netzwerkeinstellungen (siehe Kapitel 6.2.2):

- Konfigurieren Sie die LAN-Schnittstelle entsprechend dem bestehenden Netzwerk.

  Wenn der vorhandene Router als DHCP-Server verwendet wird, aktivieren Sie in den LAN-Einstellungen die Option **DHCP-Client benutzen**.
- Konfigurieren Sie die WAN-Schnittstelle für die Verbindung mit dem IAG.

▶ Richten Sie die Verbindung zum VPN-Zugangsdienst ein (siehe Kapitel 6.2.6).

▶ Führen Sie die Freischaltung des Modularen Konnektors durch und aktivieren Sie die Verbindungen mit TI und gegebenenfalls SIS (siehe Kapitel 6.2.6.1).

6.4.5.4 Ergebnis

Nach der Installation sind folgende Ergebnisse erreicht:

- Die Produkte der Telematik sind mit geringstmöglichem Änderungsaufwand in die bestehende Netzwerk-Infrastruktur integriert. Bestehende Kommunikationswege können weiter genutzt werden.
- Die Default-Gateway-Konfiguration der Clientsysteme muss nicht geändert werden.

6.4.6 Szenario 5: Zentrale Verwendung des Heilberufsausweises

6.4.6.1 Beschreibung

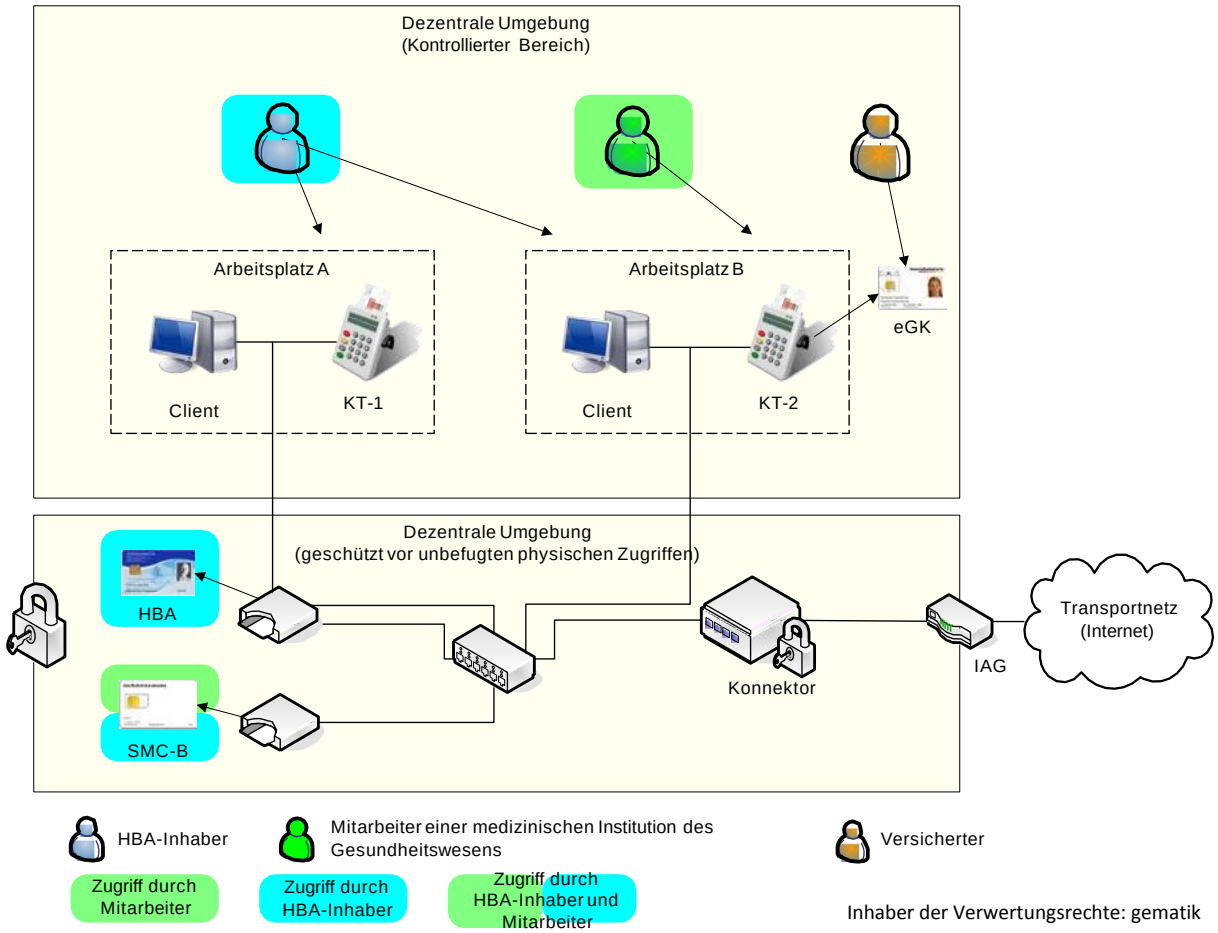


Abbildung 48: Szenario mit zentral gesteckten HBA und SMC-B

In diesem Szenario wird ein HBA nicht durch seinen Inhaber mitgeführt und am Arbeitsplatz in das lokale Kartenterminal gesteckt, sondern bleibt zentral in einem vor unbefugten physischen Zugriffen geschützten Kartenterminal permanent eingesteckt.

Der HBA-Inhaber greift von jedem konfigurierten Arbeitsplatz aus auf seinen HBA zu. Die Remote-PIN-Eingabe erfolgt unter Verwendung eines am jeweiligen Arbeitsplatz vorhandenen lokalen eHealth-Kartenterminals.

Der Zugriff auf eine zentral gesteckte SMC-B funktioniert analog.

6.4.6.2 Vorgehensweise

So richten Sie dieses Szenario ein:

- Stecken Sie HBA und SMC-B in ein Kartenterminal in der gesicherten Umgebung und stellen Sie den Schutz vor unbefugtem Zugriff sicher.
- Richten Sie den Modularen Konnektor entsprechend dem Standard-Szenario ein:
  - Mandanten
  - Clientsysteme
  - Arbeitsplätze mit zugewiesenen Kartenterminals
  - Kartenterminals für HBA und SMC-B in der gesicherten Umgebung
  - Netzwerkschnittstellen
- Weisen Sie den Arbeitsplätzen die lokalen Kartenterminals für die entfernte PIN-Eingabe zu (siehe Kapitel 6.2.3.4).

  Im abgebildeten Beispiel ist KT-1 dem Arbeitsplatz A zugeordnet und KT-2 dem Arbeitsplatz B.
- Weisen Sie den Mandanten die zentralen Kartenterminals in der gesicherten Umgebung zu (siehe Kapitel 6.2.3.5):

  Im Beispiel sind die zentralen Kartenterminals wie folgt zugeordnet:
  - Dem Arzt (HBA-Inhaber) sind beide zentralen Kartenterminals mit eingesteckter HBA und SMC-B zugeordnet.
  - Dem Praxismitarbeiter ist nur das Kartenterminal mit eingesteckter SMC-B zugeordnet.

6.4.6.3 Ergebnis

Nach der Installation sind folgende Ergebnisse erreicht:

- Der HBA muss nicht mehr durch seinen Inhaber mitgeführt werden.
- Die SMC-B muss nicht mehr unter ständiger Aufsicht eines Praxismitarbeiters stehen.

6.4.7 Szenario 6: Zentrales Primärsystem als Clientsystem

6.4.7.1 Beschreibung

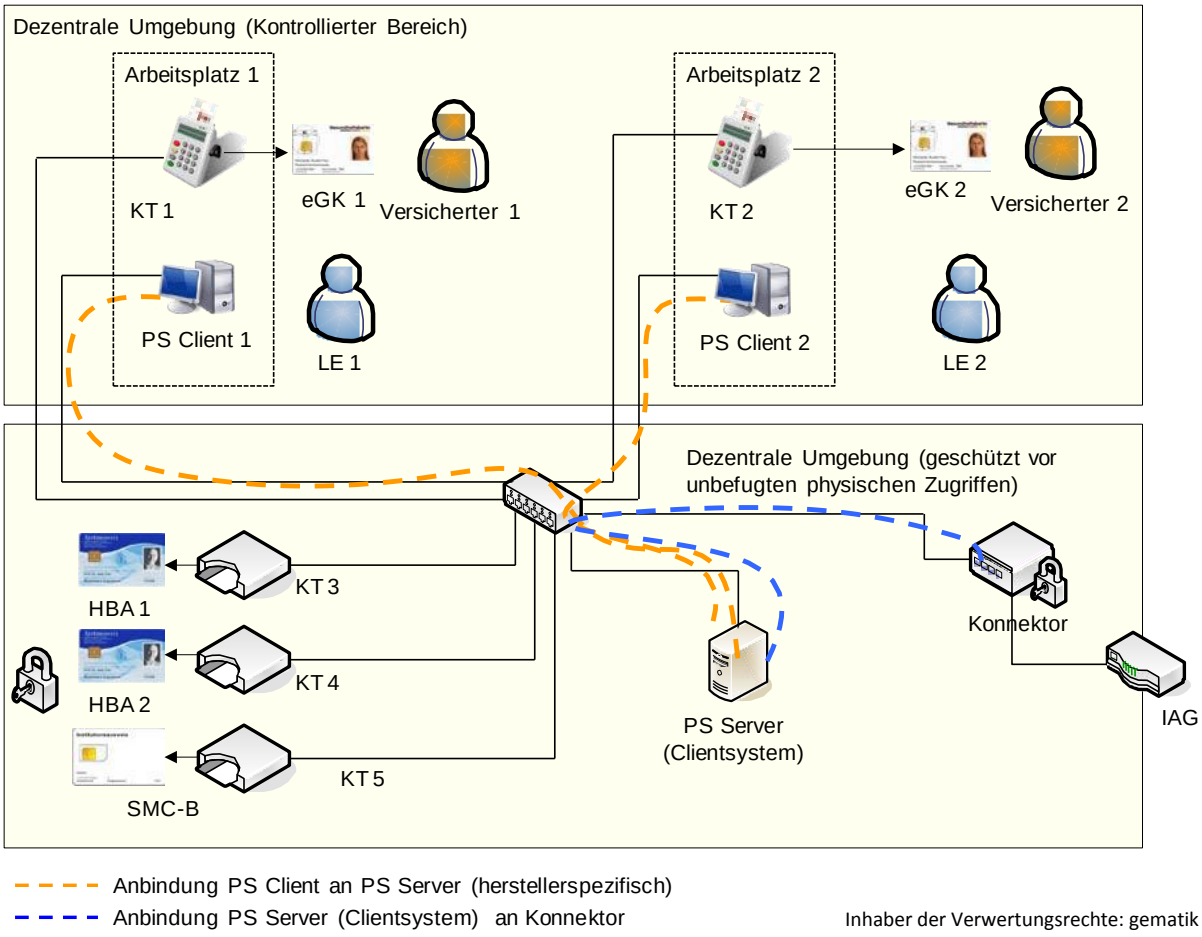


Abbildung 49: Szenario mit zentralem Primärsystem als Clientsystem

In diesem Netzwerkszenario ist das Primärsystem in einen Serveranteil *PS Server* und mehrere Clientanteile *PS Client* aufgeteilt. Die Anbindung zwischen dem *PS Server* und den *PS Clients* ist herstellerspezifisch. Das System *PS Server* ist als einziges mit dem Modularen Konnektor und der TI verbunden (z. B. als Terminalserver). Die LAN-Schnittstelle des Modularen Konnektors wird ausschließlich vom *PS Server* genutzt. Der *PS Server* übersetzt bei der Kommunikation die zugreifenden PS Clients auf die im Modularen Konnektor angelegten Arbeitsplätze.

Das Beispiel zeigt zwei Arbeitsplätze mit jeweils einem lokalen Kartenterminal für die eGK sowie in einer gesicherten Umgebung zentral eingesteckte SMC-B und HBAs. Alternativ können HBAs auch an lokalen Kartenterminals am jeweiligen Arbeitsplatz eingesteckt werden.

6.4.7.2 Voraussetzung

Folgende Voraussetzungen müssen erfüllt sein:

- SMC-B, HBA, eGK sind eingesteckt.
- Die Benutzer sind an den *PS Clients* angemeldet.

6.4.7.3 Vorgehensweise

So richten Sie dieses Szenario ein:

- Binden Sie alle Systeme in das lokale Netzwerk ein, u.a.:
  - *PS-Clients*
  - *PS-Server*
  - Kartenterminals
  - Modularer Konnektor
- Konfigurieren Sie das Primärsystem mit seinen Anteilen *PS Server* und den *PS Clients* passend zum Informationsmodell des Modularen Konnektors (herstellerspezifisch).
- Legen Sie die erforderlichen Mandanten und bestehenden Systeme des bestehenden Netzwerks an (siehe Kapitel 6.2.3).
- Verbinden Sie den *PS Server* ggf. über TLS (siehe Kapitel 6.5).
- Führen Sie das Pairing der Kartenterminals durch (siehe Kapitel 6.3.1).

6.4.7.4 Ergebnis

Nach der Installation sind folgende Ergebnisse erreicht:

- An den verschiedenen Arbeitsplätzen können für die definierten Mandaten und Benutzer Anwendungsfälle der TI initiiert werden.
- HBA-Inhaber müssen je nach Konfiguration entweder ihren HBA in der gesicherten Umgebung zentral einstecken und über das Remote-PIN-Verfahren zugreifen oder ihren HBA mit sich führen und in das lokale Kartenterminal des jeweils genutzten Arbeitsplatzes einstecken.

6.4.8 Szenario 7: Gemeinschaftspraxis mit mehreren Mandanten

6.4.8.1 Beschreibung

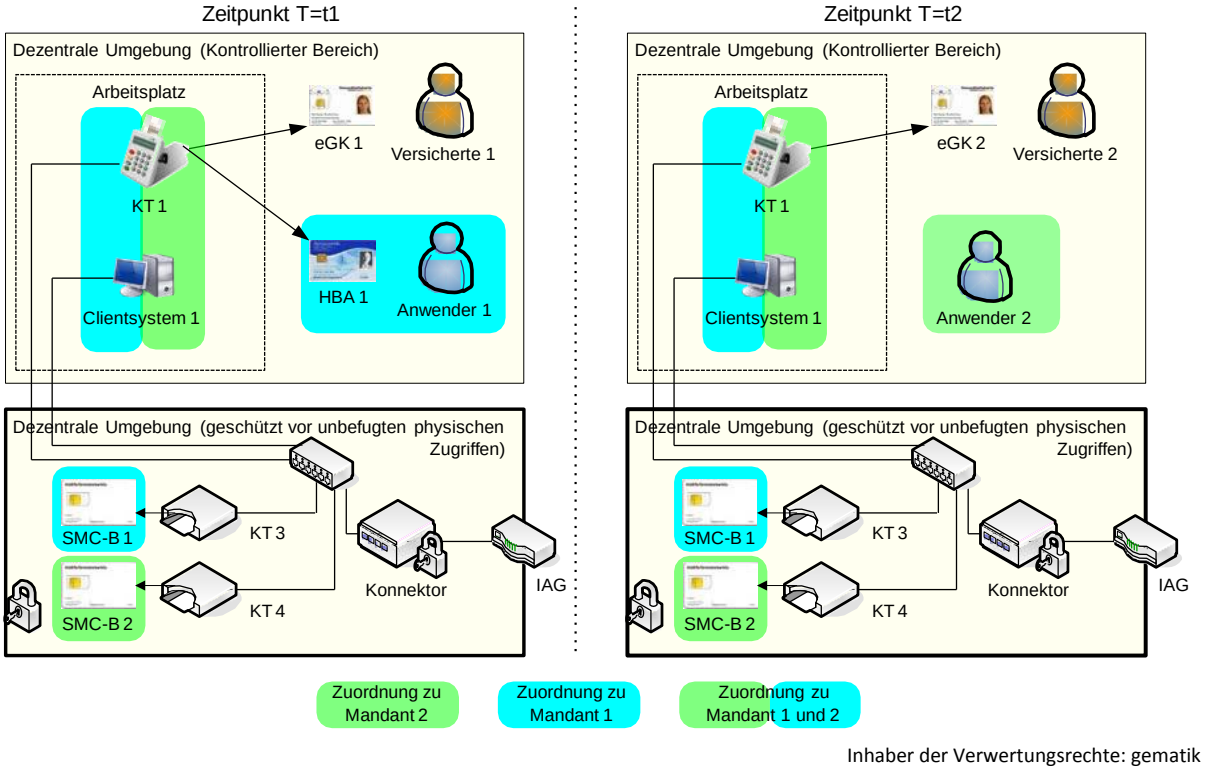


Abbildung 50: Szenario für den Zugriff

Dieses Szenario zeigt eine Netzwerkkonfiguration für zwei Mandanten, wobei jedem Mandanten eine eigene SMC-B zugeordnet ist. Die SMC-Bs befinden sich zusammen mit dem Modularen Konnektor zentral in einer gesicherten Umgebung. Alle Arbeitsplätze, Clientsysteme und Kartenterminals besitzen eine Zuordnung zu mindestens einem Mandanten, wobei Zuordnungen zu mehreren Mandaten möglich sind.

Das Beispiel zeigt einen Arbeitsplatz mit dem Clientsystem 1 und Kartenterminal 1, der zu unterschiedlichen Zeiten durch beide Mandanten verwendet wird:

- Zum Zeitpunkt T=t1 greift ein Benutzer 1 mit der HBA 1 im Kontext von Mandant 1 auf die TI zu, wobei der Versicherte 1 mit der eGK 1 am Anwendungsfall beteiligt ist.
- Zum Zeitpunkt T=t2 wird ein anderer Anwendungsfall im Kontext von Mandant 2 durch den Anwender 2 ohne HBA initiiert, wobei der Versicherte 2 mit der eGK 2 am Anwendungsfall beteiligt ist.

Das Clientsystem stellt hierbei den Bezug zum jeweiligen Mandanten und die Nutzer-Authentisierung sicher.

Alternativ können auch mehrere Mandanten eine Zuordnung zu einer einzelnen SMC-B besitzen. HBAs können in diesem Szenario auch in einer gesicherten Umgebung zentral gesteckt werden.

6.4.8.2 Voraussetzung

Folgende Voraussetzungen müssen erfüllt sein:

- SMC-B 1, SMC-B 2, HBA 1, eGK 1 und eGK 2 sind eingesteckt.
- Ein Benutzer mit Mandantenbezug ist am Clientsystem angemeldet.

6.4.8.3 Vorgehensweise

So richten Sie dieses Szenario ein:

- Binden Sie alle Systeme in das lokale Netzwerk ein, u.a.:
  - Clientsysteme
  - Kartenterminals
  - Modularer Konnektor
- Konfigurieren Sie die Clientsysteme passend zum Informationsmodell des Modularen Konnektors (herstellerspezifisch).
- Legen Sie die erforderlichen Mandanten und bestehenden Systeme des bestehenden Netzwerks an (siehe Kapitel 6.2.3):
  - Die Mandanten 1 und 2.
  - Ein Clientsystem für das Clientsystem 1.
  - Ein Arbeitsplatz für den Arbeitsplatz 1.
  - Die lokalen und entfernten Kartenterminals.
- Führen Sie das Pairing der Kartenterminals durch (siehe Kapitel 6.3.1).

6.4.8.4 Ergebnis

Nach der Installation sind folgende Ergebnisse erreicht:

- An den verschiedenen Arbeitsplätzen können für die Mandanten und Benutzer Anwendungsfälle der TI initiiert werden.
- HBA-Inhaber müssen je nach Konfiguration entweder ihren HBA in der gesicherten Umgebung zentral einstecken und über das Remote-PIN-Verfahren zugreifen oder ihren HBA mit sich führen und lokal in das Kartenterminal des jeweils genutzten Arbeitsplatzes einstecken.

6.5 TLS-Zertifikate für Clientsysteme verwalten

Für die Anbindung von Anwendungen auf Clientsystemen können TLS-Zertifikate generiert und im Browser importiert werden.

6.5.1 TLS-Zertifikat generieren und im Browser importieren

Um im Modularen Konnektor ein Zertifikat für ein Clientsystem zu generieren, gehen Sie wie folgt vor:

- Öffnen Sie im Menü **Praxis** den Bereich **Clientsysteme**.
- Falls nicht bereits erfolgt, erstellen Sie das Clientsystem (siehe Kapitel 6.2.3.3).
- Klicken Sie auf das gewünschte Clientsystem und wählen Sie **Zertifikat erstellen …**
- Geben Sie ein Passwort ein und bestätigen Sie die Eingabe.

  Das generierte Zertifikat wird mit der Namen des Clientsystems und der Erweiterung *.p12* angezeigt.
- Klicken Sie auf das Zertifikat und wählen Sie **Zertifikat herunterladen …** und speichern Sie das Zertifikat.

Der Import des Zertifikats geschieht wie in Kapitel 5.3.4 beschrieben.

6.5.2 TLS-Zertifikat in den Modularen Konnektor importieren

Diese Funktion darf nur dazu verwendet werden, um nach einem Werksreset ein zuvor vom Modularen Konnektor generiertes Zertifikat zu importieren.

Um ein Zertifikat für ein Clientsystem zu importieren, gehen Sie wie folgt vor:

- Öffnen Sie im Menü **Praxis** den Bereich **Clientsysteme**.
- Klicken Sie auf das gewünschte Clientsystem und wählen Sie **Zertifikat hochladen …**
- Klicken Sie **Datei auswählen**, um das Zertifikat zu suchen und geben Sie das zugehörige Passwort ein.

6.6 Werksreset und alternativer Werksreset

Bitte lesen Sie vor Durchführung des Werksreset das Kapitel 11 durch.

Mit dem Werksreset werden alle Parameter mit Ausnahme der aktuellen Firmware und Meldungen des Typs SECURITY zurückgesetzt.

Ein Werksreset setzt die Konfiguration unwiderruflich auf den Auslieferungszustand zurück. Alle konfigurierten Einstellungen gehen dabei verloren.

Nach dem Werksreset befindet sich das Gerät im Auslieferungszustand, die Anmeldung erfolgt analog der Erstanmeldung (siehe Kapitel 5.3).

Wenn der Werksreset bzw. der alternative Werksreset nicht erfolgreich abgeschlossen werden kann, wiederholen Sie diesen. Wenn auch dann der Werksreset bzw. alternative Werksreset nicht erfolgreich abgeschlossen werden kann, muss eine dauerhafte Außerbetriebnahme des Gerätes erfolgen (siehe Kapitel 11).

6.6.1 Werksreset durchführen

Der Werksreset wird über das Menü **System** im Bereich **Allgemein** durchgeführt (siehe Kapitel 6.2.5.1).

Der erfolgreiche Abschluss des Werksresets wird Ihnen am Gerät durch die Betriebsanzeigen (LEDs) angezeigt (siehe Tabelle 3). Danach wird der Modulare Konnektor heruntergefahren. Zum Einschalten des Modularen Konnektors siehe Kapitel 3.2.

6.6.2 Alternativen Login durchführen

Falls Sie sich nicht mehr an der Bedienoberfläche anmelden können weil das Passwort nicht mehr bekannt ist, können Sie einen alternativen Login durchführen.

Am Gehäuse befindet sich dazu ein gegen unbeabsichtigte Auslösung gesicherter Reset-Taster (siehe Kapitel 3.1.2).

Abbildung 51: Reset-Taster für alternativen Login und Werksreset

Beim alternativen Login werden alle Benutzerkonten zurückgesetzt. Benutzen Sie für die anschließende Anmeldung die initialen Zugangsdaten (siehe Kapitel 5.3) und legen Sie neue Benutzerkonten an.

Verbinden sie den Modularen Konnektor direkt über die LAN-Schnittstelle mit einem Clientsystem und gehen Sie wie folgt vor:

- Halten Sie den Reset-Taster mit einem geeigneten Gegenstand (z.B. Draht) 5 Sekunden lang gedrückt.

  Sobald der alternative Login beginnt, leuchten alle Anzeigen am Gerät auf.

- Rufen Sie die webbasierte Bedienoberfläche des Modularen Konnektors auf.

- Kontaktieren Sie den DVO und klicken Sie im Anmeldebildschirm unter **Weitere Optionen anzeigen …** auf **Alternativer Login (Reset) …**

  Es wird eine Zeichenfolge (Challange) angezeigt und zum Fortsetzen die Eingabe einer Antwort (Response) gefordert. Dies muss innerhalb einer Zeitdauer von 10 Minuten erfolgen, danach verfällt die Challenge und kann ggf. erneut generiert werden.

- Teilen Sie dem DVO die Challange-Zeichenfolge zusammen mit dem Geheimnis mit (siehe Kapitel 5.2). Das Geheimnis ist auf dem Sicherheitsbeiblatt *Aufstellung und Inbetriebnahme* notiert.

  Der DVO teilt Ihnen die Response-Zeichenfolge mit.

- Geben Sie die Response-Zeichenfolge an der Bedienoberfläche des Modularen Konnektors ein.

  Bei korrekter Eingabe wird anschließend das Passwort zurückgesetzt. Der Benutzer wird bei der nächsten Anmeldung dazu aufgefordert, ein neues Passwort einzugeben.

- Nach erfolgreichem Login können Sie nun bei Bedarf einen Werksreset über das Menü **System** im Bereich **Allgemein** durchführen (siehe Kapitel 6.2.5.1).

6.6.3 Alternativen Werksreset durchführen

Falls Sie sich nicht mehr an der Bedienoberfläche anmelden können, weil diese nicht mehr erreichbar ist, kann ein alternativer Werksreset über die REST-Schnittstelle des Modularen Konnektors durchgeführt werden. Um die REST-Schnittstelle des Modularen Konnektors direkt ansprechen zu können, benötigen Sie ein entsprechendes Tool (z.B. das Werkzeug cURL).

Dieses Vorgehen empfiehlt sich nur für technisch versierte Nutzer mit einem Vorwissen in Bezug auf die Verwendung von REST-Schnittstellen.

Verbinden sie den Modularen Konnektor direkt über die LAN-Schnittstelle mit einem Clientsystem und gehen Sie wie folgt vor:

- Halten Sie analog zum alternativen Login den Reset-Taster mit einem geeigneten Gegenstand (z.B. Draht) 5 Sekunden lang gedrückt.

  Sobald der alternative Werksreset beginnt, leuchten alle Anzeigen am Gerät auf. Es werden nun an der LAN Schnittstelle für den alternativen Werksreset notwendige Funktionen freigeschaltet.

- Kontaktieren Sie den DVO und senden Sie folgenden Aufruf:

  ```
  curl http://<ip address_lan>:18888/getchallenge
  ```

  In der Antwortnachricht ist eine Zeichenfolge (Challenge) bestehend aus 8 dezimalen Stellen enthalten.

- Teilen Sie dem DVO die Challange-Zeichenfolge zusammen mit dem Geheimnis mit (siehe Kapitel 5.2). Das Geheimnis ist auf dem Sicherheitsbeiblatt *Aufstellung und Inbetriebnahme* notiert.

  Der DVO teilt Ihnen die Response-Zeichenfolge mit.

  Dies muss innerhalb einer Zeitdauer von 10 Minuten erfolgen. Wird nicht innerhalb dieses Zeitraums eine passende Response-Zeichenfolge an den

Modularen Konnektor übertragen, dann wird der alternative Werksreset abgebrochen.

- Senden Sie folgenden Aufruf; dabei ist bei `<response>` die Response-Zeichenfolge des DVOs anzugeben:

```
curl -X POST http://<IP-Adresse-LAN>:18888/
checkresponse/_<response>_
```

Bei korrekter Eingabe führt der Modulare Konnektor anschließend den alternativen Werksreset durch.

Der erfolgreiche Abschluss des alternativen Werksresets wird Ihnen am Gerät durch die Betriebsanzeigen (LEDs) angezeigt (siehe Tabelle 3). Danach wird der Modulare Konnektor heruntergefahren. Zum Einschalten des Modularen Konnektors siehe Kapitel 3.2.

6.7 Werksreset zum Versand

Der Modulare Konnektor darf nur versendet werden, wenn zuvor der Werksreset zum Versand erfolgreich abgeschlossen wurde.

Bitte lesen Sie sich vor Durchführung des Werksreset zum Versand das Kapitel 11 (Dauerhafte Außerbetriebnahme) durch.

Mit dem Werksreset zum Versand wird ein notwendiges Geheimnis, das zum Entschlüsseln der Daten des kryptografisch gesicherten Speichers (siehe Kapitel 1.2.6) notwendig ist, überschrieben. Nach erfolgreichem Abschluss des Werksreset zum Versand ist weder ein Zugriff auf Protokolleinträge noch auf die zum Betrieb des Modularen Konnektors erforderliche Konfiguration möglich. Der Modulare Konnektor ist danach nicht mehr funktionsfähig.

Ein Werksreset zum Versand führt unwiderruflich dazu, dass der Modulare Konnektor nicht mehr funktionsfähig ist.

Wenn der Werksreset zum Versand nicht erfolgreich abgeschlossen werden kann, wiederholen Sie diesen. Wenn auch dann der Werksreset zum Versand nicht erfolgreich abgeschlossen werden kann, muss die dauerhafte Außerbetriebnahme des Gerätes erfolgen (siehe Kapitel 11).

6.7.1 Werksreset zum Versand durchführen

- Führen Sie den Werksreset zum Versand über das Menü **System** im Bereich **Allgemein** durch (siehe Kapitel 6.2.5.1).

Der erfolgreiche Abschluss des Werksresets zum Versand wird durch die Betriebsanzeigen (LEDs) am Gerät angezeigt (siehe Tabelle 3).

6.8 Werksreset für Fail Safe (feste IP)

Durch Fehler in der Einsatzumgebung des Modularen Konnektors (z.B. fehlende oder fehlerhaft konfigurierte DHCP-Server) sowie durch administrative Konfigurationsfehler kann nicht ausgeschlossen werden, dass der Modulare Konnektor über die LAN-Schnittstelle nicht mehr erreicht werden kann. Eine Administration ist dann nicht mehr möglich.

Ein Werksreset für Fail Safe (feste IP) setzt die Konfiguration des Netzkonnektors in den Auslieferungszustand zurück und weist der LAN-Schnittstelle eine definierte statische IP-Adresse (192.168.210.1) zu. Benutzerkonten, die Konfiguration des Anwendungskonnektors sowie alle Protokolleinträge bleiben erhalten.

Wenn der Werksreset für Fail Safe (feste IP) nicht erfolgreich abgeschlossen werden kann, wiederholen Sie diesen. Wenn auch dann der Werksreset für Fail Safe (feste IP) nicht erfolgreich abgeschlossen werden kann, muss die dauerhafte Außerbetriebnahme des Gerätes erfolgen (siehe Kapitel 11).

Nach einem erfolgreich abgeschlossenen Werksreset für Fail Safe (feste IP) ist die Konfiguration des Netzkonnektors erforderlich (ggf. über das Einspielen eines bestehenden Backups, siehe Kapitel 6.2.5.5.

6.8.1 Werksreset für Fail Safe (feste IP) durchführen

Zum Durchführen des Werksreset für Fail Safe (feste IP) muss das Gerät ausgeschaltet sein.

- Schalten Sie den Modularen Konnektor aus (siehe Kapitel 3.2).
- Halten Sie den Reset-Taster auf der Gehäuserückseite mit einem geeigneten Gegenstand (z.B. Draht) gedrückt.
- Schalten Sie den Modularen Konnektor ein (siehe Kapitel 3.2) während Sie den Reset-Taster weiter gedrückt halten. Sobald der Werksreset für Fail Safe (feste IP) beginnt, leuchten alle LEDs am Gerät auf.

- Sobald alle LEDs am Gerät leuchten, können Sie den Reset-Taster loslassen.

Der erfolgreiche Abschluss des Werksresets für Fail Safe (feste IP) wird durch die Betriebsanzeigen (LEDs) am Gerät angezeigt (siehe Tabelle 3).

6.9 Updates

Updates (Systemaktualisierungen) können für den Modularen Konnektor selbst sowie für andere Komponenten der TI wie z.B. Kartenleser durchgeführt werden. Dies kann online über die TI oder offline von einem Speichermedium aus erfolgen.

Updates können von Benutzern mit den Benutzerrollen **Super-Admin** und **Lokaler Admin** durchgeführt werden.

Ein Update enthält neben der Firmware auch Informationen über Firmwaregruppen. Ein Update von Informationen über Firmwaregruppen erfolgt nur, falls die Versionsstände jeweils aktueller sind als die im Modularen Konnektor bereits vorliegenden.

Führen Sie ein Update nur dann durch, wenn Sie ausreichend Informationen über dessen Inhalt haben.

TSL und CRL können über ein Update nicht aktualisiert werden. Dies kann durch das Hochladen der TSL und der Zertifikats-Sperrliste (CRL) erfolgen (siehe Kapitel 6.2.5.2).

6.9.1 Update online durchführen

Bei bestehender Anbindung an die TI haben Sie die Möglichkeit, die Firmware von Geräten über das Netzwerk zu aktualisieren. Es können wahlweise einzelne Geräte oder Gerätegruppen, beispielsweise Kartenterminals mit der identischen Firmware, aktualisiert werden.

6.9.1.1 Informationen über verfügbare Updates aktualisieren

Gehen Sie wie folgt vor:

- Öffnen Sie im Menü System den Bereich **Aktualisierungen**.
- Klicken Sie auf **Aktualisierungsinformationen aktualisieren**.

  Dadurch werden Updateinformationen angefragt und die Übersicht entsprechend auf den aktuellen Stand gebracht. Wenn ein Update verfügbar und dem Modularen Konnektor bekannt ist, wird ein entsprechender Indikator für das Gerät oder die Gerätegruppe angezeigt.

6.9.1.2 Update durchführen

Wenn ein Update für die verwendeten Komponenten vorliegt, gehen Sie wie folgt vor, um das Update durchzuführen.

Der Modulare Konnektor prüft vor der Durchführung eines Updates unter anderem, ob das Update authentisch ist. Falls nicht, führt der Modulare Konnektor das Update nicht durch.

- ▶ Öffnen Sie im Menü System den Bereich **Aktualisierungen**.
- ▶ Klicken Sie unter **Geräte** das gewünschte Gerät oder die Gerätegruppe an, um weitere Optionen anzuzeigen.
- ▶ Laden Sie das Update herunter:
  - Falls das Update nicht bereits automatisch heruntergeladen wurde, wird es unter **Verfügbare Aktualisierungen** aufgeführt; klicken Sie es an, um weitere Informationen anzuzeigen.

    Die zum Update gehörigen Releasenotes können in der Übersicht zum Update heruntergeladen werden. Mit **Herunterladen …** wird das Update auf den Modularen Konnektor übertragen.
  - Optional können verfügbare Updates automatisch heruntergeladen werden. Diese Funktion können Sie im Bereich **Aktualisierungen** unter **Einstellungen …** aktivieren.

  Das Update wird nach dem Herunterladen unter **Heruntergeladene Aktualisierungen** angezeigt und steht für die Installation bereit.
- ▶ Klicken Sie das Update an, um die Aktualisierung zu terminieren.

Vor der Terminierung des Update-Prozesses muss geprüft werden, dass die korrekte Update-Version ausgewählt wurde. Sie können die Version des Updates im Bereich Aktualisierungen unter Verfügbare Aktualisierungen bzw. Mögliche Downgrades ermitteln

Damit Kartenterminals aktualisiert werden können, muss für jedes Kartenterminal unter **Praxis** > **Terminals** > **Kartenterminal** > **Bearbeiten …** ein Administrator mit Benutzername und Passwort hinterlegt sein.

6.9.1.3 Update löschen

Sie können ein Update auch wieder löschen, wenn es nicht eingespielt werden soll. Gehen Sie dazu wie folgt vor:

- Öffnen Sie im Menü System den Bereich **Aktualisierungen**.
- Klicken Sie unter **Geräte** das gewünschte Gerät oder die Gerätegruppe an, um weitere Optionen anzuzeigen.
- Klicken Sie das Update an.

  Sofern der Statusindikator **Heruntergeladen** anzeigt, kann das Update über die entsprechende Option wieder vom Modularen Konnektor gelöscht werden.

6.9.2 Update offline durchführen

Updates können von einem Clientsystem direkt an den Modularen Konnektor übertragen werden, beispielsweise wenn keine Anbindung an die TI besteht.

Informationen über verfügbare Updates erhalten Sie auf der Webseite des Herstellers (www.secunet.com/de). Es dürfen nur von der gematik zugelassene Updates für den Modularen Konnektor eingespielt werden.

- Laden Sie das Update von der Webseite des Herstellers und speichern Sie es auf dem Clientsystem.
- Entpacken Sie das Update (ZIP-Archiv) auf dem Clientsystem.
- Verbinden Sie das Clientsystem mit der LAN-Schnittstelle des Modularen Konnektors.
- Melden Sie sich an der Bedienoberfläche des Modularen Konnektors an (siehe Kapitel 6.1.1)

Der Modulare Konnektor prüft vor der Durchführung eines Updates unter anderem, ob das Update authentisch ist. Falls nicht, führt der Modulare Konnektor das Update nicht durch.

- Öffnen Sie im Menü **System** den Bereich **Aktualisierungen**.
- Klicken Sie unter **Geräte** den **Konnektor** an, um weitere Optionen anzuzeigen.
- Klicken Sie **Aktualisierung hochladen**.

  Ein Suchdialog öffnet sich.
- Folgen Sie den Anweisungen in der Benutzeroberfläche.

- Das Update wird unter **Heruntergeladene Aktualisierungen** angezeigt und steht für die Installation bereit. Klicken Sie das Update an, um die Aktualisierung zu terminieren.

Vor der Terminierung des Update-Prozesses muss geprüft werden, dass die korrekte Update-Version ausgewählt wurde. Sie können die Version des Updates im Bereich Aktualisierungen unter Verfügbare Aktualisierungen bzw. Mögliche Downgrades ermitteln

6.10 Remote Management

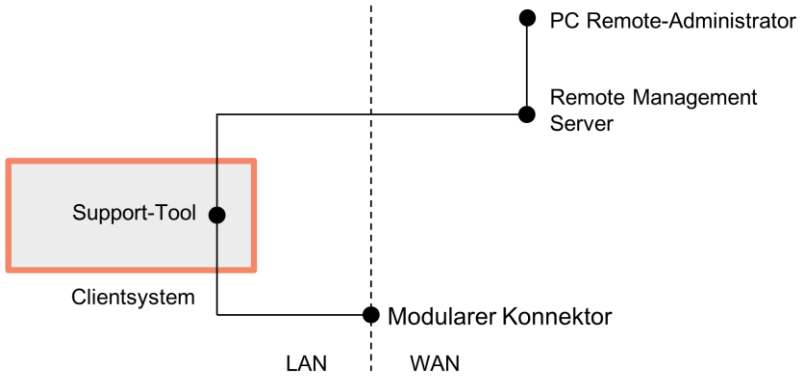


Abbildung 52: Benötigte Komponenten für das Remote Management

Abbildung 52 zeigt die für das Remote Management erforderlichen Komponenten. Das Remote Management des Modularen Konnektors erfolgt über die LAN-Schnittstelle. Der Remote-Administrator administriert den Modularen Konnektor über einen Remote Management Server. Für den Zugriff auf die LAN-Schnittstelle durch den Remote Management Server wird ein Support-Tool benötigt, das auf dem Clientsystem des Leistungserbringers installiert werden muss. Dieses unterstützt den Remote-Administrator beim Aufbau einer gesicherten TLS-Verbindung zum Modularen Konnektor.

Für die Einrichtung der Komponenten für das Remote Management wenden Sie sich an Ihren DVO. Dieser richtet den Modularen Konnektor, das Clientsystem mit Support-Tool und den Remote Management Server ein.

6.10.1 Support-Tool

Das Support-Tool ist eine Softwarekomponente, die auf dem Clientsystem des Leistungserbringers installiert ist und den Aufbau einer TLS-Verbindung zwischen Remote Management Server und Modularen Konnektor unterstützt. Dazu wird eine SSH-Verbindung zwischen Clientsystem und Remote Management Server aufgebaut, die es ermöglicht, eine direkte TLS-Verbindung vom Remote Management Server zur LAN-Schnittstelle des Modularen Konnektors einzurichten. Sollte es aus der Praxis oder Praxisgemeinschaft heraus wegen bestehender Firewall-Regeln technisch nicht erlaubt sein, eine SSH-Verbindung aufzubauen, kann man diese selbst in einen TLS-Kanal legen, der über einen erlaubten Port etabliert wird (SSH über TLS).

6.10.2 Betriebsmodi für das Remote Management

Je nach Internetmodus und Anbindungsmodus muss für Remote Management das Support-Tool entsprechend durch den Administrator des Clientsystems konfiguriert werden. Bitte sprechen Sie sich dazu mit dem Administrator des Clientsystems ab.

Internetmodus	**Über IAG**		**Über VPN-SIS**	
Konfiguration des Support Tool	SSH	SSH über TLS	SSH	SSH über TLS
Anbindungsmodus Parallel	Technisch möglich und empfohlen	Technisch möglich	Ggf. möglich (siehe Beschreibung)	Technisch möglich
Anbindungsmodus In Reihe	Technisch nicht möglich	Technisch nicht möglich	Ggf. möglich (siehe Beschreibung	Technisch möglich und empfohlen

Tabelle 12: Betriebsmodi für das Remote Management

6.10.2.1 Anbindungsmodus Parallel

Im Anbindungsmodus Parallel kann die Remote Management Verbindung unter Verwendung des SSH-Protokolls sowie SSH über TLS direkt über das IAG bzw. alternativ über den VPN-Konzentrator des SIS erfolgen.

Der VPN-Kanal des SIS ist nur in Verbindung mit einem etablierten VPN Kanal zur TI nutzbar. Weiterhin kann nicht ausgeschlossen werden, dass es technische Einschränkungen bzgl. der nutzbaren Protokolle bei Verwendung des VPN-Kanal des SIS geben wird, die eine Nutzung des SSH-Protokolls zur Etablierung des Transportkanals zwischen dem Clientsystem in der Praxis und dem Remote Management Server verhindern.

Für den Anbindungsmodus Parallel wird daher empfohlen, eine Verbindung über den IAG in der Support-Tool Konfiguration „SSH“ für Remote Management zu verwenden.

6.10.2.2 Anbindungsmodus In Reihe

Für den Anbindungsmodus In Reihe muss die Remote Management Verbindung über den VPN-Konzentrator des SIS erfolgen, da der Modulare Konnektor einen Zugriff auf Systeme im Internet nur über einen VPN-Kanal zum SIS erlaubt. Es kann nicht ausgeschlossen werden, dass es technische Einschränkungen bzgl. der nutzbaren Protokolle bei Verwendung des VPN-Kanals des SIS geben wird, die eine Nutzung des SSH-Protokolls zur Etablierung des Transportkanals zwischen Clientsystem und Remote Management Server verhindern.

Für den Anbindungsmodus In Reihe wird daher empfohlen, eine Verbindung über den VPN-SIS Konzentrator in der Support-Tool Konfiguration „SSH über TLS“ für Remote Management zu verwenden.

6.10.3 Remote Management Verbindung einrichten

Führen Sie für die Einrichtung von Remote Management am Modularen Konnektor die folgenden Schritte durch. Die Schritte richten sich an einen lokalen Administrator des Konnektors und an den Remote-Administrator:

1. Auf dem Clientsystem des Leistungserbringers muss das Support-Tool installiert und entsprechend des verwendeten Betriebsmodus des Modularen Konnektors konfiguriert werden. Wenden Sie sich dazu bitte an den Administrator des Clientsystems.
2. Richten Sie den Modularen Konnektor für Remote Management ein. Die Nutzung des Remote-Managements muss über die Management-Oberfläche des Konnektors erlaubt und aktiviert werden (siehe Kapitel 6.2.5.1).

   Nach Aktivierung akzeptiert der Modulare Konnektor Remote Management Verbindungen auf der LAN-Schnittstelle.
3. Legen Sie einen Benutzer mit der Rolle *Remote-Admin* an (siehe Kapitel 6.2.1).

   Der Administrator des Konnektors muss das initiale Passwort dem Remote-Administrator auf sicherem Wege mitteilen. Beachten Sie dazu die Warnhinweise in Kapitel 6.2.1.
4. Validieren Sie das TLS-Zertifikat des Modularen Konnektors und Importieren Sie das Zertifikat in den Browser des Remote Management Servers. Führen Sie dazu die in Kapitel 5.3.4 beschriebenen Schritte durch.
5. Unter Verwendung des Support-Tools kann nun eine Verbindung zum Remote Management Server entweder über den VPN-Kanal des SIS oder das Internet-Access-Gateway (IAG) aufgebaut werden. Der Zugriff vom Remote Management Server über das Clientsystem auf den Remote Management Endpunkt des Modularen Konnektors erfolgt dann über eine TLS-Verbindung auf die Managementschnittstelle des Konnektors.

6. Der Remote-Administrator greift über den Remote Management Server auf das mit HTTPS gesicherte Management-Interface des Konnektors zu. Dazu kann ein auf dem Remote Management Server installiertes Tool verwendet werden.

   An der lokalen LAN-Schnittstelle des Modularen Konnektors ist das Interface für Remote Management unter folgender IP-Adresse erreichbar:

   ```
   https://<IP-Adresse des Modularen Konnektors>:8501/management
   ```

7. Nach erfolgreicher Verbindung zum Modularen Konnektor erscheint der Anmeldedialog und fordert den Remote-Administrator zur Eingabe von Benutzernamen und Passwort auf. Bei der Erstanmeldung des Remote-Administrators muss das in Schritt 3 erstellte initiale Passwort verwendet werden. Anschließend wird der Remote-Administrator aufgefordert, ein neues Passwort zu erstellen. Beachten Sie dabei die Hinweise zu Passwörtern in Kapitel 4.2.

8. Der Remote-Administrator kann nun den Modularen Konnektor vom Remote Management Server administrieren. Beachten Sie dabei die eingeschränkten Rechte des Remote-Administrators (siehe Kapitel 6.2.1.3)

Falls der Remote-Administrator bei der ersten Anmeldung nicht zum Passwortwechsel aufgefordert wird, darf dieses Benutzerkonto nicht verwendet werden. Der Administrator des Konnektors muss in diesem Fall umgehend das Benutzerkonto löschen und Schritt 3 wiederholen. Zudem sind sämtliche Einstellungen im Konnektor zu prüfen.

Eine Remote Management Verbindung darf nur über Port 8501 aufgebaut werden. Die Schnittstelle für lokale Administration darf nur mit einem Clientsystem im lokalen Netzwerk verwendet werden.

7 Hinweise für Praxispersonal

Wenden Sie sich bei Fragen oder bei Störungen an den Dienstleister vor Ort (DVO). Die Kontaktdaten finden Sie im Sicherheitsbeiblatt *Empfang und Prüfung*.

Beachten Sie die Hinweise zur Reinigung in Kapitel 8.1 und die Hinweise zur Dauerhafte Außerbetriebnahme in Kapitel 10. Versenden Sie den Modularen Konnektor nicht selbstständig über einen Lieferdienst, sondern kontaktieren Sie für jeden Transport den DVO.

7.1 Gerät ein- /ausschalten

- Einschalten: An/Aus-Taster kurz drücken.
- Ausschalten: An/Aus-Taster innerhalb von 3 Sekunden zweimal drücken (Schutz vor unabsichtlicher Betätigung).

Abbildung 53: Gerät ein-/ausschalten

Beachten Sie:

- **Nehmen Sie bei einer Beschädigung des Gehäuses oder des Netzteils den Modularen Konnektor bzw. das Netzteil sofort außer Betrieb.**
- **Schalten Sie den Modularen Konnektor durch die zweimalige kurze Betätigung des An/Aus-Tasters aus. Das Trennen der Spannungsversorgung im Betrieb kann das Gerät irreparabel beschädigen.**

Heiße Oberfläche

Verbrennungsgefahr bei Berührung im Betrieb erhitzter Gehäuseteile

Nach dem Abschalten des Geräts mindestens fünf Minuten warten, bis das Gehäuse berührt wird. Dieses gilt für den Betrieb sowohl mit wie auch ohne die optional verfügbare Wandhalterung.

7.2 Betriebsanzeigen

Über die Betriebsanzeigen an der Geräteoberseite erhalten Sie Rückmeldung über den aktuellen Gerätezustand. Für eine detaillierte Beschreibung siehe Kapitel 3.1.1.

Bezeichnung	Funktion
Power	Gerät Ein-/Ausgeschaltet
System	Gerät Betriebsbereit
VPN TI	Verbindung zur Telematikinfrastruktur
VPN SIS	Verbindung zum Sicheren Internet-Dienst
Service	Fehler/Warnung Blinken deutet Fehler mit hoher Priorität an. Kontaktieren Sie den Administrator.
Update	Systemaktualisierung ist verfügbar
Remote	Remote Management ist aktiviert Blinken deutet eine gerade durchgeführte Administrierung per Remote Management an.

Tabelle 13: Betriebsanzeigen (Kurzübersicht)

7.3 Sicherheitssiegel und Gehäuse prüfen

Das Gehäuse des Modularen Konnektors ist mit Sicherheitssiegeln versehen.

- ▶ Prüfen Sie die Sicherheitssiegel und das Gehäuse (siehe Kapitel 0).
- ▶ Bringen Sie keine Aufkleber oder sonstige Anbauteile am Gehäuse an.

8 Wartung und Pflege

8.1 Reinigung

Zur Reinigung genügt es, bei Bedarf das Gehäuse mit einem fusselfreien Tuch oder Antistatik-Tuch trocken abzuwischen.

- Verwenden Sie keine Reinigungs- oder Lösungsmittel.
- Achten Sie darauf, bei der Reinigung die Netzwerkverbindungen und die Stromversorgung nicht zu unterbrechen und den Ein-/Aus-Taster nicht zu betätigen.

Die Sicherheitssiegel sind von der Pflege auszunehmen, da die Sicherheitssiegel bzw. die Siegelmerkmale zerstört werden könnten und das Gerät dann nicht mehr benutzt werden darf (siehe Kapitel 9).

Heiße Oberfläche

Verbrennungsgefahr bei Berührung im Betrieb erhitzter Gehäuseteile

Nach dem Abschalten des Geräts mindestens fünf Minuten warten, bis das Gehäuse berührt wird. Dieses gilt für den Betrieb sowohl mit wie auch ohne die optional verfügbare Wandhalterung.

8.2 Sicherheitssiegel und Gehäuse prüfen

Prüfen Sie die Sicherheitssiegel und das Gehäuse des Modularen Konnektors in regelmäßigen Zeitabständen und bei Verdacht von Manipulationen (z.B. nach einem Einbruch). Informationen zum Prüfen der Sicherheitssiegel und des Gehäuses finden Sie in Kapitel 2.4.

Nur Personen mit berechtigtem Zugriff zum Modularen Konnektor dürfen die Sicherheitssiegel prüfen.

Das Gerät darf bei beschädigten Sicherheitssiegeln oder beschädigtem Gehäuse auf keinen Fall weiterverwendet werden.

Wenn beschädigte Sicherheitssiegel oder ein beschädigtes Gehäuse festgestellt werden, befolgen Sie die Hinweise zur Meldung von Verlust oder Kompromittierung in Kapitel 9.

8.3 Systemzeit synchronisieren

Synchronisieren Sie im Offline-Betrieb mindestens einmal jährlich die Systemzeit (siehe Kapitel 6.2.5.3).

9 Meldung von Verlust oder Kompromittierung

Wenn der Modulare Konnektor gestohlen wird, abhandenkommt oder in irgendeiner Form kompromittiert erscheint (z.B. nicht mehr am sicheren Aufstellungsort, Sicherheitssiegel oder Gehäuse beschädigt oder unsachgemäß geöffnet), ist umgehend der Dienstleister vor Ort (DVO) zu informieren.

Ein gestohlenes oder abhandengekommenes Gerät wird anhand der Seriennummer identifiziert, die bei Empfang auf dem Sicherheitsbeiblatt *Empfang und Prüfung* notiert wurde (siehe Kapitel 2.3).

10 Meldung von möglichen Schwachstellen

Sie können mögliche Schwachstellen des Modularen Konnektors über den DVO an den Hersteller melden. Eine mögliche Schwachstelle liegt beispielsweise vor, wenn sich der Modulare Konnektor anders verhält, als im Handbuch beschrieben.

Wenden Sie sich in diesem Fall an den DVO. Die Kontaktdaten des DVO finden Sie auf dem Sicherheitsbeiblatt „Empfang und Prüfung“. Teilen Sie dem DVO folgende Informationen mit, die Sie auf dem Typenschild finden:

- Hersteller
- Modell
- Version

Beschreiben Sie dem DVO darüber hinaus das Verhalten des Modularen Konnektors, welches eine mögliche Schwachstelle anzeigt. Der DVO leitet diese Meldung zwecks Klärung an den Hersteller weiter.

11 Dauerhafte Außerbetriebnahme

Die dauerhafte Außerbetriebnahme des Modularen Konnektors kann z.B. aufgrund eines Austausches mit einem neuen Gerät, Wechsel des Anbieters oder einem Defekt erfolgen.

Ein Modularer Konnektor, der nicht über den Prozess der sicheren Auslieferung bezogen wurde, darf nicht in der TI in Betrieb genommen werden.

Die Außerbetriebnahme ist vom DVO durchzuführen. Hierzu ist die Seriennummer anzugeben, die dem Typenschild des Geräts oder dem Sicherheitsbeiblatt *Empfang und Prüfung* entnommen werden kann. Der DVO veranlasst die Sperrung des Geräts.

Dies umfasst:

- Die Deregistrierung beim VPN-Zugangsdienst
- Den Sperrauftrag beim Hersteller
- Die Durchführung eines Werksresets (siehe Kapitel 6.6) oder Werksresets zum Versand (siehe Kapitel 6.7)
- Die Rücksendung an den Hersteller durch den DVO nach erfolgreichem Abschluss eines Werksresets zum Versand

Verschicken Sie das Gerät nicht eigenständig.

Wenn der Werksreset zum Versand nicht erfolgreich abgeschlossen werden kann, muss das Gerät vor der Rücksendung an den Hersteller vom DVO vor Ort geöffnet und die gSMC-Ks entfernt werden. Das Gerät muss bis zum Entfernen der gSMC-Ks sicher gelagert werden. Lagern Sie das Gerät nur in Bereichen, die ausschließlich autorisierten Personen zugänglich sind (z.B. in einem Bereich, in dem Betäubungsmittel aufbewahrt werden).

12 Anhang

12.1 Unterstützte Netzwerkprotokolle

12.1.1 TCP/IP

Der Modulare Konnektor unterstützt TCP-/IPv4-Pakete gemäß RFC 793 /RFC 791.

Der Modulare Konnektor prüft mittels Paketfilter eingehende und ausgehende Pakete und leitet nur Pakete weiter, die dem konfigurierten Regelwerk entsprechen. Regelverletzungen werden protokolliert.

12.1.2 VPN

Während des VPN-Verbindungsaufbaus mit der TI werden die für die kryptographische Absicherung des VPN-Nutzdatentransfers benötigten Sitzungsschlüssel bzw. das Schlüsselmaterial unter Verwendung des Internet Key Exchange (IKEv2) Protokolls gemäß RFC 7296 ausgetauscht. Traffic Flow Confidentiality wird vom Modularen Konnektor nicht unterstützt.

Der Modulare Konnektor fordert das Zertifikat des VPN-Konzentrators an (siehe Kapitel 1.2.1) und führt folgende Prüfungen durch:

- Zeitliche Gültigkeit
- Sperrzustand
- Gültigkeit des Ausstellerzertifikats (Prüfung anhand TSL)

Parameter:

- Die Parameter zur Festlegung des Tunnel-Modes des IPSEC-Protokolls werden gemäß RFC 4302 Abschnitt 3.1.2 verwendet.
- Die Parameter von Encapsulating Security Payload (ESP) werden gemäß RFC 4303 Abschnitt 2 verwendet.

Meldungen werden gemäß RFC 7296 generiert. Der Modulare Konnektor unterstützt IP Compression gemäß RFC 3173.

12.1.3 TLS

Der Modulare Konnektor nutzt TLS zur sicheren Kommunikation mit den Clientsystemen, z.B. zur Administration von Terminals. Dazu wird ein TLS-Kanal gemäß RFC 5246 und RFC 4346 aufgebaut.

Parameter

Der Modulare Konnektor sendet folgende Parameter:

Für die Nachrichten ClientHello (RFC 5246 Abschnitt 7.4.1.2, RFC 4346 Abschnitt 7.4.1.2) und ServerHello (RFC 5246 Abschnitt 7.4.1.3, RFC 4346 Abschnitt 7.4.1.3):

- ProtocolVersion
- Random
- Session ID
- Cipher suites

  Folgende Werte werden unterstützt:
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, and
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- Compression methods (RFC 3749 Abschnitt 2)
- Signature algorithms extensions (RFC 5246 Abschnitt 7.4.1.4)

Für die Nachricht Certificate (RFC 5246 Abschnitt 7.4.2, RFC 4346 Abschnitt 7.4.2) verwendet der Modulare Konnektor ein eigenes Zertifikat für die Authentisierung.

Für die Nachricht CertificateRequest (RFC 5246 Abschnitt 7.4.4), RFC 4346 Abschnitt 7.4.4) sendet der Modulare Konnektor folgende Parameter:

- certificate_types
- supported_signature_algorithms
- certificate_authorities

TLS-Handshake

Der Modulare Konnektor führt einen TLS-Handshake gemäß RFC 4346 Abschnitt 7.3, Fig. 1 (TLS 1.1) oder gemäß RFC 5246 Abschnitt 7.3 Fig. 1 TLS 1.2 durch.

Verwendete Nachrichten:

- ClientHello (RFC 5246 Abschnitt 7.4.1.2, RFC 4346 Abschnitt 7.4.1.2); für den Wert protocol version wird vom Modularen Konnektor für TLS 1.2 immer der Wert (3, 3) gesetzt.
- ServerHello (RFC 5246 Abschnitt 7.4.1.3, RFC 4346 Abschnitt 7.4.1.3); für den Wert protocol version werden vom Modularen Konnektor die Werte (3, 2) für TLS 1.1 und (3, 3) für TLS 1.2 gesetzt.
- Certificate (RFC 5246 Abschnitt 7.4.2 , RFC 4346 Abschnitt 7.4.2)
- ServerKeyExchange (RFC 5246 Abschnitt 7.4.3, RFC 4346 Abschnitt 7.4.3, RFC 4492 Abschnitt 2.4)
- CertificateRequest (RFC 5246 Abschnitt 7.4.4, RFC 4346 Abschnitt 7.4.4)
- ServerHelloDone (RFC 5246 Abschnitt 7.4.5, RFC 4346 Abschnitt 7.4.5)
- ClientKeyExchange (RFC 5246 Abschnitt 7.4.7, RFC 4346 Abschnitt 7.4.7)
- CertificateVerify (RFC 5246 Abschnitt 7.4.8, RFC 4346 Abschnitt 7.4.8)
- Finished (RFC 5246 Abschnitt 7.4.9, RFC 4346 Abschnitt 7.4.9)
- ChangeCipherSpec (RFC 5246 Abschnitt 7.1, RFC 4346 Abschnitt 7.1)

Meldungen

Der Modulare Konnektor generiert Meldungen (alert messages) entsprechend RFC 4346 Abschnitt 7.2 (TLS 1.1) und RFC 5246 Abschnitt 7.2 (TLS 1.2).

12.1.4 NTP

NTP-Server

Der Modulare Konnektor nutzt NTP für die Bereitstellung von Zeitinformationen für die angeschlossenen Clientsysteme.

Der Modulare Konnektor unterstützt Anfragen von Clientsystemen über ein UDP-Paket mit einem Aufbau gemäß RFC 5905 Abschnitt 7 (mode 3, client mode) und versendet als Antwort ein UDP-Paket mit einem Aufbau gemäß RFC 5905 Abschnitt 7 (mode 4, server mode). Die NTP-Parameter werden gemäß RFC 5905 Abschnitt 9.1 verwendet.

Der NTP-Dienst des Modularen Konnektors arbeitet im Modus secondary server gemäß RFC 5905 Abschnitt 2. Fehlermeldungen werden gemäß RFC 5905 Abschnitt 9.2 generiert.

NTP-Client

Der Modulare Konnektor gleicht seine Systemzeit über eine per NTP angebundene externe Zeitquelle in der zentralen Telematikinfrastruktur ab. Bei zu großer Zeitabweichung aktualisiert der Modulare Konnektor die Systemzeit nicht und stellt die Funktionalität ein; in diesem Fall ist eine manuelle Prüfung erforderlich.

Des Weiteren kann der Administrator die Systemzeit über die Wartungsschnittstelle festlegen.

Die Parameter werden gemäß RFC 5905 Appendix A verwendet. Meldungen werden gemäß RFC 5905 Abschnitt 9.2 generiert.

12.1.5 DHCP

DHCP-Server

Der Modulare Konnektor stellt einen DHCP-Server bereit, um die angeschlossenen Clientsysteme in das lokale Netzwerk einzubinden. Kommunikation, Parameter und Meldungen werden dabei gemäß RFC 2131 Abschnitt 4.3 unterstützt.

DHCP-Client

Der Modulare Konnektor kann einen bestehenden DHCP-Server für die Anbindung zum lokalen Netzwerk nutzen.

Kommunikation, Parameter und Meldungen werden dabei gemäß RFC 2131 Abschnitt 4.4 unterstützt. Der Modulare Konnektor wertet folgende Parameter aus:

- IP-Adresse und Subnetzmaske
- Default Gateway
- DNS-Server

Weitere Parameter werden nicht berücksichtigt.

12.1.6 DNS

Der Modulare Konnektor bietet einen Domain Name Server (DNS) zur Auflösung von DNS-Anfragen von Clientsystemen im lokalen Netzwerk und unterstützt DNS-Abfragen gemäß RFC 1035. Die Anfragen werden nach DNSSEC-Protokoll gemäß RFC 2535 validiert.

12.1.7 Aktualisierung von TSL und CRL

Die TSL wird vom Modularen Konnektor über die Verbindung zur TI aktualisiert. Dazu werden folgende Übertragungsprotokolle unterstützt:

- HTTP nach RFC 7230
- HTTP over TLS (HTTPS) nach RFC 2818

Die CRL wird beim VPN-Verbindungsaufbau aktualisiert. Dazu werden folgende Übertragungsprotokolle unterstützt:

- HTTP nach RFC 7230
- HTTP over TLS (HTTPS) nach RFC 2818
- LDAP nach RFC 2251

Parameter

- Die Parameter des HTTP-Headers werden gemäß RFC 7230 Abschnitt 3.2 verwendet.
- Die Parameter für den TLS-Handshake werden gemäß RFC 2246 Abschnitt 7.4 verwendet.
- Die Parameter des LDAP-Protokolls werden gemäß RFC 2251 Abschnitt 4 verwendet.

Meldungen

- HTTP-Meldungen werden gemäß RFC 7231 Abschnitte 6.5 und 6.6 generiert.
- TLS-Meldungen werden gemäß RFC 2246 Abschnitt 7.2 generiert.
- LDAP-Meldungen werden gemäß RFC 2251 Abschnitt 4.1.10 generiert.

Bei der Aktualisierung der CRL werden folgende Meldungen verwendet:

- NK_IKE_CRL_RETRIEVE

  Die unter der URL erwartete CRL konnte nicht über den transparenten CRL-Cache des Management-Service bezogen werden.
- NK_IKE_CRL_DECODE64

  Die von dem Management-Service gelieferte CRL ist nicht base64-codiert (Kommunikationsfehler).

- NK_IKE_CRL_PARSE

  Die von dem Management-Service gelieferte CRL kann nicht eingelesen werden.

TSL und CRL können bei Bedarf auch über die Managementschnittstelle importiert werden (siehe Kapitel 6.2.5.2).

12.2 Standardwerte bei Auslieferung

12.2.1 Menü „Benutzer“

Wert	Standardeinstellung	Wertebereich
Ablaufzeit Passwörter	120 Tage	-

12.2.2 Menü „Netzwerk“

12.2.2.1 Bereich „Allgemein“

Wert	Standardeinstellung	Wertebereich
Leistungsumfang Online	Aus	An/Aus
Internet Modus	SIS	SIS, IAG, Keiner
Intranet Routing Modus	Redirect	Redirect, Block
Service Timeout	60 Sekunden	-
Bandbreitenbeschränkung	Mbit/s	-

12.2.2.2 Bereich „LAN“

Wert	Standardeinstellung	Wertebereich
DHCP-Client benutzen	An	An/Aus
LAN-Netzwerk	-	-
LAN-seitige IP-Paketlänge (MTU)	1500	-
Weitere Parameter	-	-

12.2.2.3 Bereich „WAN“

Wert	Standardeinstellung	Wertebereich
DHCP-Client benutzen	An	An/Aus
WAN-Netzwerk	-	-
IP-Adresse des Standard-Gateway	-	-
WAN-seitige IP-Paketlänge (MTU)	1500	-
Weitere Parameter	-	-

12.2.2.4 Bereich „DHCP-Server“

Wert	Standardeinstellung	Wertebereich
DHCP-Server aktiv	Aus	An/Aus
IP-Netzwerk	-	-
Broadcast-Adresse	-	-
Addressbereich Untergrenze	-	-
Addressbereich Obergrenze	-	-

12.2.2.5 Bereich „DNS“

Wert	Standardeinstellung	Wertebereich
DNS-Server für das Transportnetz	-	-
DNS-Server zur Namensauf-lösung von Namensräumen in der Einsatzumgebung	-	-
DNS-Domain Zugangsdienst	-	-

Wert	Standardeinstellung	Wertebereich
DNS-Domain Einsatzumge-bung	-	-
DNSSEC Trustanchor Internet	-	-

12.2.2.6 „Bereich Erweiterte TLS-Einstellungen“

Wert	Standardeinstellung	Wertebereich
Permanente Verbindungen	1	0 - 10
Maximale Verbindungen	1	0 - 20
Lebensdauer Verbindungen	10 Sekunden	Mind. 1 Sekunde
Aufräum-Intervall	5 Minuten	Mind. 1 Sekunde
Aufräum-Threads	1	Mind. 1
Wartedauer vor Verbindungserstellung	100 Millisekunden	1 - 500 Millisekunden
Wartedauer vor Verbindungsabbau	10 Millisekunden	1 - 100 Millisekunden
Timeout Verbindungserstel-lung	5 Sekunden	1 Millisekunde – 10 Sekunden

12.2.3 Menü „Praxis“

12.2.3.1 Bereich „Karten“

Wert	Standardeinstellung	Wertebereich
Timeout für Kartenoperationen	60 Sekunden	-
Zertifikatsprüf-Intervall	1 Tage	0 - 365 Tage
Zertifikats-Ablauf Warnung	90 Tage	0 - 180 Tage (0 = keine Warnung)

12.2.3.2 Bereich „Terminals“

Wert	Standardeinstellung	Wertebereich
Service Discovery Port	4742	-
Service Discovery Timeout	3 Sekunden	-
Service Discovery Zyklus	10 Minuten	-
Service Announcement Port	4742	-
Keep-Alive Intervall	10 Sekunden	3 - 10 Sekunden
Anzahl Keep-Alive Versuche	3	3 - 10
TLS Handshake Timeout	10 Sekunden	1 - 60 Sekunden

12.2.3.3 Bereich „Clientsysteme“

Wert	Standardeinstellung	Wertebereich
Authentifizierung	Zertifikat	Keine Authentifizierung, Zertifikat, Benutzername/Passwort
Verwendung TLS	An	An/Aus
Ungesicherter Zugriff auf Dienstverzeichnisdienst	An	An/Aus
Von Konnektor zu Clientsystem		
Maximale Anzahl Fehlversuche	3	-

12.2.4 Menü „Diagnose“

Wert	Standardeinstellung	Wertebereich
Erfolgreiche Kryptooperationen protokollieren	Aus	An/Aus
Protokollierungslevel	Warning	Debug, Info, Warnung, Fehler, Fatal
Vorhaltedauer	180 Tage	10 - 365 Tage
Performance-Log	Aus	An/Aus
VSDM		
Protokollierungslevel	Warning	Debug, Info, Warnung, Fehler, Fatal
Vorhaltedauer	180 Tage	10 - 365 Tage
Performance-Log	Aus	An/Aus

12.2.5 Menü „System“

12.2.5.1 Bereich „Allgemein“

Wert	Standardeinstellung	Wertebereich
Name	-	-
Remote-Management erlauben	Aus	An/Aus
Remote-Management aktivieren	Aus	An/Aus
Standalone-Szenario	Aus	An/Aus

12.2.5.2 Bereich „Zertifikate“

Wert	Standardeinstellung	Wertebereich
Timeout Download TSL-Datei	10 Sekunden	1 - 60 Sekunden
Default Grace Period TSL	30 Tage	1 - 30 Tage
Default Grace Period OCSP für nonQES	10 Minuten	0 - 20 Minuten
Timeout OCSP-Abfragen (Prüfung nonQES-Zertifikate)	10 Sekunden	1 - 120 Sekunden
Missbrauch-Erkennung Einstellungen		
Zertifikat prüfen (Versuche)	401	0 - 9999 (0 = deaktiviert)

12.2.5.3 Bereich „Zeit“

Wert	Standardeinstellung	Wertebereich
Land (Zeitzonenfilter)	Deutschland	Auswahlliste
Zeitzone	Europe/Berlin (CET)	Auswahlliste
Zeitsynchronisierung		
Warnung nach	30 Tage	-
Fehlerzustand nach	50 Tage	-
Maximale Zeitabweichung	3600 Sekunden	-

12.2.5.4 Bereich „Aktualisierungen“

Wert	Standardeinstellung	Wertebereich
Automatische Prüfung	An	An/Aus
Automatischer Download	Aus	An/Aus
Erprobung-Update-Pakete anzeigen	Aus	An/Aus
Neue Bestandsnetze automatisch aktivieren	An	An/Aus

12.2.6 Menü „VPN“

12.2.6.1 Bereich „VPN-Zugangsdienst“

Wert	Standardeinstellung	Wertebereich
hash&URL Verfahren für Zertifikatsaustausch	Aus	An/Aus
Internet-Key-Exchange (IKE)		
Keep Alive Modus	An	An/Aus
Keep Alive Intervall	30 Sekunden	-
Keep Alive Versuche	3	-
Network Address Translation (NAT)		
Keep Alive Modus	An	An/Aus
Keep Alive Intervall	20 Sekunden	-
VPN Inaktivität		
Timeout Mode	Aus	An/Aus
Timeout	600 Sekunden	-

Wert	Standardeinstellung	Wertebereich
Maximale Paketgrößen (MTU)		
SIS	1418 Byte	576 - 8076 Byte
TI	1418 Byte	576 - 8076 Byte
IPSec		
Auswertung der Sequenz-nummern	An	An/Aus
Fenstergröße Sequenznum-mern	32	-
Keying Versuche	1	0 - 999 Sekunden
IKE Rekeying Zeit	84500 Sekunden	77760 - 86400 Sekunden
IKE Reauthentifizierung Zeit	544320 Sekunden	544320 - 604800 Sekunden
IKE Lebenszeit	1800 Sekunden	600 - 8640 Sekunden
IKE Random Zeit	1800 Sekunden	600 - 14400 Sekunden
IPSec Rekeying Zeit	77760 Sekunden	77760 - 85800 Sekunden
IPSec Lebenszeit	79560 Sekunden	78360 - 86400 Sekunden
IPSec Random Zeit	1800 Sekunden	600 - 8640 Sekunden

Für die in der folgenden Tabelle angegebenen Einstellungen kann durch setzten des Query-Parameter strict auf den Wert false der erlaubte Wertebereich ausgeweitet werden (Der Default-Wert für diesen Parameter ist true). Erweitern Sie dazu die URL in der Adresszeile des Browsers um den Zusatz **?strict=false**. Wird ein Wert aus dem erweiterten Wertebereich gewählt, erscheint ein Warnhinweis auf der Oberfläche. Der Administrator muss die Warnung durch das Setzen eines Schalters (Umschaltfläche am Seitenanfang) explizit bestätigen, bevor die Werte übernommen werden können.

Wert	Erweiterter Wertebereich
IKE Rekeying Zeit	0 oder 300 - 86400 Sekunden

Wert	Erweiterter Wertebereich
IKE Reauthentifizierung Zeit	0 oder 600 - 604800 Sekunden
IKE Lebenszeit	600 - 14400 Sekunden
IKE Random Zeit	600 - 14400 Sekunden
IPSec Rekeying Zeit	0 oder 300 - 85800 Sekunden

Der Konnektor darf nicht mit Einstellungen im erweiterten Wertebereich betrieben werden.

12.2.7 Menü „Fachmodule“

12.2.7.1 Bereich „VSDM“

Wert	Standardeinstellung	Wertebereich
Intermediär-Servicename	_vsdmintermediaer._tcp	
Max. Dauer TI Offline	0 (keine Prüfung)	-
Timeout Aufrufe TI	10 Sekunden	-
Timeout für Read VSD	30 Sekunden	-
Automatische Onlineprüfung VSD	Aus	An/Aus
Kontext für Auto UpdateVSD	-	
Verschlüsselung der Prüfungsnachweise (VSDM-PNW-Key)	-	16 Zeichen

12.3 Meldungen

Der Modulare Konnektor erzeugt im Betrieb Meldungen und protokolliert diese im Protokollspeicher. Sie können über die Bedienoberfläche ausgelesen werden (siehe Kapitel 6.2.4).

Meldungen des Typs SECURITY mit dem Level FATAL, die seit dem letzten Einloggen des Administrators ausgegeben wurden, werden zusätzlich auf der Bedienoberfläche in der Ansicht **Home** angezeigt (siehe Kapitel 6.1.2). Bei Meldungen mit hoher Priorität blinkt am Gehäuse zudem die Betriebsanzeige **Service**.

12.3.1 Übersicht der Meldungen

Legende:

Code	Fehler-ID (dient als Referenz der gematik)
Beschreibung	Kurze Zusammenfassung
Typ	Je nach Typ werden Meldungen in verschiedene Logdateien geschrieben (SECURITY,TECHNICAL).
Level	Einstufung nach Schwere des Vorfalls (FATAL, ERROR, WARNING, INFO)
PVS	Gekennzeichnete Meldungen werden zusätzlich an die Praxisverwaltungssoftware gemeldet.
Fehlerbehebung/ Weitere Angaben für PVS	Anleitung zur Behebung, falls möglich. Wenden sie sich bei Fragen an den DVO.

Für Meldungen, die zusätzlich an die Praxisverwaltungssoftware gemeldet werden, wird in der Spalte „Fehlerbehebung/Weitere Angaben PVS“ angegeben, wie der Leistungserbringer einen Fehler beheben kann. Alle anderen Meldungen werden nur in den Protokollspeicher geschrieben. Diese Meldungen wertet nur der DVO (nicht der Leistungserbringer) aus.

Beachten Sie zusätzlich folgende Hinweise:

- Wenn der Protokollspeicher gefüllt ist, werden ältere Meldungen überschrieben.
- Protokolldaten werden im gesicherten Dateisystem des Modularen Konnektors abgelegt. Bei einem Werksreset werden Meldungen des Typs SECURITY nicht gelöscht.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
101	Kartenfehler	SECURITY	FATAL	PVS	Eine Karte reagiert nicht oder nicht wie vorgesehen. ▶ Stecken Sie die Karte erneut ein und wiederholen Sie den Vorgang. Wenn das Problem nur bei einer bestimmten Karte auftritt, ist möglicherweise die Karte defekt. ▶ Verweisen Sie den Versicherten mit den entsprechenden Fehlerinformationen an seine Krankenkasse, wenn der Fehler bei einer eGK auftritt. ▶ Es kann das Ersatzverfahren gemäß Bundesmantelvertrag angewendet werden. Wenn der Fehler häufiger bzw. bei verschiedenen eGKs auftritt, wenden Sie sich an den DVO. Fehlerbehebung durch DVO: ▶ Wenn der Fehler bei verschiedenen eGKs auftritt, überprüfen Sie anhand der Protokolle des Modularen Konnektors bzw. des Fachmoduls VSDM, in welchem Kontext der Fehler auftritt bzw. von welcher Krankenkasse und von welchem Fachdienstbetreiber die betroffenen Karten stammen. ▶ Stellen Sie für den betroffenen Fachdienstbetreiber ein Ticket im TI ITSM ein.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
102	Gerätefehler	SECURITY	FATAL	PVS	Hardware reagiert nicht oder nicht wie vorgesehen. ▶ Wenden Sie sich an den DVO.
103	Softwarefehler	SECURITY	FATAL	PVS	Hardware reagiert nicht oder nicht wie vorgesehen. ▶ Wenden Sie sich an den DVO.
104	Fachmodul reagiert nicht	SECURITY	FATAL	PVS	Hardware reagiert nicht oder nicht wie vorgesehen. ▶ Wenden Sie sich an den DVO.
105	eGK nicht lesbar	SECURITY	FATAL	PVS	Ein technisches Problem ist beim Auslesen der eGK aufgetreten. ▶ Stecken Sie die Karte erneut und versuchen Sie sie einzulesen. ▶ Wenn das Problem nur bei einer bestimmten Karte auftritt, ist ggf. die Karte defekt. Verweisen Sie den Versicherten mit den entsprechenden Fehlerinformationen an seine Krankenkasse. Es kann das Ersatzverfahren gemäß Bundesmantelvertrag angewendet werden. ▶ Wenn der Fehler häufiger bzw. bei verschiedenen eGKs auftritt, wenden Sie sich an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
106	Zertifikat auf eGK ungültig	SECURITY	FATAL	PVS	Die eGK ist kein gültiger Leistungsanspruchsnachweis. ▶ Fragen Sie den Versicherten, ob er in der Zwischenzeit eine neuere eGK von der Krankenkasse zugeschickt bekommen hat. Wenn der Versicherte keine aktuellere eGK besitzt, ist gemäß BMV-Ä Anlage 4a Anhang 1 Kap. 2.1. bzw. §8 BMV-Z und §12 EKVZ vorzugehen oder eine Ersatzbescheinigung von der Krankenkasse anzufordern. ▶ Verweisen Sie den Versicherten mit Verweis auf die Meldung (z.B. Zertifikat ungültig) an seine Krankenkasse.
107	Zertifikat auf eGK ungültig	SECURITY	FATAL	PVS	Die eGK ist kein gültiger Leistungsanspruchsnachweis. ▶ Fragen Sie den Versicherten, ob er in der Zwischenzeit eine neuere eGK von der Krankenkasse zugeschickt bekommen hat. Wenn der Versicherte keine aktuellere eGK besitzt, ist gemäß BMV-Ä Anlage 4a Anhang 1 Kap. 2.1. bzw. §8 BMV-Z und §12 EKVZ vorzugehen oder eine Ersatzbescheinigung von der Krankenkasse anzufordern. ▶ Verweisen Sie den Versicherten mit Verweis auf die Meldung (z.B. Zertifikat ungültig) an seine Krankenkasse.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
108	Protokollierung auf eGK nicht möglich	TECHNICAL	FATAL	PVS	Ein technisches Problem ist beim Schreiben auf die eGK aufgetreten. ▶ Stecken Sie die Karte erneut und wiederholen Sie den Vorgang. ▶ Wenn das Problem nur bei einer bestimmten Karte auftritt, ist ggf. die Karte defekt. Verweisen Sie den Versicherten mit den entsprechenden Fehlerinformationen an seine Krankenkasse. Es kann das Ersatzverfahren gemäß Bundesmantelvertrag angewendet werden. ▶ Wenn der Fehler häufiger bzw. bei verschiedenen eGKs auftritt, wenden Sie sich an den DVO.
109	Fehler beim Lesen von Daten der SMC-B/HBA	TECHNICAL	FATAL	PVS	Ein technisches Problem ist beim Lesen der SMC-B aufgetreten. ▶ Stecken Sie die Karte erneut und wiederholen Sie die Freischaltung. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
110	Fehler beim Verarbeiten von Befehlen auf der eGK	TECHNICAL	FATAL	PVS	Ein technisches Problem ist beim Lesen der eGK aufgetreten. ▶ Stecken Sie die Karte erneut und wiederholen Sie den Vorgang. ▶ Wenn das Problem nur bei einer bestimmten Karte auftritt, ist ggf. die Karte defekt. Verweisen Sie den Versicherten mit den entsprechenden Fehlerinformationen an seine Krankenkasse. Es kann das Ersatzverfahren gemäß Bundesmantelvertrag angewendet werden. ▶ Wenn der Fehler häufiger bzw. bei verschiedenen eGKs auftritt, wenden Sie sich an den DVO.
111	Fehler beim Lesen von Daten der eGK	TECHNICAL	FATAL	PVS	Ein technisches Problem ist beim Lesen der eGK aufgetreten. ▶ Stecken Sie die Karte erneut und wiederholen Sie den Vorgang. ▶ Wenn das Problem nur bei einer bestimmten Karte auftritt, ist ggf. die Karte defekt. Verweisen Sie den Versicherten mit den entsprechenden Fehlerinformationen an seine Krankenkasse. Es kann das Ersatzverfahren gemäß Bundesmantelvertrag angewendet werden. ▶ Wenn der Fehler häufiger bzw. bei verschiedenen eGKs auftritt, wenden Sie sich an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
112	Fehler beim Schreiben von Daten der eGK	TECHNICAL	FATAL	PVS	Ein technisches Problem ist beim Schreiben auf die eGK aufgetreten. ▶ Stecken Sie die Karte erneut und wiederholen Sie die Freischaltung. ▶ Wenn das Problem nur bei einer bestimmten Karte auftritt, ist ggf. die Karte defekt. Verweisen Sie den Versicherten mit den entsprechenden Fehlerinformationen an seine Krankenkasse. Es kann das Ersatzverfahren gemäß Bundesmantelvertrag angewendet werden. ▶ Wenn der Fehler häufiger bzw. bei verschiedenen eGKs auftritt, wenden Sie sich an den DVO.
113	Leseversuch von veralteter eGK	TECHNICAL	FATAL	PVS	Die eGK ist kein gültiger Leistungsanspruchsnachweis. ▶ Fragen Sie den Versicherten, ob er in der Zwischenzeit eine neuere eGK von der Krankenkasse zugeschickt bekommen hat. Wenn der Versicherte keine aktuellere eGK besitzt, ist gemäß BMV-Ä Anlage 4a Anhang 1 Kap. 2.1. bzw. §8 BMV-Z und §12 EKVZ vorzugehen oder eine Ersatzbescheinigung von der Krankenkasse anzufordern. ▶ Verweisen Sie den Versicherten mit Verweis auf die Meldung (veraltete eGK) an seine Krankenkasse.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
114	Gesundheits-anwendung auf eGK gesperrt	TECHNICAL	FATAL	PVS	Die eGK ist kein gültiger Leistungsanspruchsnachweis. ▶ Fragen Sie den Versicherten, ob er in der Zwischenzeit eine neuere eGK von der Krankenkasse zugeschickt bekommen hat. Wenn der Versicherte keine aktuellere eGK besitzt, ist gemäß BMV-Ä Anlage 4a Anhang 1 Kap. 2.1. bzw. §8 BMV-Z und §12 EKVZ vorzugehen oder eine Ersatzbescheinigung von der Krankenkasse anzufordern. ▶ Verweisen Sie den Versicherten mit Verweis auf die Meldung (Gesundheitsanwendung gesperrt) an seine Krankenkasse.
500	Internal Server Error	TECHNICAL	FATAL	PVS	Bei der Onlineprüfung der eGK ist ein Fehler aufgetreten. Der Server ist in einen unerwarteten Zustand geraten, der die weitere Verarbeitung der Nachricht verhindert. Die eGK ist ein gültiger Leistungsanspruchsnachweis. VSD können mit Prüfungsnachweis 3 („Aktualisierung VSD auf eGK technisch nicht möglich") eingelesen werden. ▶ Wenn der Fehler über einen längeren Zeitraum häufiger auftritt, wenden Sie sich an den DVO.
1001	Es liegt keine gültige TSL vor	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
1002	Zertifikate lassen sich nicht extrahieren	TECHNICAL	ERROR		-
1003	Mehr als ein markierter V-Anker gefunden	SECURITY	ERROR		-
1004	TSL-Signer-CA lässt sich nicht extrahieren	TECHNICAL	ERROR		-
1005	Element <TSL> nicht vorhanden	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
1006	Nachricht zurückgewiesen. Die Nachricht wurde an einen für diese Anfrage nicht zuständigen Fachdienst weitergeleitet.	SECURITY	FATAL	PVS	Bei der Onlineprüfung der eGK ist ein Fehler des Fachdienstes aufgetreten. Die Überprüfung der Lokalisierungsinformationen innerhalb eines Fachdienstes führt zu dem Ergebnis, dass die Nachricht an den falschen Empfänger (Fachdienst) gesendet wurde. Die eGK ist ein gültiger Leistungsanspruchsnachweis. VSD können mit dem/einem Prüfungsnachweis 3 („Aktualisierung VSD auf eGK technisch nicht möglich") eingelesen werden. ▶ Wenn der Fehler über einen längeren Zeitraum häufiger und bei verschiedenen eGKs auftritt, wenden Sie sich an den DVO.
1006	TSL-Downloadadressen wiederholt nicht erreichbar	TECHNICAL	ERROR		-
1007	Vergleich der ID und SequenceNumber entspricht nicht der Vergleichsvariante 6a	SECURITY	ERROR		-
1008	Die TSL ist nicht mehr aktuell	SECURITY	WARNING		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
1009	Überschreitung des Elements NextUpdate um TSL-Grace-Period	SECURITY	WARNING		-
1011	Die aufgerufene Komponente ist nicht verfügbar	TECHNICAL	FATAL	PVS	Bei der Onlineprüfung der eGK ist ein Fehler des Fachdienstes aufgetreten. Bei der Verarbeitung einer Nachricht wurde festgestellt, dass für die Verarbeitung dieser Nachricht eine benötigte Komponente nicht verfügbar ist. Die eGK ist gültiger ein Leistungsanspruchsnachweis. VSD können mit Prüfungsnachweis 3 („Aktualisierung VSD auf eGK technisch nicht möglich") eingelesen werden. ▶ Wenn der Fehler über einen längeren Zeitraum häufiger auftritt, wenden Sie sich an den DVO.
1011	TSL-Datei nicht wellformed	TECHNICAL	ERROR		-
1012	Schemata der TSL-Datei nicht korrekt	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
1013	Signatur ist nicht gültig	SECURITY	ERROR		-
1014	Die zu dieser ConversationID zugehörige Fachdienst-Session ist abgelaufen.	TECHNICAL	FATAL	PVS	Bei der Onlineprüfung der eGK ist ein Fehler des Fachdienstes aufgetreten. Die eGK ist ein gültiger Leistungsanspruchsnachweis. VSD können mit Prüfungsnachweis 3 („Aktualisierung VSD auf eGK technisch nicht möglich") eingelesen werden.
1016	KeyUsage ist nicht vorhanden bzw. entspricht nicht der vorgesehenen KeyUsage	SECURITY	ERROR		-
1017	ExtendedKeyUsage entspricht nicht der vorgesehenen ExtendedKeyUsage	SECURITY	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
1018	Zertifikatstyp-OID stimmt nicht überein	SECURITY	ERROR		-
1019	Zertifikat nicht lesbar	TECHNICAL	ERROR		-
1021	Zertifikat ist zeitlich nicht gültig	SECURITY	ERROR		-
1023	AuthorityKeyIdentifier des EndEntityZertifikats von SubjectKeyIdentifier des CA-Zertifikats unterschiedlich	SECURITY	ERROR		-
1024	Zertifikats-Signatur ist mathematisch nicht gültig.	SECURITY	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
1026	Das Element <ServiceSupplyPoint> konnte nicht gefunden werden.	TECHNICAL	ERROR		-
1027	CA kann nicht in den TSL-Informationen ermittelt werden. Keine Adresse hinterlegt.	TECHNICAL	ERROR		-
1028	Die OCSP-Prüfung konnte nicht durchgeführt werden (1) TOLERATE_OCSP_FAILURE=true	TECHNICAL	WARNING		-
1029	Die OCSP-Prüfung konnte nicht durchgeführt werden (2) TOLERATE_OCSP_FAILURE=false	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
1030	OCSP-Zertifikat nicht in TSL Informationen enthalten	SECURITY	ERROR		-
1031	Signatur der Response ist nicht gültig.	SECURITY	ERROR		-
1032	OCSP-Responder nicht verfügbar	TECHNICAL	ERROR		-
1033	Kein Element PolicyInformation vorhanden	SECURITY	ERROR		-
1036	Das Zertifikat ist ungültig. Es wurde nach der Sperrung der ausgebenden CA ausgestellt.	SECURITY	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
1039	Warnung, dass Offline-Modus aktiviert ist und keine OCSP-Statusabfrage durchgeführt wurde	SECURITY	WARNING		-
1040	Bei der Online-statusprüfung ist ENFORCE_CERTHASH_CHECK auf ´true´ gesetzt, die OCSP-Response enthält jedoch keine certHashErweiterung	SECURITY	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
1041	Der certHash in der OCSP-Response stimmt nicht mit dem certHash des vorliegenden Zertifikats überein.	SECURITY	ERROR		-
1042	Das TSL-Signer-CA-Zertifikat kann nicht aus dem sicheren Speicher des Systems geladen werden.	TECHNICAL	ERROR		-
1043	CRL kann aus technischen Gründen nicht ausgewertet werden.	TECHNICAL	ERROR		-
1044	Warnung, dass zum angefragten Zertifikat keine Statusinformationen verfügbar sind.	TECHNICAL	WARNING		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
1047	Das Zertifikat wurde vor oder zum Referenz-zeitpunkt wider-rufen.	SECURITY	WARNING		-
1048	Es ist ein Feh-ler bei der Prü-fung des QCStatements aufgetreten (z. B. nicht vor-handen, obwohl gefordert).	TECHNICAL	ERROR		-
1050	Die einem TUC zur Zertifikats-prüfung beige-fügte OCSP-Response zu dem zu prüfen-den Zertifikat kann nicht er-folgreich gegen das Zertifikat validiert wer-den.	TECHNICAL	WARNING		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
1051	Die in einem OCSP-Response zurückgelieferte Nonce stimmt nicht mit der Nonce des OCSP-Requests überein.	SECURITY	ERROR		-
1052	Attribut-Zertifikat kann dem übergebenen Basis-Zertifikat nicht zugeordnet werden.	SECURITY	ERROR		-
1053	Die CRL kann nicht heruntergeladen werden.	TECHNICAL	ERROR		-
1054	Eine verwendete CRL ist zum aktuellen Zeitpunkt nicht mehr gültig.	TECHNICAL	ERROR		Aktualisieren Sie die CRL.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
1055	CRL-Signer-Zertifikat nicht in TSLInformationen enthalten	SECURITY	ERROR		-
1057	Signatur der CRL ist nicht gültig.	SECURITY	ERROR		-
1058	Die OCSP-Response enthält eine Exception-Meldung.	TECHNICAL	ERROR		-
1059	CA-Zertifikat für QES-Zertifikatsprüfung nicht qualifiziert	SECURITY	ERROR		-
1060	Die VL kann nicht aktualisiert werden.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
3001	VSD nicht konsistent	TECHNICAL	ERROR	PVS	Die Versichertendaten sind aufgrund eines Fehlers bei einer vorangegangenen Aktualisierung nicht mehr konsistent und können nicht eingelesen werden. ▶ Versuchen Sie, die Karte erneut zu aktualisieren. Falls nach 2-3 Versuchen die Karte immer noch denselben Fehler aufweist, ist die eGK ggf. defekt. ▶ Verweisen Sie den Versicherten mit Verweis auf die Meldung an seine Krankenkasse. Es kann das Ersatzverfahren gemäß Bundesmantelvertrag angewendet werden.
3011	Verarbeiten der Versichertendaten gescheitert	TECHNICAL	ERROR	PVS	Beim Einlesen der Versichertendaten von der eGK ist ein Fehler aufgetreten. ▶ Stecken Sie die Karte erneut und wiederholen Sie den Vorgang. ▶ Wenn das Problem nur bei einer bestimmten Karte auftritt, ist ggf. die Karte defekt. Verweisen Sie den Versicherten an seine Krankenkasse. Es kann das Ersatzverfahren gemäß Bundesmantelvertrag angewendet werden. ▶ Wenden Sie sich ansonsten an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
3020	Lesen KVK gescheitert	TECHNICAL	ERROR	PVS	Beim Einlesen der Krankenversichertenkarte (KVK) ist ein Fehler aufgetreten. ▶ Stecken Sie die Karte erneut und wiederholen Sie den Vorgang. ▶ Wenn das Problem nur bei einer bestimmten Karte auftritt, ist ggf. die Karte defekt. ▶ Wenden Sie sich ansonsten an den DVO. Hinweis: Die KVK ist seit 01.01.2015 nur noch für Versicherte sogenannter sonstiger Kostenträger (z.B. Heilfürsorge) sowie im Rahmen der Privatversicherung zulässig.
3021	KVK-Prüfsumme falsch, Daten korrupt	TECHNICAL	ERROR	PVS	Beim Einlesen der Krankenversichertenkarte (KVK) ist ein Fehler aufgetreten. Die KVK ist ungültig oder defekt. ▶ Fragen Sie den Versicherten, ob er in der Zwischenzeit eine neuere KVK von seinem Kostenträger zugeschickt bekommen hat. Ansonsten ist der Versicherte an seinen Kostenträger zu verweisen. Hinweis: Die KVK ist seit 01.01.2015 nur noch für Versicherte sogenannter sonstiger Kostenträger (z.B. Heilfürsorge) sowie im Rahmen der Privatversicherung zulässig.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
3039	Prüfungsnachweis nicht entschlüsselbar	TECHNICAL	ERROR	PVS	Der vorhandene Prüfungsnachweis auf der eGK ist nicht entschlüsselbar und stammt vermutlich von einem anderen Leistungserbringer oder Mandanten. ▶ Wiederholen Sie die Onlineprüfung für die eGK am Online-Konnektor und lesen Sie die Karte erneut ein. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
3040	Es ist kein Prüfungsnachweis auf der eGK vorhanden	TECHNICAL	ERROR	PVS	Es ist kein aktueller Prüfungsnachweis auf der eGK vorhanden. ▶ Wiederholen Sie die Onlineprüfung für die eGK am Online-Konnektor und lesen Sie die Karte erneut ein.
3041	SM-B nicht freigeschaltet	TECHNICAL	ERROR	PVS	Die verwendete SMC-B ist nicht freigeschaltet. ▶ Schalten Sie die entsprechende SMC-B frei.
3042	HBA nicht freigeschaltet	TECHNICAL	ERROR	PVS	Der verwendete HBA ist nicht freigeschaltet. ▶ Schalten Sie den entsprechenden HBA frei.
4000	Syntaxfehler	TECHNICAL	ERROR	PVS	Beim Aufruf einer Operation ist ein Syntaxfehler aufgetreten. ▶ Wiederholen Sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4001	Interner Fehler	TECHNICAL	ERROR	PVS	Ein technisches Problem ist aufgetreten. ▶ Wiederholen Sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
4002	Der Konnektor befindet sich in einem kritischen Betriebszustand	SECURITY	FATAL	PVS	Ein kritisches Problem des Konnektors ist aufgetreten. ▶ Starten Sie den Modularen Konnektor neu. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
4003	Keine User-Id angegeben, die zur Identifikation der Kartensitzung_HBA benötigt wird.	TECHNICAL	ERROR	PVS	Fehler beim Zugriff auf einen HBA. Die notwendige UserID zur Identifikation der Kartensitzung wurde beim Aufruf nicht mitgegeben. ▶ Wiederholen Sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
4004	Ungültige Mandanten-ID	TECHNICAL	ERROR	PVS	Es liegt eine Inkonsistenz im Informationsmodell zwischen dem Modularen Konnektor und dem Primärsystem vor. Die Mandaten-ID aus dem Aufrufkontext ist dem Modularen Konnektor nicht bekannt. Die Konfiguration muss überprüft werden. ▶ Wenden Sie sich an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4005	Ungültige Clientsystem-ID	TECHNICAL	ERROR	PVS	Es liegt eine Inkonsistenz im Informationsmodell zwischen dem Modularen Konnektor und Primärsystem vor. Die Clientsystem-ID aus dem Aufrufkontext ist dem Modularen Konnektor nicht bekannt. Die Konfiguration muss überprüft werden. ▶ Wenden Sie sich an den DVO.
4006	Ungültige Arbeitsplatz-ID	TECHNICAL	ERROR	PVS	Es liegt eine Inkonsistenz im Informationsmodell zwischen dem Modularen Konnektor und dem Primärsystem vor. Die Arbeitsplatz-ID aus dem Aufrufkontext ist dem Modularen Konnektor nicht bekannt. Die Konfiguration muss überprüft werden. ▶ Wenden Sie sich an den DVO.
4007	Ungültige Kartenterminal-ID	TECHNICAL	ERROR	PVS	Es liegt eine Inkonsistenz im Informationsmodell zwischen dem Modularen Konnektor und dem Primärsystem vor. Die Kartenterminal-ID aus dem Aufrufkontext ist dem Modularen Konnektor nicht bekannt. Die Konfiguration muss überprüft werden. ▶ Wenden Sie sich an den DVO.
4008	Karte nicht als gesteckt identifiziert	TECHNICAL	ERROR	PVS	Ein technisches Problem beim Zugriff auf die Karte ist aufgetreten. Die Karte wurde nicht erkannt. ▶ Stecken Sie die Karte erneut und wiederholen Sie den Vorgang. ▶ Wenn das Problem weiterhin besteht, wenden Sie sich an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4009	SM-B ist dem Konnektor nicht als SM-B_Verwaltet bekannt	SECURITY	ERROR	PVS	Es liegt eine Inkonsistenz im Informationsmodell zwischen dem Modularen Konnektor und dem Primärsystem vor. Die SMC-B aus dem Aufrufkontext ist dem Modularen Konnektor nicht bekannt. Die Konfiguration muss überprüft werden. ▶ Wenden Sie sich an den DVO.
4010	Clientsystem ist dem Mandanten nicht zugeordnet	SECURITY	ERROR	PVS	Es liegt eine Inkonsistenz im Informationsmodell zwischen dem Modularen Konnektor und dem Primärsystem vor. Das Clientsystem aus dem Aufrufkontext ist dem Mandanten nicht zugeordnet. Die Konfiguration muss überprüft werden. ▶ Wenden Sie sich an den DVO.
4011	Arbeitsplatz ist dem Mandanten nicht zugeordnet	SECURITY	ERROR	PVS	Es liegt eine Inkonsistenz im Informationsmodell zwischen dem Modularen Konnektor und dem Primärsystem vor. Der Arbeitsplatz aus dem Aufrufkontext ist dem Mandanten nicht zugeordnet. Die Konfiguration muss überprüft werden. ▶ Wenden Sie sich an den DVO.
4012	Kartenterminal ist dem Mandanten nicht zugeordnet	SECURITY	ERROR	PVS	Es liegt eine Inkonsistenz im Informationsmodell zwischen dem Modularen Konnektor und dem Primärsystem vor. Das Kartenterminal aus dem Aufrufkontext ist dem Mandanten nicht zugeordnet. Die Konfiguration muss überprüft werden. ▶ Wenden Sie sich an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4013	SM-B_Verwaltet ist dem Mandanten nicht zugeordnet	SECURITY	ERROR	PVS	Es liegt eine Inkonsistenz im Informationsmodell zwischen dem Modularen Konnektor und dem Primärsystem vor. Die SMC-B aus dem Aufrufkontext ist dem Mandanten nicht zugeordnet. Die Konfiguration muss überprüft werden. ▶ Wenden Sie sich an den DVO.
4014	Für den Mandanten ist der Arbeitsplatz nicht dem Clientsystem zugeordnet	SECURITY	ERROR	PVS	Es liegt eine Inkonsistenz im Informationsmodell zwischen dem Modularen Konnektor und dem Primärsystem vor. Der Arbeitsplatz aus dem Aufrufkontext ist für diesen Mandanten nicht dem Clientsystem zugeordnet. Die Konfiguration muss überprüft werden. ▶ Wenden Sie sich an den DVO.
4015	Kartenterminal ist weder lokal noch entfernt vom Arbeitsplatz aus zugreifbar	SECURITY	ERROR	PVS	Es liegt eine Inkonsistenz im Informationsmodell zwischen dem Modularen Konnektor und dem Primärsystem vor. Das Kartenterminal aus dem Aufrufkontext ist vom Arbeitsplatz nicht zugreifbar. Die Konfiguration muss überprüft werden. ▶ Wenden Sie sich an den DVO.
4016	Kartenterminal ist nicht lokal vom Arbeitsplatz aus zugreifbar	SECURITY	ERROR	PVS	Es liegt eine Inkonsistenz im Informationsmodell zwischen dem Modularen Konnektor und dem Primärsystem vor. Das Kartenterminal aus dem Aufrufkontext ist vom Arbeitsplatz nicht zugreifbar. Die Konfiguration muss überprüft werden. ▶ Wenden Sie sich an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4017	Die eGK hat bereits eine Kartensitzung, die einem anderen Arbeitsplatz zugeordnet ist.	SECURITY	ERROR	PVS	Fehler beim Zugriff auf eine eGK. Die eGK wird derzeit von einem anderen Arbeitsplatz verwendet. ▶ Wiederholen Sie den Vorgang.
4018	Der HBA hat mindestens eine Kartensitzung zu einer anderen UserId, deren Sicherheitszustand erhöht ist.	SECURITY	ERROR	PVS	Fehler beim Zugriff auf einen HBA. Der HBA wird derzeit von einem anderen Benutzer verwendet. ▶ Wiederholen Sie den Vorgang.
4019	Zu den Parametern konnte keine Regel ermittelt werden.	TECHNICAL	ERROR	PVS	Es ist ein Fehler bei einem Operationsaufruf des Primärsystems aufgetreten. Zu den Aufrufparametern konnten keine Zugriffsregeln ermittelt werden. ▶ Wenden Sie sich an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4020	Kartenterminal ist weder lokal noch entfernt über irgendeinen dem Clientsystem zugeordneten Arbeitsplatz aus zugreifbar	SECURITY	ERROR	PVS	Es liegt eine Inkonsistenz im Informationsmodell zwischen Modularem Konnektor und Primärsystem vor. Das Kartenterminal aus dem Aufrufkontext ist vom keinem Arbeitsplatz zugreifbar. Die Konfiguration muss überprüft werden. ▶ Wenden Sie sich an den DVO.
4021	Es sind nicht alle Pflichtparameter MandantId, clientSystemId, workplaceId gefüllt.	TECHNICAL	ERROR	PVS	Es ist ein Fehler bei einem Operationsaufruf des Primärsystems aufgetreten. Es wurden nicht alle notwendigen Parameter übergeben. ▶ Wenden Sie sich an den DVO.
4027	Die Endpunktinformationen konnten nicht übernommen werden.	TECHNICAL	ERROR	PVS	Es ist ein technischer Fehler während der Bootup-Phase aufgetreten. ▶ Starten Sie den Modularen Konnektor neu. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
4028	Fehler beim Versuch eines Verbindungsaufbau zum KT	TECHNICAL	ERROR	PVS	Es ist ein technischer Fehler beim Aufbau einer Kartenterminal-Sitzung aufgetreten. ▶ Wenden Sie sich an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4029	Fehler bei der KT-Authentisierung. KT möglicher Weise manipuliert	SECURITY	ERROR	PVS	Es ist ein technischer Fehler beim Pairing eines Kartenterminals aufgetreten. ▶ Wenden Sie sich an den DVO.
4030	Admin-Werte für KT fehlerhaft	SECURITY	ERROR	PVS	Es ist ein technischer Fehler beim Aufbau einer Kartenterminal-Sitzung aufgetreten. ▶ Wenden Sie sich an den DVO.
4031	Interner Fehler	TECHNICAL	ERROR	PVS	Es ist ein technischer Fehler im Kartenterminaldienst aufgetreten. ▶ Wenden Sie sich an den DVO.
4032	Verbindung zu HSM konnte nicht aufgebaut werden	TECHNICAL	ERROR	PVS	Es ist ein technischer Fehler beim Aufbau einer Kartenterminal-Sitzung aufgetreten. ▶ Wenden Sie sich an den DVO.
4033	Kartenterminal antwortet nicht, Zufügen fehlgeschlagen	TECHNICAL	ERROR	PVS	Es ist ein technischer Fehler beim Hinzufügen eines Kartenterminals aufgetreten. ▶ Wenden Sie sich an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4034	Kartenterminal mit gleichem Hostname bereits in der Liste der Kartenterminals vorhanden. Bitte Hostname des Kartenterminals ändern.	TECHNICAL	ERROR	PVS	Es ist ein technischer Fehler beim Hinzufügen eines Kartenterminals aufgetreten. ▶ Wenden Sie sich an den DVO.
4035	Angegebener IP-Adresse gehört zu einer anderen MAC-Adresse als die, die übergeben wurde. Angaben zur MAC prüfen	TECHNICAL	ERROR	PVS	Es ist ein technischer Fehler beim Hinzufügen eines Kartenterminals aufgetreten. ▶ Wenden Sie sich an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4036	Angegebener IP-Adresse gehört zu einem anderen Hostname als der, der übergeben wurde. Angaben zum Hostname prüfen	TECHNICAL	ERROR	PVS	Es ist ein technischer Fehler beim Hinzufügen eines Kartenterminals aufgetreten. ▶ Wenden Sie sich an den DVO.
4037	Verwaltung der Kartenterminals inkonsistent	TECHNICAL	ERROR	PVS	Es ist ein technischer Fehler beim Hinzufügen eines Kartenterminals aufgetreten. ▶ Wenden Sie sich an den DVO.
4039	Kartenterminal durch andere Nutzung aktuell belegt	TECHNICAL	ERROR	PVS	Es ist ein Fehler bei der Displayanzeige auf dem Kartenterminal aufgetreten. Das Kartenterminal-Display ist durch einen anderen, zeitgleich im Modularen Konnektor ablaufenden Vorgang reserviert. ▶ Wiederholen Sie den Vorgang.
4040	Fehler beim Versuch eines Verbindungsaufbaus zum KT	SECURITY	ERROR	PVS	Es ist ein Fehler beim Pairing eines Kartenterminals aufgetreten. ▶ Wenden Sie sich an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4041	Fehler im Pairing, SICCT-Fehler: %s	TECHNICAL	ERROR	PVS	Es ist ein Fehler beim Pairing eines Kartenterminals aufgetreten. ▶ Wenden Sie sich an den DVO.
4042	Die Version des Kartenterminals wird nicht unterstützt	TECHNICAL	ERROR	PVS	Es ist ein Fehler beim Pairing eines Kartenterminals aufgetreten. ▶ Wenden Sie sich an den DVO.
4043	Timeout bei der PIN-Eingabe	TECHNICAL	WARNING	PVS	Es ist ein Timeout bei der PIN-Eingabe an dem Kartenterminal aufgetreten. ▶ Wiederholen Sie den Vorgang.
4044	Fehler beim Zugriff auf das Kartenterminal	TECHNICAL	ERROR	PVS	Es ist ein Fehler beim Zugriff auf das Kartenterminal aufgetreten. ▶ Wiederholen Sie den Vorgang. ▶ Wenn der Fehler erneut auftritt, wenden Sie sich an den DVO.
4045	Fehler beim Zugriff auf die Karte	TECHNICAL	ERROR	PVS	Es ist ein Fehler beim Zugriff auf die Karte aufgetreten. ▶ Stecken Sie die Karte erneut und wiederholen Sie den Vorgang. ▶ Wenn der Fehler erneut auftritt, wenden Sie sich an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4046	Kartenapplikation existiert nicht	TECHNICAL	ERROR	PVS	Fehler beim Aufruf einer Kartenapplikation der verwendeten Karte. ▶ Stecken Sie die Karte erneut und wiederholen Sie den Vorgang. Falls das Problem nur bei einer bestimmten Karte auftritt, ist die Karte ggf. defekt oder falsch personalisiert. ▶ Tritt der Fehler bei einer eGK auf, verweisen Sie den Versicherten mit den entsprechenden Fehlerinformationen an seine Krankenkasse. Es kann das Ersatzverfahren gemäß Bundesmantelvertrag angewendet werden. ▶ In anderen Fällen wenden sie sich an den DVO.
4047	Karten-Handle ungültig	TECHNICAL	ERROR	PVS	Es ist ein Fehler beim Zugriff auf die Karte aufgetreten. ▶ Stecken Sie die Karte erneut und wiederholen Sie den Vorgang. ▶ Wenn der Fehler erneut auftritt, wenden Sie sich an den DVO.
4048	Fehler bei der C2C-Authentisierung	TECHNICAL	ERROR	PVS	Es ist ein Fehler bei C2C-Prüfung aufgetreten. Es sollte überprüft werden, ob die eGK und die SMC-B bzw. der HBA korrekt gesteckt sind. ▶ Stecken Sie die Karte erneut und wiederholen Sie den Vorgang. ▶ Wenn der Fehler erneut auftritt, wenden Sie sich an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4049	Abbruch durch den Benutzer	TECHNICAL	ERROR	PVS	Die PIN-Eingabe wurde durch den Benutzer abgebrochen ▶ Wiederholen Sie den Vorgang. ▶ Wenn der Fehler erneut auftritt, wenden Sie sich an den DVO.
4050	Öffnen eines weiteren Kanals zur Karte nicht möglich	TECHNICAL	ERROR	PVS	Es ist ein technisches Problem beim Zugriff auf die Karte aufgetreten. ▶ Wiederholen Sie den Vorgang.
4051	Falscher Kartentyp	TECHNICAL	ERROR	PVS	Für die aufgerufene Operation wurde ein falscher Kartentyp verwendet. ▶ Überprüfen Sie die Nutzung der korrekten Karte und wiederholen Sie den Vorgang.
4052	Kartenzugriff verweigert	SECURITY	ERROR	PVS	Es ist ein Fehler beim Zugriff auf die Karte aufgetreten. ▶ Stecken Sie die Karte erneut und wiederholen Sie den Vorgang. ▶ Wenn der Fehler erneut auftritt, wenden Sie sich an den DVO.
4053	Remote-PIN nicht möglich	SECURITY	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4054	Fehler beim Secure Messaging, Zielkarte	SECURITY	ERROR		-
4055	Fehler beim Secure Messaging, Quellkarte	SECURITY	ERROR		-
4056	Fehler bei der C2C-Authentisierung, Quellkarte	TECHNICAL	ERROR		-
4057	Fehler bei der C2C-Authentisierung, Zielkarte	TECHNICAL	ERROR		-
4058	Aufruf nicht zulässig	SECURITY	ERROR		-
4060	Ressource belegt	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4061	Falsche alte PIN, verbleibende Eingabeversuche <x>	SECURITY	WARNING		-
4062	Falsche PIN (hier: PUK) verbleibende Eingabeversuche <x>	SECURITY	WARNING		-
4063	PIN bereits gesperrt (BLOCKED)	SECURITY	ERROR		-
4064	Alte PIN bereits blockiert (hier: PUK)	SECURITY	ERROR		-
4065	PIN ist transportgeschützt, Änderung erforderlich	TECHNICAL	WARNING		-
4066	PIN Pad nicht verfügbar	TECHNICAL	ERROR		-
4067	Neue PIN nicht identisch	SECURITY	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4068	Neue PIN zu kurz/lang	SECURITY	ERROR		-
4069	Korruptes Chiffrat bei asymmetrischer Entschlüsse-lung	TECHNICAL	ERROR		-
4070	Autorisierende Karte oder Kar-tensitzung fehlt	TECHNICAL	ERROR		-
4071	Keine Karte für C2C Auth ge-setzt	TECHNICAL	ERROR		-
4072	Ungültige PIN-Referenz	TECHNICAL	ERROR		-
4073	Adressiertes Passwort konn-te nicht gefun-den werden	TECHNICAL	ERROR		-
4074	Formatfehler der übergebe-nen PIN	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4075	Formatfehler der übergebenen neuen PIN	TECHNICAL	ERROR		-
4076	Formatfehler im übergebenen PUK	TECHNICAL	ERROR		-
4077	Setzen der neuen PIN nicht zulässig	SECURITY	ERROR		-
4078	PIN-Eingabe über das Clientsystem ist nicht zugelassen	SECURITY	ERROR		-
4079	Schlüsseldaten fehlen	TECHNICAL	ERROR		-
4080	Schlüssel unterstützt den geforderten Algorithmus nicht	TECHNICAL	ERROR		-
4081	Kein Signierschlüssel ausgewählt	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4082	PIN durch diese Fehleingabe blockiert (now-blocked)	SECURITY	ERROR		-
4084	Datei deaktiviert	TECHNICAL	WARNING		-
4085	Zugriffsbedingungen nicht erfüllt	TECHNICAL	WARNING		-
4086	Verzeichnis deaktiviert	TECHNICAL	ERROR		-
4087	Datei nicht vorhanden	TECHNICAL	ERROR		-
4088	Datensatz zu groß	TECHNICAL	ERROR		-
4089	Datei ist vom falschen Typ	TECHNICAL	ERROR		-
4090	Zugriff auf eGK nicht gestattet	SECURITY	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4092	Remote-PIN-KT benötigt aber für diesen Arbeitsplatz nicht definiert	TECHNICAL	ERROR		-
4093	Karte wird in einer anderen Kartensitzung exklusiv verwendet	TECHNICAL	ERROR		-
4094	Timeout beim Kartenzugriff aufgetreten	TECHNICAL	ERROR	PVS	Es ist ein Timeout beim Kartenzugriff aufgetreten. Karte antwortet nicht innerhalb der vorgegebenen Zeit. ▶ Stecken Sie die Karte erneut und wiederholen Sie den Vorgang. ▶ Wenn der Fehler erneut auftritt, wenden Sie sich an den DVO.
4095	Fehler bei der Auswertung eines XPath-Ausdruck	TECHNICAL	ERROR		-
4096	Ungültige Kartenterminal-ID	TECHNICAL	ERROR		-
4097	Ungültige Kartenslot-ID	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4098	Keine Karte im angegebenen Slot gefunden	TECHNICAL	ERROR		-
4099	Keine Karte zur angegebenen Iccsn gefunden	TECHNICAL	ERROR		-
4101	Karten-Handle ungültig	TECHNICAL	ERROR		-
4102	Ungültige Sub-scriptionId	TECHNICAL	ERROR		-
4103	XML-Element nicht gefunden	TECHNICAL	ERROR		-
4104	XML-Element nicht eindeutig identifiziert. (Überschnei-dung)	TECHNICAL	ERROR		-
4105	Hybride Ver-schlüsselung konnte nicht durchgeführt werden	TECHNICAL	ERROR		-
4106	Falscher Schlüssel	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4107	Hybride Entschlüsselung konnte nicht durchgeführt werden	TECHNICAL	ERROR		-
4108	Symmetrische Verschlüsselung konnte nicht durchgeführt werden	TECHNICAL	ERROR		-
4109	Symmetrische Entschlüsselung konnte nicht durchgeführt werden	TECHNICAL	ERROR		-
4110	Ungültiges Dokumentformat (%s)	TECHNICAL	ERROR		-
4111	Ungültiger Signaturyp oder Signaturvariante	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4112	Dokument nicht konform zu Regeln für nonQES	TECHNICAL	ERROR		-
4115	Signatur des Dokuments ungültig. Der SignatureValue des Dokuments ist falsch oder für mindestens eine Reference ist der DigestValue falsch.	SECURITY	ERROR		-
4116	Timeout (Benutzer)	TECHNICAL	WARNING		-
4118	Stapelsignaturen werden nur für den HBA unterstützt. Mit HBA-Vorläuferkarten sind nur Einzelsignaturen möglich.	TECHNICAL	ERROR		-
4120	Kartenfehler	SECURITY	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4123	Fehler bei Signaturerstellung	SECURITY	ERROR		-
4124	Dokument nicht konform zu Regeln für QES	SECURITY	ERROR		-
4125	LU_SAK nicht aktiviert	SECURITY	ERROR		-
4126	Kartentyp nicht zulässig für Signatur	SECURITY	ERROR		-
4127	Import der TSL-Datei fehlgeschlagen	SECURITY	ERROR		-
4128	Der manuelle Import der TSL-Datei schlägt fehl	TECHNICAL	ERROR		-
4129	Der manuelle Import der BNetzA-Vertrauensliste schlägt fehl	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4130	Signaturprüfung der CRL fehlgeschlagen	SECURITY	ERROR		-
4131	Zum angegebenen Card-Handle keine Karte gefunden	TECHNICAL	FATAL		-
4132	Extraktion des Ablaufsdatums fehlschlägt	SECURITY	ERROR		-
4133	Import der BNetzA-Vertrauensliste fehlgeschlagen	SECURITY	ERROR		-
4146	Kartenhandle existiert nicht	TECHNICAL	ERROR		-
4147	Zertifikat nicht vorhanden (z. B. kein QES-Zertifikat in SM-B)	TECHNICAL	ERROR		-
4148	Fehler beim Extrahieren von Zertifikatsinformationen	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4149	Ungültige Zertifikatsreferenz	TECHNICAL	ERROR		-
4150	Fehler beim Schreiben des Systemprotokolls	TECHNICAL	FATAL		-
4151	Fehler beim Schreiben eines Fachmodulprotokolls	TECHNICAL	FATAL		-
4152	Fehler beim Schreiben des Sicherheitsprotokolls	SECURITY	ERROR		-
4153	Zugriff auf Sicherheitsprotokoll nicht möglich	TECHNICAL	FATAL		-
4154	Zugriff auf Systemprotokoll nicht möglich	TECHNICAL	FATAL		-
4155	Zugriff auf Fachmodulprotokolle nicht möglich	TECHNICAL	FATAL		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4156	Server konnte bei TLS-Verbindungs-aufbau nicht authentisiert werden	SECURITY	ERROR		-
4157	Clientauthenti-sierung bei TLS-Verbindungs-aufbau fehlge-schlagen	SECURITY	ERROR		-
4158	Adressierte TLS-Verbindung nicht vorhan-den	TECHNICAL	ERROR		-
4159	Public-IP: DNS Server antwor-tet nicht	TECHNICAL	FATAL		-
4160	Public-IP: Zu einem DNS Namen konnte keine IP-Adresse gefun-den werden	TECHNICAL	FATAL		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4161	Public-IP: Ein oder mehrere IP-Adressen sind ungültig	TECHNICAL	FATAL		-
4162	Es liegt eine fehlerhafte LAN IP-Konfiguration vor.	TECHNICAL	ERROR		-
4163	Es liegt eine fehlerhafte WAN IP-Konfiguration vor.	TECHNICAL	ERROR		-
4164	Beim Aktualisieren oder Aktivieren der Firewall-Regeln ist es zu einem Fehler gekommen.	TECHNICAL	FATAL		-
4165	gSMC-K Konfiguration: Keine Netzwerk-Konfiguration gefunden.	TECHNICAL	FATAL		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4166	gSMC-K Konfiguration: Ein oder mehrere Netzwerk-Adressen sind ungültig.	TECHNICAL	FATAL		-
4167	CreateRoutes: Ein oder mehrere Adressen sind ungültig.	TECHNICAL	FATAL		-
4168	DHCP-Server konnte nicht gestartet werden	TECHNICAL	ERROR		-
4169	Konnektor erhält keine DHCP-Informationen	TECHNICAL	ERROR		-
4170	Konnektor besitzt identische IP-Adressen am WAN und LAN Interface	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4171	Der VPN-Tunnel zur TI konnte nicht beendet werden.	TECHNICAL	FATAL		-
4172	Es ist keine Online-Verbindung zulässig.	TECHNICAL	FATAL		-
4173	Die CRL ist nicht mehr gültig (outdated).	TECHNICAL	FATAL		-
4174	TI VPN-Tunnel: Verbindung konnte nicht aufgebaut werden	TECHNICAL	FATAL	PVS	Die Verbindung zum VPN-Zugangsdienst konnte nicht aufgebaut werden. ▶ Überprüfen Sie den Internetzugang ▶ Ansonsten wenden Sie sich an den DVO.
4175	Der VPN-Tunnel zum SIS konnte nicht beendet werden.	TECHNICAL	FATAL		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4176	SIS VPN-Tunnel: Verbindung konnte nicht aufgebaut werden.	TECHNICAL	FATAL		-
4177	Der NTP-Server des Konnektors konnte nicht synchronisiert werden.	TECHNICAL	WARNING		-
4178	Das Fachmodul konnte die aktuelle Systemzeit des Konnektors nicht abrufen.	TECHNICAL	ERROR		-
4179	DNS: Anfrage wurde abgebrochen, da der Timeout von ANLW_SERVICE_TIMEOUT Sekunden überschritten wurde.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4180	DNS: Es ist ein Fehler bei der Namensauflösung aufgetreten <x>	TECHNICAL	FATAL		-
4181	Integritätsprüfung UpdateInformation fehlgeschlagen.	SECURITY	ERROR		-
4182	Download nicht aller UpdateFiles möglich.	SECURITY	ERROR		-
4183	Integritätsprüfung UpdateFiles fehlgeschlagen.	SECURITY	ERROR		-
4184	Anwendung der UpdateFiles fehlgeschlagen (<Details>).	SECURITY	ERROR		-
4185	Fimware-Version liegt außerhalb der gültigen Firmware-Gruppe	SECURITY	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4186	Download nicht aller UpdateFiles möglich.	SECURITY	ERROR		-
4187	KT-Update fehlgeschlagen (<Fehlerinfo gemäß SICCT>)	SECURITY	ERROR		-
4188	Konfigurationsdienst nicht erreichbar, konfigurierte Adresse kontrollieren.	TECHNICAL	ERROR		-
4189	Konfigurationsdienst liefert falsches Zertifikat	SECURITY	FATAL		-
4190	Fehler beim Beziehen der Updatelisten	TECHNICAL	ERROR		-
4192	C2C mit eGK G1+ ab 01.01.2019 nicht mehr gestattet	SECURITY	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4196	Fehler bei der CV-Zertifikatsprüfung	TECHNICAL	ERROR		-
4197	Parameter SignaturePlacement wurde ignoriert	TECHNICAL	WARNING		-
4198	Beim Übernehmen der Bestandsnetze ist ein Fehler aufgetreten	TECHNICAL	ERROR		-
4200	Schlüssel erlaubt keinen zugelassenen Verschlüsselungsalgorithmus	SECURITY	ERROR		-
4201	Kryptographischer Algorithmus vom Konnektor nicht unterstützt	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4202	Timeout. Es wurde keine Karte innerhalb der angegebenen Zeitspanne gesteckt.	TECHNICAL	ERROR		-
4203	Karte deaktiviert, aber nicht entnommen.	TECHNICAL	ERROR		-
4204	Clientsystem aus dem Aufrufkontext konnte nicht authentifiziert werden.	SECURITY	ERROR		-
4205	Es ist nicht genügend Speicherplatz im PDF-Dokument verfügbar	TECHNICAL	ERROR		-
4206	Signaturzertifikat ermitteln ist fehlgeschlagen	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4207	Referenzzeitpunkt bestimmen ist fehlgeschlagen	TECHNICAL	ERROR		-
4208	Dokument nicht konform zu Profilierung der Signaturformate	TECHNICAL	ERROR		-
4209	Kartentyp %s wird durch diese Operation nicht unterstützt.	TECHNICAL	ERROR		-
4216	Fehler beim Schreiben des Konnektor-Performanceprotokolls	TECHNICAL	FATAL		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4217	Fehler beim Schreiben eines Fachmodul-Performanceprotokolls	TECHNICAL	FATAL		-
4218	Zugriff auf Konnektor-Performanceprotokoll nicht möglich	TECHNICAL	FATAL		-
4219	Zugriff auf Fachmodul-Performanceprotokoll nicht möglich	TECHNICAL	FATAL		-
4220	Rollenprüfung bei TLS-Verbindungsaufbau fehlgeschlagen	SECURITY	ERROR		-
4221	Kartenterminal nicht aktiv	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4222	Kartenterminal ist nicht verbunden	TECHNICAL	ERROR		-
4228	Das benötigte Cross-CV-Zertifikat ist nicht vorhanden	TECHNICAL	ERROR		-
4232	Der Aufrufer ist nicht im Besitz des Karten-Locks	TECHNICAL	ERROR		-
4233	Ausstellungsdatum des Zertifikats liegt in der Zukunft	SECURITY	ERROR		-
4235	TSL-Dienst konnte bei TLS-Verbindungsaufbau nicht authentisiert werden	SECURITY	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
4236	Rollenprüfung bei TLS-Verbindungs-aufbau zum TSL-Dienst fehlgeschlagen	SECURITY	ERROR		-
11101	Für die eGK mit der angegebe-nen ICCSN ist der aufgerufene Dienst nicht zu-ständig.	TECHNICAL	FATAL	PVS	Fehler bei der Onlineprüfung der eGK. Die eGK mit der angegebenen ICCSN ist dem Fachdienst UFS nicht bekannt. Die Fehlerursache muss vom Fachdienstbetreiber analysiert werden. Die eGK ist gültiger Leistungsanspruchsnachweis. VSD können mit Prüfungsnachweis 3 („Aktualisierung VSD auf eGK technisch nicht möglich") eingelesen werden.
11999	Ein nicht spezi-fizierter Fehler ist aufgetreten, zu dem weitere Details im Dienst protokol-liert worden sind.	nicht vorge-geben	nicht vorge-geben	PVS	Fehler bei der Onlineprüfung der eGK. Es ist ein nicht spezifizierter Fehler im Fachdienst UFS aufgetreten. Die Fehlerursache muss vom Fachdienstbetreiber analysiert werden. Die eGK ist gültiger Leistungsanspruchsnachweis. VSD können mit Prüfungsnachweis 3 („Aktualisierung VSD auf eGK technisch nicht möglich") eingelesen werden.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
11148	Die Payload ist nicht konform zum XML-Schema.	TECHNICAL	FATAL	PVS	Fehler bei der Onlineprüfung der eGK. Es ist ein Fehler im Fachdienst UFS aufgetreten. Die Fehlerursache muss vom Fachdienstbetreiber analysiert werden. Die eGK ist gültiger Leistungsanspruchsnachweis. VSD können mit Prüfungsnachweis 3 („Aktualisierung VSD auf eGK technisch nicht möglich") eingelesen werden.
12101	Für die angegebene Kombination aus ICCSN und Update-Identifier liegt kein Update vor.	TECHNICAL	FATAL	PVS	Fehler bei der Onlineprüfung der eGK. Für die eGK liegt im Fachdienst VSDD/CMS keine Aktualisierung vor. Die Fehlerursache muss vom Fachdienstbetreiber analysiert werden Die eGK ist gültiger Leistungsanspruchsnachweis. VSD können mit Prüfungsnachweis 3 („Aktualisierung VSD auf eGK technisch nicht möglich") eingelesen werden.
12102	Für das angefragte Update ist die Durchführung eines anderen Updates eine Vorbedingung.	TECHNICAL	FATAL	PVS	Fehler bei der Onlineprüfung der eGK. Für die eGK kann durch den Fachdienst VSDD/CMS keine Aktualisierung vorgenommen werden. Die Fehlerursache muss vom Fachdienstbetreiber analysiert werden. Die eGK ist gültiger Leistungsanspruchsnachweis. VSD können mit Prüfungsnachweis 3 („Aktualisierung VSD auf eGK technisch nicht möglich"") eingelesen werden.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
12103	Die Authentifizierung zwischen Fachdienst und eGK mittels des fachdienstspezifischen, kartenindividuellen symmetrischen Schlüssels ist fehlgeschlagen.	SECURITY	FATAL	PVS	Fehler bei der Onlineprüfung der eGK. Der Aufbau der gesicherten Verbindung zwischen Karte und Fachdienst ist fehlgeschlagen. Die Fehlerursache muss vom Fachdienstbetreiber analysiert werden. Die eGK ist gültiger Leistungsanspruchsnachweis. VSD können mit Prüfungsnachweis 3 („Aktualisierung VSD auf eGK technisch nicht möglich") eingelesen werden. ▶ Wenn der Fehler mehrfach bei verschiedenen eGKs auftritt, wenden Sie sich an den DVO.
12105	Die eGK ist defekt.	TECHNICAL	FATAL	PVS	Abbruch des Anwendungsfalles der Onlineprüfung der eGK, kein Einlesen der Versichertendaten möglich. ▶ Stecken Sie die Karte erneut. ▶ Wenn das Problem nur bei einer bestimmten Karte auftritt, ist ggf. die Karte defekt. Verweisen Sie in diesem Fall den Versicherten mit den entsprechenden Fehlerinformationen an seine Krankenkasse. Es kann das Ersatzverfahren gemäß Bundesmantelvertrag angewendet werden. ▶ In anderen Fällen wenden Sie sich an den DVO.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
12999	Ein nicht spezifizierter Fehler ist aufgetreten, zu dem weitere Details im Dienst protokolliert worden sind.	nicht vorgegeben	nicht vorgegeben	PVS	Fehler bei der Onlineprüfung der eGK. Es ist ein nicht spezifizierter Fehler im Fachdienst VSDD/CMS aufgetreten. Die Fehlerursache muss vom Fachdienstbetreiber analysiert werden. Die eGK ist gültiger Leistungsanspruchsnachweis. VSD können mit Prüfungsnachweis 3 („Aktualisierung VSD auf eGK technisch nicht möglich") eingelesen werden.
41000	Karte/ Kartenterminal antwortet mit einer spezifischen Meldung, Fehlercode <gemäß [gemSpec_COS]/[SICCT]>	TECHNICAL			-
41001	Kartenterminal <x> ist unzulässigerweise virtuell. Diese Eigenschaft ist ausschließlich für eine zukünftige Nutzung vorgesehen.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
41002	Es konnte keine SMC-KT in Kartenterminal <x> ermittelt werden.	TECHNICAL	ERROR		-
41003	Kartensitzung für Cardhandle <x> ungültig oder beendet.	TECHNICAL	ERROR		-
41004	Lesen eines TLV-Objekts aus Datei <x> fehlgeschlagen.	TECHNICAL	ERROR		-
41005	Kartenoperation <x> wird von Karte <x> nicht unterstützt.	TECHNICAL	ERROR		-
41006	Lesen der Datei <x> fehlgeschlagen.	TECHNICAL	ERROR		-
41007	Lesen des Zertifikats <x> fehlgeschlagen.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
41008	Signaturerstellung über eine Karte nicht möglich.	TECHNICAL	ERROR		-
41009	Kartensitzung für Kartentyp […] nicht verfügbar.	TECHNICAL	ERROR		-
41010	Es konnte keine gSMC-K ermittelt werden.	TECHNICAL	ERROR		-
41011	Ungültiger Kartentyp für TLS-Verbindung in die TI.	TECHNICAL	ERROR		-
41012	Ungültige oder fehlende Versicherungsnummer im AUT-Zertifikat.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
41013	Ungültige oder fehlende Versichertennummer im AUT-Zertifikat.	TECHNICAL	ERROR		-
41014	Unerlaubter Zugriff auf DF oder EF.	TECHNICAL	ERROR		-
41015	Verschlüsselung über eine Karte nicht möglich.	TECHNICAL	ERROR		-
41016	Keine SMC-B für den TSL-Verbindungsaufbau gesteckt oder freigeschaltet.	TECHNICAL	ERROR		-
41017	C2C-Authentisierung durch den Konnektor abgebrochen.	TECHNICAL	INFO		-
41018	Fehler beim Schreiben des PN.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
42000	Import einer Backup Datei ist fehlgeschlagen.	TECHNICAL	ERROR		-
42001	Import einer Backup Datei ist beim Entschlüsseln fehlgeschlagen.	TECHNICAL	ERROR		-
42002	Import einer Backup Datei ist bei der Versionsprüfung fehlgeschlagen.	TECHNICAL	ERROR		-
42003	Konnektor-Zertifikat (gSMC-K AUT_SAK) nicht lesbar, Export/Import nicht möglich.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
42004	Ein Export kann nicht erstellt werden, da die Version nicht exportiert werden kann.	TECHNICAL	ERROR		-
42005	Ein Import kann nicht eingespielt werden, da die Version nicht festgestellt werden kann.	TECHNICAL	ERROR		-
42010	Export einer Backup Datei ist fehlgeschlagen.	TECHNICAL	ERROR		-
42011	PublicKey für Backup-Erstellung nicht lesbar.	TECHNICAL	ERROR		-
42012	Rolle stimmt nicht mit der Vorgabe überein.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
42013	Interner Fehler bei der OCSP-Prüfung	TECHNICAL	ERROR		-
42014	OCSP-Zertifikats-Signatur ist mathematisch nicht gültig.	TECHNICAL	ERROR		-
42015	Zertifikat ist nicht mehr gültig.	TECHNICAL	WARNING		-
42016	Zertifikat ist bald nicht mehr gültig.	TECHNICAL	INFO		-
42017	Zertifikatsprüfung von Zerstifikaten mit if_QC_present wird in der Version des Konnektors nicht unterstützt.	TECHNICAL	INFO		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
42018	Das Zertifikat des Clientsystems für den TLS-Verbindungsaufbau ist nicht gültig.	TECHNICAL	ERROR		-
42019	Die OCSP-Response enthält eine certHashErweiterung, diese kann aber nicht verarbeitet werden.	TECHNICAL	WARNING		-
42020	Der TLS-Dienst konnte mit einer Gegenstelle […] keine TLS-Verbindung aufbauen	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
42021	Der TLS-Dienst kann die Karte […] nicht benutzen um eine TLS-Verbindung aufzubauen, da diese noch nicht freigeschaltet ist.	TECHNICAL	WARNING		-
42022	Der Name im Zertifikat […] entspricht nicht dem Hostname […] der Gegenstelle.	TECHNICAL	ERROR		-
42023	Der Vertrauens-Anker aus der TSL konnte nicht übernommen werden, da das Zertifikat noch nicht gültig ist.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
42024	Der Vertrauens-Anker aus der TSL konnte nicht übernommen werden, da das Zertifikat abgelaufen ist.	TECHNICAL	ERROR		Aktualisieren Sie den Vertrauens-Anker.
42025	Die TSL enthält keinen Vertrauens-Anker.	TECHNICAL	INFO		-
42026	Der Aufbau der TLS-Verbindung mit der Gegenstelle … hat das Zeitlimit von … ms überschritten.	TECHNICAL	ERROR		-
42027	Der TLS-Dienst konnte mit keiner der … bekannten Zieladressen eine TLS-Verbindung aufbauen.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
43000	Fehler bei der Kommunikation mit einem Fachdienst.	TECHNICAL	ERROR		-
43001	Ein Download für das Terminalupdate läuft bereits.	TECHNICAL	ERROR		-
43002	Nicht genügend Platz zum Download des Updates.	TECHNICAL	ERROR		-
43003	Update bereits heruntergeladen.	TECHNICAL	ERROR		-
43004	Ein Download für ein Konnektorupdate läuft bereits.	TECHNICAL	ERROR		-
43005	Ein Konnektorupdate läuft bereits.	TECHNICAL	ERROR		-
43006	Das Terminal wird bereits aktualisiert.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
43007	Das Update passt nicht zum Gerät.	TECHNICAL	ERROR		-
43008	Update noch nicht herunter-geladen.	TECHNICAL	ERROR		-
43009	Fehler beim Download der Dokumentation vom KSR.	TECHNICAL	ERROR		-
43010	Die Aktualisie-rung oder das zu aktualisie-rende Terminal wurden nicht gefunden.	TECHNICAL	ERROR		-
43011	Das zu aktuali-sierende Ter-minal ist nicht mehr gepairt.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
43012	Das zu aktualisierende Terminal ist aktuell nicht erreichbar und wird bei Wiedererreichbarkeit aktualisiert.	TECHNICAL	INFO		-
43013	Fehler bei Registrierung des Konnektors im Registrierungsserver. Fehler: […]	TECHNICAL	ERROR		-
43014	Fehler bei Registrierung des Konnektors im Konnektor.	TECHNICAL	ERROR		-
43015	Fehler bei Deregistrierung des Konnektors im Registrierungsserver. Fehler: […]	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
43016	Fehler bei Deregistrierung des Konnektors im Konnektor.	TECHNICAL	ERROR		-
43017	Fehler bei Statusabfrage beim Registrierungsserver im Registrierungsserver. Fehler: […]	TECHNICAL	ERROR		-
43018	Fehler bei Statusabfrage beim Registrierungsserver im Konnektor.	TECHNICAL	ERROR		-
43019	Beim hochladen eines Updatefiles ist ein Fehler aufgetreten.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
43022	Beim Laden der öffentlichen Schlüssel für den KSR ist ein Fehler aufgetreten. Ein Update über KSR ist daher nicht möglich.	TECHNICAL	ERROR		-
43023	Das zu aktualisierende Terminal wurde nicht gefunden.	TECHNICAL	ERROR		-
43024	Die Zugangsdaten für die Admin-Session am Terminals wurden noch nicht komplett hinterlegt.	TECHNICAL	ERROR		-
43025	Der KSR steht nicht zur Verfügung, wenn der Konnektor nicht mit der TI verbunden ist.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
43026	Die URL zum KSR konnte nicht aufgelöst werden.	TECHNICAL	WARNING		-
43027	Die URL zum Registrierungs-server konnte nicht aufgelöst werden.	TECHNICAL	WARNING		-
43028	Beim Hochla-den einer Firmware-Datei ist ein Fehler aufgetreten. Datei nicht in UpdateInfo.xml enthalten.	TECHNICAL	ERROR		-
43029	Eine Aktualisie-rung wird gera-de herunter geladen. Ein Zurücksetzen des Bereiches 'Aktualisierung' ist derzeit nicht möglich.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
43030	Eine Aktualisierung wird gerade installiert. Ein Zurücksetzen des Bereiches 'Aktualisierung' ist derzeit nicht möglich.	TECHNICAL	ERROR		-
43031	Eine Aktualisierung konnte nicht installiert werden. Signature des Firmwareupdates ungültig.	TECHNICAL	ERROR		-
43032	Eine Aktualisierung konnte nicht installiert werden. Package des Firmwareupdates ungültig.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
43033	Eine Aktualisierung konnte nicht installiert werden. Nicht genug Speicherplatz für den AK.	TECHNICAL	ERROR		-
43034	Eine Aktualisierung konnte nicht installiert werden. Nicht genug Speicherplatz für den NK.	TECHNICAL	ERROR		-
43035	Eine Aktualisierung konnte nicht installiert werden. Nicht genug Speicherplatz für die Zwischenablage.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
43036	Eine Aktualisierung konnte nicht installiert werden. Firmwareversion des Updates stimmt nicht mit den übergebenen Werten überein.	TECHNICAL	ERROR		-
43037	Eine Aktualisierung konnte nicht installiert werden. Firmware-Gruppen-Information ist kleiner oder gleich der bereits installierten Firmwaregruppe.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
43038	Eine Aktualisierung konnte nicht installiert werden. Signatur der NK-Firmware ungültig.	TECHNICAL	ERROR		-
43039	Eine Aktualisierung konnte nicht installiert werden. Signatur der AK-Firmware ungültig.	TECHNICAL	ERROR		-
43040	Eine Aktualisierung konnte nicht installiert werden. Prüfschlüssel nicht verfügbar.	TECHNICAL	ERROR		-
43041	Eine Aktualisierung konnte nicht installiert werden. Der Fehler konnte nicht ermittelt werden.	TECHNICAL	ERROR		-

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
43054	Die Verarbeitung der Anfrage im Netzkonnektor hat zulange gedauert. Aktion: …	TECHNICAL	ERROR		-
43050	Fachmodul […]	TECHNICAL	INFO	43050	Fachmodul […]
43051	Fachmodul […]	TECHNICAL	WARNING	43051	Fachmodul […]
43052	Fachmodul […]	TECHNICAL	ERROR	43052	Fachmodul […]
43053	Fachmodul […]	TECHNICAL	FATAL	43053	Fachmodul […]

12.3.2 Weitere Meldungen zu Verbindungsproblemen

Legende:

Code	Fehler-ID (dient als Referenz der gematik)
Beschreibung/ Mögliche Ursache	Kurze Zusammenfassung
Typ	Je nach Typ werden Meldungen in verschiedene Logdateien geschrieben (SECURITY,TECHNICAL).
Level	Einstufung nach Schwere des Vorfalls (FATAL, ERROR, WARNING, INFO)
Fehlerbehebung/ Weitere Angaben	Anleitung zur Behebung, falls möglich. Wenden sie sich bei Fragen an den DVO.

Alle nachfolgenden Meldungen werden nur in den Protokollspeicher geschrieben und nicht an das PVS gesendet. Diese Meldungen wertet nur der DVO (nicht der Leistungserbringer) aus.

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
45000	unspecified error	Fehler beim Verbindungsaufbau zur TI	Technical	Error	Konnektor neu starten
45001	cannot connect to VICI socket	charon Dämon läuft nicht	Technical	Fatal	Konnektor neu starten
45002	failed to create or to queue VICI command	Programmfehler	Technical	Error	Operation wiederholen
45003	could not read from or write to VICI socket	charon Dämon läuft nicht	Technical	Error	Konnektor neu starten
45004	VICI command returned an error	temporäres Problem in den Umsys-temen	Technical	Error	Operation wiederholen
45005	cannot access DNS server	Fehlkonfiguration	Technical	Fatal	Konnektor neu starten
45006	initiating failed with a fatal error	Fatales Problem beim Aufbau der VPN Vernindung	Technical	Fatal	Operation wiederholen
45007	failed to configure DNS	DNS Server startet nicht	Technical	Fatal	Konnektor neu starten
45008	failed to configure or fetching DNS trusted keys	TI DNS Server wird nicht erreicht	Technical	Error	Operation wiederholen
45009	file not found	Fehlkonfiguration oder HW Problem	Technical	Fatal	Wenn nicht durch Neustart zu lö-sen, Konnektor einschicken
45010	out of memory	Programmierfehler	Technical	Error	Konnektor neu starten
45011	file problem	Hardware Schaden (vermutlich SSD)	Technical	Fatal	Wenn nicht durch Neustart zu lö-sen, Konnektor einschicken

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
45012	no answer from charon after sending command	charon Dämon läuft nicht	Technical	Error	Operation wiederholen
45013	SIS cannot be initiated while TI is down	Anwenderfehler (kein SIS ohne TI!)	Technical	Error	Manuell Verbindung zu TI starten
45014	unable to activate hash&url	Fehlkonfiguration	Technical	Fatal	Wenn nicht durch Neustart zu lösen, Konnektor einschicken
45015	unable to send mosquitto event	Mosquitto Service nicht erreichbar	Technical	Error	Konnektor neu starten
45016	unable to make strongswan settings	Fehlkonfiguration	Technical	Fatal	Wenn nicht durch Neustart zu lösen, Konnektor einschicken
45017	unable to open error notify socket	charon Dämon läuft nicht	Technical	Fatal	Konnektor neu starten
45018	cannot connect to error notify socket	charon Dämon läuft nicht	Technical	Fatal	Konnektor neu starten
45019	cannot read from error notify socket	charon Dämon läuft nicht	Technical	Error	Konnektor neu starten
45020	VPNTINET not defined or not readable	Fehlkonfiguration	Technical	Error	VPNTINET in die Konfiguration eintragen
45021	VPNSISNET not defined or not readable	Fehlkonfiguration	Technical	Error	VPNSISNET in die Konfiguration eintragen
45022	virtual IP address received from TI concentrator does not belong to configured VPNTINET	Fehlkonfiguration	Technical	Error	Konfiguration VPNTINET prüfen

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
45023	virtual IP address received from SIS concentrator does not belong to configured VPNSISNET	Fehlkonfiguration	Technical	Error	Konfiguration VPNSISNET prüfen
45024	failed parsing VICI response	Inkompatiblität (VICI-Bibliothek passt nicht zum connector-vpnman	Technical	Error	Support kontaktieren
45025	unexpected element while parsing VICI response	Fehlkonfiguration des Konnektors	Technical	Error	Konfiguration (VPN) des Konnektors überprüfen und korrigieren.
45026	could not register callback	Laufzeitfehler in der VICI-Bibliothek aufgetreten	Technical	Error	Konnektor neu starten
45027	could not unregister callback	Laufzeitfehler in der VICI-Bibliothek aufgetreten	Technical	Error	Konnektor neu starten
45028	could not set IP and/or virtual IP for TI connection	Laufzeitfehler in der VICI-Bibliothek aufgetreten	Technical	Error	Konnektor neu starten
45029	parse error: unable to read IP address	Fehlkonfiguration des Konnektors	Technical	Error	Konfiguration (VPN) des Konnektors überprüfen und korrigieren.
45030	could not set IP and/or virtual IP for SIS connectio	Laufzeitfehler in der VICI-Bibliothek aufgetreten	Technical	Error	Konnektor neu starten
45031	poll() failed	Kommunikationsfehler zwischen dem connector-vpnman und dem charon-Daemon (strongSwan VPN) aufgetreten	Technical	Error	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
45032	unknown type of connection	Laufzeitfehler in der VICI-Bibliothek aufgetreten	Technical	Error	Konnektor neu starten
45033	failed reading from file	Multiple Fehlerursachen: • Korruptes Dateisystem (HW-Fehler) • Dateisystem voll • HW-Fehler des Hintergrund-speichers Fehlkonfiguration	Technical	Error	Konnektor neu starten; wenn sich nach dem Neustart keine Veränderung ergibt, den Support kontaktieren
45034	unable to send NK/DOMAIN_SRVZONE_TI be-cause config_dns did not return the data	Laufzeitfehler des Tools config_dns aufgetreten	Technical	Error	Konfiguration und Infrastruktur überprüfen, d.h. ob eine Verbin-dung mit dem Internet hergestellt werden kann
45035	error occurred while trying to con-nect to SIS	Der sichere Internetdienst wurde kon-figuriert, ist jedoch nicht erreichbar (dessen VPN-Kanal)	Technical	Error	Konfiguration und Infrastruktur überprüfen, d.h. ob eine Verbin-dung mit dem Internet hergestellt werden kann
45036	could not create thread	Laufzeitfehler des connector-vpnman aufgetreten	Technical	Error	Konnektor neu starten
45037	could not create file	Hintergrundspeicher ist voll oder es ist ein HW-Fehler des Hintergrund-speichers aufgetreten	Technical	Error	Logdateien auf dem Konnektor löschen und neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
45038	unable to connect to MQTT broker	MQTT Broker nicht erreichbar	Technical	Fatal	Konnektor neu starten
45039	error reading certificate from smartcard	Es liegt möglicherweise ein HW-Fehler im Konnektor vor.	Technical	Error	Konnektor neu starten; wenn sich nach dem Neustart keine Veränderung ergibt, den Support kontaktieren
45040	smartcard is not readable	Es liegt möglicherweise ein HW-Fehler im Konnektor vor.	Technical	Fatal	Konnektor neu starten; wenn sich nach dem Neustart keine Veränderung ergibt, den Support kontaktieren
45041	internal error occurred while verifying certificate	Es ist ein Laufzeitfehler im connector-vpnman aufgetreten.	Technical	Error	Konnektor neu starten
45042	keyUsage extension of concentrator certififate is not critical (but must be critical)	Das X.509v3-Zertifikat des VPN-Zugangsdienstes ist fehlerhaft.	Technical	Error	Setzen Sie sich mit dem Betreiber des VPN-Zugangsdienstes in Verbindung.
45043	CRL signer certificate of CRL is expired	Es liegt eine Sperrliste (CRL) vor, deren Authentizität ist jedoch nicht überprüfbar.	Technical	Error	Setzen Sie sich mit dem Betreiber des VPN-Zugangsdienstes in Verbindung.
45044	no TSL information available - certificate verification must be aborted	Dem Konnektor steht keine TSL (Trusted Service List) zur Verfügung.	Technical	Error	Starten Sie den Konnektor neu (dies triggert u.a. Download-Vorgänge). Wenn sich nach einem Neustart keine Besserung ergibt, kontaktieren Sie den Support.

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
45045	public key of concentrators certifiate has a bit size of lesser than 2048	Das Schlüsselmaterial des VPN-Zugangsdienstes entspricht nicht den Anforderungen	Technical	Error	Setzen Sie sich mit dem Betreiber des VPN-Zugangsdienstes in Verbindung.
45046	invalid extension found in concentrator certificate marked as critical	Das X.509v3-Zertifikat des VPN-Zugangsdienstes ist fehlerhaft.	Technical	Error	Setzen Sie sich mit dem Betreiber des VPN-Zugangsdienstes in Verbindung.
45047	basic constraints extension of concentrator certifiifate is not critical (but must be critical)	Das X.509v3-Zertifikat des VPN-Zugangsdienstes ist fehlerhaft.	Technical	Error	Setzen Sie sich mit dem Betreiber des VPN-Zugangsdienstes in Verbindung.
45048	extension basic constraints not found in concentrator certificate"	Das X.509v3-Zertifikat des VPN-Zugangsdienstes ist fehlerhaft.	Technical	Error	Setzen Sie sich mit dem Betreiber des VPN-Zugangsdienstes in Verbindung.
45049	extension basic constraints of concentrator certificate indicates that this certificate is a CA	Das X.509v3-Zertifikat des VPN-Zugangsdienstes ist fehlerhaft.	Technical	Error	Setzen Sie sich mit dem Betreiber des VPN-Zugangsdienstes in Verbindung.
45050	CA certificate is revoked according to TSL	Der Aussteller (CA) des VPN-Zugangsdienst-Zertifikates ist nicht (mehr) gültig.	Technical	Error	Setzen Sie sich mit dem Betreiber des VPN-Zugangsdienstes in Verbindung.
45051	Unknown or unavailable certificate status (CA) in TSL	Die Trusted Service List (TSL) ist falsch formatiert.	Technical	Error	Setzen Sie sich mit dem Betreiber des VPN-Zugangsdienstes in Verbindung.

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
45052	Signature algorithm of EE and/or CA certificate is neither sha256WithRsaEncryption nor ecdsaWithSha256	Der Konnektor unterstützt laut Gematik-Spezifikation nur zwei Signaturalgorithmen (RSA mit SHA256 und ECDSA mit SHA256). Das Zertifikat des VPN-Zugangsdienstes und/oder der Aussteller-CA verwendet/verwenden einen anderen Algorithmus.	Technical	Error	Setzen Sie sich mit dem Betreiber des VPN-Zugangsdienstes in Verbindung.
45053	Unexpected config value at /ConfigData/VPNClient/VPNActivation	Die XML-Konfiguration ist fehlerhaft.	Technical	Error	Überprüfen Sie die VPN-Konfiguration in der Benutzeroberfläche.
45054	connector has not been activated	Der Konnektor kann sich nicht mit dem VPN-Zugangsdienst verbinden, da er noch nicht aktiviert wurde	Technical	Error	Aktivieren Sie zunächst den Konnektor oder wenden Sie sich an den Support.
45055	connector has been activated for TI only but VPN_SIS has been requested	Der Konnektor kann sich nicht mit dem VPN-Zugangsdienst (hier: SIS-Kanal) verbinden, da er noch nicht aktiviert wurde	Technical	Error	Aktivieren Sie zunächst das SIS-Feature des Konnektors oder wenden Sie sich an den Support.
45056	unable to send NK/DOMAIN_SRVZONE_SIS because config_dns did not return the data	Laufzeitfehler des Tools config_dns aufgetreten	Technical	Error	Konfiguration und Infrastruktur überprüfen, ob eine Verbindung mit dem Internet hergestellt werden kann
45100	Internal error (configuration bad) occurred.	Nicht behebbarer Laufzeitfehler	Technical	Error	Mit Log-Dateien an Hersteller wenden

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
45101	iproute2 utility reports error %i.	Laufzeitfehler (race condition)	Technical	Error	Konnektor neu starten
45102	MQTT: Unable to send event %s.	Laufzeitfehler des MQTT-Brokers	Technical	Error	Konnektor neu starten
45105	Unable to create/write configuration file %s.	SSD-Kapazität erschöpft	Technical	Error	Log-Dateien löschen oder Werksreset durchführen
45106	Unable to execute DHCP client.	ISC-DHCP-Client nicht ausführbar (z.B. DHCP renew)	Technical	Error	Mit Log-Dateien an Hersteller wenden (möglicherweise SSD defekt)
45107	IPv4 address %s overlaps with net Offene Fachdienste"	IP-Überlappung zwischen dem Geschlossenen Fachdienstenetz, dem Offenen FD-Netz und dem lokalen Netz	Technical	Error	Interne IT-Infrastruktur anpassen und DHCP-Server umkonfigurieren
45108	IPv4 address %s overlaps with net Geschlossene Fachdienste	IP-Überlappung zwischen dem Geschlossenen Fachdienstenetz und dem lokalen Netz	Technical	Error	Interne IT-Infrastruktur anpassen und DHCP-Server umkonfigurieren
45109	IPv4 address %s overlaps with net TI Zentral	IP-Überlappung zwischen dem Netz der TI, dem Zentraldiesntenetz und dem lokalen Netz	Technical	Error	Interne IT-Infrastruktur anpassen und DHCP-Server umkonfigurieren
45110	IPv4 address %s overlaps with net TI Dezentral (Konnektoren)	IP-Überlappung zwischen dem Netz der TI und dem lokalen Netz	Technical	Error	Interne IT-Infrastruktur anpassen und DHCP-Server umkonfigurieren
45111	IPv4 address %s overlaps with net TI Dezentral SIS (Konnektoren)	IP-Überlappung zwischen dem SIS-Netz und dem lokalen Netz	Technical	Error	Interne IT-Infrastruktur anpassen und DHCP-Server umkonfigurieren

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
45112	IPv4 address %s overlaps with net Lokale virtuelle Maschinen	IP-Überlappung zwischen dem internen Netz und dem lokalen Netz	Technical	Error	Interne IT-Infrastruktur anpassen und DHCP-Server umkonfigurieren
45113	IPv4 address %s overlaps with inventory network	IP-Überlappung zwischen dem Bestandsnetz und dem lokalen Netz	Technical	Error	Interne IT-Infrastruktur anpassen und DHCP-Server umkonfigurieren
45114	IPv4 address %s overlaps with client intranet route	Fehlerhaft gesetzte/unnötige lokale Netzwerkroute	Technical	Error	Interne IT-Infrastruktur anpassen und DHCP-Server umkonfigurieren
45300	iptables utility reports error %i.	Laufzeitfehler (race condition)	Technical	Error	Konnektor neu starten
45301	Unable to publish topic NK/AK/STATE	Laufzeitfehler (race condition)	Technical	Error	Konnektor neu starten
45302	Unable to create virtual machine base folder %s.	SSD-Kapazität erschöpft	Technical	Error	Log-Dateien löschen oder Werksreset durchführen
45303	Unable to change ownership of virtual machine base folder %s.	SSD-Kapazität erschöpft	Technical	Error	Log-Dateien löschen oder Werksreset durchführen
45304	Unable to change access rights of virtual machine base folder %s.	SSD-Kapazität erschöpft	Technical	Error	Log-Dateien löschen oder Werksreset durchführen
45305	Unable to create DHCP (server) base folder %s.	SSD-Kapazität erschöpft	Technical	Error	Log-Dateien löschen oder Werksreset durchführen
45306	Unable to create DHCP (server) configuration file %s.	SSD-Kapazität erschöpft	Technical	Error	Log-Dateien löschen oder Werksreset durchführen

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
45307	Unable to parse IPv4 address %s.	Fehlerhafte Konfiguration	Technical	Error	Konfiguration prüfen und neu laden
45308	Unable to start DHCP (server) for virtual machine.	Arbeitsspeicher erschöpft	Technical	Error	Konnektor neu starten
45309	Unable to spawn VBOXSvc service (1/2)	Arbeitsspeicher erschöpft	Technical	Error	Konnektor neu starten
45310	Unable to spawn VBOXSvc service (2/2)	Arbeitsspeicher erschöpft	Technical	Error	Konnektor neu starten
45311	Unable to create VBOX virtual machine (1/6)	SSD-Kapazität erschöpft	Technical	Error	Log-Dateien löschen oder Werksreset durchführen
45312	Unable to create VBOX virtual machine (2/6)	SSD-Kapazität erschöpft	Technical	Error	Log-Dateien löschen oder Werksreset durchführen
45313	Unable to create VBOX virtual machine (3/6)	SSD-Kapazität erschöpft	Technical	Error	Log-Dateien löschen oder Werksreset durchführen
45314	Unable to create VBOX virtual machine (4/6)	SSD-Kapazität erschöpft	Technical	Error	Log-Dateien löschen oder Werksreset durchführen
45315	Unable to create VBOX virtual machine (5/6)	SSD-Kapazität erschöpft	Technical	Error	Log-Dateien löschen oder Werksreset durchführen
45316	Unable to create VBOX virtual machine (6/6)	SSD-Kapazität erschöpft	Technical	Error	Log-Dateien löschen oder Werksreset durchführen
45318	Unable to start the VBOX virtual machine	AK-VM korrupt	Technical	Error	Support kontaktieren

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
45319	Unable to shutdown the VBOX virtual machine.	AK-VM hängt	Technical	Error	Konnektor neu starten
45320	Unable to start MQTT thread.	MQTT-Broker läuft nicht	Technical	Error	Konnektor neu starten
45321	Unable to initiate MQTT [1].	MQTT-Broker läuft nicht	Technical	Error	Konnektor neu starten
45322	Unable to initiate MQTT [2].	MQTT-Broker läuft nicht	Technical	Error	Konnektor neu starten
45323	Unable to connect to MQTT broker.	MQTT-Broker läuft nicht	Technical	Error	Konnektor neu starten
45324	Unable to set timesync value. [1/4]	Kommunikation mit der VBOX-API fehlgeschlagen	Technical	Error	Konnektor neu starten
45325	Unable to set timesync value. [2/4]	Kommunikation mit der VBOX-API fehlgeschlagen	Technical	Error	Konnektor neu starten
45326	Unable to set timesync value. [3/4]	Kommunikation mit der VBOX-API fehlgeschlagen	Technical	Error	Konnektor neu starten
45327	Unable to set timesync value. [4/4]	Kommunikation mit der VBOX-API fehlgeschlagen	Technical	Error	Konnektor neu starten
45500	Executable not defined (nickname=%s).	Konfiguration fehlerhaft	Technical	Error	Konfiguration prüfen, ggf. Konnektor neu starten
45502	Unable to create tap device %s.	Fehler im Netzwerkstack	Technical	Error	Konnektor neu starten
45503	Unable to bring tap device %s up.	Fehler im Netzwerkstack	Technical	Error	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
45504	Unable to parse IPv4 address %s.	Konfigurationsfehler	Techncal	Error	Konfiguration prüfen und neu laden
45506	Unable to flush IP addresses of WAN device %s.	Fehler im Netzwerkstack	Technical	Error	Konnektor neu starten
45507	Unable to flush IP addresses of LAN device %s.	Fehler im Netzwerkstack	Technical	Error	Konnektor neu starten
45508	unable to enforce rule set %s because no rule sets defined.	Konfiguration fehlerhaft	Technical	Error	Konfiguration prüfen, ggf. Konnektor neu starten
45509	unable to enforce rule set %s because it is UNKNOWN.	Konfiguration fehlerhaft	Technical	Error	Konfiguration prüfen, ggf. Konnektor neu starten
45510	insufficient memory available.	RAM-Speicherkapazität erschöpft	Technical	Error	Konnektor neu starten
45511	unable to purge limit rule - rule set tastes bad	Konfiguration fehlerhaft	Technical	Error	Konfiguration prüfen, ggf. Konnektor neu starten
45512	unable to determine route to host %s (TI concentrator).	Routing-Konfiguration fehlerhaft	Technical	Error	Konfiguration prüfen und neu laden
45513	unable to determine route to host %s (SIS concentrator).	Routing-Konfiguration fehlerhaft	Technical	Error	Konfiguration prüfen und neu laden
45514	unknown substitution prefix found.	Konfiguration fehlerhaft	Technical	Error	Konfiguration prüfen, ggf. Konnektor neu starten
45515	expected exit code is %i, returned exit code is %i.	Netfilter-Problem im Kernel	Technical	Error	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
45519	(UNWIND) expected exit code is %i, returned exit code is %i.	Netfilter-Problem im Kernel	Technical	Error	Konnektor neu starten
45520	unable to perform global (initial) main configuration.	Netfilter-Problem im Kernel	Technical	Error	Konnektor neu starten
45521	unable to perform global (initial) ip configuration.	Netzwerkstack-Problem im Kernel	Technical	Error	Konnektor neu starten
45522	unable to perform global (initial) xfrm configuration.	XFRM-Problem im Kernel	Technical	Error	Konnektor neu starten
45523	unable to perform global (initial) ip-tables configuration.	Netfilter-Problem im Kernel	Technical	Error	Konnektor neu starten
45524	Enforcement of initial (static) rules succeeded.	-	Technical	Info	-
45525	unable to create MQTT thread.	MQTT-Broker reagiert nicht	Technical	Error	Konnektor neu starten
45531	Unable to purge previous default gateway (on LAN changed).	Netzwerkstack-Fehler	Technical	Error	Konnektor neu starten
45532	Unable to parse a received (LAN) IPv4 address / netmask combination.	Konnektor-Konfiguration fehlerhaft	Technical	Error	Konfiguration prüfen und neu laden
45533	Unable to establish a new default gateway (LAN change)	Netzwerkstack-Fehler	Technical	Error	Konnektor neu starten
45534	Unable to purge previous default gateway (on WAN changed).	Netzwerkstack-Fehler	Technical	Error	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
45535	Unable to establish a new default gateway (WAN change).	Netzwerkstack-Fehler	Technical	Error	Konnektor neu starten
45536	[onConfigChanged] unable to read/parse the global XML configuration	Neue (geänderte) Konnektor-Konfiguration fehlerhaft	Technical	Error	Konfiguration prüfen und neu laden
45537	Internal error (configuration bad) occurred.	Konfiguration fehlerhaft	Technical	Error	Konfiguration prüfen, ggf. Konnektor neu starten
45538	iproute2 utility reports error %i.	Netzwerkstack-Fehler	Technical	Error	Konnektor neu starten
45542	mosquitto_new	Mosquitto Service nicht erreichbar	Technical	Error	Konnektor neu starten
45543	mosquitto_threaded_set	Mosquitto Service nicht erreichbar	Technical	Error	Konnektor neu starten
45544	mosquitto_subscribe	Mosquitto Service nicht erreichbar	Technical	Error	Konnektor neu starten
45545	Unable to flush XFRM policies	Netzwerkstack-Fehler	Technical	Error	Konnektor neu starten
45546	Unable to set host name %s of connector. EXIT	Netzwerkstack-Fehler	Technical	Error	Konnektor neu starten
46000	Enforcement of initial (static) rules failed. EXIT.	Netzwerkstack-Fehler	Technical	Fatal	Konnektor neu starten
46001	Unable to apply ANLW_LEKTR_INTRANET_ROUTES routes; current route is %s via %s (exitcode of route command is %i).	ANLW_LEKTR_INTRANET_ROUTES (siehe [gemSpec]) konneten nicht gesetzt werden	Technical	Fatal	Konfiguration prüfen und neu laden

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46002	Unable to apply ANLW_LEKTR_INTRANET_ROUTES routes; current route is %s via %s (insufficient memory available).	ANLW_LEKTR_INTRANET_ROUTES (siehe [gemSpec]) konneten nicht gesetzt werden	Technical	Fatal	Konfiguration prüfen und neu laden
46003	Unable to enforce rule stack ak. This is fatal.	Regelsatz AK kann nicht eingesetzt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten
46004	Unable to enforce rule stack lan. This is fatal.	Regelsatz LAN kann nicht eingesetzt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten
46005	Unable to enforce rule stack lanwan. This is fatal.	Regelsatz LANWAN kann nicht eingesetzt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten
46006	Unable to enforce rule stack services. This is fatal.	Regelsatz SERVICES kann nicht eingesetzt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten
46007	Unable to enforce rule stack vpn-sis (MGM ONLINE). This is fatal.	Regelsatz VPN-SIS/ONLINE kann nicht eingesetzt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten
46008	Unable to enforce rule stack vpn-sis. This is fatal.	Regelsatz VPN-SIS kann nicht eingesetzt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten
46009	Unable to enforce rule stack vpn-ti (MGM ONLINE). This is fatal.	Regelsatz VPN-TI/ONLINE kann nicht eingesetzt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46010	Unable to enforce rule stack vpn-ti. This is fatal.	Regelsatz VPN-TI kann nicht eingesetzt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten
46011	Unable to enforce rule stack wan. This is fatal.	Regelsatz WAN kann nicht eingesetzt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten
46013	Unable to execute iproute2 command because command not defined (INTERNAL ERROR).	Konfiguration fehlerhaft	Technical	Fatal	Konfiguration prüfen und neu laden
46014	Unable to install new default gateway (exit code of ip command: %i).	Neues Default-Gateway ist nicht einsetzbar (routing-Problem)	Technical	Fatal	Konnektor neu starten
46016	Unable to remove previous default gateway (exit code of ip command: %i).	Vorheriges Default-Gateway kann nicht entfernt werden (routing-Problem)	Technical	Fatal	Konnektor neu starten
46018	Unable to unwind rule stack ak. This is fatal.	Regelsatz AK kann nicht entfernt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten
46019	Unable to unwind rule stack lan. This is fatal.	Regelsatz LAN kann nicht entfernt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten
46020	Unable to unwind rule stack lanwan. This is fatal.	Regelsatz LANWAN kann nicht entfernt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46022	Unable to unwind rule stack services. This is fatal.	Regelsatz SERVICES kann nicht entfernt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten
46023	Unable to unwind rule stack vpn-sis (MGM ONLINE). This is fatal.	Regelsatz VPN-SIS/ONLINE kann nicht entfernt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten
46024	Unable to unwind rule stack vpn-sis. This is fatal.	Regelsatz VPN-SIS kann nicht entfernt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten
46025	Unable to unwind rule stack vpn-ti (MGM ONLINE). This is fatal.	Regelsatz VPN-TI/ONLINE kann nicht entfernt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten
46026	Unable to unwind rule stack vpn-ti. This is fatal.	Regelsatz VPN-TI kann nicht entfernt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten
46027	Unable to unwind rule stack wan. This is fatal.	Regelsatz WAN kann nicht entfernt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten
46028	Unable to apply firewall SIS admin rule because src and dst IPs (at least one of them) not available.	Regelsatz SIS kann nicht gesetzt werden	Technical	Fatal	Konnektor neu starten
46029	Unable to apply firewall SIS admin rule because protocol not supported.	Regelsatz SIS admin kann nicht gesetzt werden	Technical	Fatal	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46030	Unable to apply ANLW_FW_SIS_ADMIN_RULES rule #%u (insufficient memory available)	Regelsatz SIS admin kann nicht gesetzt werden	Technical	Fatal	Konnektor neu starten
46031	Unable to apply ANLW_FW_SIS_ADMIN_RULES	Regelsatz SIS admin kann nicht gesetzt werden	Technical	Fatal	Konnektor neu starten
46032	Unable to parse a received (WAN) IPv4 address / netmask combination.	Regelsatz WAN kann nicht gesetzt werden	Technical	Fatal	Konnektor neu starten
46033	Unable to purge previous default gateway (on SIS up)	Default GW kann nicht gelöscht werden	Technical	Fatal	Konnektor neu starten
46034	Unable to establish a new default gateway (SIS up)	Neues default GW kann nicht gesetzt werden	Technical	Fatal	Konnektor neu starten
46035	Unable to purge previous default gateway (on SIS down)	Default GW kann nicht gelöscht werden	Technical	Fatal	Konnektor neu starten
46036	Unable to establish a new default gateway (non-SIS, SIS down)	Neues default GW kann nicht gesetzt werden	Technical	Fatal	Konnektor neu starten
46500	Configuration xpath %s could not be determined.	Konfiguration fehlerhaft	Technical	Error	Konfiguration prüfen und neu laden
46501	[ConfigChange] Could not perform the UDP bind to socket %s.	Bind an UDP-Socket nicht möglich (in Benutzung?)	Technical	Error	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46502	[ConfigChange] Unable to make UDP socket %s (SICCT) non-blocking.	UDP-Socket (SICCT) kann nicht auf non-blocking geschaltet werden	Technical	Error	Konnektor neu starten
46503	Receive routine (SICCT, UDP) returned an error.	UDP-Packet (SICCT) konnte nicht empfangen werden (oder das SICCT-Packet ist falsch formatiert - ASN.1	Technical	Error	keine Aktion
46504	AK did not send a keep-alive within %u second(s) for %u time(s). Rebooting AK virtual machine now.	Anwendungskonnektor mutmaßlich tot	Technical	Error	keine Aktion, AK wird automatisch neu gestartet
46505	Unable to fire event with ID=%s because the PID could not be read from %s	Connector-Service kann bei einer Änderung der Konfiguration einen nachgeschalteten Prozess nicht erreichen	Technical	Error	keine Aktion
46506	Failed to send SIGHUP for event with ID=%s, pid=%lu	Connector-Service kann bei einer Änderung der Konfiguration kein SIGHUP-Signal an einen nachgeschalteten Prozess senden	Technical	Error	keine Aktion
46507	Could not compute the broadcast IP address (SICCT).	SICCT-Konfiguration fehlerhaft	Technical	Error	Konfiguration prüfen und neu laden
46508	Could not perform the UDP bind to socket %s.	bind() an UDP-Socket nicht möglich	Technical	Error	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46509	Unable to make UDP socket %s (SICCT) non-blocking.	UDP-Socket (SICCT) kann nicht auf non-blocking geschaltet werden (keine Dublette zu 46502, da dieser Fehlercode auf eine andere Ursache hindeutet - für die SW-Entwicklung)	Technical	Error	Konnektor neu starten
46510	Handling MQTT topics (events) resulted in %i failure(s).	Eine gewisse Anzahl an MQTT-Events konnte nicht verarbeitet werden	Technical	Error	keine Aktion
46511	Failed to compile XML-TSL to binary trust store.	Die übergebene TSL ist fehlerhaft (kann sogar bzgl. XML-Schema korrekt sein, ihr fehlt jedoch z.B. eine CRL-Download-URL)	Technical	Error	TSL überprüfen und neu laden
46512	ERROR: Unable to create POSIX thread.	Thread kann nicht erstellt werden	Technical	Error	Konnektor neu starten
46513	ERROR: Unable to create POSIX thread (2).	Thread kann nicht erstellt werden	Technical	Error	Konnektor neu starten
46514	ERROR: Unable to create MQTT thread.	Thread kann nicht erstellt werden	Technical	Error	Konnektor neu starten
46515	ERROR: Unable to create new MQTT client instance.	MQTT-Broker reagiert nicht	Technical	Error	Konnektor neu starten
46516	ERROR: Unable to set MQTT to threaded.	MQTT-Broker reagiert nicht	Technical	Error	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46517	ERROR: Unable to connect to MQTT broker (%s:%i).	MQTT-Broker reagiert nicht	Technical	Error	Konnektor neu starten
46518	ERROR: Unable to subscribe to ALL MQTT topics.	MQTT-Broker reagiert nicht	Technical	Error	Konnektor neu starten
46519	ERROR: Unable to initialize the protocol service.	Protokollierungsdienst nicht initialisierbar (ggf. ist eine/mehrere der SQLite-Datenbanken korrupt)	Technical	Error	Konnektor neu installieren
46520	Unable to listen on primary port %i	Connector-Service kann sich nicht an TCP-Port 18080 binden.	Technical	Error	Konnektor neu starten
46521	Unable to listen on secondary port %i	Connector-Service kann sich nicht an TCP-Port 18081 binden.	Technical	Error	Konnektor neu starten
46522	Mosquitto loop returned error: %i (MOSQ_ERR_NO_CONN).	MQTT-Broker reagiert nicht	Technical	Error	keine Aktion; der Service versucht stetig, die Verbindung neu aufzubauen
46523	Mosquitto loop returned error: %i (MOSQ_ERR_CONN_LOST).	MQTT-Broker reagiert nicht	Technical	Error	keine Aktion; der Service versucht stetig, die Verbindung neu aufzubauen
46524	Mosquitto loop returned error: %i (MOSQ_ERR_UNKNOWN).	MQTT-Broker reagiert nicht	Technical	Error	keine Aktion; der Service versucht stetig, die Verbindung neu aufzubauen
46525	Mosquitto loop returned error: %i (MOSQ_ERR_ERRNO).	MQTT-Broker reagiert nicht	Technical	Error	keine Aktion; der Service versucht stetig, die Verbindung neu aufzubauen

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46526	Mosquitto loop returned an error: %i.	MQTT-Broker reagiert nicht	Technical	Error	keine Aktion; der Service versucht stetig, die Verbindung neu aufzubauen
46527	mosquitto reconnect SUCCEEDED.	MQTT-Broker reagiert nicht	Technical	Error	keine Aktion; der Service versucht stetig, die Verbindung neu aufzubauen
46528	mosquitto reconnect FAILED.	MQTT-Broker reagiert nicht	Technical	Error	keine Aktion; der Service versucht stetig, die Verbindung neu aufzubauen
46529	Unable to perform epoll_create.	Der Aufruf des syscalls epoll_create ist fehlgeschlagen	Technical	Error	Konnektor neu starten
46530	error locking system state information (rc=%d)	Zugriff auf die Informationen zu den aktuellen Softwareständen nicht möglich	Technical	Error	Konnektor neu starten
46531	error retrieving system state information: %d	Zugriff auf die Informationen zu den aktuellen Softwareständen nicht möglich	Technical	Error	Konnektor neu starten
46532	error retrieving system ID: %d	Zugriff auf die Informationen zu den aktuellen Softwareständen nicht möglich	Technical	Error	Konnektor neu starten
46533	error retrieving application image ID: %d	Zugriff auf die Informationen zu den aktuellen Softwareständen nicht möglich	Technical	Error	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46534	Unable to open pipe to connector updater.	Ein Update des Konnektors ist nicht möglich.	Technical	Error	Konnektor neu starten und Updateprozess wiederholen; sollte ein Update immer noch scheitern, dann den Support informieren
46535	Insufficient memory available updating software.	Ein Update des Konnektors ist nicht möglich.	Technical	Error	Konnektor neu starten und Updateprozess wiederholen; sollte ein Update immer noch scheitern, dann den Support informieren
46536	Unable to write data over the update pipe.	Ein Update des Konnektors ist nicht möglich.	Technical	Error	Konnektor neu starten und Updateprozess wiederholen; sollte ein Update immer noch scheitern, dann den Support informieren
46537	Download CRL : internal parameter error.	Download-CRL mit falschen Parametern aufgerufen (software bug)	Technical	Error	Support informieren
46538	Download CRL : internal error.	Interner Fehler aufgetreten, z.B. kein RAM-Speicher mehr verfügbar	Technical	Error	Konnektor neu starten
46539	Download CRL : unable to read trust store.	Der Trust-Store ist nicht verfügbar, was bedeutet, dass keine TSL im Konnektor verfügbar ist (z.B. ist die TSL abgelaufen)	Technical	Error	TSL über die MGMT-UI neu einbringen oder Support kontaktieren

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46540	Download CRL : generic error.	Nicht näher spezifizierter Fehler beim Download der CRL aufgetreten	Technical	Error	Auto-Download der CRL in der MGMT-UI erneut anstoßen; bei wiederholtem Fehler: Support kontaktieren
46541	Download CRL : no CRL distribution point (ServiceSupplyPoint) available.	Die TSL im Konnektor ist nicht vorhanden oder fehlerhaft (weil die CRL-Download-URL in der TSL verzeichnet ist und von dort bezogen wird)	Technical	Error	Einbringen der TSL in der MGMT-UI erneut anstoßen; bei wiederholtem Fehler: Support kontaktieren
46542	Download CRL : unable to download CRL (network error).	Die CRL kann aufgrund eines Netzwerkfehlers nicht heruntergeladen werden (z.B. findet aktuell eine Umkonfigurierung statt oder der Server ist tatsächlich "down").	Technical	Error	Auto-Download der CRL in der MGMT-UI erneut anstoßen; bei wiederholtem Fehler: Support kontaktieren
46543	Download CRL : unable to ASN.1 parse the CRL.	Die CRL ist syntaktisch nicht korrekt. Dies ist ein Fehler der Telematikinfrastruktur.	Technical	Error	Auto-Download der CRL in der MGMT-UI erneut anstoßen; bei wiederholtem Fehler: Support kontaktieren
46544	Download CRL : downloaded CRL is not valid anymore.	Die CRL wurde soeben aktualisiert aber ist nicht mehr gültig. Dies ist entweder ein Fehler der Telematikinfrastruktur oder die Zeitsynchronisation des Konnektors ist fehlgeschlagen, und der Konnektor arbeitet mit einer falschen Systemzeit.	Technical	Error	Auto-Download der CRL in der MGMT-UI erneut anstoßen; bei wiederholtem Fehler: Support kontaktieren oder Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46545	Download CRL : digital signature of downloaded CRL is invalid.	Die digitale Signatur der CRL ist mathematisch nicht korrekt. Dies ist ein Fehler der Telematikinfrastruktur.	Technical	Error	Auto-Download der CRL in der MGMT-UI erneut anstoßen; bei wiederholtem Fehler: Support kontaktieren
46546	Download CRL : CRL signer not found - unable to verify digital signature of CRL.	Der CRL-Signer (entweder ein CA-Zertifikat bei direkten CRLs oder ein EE-Zertifikat bei indirekten CRLs) ist nicht in der TSL vorhanden oder es ist keine TSL im Konnektor vorrätig.	Technical	Error	Auto-Download der CRL in der MGMT-UI erneut anstoßen; bei wiederholtem Fehler: Support kontaktieren
46547	Download CRL : CRL signer found but expired - unable to verify digital signature of CRL.	Die digitale Signatur der CRL ist nicht prüfbar, da der CRL-Signer abgelaufen ist. Dies ist ein Fehler der Telematikinfrastruktur.	Technical	Error	Auto-Download der CRL in der MGMT-UI erneut anstoßen; bei wiederholtem Fehler: Support kontaktieren
46548	Download CRL : unknown error code reported. Please contact software vendor.	Dies ist ein software bug und kann im Normalbetrieb nicht auftreten (nur, wenn ein Updatefehler des Konnektors vorliegt und inkompatible Komponenten ausgerollt wurden - was durch die Architektur des Updateprozesses ausgeschlossen ist)	Technical	Error	Support kontaktieren
46549	Unable to send SICCT MQTT message (new terminal announced).	Der NK kann den AK via MQTT nicht erreichen, um die Ankunft eines neuen SICCT-Terminals anzuzeigen.	Technical	Error	SICCT-Terminal trennen und erneut verbinden.

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46550	parseTSL: Invalid CPU architecture detected (only 64bit supported).	Dies ist ein so genannter "sanity check" innerhalb der Quellcodes und kann als Fehler nur auftreten, wenn der Konnektor in einer 32bit-Firmware betrieben wird, was nicht geplant ist.	Technical	Error	Keine Aktion, siehe Beschreibung links.
46551	parseTSL: Invalid parameters passed (please contact the software vendor).	Interner Software-Fehler (sanity check)	Technical	Error	Support kontaktieren
46552	parseTSL: TSL not readable (I/O error).	Die TSL (als Datei) kann nicht vom Hintergrundspeicher (SSD) gelesen werden.	Technical	Error	TSL über die MGMT-UI erneut einbringen. Bei wiederholtem Fehler, Support kontaktieren.
46553	parseTSL: Trust store (compiled TSL) not writable (I/O error).	Die TSL kann als binarisierte Version nicht im Hintergrundspeicher abgelegt werden.	Technical	Error	TSL über die MGMT-UI erneut einbringen. Bei wiederholtem Fehler, Support kontaktieren.
46554	parseTSL: Insufficient memory available.	Nicht genügend RAM-Speicher verfügbar	Technical	Error	TSL über die MGMT-UI erneut einbringen. Bei wiederholtem Fehler, Support kontaktieren.
46555	parseTSL: Unable to parse TSL XML.	Die TSL sind syntaktisch nicht korrekt. Dies ist ein Fehler der TI.	Technical	Error	TSL über die MGMT-UI erneut einbringen. Bei wiederholtem Fehler, TI kontaktieren
46556	parseTSL: Unable to parse X.509 (DER encoded) certificate(s) from the TSL.	Die in der TSL gespeicherten Zertifikate (oder mindestens eines davon) sind nicht korrekt (binär) formatiert.	Technical	Error	TSL über die MGMT-UI erneut einbringen. Bei wiederholtem Fehler, TI kontaktieren

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46557	parseTSL: TSL is empty.	Die TSL ist leer (das darf nicht auftreten, da mindestens eine Download-URL für CRLs benötigt wird).	Technical	Error	TSL über die MGMT-UI erneut einbringen. Bei wiederholtem Fehler, TI kontaktieren
46558	parseTSL: Internal error (sanity check(s) failed). Please contact the software vendor.	Software-Fehler	Technical	Error	Support kontaktieren
46559	parseTSL: Trust store (compiled TSL) not readable (epilogue checks failed).	Software-Fehler	Technical	Error	Support kontaktieren
46560	parseTSL: Trust store (compiled TSL) is corrupt.	Der binarisierte Trust-Store (aus TSL hervorgegangen) ist korrupt. Dies deutet auf einen I/O-Fehler des Hintergrundspeichers hin.	Technical	Error	TSL über die MGMT-UI erneut einbringen. Bei wiederholtem Fehler, Support kontaktieren.
46561	parseTSL: No CRL download URL found in the TSL.	Die TSL enthält keine CRL-Download-URL.	Technical	Error	TSL über die MGMT-UI erneut einbringen. Bei wiederholtem Fehler, TI kontaktieren.
46562	I/O error: unable to open file %s	Eine Datei kann nicht vom Hintergrundspeicher gelesen werden.	Technical	Error	Konnektor neu starten
46563	I/O error: file %s has zero length	Eine Datei wurde auf Länge 0 gekürzt (fälschlicherweise).	Technical	Error	Konnektor neu starten
46564	I/O error: reading file %s - insufficient memory available	Es ist nicht genug RAM-Speicher verfügbar.	Technical	Error	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46565	I/O error: reading file %s - read operation aborted (in front of EOF)	Eine Datei ist nicht komplett im Hintergrundspeicher verfügbar.	Technical	Error	Konnektor neu starten; bei erneutem Auftreten: Support kontaktieren
46566	writeCRL: Unable to read downloaded CRL from disk (network not ready?)	Da die automatische CRL asynchron im Hintergrund heruntergeladen wird, kann es in sehr raren Einzelfällen passieren, dass die CRL benötigt aber noch nicht vorhanden ist (und auch keine manuelle CRL im Konnektor vorliegt)	Technical	Error	Konnektor neu starten
46567	writeCRL: CRL not returned from server (error response received)	Der Web-Server, der die CRL anbietet, hat einen HTTP-Fehlercodes geliefert, anstatt die CRL anzubieten.	Technical	Error	Auto-Download der CRL in MGMT-UI neu anstoßen. Bei wiederholtem Fehler: ggf. auf manuelle CRL ausweichen. Bei immer noch bestehender Fehlerursache: TI informieren.
46568	writeCRL: Invalid function parameters passed	Software-Fehler	Technical	Error	Support informieren
46569	writeCRL: unable to parse X.509v3 certificate	Ein CRL-Signer-Zertifikat (Teil der CRL-Prüfung ist die Signaturprüfung der CRL) ist syntaktisch nicht korrekt.	Technical	Error	Auto-Download der CRL in MGMT-UI neu anstoßen. Bei wiederholtem Fehler: ggf. auf manuelle CRL ausweichen. Bei immer noch bestehender Fehlerursache: TI informieren.

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46570	writeCRL: unable to base64-decode	Ein BASE64-kodiertes ASN.1-Objekt kann nicht dekodiert werden.	Technical	Error	Auto-Download der CRL in MGMT-UI neu anstoßen. Bei wiederholtem Fehler: ggf. auf manuelle CRL ausweichen. Bei immer noch bestehender Fehlerursache: TI informieren.
46571	writeCRL: unable to load TI or SIS CRL from disk (maybe: not downloaded or set by management?)	Die CRL kann nicht geladen werden.	Technical	Error	Auto-Download der CRL in MGMT-UI neu anstoßen. Bei wiederholtem Fehler: ggf. auf manuelle CRL ausweichen. Bei immer noch bestehender Fehlerursache: Support kontaktieren.
46572	writeCRL: insufficient memory available	Nicht genügend RAM-Speicher verfügbar.	Technical	Error	CRL über das MGMT erneut einbringen. Bei immer noch bestehender Fehlerursache: Support kontaktieren.
46573	writeCRL: CRL parse error	Die CRL kann gemäß X.690 DER nicht dekodiert werden.	Technical	Error	Support kontaktieren.
46574	writeCRL: nextUpdate time not available or nextUpdate time expired: do NOT use this CRL	Die CRL nicht nicht korrekt formatiert (Syntaxfehler).	Technical	Error	Support kontaktieren.
46575	writeCRL: digital signature of CRL not valid	Die CRL ist ungültig, da sie mathematisch nicht verifiziert werden kann.	Technical	Error	Support kontaktieren.

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46576	writeCRL: CRL signer of CRL in question not found in trust store	Die CRL kann vom Konnektor nicht akzeptiert werden, da kein gültiger CRL-Signer vorhanden ist.	Technical	Error	TSL prüfen (ob eine TSL im Konnektor vorhanden ist); ggf. TSL erneut einbringen; Support kontaktieren
46577	writeCRL: CRL signer certificate of CRL is expired	Die CRL kann vom Konnektor nicht akzeptiert werden, da der zu verwendende CRL-Signer nicht mehr gültig ist.	Technical	Error	TSL prüfen (ob eine TSL im Konnektor vorhanden ist); ggf. TSL erneut einbringen; Support kontaktieren
46578	writeCRL: internal error; currently returned if revocation status returned by OpenSSL is not 0, 1 or 2	Software-Fehler	Technical	Error	Support kontaktieren
46579	writeCRL: I/O error (unable to read or write a file)	Zugriff auf den Hintergrundspeicher nicht möglich	Technical	Error	Vorgang wiederholen (CRL-Einbringung); bei wiederholtem Fehler: Support kontaktieren
46580	writeCRL: Invalid function parameters passed	Software-Fehler	Technical	Error	Support kontaktieren
46581	writeCRL: unable to parse X.509v3 certificate	Ein CRL-Signer-Zertifikat kann nicht gemäß X.690 geparsed werden.	Technical	Error	Support kontaktieren
46582	writeCRL: unable to base64-decode	Ein BASE64-kodiertes ASN.1-Objekt kann nicht dekodiert werden.	Technical	Error	Auto-Download der CRL in MGMT-UI neu anstoßen. Bei wiederholtem Fehler: ggf. auf manuelle CRL ausweichen. Bei immer noch bestehender Fehlerursache: TI informieren.

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46583	writeCRL: unable to load TI or SIS CRL from disk (maybe: not downloaded or set by management?)	Die CRL kann nicht geladen werden.	Technical	Error	Auto-Download der CRL in MGMT-UI neu anstoßen. Bei wiederholtem Fehler: ggf. auf manuelle CRL ausweichen. Bei immer noch bestehender Fehlerursache: Support kontaktieren.
46584	writeCRL: insufficient memory available	Nicht genügend RAM-Speicher verfügbar.	Technical	Error	CRL über das MGMT erneut einbringen. Bei immer noch bestehender Fehlerursache: Support kontaktieren.
46585	writeCRL: CRL parse error	Die CRL kann gemäß X.690 DER nicht dekodiert werden.	Technical	Error	Support kontaktieren.
46586	writeCRL: nextUpdate time not available or nextUpdate time expired: do NOT use this CRL	Die CRL nicht nicht korrekt formatiert (Syntaxfehler).	Technical	Error	Support kontaktieren.
46587	writeCRL: digital signature of CRL not valid	Die CRL ist ungültig, da sie mathematisch nicht verifiziert werden kann.	Technical	Error	Support kontaktieren.
46588	writeCRL: CRL signer of CRL in question not found in trust store	Die CRL kann vom Konnektor nicht akzeptiert werden, da kein gültiger CRL-Signer vorhanden ist.	Technical	Error	TSL prüfen (ob eine TSL im Konnektor vorhanden ist); ggf. TSL erneut einbringen; Support kontaktieren

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46589	writeCRL: CRL signer certificate of CRL is expired	Die CRL kann vom Konnektor nicht akzeptiert werden, da der zu verwendende CRL-Signer nicht mehr gültig ist.	Technical	Error	TSL prüfen (ob eine TSL im Konnektor vorhanden ist); ggf. TSL erneut einbringen; Support kontaktieren
46590	writeCRL: internal error; currently returned if revocation status returned by OpenSSL is not 0, 1 or 2	Software-Fehler	Technical	Error	Support kontaktieren
46591	writeCRL: I/O error (unable to read or write a file)	Zugriff auf den Hintergrundspeicher nicht möglich	Technical	Error	Vorgang wiederholen (CRL-Einbringung); bei wiederholtem Fehler: Support kontaktieren
46592	AK did not send a keep-alive within %u second(s) for %u time(s). AK REBOOT DISABLED SO CONTINUING EXECUTION.	AK konnte nicht gestartet werden	Technical	Error	Konnektor neu starten
46593	restart of virtual machine %s has failed	AK konnte nicht gestartet werden	Technical	Error	Konnektor neu starten
46594	start of virtual machine %s has failed	AK konnte nicht gestartet werden	Technical	Error	Konnektor neu starten
46595	stop of virtual machine %s has failed	AK konnte nicht beendet werden	Technical	Error	Konnektor neu starten
46596	unable to OS reboot/shutdown the konnektor	Konnektor kann nicht heruntergefahren werden	Technical	Error	Konnektor neu starten
46597	unable to stop virtual machine	AK konnte nicht beendet werden	Technical	Error	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46598	unable to reboot the konnektor	Neustart des Konnektor kann nicht durchgeführt werden	Technical	Error	Konnektor neu starten
46599	[RESTGetCRL] : Unable to acquire global lock.	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46600	[STARTUP] Unable to initialize TSL/CRL facility (unable to create mutex).	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46601	STARTUP] Unable to initialize TSL/CRL facility (unable to lock down TSL/CRL facility).	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46602	[STARTUP] Have automatic CRL but nextUpdate cannot be converted to integer system time.	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46603	[STARTUP] Have manual CRL but nextUpdate cannot be converted to integer system time.	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46604	[SHUTDOWN] Unable to initialize TSL/CRL facility (unable to lock mutex).	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46605	[SHUTDOWN] Unable to initialize TSL/CRL facility (unable to lock down TSL/CRL facility).	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46606	[POLL AUTOMATIC CRL] Unable to lock mutex.	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46607	[SET TSL] Unable to acquire mutex. INVALIDATION of current TSL cannot be performed.	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46608	[SET TSL] Unable to acquire global mutex. INVALIDATION of current TSL cannot be performed.	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46609	[SET TSL] Unable to acquire mutex. Establishment of new TSL cannot be performed.	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46610	[SET TSL] Unable to acquire global lock - unable to establish new trust store.	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46611	Unable to lock TSL/CRL mutex.	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46612	Unable to lock down TSL/CRL facility.	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46613	Unable to publish system event CERT/CRL/INVALID (TUC_KON_256)	Interner Verarbeitungsfehler	Technical	Fatal	Konnektor neu starten
46614	Unable to publish system event CERT/CRL/UPDATED (TUC_KON_256)	Interner Verarbeitungsfehler	Technical	Fatal	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46615	Unable to publish system event CERT/CRL/IMPORT (TUC_KON_256)	Interner Verarbeitungsfehler	Technical	Fatal	Konnektor neu starten
46616	Unable to download CRL from %s	Automatischer Download der CRL fehlgeschlagen	Technical	Error	CRL manuell einbringen
46617	writeCRL: no valid CRL returned from server (error response received)	CRL Download fehlgeschlagen. Download-Server meldet Fehler.	Technical	Error	CRL manuell einbringen
46618	[CRL logic] Unable to lock mutex	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46619	[UpdateCRL REST] Unable to lock mutex	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46620	[UpdateCRL REST] Unable to lock global mutex	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46621	[Force automatic CRL download] Unable to lock mutex	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46622	[Force automatic CRL download] : internal parameter error	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46623	[Force automatic CRL download] : internal error	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46624	[Force automatic CRL download] : unable to read trust store	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46625	[Force automatic CRL download] : generic error	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
46626	[Force automatic CRL download] : no CRL distribution point (ServiceSupplyPoint) available	CRL Distribution Point nicht verfügbar. Dieser fehlt in der TSL oder Adresse nicht mehr gültig bzw. Server nicht verfügbar.	Technical	Error	CRL manuell einbringen, ggf. TSL aktualisieren
46627	[Force automatic CRL download] : unable to download CRL (network error)	CRL konnte aufgrund eines NEtzwerkfehlers nicht geladen wwerden.	Technical	Error	Konnektor neu starten
46628	[Force automatic CRL download] : unable to ASN.1 parse the CRL	CRL konnte nicht dekodiert werden (ASN.1)	Technical	Error	Konnektor neu starten
46629	[Force automatic CRL download] : downloaded CRL is not valid anymore	Die heruntergeladenen CRL ist nicht mehr gültig.	Technical	Error	CRL manuell einbringen
46630	[Force automatic CRL download] : digital signature of downloaded CRL is invalid	Signatur der heruntergeladenen CRL ist ungültig.,	Technical	Error	CRL manuell einbringen
46631	[Force automatic CRL download] : CRL signer not found - unable to verify digital signature of CRL	Es konnte kein gültiger CRL Signer in der aktuellen TSL gefunden werden.	Technical	Error	TSL aktualisieren
46632	[Force automatic CRL download] : CRL signer found but expired - unable to verify digital signature of CRL	CRL Signer ist ungültig. Die SIgnatur der CRL konnte nicht verifiziert werden.	Technical	Error	TSL aktualisieren

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46633	[Force automatic CRL download] : unknown error code reported. Please contact software vendor	Interner Verarbeitungsfehler	Technical	Error	Konnektor neu starten
47500	Refusing update package	Das Update-Paket konnte nicht validiert werden (z.B. inkorrekte digitale Signatur)	Technical	Error	Support kontaktieren
47501	Unable to switch to update	Der aktuelle Konnektor-Laufzeitzustand verhindert, dass zum Updater gewechselt wird.	Technical	Error	Konnektor neu starten
47502	Update failed, failover to previous system	Es wurde ein Update erfolgreich eingespielt, jedoch kann der Konnektor mit diesem Update nicht starten, d.h. die neue Softwareversion ist nicht benutzbar. Der Konnektor wird beim nächsten Start sein vorheriges System booten.	Technical	Error	Konnektor neu starten
47503	Failure transforming configuration	Die Konfiguration des Updates (z.B. Firmware-Version) konnte nicht in das Konnektor-interne Format überführt werden.	Technical	Error	Support kontaktieren
47504	I/O error: unable to read or write a file	Der Zugriff auf den Hintergrundspeicher ist fehlgeschlagen.	Technical	Error	Support kontaktieren

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
47700	I/O error: unable to fetch DNSSEC credentials of zone %s from DNS service %s	Ein DNSSEC-Schlüssel kann nicht vom DNS-Server bezogen werden.	Technical	Error	Konnektor neu starten
47701	I/O error: unable to read or write a file	Der Zugriff auf den Hintergrundspeicher ist fehlgeschlagen.	Technical	Error	Konnektor neu starten
47703	I/O error: unable to execute process	Ein benötigter Kindprozess kann nicht gestartet werden.	Technical	Error	Konnektor neu starten
47704	I/O error: unable to resolve IP of network interface %s	Der Platzhalter %s kann entweder (eth0=WAN) oder (eth1=LAN) sein: Die IP-Adresse des Interfaces ist nicht abrufbar (dies ist z.B. möglich, wenn der Adapter aktuell "down" ist, weil eine DHCP-Rekonfiguration stattfindet).	Technical	Error	Konnektor neu starten
47705	I/O error: malformed base64 encoding	Vom DNS-Server gelieferte, BASE64-kodierte Informationen sind nicht dekodierbar.	Technical	Error	I und/oder Support informieren.
47706	I/O error: unknown action %s	Fehler in der Kommunikation mit dem DNS-Server	Technical	Error	TI und/oder Support informieren.
47707	I/O error: invalid option %c	Fehler in der Kommunikation mit dem DNS-Server	Technical	Error	TI und/oder Support informieren.
47708	I/O error: missing parameter	Fehler in der Kommunikation mit dem DNS-Server	Technical	Error	TI und/oder Support informieren.

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
47709	I/O error: error configuring DNS	Der lokale DNS-Server (bind v9) konnte nicht konfiguriert werden.	Technical	Error	Konnektor neu starten.
47710	I/O error: TSL not readable	Die TSL ist nicht lesbar oder befindet sich keine TSL auf dem Konnektor.	Technical	Error	In der MGMT-UI eine neue TSL einbringen; bei wiederholtem Fehler: TI und/oder Support kontaktieren
47711	I/O error: TSL lacks DNSSEC trust-anchor element	In der TSL muss der DNSSEC-Trust-Anchor der TI-Zone verzeichnet sein. Dieses Element fehlt.	Technical	Error	In der MGMT-UI eine neue TSL einbringen; bei wiederholtem Fehler: TI und/oder Support kontaktieren
47712	I/O error: TSL contains more than one trust-anchor element	In der TSL ist mehr als ein DNSSEC-Trust-Anchor vorhanden (dieses Element muss singulär sein).	Technical	Error	In der MGMT-UI eine neue TSL einbringen; bei wiederholtem Fehler: TI und/oder Support kontaktieren
47720	I/O error: configuration not readable	Die XML-Konfiguration des Konnektors ist nicht lesbar.	Technical	Error	Konnektor neu starten
47721	I/O error: configuration lacks DNSSEC trust-anchor element (element missing or malformed base64 encoding)	Der DNSSEC-Trust-Anchor der Internet-Zone (Teil der XML-Konfiguration des Konnektors) fehlt oder ist nicht BASE64-kodiert.	Technical	Error	Manuellen Upload des DNSSEC-Trust-Anchors der Internet-Zone in der MGMT-UI anstoßen.
47722	I/O error: configuration contains more than one trust-anchor element	Es ist mehr als ein DNSSEC-Trust-Anchor (Internet-Zone) in der XML-Konfiguration vorhanden (dieses Element muss singulär sein).	Technical	Error	Manuellen Upload des DNSSEC-Trust-Anchors der Internet-Zone in der MGMT-UI anstoßen.

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
47723	I/O error: configuration lacks definition of internet DNS service	Es ist/sind kein(e) DNS-Server (Internet-Zone) in der XML-Konfiguration definiert.	Technical	Error	Konfiguration in der MGMT-UI anpassen und neu persistieren.
47730	I/O error: trust anchor lacks zone info attribute	Das DNSSEC-Trust-Anchor-Element (Internet-Zone, XML-Konfiguration) ist fehlerhaft.	Technical	Error	Konfiguration in der MGMT-UI anpassen und neu persistieren.
47731	I/O error: trust anchor lacks digests	Mindestens ein Hashwert (message digest) fehlt im Trust-Anchor.	Technical	Error	TSL prüfen (für TI-Trust-Anchor) und Konfiguration (Internet-Trust-Anchor) in der MGMT-UI prüfen. Kann der Fehler nicht beseitigt werden, Support kontaktieren.
47732	I/O error: trust anchor fails to authorize key-signing-key	Der DNS-KSK (Key-Signing-Key) kann durch den Vertrauensanker nicht geprüft werden.	Technical	Error	Mehrere Möglichkeiten: 1.) Fehlerhafter Trust Anchor konfiguriert oder über TSL bezogen. 2.) DNS-Server-Konfiguration (in der Tekematikinfrastruktur) fehlerhaft.
47740	I/O error: data-structure lacks element %s	Eingabedaten sind fehlerhaft.	Technical	Error	Konfiguration prüfen (siehe 47732).
47900	DHCP server could not be stopped (rc=%d)	Programmfehler	Technical	Error	Operation wiederholen
47901	removing DHCP configuration failed: %s	Programmfehler	Technical	Error	Operation wiederholen

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
47902	creating new DHCP configuration failed (rc=%d)	Fehlkonfiguration	Technical	Error	Konfiguration des DHCP-Servers prüfen und korrigieren
47903	testing new DHCP configuration failed (rc=%d)	Fehlkonfiguration	Technical	Error	Konfiguration des DHCP-Servers prüfen und korrigieren
47904	replacing DHCP configuration failed: %s	Programmfehler	Technical	Error	Operation wiederholen
48100	local clock runs unsynchronized for %0.2f days	Keine erfolgreiche Zeitsynchronisation seit mehr als 30 Tagen	Technical	Error	Zeitsynchronisation durchführen oder Zeit einstellen
48101	local clock runs unsynchronized for %0.2f days	Keine erfolgreiche Zeitsynchronisation seit mehr als 50 Tagen und Übergang in den kritischen Betriebszustand	Technical	Fatal	Zeitsynchronisation durchführen oder Zeit einstellen
48102	no NTP upstream servers configured, skipping NTP synchronization	Keine NTP-Server per DNS-Abfrage erhalten	Technical	Error	Operation wiederholen
48103	Online=disabled, skipping NTP synchronization	Fehlkonfiguration	Technical	Error	MGM_LU_ONLINE anschalten
48104	VPN-Tunnel to TI is not up, skipping NTP synchronization	Keine Verbindung zur TI	Technical	Error	Verbindung zur TI prüfen, ggf. herstellen und Operation wiederholen
48105	error synchronizing system time via NTP (rc=%d)	Netzwerk Problem	Technical	Error	Verbindung zur TI prüfen, ggf. herstellen und Operation wiederholen

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
48106	error synchronizing system time to hardware clock (rc=%d)	Programmfehler oder Hardware Schaden (vermutlich RTC)	Technical	Error	Operation wiederholen
48107	error reading size of file %s	Programmfehler	Technical	Error	Operation wiederholen
48108	error shutting down NTP server (rc=%d)	Programmfehler	Technical	Error	Operation wiederholen
48109	error restarting NTP server (rc=%d)	Programmfehler	Technical	Error	Operation wiederholen
48110	error reading output from ntpdc (listpeers) command: %s	Programmfehler	Technical	Error	Operation wiederholen
48111	error updating NTP server runtime configuration using ntpdc (rc=%d)	Programmfehler	Technical	Error	Operation wiederholen
48112	error reading DNS SRV records (status=%d)	Netzwerk Problem	Technical	Error	Verbindung zur TI prüfen, ggf. herstellen und Operation wieder-holen
48113	no NTP upstream servers found	Keine NTP-Server per DNS-Abfrage erhalten	Technical	Error	Operation wiederholen
48114	resolving NTP upstream server name %s failed: %s	DNS Problem	Technical	Error	Operation wiederholen
48115	no IP address for NTP upstream server %s found	DNS Problem	Technical	Error	Operation wiederholen
48116	error initializing ARES library	Programmfehler	Technical	Error	Operation wiederholen

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
48117	error initializing channel to DNS	DNS Problem	Technical	Error	Operation wiederholen
48118	value of DOMAIN_SRVZONE_TI could not be read	Programmfehler	Technical	Error	Operation wiederholen
48119	file modification time of %s could not be set	Programmfehler oder Hardware Schaden (vermutlich SSD)	Technical	Error	Operation wiederholen
48120	time is not in XSD-DateTime format	Fehlkonfiguration	Technical	Error	Konfiguration prüfen, korrigieren und Operation wiederholen
48121	error setting system time: %s	Programmfehler	Technical	Error	Operation wiederholen
48124	CRITICALTIMEDEVIATION: local clock offset to NTP reference clock exceeds limit	Zeitabweichung von mehr als einer Stunde entdeckt und Übergang in den kritischen Betriebszustand	Technical	Fatal	Zeitsynchronisation durchführen oder Zeit einstellen
48200	error locking RTC	Programmfehler oder RTC aktuell in Verwendung	Technical	Error	Operation wiederholen
48201	error reading RTC: %s	Programmfehler oder Hardware Schaden (vermutlich RTC)	Technical	Error	Operation wiederholen
48202	error setting RTC	Programmfehler oder Hardware Schaden (vermutlich RTC)	Technical	Error	Operation wiederholen
48203	error reading system time: %s	Programmfehler	Technical	Error	Operation wiederholen
48204	error setting system time: %s	Programmfehler	Technical	Error	Operation wiederholen
48205	error converting local to UTC time: %s	Programmfehler	Technical	Error	Operation wiederholen

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
48206	error converting UTC to local time: %s	Programmfehler	Technical	Error	Operation wiederholen
48207	error initializing refclock, exiting	Programmfehler	Technical	Error	Operation wiederholen
48208	error reading timecode from refclock, exiting	Programmfehler oder Hardware Schaden (vermutlich RTC)	Technical	Error	Operation wiederholen
48209	error reading system time: %s, exiting	Programmfehler	Technical	Error	Operation wiederholen
48300	current system is unknown	Programmfehler	Technical	Fatal	Wenn nicht durch Neustart zu lösen, Konnektor einschicken
48301	activating LVM volume group konnektor failed (rc=%d)	Programmfehler oder Hardware Schaden (vermutlich SSD)	Technical	Fatal	Wenn nicht durch Neustart zu lösen, Konnektor einschicken
48302	deactivating LVM logical volume %s failed (rc=%d)	LVM Volume Group ist bei der Deaktivierung noch in Verwendung	Technical	Error	keine Aktion
48303	mapping CFS failed (rc=%d)	Programmfehler oder Hardware Schaden (vermutlich SSD oder gSMC-K)	Technical	Fatal	Wenn nicht durch Neustart zu lösen, Konnektor einschicken
48304	unmapping CFS failed (rc=%d)	Verschlüsseltes Dateisystem ist beim Aushängen noch in Verwendung	Technical	Error	keine Aktion
48305	mounting %s to %s failed: %s	Programmfehler oder Hardware Schaden (vermutlich SSD)	Technical	Fatal	Wenn nicht durch Neustart zu lösen, Konnektor einschicken
48306	mounting CFS %s to %s failed: %s	Programmfehler oder Hardware Schaden (vermutlich SSD)	Technical	Fatal	Wenn nicht durch Neustart zu lösen, Konnektor einschicken

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
48307	bind mount %s to %s failed: %s	Programmfehler oder Hardware Schaden (vermutlich SSD)	Technical	Fatal	Wenn nicht durch Neustart zu lösen, Konnektor einschicken
48308	could not mount hwtools path	Programmfehler oder Hardware Schaden (vermutlich SSD)	Technical	Fatal	Wenn nicht durch Neustart zu lösen, Konnektor einschicken
48309	unmounting %s failed: %s	Dateisystem ist beim Aushängen noch in Verwendung	Technical	Error	keine Aktion
48310	%s is not a block device	Programmfehler oder Hardware Schaden (vermutlich SSD)	Technical	Fatal	Wenn nicht durch Neustart zu lösen, Konnektor einschicken
48311	filesystem check (%s) for %s failed (rc=%d)	Programmfehler oder Hardware Schaden (vermutlich SSD)	Technical	Fatal	Wenn nicht durch Neustart zu lösen, Konnektor einschicken
48400	mosquitto client instance could not be created	Programmfehler	Technical	Error	Operation wiederholen
48401	could not connect to MQTT broker (rc=%d): %s	MQTT-Broker reagiert nicht	Technical	Error	Operation wiederholen
48402	could not send data (rc=%d): %s	MQTT-Broker reagiert nicht	Technical	Error	Operation wiederholen
48403	waiting for completion failed (rc=%d): %s	MQTT-Broker reagiert nicht	Technical	Error	Operation wiederholen
48404	could not copy message (rc=%d): %s	Programmfehler	Technical	Error	Operation wiederholen
48405	could not subscribe to topic %s (rc=%d): %s	MQTT-Broker reagiert nicht	Technical	Error	Operation wiederholen

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
48406	could not read data (rc=%d): %s	MQTT-Broker reagiert nicht	Technical	Error	Operation wiederholen
48407	could not allocate memory	Arbeitsspeicher erschöpft	Technical	Error	Konnektor neu starten
48408	no topic given (null)	Programmfehler	Technical	Error	Operation wiederholen
48409	no data given (null)	Programmfehler	Technical	Error	Operation wiederholen
48410	no dataLength given (null)	Programmfehler	Technical	Error	Operation wiederholen
48411	no state given (null)	Programmfehler	Technical	Error	Operation wiederholen
48412	unexpected format	Programmfehler	Technical	Error	Operation wiederholen
48413	no tiVpnInfo given (null)	Programmfehler	Technical	Error	Operation wiederholen
48500	Updater failed, unspecified failure	Es ist ein unbestimmter Fehler aufgetreten.	Technical	Error	Softwareaktualisierung erneut ausführen
48501	Invalid firmware signature	Signatur des Firmwareupdate ungültig oder nicht vorhanden	Technical	Error	Firmwareupdate erneut abrufen
48502	Broken firmware package, failed to extract files	Package des Firmwareupdate ungültig	Technical	Error	Firmwareupdate erneut abrufen
48503	AK-component exceeding disk space	Speicherplatz für AK nicht ausreichend	Technical	Error	Softwareaktualisierung erneut ausführen
48504	NK-component exceeding disc space	Speicherplatz für NK nicht ausreichend	Technical	Error	Softwareaktualisierung erneut ausführen

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
48505	Update-package exceeding disc-space	Speicherplatz für Zwischenablage Update nicht ausreichend	Technical	Error	Softwareaktualisierung erneut ausführen
48506	Uploaded firmware does not correspond to intended version	Firmwareversion des Updates stimmt nicht mit dem übergebenen Wert überein	Technical	Error	Support kontaktieren
48507	Uploaded firmware not listed in latest firmware-group-info	Firmware-Gruppen-Information des Updates ist kleiner als die im Konfigurationsbereich gespeicherten Firmwaregruppe	Technical	Error	Support kontaktieren
48508	Invalid NK-firmware signature	Signatur der NK-Firmware ungültig oder nicht vorhanden	Technical	Error	Firmwareupdate erneut abrufen
48509	Invalid AK-firmware signature	Signatur der AK-Firmware ungültig oder nicht vorhanden	Technical	Error	Firmwareupdate erneut abrufen
48510	Missing verification certificate	Prüfschlüssel nicht verfügbar (Signaturprüfung)	Technical	Error	Support kontaktieren
49800	unable to open file %s: %s	Programmfehler, SSD-Kapazität erschöpft oder Hardware Schaden (vermutlich SSD)	Technical	Error	Operation wiederholen
49801	unable to read file %s: %s	Programmfehler oder Hardware Schaden (vermutlich SSD)	Technical	Error	Operation wiederholen

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
49802	unable to write file %s: %s	Programmfehler, SSD-Kapazität erschöpft oder Hardware Schaden (vermutlich SSD)	Technical	Error	Operation wiederholen
49803	unable to close file %s: %s	Programmfehler, SSD-Kapazität erschöpft oder Hardware Schaden (vermutlich SSD)	Technical	Error	Operation wiederholen
49804	unable to delete file %s: %s	Programmfehler oder Hardware Schaden (vermutlich SSD)	Technical	Error	Operation wiederholen
49805	file %s already exists	Programmfehler	Technical	Error	Operation wiederholen
49806	unable to create directory %s: %s	Programmfehler, SSD-Kapazität erschöpft oder Hardware Schaden (vermutlich SSD)	Technical	Error	Operation wiederholen
49807	unable to delete directory %s: %s	Programmfehler oder Hardware Schaden (vermutlich SSD)	Technical	Error	Operation wiederholen
49808	unable to aquire lock	Programmfehler	Technical	Error	Operation wiederholen
49809	unable to release lock	Programmfehler	Technical	Error	Operation wiederholen
49810	failed to create symlink %s to %s: %s	Programmfehler, SSD-Kapazität erschöpft oder Hardware Schaden (vermutlich SSD)	Technical	Error	Operation wiederholen
49811	failed to delete symlink %s: %s	Programmfehler oder Hardware Schaden (vermutlich SSD)	Technical	Error	Operation wiederholen
49812	unable to create socket: %s	Programmfehler	Technical	Error	Operation wiederholen

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
49813	unable to close socket: %s	Programmfehler	Technical	Error	Operation wiederholen
49814	reading LAN IP address failed: %s	Programmfehler oder Netzwerk Problem	Technical	Error	LAN-Verbindung prüfen, ggf. herstellen und Operation wiederholen
49815	reading LAN MAC address failed: %s	Programmfehler oder Hardware Schaden (vermutlich LAN Interface)	Technical	Error	Operation wiederholen
49816	reading WAN IP address failed: %s	Programmfehler oder Netzwerk Problem	Technical	Error	WAN-Verbindung prüfen, ggf. herstellen und Operation wiederholen
49817	reading WAN MAC address failed: %s	Programmfehler oder Hardware Schaden (vermutlich WAN Interface)	Technical	Error	Operation wiederholen
49818	error parsing xml configuration file %s	Fehlkonfiguration	Technical	Error	Konfiguration prüfen, korrigieren und Operation wiederholen
49819	parameter %s could not be read from configuration (rc=%d)	Fehlkonfiguration	Technical	Error	Konfiguration prüfen, korrigieren und Operation wiederholen
49820	error running command %s: %s	Programmfehler	Technical	Error	Operation wiederholen
49821	finished with error (rc=%d)	Programmfehler	Technical	Error	Operation wiederholen
49822	unexpected argument	Programmfehler	Technical	Error	Operation wiederholen
49823	error running command %s (rc=%d)	Programmfehler	Technical	Error	Operation wiederholen

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
49824	unable to rename file %s to %s: %s	Programmfehler oder Hardware Schaden (vermutlich SSD)	Technical	Error	Operation wiederholen

12.4 Die Notation von IP-Adressen

In der Bedienoberfläche des Modularen Konnektors wird die Classless Inter-Domain Routing (CIDR)-Notation für die Darstellung von IP-Adressen im IPv4-Format verwendet.

Eine CIDR-Adressangabe besteht aus zwei Teilen:

- IP-Adressblock, der eine IP-Adresse in dezimaler Notation darstellt.
- Netzwerk-Präfix, der die Länge der Subnetzmaske in Bit angibt, um dadurch den Adressraum eines Subnetzes zu definieren.

Dabei sind die erste und die letzte IP-Adresse eines Subnetzes jeweils als Subnetz-Adresse beziehungsweise Broadcast-Adresse reserviert. Die Subnetz-Adresse definiert das Subnetz, während die Broadcast-Adresse dazu dient, alle Adressen im Subnetz gleichzeitig ansprechen zu können.

Beispiele für IP-Adressen:

168.17.0.0/24	Subnetz
168.17.0.12/24	System im Subnetz 168.17.0.0
168.17.1.10/32	Einzelsystem ohne Subnetz
168.17.0.255/24	Alle Systeme im Subnetz 168.17.0.0 (Broadcast-Adresse)

12.5 Lizenzinformationen

Die Software beinhaltet Open-Source Bestandteile. Der Kunde verpflichtet sich zur Einhaltung der einschlägigen Lizenzbedingungen.

Informationen zu Lizenzen der jeweiligen Version des Modularen Konnektors finden Sie auf der Webseite von secunet unter https://www.secunet.com/konnektor.

12.6 Sicherheitsbeiblätter

Nachfolgend finden Sie folgende Sicherheitsbeiblätter:

- *Annahme und Prüfung*
- *Aufstellung und Inbetriebnahme*

Sicherheitsbeiblatt

Empfang und Prüfung

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen
www.secunet.com

Anhang zum Betriebshandbuch Modularer Konnektor Version 2.0.0

Bewahren Sie dieses Sicherheitsbeiblatt sicher und getrennt vom Modularen Konnektor auf. Unbefugte Personen dürfen darauf keinen Zugriff haben.

Dieses Sicherheitsbeiblatt enthält Handlungsanweisungen zu Empfang und Prüfung des Modularen Konnektors. Führen Sie die Schritte vollständig wie in Kapitel 2 des Handbuches beschrieben aus.

1. Prüfen Sie die Unversehrtheit des Siegelbandes an der Verpackung (siehe umseitig).

	Von (Name)	Datum
Siegelband geprüft		

2. Prüfen Sie die Vollständigkeit des Lieferumfangs.
3. Prüfen Sie beide Sicherheitssiegel (siehe umseitig).

	Von (Name)	Datum
Sicherheitssiegel geprüft		

4. Notieren Sie die Seriennummern beider Sicherheitssiegel.

Sicherheitssiegel 1	
Sicherheitssiegel 2	

5. Prüfen Sie das Gehäuse auf Eindringversuche (siehe umseitig).

	Von (Name)	Datum
Gehäuse geprüft		

6. Notieren Sie die Seriennummer des Gerätes; dieses ist auf dem Typenschild aufgedruckt.

Seriennummer	

7. Tragen Sie die Kontaktdaten des IT-Dienstleisters vor Ort (DVO) ein.

Kontaktdaten

Siegelband prüfen

Der Modulare Konnektor wird in einer zusätzlichen Transportverpackung geliefert. Die Transportverpackung ist mit einem Siegelband verklebt.

- Überprüfen Sie die Unversehrtheit des Siegelbandes der Transportverpackung.
- Ziehen Sie das Siegelband auf, damit sich die Transportverpackung öffnet.

Bei einem Öffnungsversuch lösen sich die Schichten des Siegelbandes und ein Schriftzug ist sichtbar. Wenn das Siegelband der Transportverpackung beschädigt ist, darf der Modulare Konnektor nicht verwendet werden. Wenden Sie sich bei einem beschädigten an den zuständigen Dienstleister vor Ort (DVO).

Sicherheitssiegel prüfen

Der Modulare Konnektor ist mit zwei Sicherheitssiegeln ausgestattet, die in Vertiefungen an den beiden Gehäuseseiten angebracht sind.

Nur berechtigte Personen dürfen die Sicherheitssiegel prüfen. Das Gerät darf bei beschädigten Sicherheitssiegeln auf keinen Fall in Betrieb genommen werden.

Sie erkennen gültige Sicherheitsmerkmale der Sicherheitssiegel wie folgt:

- Die Sicherheitssiegel stimmen mit der Abbildung überein.
- Die Sicherheitssiegel sind farblich nicht verändert.
- Die Sicherheitssiegel sind nicht entlang der kreuzförmigen Sicherheitsstanzung aufgerissen.
- Die Sicherheitssiegel sind nicht beschädigt und besitzen keine Klebereste.
- Die Sicherheitssiegel besitzen eine feste Verbindung mit dem Gehäuse und lassen sich nicht abheben.

Für weitere Sicherheitsmerkmale siehe Bedienhandbuch.

Gehäuse prüfen

Prüfen Sie das Gehäuse auf Eindringversuche:

- Beschädigungen von Gehäuse und Lackierung
- Beschädigungen im Bereich der Verbindungen
- Öffnung im Gehäuse
- Beschädigungen der Betriebsanzeigen (LEDs)
- Zusätzliche Aufkleber oder externe Anbauteile

Das Gerät darf bei beschädigtem Gehäuse oder Manipulationsverdacht auf keinen Fall in Betrieb genommen werden.

Sicherheitsbeiblatt

Aufstellung und Inbetriebnahme

Anhang zum Betriebshandbuch Modularer Konnektor Version 2.0.0

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen
www.secunet.com

Bewahren Sie dieses Sicherheitsbeiblatt sicher und getrennt vom Modularen Konnektor auf. Unbefugte Personen dürfen darauf keinen Zugriff haben.

Dieses Sicherheitsbeiblatt enthält Handlungsanweisungen zu Aufstellung und Inbetriebnahme des Modularen Konnektors. Führen Sie die Schritte vollständig wie in Kapitel 4 und 5 des Handbuches beschrieben aus.

Hinweise zur Betriebsumgebung

- Der Modulare Konnektor darf nur in einer der folgenden Umgebungen betrieben werden:
  - Innerhalb eines personalbedienten Bereichs, in dem sich der Leistungserbringer regelmäßig aufhält. Dritte dürfen auf den Modularen Konnektor keinen Zugriff haben.
  - In einem abgeschlossenen, nicht öffentlichen Betriebsraum.
  - In einem abgeschlossenen Schrank, der vor unberechtigtem Zugriff schützt.
- Die Einsatzumgebung des Modularen Konnektors muss diesen vor physischen Angriffen schützen.
- Betreiben Sie den Modularen Konnektor spritzwassergeschützt und nicht im direkten Sonnenlicht.
- Dritte dürfen zum Aufstellungsort des Modularen Konnektors keinen Zugriff haben.
- Die verwendete Steckdose muss zugänglich sein, um das Gerät bei Bedarf vom Netz trennen zu können.

Was tun bei Verlust oder Kompromittierung?

Wenn der Modulare Konnektor gestohlen wird, abhandenkommt oder in irgendeiner Form kompromittiert erscheint (z.B. nicht mehr am sicheren Aufstellungsort, Sicherheitssiegel oder Gehäuse beschädigt, unsachgemäß geöffnet), ist umgehend der Dienstleister vor Ort (DVO) zu informieren. Dieser wird die Sperrung veranlassen. Verschicken Sie das Gerät nicht eigenständig über einen Lieferdienst.

Ein gestohlenes oder abhandengekommenes Gerät wird anhand der Seriennummer identifiziert, die bei Empfang auf dem Sicherheitsbeiblatt *Empfang und Prüfung* notiert wurde.

Was Sie für die Inbetriebnahme benötigen

- Funktionierender Internetanschluss
- Mindestens ein E-Health-Kartenterminal
- Praxisverwaltungssystem, das für die Benutzung mit der Telematikinfrastruktur zugelassen ist
- Zugang zum VPN-Zugangsdienst (Vertragsnummer/Contract ID)
- Ein Clientsystem mit Browser (Mozilla Firefox ESR ab Vers.52.6 oder Google Chrome ab Vers. 64)
- Freigeschalteter Praxisausweis (SMC-B) mit zugehöriger PIN/PUK

Vor der Montage und Inbetriebnahme des Modularen Konnektors sollten Sie die Einsatzbedingungen und die vorhandene IT-Infrastruktur prüfen.

Geheimnis festlegen

Legen Sie ein Geheimnis (mindestens 6 Buchstaben) für den alternativen Login fest und notieren Sie es.

Geheimnis:	

Teilen Sie das Geheimnis dem IT-Dienstleister vor Ort (DVO) mit.

	Von (Name)	Datum
Geheimnis mitgeteilt		

Inbetriebnahme

Die Inbetriebnahme des Modularen Konnektors mit fester IP-Adresse ist in der Bedienungsanleitung beschrieben. Gehen Sie zur Inbetriebnahme des Modularen Konnektors mittels DHCP-Server wie folgt vor:

- Schließen Sie den Modularen Konnektor über einen Switch an ein Netzwerk an, das über einen DHCP-Server verfügt. Beachten Sie die Hinweise im Bedienhandbuch, falls kein DHCP-Server erreichbar ist. Verbinden Sie anschließend auch das Clientsystem mit dem Switch.
- Schalten Sie den Modularen Konnektor ein, indem Sie die Ein/Aus-Taste kurz drücken.
  Die Betriebsanzeigen leuchten auf und das Gerät startet. Wenn die Anzeige SYSTEM dauerhaft leuchtet, ist der Modulare Konnektor betriebsbereit. Eine Übersicht der Anzeigen beim Systemstart und möglicher Fehleranzeigen finden Sie im Bedienhandbuch.
- Geben Sie am Clientsystem in der Adresszeile des Browsers unter Verwendung der dem Modularen Konnektor zugewiesenen IP-Adresse folgende Adresse ein:

  `https://<IP-Adresse des Modularen Konnektors>:8500/management`

- Validieren Sie das Zertifikat des Modularen Konnektors (siehe Bedienhandbuch).
- Melden Sie sich mit den folgenden initialen Zugangsdaten an:

  Benutzername: `super`
  Passwort: `konnektor`

- Sie werden aufgefordert, ein neues Passwort einzugeben. Beachten Sie die Hinweise zu Passwörtern im Bedienhandbuch. Falls Sie bei der ersten Anmeldung nicht zum Passwortwechsel aufgefordert werden, darf der Modulare Konnektor nicht in Betrieb genommen werden. Es besteht die Gefahr einer möglichen Kompromittierung.
- Eine ausführliche Beschreibung der Bedienoberfläche finden Sie im Bedienhandbuch.
- Schalten Sie den Modularen Konnektor durch zweimaliges kurzes drücken der Ein/Aus-Taste aus.

Heiße Oberfläche

Verbrennungsgefahr bei Berührung im Betrieb erhitzter Gehäuseteile

Nach dem Abschalten des Geräts mindestens fünf Minuten warten, bis das Gehäuse berührt wird. Dieses gilt für den Betrieb sowohl mit wie auch ohne die optional verfügbare Wandhalterung.

.