secunet konnektor

Modularer Konnektor

2.0.0
2.1.0

Produkttypversion: 3.6.0-2 (PTV3)
Firmwareversion: 3.5.2

Bedienungsanleitung

Für Administratoren und Benutzer

Version 2.2

secunet
Secunet Security Networks AG

Diese Bedienungsanleitung bezieht sich auf folgende von der gematik zugelassenen und vom BSI zertifizierten Konstruktionsstände:

- Einboxkonnektor (Konstruktionsstand 2.0.0)
- Rechenzentrumskonnektor (Konstruktionsstand 2.1.0)

Weitere Versionshinweise finden Sie auf Seite 16.

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.

Versionshinweise

Dieses Handbuch bezieht sich auf folgende von der gematik zugelassenen und vom BSI zertifizierten Konstruktionsstände:

- Einboxkonnektor (Konstruktionsstand 2.0.0)
- Rechenzentrumskonnektor (Konstruktionsstand 2.1.0)

  Der Rechenzentrumskonnektor besteht aus zwei vollständig separaten Recheneinheiten mit jeweils eigenem Netzteil. Diese sind in einem Gehäuse für den Einbau in einen 19" Netzwerkschrank zusammengefasst. Die Recheneinheiten laufen unabhängig voneinander. Die Erläuterungen in diesem Handbuch gelten jeweils nur für eine Recheneinheit und sind analog für die Zweite anzuwenden.

Diese Konstruktionsstände legen jeweils eine Firmware- und Hardwareversion fest. Informationen zu den zugelassenen Softwareversionen sind der Webseite des Herstellers zu entnehmen (www.secunet.com), Informationen zu zugelassenen Software und Hardwareversion erhalten Sie von der gematik (www.gematik.de).

Dieses Handbuch bezieht sich auf folgende zugelassene Versionen:

- Firmwareversion 3.5.2
- Produkttypversion 3.6.0-2 (PTV3)

Informationen über lizenzpflichtige Systemkomponenten finden Sie in Kapitel 11.10.

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 80.

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 Informationen für Anwender und Praxispersonal

Der Modulare Konnektor dient dem sicheren Betrieb der IT-Systeme in Ihrer Praxis und bindet diese bei Bedarf an die bundesweite Telematikinfrastruktur an.

1.1 Prüfung der Zulassung

- Informieren Sie sich vor der Nutzung eines Modularen Konnektors von secunet zunächst auf der Webseite der gematik über zugelassene secunet Konnektoren.

  Sie finden eine Auflistung der zugelassenen Konnektoren unter:

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

- Lassen Sie sich die installierte Version eines Modularen Konnektors von secunet über das Primärsystem anzeigen; beachten Sie dazu die Hinweise des Primärsystem-Herstellers.

Weitere Informationen zu den zugelassenen secunet Konnektoren finden Sie auf der folgenden Webseite der secunet:

https://www.secunet.com/konnektor/

Dort ist für alle zugelassenen Modularen Konnektoren von secunet jeweils das Bedienhandbuch verfügbar.

1.2 Gerät ein- /ausschalten

- Einschalten: An/Aus-Taster kurz drücken.
- Ausschalten: An/Aus-Taster innerhalb von 3 Sekunden zweimal drücken. Zwischen den beiden Betätigungen muss eine Sekunde gewartet werden.

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.

1.3 Was muss im Betrieb beachtet werden?

Der Modulare Konnektor wurde vom Dienstleister vor Ort (DVO) für Ihre speziellen Bedürfnisse eingerichtet und benötigt im normalen Betrieb keine Bedienung.

Beachten Sie:

- Das Gerät ist mit Sicherheitssiegeln versehen und darf nicht geöffnet, verändert oder von seinem vorgesehenen Platz entfernt werden.
- Prüfen Sie regelmäßig die Sicherheitssiegel und das Gehäuse (siehe Kapitel 4).
- Bringen Sie keine Aufkleber oder sonstige Anbauteile am Gehäuse an und beachten Sie die nachfolgenden Hinweise zur Reinigung.

Kontaktieren Sie im Fall von Störungen oder sonstigen Auffälligkeiten den DVO (siehe Kapitel 1.6).

1.4 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 13).

1.5 Betriebsanzeigen (Kurzübersicht)

Über die Betriebsanzeigen an der Geräteoberseite erhalten Sie Rückmeldung über den aktuellen Gerätezustand. Für eine detaillierte Beschreibung siehe Kapitel 4.4.

Bezeichnung	Funktion
Power	Das Gerät ist eingeschaltet.
System	Das Gerät ist in Betrieb.
VPN TI	Es besteht eine Verbindung zur Telematikinfrastruktur*.
VPN SIS	Es besteht eine Verbindung zum Sicheren Internet-Dienst.
Service	Ein Fehler oder eine Warnung liegt vor. Blinken deutet Fehler mit hoher Priorität an. Kontaktieren Sie den Administrator.
Update	Eine Systemaktualisierung ist verfügbar.
Remote	Remote Management ist aktiviert. Blinken deutet eine gerade durchgeführte Administrierung per Remote Management an.

* Wenn eine Verbindungen zur TI besteht, ist nicht automatisch auch die Funktion der TI-Dienste gewährleistet.

Tabelle 1: Betriebsanzeigen (Kurzübersicht)

1.6 Ansprechpartner für Fragen und bei Störungen

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 Dauerhaften Außerbetriebnahme in Kapitel 15. Versenden Sie den Modularen Konnektor nicht selbstständig über einen Lieferdienst, sondern kontaktieren Sie für jeden Transport den DVO.

2 Funktionsbeschreibung

2.1 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.

2.2 Sicherheitsfunktionen

2.2.1 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)

2.2.2 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.

2.2.3 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.

2.2.4 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

2.2.5 Kryptographische Verfahren in der Telematikinfrastruktur

Der Modulare Konnektor verwendet z.B. zur Authentisierung externer Verbindungen (siehe Kapitel 2.2.2) kryptographische Verfahren in Form asymmetrischer Schlüssel und X.509-Zertifikaten.

Hierbei nutzt der Modulare Konnektor interne Sicherheitsmodule (Secure Module Card Konnektor, gSMC-K) zur Abbildung der Geräteidentitäten.

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

Zur Aufrechterhaltung des Sicherheitsniveau werden die Komponenten und Dienste der Telematikinfrastruktur (TI) Schrittweise u.a. auf neue kryptographische Verfahren umgestellt.

Kamen bisher Geräteidentitäten und kryptographische Verfahren auf Basis von RSA-Schlüsseln zum Einsatz, werden zukünftig Geräteidentitäten auf Basis von ECC-Schlüsseln eingesetzt. In der Übergangsphase, die bis Ende 2024 geht, können RSA-Schlüssel zur Authentisierung weiterverwendet werden. Der Modulare Konnektor von secunet ist auf die zukünftige Verwendung von ECC-Schlüsseln bereits vorbereitet. So verwenden neuere Konnektoren Geräteidentitäten, welche sowohl RSA- als auch ECC-Schlüssel beinhaltet.

Welche Konnektoren bereits auf die Verwendung von ECC-Schlüsseln vorbereitet sind, ist anhand der ersten drei Stellen der Seriennummer zu erkennen. So beinhalten Einboxkonnektoren beginnend mit der Seriennummer <307> (siehe Typenschild in Kapitel 16.2.1) sowie Rechenzentrumskonnektoren beginnend mit der Seriennummer <315> (siehe Typenschild in Kapitel 16.2.2) die neuen Geräteidentitäten.

2.2.6 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.

2.2.7 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.

2.2.8 Signaturdienst

Der Signaturdienst ermöglicht Clientsystemen und Fachmodulen die Signatur von Dokumenten und die Prüfung bestehender Signaturen.

Dies umfasst folgende Signaturniveaus:

- Nicht-qualifizierte elektronische Signatur (nonQES) mit der SM-B
- Qualifizierte elektronische Signatur (QES) mit dem HBA und den HBA-Vorläuferkarten HBA-qSig und ZOD_2.0.

Weitere unterstützte Signaturfunktionen:

- Parallele Signatur

  Die Signatur eines bereits signierten Dokumentes
- Gegensignatur

  Die Signatur aller vorhandenen parallelen Signaturen in folgenden Varianten:
  - Dokumentinkludierende Gegensignatur

    Das Dokument und alle Signaturen werden gegensigniert
  - Dokumentexkludierende Gegensignatur

    Alle Signaturen werden gegensigniert, aber nicht das Dokument selbst
- Stapelsignatur

  Die Signatur mehrerer Dokumente nach einmaliger Authentisierung (nicht bei Verwendung von HBA-Vorläuferkarten)
- Einfachsignaturmodus

  In diesem Betriebsmodus wird bei der qualifizierten Signatur eines einzelnen Dokumentes eine vereinfachte Sicherheitsumgebung ohne gegenseitige Authentisierung der Karte und des Modularen Konnektors angewendet.

Der Signaturdienst erlaubt es für CMS-Signaturen zusätzliche signierte und unsignierte Eigenschaften (Properties) bzw. Attribute in die Signatur einzubringen (CMSAttribute), siehe dazu auch Kapitel 16.18.2.1, Abschnitt „CMS-Signaturen“.

Die folgenden Attribute werden dabei vom Konnektor nicht ausgewertet, sondern ignoriert:

- **ContentType**
- **SigningTime**
- **MessageDigest**

- **SigningCertificate**
- **SigningCertificateV2**
- **CMSAlgorithmprotection**

Dabei wird keine Fehlermeldung ausgegeben, sondern die Operation ausgeführt ohne diese Attribute zu berücksichtigen.

Der Signaturdienst des Modularen Konnektor kann bei Bedarf einen Ergebnisbericht (Verification Report) an das aufrufende Client-System zurückgeben. Darin werden für die Korrektheitsprüfung der digitalen Signatur folgende Ergebnisse angegeben:

- Ob die kryptographische Prüfung der digitalen Signatur mit dem dazugehörigen öffentlichen Schlüssel deren Korrektheit bestätigt hat oder nicht
- Ob die für die Erstellung der Signatur verwendeten kryptographischen Algorithmen und Parameter zum angegeben Zeitpunkt der Signaturerstellung geeignet waren; wenn dies nicht der Fall ist, liegt keine qualifizierte elektronische Signatur vor
- Ob die für die Erstellung der Signatur verwendeten kryptographischen Algorithmen und Parameter zum Zeitpunkt der Signaturprüfung geeignet sind; wenn dies nicht der Fall ist, gibt der Modulare Konnektor als Information zum verminderten Beweiswert der qualifizierten elektronischen Signatur zusätzlich an, bis wann ein Algorithmus gültig war

Die Auswahl des für die Signaturprüfung anzunehmenden Signaturzeitpunkts erfolgt hierarchisch nach den folgenden Vorgaben:

- Falls vorhanden „Benutzerdefinierter_Zeitpunkt“, sonst
- Falls vorhanden „Ermittelter_Signaturzeitpunkt_Eingebettet“, sonst
- Ermittelter_Signaturzeitpunkt_System

Ein gegebenenfalls vorhandener qualifizierter Zeitstempel („Ermittelter_Signaturzeitpunkt_Qualifiziert“) wird nicht ausgewertet, sondern vollständig ignoriert.

Für eine Definition der Signaturzeitpunkte siehe [gemSpec_Kon], Kapitel 4.1.8.1.3.

2.2.9 Verschlüsselungsdienst

Der Verschlüsselungsdienst bietet den Clientsystemen Funktionen zur hybriden Ver- und Entschlüsselung von Dokumenten:

- Hybride Ver- und Entschlüsselung nach CMS-Standard von XML-, PDF/A-, Text-, TIFF- und Binär-Dokumenten
- Hybride Ver- und Entschlüsselung von XML-Dokumenten nach der W3C-Empfehlung „XML Encryption Syntax and Processing“
- Hybride Ver- und Entschlüsselung von MIME-Dokumenten nach dem S/MIME-Standard
- Ab Firmware-Version 3.5.2 ist auch die Ver- und Entschlüsselung mit HBA Vorläuferkarten möglich

2.2.10 Authentifizierungsdienst

Der Authentifizierungsdienst bietet Clientsystemen und Fachmodulen Funktionen für die externe Authentisierung.

Das Signaturformat PKCS#1 kann nur zu Authentisierungszwecken mit dem Authentisierungsschlüssel des HBAx und des SM-B verwendet werden. Die Nutzung ist auf Dokumente (Hash) von maximal 512 bit Länge beschränkt.

2.2.11 Selbsttest

Der Modulare Konnektor verfügt über einen Selbsttest, der die Integrität sicherheitsrelevanter Komponenten prüft. Dies geschieht bei folgenden Gelegenheiten:

- Bei jedem Start
- Während des Betriebs regelmäßig alle 24 Stunden
- Nach manuellem Anstoß über die Bedienoberfläche (siehe Kapitel 9.4.1)

Wenn der Selbsttest beim Start oder bei der regelmäßigen Durchführung fehlschlägt, fährt der Modulare Konnektor automatisch nach 60 Sekunden herunter. Bei manuellem Anstoß des Selbsttests wird das Ergebnis angezeigt, und der Modulare Konnektor fährt im Falle des Fehlschlags ebenfalls nach 60 Sekunden herunter.

Ein Fehlschlag des Selbsttests wird zusätzlich durch die Betriebsanzeigen signalisiert (siehe Kapitel 4.4).

2.2.12 Hardwarebeschleunigung (AES-NI)

Der Modulare Konnektor unterstützt Advanced Encryption Standard New Instructions (AES-NI) für die Beschleunigung von AES-Verschlüsselungsverfahren.

Der Modulare Konnektor inklusive der Implementierung des Algorithmus AES in Software ist im Rahmen der Evaluierung und Zertifizierung nach Common Criteria gemäß [PP-0097] und [PP-0098] geprüft worden. Des Weiteren unterstützt die Hardware die Nutzung der AES Routinen der verwendeten Intel CPU. Die Verwendung der AES Routinen der Intel CPU ist gemäß gematik in der Telematikinfrastruktur zulässig.

Der Administrator eines Modularen Konnektors kann bezüglich der AES-Ausführung zwischen der im Sinne der Common Criteria geprüften Software-AES-Implementierung und der im Sinne der Common Criteria ungeprüften Hardware-AES-Implementierung durch Änderung der Konfigurationseinstellung beliebig wechseln. Jeder Wechsel erfordert einen Neustart des Geräts. Bei Nutzung der ungeprüften Hardware-AES-Implementierung beinhaltet die Evaluierung und Zertifizierung des Modularen Konnektor gemäß [PP-0097] und [PP-0098] nach Common Criteria auch den korrekten Aufruf der Hardware-AES-Implementierung. Die Hardware-AES-Implementierung selbst ist jedoch nicht Gegenstand der Evaluierung und Zertifizierung des Modularen Konnektor gemäß [PP-0097] und [PP-0098] nach Common Criteria.

Die Einstellung der Hardwareunterstützung AES-NI ist in Kapitel 9.5.1 beschrieben.

2.3 Weitere Dienste

2.3.1 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.

2.3.2 DHCP-Dienst

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

2.3.3 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.

2.4 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 10.2.1.2) 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 16.7.

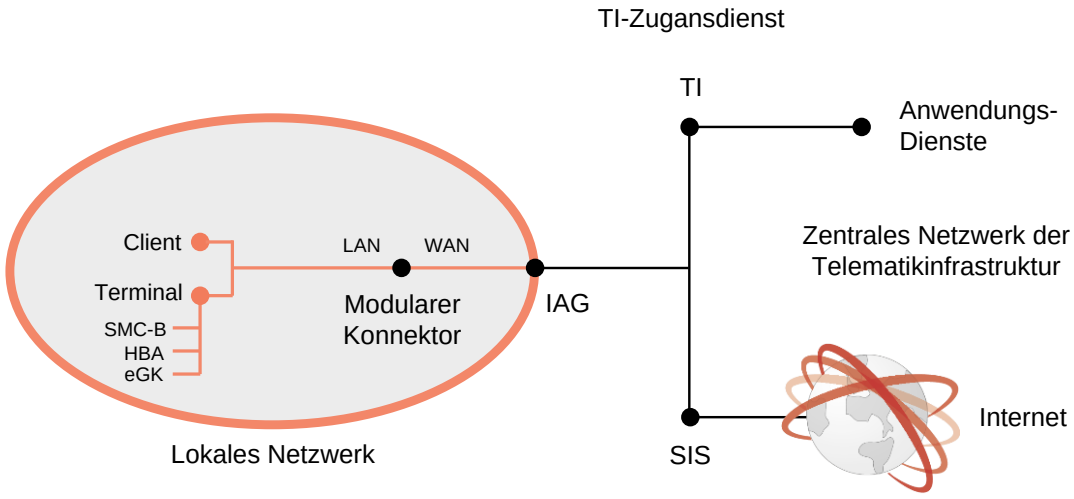


Abbildung 1: Netzwerkschnittstellen des Modularen Konnektors (Beispiel)

Der Modulare Konnektor verwendet, bis einschließlich der Firmwareversion 2.0.38, intern das Netzsegement 192.168.77.0/24. In nachfolgenden Firmwareversionen wird das Segement 169.254.77.0/24 verwendet.

Um eine Kommunikation des Modularen Konnektor mit angeschlossenen Netzsegementen zu ermöglichen, darf es keine Überschneidung mit dem intern verwendeten Netzsegement geben.

3 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.

3.1 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.

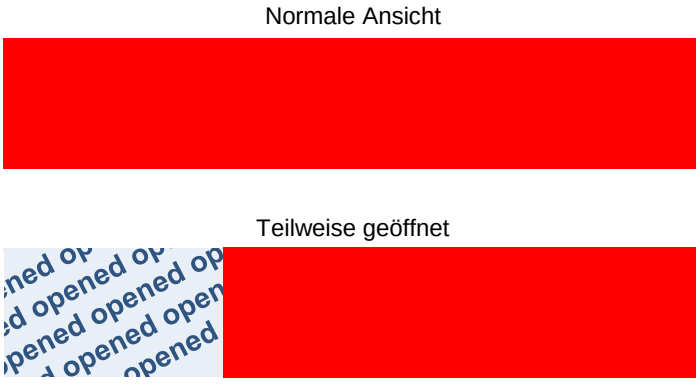


Abbildung 2: Siegelband der Transportverpackung

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

3.2 Lieferumfang

Für den Lieferumfang des Modularen Konnektors siehe:

- Anhang 16.1.1 (Einboxkonnektor, Konstruktionsstand 2.0.0)
- Anhang 16.1.2 (Rechenzentrumskonnektor, Konstruktionsstand 2.1.0)

Die Sicherheitsbeiblätter "Empfang und Prüfung" und "Aufstellung und Inbetriebnahme" enthalten Sicherheitshinweise für den Modularen Konnektors. Diese Sicherheitsbeiblätter finden Sie auch in Anhang 16.16. Verwenden Sie entweder Ausdrucke der entsprechenden Anhänge des Handbuches oder prüfen Sie, dass die beigelegten Sicherheitsbeiblätter der Gerätelieferung mit den Inhalten von Anhang 16.16 des Handbuches übereinstimmen.

Als optionales Zubehör ist eine Halterung für die Wandmontage erhältlich.

3.3 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 4.3).
  - 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.

3.4 Typschild und Verpackungskennzeichnung

Für Abbildungen von Typschild und Verpackungskennzeichnung siehe:

- Anhang 16.2.1 (Einboxkonnektor, Konstruktionsstand 2.0.0)
- Anhang 16.2.2 (Rechenzentrumskonnektor, Konstruktionsstand 2.1.0)

  Der Rechenzentrumskonnektor besitzt an Vorder- und Rückseite eine Kennzeichnung der Seriennummer.

4 Gerätebeschreibung

4.1 Schnittstellen und Bedienelemente

Für eine Übersicht der Schnittstellen und Bedienelemente siehe:

- Anhang 16.4.1 (Einboxkonnektor, Konstruktionsstand 2.0.0)
- Anhang 16.4.2 (Rechenzentrumskonnektor, Konstruktionsstand 2.1.0)

4.2 Produkt- und Betriebsmerkmale

Für eine Übersicht der Produkt- und Betriebsmerkmale siehe:

- Anhang 16.5.1 (Einboxkonnektor, Konstruktionsstand 2.0.0)
- Anhang 16.5.2 (Rechenzentrumskonnektor, Konstruktionsstand 2.1.0)

4.3 Manipulationsversuche erkennen

4.3.1 Sicherheitssiegel

Für die Anbringung der Sicherheitssiegel siehe:

- Anhang 16.3.1 (Einboxkonnektor, Konstruktionsstand 2.0.0)
- Anhang 16.3.2 (Rechenzentrumskonnektor, Konstruktionsstand 2.1.0)

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 13.**
- **Nur berechtigte Personen dürfen die Sicherheitssiegel prüfen.**

4.3.1.1 Merkmale von Sicherheitssiegeln

Die Größe der Sicherheitssiegel beträgt 30 mm x 10 mm.

Abbildung 3: 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. Bei Unterschreitung der angegebenen Temperatur erscheinen wieder die roten Guillochen-Linien.

Abbildung 4: Thermoreaktive Linienzüge

- UV-aktiver Schriftzug „SECURITY“

  Der Schriftzug wird unter UV-Licht von ca. 365nm sichtbar.

Abbildung 5: Sicherheitssiegel unter UV-Licht

4.3.1.2 Beschädigt Sicherheitssiegel erkennen

So erkennen Sie Beschädigungen der Sicherheitssiegel:

▶ Prüfen Sie, ob die Sicherheitsmerkmale beeinträchtigt sind.

Abbildung 6: Beschädigtes Sicherheitssiegel

Abbildung 7: 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.

4.3.2 Gehäuse

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

4.3.2.1 Eindringversuche erkennen

Prüfen Sie das Gehäuse auf Eindringversuche (siehe Anhang 16.4):

- 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.

Auf dem Gehäuse kann sich der Aufdruck eines Partnerunternehmens befinden. Dies stellt keine Sicherheitseinschränkung dar.

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

4.4 Betriebsanzeigen

4.4.1 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	VPN-Verbindung zur TI wird aufgebaut
		Aus	Keine VPN-Verbindung zur TI
VPN SIS	Verbindung mit SIS	An	VPN-Verbindung zum SIS
		Blinkt	VPN-Verbindung zum SIS wird aufgebaut
		Aus	Keine VPN-Verbindung zum SIS
Service	Fehler	An	Fehler / Warnung
		Blinkt	Fehler mit hoher Priorität (siehe Kapitel 11.1)
		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

* Wenn eine Verbindungen zur TI besteht, ist noch nicht die Funktion der TI-Dienste gewährleistet. Siehe Kapitel 11.2 zur Prüfung der Funktion einzelner Dienste.

Tabelle 2: Anzeigen im laufenden Betrieb

Je nach Betriebszustand können mehrere oder alle Betriebsanzeigen zur selben Zeit leuchten.

4.4.2 Anzeigen bei besonderen Betriebszuständen

LED(s)	Signal	Erläuterung
Service, Update, Remote	Blinkt	Werksreset wird durchgeführt (siehe Kapitel 11.5); beim Anstoßen des Werksresets leuchten alle Anzeigen kurz.
Service, Update, Remote	An	Vollständiger Werksreset erfolgreich abgeschlossen; die Anzeigen leuchten für 15 Sekunden
Update, Remote	Blinkt	Sperrung für den Versand wird durchgeführt (siehe Kapitel 11.7.2)
Update, Remote	An	Sperrung für den Versand erfolgreich abgeschlossen; die Anzeigen leuchten für 15 Sekunden
Remote	An	Werksreset Failsafe erfolgreich abgeschlossen
Service	An	Werksreset fehlgeschlagen; die Anzeige leuchten für 15 Sekunden (betrifft vollständigen Werksreset, Sperrung für den Versand und Werksreset Failsafe)
System Service	An Blinkt	Fehler bei Selbsttest (siehe Kapitel 2.2.11)
Alle bis auf Power	Blinkt	System wird heruntergefahren (Dauer bis zu 3 Minuten)

Tabelle 3: Anzeigen bei besonderen Betriebszuständen

4.4.3 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 Bei einem Fehler während des BIOS-Starts leuchtet zusätzlich die Anzeige "System".
Update, Remote	An	Boot-Prozess des BIOS wird fortgesetzt
Remote	An	Boot-Prozess des BIOS erfolgreich abgeschlossen
Alle	An	Fehler beim Systemstart
System, VPN TI, VPN SIS	Abfolge	Systemstart des Netzkonnektors
System	Blinkt	Anwendungskonnektor startet
System	An	System in Betrieb Je nach Betriebszustand leuchten zusätzlich die Anzeigen "VPN TI" und "VPN SIS".
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

4.4.4 Anzeigen bei Fehlerzuständen

Fehlerzustände werden von den Betriebsanzeigen 60 Sekunden lang angezeigt, anschließend fährt das System herunter. Eine Übersicht der signalisierten Fehlerzustände finden Sie in Anhang 16.11.

- Wenn das System aufgrund eines Fehlerzustandes heruntergefahren ist, starten sie es erneut durch kurzes Drücken des An/Aus-Tasters und beobachten Sie den Verlauf der Betriebsanzeigen.
- Falls der Fehler wieder auftritt, notieren Sie den zuletzt angezeigten Zustand der Betriebsanzeigen und kontaktieren Sie den DVO (siehe Kapitel 1.6).

4.5 Gerät ein-/ausschalten

Die Unterbrechung der Versorgungsspannung im laufenden Betrieb ist zu vermeiden. Schalten Sie den Modularen Konnektor immer ordnungsgemäß aus. Ziehen Sie den Netzstecker erst, nachdem alle LEDs am Modularen Konnektor erloschen sind. Bei Nichtbeachtung kann das Gerät fahrlässig beschädigt werden.

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

Einschalten:

- An/Aus-Taster kurz drücken (siehe Kapitel 16.4).

  Für die Anzeigen beim Systemstart siehe Kapitel 4.4.3. 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.

4.6 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.

5 Sicherheitshinweise

5.1 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 oder Serverschrank, der den Modularen Konnektor vor unberechtigtem Zugriff schützt.**
- **Die Einsatzumgebung des Modularen Konnektors muss diesen vor physischen Angriffen schützen.**
- **Für den Zugriff befugt sind nur Personen (z.B. medizinisches Personal), die vom Leistungserbringer namentlich autorisiert wurden.**
- **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 4.3.1.2 und 4.3.2), sodass eingeleitete materielle, organisatorische und/oder personelle Maßnahmen größeren Schaden abwehren.**
- **Die verwendeten Steckdosen müssen 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.

5.2 Sicherheitshinweise zu Benutzerpasswörtern

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.

Passwörter dürfen nicht schriftlich aufbewahrt und nicht an Dritte weitergegeben werden.

Benutzer müssen die PIN und PUK der Chipkarten, sowie Passwörter für die Authentisierung gegenüber dem Modularen Konnektor, vor Offenbarung und Missbrauch schützen. Karteninhaber dürfen ihre PIN nur dann an einem Kartenterminal eingeben, wenn der initiierte Anwendungsfall dies erfordert und das Kartenterminal dem Karteninhaber einen sicheren PIN-Eingabemodus anzeigt. Wenn der Karteninhaber von einem Kartenterminal zur PIN-Eingabe aufgefordert wird, ohne dass das Kartenterminal gleichzeitig den sicheren PIN-Eingabemodus anzeigt, muss der Karteninhaber den Vorgang abbrechen und darf seine PIN nicht eingeben. Der Karteninhaber muss kontrollieren, dass die PIN-Eingabe-Aufforderung (einschließlich Jobnummer) konsistent angezeigt wird, sowohl in seiner Clientsoftware, als auch auf dem PIN-Kartenterminal.

5.3 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 13.
- ▶ Halten Sie das Sicherheitsbeiblatt *Empfang und Prüfung* bereit, auf dem die Seriennummer des Geräts notiert ist.

5.4 Sicherheitshinweise zur Netzwerkumgebung

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

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.

Die Einsatzumgebung muss Prozesse etablieren, die dafür sorgen, dass Update-Pakete und nachzuladende Fachmodule für den Modularen Konnektor nur dann signiert und ausgeliefert werden, wenn der Code von einer dazu autorisierten Stelle geprüft und freigegeben wurde. Zertifizierte Komponenten des Modularen Konnektors dürfen nur durch zertifizierte Komponenten ersetzt werden.

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

5.4.1 Internet-Anbindung

Wenn außer durch dem Modularen Konnektor weitere Anbindungen des lokalen Netzwerks an das Internet genutzt werden, kann dies zu erheblichen Sicherheitsrisiken führen. Auch Angriffe aus dem Internet über den SIS sind nicht auszuschließen. 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.

5.4.2 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.

Es muss sichergestellt sein, dass alle Personen, die Zugriff auf medizinische Daten haben, welche auf Clientsystemen lokal gespeichert werden, verantwortungsvoll mit diesen Daten umgehen. HBA-Inhaber dürfen den HBA nur in IT-Umgebungen verwenden, die wie in diesem Kapitel beschrieben sicher administriert werden.

Die Clientsysteme, die mit dem Modularen Konnektor kommunizieren, müssen vertrauenswürdig sein, d.h., es dürfen keine Angriffe aus den Clientsystemen erfolgen und muss sichergestellt sein, dass sie die ihnen anvertrauten Daten / Informationen nicht missbrauchen. Sofern ein Clientsystem eine gesicherte Kommunikation mit dem Modularen Konnektor unterstützt, muss das Schlüsselmaterial zum Aufbau und Betrieb des sicheren Kommunikationskanals adäquat geschützt werden. Dies gilt auch bei Verwendung von Terminal-Servern: Hier werden die Terminal-Server und die genutzten Thin-Clients in der angegebenen Weise als vertrauenswürdig angesehen.

Alle genutzten kryptographischen Sicherheitsmechanismen müssen im Einklang mit den relevanten Vorgaben des Dokuments [BSI TR-03116-1] implementiert werden.

Clientsysteme müssen korrekt arbeiten. Sie müssen fachliche Anwendungsfälle korrekt durchführen und die korrekten Daten nutzen. Sie müssen dem Modularen Konnektor die korrekten, vom Leistungserbringer beabsichtigen Daten übergeben. Sofern ein fachlicher Anwendungsfall durchgeführt werden soll, der einen HBA erfordert, identifiziert ein Clientsystem den HBA-Inhaber bzw. den zu verwendenden HBA und das zuständige Fachmodul. Der Leistungserbringer muss sicherstellen, dass die in seiner Umgebung betriebene Clientsystem-Software die Leistungserbringer (HBA-Inhaber) korrekt authentisiert.

Ein Clientsystem dient dem Leistungserbringer als Benutzerschnittstelle zum Modularen Konnektor. Es übermittelt die vom Leistungserbringer gewünschten Aufrufe an den Modularen Konnektor.

Ohne gesicherte beidseitig-authentisierte Verbindung zwischen dem Clientsystem und dem Modularen Konnektor bestehen Sicherheitseinschränkungen. Beachten Sie die Hinweise zur Absicherung der Verbindung zu Clientsystemen in Kapitel 9.3.3.

Beim Aufruf des Modularen Konnektors mit einem Kartenzugriff muss das Clientsystem einen geeigneten Satz von Parametern übergeben, anhand dessen der Konnektor die Zuweisung oder Verweigerung von Sicherheitsstatus vornehmen kann.

Das Clientsystem muss den Zugriff auf die Entschlüsselungsfunktion des Modularen Konnektors kontrollieren, so dass keine unkontrollierten Entschlüsselungen (ohne Zustimmung des HBA-Inhabers, z. B. durch nicht autorisiertes medizinisches Personal) möglich sind, und keine nicht beabsichtigen Empfänger an den Modularen Konnektor übergeben werden.

Das Clientsystem muss Rückmeldungen, Warnungen und Fehlermeldungen des Konnektors sowie über den Systeminformationsdienst gemeldete kritische Betriebszustände korrekt, sofort und verständlich darstellen.

Das Clientsystem muss im Rahmen der Erzeugung und Prüfung einer QES die Dokumente, Zertifikate, Jobnummer und Fortschrittsanzeige der Stapelsignatur korrekt und vertrauenswürdig darstellen und die Nutzung der vom Modularen Konnektor angebotenen Abbruchfunktion der Stapelsignatur ermöglichen.

5.5 Sicherheitshinweise zur sicheren Administrierung

Der Leistungserbringer muss sicherstellen, dass administrative Tätigkeiten in Übereinstimmung mit der Dokumentation des Modularen Konnektors durchgeführt werden. Insbesondere muss für diese Tätigkeiten vertrauenswürdiges und hinreichend geschultes Personal eingesetzt werden. Der Administrator darf nur im Sinne des verantwortlichen Leistungserbringers und in dessen Auftrag handeln. Der Administrator ist verantwortlich dafür, die automatische Aktualisierung des Konnektors zu konfigurieren und hat im Falle des manuellen Anwendens von Aktualisierungen das Recht, das Update anzustoßen. Während des Updates müssen alle angeschlossenen (gepairten) Kartenterminals organisatorisch vor unberechtigtem Zugriff geschützt werden. Der Modulare Konnektor unterstützt das automatische Anwenden von Aktualisierungen (Autoupdate) nicht.

Der Administrator muss Authentisierungsinformationen und –token geheim halten bzw. darf diese nicht weitergeben (z. B. PIN bzw. Passwort oder Schlüssel-Token). Der Leistungserbringer als Nutzer des Modularen Konnektors hat die Verantwortung, die Eignung der aktuell genutzten Firmware-Version zu prüfen. Dies beinhaltet die Überprüfung, welche Firmware-Version aktuell eingesetzt wird (siehe Kapitel 11.11.3.2). Weiter beinhaltet dies die Überprüfung, ob die aktuell eingesetzte Firmware-Version eine von der gematik zugelassene Version ist; Informationen dazu erhalten Sie unter www.gematik.de.

Der Leistungserbringer muss sicherstellen, dass die Administrationskonsole (die Benutzerschnittstelle zur Administration des Modularen Konnektors vertrauenswürdig ist. An dieser Benutzerschnittstelle vom Administrator eingegebene Authentisierungsgeheimnisse (z. B. Passwort, PIN, Passphrase) müssen von der Administrationskonsole vertraulich behandelt und nicht zwischengespeichert werden. Die Administrationskonsole muss Bildschirminhalte unverfälscht darstellen.

5.6 Sicherheitshinweise zum Personal

Für den Zugriff befugt sind nur Personen (z.B. medizinisches Personal), die vom Leistungserbringer namentlich autorisiert wurden.

Durch den Einsatz von qualifiziertem und vertrauenswürdigem Personal müssen Fehler und Manipulationen bei Installation, Betrieb, Nutzung, Wartung und Reparatur des Modularen Konnektors ausgeschlossen werden.

Die Benutzer von Clientsystemen müssen vor der Übermittlung an den Modularen Konnektor sicherstellen, dass nur solche Daten zur Signaturerzeugung und zur Signaturprüfung über die Clientsysteme an den Modularen Konnektor übergeben werden, die sie auch tatsächlich signieren bzw. verifizieren wollen.

Leistungserbringer und Praxispersonal müssen kontrollieren, ob der Modulare Konnektor sicherheitstechnische Veränderungen anzeigt. Der Modulare Konnektor verfügt über einen Selbsttest, der die Integrität sicherheitsrelevanter Komponenten prüft und anzeigt (siehe Kapitel 2.2.11). Weiter müssen Leistungserbringer und Praxispersonal kontrollieren, ob Manipulationsversuche am Gehäuse erkennbar sind (siehe Kapitel 4.3).

5.7 Sicherheitshinweise zu Karten

Es dürfen nur von der gematik Zugelassene SMC-B verwendet werden.

Der Leistungserbringer muss gewährleisten, dass nur authentische HBA und SMC-B in den Kartenlesern des lokalen Netzwerkes verwendet werden. Daten der eGK, die vor der Authentisierung der eGK gegenüber dem Modularen Konnektor gelesen werden, dürfen nur zur Identifizierung einer gesteckten Karte anhand des Kartenhandles verwendet werden. Elektronisch gespeicherte personenbezogene Daten auf der eGK dürfen nur nach erfolgreicher Authentisierung der eGK gegenüber dem Modularen Konnektor verwendet werden.

Der Inhaber der SMC-B muss sicherstellen, dass diese nur freigeschaltet ist, wenn sie und der Modulare Konnektor unter seiner Kontrolle arbeiten. Wenn der Karteninhaber keine Kontrolle mehr über den Konnektor oder die SMC-B hat, muss er die Freischaltung der SMC-B zurücksetzen (z.B. durch Ausschalten des Kartenterminals oder Ziehen der Karte).

5.8 Hinweise zur Sorgfaltspflicht der Versicherten

Versicherte dürfen ihre eGK nur dann und nur dort HBA-Inhabern oder ihren Mitarbeitern aushändigen, wenn sie diesen Zugriff auf ihre Daten gewähren wollen. Nach Abschluss der Konsultation nehmen sie ihre eGK wieder an sich.

5.9 Hinweise zur Verarbeitung von XML-Dokumenten

Bitte beachten Sie, dass die Verarbeitung von XML-Dokumenten (z. B. Signaturprüfung) durch nicht von der gematik zugelassene Komponenten (z. B. nicht zugelassene Konnektoren) ein Sicherheitsrisiko (z. B. XML-Signature-Wrapping-Angriffe) darstellen kann.

Vom Modularen Konnektor werden durch den Verschlüsselungsdienst und den Signaturdienst XML-Dokumente verarbeitet. Es gelten die in den Kapiteln 16.17, 16.18 und 16.19 beschriebenen Einschränkungen. Der Konnektor schützt sich damit vor möglichen Angriffen auf die Verarbeitung von XML-Dokumenten. Externe Komponenten, die solche XML-Daten verarbeiten, müssen sich selbst vor möglichen XML-Angriffen schützen. Insbesondere werden Kommentare in den XML-Dokumenten nicht in die Signatur einbezogen oder inhaltlich durch den Konnektor bewertet.

6 Montage

Überprüfen Sie vor der Inbetriebnahme die Unversehrtheit der Sicherheitssiegel und des Gehäuses (siehe Kapitel 4.3.1 und 4.3.2). Bei Beschädigungen darf das Gerät nicht in Betrieb genommen werden.

Beachten Sie die Sicherheitshinweise (siehe Kapitel 5).

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 im Anhang 16.5. Achten Sie insbesondere auf eine ausreichende Belüftung und vermeiden Sie direkte Sonneneinstrahlung.

Beachten Sie:

- **Nehmen Sie bei einer Beschädigung des Gehäuses oder des Netzteils den Modularen Konnektor bzw. das Netzteil sofort außer Betrieb.**
- **Beachten Sie die Hinweise zur Außerbetriebnahme/Entsorgung in Kapitel 15.**
- **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.

Für Hinweise zur Montage siehe:

- Anhang 16.6.1 (Einboxkonnektor, Konstruktionsstand 2.0.0)
- Anhang 16.6.2 (Rechenzentrumskonnektor, Konstruktionsstand 2.1.0)

7 Erstmalige Inbetriebnahme

7.1 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).
- 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.

7.1.1 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

7.1.2 Unterstützte Browser

Um die webbasierte Bedienoberfläche des Modularen Konnektors zu benutzen, ist die Verwendung des Browsers Google Chrome ab Version 80 empfohlen. Die aktuellen Versionen für Windows-, Linux- und Mac OS-Betriebssysteme sind auf der Webseite des Herstellers verfügbar (https://www.google.de/chrome).

7.2 Anforderungen an die Netzwerkumgebung

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 7.2.1). Dies bedeutet, dass auf Basis der vom Modularen Konnektor ausgehenden UDP Pakete die zugehörige UDP Antwort zugelassen wird. Beachten Sie die nachfolgenden Hinweise.

7.2.1 An der LAN-Schnittstelle verwendete Ports

- Management: 8500
- Remote Management: 8501
- Kommunikation mit SICCT-Kartenterminals: 4742
- Der für den Systeminformationsdienst (CETP) benutzte Port wird durch das PVS festgelegt. Beachten Sie die Hinweise des PVS-Herstellers.

7.2.2 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.

- Ausgehend:
  - TCP/UDP: 53 (DNSSec)
  - TCP: 80 (HTTP)
  - TCP: 443 (HTTPS)
  - UDP: 500 (IKE)
  - UDP: 4500 (IKE/IPsec)
  - TCP: 8443 (HTTPS)

Wenn eine Verbindung nicht mit der erstgenannten Konfiguration aufgebaut werden kann, versuchen Sie den Verbindungsaufbau mit folgenden zusätzlich freigegebenen Protokollen aufzubauen:

- ESP Eingehend
- ESP Ausgehend

7.2.3 Übersicht der verwendeten IP-Protokolle

IP-Protokollnummer	Protokoll	Anmerkungen
1	ICMP	
4	IP-in-IP	IP Tunnelung, je nach Konfiguration sowie bei Verwendung von IPComp
6	TCP	
17	UDP	
50	ESP	Sofern NAT nicht verwendet wird
108	IPComp	

Außerdem wird bei Verwendung von NAT die ESP-Kapselung über UDP auf Port 4500 eingesetzt (IPSec NAT Traversal).

7.3 Geheimnis festlegen

Das Geheimnis dient der Identifikation des Leistungserbringers gegenüber einem DVO. Es wird für den Fall benötigt, dass der Leistungserbringer aufgrund fehlender Zugangsdaten keinen Zugriff mehr auf die grafische Bedienoberfläche des Modularen Konnektors hat und wahlweise einen vollständigen Werksreset (siehe Kapitel 11.7.1) oder einen Werksreset der Benutzerkonten (siehe Kapitel 11.7.3) durchführen möchte.

▶ 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.

7.4 Erstanmeldung

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.

Bei Auslieferung ist die Funktion des DHCP-Clients aktiviert, um die IP-Adresse von einem bestehenden DHCP-Server zu beziehen.

In folgenden Ausnamefällen kann für den Modularen Konnektor auch eine feste IP-Adresse mittels Werksreset für Fail Safe vergeben werden (siehe Kapitel 7.4.2):

- Wenn vom DHCP-Server keine IP-Adresse bezogen werden konnte
- Wenn ein Fehler in der Netzwerkkonfiguration vorliegt

7.4.1 Erstanmeldung mittels DHCP-Server (Standardvorgehensweise)

- Schließen Sie den Modularen Konnektor 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 4.4.3.

  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), werden nach ca. 60 Sekunden die folgenden IP-Adressen aus dem Link Local Adressbereich 169.254.0.0/16 zugewiesen: Die LAN-Schnittstelle erhält grundsätzlich die Adresse 169.254.1.1/16, die WAN-Schnittstelle dagegen 169.254.2.1/16. Nach erfolgreich abgeschlossener Erstanmeldung können Sie dem Modularen Konnektor bei Bedarf auch eine feste IP-Adresse manuell zuweisen (siehe Kapitel 9.2.2)

- 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 7.4.3) und importieren Sie es im Browser (siehe Kapitel 7.4.4).

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

- Rufen Sie die Bedienoberfläche erneut auf.

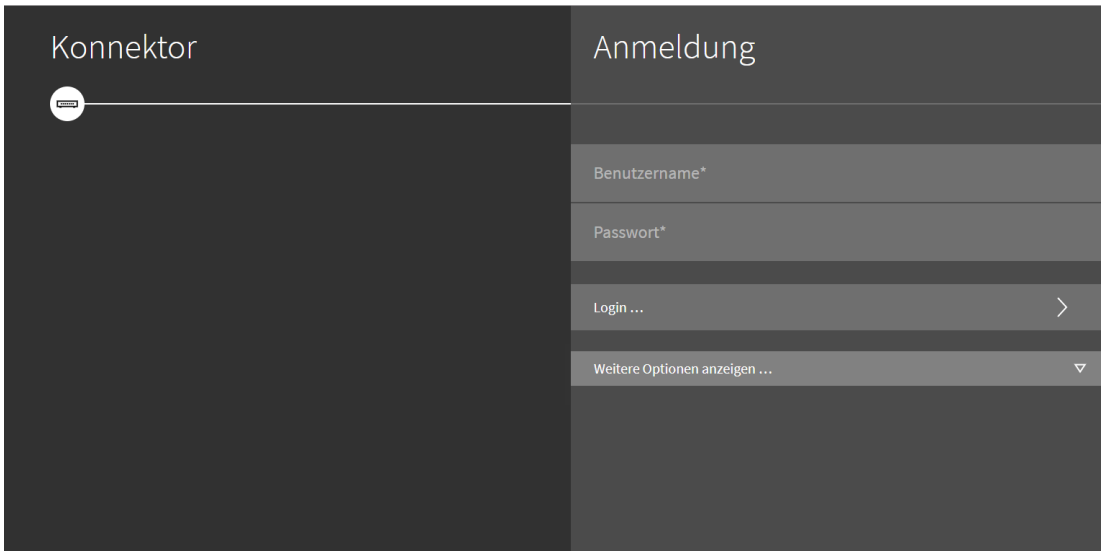


Abbildung 8: Anmeldedialog

- Melden Sie sich mit folgenden initialen Zugangsdaten an:

Benutzername:	`super`
Passwort:	`konnektor`

Sie werden aufgefordert, ein neues Passwort einzugeben.

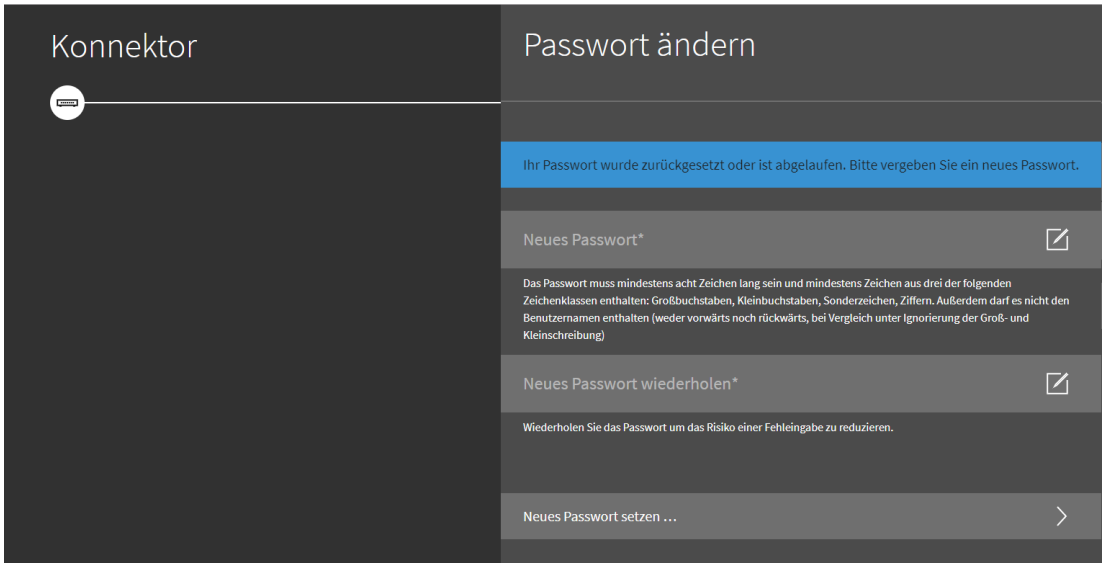


Abbildung 9: Passwort ändern

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 13.

- Geben Sie ein neues Passwort ein. Beachten Sie die Hinweise zu Passwörtern in Kapitel 5.2.
- 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 9.5.3) und passen Sie sie wenn notwendig an.

7.4.2 Erstanmeldung mit fester IP-Adresse

Gehen Sie in den in Kapitel 7.4 genannten Ausnamefällen wie folgt vor:

- Schließen Sie den Modularen Konnektor 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 für Fail Safe (feste IP) durch (siehe Kapitel 11.7.2). Dem Modularen Konnektor wird dadurch die feste IP-Adresse `192.168.210.1/24` zugewiesen.
- Geben Sie nach einem erfolgreich durchgeführten Werksreset für Fail Safe am Clientsystem in der Adresszeile des Browsers folgende Adresse ein:

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

- Fahren Sie danach wie im Kapitel 7.4.1 (Erstanmeldung mittels DHCP-Server) ab dem Schritt „Validieren Sie das Zertifikat des Modularen Konnektors.“ fort.

7.4.3 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 Verbindunganfragen 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.

Alle Anleitungen zu Browsern in diesem Dokument beziehen sich auf den Browser Google Chrome Version 80.

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 7.4). Es sollte nun eine entsprechende Fehlermeldung im Browser angezeigt werden:

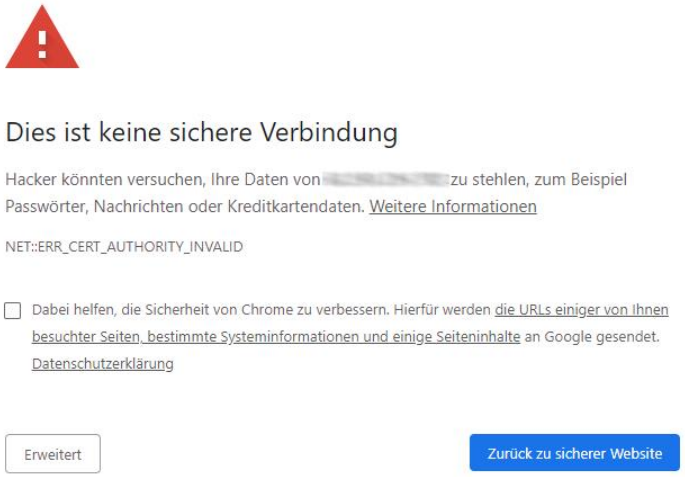


Abbildung 10: Zertifikatsfehler (Beispiel)

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

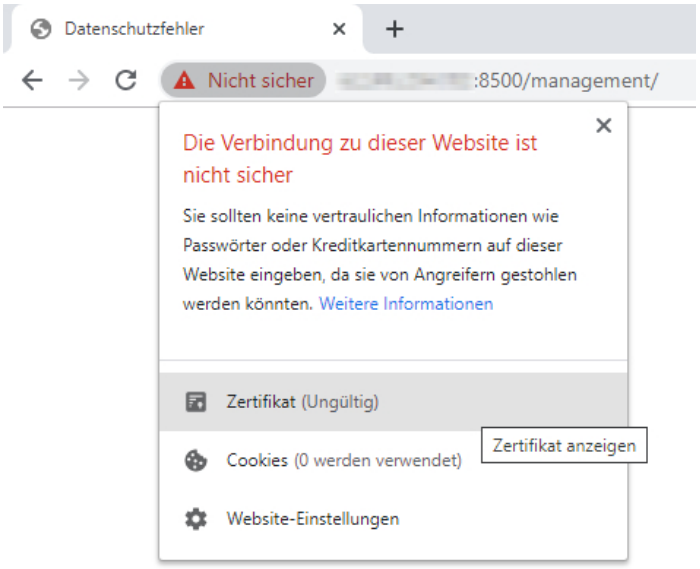


Abbildung 11: Informationen zu unsicherer Verbindung (Beispiel)

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

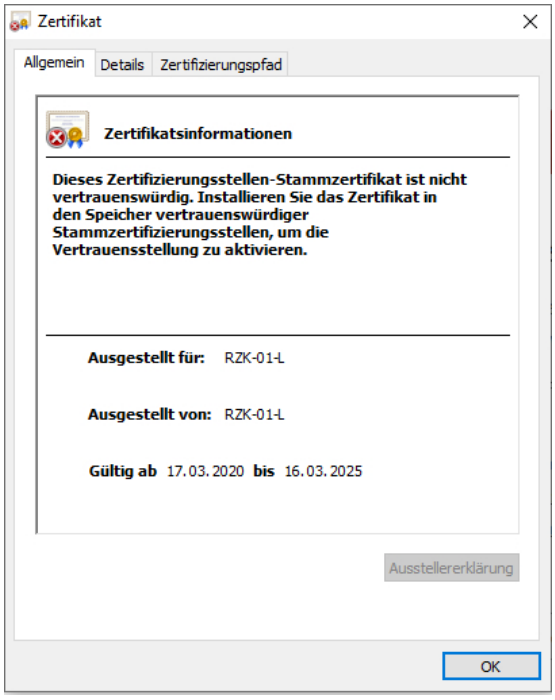


Abbildung 12: Zertifikatsinformationen

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

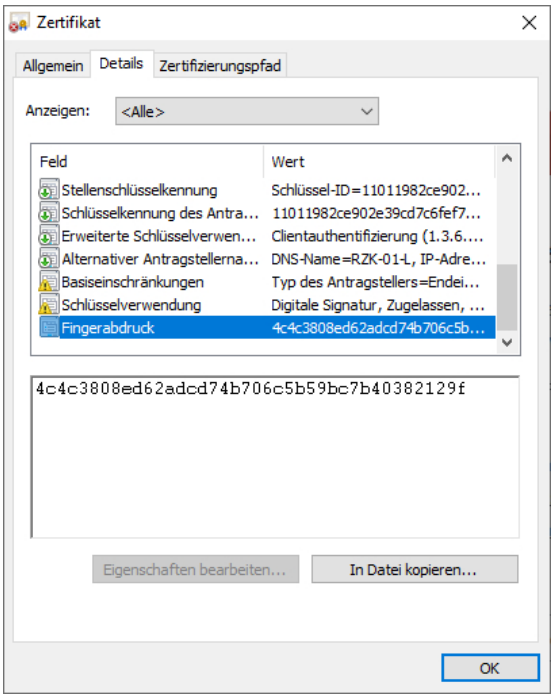


Abbildung 13: Zertifikatsdetails (Beispiel)

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

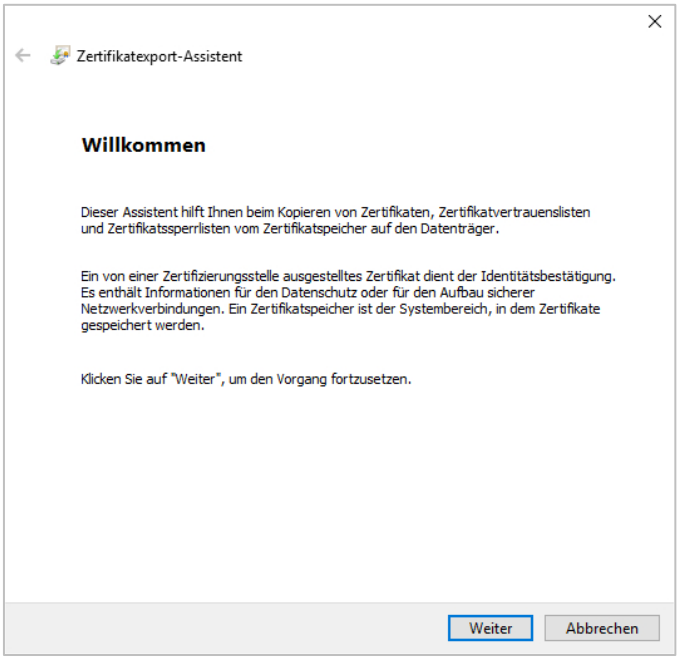


Abbildung 14: Zertifikatexport-Assistent

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

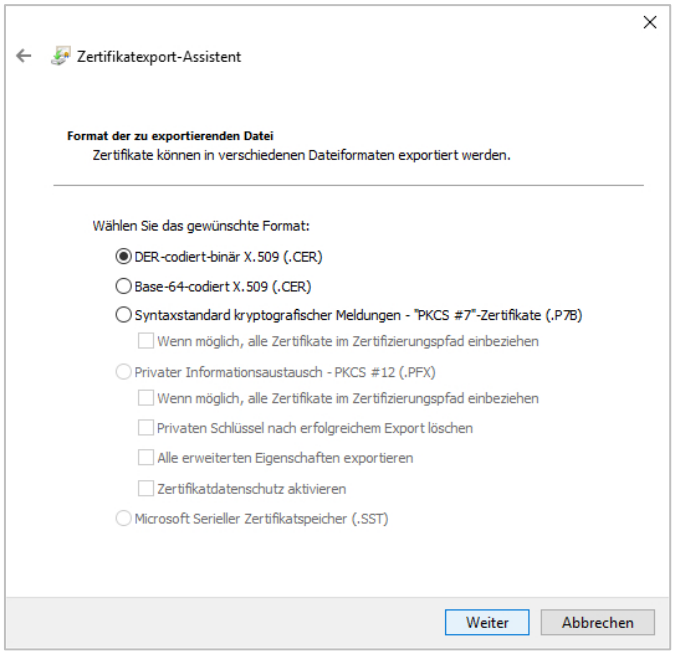


Abbildung 15: Zertifikatsformat

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

7.4.4 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**.

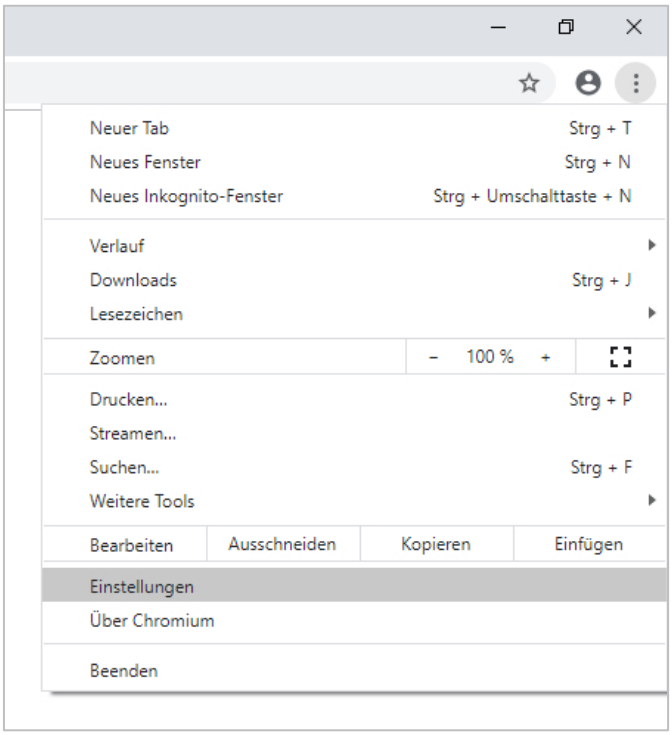


Abbildung 16: Browser-Einstellungen

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

- Klicken Sie **Zertifikate verwalten**.

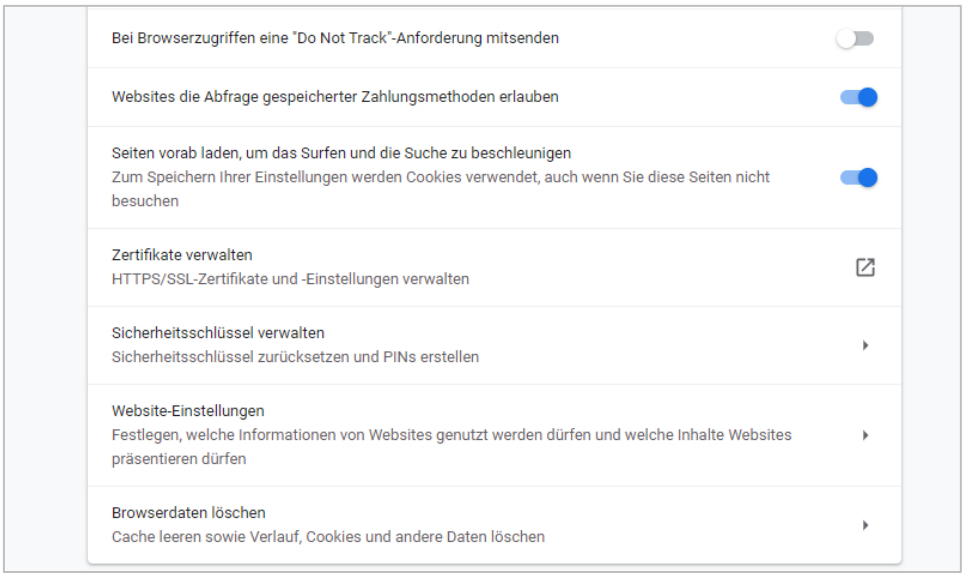


Abbildung 17: Zertifikate verwalten

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

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

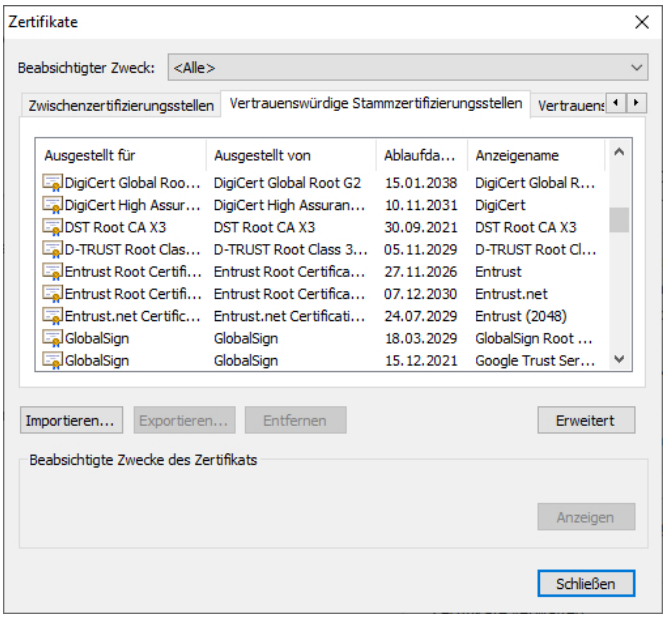


Abbildung 18: Importierte Zertifikate (Beispiel)

Der Zertifikatimport-Assistent öffnet sich:

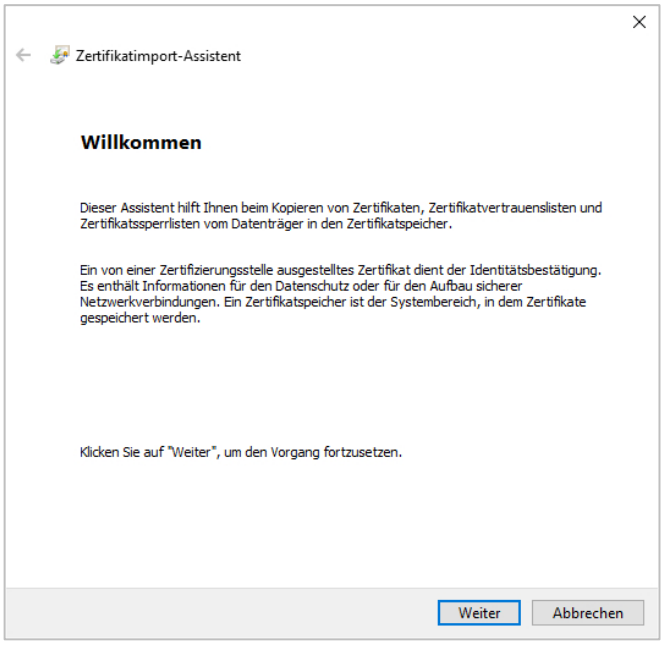


Abbildung 19: Zertifikatimport-Assistent

- 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 Stammzertifizierungsstellen** aus und schließen sie den Import ab.

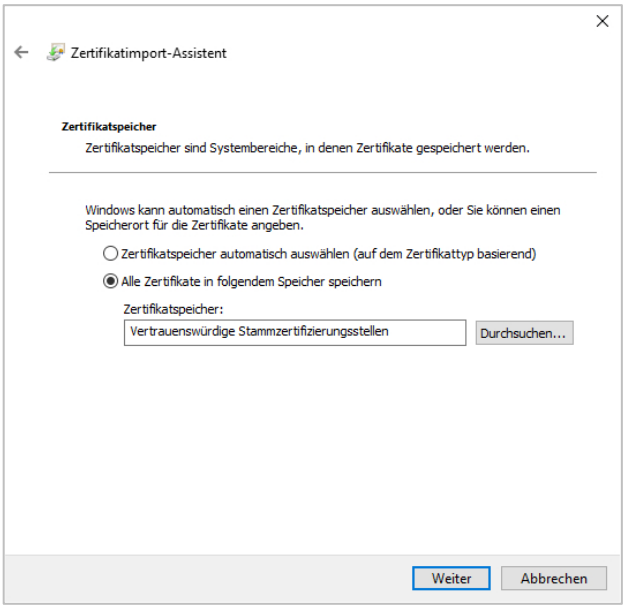


Abbildung 20: Zertifikatsspeicher

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

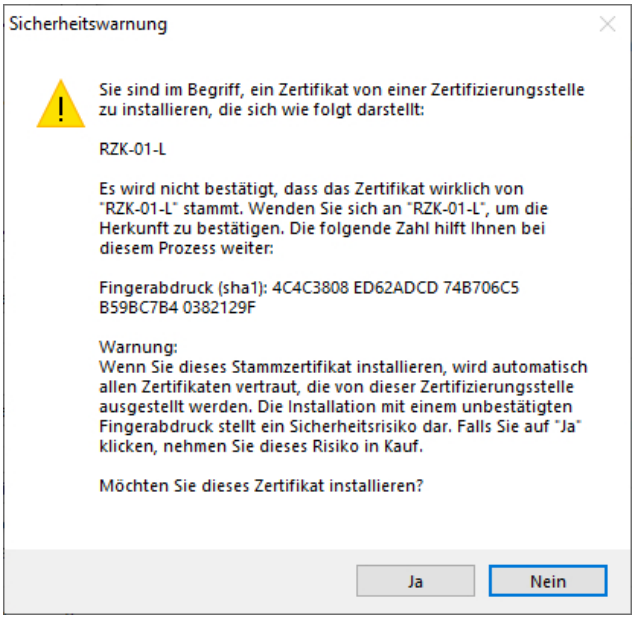


Abbildung 21: Sicherheitswarnung bei Import

- 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).

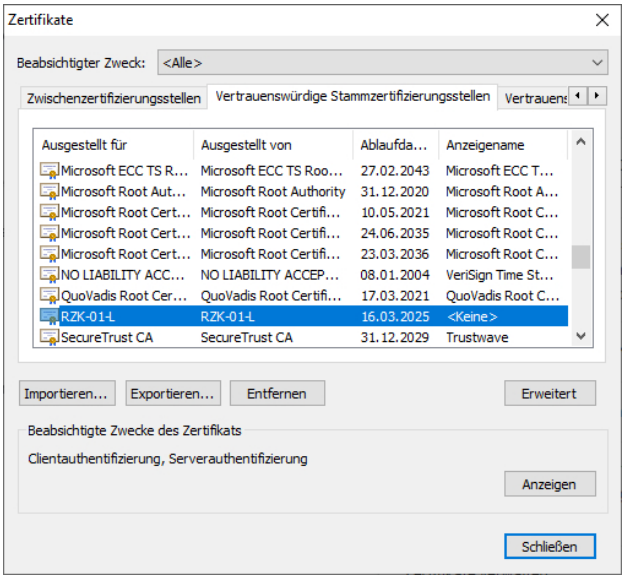


Abbildung 22: Importiertes Zertifikat des Modularen Konnektors

- 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 10 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 8.1).

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.

7.5 Vorgehensweise bei der ersten Konfiguration

Die Konfiguration des Modularen Konnektors ist in Kapitel 8 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 9.5.3).
2. Legen Sie im Menü **System** die grundlegenden Betriebsbedingungen fest (siehe Kapitel 9.5).
3. Legen Sie Benutzer für die Personen an, die den Modularen Konnektor über die Bedienoberfläche administrieren (siehe Kapitel 9.1).

   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 9.5.1).
5. Konfigurieren Sie die Netzwerkschnittstellen und Dienste für die Anbindung an das lokale Netzwerk und nach Bedarf den IAG (siehe Kapitel 9.2 und 9.5). Die WAN-Schnittstelle ist im Auslieferungszustand aktiviert und muss bei Bedarf manuell deaktiviert werden (siehe Kapitel 9.2.3).

Der Modulare Konnektor verwendet, bis einschließlich der Firmwareversion 2.0.38, intern das Netzsegement 192.168.77.0/24. In nachfolgenden Firmwareversionen wird das Segement 169.254.77.0/24 verwendet.

Um eine Kommunikation des Modularen Konnektor mit angeschlossenen Netzsegementen zu ermöglichen, darf es keine Überschneidung mit dem intern verwendeten Netzsegement geben.

6. Verbinden Sie die Kartenterminals des lokalen Netzwerks (siehe Kapitel 10.1).
7. Legen Sie die weiteren Komponenten der Betriebsumgebung, wie Mandanten, Arbeitsplätze und Clientsysteme an (siehe Kapitel 9.3).

   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 9.5.2).

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 9.6).

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

10. Konfigurieren Sie nach Bedarf die Fachmodule (siehe Kapitel 9.7).

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

8 Grundlagen zur 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 7.1.

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.

8.1 An- und Abmeldung

Sie benötigen für die Anmeldung einen unterstützten Browser (siehe Kapitel 7.1.2).

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

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

Verwenden Sie für Remote Management (siehe Kapitel 11.12) folgende Adresse:

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

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

Abbildung 23: Anmeldebildschirm

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 11.7.2).

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.

8.2 Die Ansicht „Home“

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

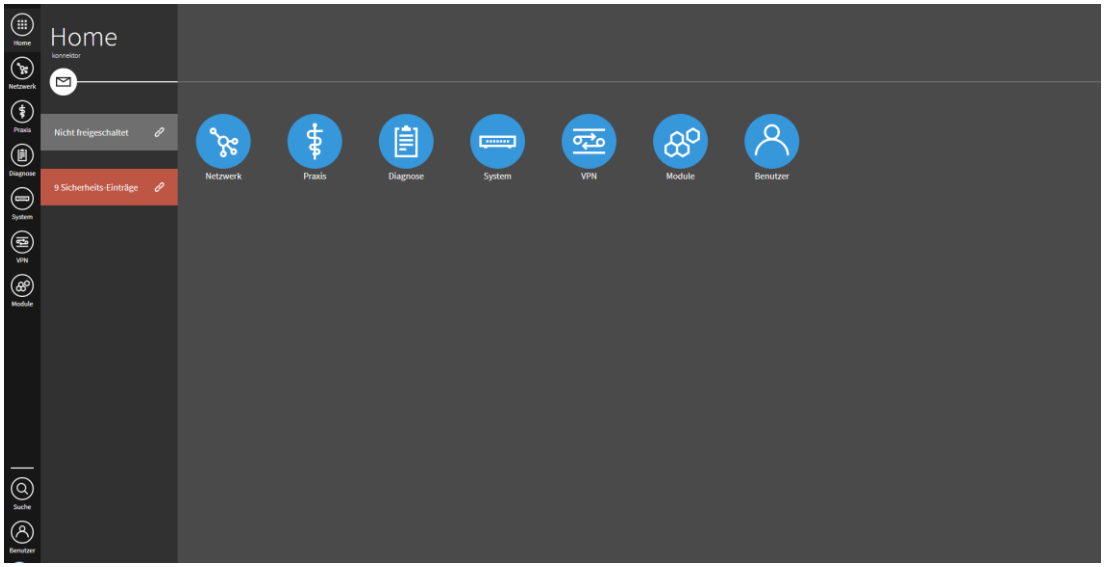


Abbildung 24: Ansicht „Home“

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 16.9).

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

8.3 Übersicht der Menüs

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 9.1.1).

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 9.1).

Netzwerk

In diesem Menü konfigurieren Sie die Netzwerkschnittstellen und Netzwerkdienste (siehe Kapitel 9.2).

Praxis

In diesem Menü verwalten Sie Clientsysteme, Mandanten, Arbeitsplätze, Karten und Terminals (siehe Kapitel 9.3).

Diagnose

In diesem Menü haben Sie Zugriff auf Meldungen (siehe Kapitel 9.4).

System

In diesem Menü treffen Sie allgemeine Einstellungen zum System und verwalten Backups (siehe Kapitel 9.5).

VPN

In diesem Menü konfigurieren Sie die Anbindung an die TI und den SIS (siehe Kapitel 9.6).

Module

In diesem Menü verwalten Sie die auf dem Modularen Konnektor betriebenen Fachanwendungen (siehe Kapitel 9.7) und Lizenzen für lizenzierbare Funktionen (siehe Kapitel 11.10.1).

8.4 In der Bedienoberfläche navigieren

In den Dialogfenstern der Bedienoberfläche navigieren Sie mit folgenden Symbolen:


Zurück


Löschen


Abbrechen (Eingabe verwerfen)


Die Seite enthält ungesicherte Änderungen


Bestätigen

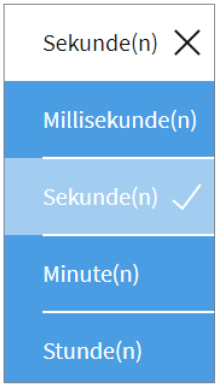

Eingabe in untergeordnetem Formular abschließen; Beachten Sie: Die Eingaben werden erst durch nochmaliges bestätigen mit ✓ gespeichert.


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):



Verknüpfung zu einem Dialogfenster in einem anderen Menü

... Führt zu weiteren Einstellungen

Lade-/Warteanzeigen:

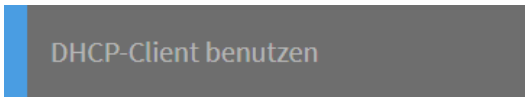
Seite lädt

Aktion wird durchgeführt

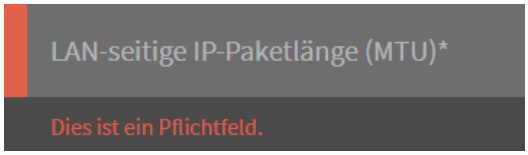
8.4.1 Die Prüfung von Eingaben

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



8.4.2 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.

8.4.3 Die Suchfunktion

Die Suchfunktion erlaubt die schnelle und komfortable Navigation in der Bedienoberfläche.

8.4.3.1 Öffnen/Schließen der Suchfunktion

Die Suchfunktion kann wie folgt geöffnet werden:

- Klicken Sie das Lupensymbol in der linken Navigationsleiste

  oder

- drücken Sie die Taste **S** (sofern nicht gerade ein Eingabefeld geöffnet ist).

Die Suchfunktion kann wie folgt geschlossen werden:

- Klicken Sie das Schließsymbol rechts oben im Fenster

  oder

- drücken Sie die Taste **ESC**.

8.4.3.2 Die Suchfunktion benutzen

Während der Eingabe eines Suchbegriffs werden die angezeigten Suchergebnisse laufend aktualisiert. Die Groß- und Kleinschreibung wird dabei nicht berücksichtigt. Wenn mehrere Suchbegriffe eingegeben werden, reicht es, wenn einer davon für eine Seite gefunden wird (ODER-Verknüpfung).

Weitere Suchfunktionen:

- Das Voranstellen eines Pluszeichens (**+**) erzwingt einen Suchbegriff.
- Das Voranstellen eines Minuszeichens (**-**) schließt einen Suchbegriff aus.
- Begriffe aus der Konnektor-Spezifikation der gematik erscheinen zwar nicht in der grafischen Bedienoberfläche, können jedoch trotzdem über die Suchfunktion gefunden werden. Beispiel: CTM_SERVICE_DISCOVERY_CYCLE findet das Dialogfenster der Terminal-Einstellungen.

Einschränkungen:

- Dynamischen Informationen können nicht über die Suchfunktion gefunden werden. Dazu zählen u.a. IP-Adressen, Karten-Handles, Netzwerke oder Terminalnamen.
- Dialogfenster, deren URL dynamische IDs enthalten (z.B. für spezifische Terminals) können über die Suchfunktion nicht gefunden werden. Stattdessen wird die Auswahlseite mit allen Objekten als Suchergebnis angezeigt; navigieren Sie anschließend manuell zum jeweiligen spezifischen Objekt weiter.

8.4.3.3 In den Suchergebnissen navigieren

Neben dem manuellen Anklicken von Suchergebnissen, um die betreffenden Dialogfenstern aufzurufen, bestehen folgende Möglichkeiten zur Auswahl:

- Die Taste **TAB** wechselt den Fokus vom Suchfeld schrittweise zu jedem Suchergebnis.
- Die Tastenkombination **SHIFT**+**TAB** wechselt den Fokus wieder schrittweise zurück bis zum Suchfeld.
- Wenn ein Suchergebnis mit der Taste **TAB** fokussiert wurde, kann es durch Drücken **ENTER** aufgerufen werden.
- Das Drücken von **ENTER** im Suchfeld ruft sofort das erste Suchergebnis auf.

8.5 Konfigurationsänderungen, die einen Neustart erfordern

Manche Konfigurationsänderungen erfordern bei der Administration des Modularen Konnektors einen Neustart.

Wenn Einstellungen vorgenommen werden, die einen Neustart des Modularen Konnektors erfordern, wird ein Warnhinweis angezeigt. Bestätigen Sie diesen, um die Aktion durchzuführen.

Allgemein gilt:

Sobald eine Konfigurationsänderung mindestens eine Sektion verändert, welche einen Neustart benötigt, werden alle Änderungen dieser Konfigurationsoperation erst nach einem Neustart angewendet. Das gilt auch für Änderungen in Bereichen, die sonst keinen Neustart benötigen.

Wenn nach einer solchen Konfigurationsoperation kein Neustart durchgeführt wird, werden die Änderungen jeder folgenden Konfigurationsänderung auch erst nach einem Neustart angewendet, unabhängig davon, ob die geänderte Sektion einen Neustart erfordert, oder nicht.

Die nachfolgende Tabelle gibt eine Übersicht über Konfigurationsänderungen, die einen Neustart erfordern.

Menü Netzwerk		
Allgemein	Allgemeine Netzwerk-Einstellungen	Internet Modus
Allgemein	Allgemeine Netzwerk-Einstellungen	Intranet Routing Modus

Allgemein	Allgemeine Netzwerk-Einstellungen	Bandbreiten
Allgemein	Erweiterte TLS-Einstellungen	ALLE
WAN	WAN-Modus	WAN-Schnittstelle aktiv
Menü Praxis		
Karten	Einstellungen	Timeout für Kartenoperationen
Karten	Einstellungen	Timeout für PIN-Kommandos
Karten	Einstellungen	Service Discovery Zyklus
Karten	Einstellungen	Service Announcement Port
Karten	Einstellungen	Anzahl Keep-Alive Versuche
Karten	Einstellungen	TLS Handshake Timeout
Karten	Einstellungen	Display Anzeigedauer
Karten	Einstellungen	Timeout für Pairing-Kommandos
Client-system	Clientsystem-Einstellungen	TLS-Pflicht
Client-system	Clientsystem-Einstellungen	Authentifizierung
Client-system	Clientsystem-Einstellungen	Ungesicherter Zugriff auf Dienstverzeichnisdienst
Menü System		
Allgemein	Name	Hostname
Allgemein	Standalone-Szenario	Standalone-Szenario
Menü VPN		
VPN-Zugangsdienst	Netzwerk-Segmente	ALLE
VPN-Zugangsdienst	SIS-Firewall-Regeln	

Bestandsnetze	Bestandsnetze aktivieren / deaktivieren	
Menü Fachmodule		
VSDM	Einstellungen	Intermediär-Servicename

Tabelle 5: Konfigurationsänderungen, die einen Neustart erfordern

9 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 16.8.

Die Konfiguration beispielhafter Netzwerkszenarien ist in Kapitel 10.2 beschrieben.

9.1 Das Menü „Benutzer“

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

Abbildung 25: Menü „Benutzer“

9.1.1 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.

9.1.2 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 9.1.3). Beachten sie die Hinweise zu Passwörtern in Kapitel 5.2.

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.

9.1.3 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 8.1)	Ja	Ja	Nein
Administrationszugriff über Remote Management	Nein	Nein	Ja
Werksreset durchführen (siehe Kapitel 11.5)	Ja	Ja	Nein
Sperrung für den Versand durchführen (siehe Kapitel 11.8)	Ja	Ja	Nein
Verwaltung von Benutzerkonten (siehe Kapitel 9.1.2)	Ja	Nein	Nein
Passwörter zurücksetzen (siehe Kapitel 9.1.4)	Ja	Nein	Nein
Zeitintervall für den Passwortwechsel konfigurieren (siehe Kapitel 9.1.2)	Ja	Nein	Nein
Backup exportieren (siehe Kapitel 9.5.5)	Ja	Ja	Ja
Backup importieren (siehe Kapitel 9.5.5)	Ja	Nein	Nein
Remote Management initialisieren (siehe Kapitel 9.5.1, Einstellung „Remote-Management aktivieren“)	Ja	Ja	Nein
Remote Mangement konfigurieren (siehe Kapitel 9.5.1, Einstellung „Remote-Management erlauben“)	Ja	Nein	Nein
Verwaltung aller übrigen Konfigurationsdaten	Ja	Ja	Ja

Tabelle 6: Berechtigungen der Benutzerrollen

In Ergänzung zur vorstehenden Tabelle besitzen Benutzerkonten mit der Rolle Remote-Admin keine Berechtigung für folgende Vorgänge:

- Schlüssel und X.509-Zertifikate für die Authentisierung eines Clientsystems importieren, erzeugen, löschen und exportieren
- Konfiguration der Anbindung der Clientsysteme
- PIN-Management der SM-Bs für den Administrator
- Einsichtnahme in personenbezogene Daten in den Protokollen
- Hochladen von Offline Updates

Des Weiteren werden dem Remote-Administrator bei den folgenden Vorgängen Karten vom Typ eGK und HBA nicht angezeigt:

- Anzeige der Übersicht über alle verfügbaren Karten
- Anzeige der verfügbaren Karten pro Terminal
- Anzeige des Zertifikatsablaufs

9.1.4 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.

9.2 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.

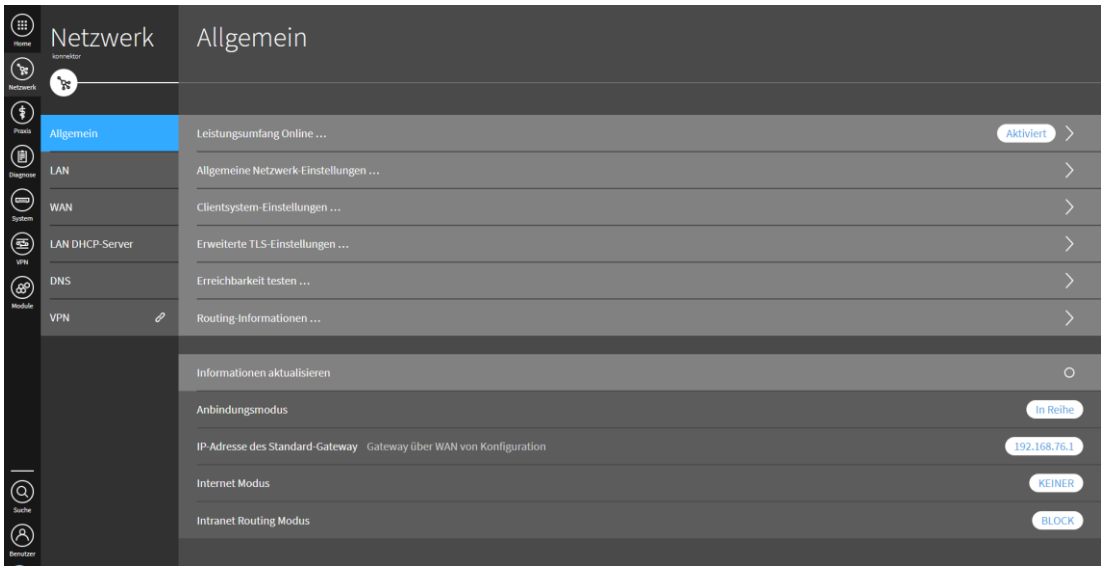


Abbildung 26: Menü „Netzwerk“

9.2.1 Bereich „Allgemein“

Im Bereich **Allgemein** konfigurieren Sie die Funktionalität des Modularen Konnektors im Netzwerk. Im unteren Fensterbereich wird eine Übersicht der aktuellen Einstellungen angezeigt.

- Unter **Leistungsumfang Online …** legen Sie fest, ob der Modulare Konnektor online oder offline betrieben wird (siehe Kapitel 10.2.1.1).
- Unter **Allgemeine Netzwerk-Einstellungen …** konfigurieren sie die grundlegende Infrastruktur der Einsatzumgebung:
  - **Internet Modus** (siehe Kapitel 10.2.1.3)
  - **Intranet Routing Modus**

    Die Weiterleitung oder Blockade von Datenpaketen aus den internen Netzwerken
  - **Service Timeout**

    Die Zeitdauer innerhalb der ein Netzwerkdienst antworten muss, bevor das System einen Timeout-Fehler meldet

- **Intranet Routen**

  Die Routing-Tabelle, anhand derer Datenpakete zu internen Netzwerken geleitet werden

- **Netzwerke der Einsatzumgebung**

  Die internen Netzwerke

- **Bandbreiten**

  Bandbreitenbeschränkung des ausgehenden Datenverkehrs für die Kommunikation mit der TI

- **Minimale Bandbreiten**

  Dienstklassen (DiffServ-Einstufung); diese müssen ggf. mit der Konfiguration der weiteren Komponenten im lokalen Netzwerk übereinstimmen.

- Unter **Clientsystem-Einstellungen …** legen Sie Einstellungen zur Verbindung mit Clientsystemen konfiguriert werden (siehe Kapitel 9.3.3).

Beachten Sie die Sicherheitshinweise in Kapitel 9.3.3.

- 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 (Ping).

- Unter **Routing Informationen …** werden Informationen zum Routing im lokalen Netzwerk angezeigt.

9.2.2 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), werden nach ca. 60 Sekunden die folgenden IP-Adressen aus dem Link Local Adressbereich 169.254.0.0/16 zugewiesen: Die LAN-Schnittstelle erhält grundsätzlich die Adresse 169.254.1.1/16, die WAN-Schnittstelle dagegen 169.254.2.1/16.. 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.

9.2.3 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 10.2.1.2). 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 10.2.1.2).

- 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.

9.2.4 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- Server (der konnektoreigene oder ein externer DNS-Server)
  - NTP-Server (der Modulare Konnektor selbst oder ein externer Server)
  - Default-Gateway (der Modulare Konnektor selbst oder ein anderes gateway)
  - Netzmaske und Domain-Name
  - Lease-Dauer, nach der regelmäßig eine neue IP-Adresse angefordert wird
  - Routen
  - DHCP-Optionen

Bei der Konfiguration des DHCP-Servers kann die Meldung "500 Internal Server Error" ohne zusätzliche Informationen ausgegeben und im Systemprotokoll gespeichert werden. In diesem Fall können Sie Details dem Systemprotokoll entnehmen (siehe Kapitel 9.4.2). Suchen Sie dazu nach dem Begriff **dhcpd_lan**.

9.2.5 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.

  Der DNSSEC Trustanchor ist bis zu 5 Jahre gültig und bedarf keiner Administrierung.

- Mit **Status aktualisieren ...** kann die Anzeige aktualisiert werden.

9.2.6 Verknüpfung „VPN“

Der Menüpunkt **VPN** öffnet das verknüpfte Menü **VPN** (siehe Kapitel 9.6).

9.3 Das Menü „Praxis“

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

Abbildung 27: Menü „Praxis“

9.3.1 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 Dauer von Kartenoperationen und PIN-Eingaben und weitere Einstellungen zur Zertifikatsprüfung festgelegt werden.
- Mit **Zertifikate für gesteckte SMC-B, HBA, SMC-K prüfen** können die Zertifikate der gesteckten Karten verifiziert werden.
- Die im Konnektor verbaute gSMC-K können Sie anhand der Identifikationsnummer (ICCSN) ermitteln. Die ICCSN der Karte besteht aus 20 Stellen. Die elfte Stelle der ICCSN gibt dabei an, ob im Modularen Konnektor gSMC-Ks vom Typ STARCOS (Wert `0`) oder TCOS (Wert `1`) verbaut sind (siehe Tabelle 18 bzw. Tabelle 20).

Um die SMC-B in Betrieb zu nehmen, muss sie freigeschaltet und aktiviert werden. Nach der Auslieferung ist die SMC-B mit einer Transport-PIN geschützt, die Sie getrennt im PIN-Brief erhalten. Weitere Informationen zur Freischaltung der SMC-B erhalten Sie vom Anbieter.

Der Inhaber der SMC-B muss sicherstellen, dass diese nur freigeschaltet ist, wenn sie und der Modulare Konnektor unter seiner Kontrolle arbeiten. Wenn der Karteninhaber keine Kontrolle mehr über den Konnektor oder die SMC-B hat, muss er die Freischaltung der SMC-B zurücksetzen (z.B. durch Ausschalten des Kartenterminals oder Ziehen der Karte).

9.3.2 Bereich „Terminals“

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

Die maximale Zahl der Kartenterminals, die verwaltet werden können, hängt vom lizenzierten Funktionsumfang ab (siehe Kapitel 11.10).

Der Einboxkonnektor ist für mindestens 45 Kartenterminals zugelassen. Die Lizenz gilt für 50 Kartenterminals und ist erweiterbar.

Um das Performanceniveau garantiert aufrecht zu erhalten, sollte vorab mit dem technischen Dienstleister besprochen werden, welche Anzahl als sinnvoll anzusehen ist. Wir empfehlen die Nutzung von 25 Kartenterminals je Konnektor.

Der Rechenzentrumskonnektor ist für mindestens 50 Kartenterminals zugelassen. Die Lizenz gilt für 50 Kartenterminals je Recheneinheit, folglich für 100 Kartenterminals insgesamt. Eine Erweiterung der Lizenz ist möglich.

Um das Performanceniveau garantiert aufrecht zu erhalten, sollte vorab mit dem technischen Dienstleiter besprochen werden, welche Anzahl als sinnvoll anzusehen ist. Wir empfehlen die Nutzung von 50 Kartenterminals je RZ-Konnektor.

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 **Kartenterminal neu hinzufügen …** kann ein neues Terminal manuell unter Eingabe von IP-Adresse, MAC-Adresse und Hostname angelegt werden.

  Beachten Sie, dass beim manuellen Hinzufügen eines Kartenterminals das Feld zur Angabe einer Portnummer leer sein muss. Der Konnektor verwendet automatisch die spezifizierten Ports.

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:

- **Bearbeiten …**

  Geben Sie ggf. Benutzername und Passwort des Administrationszugangs ein, um im Modularen Konnektor Updates für das Kartenterminal durchführen zu können (siehe Kapitel 11.11). Die Zugangsdaten werden im Terminal selbst verwaltet.

- **Verbindungsdaten bearbeiten**

  Passen sie ggf. manuell die Netzwerkeinstellung des Kartenterminals an.

- **Terminal erneut auslesen**

  Stößt die erneute automatische Erkennung der Verbindungseinstellungenan.

- **Kartenterminal dem Konnektor zuweisen …**

  Bevor ein Kartenterminal genutzt werden kann, muss es dem Modularen Konnektor durch Pairing zugeordnet werden (siehe Kapitel 10.1.1).

Der Administrator ist für die korrekte Zuordnung von Kartenterminals verantwortlich.

Nach dem Pairing sind weitere Zuordnungen des Kartenterminals erforderlich (siehe Kapitel 10.1.2).

- **Kartenterminal entfernen**

9.3.3 Bereich „Clientsysteme“

Im Bereich **Clientsysteme** verwalten Sie die Clientsysteme des lokalen Netzwerks.

Der Administrator ist für die korrekte Zuordnung von Clientsystemen verantwortlich.

Sie haben folgende Möglichkeiten:

- Mit **Konnektor-Zertifikat herunterladen …** kann das Zertifikat des Modularen Konnektors heruntergeladen werden.
- Mit **Clientsystem anlegen …** kann ein Clientsystem unter Angabe einer ID (interne Kennung) angelegt werden.

  Klicken Sie bei Bedarf ein Clientsystem an, um dessen Einstellungen zu bearbeiten.

- Der Menüpunkt **Clientsystem-Einstellungen** 🔗 öffnet die verknüpften Einstellungen zur Konfiguration der Absicherungsmethode für Verbindungen zu Clientsystemen.

Der Modulare Konnektor und die Clientsysteme tauschen Daten über die SOAP/HTTP-Schnittstelle aus; zudem werden optional Benachrichtigungen über Ereignisse des Systeminformationsdienstes vom Modularen Konnektor über das CETP-Protokoll an die Clientsysteme versendet (siehe Kapitel 9.4.5).

Im Modularen Konnektor kann die Absicherung der SOAP/HTTP-Verbindung zu Clientsystemen auf vier verschiedene Arten konfiguriert werden:

1. TLS deaktiviert (keine Absicherung auf Transportebene)

   ▶ Deaktivieren Sie dazu in den **Clientsystem-Einstellungen** die Option **TLS-Pflicht** und wählen Sie die Authentifizierungsmethode **Keine Authentifizierung** aus.

2. TLS aktiviert, mit Server-Authentisierung jedoch ohne Client-Authentisierung

   ▶ Aktivieren Sie dazu in den **Clientsystem-Einstellungen** die Option **TLS-Pflicht** und wählen Sie die Authentifizierungsmethode **Keine Authentifizierung** aus.

   ▶ Laden Sie für die Server-Authentifizierung mit **Konnektor-Zertifikat herunterladen …** das Zertifikat des Modularen Konnektors herunter und importieren Sie es im PVS.

3. TLS aktiviert, mit Server-Authentisierung und Client-Authentisierung mittels Benutzername und Passwort

   ▶ Aktivieren Sie dazu in den **Clientsystem-Einstellungen** die Option **TLS-Pflicht** und wählen Sie die Authentifizierungsmethode **Benutzername/ Passwort** aus.

   ▶ Legen Sie in den Einstellungen der einzelnen Clientsysteme mit **Benutzerkennung hinzufügen …** jeweils die Anmeldedaten für die Authentifizierung des PVS fest.

   Das Passwort zur Client-Authentisierung muss mindestens 20 Zeichen lang sein und Zeichen aus den folgenden vier Zeichenarten enthalten:

   - Großbuchstaben (`ABCDEFGHIJKLMNOPQRSTUVWXYZÄÖÜ`)
   - Kleinbuchstaben (`abcdefghijklmnopqrstuvwxyzäöü`)
   - Sonderzeichen (`ß#?!@$%^&*-`)

- Ziffern (1234567890)

Beachten Sie die Sicherheitshinweise zum Passwort zur Client-Authentisierung:

Das Passwort zur Client-Authentisierung darf nicht schriftlich aufbewahrt und nicht an Dritte weitergegeben werden. Werden die oben genannten Vorgaben zur Festlegung des Passworts nicht beachtet, besteht die Gefahr, dass kein ausreichender Schutz gegen Man-in-the-Middle Attacken besteht. Zudem müssen die Passwörter zufällig und für jedes Clientsystem unterschiedlich und unabhängig voneinander gewählt werden

Die Möglichkeit zur Nutzung eines Passworts zur Client-Authentisierung mit mindestens 20 Zeichen und den vier Zeichenarten ist davon abhängig, ob das verwendete Primärsystem diese Funktion unterstützt. Falls nicht, darf TLS aktiviert, mit Server-Authentisierung und Client-Authentisierung mittels Benutzername und Passwort nicht verwendet werden.

- ▶ Konfigurieren Sie im PVS die Anmeldedaten für die Client-Authentisierung, sodass eine Übereinstimmung mit der Konfiguration im Modularen Konnektor besteht. Beachten Sie die Hinweise des PVS-Herstellers.
- ▶ Laden Sie für die Server-Authentifizierung mit **Konnektor-Zertifikat herunterladen …** das Zertifikat des Modularen Konnektors herunter und importieren Sie es im PVS.

4. TLS aktiviert, mit Server-Authentisierung und Client-Authentisierung per Zertifikat

- ▶ Aktivieren Sie dazu in den **Clientsystem-Einstellungen** die Option **TLS-Pflicht** und wählen Sie die Authentifizierungsmethode **Zertifikat** aus.
- ▶ Legen Sie in den Einstellungen der einzelnen Clientsysteme jeweils das zu verwendende Zertifikat fest. Die Client-Authentisierung erfolgt mit einem Zertifikat, das Sie im Modularen Konnektor erzeugen und in das PVS importieren.

  Klicken Sie dazu **Zertifikat erstellen …** und geben Sie ein Passwort für die zu erzeugende P12-Datei ein.

  Klicken Sie das erzeugte Zertifikat an und wählen Sie **Zertifikat herunterladen …** , um es anschließend im PVS zu importieren. Dazu benötigen Sie das beim Erzeugen eingegebene Passwort.

  Beachten Sie die Hinweise des PVS-Herstellers.

Nutzen Sie zur Client-Authentisierung nach einem Werksreset das im Modularen Konnektor erzeugte und heruntergeladene X.509-Zertifikat. Dieses können Sie mit der Option **Zertifikat hochladen …** in den Modularen Konnektor einspielen. Gehen Sie dazu wie im Kapitel 11.4.2 beschrieben vor.

- Laden Sie für die Server-Authentifizierung mit **Konnektor-Zertifikat herunterladen …** das Zertifikat des Modularen Konnektors herunter und importieren Sie es im PVS.

Die Absicherung der CETP-Verbindung geschieht wie folgt:

1. TLS deaktiviert.

   Verwendung von CETP ohne Absicherung auf Transportebene

   - Diese Methode wird verwendet, wenn die Option **TLS-Pflicht** deaktiviert ist.

2. TLS mit Server-Authentisierung

   Wenn das PVS (TLS-Server) eine Authentisierung vom Modularen Konnektor im Rahmen des TLS-Verbindungsaufbaus anfordert, authentisiert sich der Modulare Konnektor, so dass eine beidseitig authentisierte Verbindung erreicht wird.

   - Diese Methode wird verwendet, wenn die Option **TLS-Pflicht** aktiviert ist.

Beachten Sie folgende Hinweise zu Verbindungen mit Clientsystemen:

Ohne gesicherte beidseitig-authentisierte Verbindung zwischen dem Clientsystem und dem Modularen Konnektor bestehen Sicherheitseinschränkungen. Ohne Authentisierung des Modularen Konnektors durch das Clientsystem ist keine TLS-basierte Funktion des CETP-Protokolls möglich; Nachrichten des Systeminformationsdienstes können dadurch nicht authentisch, integer und vertraulich empfangen werden. Beachten Sie die Hinweise des PVS-Herstellers, um im PVS eine zertifikatsbasierte Authentisierung einzurichten.

Ungesicherte Verbindung zwischen dem Clientsystem und dem Modularen Konnektor bietet keinen Schutz gegen Man-in-the-Middle Attacken.

Eine einseitige TLS-Authentisierung des Modularen Konnektors kann dazu führen, dass unbemerkt qualifizierte elektronische Signaturen über von Angreifern vorgegebene Dokumente erstellt werden.

Verwenden Sie eine Verbindung ohne TSL-Absicherung nur zu Testzwecken.

Der für den Systeminformationsdienst (CETP) benutzte Port wird durch das PVS festgelegt. Beachten Sie die Hinweise des PVS-Herstellers.

9.3.3.1 Sichere Anbindung des Clientsystems

Das Clientsystem kommuniziert mit dem Modularen Konnektor über verschiedene Protokolle (SOAP, CETP, LDAP). Wie in Kapitel 9.3.3 beschrieben, kann die Kommunikation dabei durch einen TLS-Kanal abgesichert werden (siehe dazu Warnhinweis zu TLS in Kapitel 9.3.3).

In der folgenden Tabelle sind die verschiedenen Konfigurationsmöglichkeiten zusammengefasst:

Protokoll	**Clientsystem**	**Modularer Konnektor**
TLS-Pflicht deaktiviert (ANCL_TLS_MANDATORY=Disabled, ANCL_CAUT_MANDATORY=Disabled)		
SOAP	TLS ist optional. Wenn TLS verwendet wird, dann: [ANCL_CAUT_MODE=CERTIFICATE oder ANCL_CAUT_MODE=PASSWORD oder NOAUTH]	TLS ist optional. Wenn TLS verwendet wird, dann: CERTIFICATE
CETP	Kein TLS	Kein TLS
LDAP-Proxy	TLS ist optional. Wenn TLS verwendet wird, dann: [ANCL_CAUT_MODE=CERTIFICATE or NOAUTH]	TLS ist optional. Wenn TLS verwendet wird, dann: CERTIFICATE
TLS-Pflicht aktiviert (ANCL_TLS_MANDATORY=Enabled **Authentifizierungsmethode Benutzername/Passwort** (ANCL_CAUT_MANDATORY=Enabled, ANCL_CAUT_MODE=PASSWORD		
SOAP	PASSWORD	CERTIFICATE
CETP	CERTIFICATE	Optional CERTIFICATE (wenn vom Clientsystem angefordert)
LDAP-Proxy	NOAUTH	CERTIFICATE

TLS-Pflicht aktiviert (ANCL_TLS_MANDATORY=Enabled) **Authentifizierungsmethode: Zertifikat** (ANCL_CAUT_MANDATORY=Enabled, ANCL_CAUT_MODE= CERTIFICATE)		
SOAP	CERTIFICATE	CERTIFICATE
CETP	CERTIFICATE	CERTIFICATE
LDAP-Proxy	CERTIFICATE	CERTIFICATE
TLS-Pflicht aktiviert (ANCL_TLS_MANDATORY=Enabled) **Authentifizierungsmethode: Keine Authentifizierung** (ANCL_CAUT_MANDATORY=Disabled)		
SOAP	NOAUTH	CERTIFICATE
CETP	CERTIFICATE	Optional CERTIFICATE (wenn vom Clientsystem angefordert)
LDAP-Proxy	NOAUTH	CERTIFICATE

Tabelle 7: Konfigurationsmöglichkeiten für die Anbindung des Clientsystems

Dabei gelten folgende Festlegungen:

CERTIFICATE = Zertifikatsbasierte Authentisiserung

PASSWORD = Authentifizierung mit Benutzername/Passwort

NOAUTH = Keine Authentisierung des Clientsystems

9.3.4 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. Anschließend können dem Arbeitsplatz lokale und entfernte Kartenterminals zugewiesen werden.

Klicken Sie bei Bedarf einen Arbeitsplatz an, um seine Einstellungen zu bearbeiten.

9.3.5 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 10.2.7).
- 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 bei Bedarf einen Mandanten an, um seine Einstellungen zu bearbeiten.

9.3.6 Bereich „Aufrufkontexte“

Ein Aufrufkontext ist eine Kombination aus Clientsystem, Mandant und Arbeitsplatz für die Kommunikation zwischen dem PVS und dem Modularen Konnektor.

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.

9.4 Das Menü „Diagnose“

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

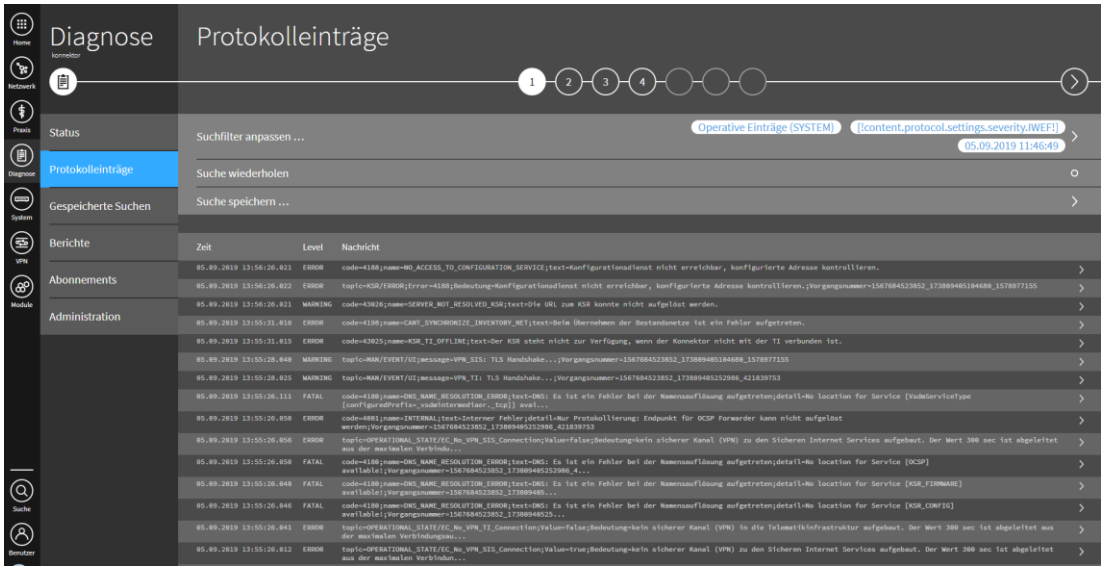


Abbildung 28: Menü „Diagnose“

9.4.1 Bereich „Status“

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

Mit **Selbst-Test …** können Sie eine Prüfung der Integrität sicherheitsrelevanter Komponenten durchführen (siehe Kapitel 2.2.11).

9.4.2 Bereich „Protokolleinträge“

Im Bereich **Protokolleinträge** werden die protokollierten Meldungen angezeigt. Um sie zu durchsuchen, können Sie unter **Suchfilter anpassen ...** Suchkriterien festlegen. Die Suche wird daraufhin automatisch durchgeführt und die gefundenen Meldungen werden angezeigt. Eine ausführliche Beschreibung der Meldungen finden Sie im Kapitel 16.9.

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 9.4.3).

Optional können Sie Meldungen exportieren und herunterladen:

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

9.4.3 Bereich „Gespeicherte Suchen“

Im Bereich **Gespeicherte Suchen** werden gespeicherte Suchfilter-Einstellungen angezeigt. Wenn Sie eine gespeicherte Suche anklicken, 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.

9.4.4 Bereich „Berichte“

Im Bereich **Berichte** können Sie im CSV-Format Berichte über die erstellten Protokolleinträge herunterladen. Dabei werden nur die entsprechend der Protokolleinstellungen (siehe Kapitel 9.4.6) erstellten Einträge erfasst:

- Fehlerstistiken
- Ereignisse
- Performancedaten, sofern das Performance-Protokoll aktiv ist

9.4.5 Bereich „Abonnements“

Benachrichtigungen über Ereignisse werden vom Modularen Konnektor über das CETP-Protokoll an die Clientsysteme versendet.

Im Bereich **Abonnements** wird angezeigt, ob und mit welchen Adressen sich Clientsysteme dazu erfolgreich am Systeminformationsdienst des Modularen Konnektor registriert haben. Abonnementen können bei Bedarf gelöscht werden.

9.4.6 Bereich „Administration“

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

- Unter **Protokoll-Einstellungen …** können Sie für die verschiedenen Protokolle (siehe Kapitel 16.9.1) festlegen, welche Ereignisse protokolliert werden und wie lange Protokolleinträge gespeichert bleiben.
  - Unter **Allgemein** konfigurieren Sie die Einstellungen für Einträge in das Sicherheitsprotokoll.
  - Unter **System** konfigurieren Sie die Einstellungen für operative Einträge in das Systemprotokoll und das Performanceprotokoll
  - Unter **VSDM**, **AMTS** und **NFDM** konfigurieren Sie die Einstellungen für operative Einträge in die Systemprotokolle und Performanceprotokolle der jeweiligen Fachmodule.
- Unter **Protokolle leeren** können Sie bestehende Protokolleinträge löschen.

Es können nur System- und Performance-Protokolle geleert werden. Das Sicherheitsprotokoll kann nicht geleert werden und bleibt auch bei einem vollständigen Werksreset erhalten (siehe Kapitel 11.5).

9.5 Das Menü „System“

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

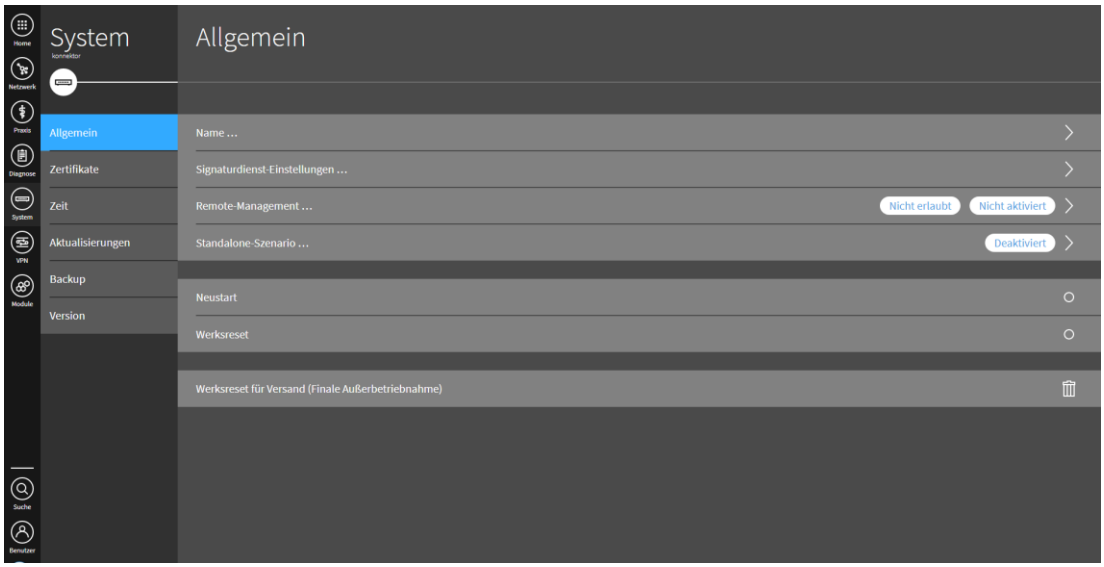


Abbildung 29: Menü „System“

9.5.1 Bereich „Allgemein“

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

Sie haben folgende Möglichkeiten:

- **Name …**

  Legt den Hostnamen des Modularen Konnektors fest.

  Dieser kann maximal 12 Zeichen lang sein und kann aus folgenden Zeichen bestehen:

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

Beachten Sie bei einer Änderung des Hostnamens die Hinweise in Kapitel 11.5. Vor der Validierung des nach der Änderung des Hostnamens neu generierten Konnektor-Zertifikates dürfen keine Zugangsdaten an der Administrationsschnittstelle eingegeben werden.

- **Signaturdienst-Einstellungen**
  Legt fest, ob die Signaturanwendungskomponente aktiv ist und steuert den Einfachsignaturmodus (siehe Kapitel 2.2.8).

- **AES-NI-Einstellungen**
  Steuert die Hardwareunterstützung AES-NI (beachten sie die Hinweise in Kapitel 2.2.12).

Nach jeder Änderung der Hardwareunterstützung AES-NI ist der Neustart des Modularen Konnektors erforderlich.

- **Remote-Management …**
  Wenn Remote Management erlaubt und aktiviert ist, kann der Modulare Konnektor über das öffentliche Netzwerk administriert werden (siehe Kapitel 10.2.1.5).

- **Standalone-Szenario …**
  Wenn aktiviert, arbeitet der Modulare Konnektor ohne angeschlossene Clientsysteme (siehe Kapitel 10.2.1).

- **Neustart**
  Startet das Gerät unter Beibehaltung der bisherigen Konfiguration neu.

- **Werksreset**
  Führt einen vollständigen Werksreset aus; beachten Sie das Kapitel 11.5.

- **Werksreset für Versand (Finale Außerbetriebnahme)**
  Führt die Sperrung für den Versand aus (siehe Kapitel 11.8).

9.5.2 Bereich „Zertifikate“

Der Zertifikatsdienst stellt Funktionen zur Validierung von Zertifikaten zur Verfügung (siehe Kapitel 2.2.4).

Sie haben folgende Möglichkeiten:

- Unter **Einstellungen …** können Zeitfristen für Aktualisierungen und OCSP-Abfragen konfiguriert werden.
- Unter **Missbrauch-Erkennung-Einstellungen …** können die Obergrenzen für die Häufigkeit angepasst werden, ab denen bei bestimmten Aktivitäten ein Missbrauchs-Alarm abgegeben wird. Der aktuelle Stand der Zählung kann unter **Missbrauch-Erkennung-Status …** angezeigt werden.

- Mit **CA-Zertifikate …** können CA-Zertifikate importiert werden und stehen dann für den Verschlüsselungsdienst zur Verfügung (siehe Kapitel 11.4).

Der Administrator ist für die Verlässlichkeit der importierten CA-Zertifikate verantwortlich. Für den Administrator sind dazu von der gematik Informationen für die Entscheidung über den Import von CA-Zertifikaten verfügbar. Die gematik veröffentlicht dazu Informationen über CA-Betreiber, welche die Erfüllung der Sicherheitsanforderungen der gematik nachgewiesen haben.

- Weiterhin können folgende Dateien manuell hochgeladen oder aktualisiert werden:
  - TSL
  - CRL
  - BNetzA-VL (Vertrauensliste der BNetzA)

  Bei einer bestehenden Verbindung zur TI werden diese Dateien normalerweise automatisch aktualisiert. Ein manuelles hochladen ist nur möglich, wenn im Modularen Konnektor die Option **Leistungsumfang Online** deaktiviert ist (siehe Kapitel 9.2.1).

  Im Weiteren werden Informationen zu den aktuell verwendeten TSL/CRL/ BNetzA-V angezeigt; diese können bei Bedarf heruntergeladen werden.

- Unter **OCSP-Forwarder** werden die aktuellen Gegenstellen des OCSP-Dienstes der TI zur automatischen Aktualisierung von TSL und CRL angezeigt.

- Mit **Erreichbarkeit der OSCP-Forwarder prüfen ...** kann geprüft werden, ob der OCSP-Dienst erreichbar ist.

9.5.3 Bereich „Zeit“

In diesem Bereich konfigurieren Sie die Systemzeit:

- Unter **Zeit einstellen …** können Zeit und Zeitzone vom aktuell verwendeten Rechner übernommen oder manuell festgelegt werden.

- Mit **Zeitsynchronisierung auslösen …** kann bei Online-Betrieb die Synchronisierung der Systemzeit mit dem NTP-Server der TI durchgeführt werden.

Unter **NTP-Server** werden Informationen zum aktuell verwendeten NTP-Server angezeigt (siehe Kapitel 16.7.4).

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.**

9.5.4 Bereich „Aktualisierungen“

In diesem Bereich verwalten Sie Systemaktualisierungen (Updates/Downgrades, siehe auch Kapitel 11.11):

- 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 hochgeladen werden (Offline-Update).
  - Unter **Mögliche Downgrades** werden verfügbare Downgrades auf frühere Versionen angezeigt. Klicken Sie ein Downgrade an, um es zu installieren.

- Unter **Mögliche Neuinstallation der bereits installierten Version** wird angezeigt, ob eine Neuinstallation der aktuellen Version möglich ist.

9.5.5 Bereich „Backup“

In diesem Bereich können Sie Systemsicherungen (Backups) erstellen und importieren (siehe Kapitel 11.9).

9.5.6 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 zu einzelnen Softwarekomponenten angezeigt werden.

9.6 Das Menü „VPN“

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

Abbildung 30: Menü „VPN“

9.6.1 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
- Erweiterte Einstellungen zu IKE und IPSec.

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.

Unter **Freischaltung ...** können Sie den Freischaltungsstatus abfragen oder den Modularen Konnektorn am VPN-Zugangsdienst der TI freischalten. Sie benötigen dazu die Vertragsnummer (Contract ID), die Sie von Ihrem Zugangsdienst-Anbieter erhalten.

9.6.1.1 Modularen Konnektor freischalten

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.

9.6.1.2 Freischaltung des Modularen Konnektors zurückzunehmen

Gehen Sie wie folgt vor:

- ▶ Sofern Sie den Sicheren Internetservice (SIS) nutzen, beenden Sie diesen, bevor Sie die Freischaltung zurücknehmen (siehe Kapitel 9.6.3 zum Trennen einer bestehenden VPN-Verbindung zum SIS).
- ▶ Klicken Sie **Konnektorfreischaltung zurücknehmen**.
- ▶ Um eine zurückgenommene Freischaltung wieder Herzustellen, klicken Sie bei Bedarf **Konnektor erneut freischalten**.

9.6.2 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.

9.6.3 Verbindungen zur TI und SIS

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

9.6.4 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 Clientsystemen 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 9.6.1). Je nach Anbindungsmodus des Modularen Konnektors (siehe Kapitel 10.2.1.2) 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.

9.7 Das Menü „Module“

Im Menü **Module** werden Informationen über die auf dem Modularen Konnektor betriebenen FachModule angezeigt. Standardmäßig sind folgende Fachmodule installiert:

- Versichertenstammdatenmanagement (VSDM)
- Notfalldatenmanagement (NFDM)
- Elektronischer Medikationsplan/Arzneimitteltherapiesicherheit (eMP/AMTS)

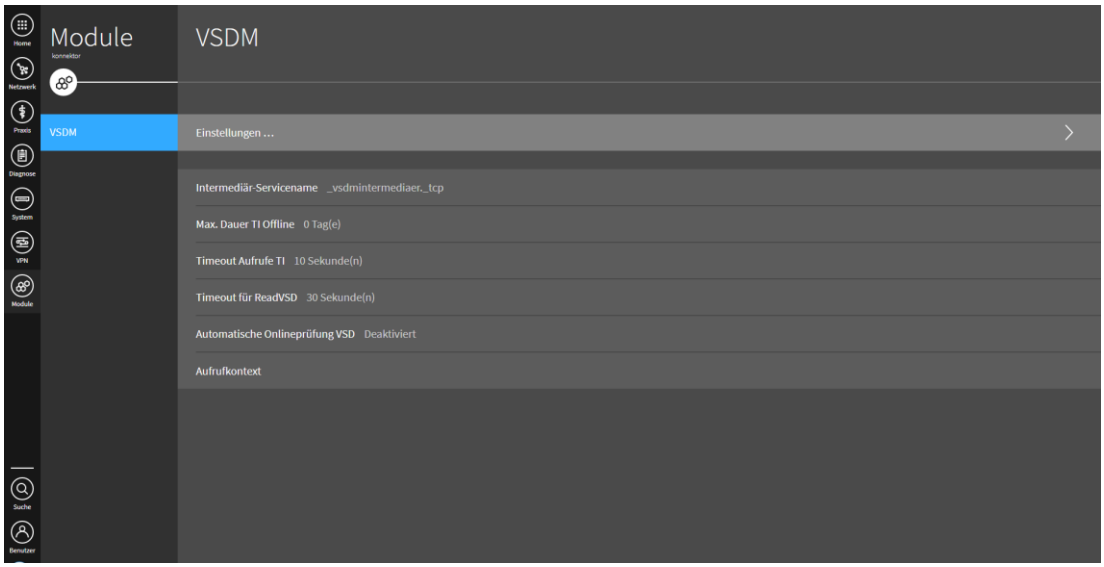


Abbildung 31: Menü „Module“

9.7.1 Das Fachmodul VSDM

Das Fachmodul VSDM ermöglicht den Abgleich der 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.

9.7.2 Hinweise zum Fachmodul NFDM

Das Fachmodul VSDM ermöglicht es dem PS, über den Modularen Konnektor auf eine eGK zuzugreifen um Informationen für die Notfallversorgung zu speichern.

Die Bedienung ist der Security Guidance Fachmodul NFDM beschrieben (siehe Anhang 16.14).

Der Modulare Konnektor setzt die Signaturrichtlinie [gemRL_QES_NFDM] um. Die signierten/zu signierenden Daten sind in der Signaturrichtlinie [gemRL_QES_NFDM] festgelegt.

9.7.3 Hinweise zum Fachmodul eMP/AMTS

Das Fachmodul eMP/AMTS ermöglicht es Clientsystemen, einen eMP und AMTS-relevante Daten auf der eGK zu speichern.

Die Bedienung ist der Security Guidance Fachmodul AMTS beschrieben (siehe Anhang 16.15).

9.7.4 Bereich Lizenz

In diesem Bereich wird der Status der lizenzierbaren Funktionalitäten angezeigt (siehe Kapitel 11.10).

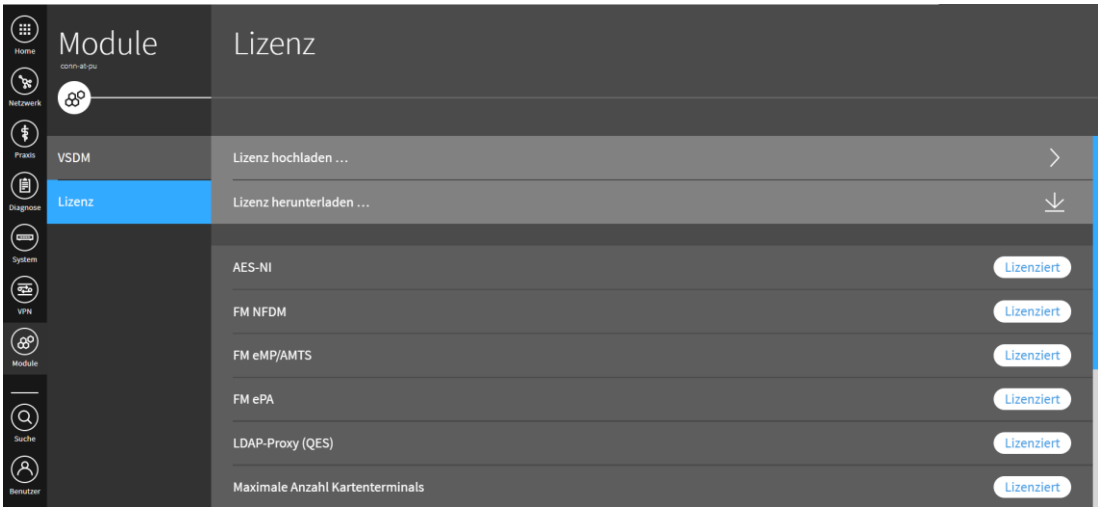


Abbildung 32: Bereich „Lizenz“

- Mit **Lizenz herunterladen …** können Sie die aktuelle Lizenzdatei lokal speichern.
- Mit **Lizenz hochladen …** können Sie eine Lizenzdatei auf den Modularen Konnektor hochladen. Änderungen der lizenzierten Funktionalitäten erfordern den Neustart des Modularen Konnektors.

10 Den Modularen Konnektor für die Einsatzumgebung konfigurieren

10.1 Kartenterminals anbinden und benutzen

Es dürfen nur zugelassene, zertifizierte Kartenterminals verwendet werden.

10.1.1 Kartenterminal verbinden (Pairing)

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

Vor jedem Pairing-Prozess ist das Gehäuse des Kartenterminals auf Unversehrtheit zu überprüfen. Sollten darüber hinaus Unregelmäßigkeiten beim Kartenterminal auffallen, so ist ebenfalls das Gehäuse des Kartenterminals auf Unversehrtheit zu überprüfen.

Das Pairing kann nur durchgeführt werden, wenn im Konnektor eine gültige TSL und CRL vorliegt. Aktualisieren Sie diese ggf. vorher (siehe Kapitel 11.2).

- 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. Beachten Sie dass beim manuellen Hinzufügen eines Kartenterminals das Feld zur Angabe einer

Portnummer leer sein muss. Der Konnektor verwendet automatisch die spezifizierten Ports.

- Klicken Sie das neu hinzugefügte Kartenterminal an, um weitere Optionen anzuzeigen.
- Klicken Sie bei Bedarf **Bearbeiten …** und geben Sie Benutzername und Passwort des Administrationszugangs ein, um im Modularen Konnektor Updates für das Kartenterminal durchführen zu können (siehe Kapitel 11.11).

  Die Zugangsdaten werden im Terminal selbst verwaltet. Optional können Sie die Eingabe über die Option **Administrator validieren** überprüfen.
- 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**.

Wenn das Pairing durch einen Remote-Administrator durchgeführt wird, erfordert dies zusätzlich die Anwesenheit eines autorisierten Personals vor Ort (z.B. durch Praxispersonal oder den Leistungserbringer), um den Vergleich des Fingerprints und die Bestätigung des Pairings am Kartenterminal durchzuführen.

- 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.

10.1.2 Kartenterminal zuordnen

Nach dem Pairing sind folgende Zuordnungen des Kartenterminals erforderlich:

- Einem Arbeitsplatz (siehe Kapitel 9.3.3.1)
- Mindestens einem Mandanten (siehe Kapitel 9.3.5)

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 Karten-

terminal. 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 10.2.7 beschrieben.

- Klicken Sie dazu im Bereich **Arbeitsplätze** einen Arbeitsplatz an, um ihm lokale und entfernte Kartenterminals zuzuweisen.
  - Unter **Lokale Terminals zuweisen / entfernen …** verwalten Sie lokale Kartenterminals, die sich am Arbeitsplatz befinden.
  - Unter **Entfernte Terminals zuweisen / entfernen …** verwalten Sie entfernte Kartenterminals.

    Um ein Kartenterminal als Remote-Kartenterminal zu verwenden, weisen Sie es dem Arbeitsplatz, an dem es sich befindet, als lokales Kartenterminal zu.

    Weisen sie es anschließend dem Mandanten mit der **Einstellung Kartenterminals zuweisen …** zu und wählen Sie es unter **Remote-Pin Kartenterminal hinzufügen …** als entferntes Kartenterminal aus.

10.1.3 Verbindung zu Kartenterminal wiederherstellen

Prüfen Sie vor der Wiederherstellung der Verbindung das Gehäuse des Kartenterminals auf Unversehrtheit.

Wenn im laufenden Betrieb die Verbindung zu einem Kartenterminal abbricht, gehen Sie wie folgt vor:

- Schalten Sie das Kartenterminal aus.
- Warten Sie mindestens 10 Sekunden.
- Schalten Sie das Kartenterminal wieder ein.

  Nach der Startphase verbindet sich das Kartenterminal neu.

10.1.4 Verwendung einer Karte nach Änderung der PIN

Wenn eine Karte nach der Änderung der PIN nicht verwendet werden kann, muss diese im Kartenterminal neu gesteckt und freigeschaltet werden.

10.1.5 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 im Menü **Praxis** aus der Liste der Kartenterminals (siehe Kapitel 9.3).

10.2 Netzwerkszenarien

10.2.1 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 10.2.1.1)

- Anbindungsmodus (siehe Kapitel 10.2.1.2)

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

- Internetmodus (siehe Kapitel 10.2.1.3)

  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 10.2.1.4)
- Art der Administration (Lokal oder Remote, siehe Kapitel 10.2.1.5)

10.2.1.1 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 9.5.3).

10.2.1.2 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).

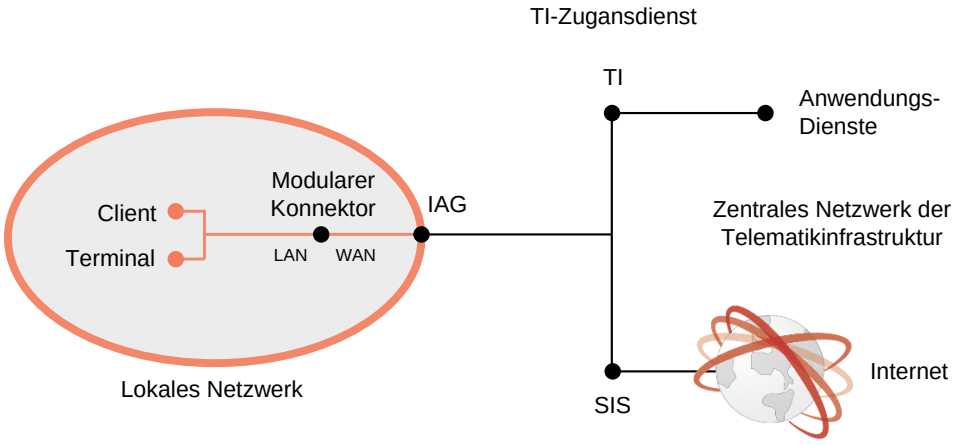


Abbildung 33: Anbindungsmodus In Reihe

- **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 7.1).

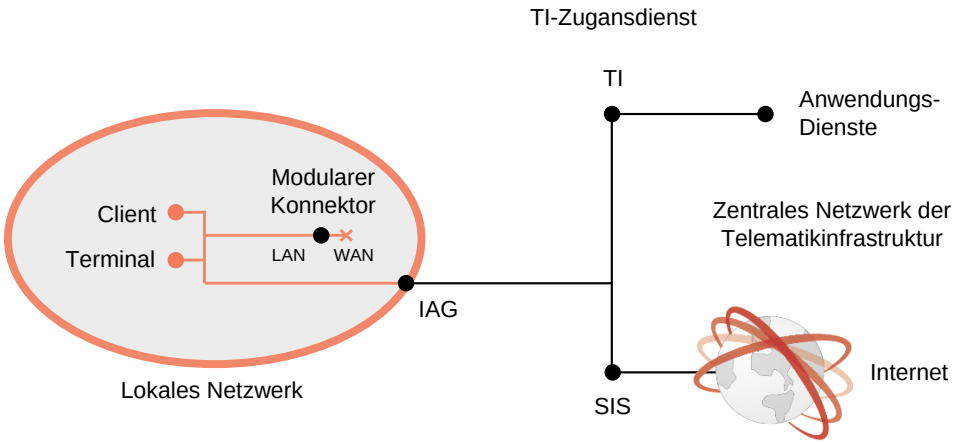


Abbildung 34: Anbindungsmodus Parallel

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 10.2.5 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

10.2.1.3 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 8: Internetmodus

10.2.1.4 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.

10.2.1.5 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 11.7.2). 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.

10.2.2 Hinweise zur Netzsegmentierung

Wenn der Modulare Konnektor im lokalen Netzwerk als Router eingesetzt wird, müssen bei Verwendung von Netzsegmenten die Netzwerkeinstellungen entsprechend konfiguriert werden (siehe Kapitel 9.2.1):

- Wählen Sie für die Einstellung **Intranet Routing Modus** die Option REDIRECT.
- Legen Sie unter **Intranet Routen** Routing-Einträge an, um die Erreichbarkeit der entfernten Netzsegmente aus dem lokalen Netzwerk sicherzustellen.
- Tragen Sie unter **Netzwerke der Einsatzumgebung** alle Netzsegmente ein, aus denen heraus Zugriff auf den Modularen Konnektor erforderlich ist.

10.2.3 Szenario 1: Keine bestehende Infrastruktur, keine speziellen Anforderungen

10.2.3.1 Beschreibung

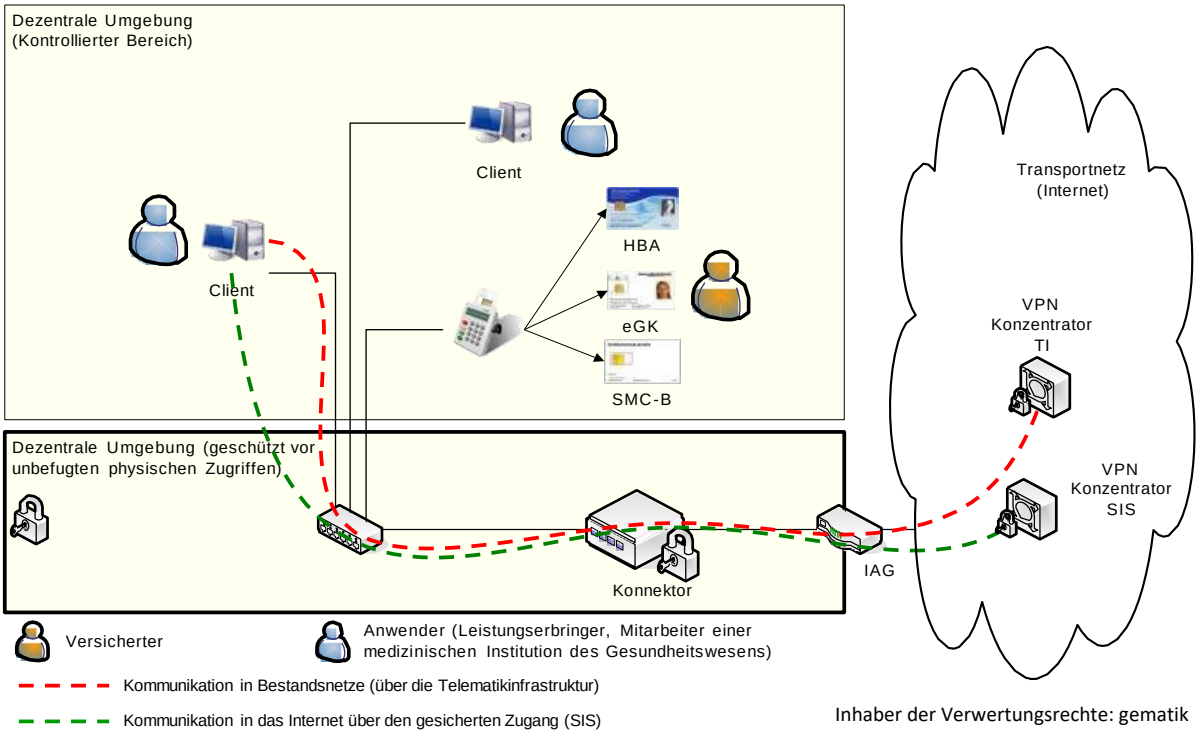


Abbildung 35: Szenario einer einfachen Installation

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.

10.2.3.2 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 ist verfügbar.
- Der Kartenleser befindet sich in einem kontrollierten Bereich, der vom Praxispersonal überwacht wird.

10.2.3.3 Vorgehensweise

So richten Sie dieses Szenario ein:

1. Konfigurieren Sie den Modularen Konnektor in den Clientsystemen als Default-Gateway.
2. Konfigurieren Sie die LAN-Schnittstelle entsprechend der lokalen Netzwerkumgebung und die WAN-Schnittstelle für die Verbindung mit dem IAG (siehe Kapitel 9.2).

   Die notwendigen Einstellungen für die WAN-Schnittstelle erhalten Sie vom Internet Service Provider (ISP).
3. Legen Sie die erforderlichen Mandanten, Clientsysteme und einen Arbeitsplatz mit zugewiesenem Kartenterminal an (siehe Kapitel 9.3).

- Richten Sie die Verbindung zum VPN-Zugangsdienst ein (siehe Kapitel 9.6).
- Führen Sie die Freischaltung des Modularen Konnektors durch und aktivieren Sie die Verbindungen mit TI und SIS (siehe Kapitel 9.6.1).

10.2.3.4 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.

10.2.4 Szenario 2: Mehrere Behandlungsräume

10.2.4.1 Beschreibung

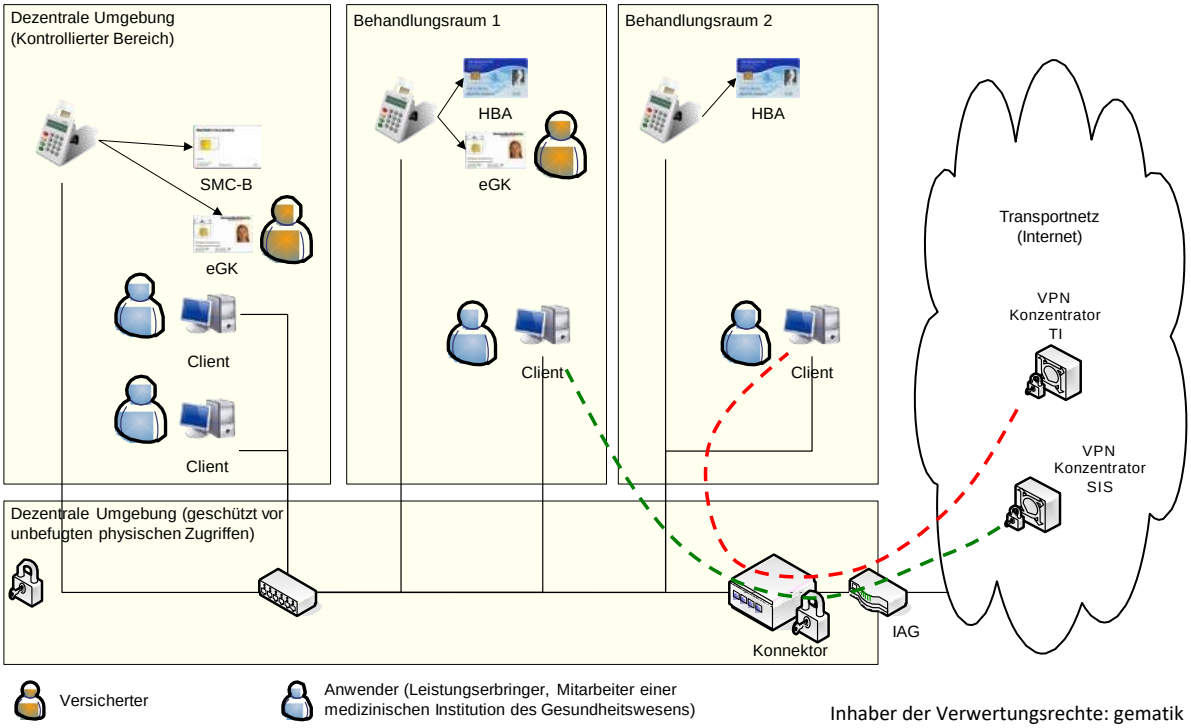


Abbildung 36: Szenario einer Installation mit mehreren Behandlungsräumen

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.

10.2.4.2 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.

10.2.4.3 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 9.3). 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 9.2).

  Die notwendigen Einstellungen für die WAN-Schnittstelle erhalten Sie vom ISP.
- ▶ Richten Sie die Verbindung zum VPN-Zugangsdienst ein (siehe Kapitel 9.6).
- ▶ Führen Sie die Freischaltung des Modularen Konnektors durch und aktivieren Sie die Verbindungen mit TI und SIS (siehe Kapitel 9.6.1).

10.2.4.4 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.

10.2.5 Szenario 3: Bestehende Infrastruktur ohne Netzsegmentierung

10.2.5.1 Beschreibung

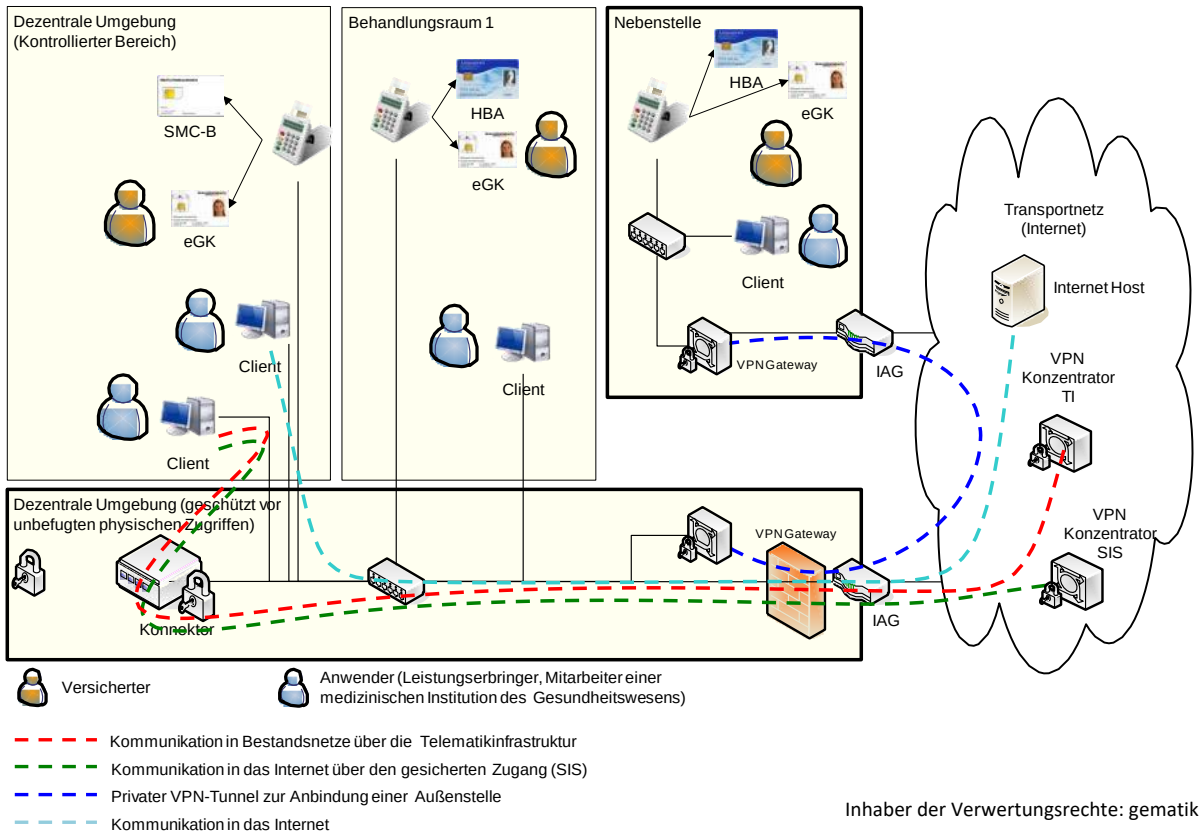


Abbildung 37: Szenario einer Integration in eine bestehende Infrastruktur

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 *Parallel* genutzt (siehe Kapitel 10.2.1.2).

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.

10.2.5.2 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 7.1).
- Eine SMC-B und mehrere Kartenterminals sind verfügbar.

10.2.5.3 Vorgehensweise

So richten Sie dieses Szenario ein:

- Legen Sie die erforderlichen Mandanten und bestehenden Systeme des bestehenden Netzwerks an (siehe Kapitel 9.3).
- Konfigurieren Sie die Netzwerkeinstellungen (siehe Kapitel 9.2):
  - 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 9.6).
- Führen Sie die Freischaltung des Modularen Konnektors durch und aktivieren Sie die Verbindungen mit TI und gegebenenfalls SIS (siehe Kapitel 9.6.1).

10.2.5.4 Ergebnis

Nach der Installation sind folgende Ergebnisse erreicht:

- Die Produkte der Telematik sind mit geringstmöglichem Änderungsaufwand in die bestehende Netzwerk-Infrastruktur integriert. Bestehende Kommunikations-wege 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.

10.2.6 Szenario 4: Bestehende Infrastruktur mit Netzsegmentierung

10.2.6.1 Beschreibung des Szenarios

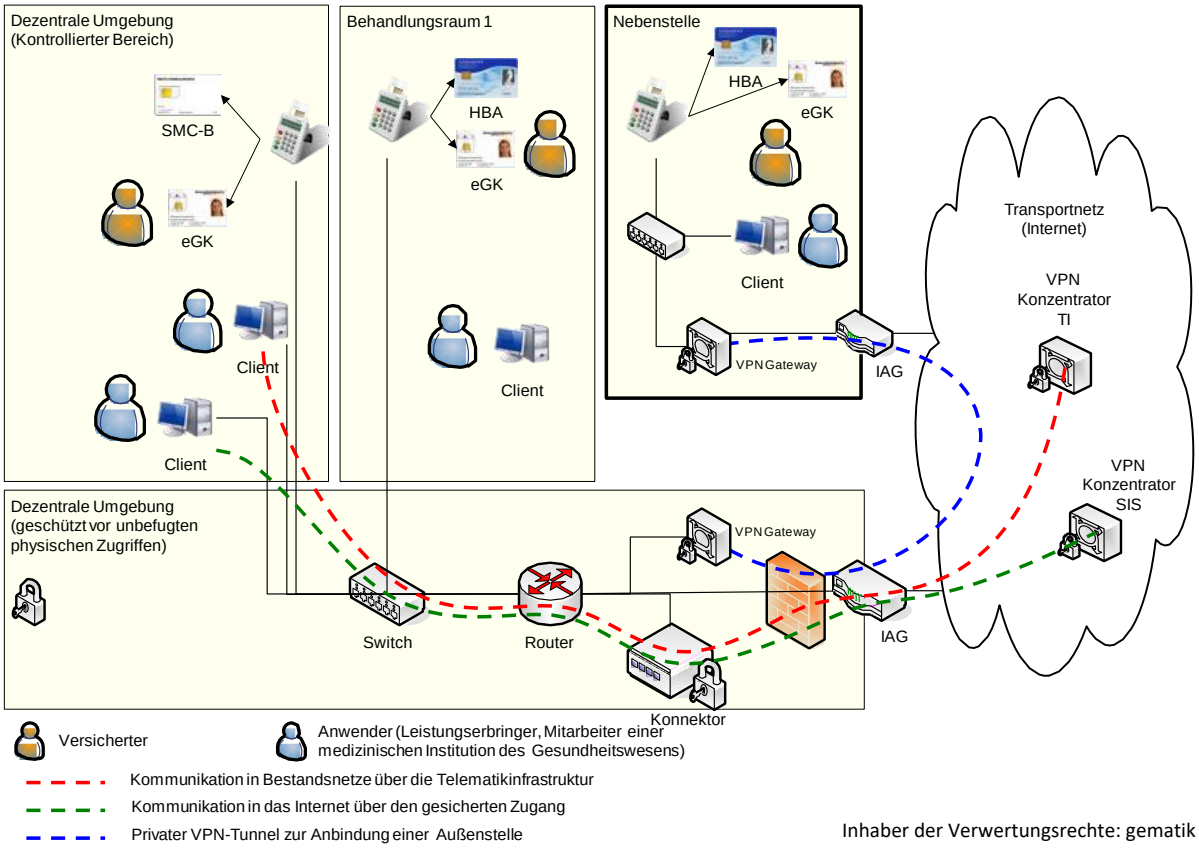


Abbildung 38: Szenario einer Integration in eine bestehende Infrastruktur mit existierendem Router

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 10.2.1.2).

10.2.6.2 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 7.1).
- Eine SMC-B und mehrere Kartenterminals sind verfügbar.
- Die Netzwerkverbindung zur Nebenstelle ist im bestehenden Router mit entsprechenden Routing-Einträgen eingerichtet.

10.2.6.3 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 9.3).

▶ Konfigurieren Sie die Netzwerkeinstellungen (siehe Kapitel 9.2):

- 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 9.6).

▶ Führen Sie die Freischaltung des Modularen Konnektors durch und aktivieren Sie die Verbindungen mit TI und gegebenenfalls SIS (siehe Kapitel 9.6.1).

10.2.6.4 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.

10.2.7 Szenario 5: Zentrale Verwendung des Heilberufsausweises

10.2.7.1 Beschreibung

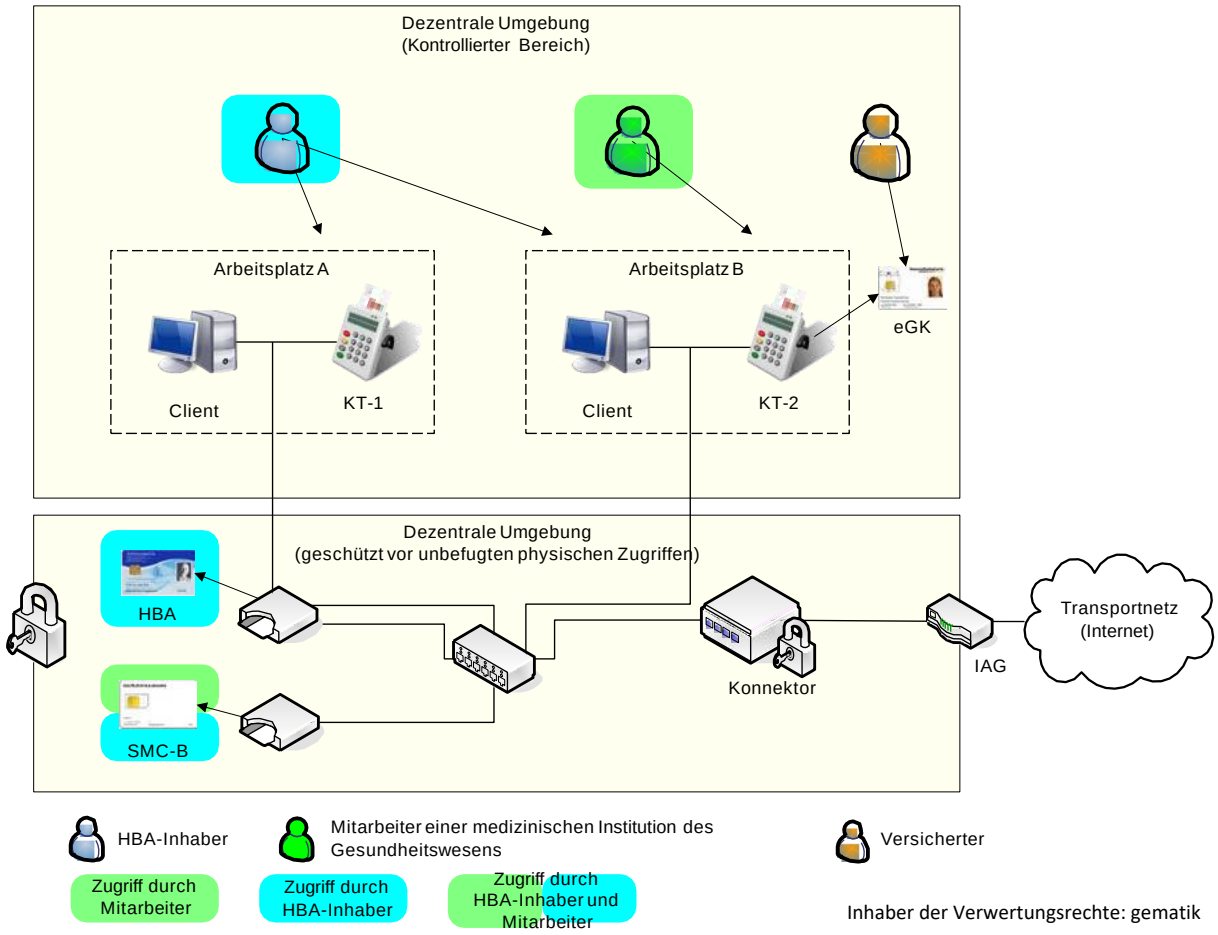


Abbildung 39: Szenario mit zentral gesteckten HBA und SMC-B

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.

10.2.7.2 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 9.3.3.1).

  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 9.3.5):

  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.

10.2.7.3 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.

10.2.8 Szenario 6: Zentrales Primärsystem als Clientsystem

10.2.8.1 Beschreibung

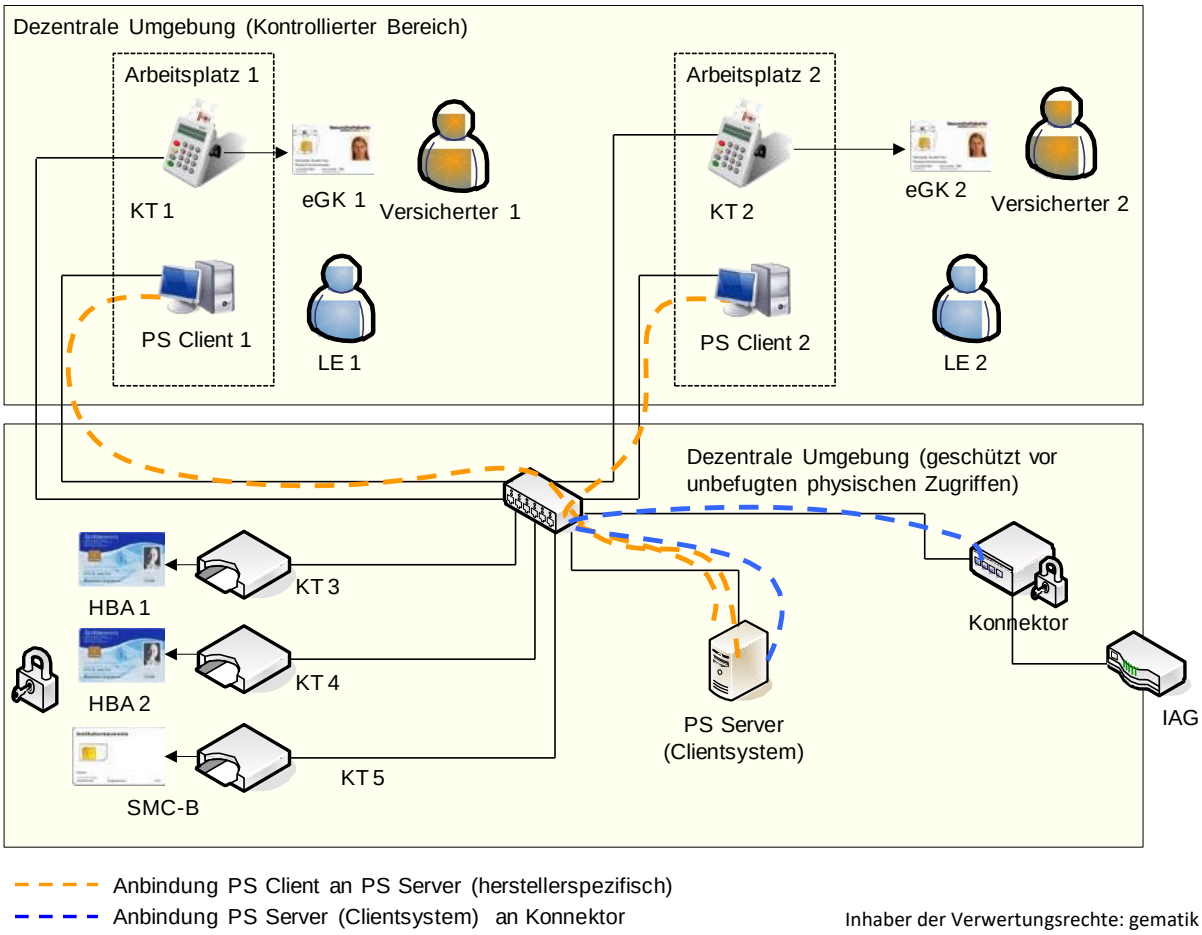


Abbildung 40: Szenario mit zentralem Primärsystem als Clientsystem

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.

10.2.8.2 Voraussetzung

Folgende Voraussetzungen müssen erfüllt sein:

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

10.2.8.3 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 9.3).
- Verbinden Sie den *PS Server* ggf. über TLS (siehe Kapitel 11).
- Führen Sie das Pairing der Kartenterminals durch (siehe Kapitel 10.1.1).

10.2.8.4 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.

10.2.9 Szenario 7: Gemeinschaftspraxis mit mehreren Mandanten

10.2.9.1 Beschreibung

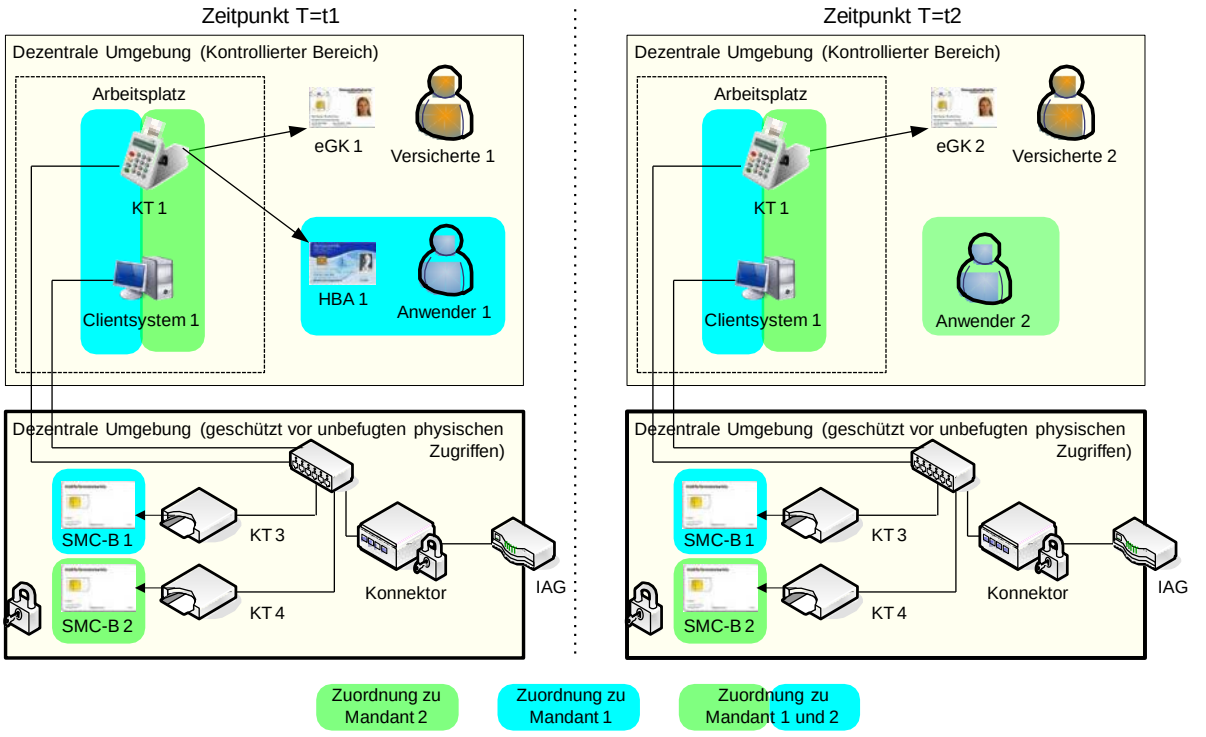


Abbildung 41: Szenario für den Zugriff

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.

10.2.9.2 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.

10.2.9.3 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 9.3):
  - 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 10.1.1).

10.2.9.4 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.

11 Den Modularen Konnektor administrieren

11.1 Hinweise zur Fehlersuche

Wenn die Betriebsanzeige "Service" blinkt (siehe Kapitel 4.4), gehen Sie wie folgt vor:

- Prüfen Sie die vorliegenden Fehlermeldungen (siehe Kapitel 9.4.2).
- Prüfen Sie, ob die TSL und CRL noch gültig sind (siehe Kapitel 9.5.2) und laden Sie diese ggf. manuell hoch (siehe Kapitel 11.2).
- Wenn der Modulare Konnektor hinter einer Firewall betrieben wird, prüfen Sie, ob die Anforderungen an die freigegebenen Ports/Protokolle erfüllt sind (siehe Kapitel 7.2)

Wenn eine Verbindung zur TI besteht, ist noch nicht die Funktion der TI-Dienste gewährleistet.

11.2 Erreichbarkeit/Funktion der TI-Dienste prüfen

Wenn eine funktionierende Verbindung zur TI besteht, ist noch nicht garantiert, dass die einzelnen Dienste fehlerfrei arbeiten. Sie können wie nachfolgend beschrieben einzelne Dienste auf ihre Funktion prüfen. Wenn alle oder einzelne Dienste trotz einer bestehenden Verbindung zur TI nicht verfügbar sind, deutet dies auf ein Problem des Zugangsdienstes hin.

OCSP-Forwarder

- Klicken Sie im Menü **System** > **Zertifikate** im Bereich **OCSP-Forwarder** auf **Erreichbarkeit der OCSP-Forwarder prüfen …**

  Bei erfolgreicher Prüfung wird angezeigt, dass ein OCSP-Forwarder erreichbar war. Im Fehlerfall wird eine Fehlermeldung angezeigt.

TSL-Aktualisierung

- Klicken Sie im Menü **System** > **Zertifikate** auf **TSL aktualisieren**.

  Bei korrekter Funktion wird angezeigt, dass die TSL, je nachdem ob eine Aktualisierung vorliegt, aktualisiert oder nicht aktualisiert wurde. Im Fehlerfall wird eine Fehlermeldung angezeigt.

Zeit-Synchronisation

- Klicken Sie im Menü **System** > **Zeit** auf **Zeitsynchronisierung auslösen**.

  Bei korrekter Funktion wird die Systemzeit ohne weitere Rückmeldung synchronisiert. Im Fehlerfall wird eine Fehlermeldung angezeigt.

KSR (Konfigurations- und Software-Repository)

- Klicken Sie im Menü **System** > **Aktualisierungen** auf **Aktualisierungsinformationen aktualisieren**.

  Wenn der Dienst für die Bereitstellung von Aktualisierungen für den Modularen Konnektor erreichbar ist und korrekt funktioniert, werden Datum und Zeit der erfolgreichen Prüfung angezeigt. Im Fehlerfall wird eine Fehlermeldung angezeigt.

11.3 TSL und CRL manuell hochladen

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.

- Deaktivieren Sie dazu vorübergehend den Leistungsumfang Online (siehe Kapitel 9.2.1).

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

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

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

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

11.3.1 Import aktueller TSL nach Wechsel des TSL-Vertrauensankers

Wenn der Modulare Konnektor über einen längeren Zeitraum nur offline betrieben wird, kann der Zustand eintreten, dass die installierte Trust-Service Status List (TSL) abgelaufen ist. Gleichzeitig besteht die Möglichkeit, dass in diesem Zeitraum auch

ein oder mehrere Wechsel des TSL-Vertrauensankers vollzogen wurden. In diesem Fall würde ein manueller Import der aktuellen TSL fehlschlagen.

Um die aktuelle TSL importieren zu können, gehen Sie wie folgt vor:

- Spielen Sie alle TSL ein, bei denen ein Wechsel des Vertrauensankers erfolgt ist (siehe Kapitel 9.5.2). Spielen Sie dabei die TSL in zeitlichen aufsteigender Abfolge ein, beginnend mit der ältesten TSL.

Weiterführende Supportinformationen werden im Bedarfsfall über die Wissensdatenbank bereitgestellt.

11.4 TLS-Zertifikate für Clientsysteme verwalten

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

11.4.1 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 9.3.3).
- 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 7.4.4 beschrieben.

11.4.2 TLS-Zertifikat in den Modularen Konnektor importieren

Diese Funktion darf nur dazu verwendet werden, um nach einem vollständigen 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.

11.5 Hostname ändern

- Den Hostnamen des Modularen Konnektors können Sie im Menü **System** im Bereich **Allgemein** ändern (siehe Kapitel 9.5.1).

Nach einer Änderung des Hostnamens ist der Neustart des Modularen Konnektors erforderlich. Dabei wird ein neues Zertifikat mit neuem Gültigkeitszeitraum generiert. Dieses Zertifikat muss für die Benutzung der Administrationsschnittstelle erneut validiert werden, die Vorgehensweise ist analog zur Erstanmeldung (siehe Kapitel 7.4).

Vor der Validierung des nach der Änderung des Hostnamens neu generierten Konnektor-Zertifikates dürfen keine Zugangsdaten an der Administrationsschnittstelle eingegeben werden.

- Rufen Sie zum Validieren des neuen Zertifikats die Bedienoberfläche des Modularen Konnektors auf.

  Der Browser zeigt eine Warnmeldung mit dem Hinweis **Dies ist keine sichere Verbindung** an.

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

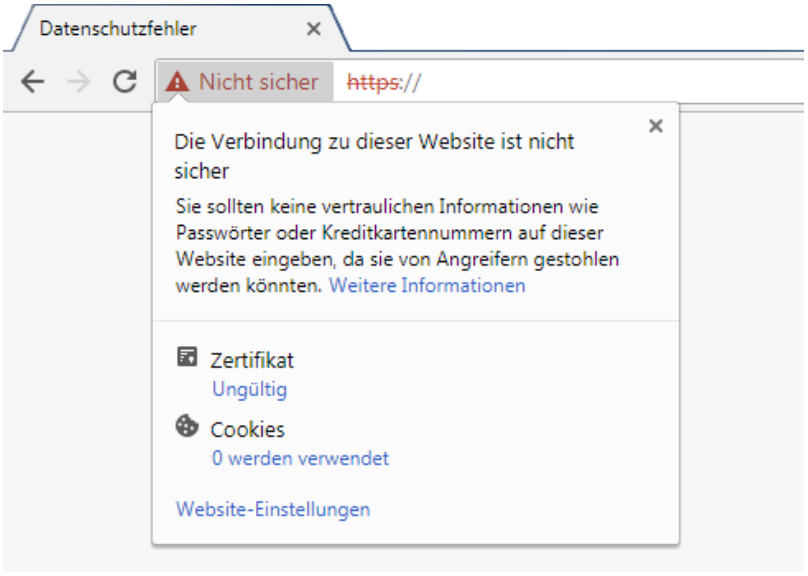


Abbildung 42: Informationen zu unsicherer Verbindung

- Klicken Sie unter **Zertifikat** auf **Ungültig**, um weitere Informationen zum neuen Zertifikat und dessen Gültigkeitszeitraum anzuzeigen.

In folgendem Beispiel wurde der Hostnamen am 16.09.2019 auf „conn-at-pu“ geändert:

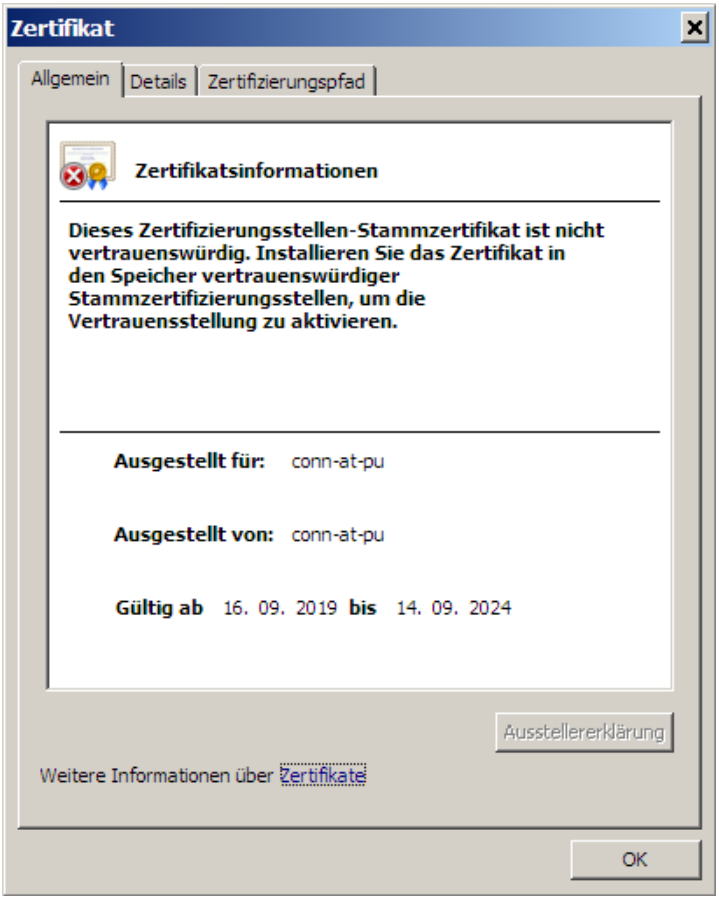


Abbildung 43: Zertifikatsinformationen

- Gehen Sie wie in Kapitel 7.4.3 und 7.4.4 beschrieben vor, um das neue Zertifikat zu validieren.

11.6 Selbst-Test durchführen

Im Menü **Diagnose** können Sie im Bereich **Status** mit **Selbst-Test …** eine Prüfung der Integrität sicherheitsrelevanter Komponenten anstoßen (siehe Kapitel 2.2.11).

Anschließend werden die Ergebnisse der einzelnen Prüfvorgänge angezeigt. Im Falle eines Fehlschlags fährt der Modulare Konnektor nach 60 Sekunden herunter.

11.7 Werksreset durchführen

Mit den verschiedenen Arten von Werksreset können bestimmte oder alle Parameter des Modularen Konnektors in den Auslieferungszustand zurückversetzt werden.

	Konfigurationsdaten	Netzwerkeinstellungen	Benutzerkonten
Vollständiger Werksreset (siehe Kapitel 11.7.1)	x	x	x
Werksreset für Fail Safe (siehe Kapitel 11.7.2)	-	x*	-
Werksreset der Benutzerkonten (siehe Kapitel 11.7.3)	-	-	x

* Es erfolgt zusätzlich die Zuweisung einer festen IP-Adresse

Tabelle 9: Werksreset – Übersicht

11.7.1 Vollständiger Werksreset

Bitte lesen Sie vor Durchführung des vollständigen Werksreset das Kapitel 15 durch.

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

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

Nach dem vollständigen Werksreset befindet sich das Gerät im Auslieferungszustand, die Anmeldung erfolgt analog der Erstanmeldung (siehe Kapitel 7.4). Beachten Sie bei Client-Authentisierung per Zertifikat die Hinweise zur Client-Authentisierung nach einem Werksreset (siehe Kapitel 9.3.3).

Wenn der vollständige Werksreset nicht erfolgreich abgeschlossen werden kann, wiederholen Sie diesen. Wenn auch dann der vollständige Werksreset nicht erfolgreich abgeschlossen werden kann, muss eine dauerhafte Außerbetriebnahme des Gerätes erfolgen (siehe Kapitel 15).

11.7.1.1 Vollständiger Werksreset über die Bedienoberfläche

Der vollständige Werksreset wird über das Menü **System** im Bereich **Allgemein** durchgeführt (siehe Kapitel 9.5.1).

Der erfolgreiche Abschluss des vollständigen 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 4.5.

11.7.1.2 Vollständiger Werksreset über die REST-Schnittstelle

Falls Sie sich nicht mehr an der Bedienoberfläche anmelden können, weil diese nicht mehr erreichbar ist, kann ein vollständiger 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.

Am Gehäuse befindet sich ein gegen unbeabsichtigte Auslösung gesicherter Reset-Taster (siehe Anhang 16.4).

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 vollständiger Werksreset über die REST-Schnittstelle beginnt, leuchten alle Anzeigen am Gerät auf. Es werden nun an der LAN Schnittstelle die für den vollständigen Werksreset über die REST-Schnittstelle notwendigen 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 7.3). 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 vollständige Werksreset über die REST-Schnittstelle 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 vollständigen 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 4.5.

11.7.2 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 (192.168.210.1/24) 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 15).

Der Werksreset für Fail Safe ist nur für den Fall einzusetzen, dass sich der Konnektor in einem undefinierten Zustand befindet und in einem definierten Zustand gestartet werden soll. Für andere Szenarien, z.B. um eine feste IP-Adresse des Konnektors zu erhalten oder bei vergessenem Passwort, ist der Werksreset für Fail Safe nicht zu verwenden.

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 9.5.5.

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 4.5).
- Halten Sie den Reset-Taster (siehe Anhang 16.4) mit einem geeigneten Gegenstand (z.B. Draht) gedrückt.
- Schalten Sie den Modularen Konnektor ein (siehe Kapitel 4.5) 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).

11.7.3 Werksreset der Benutzerkonten

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

Beim Werksreset der Benutzerkonten werden alle Benutzerkonten zurückgesetzt. Benutzen Sie für die anschließende Anmeldung die initialen Zugangsdaten (siehe Kapitel 7.4) 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 (siehe Anhang 16.4) mit einem geeigneten Gegenstand (z.B. Draht) 5 Sekunden lang gedrückt.

  Sobald der Werksreset der Benutzerkonten 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 7.2). 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 vollständigen Werksreset über das Menü **System** im Bereich **Allgemein** durchführen (siehe Kapitel 9.5.1).

11.8 Sperrung für den Versand

Der Modulare Konnektor darf nur versendet werden, wenn zuvor sie Sperrung für den Versand erfolgreich abgeschlossen wurde.

Bitte lesen Sie sich vor Durchführung der Sperrung für den Versand das Kapitel 15 (Dauerhafte Außerbetriebnahme) durch.

Mit der Sperrung für den Versand wird ein notwendiges Geheimnis, das zum Entschlüsseln der Daten des kryptografisch gesicherten Speichers (siehe Kapitel 2.2.7) notwendig ist, überschrieben. Nach erfolgreichem Abschluss der Sperrung für den 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.

Die Sperrung für den Versand führt unwiderruflich dazu, dass der Modulare Konnektor nicht mehr funktionsfähig ist.

Wenn die Sperrung für den Versand nicht erfolgreich abgeschlossen werden kann, wiederholen Sie diese. Wenn auch dann die Sperrung für den Versand nicht erfolgreich abgeschlossen werden kann, muss die dauerhafte Außerbetriebnahme des Gerätes erfolgen (siehe Kapitel 15).

11.8.1 Sperrung für den Versand durchführen

- Führen Sie die Sperrung für den Versand über das Menü **System** im Bereich **Allgemein** durch (siehe Kapitel 9.5.1).

Der erfolgreiche Abschluss der Sperrung für den Versand wird durch die Betriebsanzeigen (LEDs) am Gerät angezeigt (siehe Tabelle 3).

11.9 Backups erstellen und einspielen

Systemsicherungen (Backups) verwalten Sie im Menü **System** im Bereich **Backups**.

Es wird empfohlen, Systemsicherungen zur einfachen Identifizierung eindeutig zu kennzeichnen, beispielsweise durch eine physische Beschriftung des Datenträgers.

11.9.1 Backup 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 (sogenanntes Backup-Passwort).

Das Backup-Passwort muss mindestens 20 Zeichen lang sein und Zeichen aus den folgenden vier Zeichenarten enthalten:

- Großbuchstaben (`ABCDEFGHIJKLMNOPQRSTUVWXYZÄÖÜ`)
- Kleinbuchstaben (`abcdefghijklmnopqrstuvwxyzäöü`)
- Sonderzeichen (`ß#?!@$%^&*-`)
- Ziffern (`1234567890`)

Beachten Sie die Sicherheitshinweise zum Backup-Passwort:

Das Backup-Passwort darf nicht schriftlich aufbewahrt und nicht an Dritte weitergegeben werden. Werden die oben genannten Vorgaben zur Festlegung des Backup-Passworts nicht beachtet, besteht die Gefahr, dass kein geeigneter Schutz der verschlüsselten Daten gewährleistet ist. Zudem müssen die Passwörter zufällig und für jedes Backup unterschiedlich und unabhängig voneinander gewählt werden.

Die Backup-Datei wird 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.

11.9.2 Backup importieren

Backups können nur zwischen Geräten mit gleichem Umfang der lizenzierten Funktionen ausgetauscht werden.

Achten Sie bei der Wiederherstellung einer Konfiguration aus einem Backup auf die Kompatibilität mit der aktuell verwendeten Softwareversion. Stellen Sie dazu den Ursprung der wiederherzustellenden Konfiguration sicher, z. B. die Versionierung der Konfiguration.

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.

Zur Aktivierung der eingelesenen Konfigurationswerte ist nach dem Import ein Neustart des Modularen Konnektors durchzuführen.

Bitte prüfen Sie nach dem Neustart über die grafische Bedienoberfläche zunächst, ob die gewünschte Konfiguration importiert wurde. Eine fehlerhafte Konfiguration stellt ein mögliches Sicherheitsrisiko dar. Änderungen an der Konfiguration können über die grafische Bedienoberfläche erfolgen (siehe Kapitel 9).

11.10 Lizenzen verwalten

Die Lizenzierung von Funktionalitäten wird mit dem eHealth Konnektor (Produkttypversion PTV3) eingeführt. Eine Lizenzierung erfolgt individuell für einen Konnektor, identifiziert anhand seiner Seriennummer.

Der Umfang der zu lizenzierenden Funktionen wird vom Hersteller je Release definiert.

Um die lizenzierten Funktionalitäten bei einem Rechenzentrumskonnektor mit beiden Konnektoreinheiten verwenden zu können, muss die Lizenz auf beiden Einheiten eingespielt werden. Die Lizenz eines RZ-Konnektors ist wie beim Einbox-Konnektor nur an die Seriennummer des Gesamtgerätes gebunden.

Die Lizenzinformationen des Modularen Konnektors sind in einer Lizenzdatei gespeichert. Diese ist an das Gerät gebunden (Bindung an die Seriennummer) und wird von einem Werksreset nicht zurückgesetzt.

Bei einer Systemsicherung zum Zweck des Transfers zwischen verschiedenen Geräten wird die Lizenzdatei nicht mit übertragen.

- Lizenzdateien können im Menü **Module** im Bereich **Lizenz** hoch- oder heruntergeladen werden (siehe Kapitel 9.7.4).

  Die Möglichkeit zum Herunterladen einer Lizenz dient zur Sicherung der aktivierten Lizenzen.

11.10.1 Lizenzierbare Funktionen

Folgende Funktionen können einzeln lizenziert werden:

- SIGNSERVICE

  QES und nonQES

  Funktion wird als Standard für alle Konnektoren (keine Bindung an die Seriennummer) lizenziert

- LDAP für KIM

  Funktion wird als Standard für alle Konnektoren (keine Bindung an die Seriennummer) lizenziert

- ENSERVICE

  Ver-/Entschlüsselung

  Funktion wird als Standard für alle Konnektoren (keine Bindung an die Seriennummer) lizenziert

- AES-NI

  Funktion wird als Standard für alle Konnektoren (keine Bindung an die Seriennummer) lizenziert.

  Die Aktivierung/Deaktivierung erfolgt über die Bedienoberfläche (siehe Kapitel 9.5.1).

- BSNR

  Anzahl der Betriebsstätten (BSNR bzw. SMC-B); Defaultanzahl ist 10 SMC-Bs

- KTNR

  Anzahl der Kartenterminals

  Defaultanzahl der Kartenterminals ist 50 beim Einboxkonnektor und 100 beim Rechenzentrumskonnektor.

- Fachmodule für den eHealth Konnektor (PTV3)

  Die Lizenzierung der nachfolgend aufgeführten Fachmodule erfolgt zusammenhängend; eine separate Lizenzierung ist nicht möglich:

  - AMTS: Fachmodul eMP/AMTS
  - NFDM: Fachmodul NFDM (inkl. Signaturrichtlinie NFDM)

11.10.2 Lizenzfreie Verwendung

Zur lizenzfreien Verwendung sind die folgenden Funktionen verfügbar:

- QES/nonQES
- LDAP
- Ver-/Entschlüsselung
- AES-NI
- bis zu 10 SMC-Bs
- bis zu 50 KTs pro Konnektoreinheit (dies entspricht 50 KTs beim Einbox- und 100 KTs beim RZ-Konnektor)

11.11 Updates durchführen

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.

Mit dem Modularen Konnektor besteht die Möglichkeit sich per Event (CETP-Protokoll) über die Verfügbarkeit von Aktualisierungen für die Firmware des Modularen Konnektors informieren zu lassen. Die Möglichkeit zur Nutzung ist abhängig davon, ob das verwendete Primärsystem diese Funktion unterstützt. Beachten Sie dazu das Handbuch der eingesetzten Praxissoftware oder treten Sie direkt mit dem Hersteller in Kontakt.

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.

Beachten Sie die Sicherheitshinweise zur sicheren Administrierung in Kapitel 5.5. 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 9.5.2).

Vor der Durchführung eines Softwareupdates wird empfohlen, ein Backup der funktionierenden Konfiguration durchzuführen und eine Systemsicherung aufzubewahren (siehe Kapitel 11.9). Falls im Anschluss an das Update ein Rückfall auf die vorherige Softwareversion erforderlich ist, können Sie nach dem

Downgrade die vorherige Konfiguration durch Einspielen des Backups wieder herstellen.

Nach der Durchführung eines Updates muss der Administrator prüfen, ob die Installation der von ihm ausgewählten Version erfolgreich war. Dazu kann der Administrator die aktuelle Version des Modularen Konnektors über die Bedienoberfläche auslesen (siehe Kapitel 9.5.6).

Sobald dem Administrator bekannt wird, dass ein kryptografischer Algorithmus für die Verarbeitung von qualifizierten elektronischen Signaturen nicht mehr geeignet ist, muss er die Anwender darüber informieren und ein Update durchführen, sobald dieses verfügbar ist.

11.11.1 Übersicht

Der Konfigurationsdienst (KSR) der Telematikinfrastruktur (TI) stellt für den Modularen Konnektor sowie für Kartenterminals eine Schnittstelle für Softwareupdatepakete zur Verfügung. Als Notfallmaßnahme ist auch ein Offline-Update möglich, wenn keine Verbindung zum KSR aufgebaut werden kann.

Der Modulare Konnektor unterstützt dabei folgende Updateverfahren:

- Online-Update über den KSR (siehe Kapitel 11.11.2):
  - Update der Firmware-Gruppen Informationen des Konnektors
  - Update der Konnektorsoftware
  - Abruf und Übertragung von Updates an angeschlossene Kartenterminals
  - Abruf der Konfigurationsdaten zur Anbindung von Bestandsnetzen
- Offline-Update (siehe Kapitel 11.11.4):
  - Update der Konnektorsoftware

Bei der Aktualisierung bleiben die folgenden Einstellungen unverändert erhalten:

- Benutzer, Benutzerrollen und Passwörter
- Passwörter zur Erstellung bzw. Import eines Backups

Zur Nutzung erweiterter Funktionalitäten, die im Rahmen eines Updates bereitgestellt wurden, kann eine Lizenz erforderlich sein (siehe Kapitel 11.10).

11.11.2 Die Aktualisierung von Fachmodulen

Fachmodule sind ein Bestandteil der Konnektorsoftware und können nur durch ein Update des Modularen Konnektors aktualisiert werden.

Informationen über zugelassene Software- und Hardwareversionen erhalten Sie unter www.gematik.de (siehe auch die Versionshinweise auf Seite 16). Für einen von der gematik zugelassenen Modularen Konnektor können Sie die Version der installierbaren Fachmodule dem Security Target des Modularen Konnektors entnehmen, das Sie auf den Webseiten des BSI unter https://www.bsi.bund.de finden. Darüber hinaus kann die Version eines installierten Fachmoduls über die Bedienoberfläche angezeigt werden (siehe Kapitel 9.5.6).

11.11.3 Update online durchführen

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

11.11.3.1 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.

Für Kartenterminals müssen Benutzername und Passwort des Administrationszugangs konfiguriert sein, um im Modularen Konnektor Updates für das Kartenterminal durchführen zu können (siehe Kapitel 9.3.2).

11.11.3.2 Aktuelle Firmware-Version prüfen

- Öffnen Sie im Menü **System** den Bereich **Aktualisierungen**.
- Klicken Sie unter **Geräte** das gewünschte Gerät an.

  Unter **Aktuelle Firmware-Version** wird die derzeit verwendete Version der Firmware angezeigt.

11.11.3.3 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 und verfügbare Updates anzuzeigen.
- Laden Sie das Update herunter:
  - Falls das Update nicht bereits automatisch heruntergeladen wurde, wird es unter **Verfügbare Aktualisierungen** mit dem Status **Nicht heruntergeladen** aufgeführt; klicken Sie es an, um weitere Informationen anzuzeigen.

    Die zum Update gehörigen Releasenotes können sie im Bereich **Dokumentations-Dateien** herunterladen.

    Klicken Sie **Herunterladen …** , um das Update auf den Modularen Konnektor herunterzuladen.
  - Optional können verfügbare Updates automatisch heruntergeladen werden. Diese Funktion können Sie im Bereich **Aktualisierungen** unter **Einstellungen …** aktivieren.

  Das Update wird nach dem Herunterladen mit dem Status **Heruntergeladen** angezeigt. Falls nicht der korrekte Status angezeigt wird, drücken Sie die Taste **F5**, um die Anzeige des Browsers zu aktualisieren.

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

- Klicken Sie das Update an und wählen Sie **Aktualisierung einplanen/ändern**, um die Aktualisierung zu terminieren.

  Legen Sie dazu entweder unter **Zeitpunkt** eine bestimmte Zeit fest, oder wählen sie **Zuletzt**, um das Update automatisch durchzuführen, sobald alle anstehenden Updates für Kartenterminals abgeschlossen sind.

  Nach dem Update startet der Modulare Konnektor automatisch neu.

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

11.11.3.4 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 mit dem Status **Heruntergeladen** an.
- Klicken sie **Vom Konnektor löschen**, um das Update zu entfernen.

11.11.4 Update offline durchführen

Zur Durchführung des Offline-Updates ist eine direkte Netzwerkverbindung zwischen dem Modularen Konnektor und dem zu dessen Administration verwendeten Gerät erforderlich. Ein Offline-Update ist nicht über Remote Management möglich.

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

- Rufen Sie den zur Entschlüsselung des Updates erforderlichen Schlüssel bei Ihrem Vertragspartner für den VPN-Zugangsdienst ab.
- Laden Sie ein für die verwendete Geräteversion geeignetes Update von der Webseite des Herstellers herunter und speichern Sie es auf dem Clientsystem.

  Informationen über die Geräteversion erhalten Sie im Menü **System** (siehe Kapitel 9.5.6).

Bei Verwendung eines Apple Rechners oder Tablets zum Entpacken und Entschlüsseln des Offline-Updates kann die Entschlüsselung bei Verwendung der Standardanwendung des Betriebssystems fehlschlagen. Verwenden Sie in diesem Fall bitte alternative Softwarelösungen wie z.B. "The Unarchiver" oder "KeKa“, die für Apple Geräte angeboten werden.

- Entschlüsseln und Entpacken Sie das Update (AES256 verschlüsseltes ZIP-Archiv) auf dem Clientsystem.

- Verbinden Sie das Clientsystem mit der LAN-Schnittstelle des Modularen Konnektors.

Trennen Sie für den Zeitraum des Offline-Updates alle anderen LAN- und WAN-Verbindungen des Modularen Konnektors physisch.

- Melden Sie sich an der Bedienoberfläche des Modularen Konnektors an (siehe Kapitel 8.1)

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.

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

- Klicken Sie das Update an, um die Aktualisierung zu terminieren.

11.11.5 Hinweis zur Durchführung von Downgrades

<u>Warnung</u>

Bei einem als PTV3 (eHealth Konnektor) mit der Firmwareversion 3.5.0 oder neuer ausgelieferten Konnektor ist ein Downgrade auf PTV1 (VSDM Konnektor, Firmwareversion 2.0.x) zu vermeiden.

Wenn trotzdem ein Downgrade durchgeführt wird, kann es bei Durchführung eines vollständigen Werksresets (siehe Kapitel 11.7.1) vorkommen, dass der Konnektor bei nächsten Neustart einen Fehlerzustand signalisiert.

Wenn der Konnektor diesen Zustand anzeigt, kann durch die Durchführung eines Werksrests für FailSafe (siehe Kapitel 11.7.2) der Fehlerzustand aufgehoben werden. Es ist anschließend ein Neustart durchzuführen.

Hintergrundinformationen zu den Hinweisen:

Ein als PTV3 (Firmware 3.5.0 oder neuer) ausgelieferter Konnektor verwendet ein neueres Konfigurationsschema im Vergleich zum PTV1 Konnektor.

Wenn bei so einem Konnektor ein Downgrade auf PTV1 durchgeführt wird, verbleibt dieses neuere Konfigurationsschema als Defaultkonfiguration für den vollständigen Werksreset.

Wenn in dieser Situation der vollständige Werksreset durchgeführt wird, kann die nach dem Downgrade aktivierte PTV1-Software dieses neuere Konfigurationsschema nicht interpretieren. Erst mit einem zusätzlichen Werksreset für FailSafe wird die für PTV1 Firmware passenden Defaultkonfiguration hergestellt.

Vor der Durchführung eines Downgrades muss ein Neustart durchgeführt werden (siehe Kapitel 9.5.1), um den Modularen Konnektor in einen definierten Systemzustand zu versetzen. Ein Downgrade darf nur unmittelbar nach dem Neustart durchgeführt werden.

Die Auswahl und Durchführung von Downgrades ist in Kapitel 9.5.4 beschrieben.

11.11.6 Bei Anzeigefehlern nach einem Update

Sollte es nach einem Update zu Anzeigefehlern kommen, leeren Sie wie folgt den Browser-cache:

- Drücken Sie in Chrome die Tastenkombination **STRG** + **SHIFT** + **ENTF**.
  Ein Fenster wir angezeigt, in dem Sie ggf. einen Zeitraum wählen können.
- Klicken Sie Daten löschen.

11.12 Remote Management

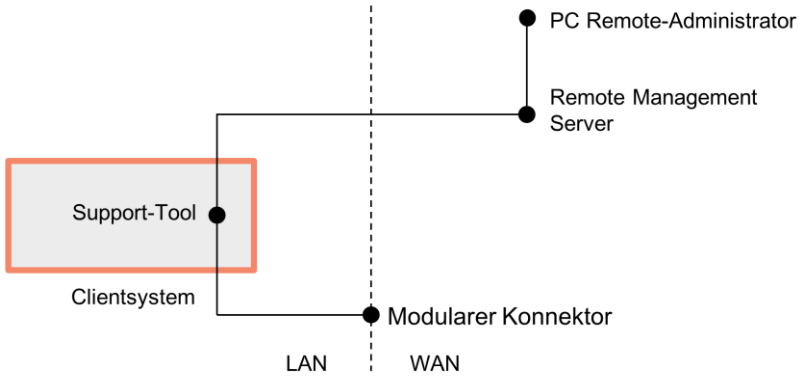


Abbildung 44: Benötigte Komponenten für das Remote Management

Abbildung 44 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.

11.12.1 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).

11.12.2 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 10: Betriebsmodi für das Remote Management

11.12.2.1 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.

11.12.2.2 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.

11.12.3 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 9.5.1).

   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 9.1).

   Der Administrator des Konnektors muss das initiale Passwort dem Remote-Administrator auf sicherem Wege mitteilen. Beachten Sie dazu die Warnhinweise in Kapitel 9.1.
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 7.4.4 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 5.2.

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 9.1.3)

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.

12 Wartung und Pflege

12.1 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 13).

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.

12.2 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 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 13.

12.3 Systemzeit synchronisieren

Synchronisieren Sie im Offline-Betrieb mindestens einmal jährlich die Systemzeit (siehe Kapitel 9.5.3).

13 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 3.3).

14 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.

15 Dauerhafte Außerbetriebnahme/Entsorgung

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 Rücknahme der Freischaltung des Modularen Konnektors beim VPN-Zugangsdienst (siehe Kapitel 9.6.1.2)
- Den Sperrauftrag beim Hersteller
- Die Durchführung eines vollständigen Werksresets (siehe Kapitel 11.7) oder einer Sperrung für den Versand (siehe Kapitel 11.8)
- Die Rücksendung an den Hersteller durch den DVO nach erfolgreicher Sperrung für den Versand

Verschicken Sie das Gerät nicht eigenständig.

Bei fehlgeschlagenem Werksreset für den Versand muss der Hersteller umgehend informiert werden. Der Hersteller wird die Entnahme der gSMC-Ks aus dem Gerät autorisieren. Erst nach Autorisierung durch den Hersteller darf das Gerät 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

Beachten Sie für die Entsorgung die Hinweise des Herstellers unter https://www.secunet.com/konnektor/.

16 Anhang

16.1 Lieferumfang

16.1.1 Einboxkonnektor (Konstruktionsstand 2.0.0)

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

Tabelle 11: Lieferumfang und Zubehör (Einboxkonnektor)

16.1.2 Rechenzentrumskonnektor (Konstruktionsstand 2.1.0)

Komponente	Beschreibung
Modularer Konnektor	
2 x Netzkabel	Kaltgerätestecker
Sicherheitsbeiblätter	*Empfang und Prüfung* *Aufstellung und Inbetriebnahme*
CD/DVD	Bedienhandbuch als PDF

Tabelle 12: Lieferumfang und Zubehör (Rechenzentrumskonnektor)

Die 90°-Winkel zur Befestigung in einem 19" Netzwerkschrank sind bei Auslieferung bereits am Gerät angebracht. Die Schrauben zur Befestigung in einem 19" Netzwerkschrank sind nicht Bestandteil des Lieferumfangs.

16.2 Typschild und Verpackungskennzeichnung

16.2.1 Einboxkonnektor (Konstruktionsstand 2.0.0)

Abbildung 45: Typenschild Gehäuse (Einboxkonnektor)

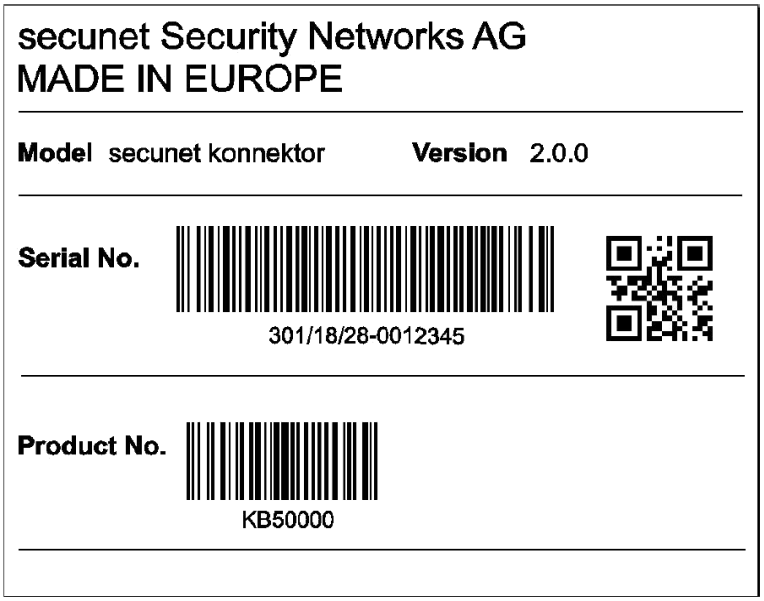


Abbildung 46: Verpackungskennzeichnung (Einboxkonnektor)

16.2.2 Rechenzentrumskonnektor (Konstruktionsstand 2.1.0)

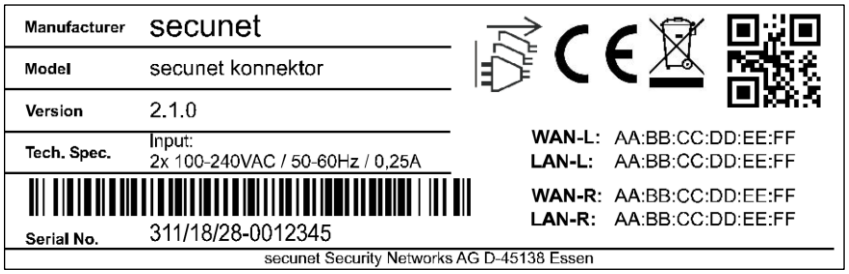


Abbildung 47: Typenschild (Rechenzentrumskonnektor)

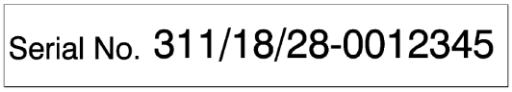


Abbildung 48: Kennzeichnung Seriennummer (Rechenzentrumskonnektor)

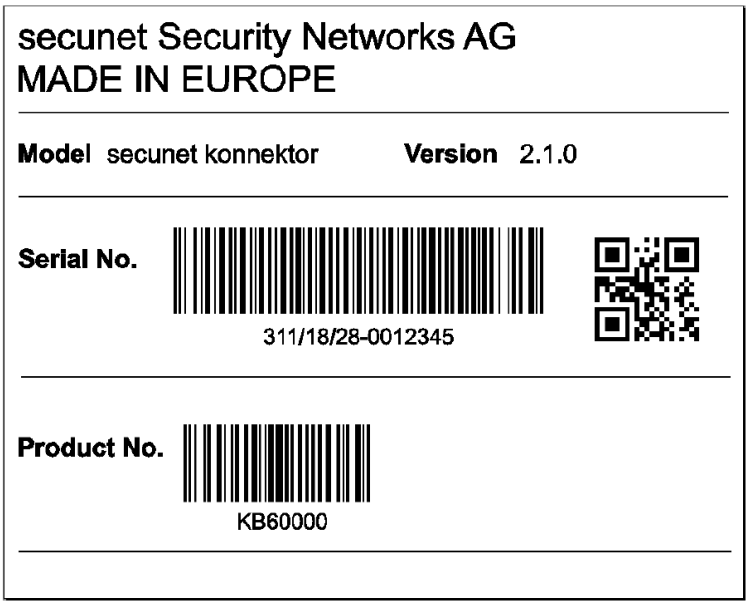


Abbildung 49: Verpackungskennzeichnung (Rechenzentrumskonnektor)

16.3 Sicherheitssiegel

16.3.1 Einboxkonnektor (Konstruktionsstand 2.0.0)

Das Gerät ist mit zwei Sicherheitssiegeln ausgestattet, die in Vertiefungen an den beiden Gehäuseseiten angebracht sind.

Abbildung 50: Sicherheitssiegel (Einboxkonnektor)

16.3.2 Rechenzentrumskonnektor (Konstruktionsstand 2.1.0)

Das Gerät ist mit einem Sicherheitssiegel ausgestattet, das an der Gerätevorderseite angebracht ist.

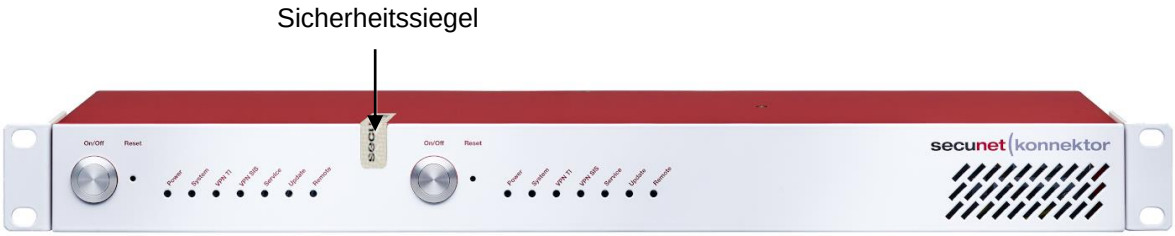


Abbildung 51: Sicherheitssiegel (Rechenzentrumskonnektor)

16.4 Schnittstellen und Bedienelemente

16.4.1 Einboxkonnektor (Konstruktionsstand 2.0.0)

16.4.1.1 Geräteoberseite

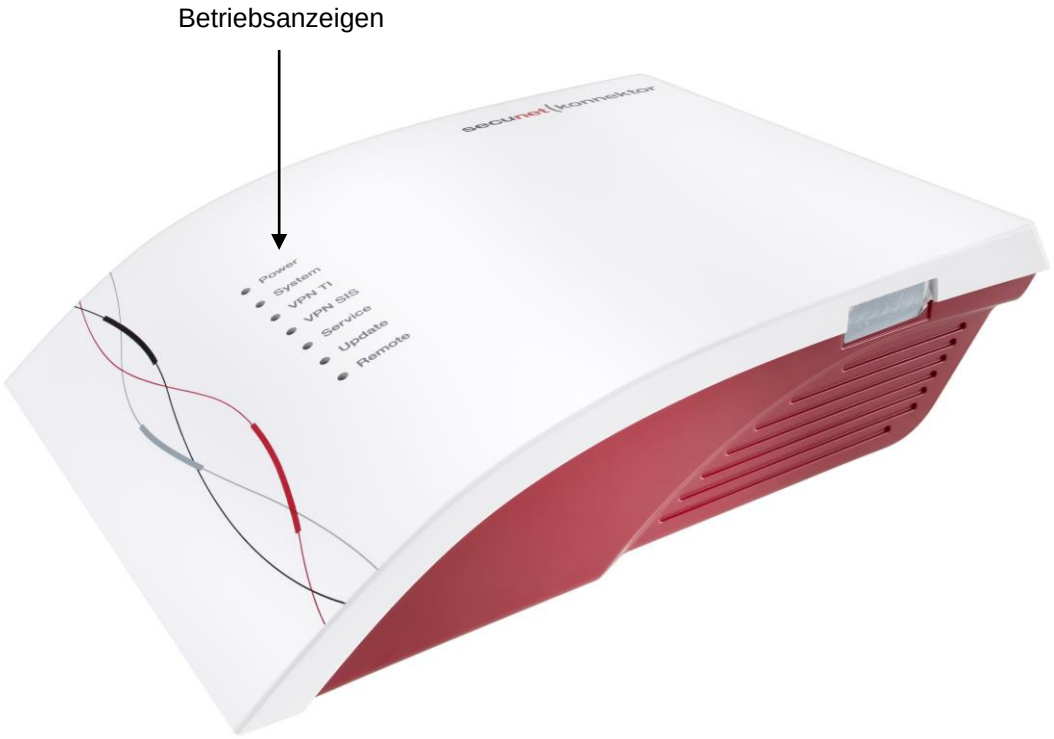


Abbildung 52: Gehäuseoberseite (Einboxkonnektor)

Die roten Betriebsanzeigen (LEDs) signalisieren aktuelle Betriebszustände.

16.4.1.2 Gehäuserückseite

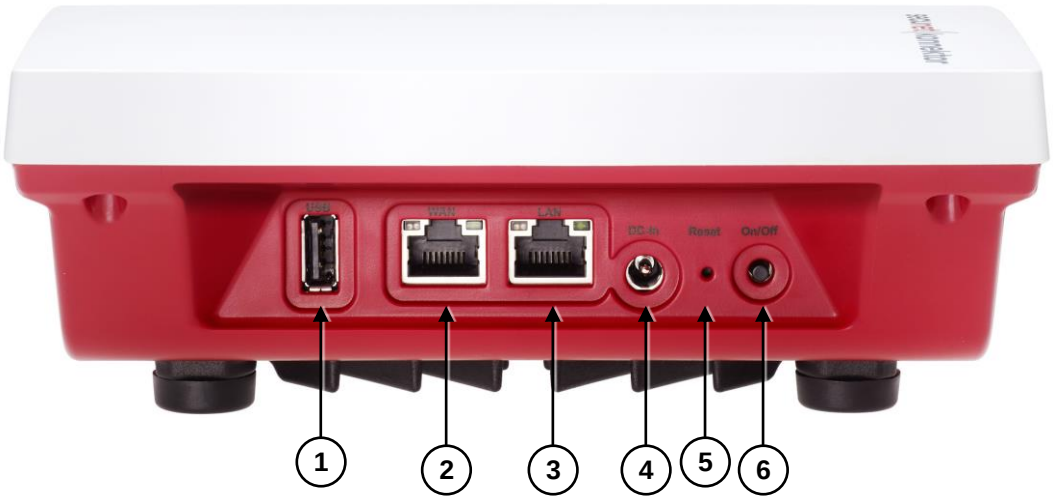


Abbildung 53: Gehäuserückseite (Einboxkonnektor)

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 Werksreset (siehe Kapitel 11.5)
6	An/Aus-Taster (Beachten Sie die Hinweise in Kapitel 4.5)

Tabelle 13: Bedienelemente und Schnittstellen (Einboxkonnektor)

16.4.1.3 Gehäuseunterseite ohne Wandhalterung

Abbildung 54: Gehäuseunterseite ohne Wandhalterung (Einboxkonnektor)

Position	Bezeichnung
1	Gummifüße
2	Kühlplatte

Tabelle 14: Gehäuseunterseite Einboxkonnektor

16.4.1.4 Gehäuseunterseite mit Wandhalterung (optional)

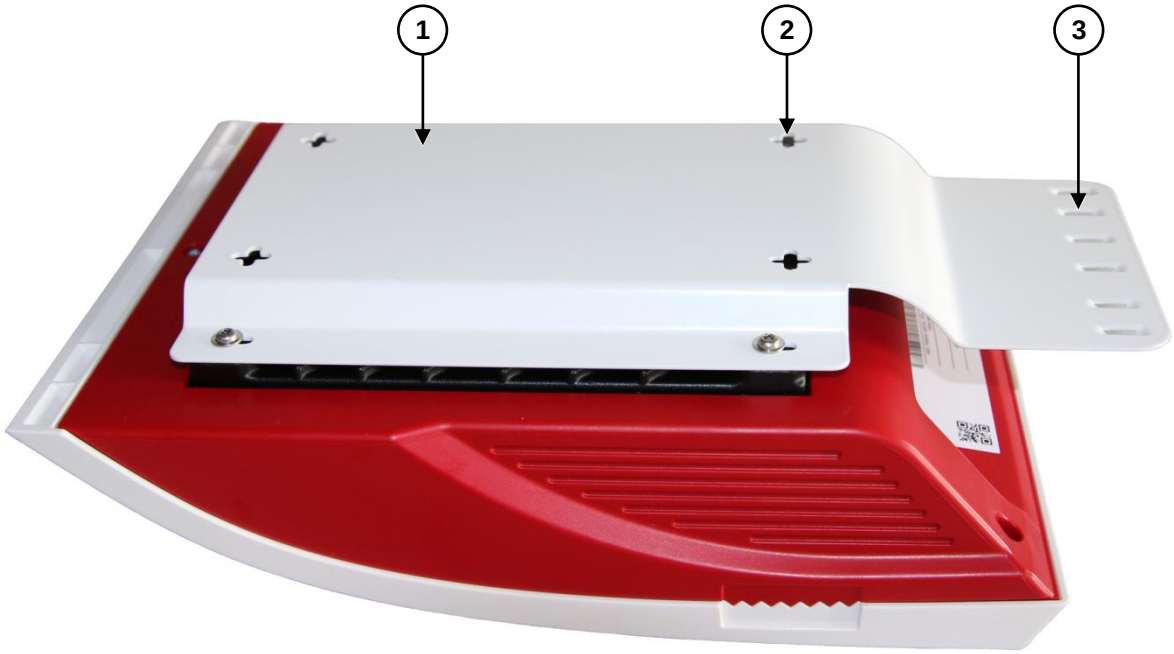


Abbildung 55: Gehäuseunterseite mit Wandhalterung (Einboxkonnektor)

Position	Bezeichnung
1	Wandhalterung
2	Montageöffnungen
3	Kabelfixierungen

Tabelle 15: Gehäuseunterseite mit Wandhalterung (Einboxkonnektor)

16.4.2 Rechenzentrumskonnektor (Konstruktionsstand 2.1.0)

16.4.2.1 Gerätevorderseite

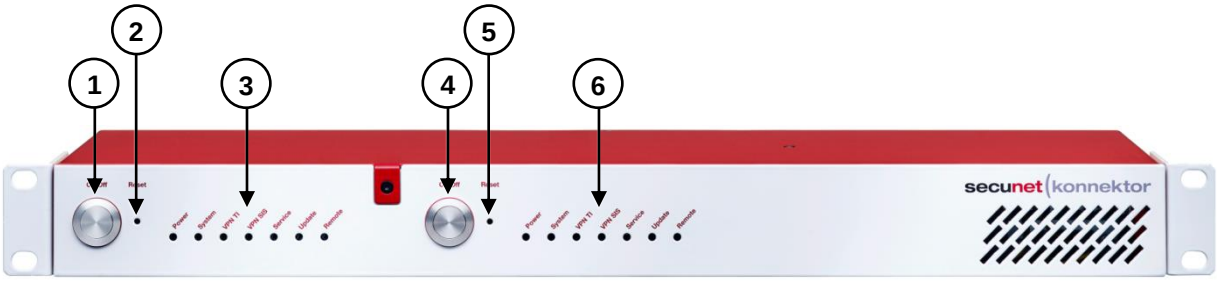


Abbildung 56: Gehäusevorderseite (Rechenzentrumskonnektor)

Position	Bezeichnung
1	An/Aus-Taster Konnektor Links (beachten Sie die Hinweise in Kapitel 4.5)
2	Reset-Taster für Werksreset Konnektor Links (siehe Kapitel 11.5)
3	Betriebsanzeigen Konnektor Links
4	An/Aus-Taster Konnektor Rechts
5	Reset-Taster für Werksreset Konnektor Rechts (siehe Kapitel 11.5)
6	Betriebsanzeigen Konnektor Rechts

Tabelle 16: Gehäusevorderseite (Rechenzentrumskonnektor)

16.4.2.2 Geräterückseite

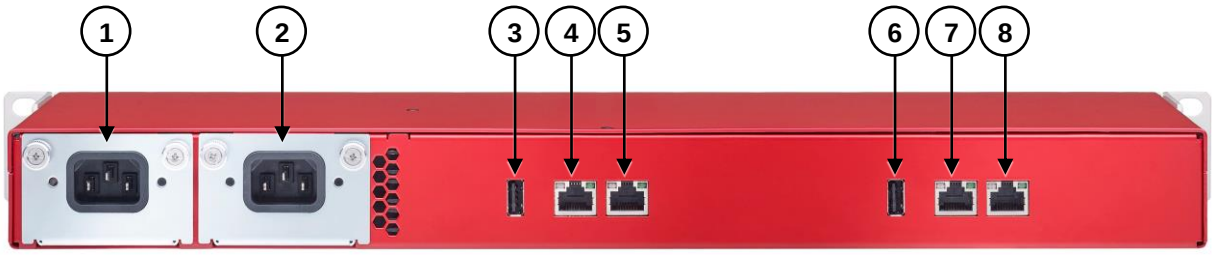


Abbildung 57: Gehäuserückseite Rechenzentrumskonnektor (Konstruktionsstand 2.1.0)

Position	Bezeichnung
1	Spannungsversorgung Konnektor Rechts
2	Spannungsversorgung Konnektor Links
3	Schnittstelle USB 2.0 Konnektor Rechts
4	Netzwerkanschluss WAN Konnektor Rechts
5	Netzwerkanschluss LAN Konnektor Rechts
6	Schnittstelle USB 2.0 Konnektor Links
7	Netzwerkanschluss WAN Konnektor Links
8	Netzwerkanschluss LAN Konnektor Links

Tabelle 17: Geräterückseite (Rechenzentrumskonnektor)

Beachten Sie:

- **Netzteile dürfen nur nach vollständiger Spannungsfreischaltung entnommen werden.**
- **Netzteile dürfen nur durch Module ersetzt werden, die vom Hersteller bereitgestellt wurden.**

16.5 Produkt- und Betriebsmerkmale

16.5.1 Einboxkonnektor (Konstruktionsstand 2.0.0)

16.5.1.1 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	Entweder 2 x STARCOS 3.6 Health SMCK R1 oder 2 x TCOS Security Module Card - K Version 2.0 Release 1
Festplatte	16 GB SSD
Netzwerk	Zwei getrennte Netzwerkcontroller für WAN/LAN
RTC	Real Time Clock, max. Drift +/- 20 ppm

Tabelle 18: Produktmerkmale (Einboxkonnektor)

16.5.1.2 Betriebsmerkmale

Betriebsmerkmale	
Stromversorgung	12 V DC vom Steckernetzteil, 100 - 240 V AC 50Hz (Steckdose)
Leistungsaufnahme	Mittlerer Wert 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 19: Betriebsmerkmale (Einboxkonnektor)

16.5.2 Rechenzentrumskonnektor (Konstruktionsstand 2.1.0)

16.5.2.1 Produktmerkmale

Allgemein	
Abmessungen	ca. L × B × H: 480 mm × 201 mm × 45 mm
Gewicht	ca. 3 kg
Schnittstellen	2 × USB 2.0 2 × WAN 1 GB Ethernet 2 × LAN 1 GB Ethernet 2 × Spannungsversorgung (Kaltgerätestecker) 2 × Werksreset 2 × 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	2 × Intel® X86-64
Arbeitsspeicher	2 × 8 GB RAM
gSMC-K	Entweder 4 × STARCOS 3.6 Health SMCK R1 oder 4 x TCOS Security Module Card - K Version 2.0 Release 1
Festplatte	2 × 16 GB SSD
Netzwerk	2 × 2 getrennte Netzwerkcontroller für WAN/LAN
RTC	2 × Real Time Clock, max. Drift +/- 20 ppm

Tabelle 20: Produktmerkmale (Rechenzentrumskonnektor)

16.5.2.2 Betriebsmerkmale

Betriebsmerkmale	
Stromversorgung	100 - 240 V AC 50Hz (Steckdose)
Leistungsaufnahme	Mittlerer Wert 2 × 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 21: Betriebsmerkmale (Rechenzentrumskonnektor)

Beachten Sie:

- **Netzteile dürfen nur nach vollständiger Spannungsfreischaltung entnommen werden.**
- **Netzteile dürfen nur durch Module ersetzt werden, die vom Hersteller bereitgestellt wurden.**

16.6 Montage

16.6.1 Einboxkonnektor (Konstruktionsstand 2.0.0)

16.6.1.1 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.

16.6.1.2 Wandmontage

Für die Wandmontage ist eine Wandhalterung verfügbar (siehe Kapitel 16.4.1.4). 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.

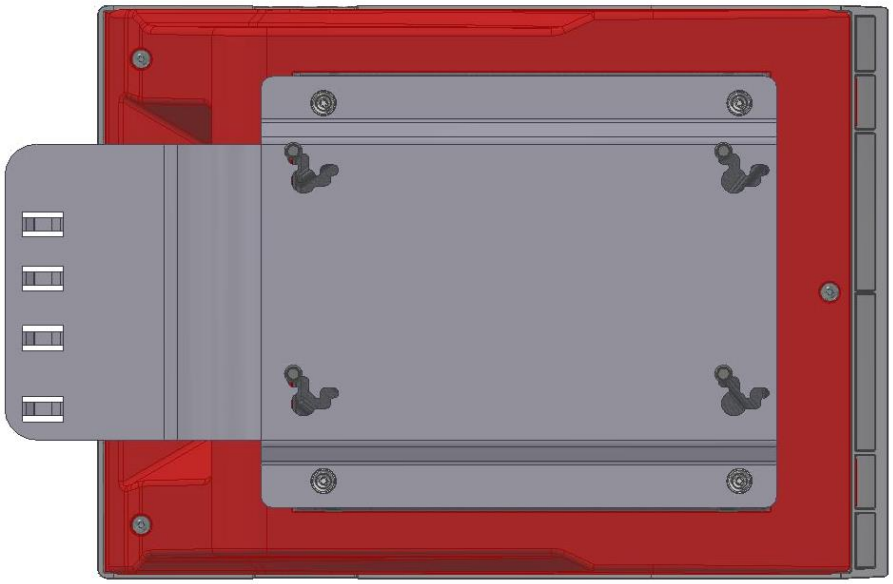


Abbildung 58: Gehäuse mit Wandhalterung (Einboxkonnektor)

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

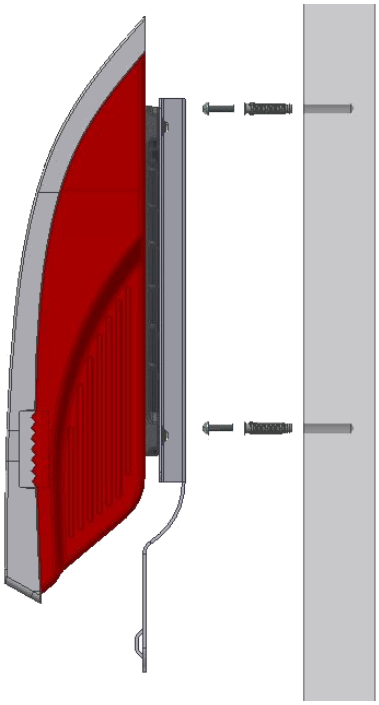


Abbildung 59: Wandmontage (Einboxkonnektor)

16.6.1.3 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 10.2).

Abbildung 60: Gehäuserückseite (Einboxkonnektor)

16.6.2 Rechenzentrumskonnektor (Konstruktionsstand 2.1.0)

Der Rechenzentrumskonnektor ist für die Montage in einem 19" Netzwerkschrank vorgesehen.

Für die Stromversorgung dürfen nur Steckdosen mit Schutzleiter-anschluss verwendet werden.

Beachten Sie, dass zum Trennen des Geräts von der Stromversorgung beide Netzkabel gezogen werden müssen.

Das Gerät enthält Batterien. Diese sind nicht durch den Nutzer zu warten.

- Beachten Sie die Hinweise des Netzwerkschrankherstellers und verwenden Sie das von ihm empfohlene Montagematerial.

Die Schrauben zur Befestigung in einem 19" Netzwerkschrank sind nicht Bestandteil des Lieferumfangs.

- Verbinden Sie den Modularen Konnektor mit den beiliegenden Netzkabeln mit der Stromversorgung an (Schutzklasse 2).
- Verbinden Sie die WAN- und LAN-Anschlüsse entsprechend des geplanten Einsatzszenarios (siehe Kapitel 10.2).

16.7 Unterstützte Netzwerkprotokolle

16.7.1 TCP/IP

Der Modulare Konnektor unterstützt TCP-/IPv4-Pakete gemäß RFC 793 /RFC 791 (siehe Kapitel 7.2.3 für eine Übersicht der verwendeten IP-Protokolle).

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

16.7.2 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 2.2.1) 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.

16.7.3 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 aufgebaut.

Parameter

Der Modulare Konnektor sendet folgende Parameter:

Für die Nachrichten ClientHello (RFC 5246 Abschnitt 7.4.1.2) und ServerHello (RFC 5246 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) verwendet der Modulare Konnektor ein eigenes Zertifikat für die Authentisierung.

Für die Nachricht CertificateRequest (RFC 5246 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 5246 Abschnitt 7.3 Fig. 1 TLS 1.2 durch.

Verwendete Nachrichten:

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

Meldungen

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

16.7.4 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.

16.7.5 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.

16.7.6 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.

16.7.7 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 5246 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 5246 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 9.5.2).

16.8 Standardwerte bei Auslieferung

16.8.1 Menü „Benutzer“

Wert	Standardeinstellung	Wertebereich
Ablaufzeit Passwörter	120 Tage	-

16.8.2 Menü „Netzwerk“

16.8.2.1 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	100 Mbit/s	1-1000 Mbit/s

Allgemeine Netzwerkeinstellungen

Wert	Standardeinstellung	Wertebereich
Internet Modus	SIS	SIS, IAG, Keiner
Intranet Routing Modus	Redirect	Redirect, Block
Service Timeout	60 Sekunden	-
Intranet Routen	-	-
Bandbreitenbeschränkung	100 Mbit/s	1-1000 Mbit/s
Minimale Bandbreite	-	-

Clientsystem-Einstellungen

Wert	Standardeinstellung	Wertebereich
TLS-Pflicht	An	An/Aus
Authentifizierung	Zertifikat	Keine Authentifizierung, Zertifikat, Benutzername/Passwort
Ungesicherter Zugriff auf Dienstverzeichnisdienst	An	An/Aus
Maximale Anzahl Fehlversuche	3	-

Erweiterte TLS-Einstellungen

Wert	Standardeinstellung	Wertebereich
Permanente Verbindungen	1	0 - 100
Maximale Verbindungen	1	0 - 100
Lebensdauer Verbindungen	5 Minuten	Mind. 1 Millisekunde
Aufräum-Intervall	5 Minuten	Mind. 1 Millisekunde
Aufräum-Threads	1	Mind. 1
Wartedauer vor Erstellung	100 Millisekunden	1 - 1000 Millisekunden
Wartedauer vor Abbau	10 Millisekunden	1 Millisekunde - 10 Sekunden
Timeout Erstellung	10 Sekunden	1 Millisekunde - 10 Sekunden

Erreichbarkeit testen

Wert	Standardeinstellung	Wertebereich
Test-Quelle	Netzkonnektor	-
IP-Adresse/FQDN	-	-

Wert	Standardeinstellung	Wertebereich
Port	-	-
Anzahl zusätzlicher Versuche	0	-
Timeout	2000 Millisekunden	-

16.8.2.2 Bereich „LAN“

Wert	Standardeinstellung	Wertebereich
DHCP-Client benutzen	An	An/Aus
LAN-Netzwerk	-	-
LAN-seitige IP-Paketlänge (MTU)	1400	-
Weitere Parameter	-	-

16.8.2.3 Bereich „WAN“

Wert	Standardeinstellung	Wertebereich
DHCP-Client benutzen	An	An/Aus
WAN-Netzwerk	-	-
IP-Adresse des Standard-Gateway	-	-
WAN-seitige IP-Paketlänge (MTU)	1400	-
Weitere Parameter	-	-
WAN Modus	An	An/Aus

16.8.2.4 Bereich „LAN DHCP-Server“

Wert	Standardeinstellung	Wertebereich
DHCP-Server aktiv	Aus	An/Aus
IP-Netzwerk	-	-
Broadcast-Adresse	-	-
Addressbereich Untergrenze	-	-
Addressbereich Obergrenze	-	-
Standard-Clientgroup wählen	ClientGroup1	-
Clientgroup anlegen	ClientGroup1	-

16.8.2.5 Bereich „DNS“

Wert	Standardeinstellung	Wertebereich
DNS-Server für das Transportnetz	-	-
DNS-Server zur Namensauflösung von Namensräumen in der Einsatzumgebung	-	-
DNS-Domain Zugangsdienst	gto1-ref.service-ti.de	-
DNS-Domain Einsatzumgebung	Arzt.local	-
DNSSEC Trustanchor Internet	<Vorkonfiguriert>	-

16.8.3 Menü „Praxis“

16.8.3.1 Bereich „Karten“

Wert	Standardeinstellung	Wertebereich
Timeout für Kartenoperationen	60 Sekunden	-
Timeout für PIN-Kommandos	60 Sekunden	10 - 120 Sekunden
Zertifikatsprüf-Intervall	1 Tag	0 - 365 Tage
Zertifikats-Ablauf Warnung	90 Tage	0 - 180 Tage (0 = Keine Warnung)
Timeout für Kartenreservierung	5 Sekunden	500 Millisekunden - 10 Sekunden

16.8.3.2 Bereich „Terminals“

Wert	Standardeinstellung	Wertebereich
Service Discovery Port	4742	-
Service Discovery Timeout	3 Sekunden	Mind. 1 Sekunde
Service Discovery Zyklus	10 Minuten	Mind. 1 Minute (0 = Deaktiviert)
Service Announcement Port	4742	-
Keep-Alive Intervall	10 Sekunden	1 - 10 Sekunden
Anzahl Keep-Alive Versuche	3	3 - 10
TLS Handshake Timeout	10 Sekunden	1 - 60 Sekunden
Display Anzeigedauer	10 Sekunden	1 - 60 Sekunden
Timeout für Pairing-Kommandos	60 Sekunden	10 - 120 Sekunden

Wert	Standardeinstellung	Wertebereich
Timeout für Update-Kommandos	60 Sekunden	10 - 600 Sekunden

16.8.4 Menü „Diagnose“

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

16.8.5 Menü „System“

16.8.5.1 Bereich „Allgemein“

Wert	Standardeinstellung	Wertebereich
Name	conn-at-pu	-
Leistungsumfang Signaturanwendungskomponente	Aus	An/Aus
Einfachsignaturmodus	An	An/Aus

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

16.8.5.2 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	10 Minuten	0 - 20 Minuten
Timeout OCSP-Abfragen	3 Sekunden	1 - 120 Sekunden
Missbrauch-Erkennung Einstellungen		
Zertifikat prüfen (Versuche)	401	0 - 9999 (0 = deaktiviert)

16.8.5.3 Bereich „Zeit“

Wert	Standardeinstellung	Wertebereich
Zeit	-	-
Zeitzone	CET	Auswahlliste
Zeitsynchronisierung		
Warnung nach	30 Tage	-
Fehlerzustand nach	50 Tage	-
Maximale Zeitabweichung	3600 Sekunden	-

16.8.5.4 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

16.8.6 Menü „VPN“

16.8.6.1 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		
Inaktive Verbindung abbauen	Aus	An/Aus
Timeout nach Inaktivität	600 Sekunden	-

Wert	Standardeinstellung	Wertebereich
Maximale Paketgrößen (MTU)		
SIS	1418 Byte	576 - 8076 Byte
TI	1418 Byte	576 - 8076 Byte
IPSec		
Auswertung der Sequenznummern	An	An/Aus
Fenstergröße Sequenznummern	32	-
Keying Versuche	1	1 - 100
IKE Rekeying Zeit	84500 Sekunden	77760 - 86400 Sekunden
IKE Reauthentifizierung Zeit	558720 Sekunden	IKE Random Zeit zzgl. 544320 - 604800 Sekunden
IKE Overtime	1800 Sekunden	600 - 8640 Sekunden
IKE Random Zeit	1800 Sekunden	600 - 8640 Sekunden
IPSec Rekeying Zeit	77760 Sekunden	77760 - 85800 Sekunden
IPSec Lebenszeit	79560 Sekunden	IPSec Rekeying Zeit“ zzgl. 600 - 86400 Sekunden
IPSec Random Zeit	1800 Sekunden	600 - 8640 Sekunden
Netzwerk-Segmente	<vorkonfiguriert>	-
Firewall-Regeln	-	-

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	300 - 86400 Sekunden
IKE Reauthentifizierung Zeit	600 - 604800 Sekunden
IKE Lebenszeit	600 - 14400 Sekunden
IKE Random Zeit	600 - 14400 Sekunden
IPSec Rekeying Zeit	300 - 85800 Sekunden

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

16.8.7 Menü „Fachmodule“

16.8.7.1 Bereich „VSDM“

Wert	Standardeinstellung	Wertebereich
Intermediär-Servicename	_vsdmintermediaer._tcp	
Max. Dauer TI Offline	0 Tage (keine Prüfung)	- (0 = Keine Prüfung)
Timeout Aufrufe TI	10 Sekunden	-
Timeout für ReadVSD	30 Sekunden	-
Automatische Onlineprüfung VSD	Aus	An/Aus
Aufrufkontext	-	
Verschlüsselung der Prüfungsnachweise (VSDM-PNW-Key)	-	16 ASCII Zeichen, Dezimal-Codes von 32 (Leerzeichen) bis 126 (Tilde)

16.9 Meldungen und Protokolle

Der Modulare Konnektor erzeugt im Betrieb Meldungen und protokolliert diese im Protokollspeicher. Sie können über die Bedienoberfläche ausgelesen werden (siehe Kapitel 9.4). 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 8.2). Bei Meldungen mit hoher Priorität blinkt am Gehäuse zudem die Betriebsanzeige **Service**.

16.9.1 Übersicht der Protokolle

Meldungen werden in verschiedenen Protokollen gespeichert:

- Sicherheitseinträge (SEC, Securityprotokoll)

  Meldungen zu allen sicherheitsrelevanten Ereignissen, sowohl im System als auch in den Fachmodulen

- Operative Einträge (OP, Systemprotokoll)

  Meldungen zum Betrieb der Basisdienste des Systems und zu Lizenzen

- Performance-Einträge (PERF, Performanceprotokoll)

  Meldungen zu Operationen an den Außenschnittstellen sowie zu Performance-relevanten internen Abläufen

- Pro Fachmodul:
  - Operative Einträge (OP, Fachmodulprotokoll)

    Meldungen zum Betrieb des Fachmoduls
  - Performance-Einträge (PERF, Fachmodul-Performanceprotokoll)

    Performance-Einträge des Fachmoduls

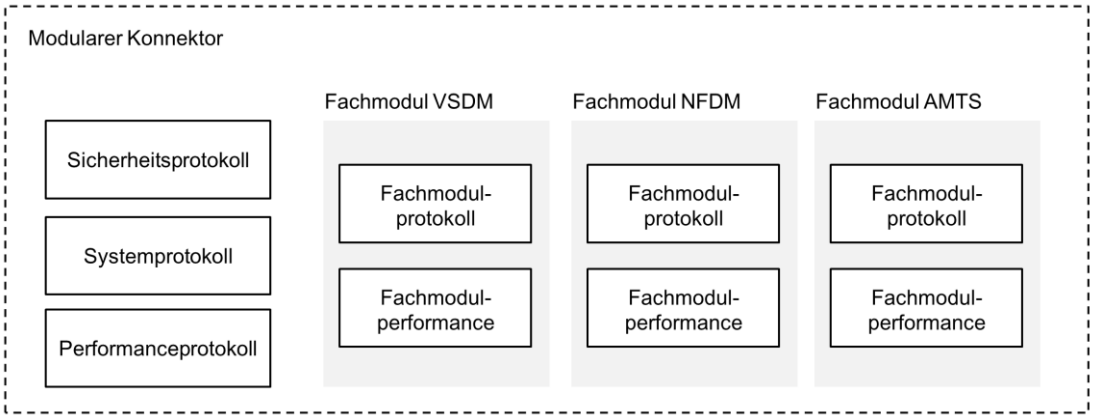


Abbildung 61: Übersicht der Protokolle

Welche Ereignisse protokolliert werden, können Sie im Menü **Diagnose** im Bereich **Administration** festlegen (siehe Kapitel 9.4.6).

Ob Einträge einer bestimmten Severity geschrieben werden, hängt von dem eingestellten Log-Level ab. Im Auslieferungszustand ist ein Log-Level der Stufe WARNING voreingestellt und es werden zudem keine Performancemeldungen erstellt. Dies ist zu beachten, weil bestimmte Arten von Protokolleinträgen immer eine bestimmte Severity-Stufe besitzen. Beispielsweise besitzen Ablaufprotokolleinträge die Severity-Stufe INFO bzw. DEBUG und werden somit im Auslieferungszustand nicht erzeugt

- Um Meldungen der Stufen INFO oder DEBUG zu schreiben, stellen Sie den Log-Level entsprechend ein.

In manchen Anwendungsfällen können Einträge in verschiedene Protokolle geschrieben werden. Beispielsweise werden im Anwendungsfall `ReadVSD` sowohl Einträge in das VSDM Fachmodul-Performanceprotokoll als auch in das systemübergreifende Performanceprotokoll geschrieben. Im systemweite Performanceprotokoll werden in diesem Fall unter anderem die OCSP-Anfragen protokolliert, da OCSP-Anfragen von dem Basis-System des Modularen Konnektors ausgeführt werden.

16.9.2 Format der Protokolleinträge

Die Protokollierung erfolgt in einem einheitlichen Format. Grundsätzlich gilt die Vorgabe, dass ein Protokolleintrag aus mehreren Key/Value-Paaren besteht. Die Key/Value-Paare sind untereinander mit dem Semikolon („;“) getrennt. Als Trennzeichen zwischen Key und Value wird das Gleichheitszeichen („=“) verwendet. Jeder Protokolleintrag beginnt mit den Key/Value-Paaren „timestamp“, „type“ und „severity“. Der Timestamp wird im Format dd.MM.yyyy HH:mm:ss.SSS in der Zeitzone UTC geschrieben. Gültige Werte für Type sind „sec“ = Sicherheitsprotokoll, „op“ = Systemprotokoll und „perf“ = Performanceprotokoll. Die Severity kann „debug“, „info“, „warning“, „error“ oder „fatal“ sein. Die weiteren Key/Value-Paare hängen von dem jeweiligen Protokolleintrag ab.

Anhand des Key/Value-Paares „Vorgangsnummer" können Protokolleinträge, die im Rahmen eines Aufrufs erfolgt sind, zugeordnet bzw. verfolgt werden. Eine Vorgangsnummer wird pro Aufruf bzw. je gestarteten Prozess vergeben. Über die Vorgangsnummer lassen sich auch Einträge in verschiedenen Protokollen einander zuordnen.

16.9.3 Art der Protokolleinträge

Es existieren verschiedene Arten von Protokolleinträgen die auch jeweils in den verschiedenen Protokollen enthalten sein können. Die Protokolleinträge unterschieden sich im Wesentlichen anhand der zusätzlich enthalten Key/Value-Paaren. Folgende relevante Arten von Protokolleinträgen werden geschrieben:

- Ablaufprotokolleinträge
- Konfigurationsänderungsprotokolleinträge
- Fehlerprotokolleinträge
- Eventprotokolleinträge
- Betriebszustandsprotokolleinträge
- Performanceprotokolleinträge

16.9.3.1 Ablaufprotokolleinträge

Ablaufprotokolleinträge dienen dazu, den Ablauf eines Anwendungsfalls nachvollziehen zu können. Diese Ablaufprotokolleinträge enthalten immer einen Text und ggf. die zugehörige Vorgangsnummer. Weitere Key/Value-Paare sind je nach Ablaufprotokolleintrag möglich. Die Severity-Stufe für diese Einträge ist „info“ oder „debug“.

Beispiele für Ablaufprotokolleinträge im VSDM Fachmodulprotokoll:

```
timestamp=19.06.2018 09:43:52.853;type=op;severity=info;
text=Beginn des Anwendungsfalls: VSD lesen; Vorgangsnum-
mer=9e49ad88-9fd2-4e4f-8c3e-a4a620480bac

…

timestamp=19.06.2018 09:44:00.032;type=op;severity=info;
text=Aufruf: Prüfungsnachweis erzeugen für Ereignis [UPDATED];
Vorgangsnummer=9e49ad88-9fd2-4e4f-8c3e-a4a620480bac

…

timestamp=19.06.2018 09:44:01.763;type=op;severity=info;
text=Aufruf: GVD von eGK [EGK-12] lesen; Vorgangsnum-
mer=9e49ad88-9fd2-4e4f-8c3e-a4a620480bac
```

```
timestamp=19.06.2018 09:44:02.214;type=op;severity=info;
text=Ende des Anwendungsfalls: VSD lesen; Vorgangsnum-
mer=9e49ad88-9fd2-4e4f-8c3e-a4a620480bac
```

16.9.3.2 Fehlerprotokolleinträge

Wenn während der Verarbeitung von Anfragen Fehler auftreten, werden diese protokolliert. Die Spezifikation der gematik definieren je nach Fehlerfall unterschiedliche Fehlermeldungen inkl. Fehlercodes. Darüber hinaus werden zusätzlich herstellerspezifische Fehlermeldungen unterschieden. Eine Liste der möglichen Fehlermeldungen mit zusätzlich Informationen und ggf. Hinweisen zur Fehlerbehebung finden Sie im Anhang Kapitel 16.9.6.

Alle Protokolleinträge für die Fehlermeldungen enthalten zusätzlich die folgenden Key/Value-Paare:

- „code“
  Definierter Fehlercode
- „name“
  Bezeichnung des Fehlers
- „text“
  Definierter Fehlertext

Je nach Fehlerfall enthält ein Eintrag zudem die folgenden Key/Value-Paare:

- „Details“
  Weitere Informationen zum Fehler
- „Vorgangsnummer“
  ID eines von außen angestoßenen Vorgangs

Beispiel für einen Protokolleintrag von einer definierten Fehlermeldung:

```
timestamp=14.05.2018 13:06:41.479;type=sec;severity=fatal;
code=106; name=EHC_CERT_ONLINE_INVALID;text=Zertifikat auf eGK
ungültig;Vorgangsnummer=1526288338443_64841856901_421307549
```

Für die Protokollierung eines Fehlerfalls im Ablauf des Anwendungsfalls ReadVSD gilt eine Sonderregelung. Diese Sonderregelung erlaubt es, im Fehlerfall auch personenbezogene Daten zu protokollieren. Konkret geht es um die ICCSN der verwendeten eGK und ggf. um die SOAP-Nachricht, welche zu dem Fehler geführt hat.

Einträge mit Personenbezug werden vom Konnektor automatisch nach spätestens 30 Tagen gelöscht. Um nach 30 Tagen weiterhin einen Eintrag zu dem Fehler zu haben, werden die entsprechenden Einträge daher immer doppelt geschrieben, einmal mit und einmal ohne Personenbezug.

16.9.3.3 Eventprotokolleinträge

Durch die Spezifikation der gematik sind verschiedene Events vorgegeben, die im Ablauf für bestimmte Ereignisse erzeugt werden müssen. Die Clientsysteme können sich für die Events registrieren und werden dann mittels CETP-Eventnachricht über das Ereignis informiert. Neben der Benachrichtigung ist auch vorgegeben, dass einige dieser Event zu protokollieren sind. Bestimmte Events werden nicht als CETP-Eventnachricht versendet, sondern nur protokolliert.

Die Einträge können ins Systemprotokoll, in ein Fachmodulprotokoll oder in das Sicherheitsprotokoll geschrieben werden. Die Severity-Stufe hängt dabei von der für das jeweilige Event in der Spezifikation festgelegten Severity-Stufe ab.

Alle protokollierten Events enthalten das Key/Value-Paar „topic“ und die für das Event in der Spezifikation definierten Parameter mit den definierten Parameternamen.

Beispiel für den Protokolleintrag eines Events:

```
timestamp=25.05.2018 11:26:13.794;type=op;severity=info; to-
pic=OPERATIONAL_STATE/EC_TSL_Update_Not_Successful;Value=true;
LastUpdateTSL=25.05.2018 08:18:58.749;Bedeutung=das letzte Up-
date der TSL war nicht erfolgreich.;Vorgangsnummer=
1527232951219_92625886727_662519268
```

16.9.3.4 Betriebszustandsprotokolleinträge

Bei den Betriebszustandsprotokolleinträgen handelt es sich um eine spezielle Art von Eventprotokolleinträgen. Mit ihnen werden Änderungen der Betriebszustände protokolliert. Das Key/Value-Paar „topic“ beginnt bei diesen Einträgen immer mit „OPERATIONAL_STATE/“.

Die Einträge können ins Systemprotokoll oder in das Sicherheitsprotokoll geschriebene werden. Die Severity-Stufe hängt dabei von der für das jeweilige Event in der Spezifikation festgelegten Severity-Stufe ab.

Alle Betriebszustandsprotokolleinträge enthalten mindestens noch zusätzlich das Key/Value-Paar „Value“. Der Wert kann „true“ oder „false“ sein. Wenn der Wert „true“ lautet, ist der Fehlerzustand eingetreten. Wenn der Wert „false“ lautet, wurde der Fehlerzustand wieder beseitigt. In beiden Fällen wird die Severity-Stufe, die für das Event spezifiziert ist, verwendet. Dies führt dazu, dass auch die Behebung eines Fehlerzustands z.B. mit der Severity-Stufe „fatal“ protokolliert werden kann.

16.9.3.5 Konfigurationsänderungsprotokolleinträge

Die Protokollierung von Änderungen der Konfiguration erfolgt gemäß den gematik Vorgaben (Anforderung TIP1-A_5005). Jede Änderung, die ein Benutzer (Administrator) vornimmt, wird protokolliert. Eine Protokollierung von Passwörtern oder personenbezogenen Daten erfolgt dabei nicht.

Bei den Konfigurationsänderungsprotokolleinträgen handelt es sich ebenfalls um eine spezielle Art von Eventprotokolleinträgen. Das Key/Value-Paar „topic“ lauet bei diesen Einträgen immer „MGM/ADMINCHANGES“. Die Einträge werden ins Systemprotokoll mit der Severity-Stufe „info“ geschriebene. Sie werden somit im Auslieferungszustand nicht erzeugt.

Weitere Key/Value-Paare für Konfigurationsänderungsprotokolleinträge:

- „User“

  Username des Administrators, der die Änderung vorgenommen hat.

- „RefID“

  Bezeichnung des geänderten Werts. Sofern es sich um eine Konfiguration handelt, die durch die gematik vorgeschrieben ist, werden die Bezeichner aus der Spezifikation als ReferenzID verwendet.

- „NewVal“

  Der neue Konfigurationswert. Sofern es sich um einen Listeneintrag handelt, wird zusätzlich ein Referenzwert („Ref: […]“) angegeben, der diesen Listeneintrag identifiziert.

  Wenn es sich bei dem Konfigurationswert um die Angabe einer Dauer handelt, dann erfolgt die Ausgabe gemäß ISO 8601 in der Form »PnYnMnDTnHnMnS«, wobei die Großbuchstaben Trennzeichen sind, die weggelassen werden können, wenn die entsprechende Angabe nicht verwendet wird. So bedeutet z.B. die Angabe „PT5H30S“ eine Dauer von 5 Stunden und 30 Sekunden.

Zusätzlich werden auch automatisch erfolgte Änderungen in dieser Form protokolliert. In diesem Fall besitzt "User" den Wert „_konnektor_“ und die Severity-Stufe den Eert „debug“.

16.9.3.6 Performanceprotokolleinträge

Entsprechend den Vorgaben der gematik muss der Konnektor für Aktionen an den Außenschnittstellen Einträge in das Performanceprotokoll erstellen. Die Einträge erfolgen jeweils nur im Performanceprotokoll. Die Severity-Stufe ist entweder „info“ oder „debug“.

Die Performanceprotokollierung muss dediziert aktiviert werden (siehe Kapitel 9.4.6).

Einträge mit der Severity-Stufe „debug“ werden zusätzlich für interne Abläufe erstellt, die im Rahmen von Operationen erfolgen, die über eine Außenschnittstelle angestoßen wurden.

Alle Performanceprotokolleinträge enthalten die folgenden Key/Value-Paare:

- „StartzeitpunktMillis“

  Anzahl der Millisekunden seit dem 1. Januar 1970
- „Dauer in ms“

  Ausführungsdauer der Aktion in Millisekunden.
- „Aktion“

  Bezeichnung der Aktion
- „Beschreibung“

  Details zur Aktion
- „Startzeitpunkt“

  Startzeitpunk im dd.MM.yyyy HH:mm:ss.SSS Format.

Beispiel für Performanceprotokolleinträge für einen ReadVSD Aufruf:

```
timestamp=19.06.2018 16:42:59.701;type=perf;severity=info;
StartzeitpunktMillis=1529419375065;Dauer in ms=4636;
Aktion=FM_VSDM.ReadVSD.OnlineCheck.Update;
Beschreibung=ReadVSD(EhcHandle=EGK-18, HpcHandle=SMC-B-17,
PerformOnlineCheck=true, ReadOnlineReceipt=true);
Startzeitpunkt=19.06.2018 14:42:55.065;
Vorgangsnummer=a6bc500c-9b6c-4daa-a155-d7294606479d
```

16.9.4 Abruf der Protokolle

In der Bedienoberfläche des Modularen Konnektors können Administratoren im Menü **Diagnose** im Bereich **Protokolleinträge** die vorhandenen Meldungen abrufen (siehe Kapitel 9.4.2).

Beim Abrufen wird unter anderem festgelegt, aus welchem Protokoll und für welche Severity-Stufe die Meldungen gelesen werden sollen. Je nachdem welche Einträge gesucht werden, müssen die Suchkriterien entsprechend angepasst werden.

16.9.5 Löschen von Protokolleinträgen

In der Bedienoberfläche des Modularen Konnektors können im Menü **Diagnose** im Bereich **Administration** Protokolleinträge löschen (siehe Kapitel 9.4.6). Dabei können immer nur alle bisherigen Protokolleinträge insgesamt gelöscht werden. Ein Löschen einzelner Protokolleinträge ist nicht möglich.

Das Sicherheitsprotokoll kann nicht durch einen Administrator gelöscht werden. Auch bei einem Werksreset bleibt das Sicherheitsprotokoll erhalten.

Für alle Protokolle kann eingestellt werden, für wie viele Tage die Protokolleinträge gespeichert bleiben. Protokolleinträge, die älter als die festgelegte Zahl an Tagen sind, werden selbständig vom Modularen Konnektor gelöscht. Dieser Mechanismus gilt auch für Sicherheitsprotokolleinträge.

Zudem werden ältere Einträge überschrieben, wenn die Anzahl der Einträge im Sicherheitsprotokoll den konfigurierten Maximalwert übersteigt.

Für die anderen Protokolle beginnt das Überschreiben, wenn der jeweilige Speicherplatz für das Protokoll erschöpft ist. In diesem Fall werden vor dem Schreiben neuer Einträge die ältesten Einträge mit der gleichen oder niedrigeren Severity-Stufe gelöscht.

16.9.6 Übersicht der Meldungen

Legende

Code	Fehler-ID (dient als Referenz der gematik)
Beschreibung	Kurze Zusammenfassung
Typ	Art der Meldung; diese bestimmt, in welche Protokolldatei die Meldung geschrieben wird: SECURITY Sicherheitsprotokoll TECHNICAL Systemprotokoll bzw. Fachmodulprotokoll
Level	Einstufung nach Schwere des Vorfalls (FATAL, ERROR, WARNING, INFO, DEBUG)
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 für 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 vollständigen Werksreset werden Meldungen des Typs SECURITY nicht gelöscht.

Code	Beschreibung	Typ	Level	PVS	Fehlerbehebung/Weitere Angaben für PVS
3	Nachrichten-schema fehlerhaft	TECHNICAL	FATAL		Beim Aufruf einer Operation ist ein Syntaxfehler aufgetreten. ▶ Wiederholen Sie den Vorgang. Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.

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 ein.
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.

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.

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.

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.

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.

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		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		-

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 "PointersTo OtherTSL" nicht vorhanden	TECHNICAL	ERROR		-
1006	TSL-Downloadadressen wiederholt nicht erreichbar	TECHNICAL	ERROR	PVS	-

1007	Vergleich der ID und SequenceNumber entspricht nicht der Vergleichsvariante 6a	SECURITY	ERROR		-
1008	Die TSL ist nicht mehr aktuell	SECURITY	WARNING		-
1009	Überschreitung des Elements NextUpdate um TSL-Grace-Period	SECURITY	WARNING		-
1011	TSL-Datei nicht wellformed	TECHNICAL	ERROR	PVS	-
1012	Schemata der TSL-Datei nicht korrekt	TECHNICAL	ERROR		-
1013	Signatur ist nicht gültig	SECURITY	ERROR		-

1016	KeyUsage ist nicht vorhanden bzw. entspricht nicht der vorgesehenen KeyUsage	SECURITY	ERROR		-
1017	ExtendedKey Usage entspricht nicht der vorgesehenen ExtendedKey Usage	SECURITY	ERROR		-
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 End-Entity-Zertifikats von SubjectKey Identifier des CA-Zertifikats unterschiedlich	SECURITY	ERROR		-
1024	Zertifikats-Signatur ist mathematisch nicht gültig.	SECURITY	ERROR		-
1026	Das Element „ServiceSupplyPoint“ konnte nicht gefunden werden.	TECHNICAL	ERROR		-
1027	CA kann nicht in den TSL-Informationen ermittelt werden.	TECHNICAL	ERROR		-
1028	Die OCSP-Prüfung konnte nicht durchgeführt werden (1)	TECHNICAL	WARNING		-

1029	Die OCSP-Prüfung konnte nicht durchge-führt werden (2)	TECHNICAL	ERROR		-
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 PolicyInforma-tion vorhanden	SECURITY	ERROR		-

1036	Das Zertifikat ist ungültig. Es wurde nach der Sperrung der ausgebenden CA ausgestellt.	SECURITY	ERROR		-
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 certHash Erweiterung	SECURITY	ERROR		-

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		-

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		-

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.

1055	CRL-Signer-Zertifikat nicht in TSL-Informationen 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		-
1061	CA (laut TSL) nicht autorisiert für die Herausgabe dieses Zertifikatstyps.	SECURITY	ERROR		-

1062	Das QES EE-Zertifikat ist ungültig. Es wurde nach der Sperrung der ausgebenden QES CA ausgestellt.	SECURITY	ERROR		Prüfen sie das verwendete QES Zertifikat bzw. die verwendet HBA auf ihre Gültigkeit.
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.
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.
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.
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.
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.

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.

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.
4022	XML-Dokument nicht wohlgeformt	SECURITY	ERROR	PVS	Das verwendete Dokument ist nicht wohlgeformt. ▶ Wiederholen Sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
4023	XML-Dokument nicht valide in Bezug auf XML-Schema	SECURITY	ERROR	PVS	Das verwendete Dokument ist nicht valide. ▶ Wiederholen Sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.

4024	Formatvalidierung fehlgeschlagen (%Dokumentformat%) Der Parameter Dokumentformat kann die Werte XML, PDF/A, TIFF, MIME und Text annehmen.	TECHNICAL	ERROR	PVS	Der Aufruf der Operation ist nicht gültig in Bezug auf das verwendete Dokument. ▶ Wiederholen Sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
4026	XML-Schema nicht valide	SECURITY	ERROR		Das verwendete XML-Schema ist nicht valide. ▶ Wiederholen Sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, 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 Verbindungsaufbaus zum KT	TECHNICAL	ERROR	PVS	Es ist ein technischer Fehler beim Aufbau einer Kartenterminal-Sitzung aufgetreten. ▶ Wenden Sie sich an den DVO.

4029	Fehler bei der KT-Authenti-sierung. KT möglicherweise 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 fehler-haft	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 fehl-geschlagen	TECHNICAL	ERROR	PVS	Es ist ein technischer Fehler beim Hinzufügen eines Kartenterminals aufgetreten. ▶ Wenden Sie sich an den DVO.

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.
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.
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.
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-Authenti-sierung	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.
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 Ka-nals 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		-
4054	Fehler beim Secure Messaging, Zielkarte	SECURITY	ERROR		-
4055	Fehler beim Secure Messaging, Quellkarte	SECURITY	ERROR		-
4056	Fehler bei der C2C-Authenti-sierung, Quellkarte	TECHNICAL	ERROR		-
4057	Fehler bei der C2C-Authenti-sierung, Zielkarte	TECHNICAL	ERROR		-
4058	Aufruf nicht zulässig	SECURITY	ERROR		-
4060	Ressource belegt	TECHNICAL	ERROR		-

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		-
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 gesetzt	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		-
4075	Formatfehler der übergebe-nen 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		-
4082	PIN durch diese Fehleingabe blockiert (nowblocked)	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		-
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-Ausdrucks	TECHNICAL	ERROR		-
4096	Ungültige Kartenterminal-ID	TECHNICAL	ERROR		-
4097	Ungültige Kartenslot-ID	TECHNICAL	ERROR		-
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 SubscriptionId	TECHNICAL	ERROR		-
4103	XML-Element nicht gefunden	TECHNICAL	ERROR		-
4104	XML-Element nicht eindeutig identifiziert (Überschneidung)	TECHNICAL	ERROR		-

4105	Hybride Ver-schlüsselung konnte nicht durchgeführt werden	TECHNICAL	ERROR		-
4106	Falscher Schlüssel	TECHNICAL	ERROR		-
4107	Hybride Ent-schlüsselung konnte nicht durchgeführt werden	TECHNICAL	ERROR		-
4108	Symmetrische Verschlüsse-lung konnte nicht durchge-führt werden	TECHNICAL	ERROR		-
4109	Symmetrische Entschlüsse-lung konnte nicht durchge-führt werden	TECHNICAL	ERROR		-

4110	Ungültiges Dokumentformat	TECHNICAL	ERROR	PVS	Der Aufruf der Operation ist nicht gültig in Bezug auf das verwendete Dokument. ▶ Wiederholen Sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
4111	Ungültiger Signaturyp oder Signaturvariante	TECHNICAL	ERROR		-
4112	Dokument nicht konform zu Regeln für nonQES	TECHNICAL	ERROR	PVS	Der Aufruf der Operation ist nicht gültig in Bezug auf das verwendete Dokument. ▶ Wiederholen Sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
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		-
4123	Fehler bei Signaturerstellung	SECURITY	ERROR		Die Signatur konnte nicht erstellet werde. ▶ Wiederholen Sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
4124	Dokument nicht konform zu Regeln für QES	SECURITY	ERROR		Der Aufruf der Operation ist nicht gültig in Bezug auf das verwendete Dokument. ▶ Wiederholen Sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.

4125	LU_SAK nicht aktiviert	SECURITY	ERROR		Um die Operation durchführen zu können muss LU_SAK aktiviert sein. ▶ Aktivieren die LU_SAK in der Administration, wenn sie diese Funktion nutzen wollen.
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		-
4130	Signaturprüfung der CRL fehlgeschlagen	SECURITY	ERROR		-
4131	Zum angegebenen Card-Handle keine Karte gefunden	TECHNICAL	FATAL		-

4132	Extraktion des Ablaufsdatums schlägt fehl	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 Zertifikatsin-formationen	TECHNICAL	ERROR		-
4149	Ungültige Zerti-fikatsreferenz	TECHNICAL	ERROR		-
4150	Fehler beim Schreiben des Systemproto-kolls	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		-
4156	Server konnte bei TLS-Verbindungsaufbau nicht authentisiert werden	SECURITY	ERROR		-

4157	Clientauthentisierung bei TLS-Verbindungsaufbau fehlgeschlagen	SECURITY	ERROR		-
4158	Adressierte TLS-Verbindung nicht vorhanden	TECHNICAL	ERROR		-
4159	Public-IP: DNS Server antwortet nicht	TECHNICAL	FATAL		-
4160	Public-IP: Zu einem DNS Namen konnte keine IP-Adresse gefunden werden	TECHNICAL	FATAL		-
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		-
4166	gSMC-K Konfiguration: Ein oder mehrere Netzwerk-Adressen sind ungültig.	TECHNICAL	FATAL		-
4167	CreateRoutes: Eine 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		-
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		-
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		-
4180	DNS: Es ist ein Fehler bei der Namensauflösung aufgetreten	TECHNICAL	FATAL		-
4181	Integritätsprüfung UpdateInformation fehlgeschlagen.	SECURITY	ERROR		-
4182	Download nicht aller Update Files möglich.	SECURITY	ERROR		-
4183	Integritätsprüfung Update Files fehlgeschlagen.	SECURITY	ERROR		-

4184	Anwendung der UpdateFiles fehlgeschlagen <Details>.	SECURITY	ERROR		-
4185	Fimware-Version liegt außerhalb der gültigen Firm-ware-Gruppe	SECURITY	ERROR		-
4186	Download nicht aller Update Files möglich.	SECURITY	ERROR		-
4187	KT-Update fehlgeschlagen (<Fehlerinfo gemäß SICCT>)	SECURITY	ERROR		-
4188	Konfigurations-dienst nicht erreichbar, konfigurierte Adresse kon-trollieren.	TECHNICAL	ERROR		-
4189	Konfigurations-dienst liefert falsches Zertifi-kat	SECURITY	FATAL		-

4190	Fehler beim Beziehen der Updatelisten	TECHNICAL	ERROR		-
4192	C2C mit eGK G1+ ab 01.01. 2019 nicht mehr gestattet	SECURITY	ERROR		-
4193	Kein XML-Schema für XML-Dokument vorhanden	SECURITY	WARNING		-
4196	Fehler bei der CV-Zertifikats-prüfung	TECHNICAL	ERROR		-
4197	Parameter Signature-Placement wurde ignoriert	TECHNICAL	WARNING		-
4198	Beim Über-nehmen 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		-
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		-
4207	Referenzzeitpunkt bestimmen ist fehlgeschlagen	TECHNICAL	ERROR		-
4208	Dokument nicht konform zu Profilierung der Signaturformate	TECHNICAL	ERROR		-
4209	Kartentyp <x> wird durch diese Operation nicht unterstützt.	TECHNICAL	ERROR		-
4216	Fehler beim Schreiben des Konnektor-Performanceprotokolls	TECHNICAL	FATAL		-

4217	Fehler beim Schreiben eines Fachmodul-Performance-protokolls	TECHNICAL	FATAL		-
4218	Zugriff auf Konnektor-Performance-protokoll nicht möglich	TECHNICAL	FATAL		-
4219	Zugriff auf Fachmodul-Performance-protokoll nicht möglich	TECHNICAL	FATAL		-
4220	Rollenprüfung bei TLS-Verbindungs-aufbau fehlge-schlagen	SECURITY	ERROR		-
4221	Kartenterminal nicht aktiv	TECHNICAL	ERROR		-
4222	Kartenterminal ist nicht ver-bunden	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		-
4236	Rollenprüfung bei TLS-Verbindungsaufbau zum TSL-Dienst fehlgeschlagen	SECURITY	ERROR		-
4243	Jobnummer unbekannt	TECHNICAL	ERROR		-

4252	Jobnummer wurde in den letzten 1.000 Aufrufen bereits verwendet und ist nicht zulässig	TECHNICAL	ERROR		-
4253	Keine Signatur im Aufruf	TECHNICAL	ERROR		-
4262	Signatur umfasst nicht das gesamte Dokument	TECHNICAL	ERROR		-
4412	NonQES XAdES Signatur gefunden	TECHNICAL	ERROR		-
41000	Karte/ Kartenterminal antwortet mit einer spezifischen Fehlermeldung, Fehlercode:	TECHNICAL	ERROR		-

41001	Kartenterminal <x> ist unzulässigerweise virtuell. Diese Eigenschaft ist ausschließlich für eine zukünftige Nutzung vorgesehen.	TECHNICAL	ERROR		-
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		-
41008	Signaturerstellung über eine Karte nicht möglich.	TECHNICAL	ERROR		-
41009	Kartensitzung für Kartentyp <x> 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		-
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 TLS-Verbindungs-aufbau gesteckt oder freige-schaltet.	TECHNICAL	ERROR		-
41017	C2C-Authenti-sierung durch den Konnektor abgebrochen.	TECHNICAL	INFO		-
41018	Fehler beim Schreiben des PN.	TECHNICAL	ERROR		-
42000	Import einer Backup Datei ist fehlgeschla-gen.	TECHNICAL	ERROR		-
42001	Import einer Backup Datei ist beim Ent-schlüsseln 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		-
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 fehlgeschla-gen.	TECHNICAL	ERROR		-
42011	PublicKey für Backup-Erstellung nicht lesbar.	TECHNICAL	ERROR		-
42012	Rolle stimmt nicht mit der Vorgabe über-ein.	TECHNICAL	ERROR		-
42013	Interner Fehler bei der OCSP-Prüfung	TECHNICAL	ERROR		-
42014	OCSP-Zertifikats-Signatur ist ma-thematisch nicht gültig.	TECHNICAL	ERROR		-
42015	Zertifikats ist nicht mehr gültig.	TECHNICAL	WARNING		-

42016	Zertifikats 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		-
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 <x> keine TLS-Verbindung aufbauen	TECHNICAL	ERROR		-
42021	Der TLS-Dienst kann die Karte <x> nicht benutzen um eine TLS-Verbindung aufzubauen, da diese noch nicht freigeschaltet ist.	TECHNICAL	WARNING		-
42022	Der Name im Zertifikat <x> entspricht nicht dem Hostname <x> der Gegenstelle.	TECHNICAL	ERROR		-

42023	Der Vertrauens-Anker aus der TSL konnte nicht übernommen werden, da das Zertifikat noch nicht gültig ist <x>.	TECHNICAL	ERROR		-
42024	Der Vertrauens-Anker aus der TSL konnte nicht übernommen werden, da das Zertifikat abgelaufen ist <x>.	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 <x> hat das Zeitlimit von <x>ms überschritten.	TECHNICAL	ERROR		-
42027	Der TLS-Dienst konnte mit keiner der <x> bekannten Zieladressen eine TLS-Verbindung aufbauen.	TECHNICAL	ERROR		-
42028	Die TSL enthält keinen BNetzA-VL-Vertrauens-Anker.	TECHNICAL	INFO		-
42029	Mehr als ein BNetzA-VL-Vertrauens-Anker gefunden	TECHNICAL	ERROR		-

42030	BNetzA-VL-Vertrauens-Anker lässt sich nicht extrahie-ren	TECHNICAL	ERROR		-
42031	BNetzA-VL-Downloadad-ressen wieder-holt nicht erreichbar	TECHNICAL	ERROR		-
42032	BNetzA-VL ist abgelaufen.	TECHNICAL	ERROR		Aktuallisieren sie die BNetzA-VL
42033	Import der BNetzA-VL-Datei fehlge-schlagen	TECHNICAL	ERROR		-
43000	Fehler bei der Kommunikation mit dem einem Fachdienst.	TECHNICAL	ERROR		-
43001	Ein Download für das Termi-nalupdate 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		-
43007	Das Update passt nicht zum Gerät.	TECHNICAL	ERROR		-
43008	Update noch nicht heruntergeladen.	TECHNICAL	ERROR		-

43009	Fehler beim Download der Dokumentation vom KSR.	TECHNICAL	ERROR		-
43010	Die Aktualisierung oder das zu aktualisierende Terminal wurden nicht gefunden.	TECHNICAL	ERROR		-
43011	Das zu aktualisierende Terminal ist nicht mehr gepairt.	TECHNICAL	ERROR		-
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: <x>	TECHNICAL	ERROR		-
43014	Fehler bei Registrierung des Konnektors im Konnektor.	TECHNICAL	ERROR		-
43015	Fehler bei Deregistrierung des Konnektors im Registrierungsserver. Fehler: <x>	TECHNICAL	ERROR		-
43016	Fehler bei Deregistrierung des Konnektors im Konnektor.	TECHNICAL	ERROR		-

43017	Fehler bei Statusabfrage beim Registrierungsserver im Registrierungsserver. Fehler: <x>	TECHNICAL	ERROR		-
43018	Fehler bei Statusabfrage beim Registrierungsserver im Konnektor.	TECHNICAL	ERROR		-
43019	Beim Hochladen einer Update-XML-Datei ist ein Fehler aufgetreten. Datei nicht lesbar.	TECHNICAL	ERROR		-

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		-

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 gerade heruntergeladen. Ein Zurücksetzen des Bereiches 'Aktualisierung' ist derzeit nicht möglich.	TECHNICAL	ERROR		-

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		-

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		-

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		-

43038	Eine Aktualisierung konnte nicht installiert werden. Signature der NK-Firmware ungültig.	TECHNICAL	ERROR		-
43039	Eine Aktualisierung konnte nicht installiert werden. Signature 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		-
43042	Das Internet-Access-Gateway <x> der initialen Konfiguration konnte weder auf das LAN-<x>, noch WAN-Netzwerk <x> gemappt werden. Prüfen Sie die IAG-Einstellungen.	TECHNICAL	ERROR		-
43043	Der WAN-Modus ist aktiviert, aber es wurde kein Carrier gefunden.	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 […]
43054	Die Verarbeitung der Anfrage im Netzkonnektor hat zu lange gedauert. Aktion: <x>	TECHNICAL	ERROR		-

16.9.6.1 Fachmodul VSDM

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.

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.

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.
11101	Für die eGK mit der angegebenen ICCSN ist der aufgerufene Dienst nicht zuständig.	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 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 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.
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.
12103	Die Authentifizierung zwischen Fachdienst und eGK mittels des fachdienstspezifischen, karteninidividuellen 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.

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.

16.9.6.2 Fachmodul NFDM

5000	Die eGK ist defekt.	TECHNICAL	FATAL	PVS	Ein technisches Problem ist beim Nutzen 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.
5001	HBA/SMC-B nicht freige-schaltet	TECHNICAL	ERROR	PVS	Die verwendete SMC-B ist nicht freigeschaltet. ▶ Schalten Sie die entsprechende SMC-B frei.
5002	Fachliche Rolle nicht berechtigt zur Ausführung	SECURITY	ERROR	PVS	Die verwendete Leistungserbringer Karte ist nicht berechtigt diese Ope-ration durchzuführen. ▶ Verwenden Sie ggf. eine andere Karte.
5003	Notfalldatensatz nicht konsistent	TECHNICAL	ERROR	PVS	Die Notfalldaten auf der Karte sind nicht konsistent geschrieben worden und können daher nicht gelesen werden. ▶ Die Notfalldaten müssen neu geschrieben werden.

5004	Unbekannte Version der Speicherstruk-tur für den Not-falldatensatz auf der eGK	TECHNICAL	FATAL	PVS	Ein technisches Problem ist beim Nutzen der eGK aufgetreten. ▶ Stecken Sie die Karte erneut und wiederholen sie den Vorgang. ▶ Wenn das Problem nur bei einer bestimmten Karte auftritt, ist gg. Die Karte defekt. Verweisen Sie den Versicherten mit den entsprechenden Fehlerinformationen an seine Krankenkasse. Es kann das
5006	Dekomprimie-rung des Not-falldatensatzes gescheitert	TECHNICAL	ERROR	PVS	-
5007	Decodierung des Notfallda-tensatzes ge-scheitert	TECHNICAL	ERROR	PVS	-
5008	Die Versicher-ten-ID des Not-falldatensatzes stimmt nicht mit der Versicher-ten-ID der eGK überein.	SECURITY	ERROR	PVS	Die Notfalldaten, die auf die Karte geschrieben werden sollen, passen nicht zur verwendeten Karte. ▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.

5009	Die Kodierung (base64) des Notfalldatensatzes ist gescheitert.	TECHNICAL	ERROR	PVS	-
5010	Die Komprimierung des Notfalldatensatzes ist gescheitert.	TECHNICAL	ERROR	PVS	-
5011	Es konnte keine Berechtigungsregel ermittelt werden.	SECURITY	ERROR	PVS	-
5012	Das Löschen des Notfalldatensatzes ist gescheitert.	TECHNICAL	ERROR	PVS	Ein technisches Problem ist beim Nutzen 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

5013	Der Notfalldatensatz überschreitet die maximal zulässige Größe.	BUSINESS	ERROR	PVS	Die Notfalldaten, die auf die Karte geschrieben werden sollen, sind zu groß für die Karte. ▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
5014	Das Primärsystem hat keine Zugriffsberechtigung auf die eGK.	SECURITY	ERROR	PVS	-
5015	Das Primärsystem hat keine Zugriffsberechtigung auf den HBA/die SMC-B.	SECURITY	ERROR	PVS	-
5016	Die gegenseitige Authentisierung von eGK und HBA/SMC-B (Card-toCard-Authentisierung) ist gescheitert.	SECURITY	ERROR	PVS	Ein technisches Problem ist beim Nutzen 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

5017	Der Notfalldatensatz ist nicht valide.	SECURITY	ERROR	PVS	Die Notfalldaten, die auf die Karte geschrieben werden sollen, sind ungültig. ▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
5018	Die Signaturprüfung konnte nicht durchgeführt werden.	SECURITY	ERROR	PVS	Die Notfalldaten, die auf die Karte geschrieben werden sollen, sind ungültig. ▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
5019	PIN-Verifikation gescheitert	SECURITY	ERROR	PVS	-
5020	Der Notfalldatensatz ist verborgen.	BUSINESS	ERROR	PVS	Die Notfalldaten sind verborgen. ▶ Aktivieren sie mit dem Versicherten die Anwendung NFD.
5021	Es ist kein Notfalldatensatz auf der eGK gespeichert.	BUSINESS	ERROR	PVS	-

5022	Es ist bereits ein Notfalldatensatz auf der eGK gespeichert.	BUSINESS	ERROR	PVS	-
5103	Datensatz „Persönliche Erklärungen“ nicht konsistent	TECHNICAL	ERROR	PVS	Der Datensatz „Persönliche Erklärungen“ auf der Karte ist nicht konsistent geschrieben worden und können daher nicht gelesen werden. ▶ Der Datensatz „Persönliche Erklärungen“ muss neu geschrieben werden.
5104	Unbekannte Version der Speicherstruktur für den Datensatz „Persönliche Erklärungen“ auf der eGK	TECHNICAL	FATAL	PVS	Ein technisches Problem ist beim Nutzen 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
5106	Dekomprimierung des Datensatz „Persönliche Erklärungen“ gescheitert	TECHNICAL	ERROR	PVS	-

5107	Decodierung des Datensatz „Persönliche Erklärungen“ gescheitert	TECHNICAL	ERROR	PVS	-
5108	Die Versicherten-ID des Datensatz „Persönliche Erklärungen“ stimmt nicht mit der Versicherten-ID der eGK überein.	SECURITY	ERROR	PVS	Der Datensatz „Persönliche Erklärungen“, der auf die Karte geschrieben werden sollen, passt nicht zur verwendeten Karte. ▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
5109	Die Kodierung (base64) des Datensatz „Persönliche Erklärungen“ ist gescheitert.	TECHNICAL	ERROR	PVS	-

5110	Die Komprimierung des Datensatz „Persönliche Erklärungen“ ist gescheitert.	TECHNICAL	ERROR	PVS	-
5112	Das Löschen des Datensatz „Persönliche Erklärungen“ ist gescheitert.	TECHNICAL	ERROR	PVS	Ein technisches Problem ist beim Nutzen 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
5113	Der Datensatz „Persönliche Erklärungen“ überschreitet die maximal zulässige Größe.	BUSINESS	ERROR	PVS	Der Datensatz „Persönliche Erklärungen“, der auf die Karte geschrieben werden sollen, ist zu groß für die Karte. ▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
5114	Der Datensatz „Persönliche Erklärungen“ ist nicht valide.	SECURITY	ERROR	PVS	Der Datensatz „Persönliche Erklärungen“, der auf die Karte geschrieben werden sollen, ist ungültig. ▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.

5120	Der Datensatz „Persönliche Erklärungen“ ist verborgen.	BUSINESS	ERROR	PVS	Der Datensatz „Persönliche Erklärungen“ ist verborgen. ▶ Aktivieren sie mit dem Versicherten die Anwendung DPE.
5121	Es ist kein Datensatz „Persönliche Erklärungen“ auf der eGK gespeichert.	BUSINESS	ERROR	PVS	-
5122	Es ist bereits ein Datensatz „Persönliche Erklärungen“auf der eGK gespeichert.	BUSINESS	ERROR	PVS	-
5501	Prüfung der qualifizierten elektronischen Signatur unvollständig oder nicht durchführbar bzw. Signatur ungültig.	SECURITY	WARNING	PVS	-

5504	Signatur des Notfalldatensatzes ungültig. Prüfung der Hashwertkette bzw. kryptographische Prüfung der Signatur fehlgeschlagen.	SECURITY	ERROR	PVS	Die Notfalldaten, die auf die Karte geschrieben werden sollen, sind ungültig. ▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
5505	Die Prüfung des Signaturzertifikats des Notfalldatensatzes auf Konformität zu einer qualifizierten elektronischen Signatur ist gescheitert.	SECURITY	ERROR	PVS	Die Notfalldaten, die auf die Karte geschrieben werden sollen, sind ungültig. ▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
5500	Interner Fehler	TECHNICAL	FATAL	PVS	-

16.9.6.3 Fachmodul AMTS

6000	Interner Fehler - Die Operation konnte nicht durchgeführt werden.	TECHNICAL	FATAL	PVS	-
6010	Einwilligung bereits vorhanden	TECHNICAL	FATAL	PVS	-
6049	Smartcard nicht freigeschaltet	SECURITY	ERROR	PVS	Die verwendete SMC-B ist nicht freigeschaltet. ▶ Schalten Sie die entsprechende SMC-B frei.
6051	eGK-Generation 1 und 1+ nicht unterstützt	TECHNICAL	ERROR	PVS	-
6052	Verbindungsfehler zwischen Karten	SECURITY	ERROR	PVS	-

6054	eMP/AMTS-Daten sind inkonsistent. Bitte Daten erneut schreiben.	TECHNICAL	ERROR	PVS	Die eMP/AMTS-Daten auf der Karte sind nicht konsistent geschrieben worden und können daher nicht gelesen werden. ▶ Die eMP/AMTS-Daten müssen neu geschrieben werden.
6056	Einverständnis nicht erteilt	TECHNICAL	ERROR	PVS	-
6057	Versicherten-ID von eGK und zu speichernden Daten unterscheiden sich	BUSINESS	ERROR	PVS	Die eMP/AMTS-Daten, die auf die Karte geschrieben werden sollen, passen nicht zur verwendeten Karte. ▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
6058	eMP/AMTS-Daten konnten nicht validiert werden	TECHNICAL	ERROR	PVS	Die eMP/AMTS-Daten, die auf die Karte geschrieben werden sollen, sind ungültig. ▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.

6059	Nicht genügend Speicherplatz auf der eGK	BUSINESS	ERROR	PVS	Die eMP/AMTS-Daten, die auf die Karte geschrieben werden sollen, sind zu groß für die Karte. ▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang. ▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.
6060	Einwilligung konnte nicht validiert werden	TECHNICAL	ERROR	PVS	-
6061	Keine Einwilligung vorhanden	BUSINESS	ERROR	PVS	-

6063	eGK gesperrt	SECURITY	ERROR	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.
6064	Fachanwendung verborgen	BUSINESS	ERROR	PVS	Die eMP/AMTS-Daten sind verborgen. ▶ Aktivieren sie mit dem Versichtern die Anwendung AMTS.
6065	Löschung der AMTS-Daten nicht zugestimmt	BUSINESS	ERROR	PVS	-
6072	Operation durch Ziehen der eGK vorzeitig beendet	TECHNICAL	ERROR	PVS	-

16.9.7 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 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.
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 concentrator's 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
45193	Unable to execute DHCP client (1/2).		Technical	Error	
45104	Unable to execute DHCP client (2/2).		Technical	Error	
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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
45115	Unable to send MQTT event		Technical	Error	
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
45317	Unable to enable VRDE		Technical	Error	
45318	Unable to start the VBOX virtual machine	AK-VM korrupt	Technical	Error	Support kontaktieren
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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 (nick-name='%s').	Konfiguration fehlerhaft	Technical	Error	Konfiguration prüfen, ggf. Konnektor neu starten
45501	Unable to flush IP addresses of loopback device '%s'.		Technical	Error	
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
45504	Unable to parse IPv4 address '%s'.	Konfigurationsfehler	Techncal	Error	Konfiguration prüfen und neu la-den
45505	Unable to bring tap device '%s' up.		Technical	Error	
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' be-cause no rule sets defined.	Konfiguration fehlerhaft	Technical	Error	Konfiguration prüfen, ggf. Konnektor neu starten
45509	unable to enforce rule set '%s' be-cause it is UNKNOWN.	Konfiguration fehlerhaft	Technical	Error	Konfiguration prüfen, ggf. Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
45516	unable to purge limit rule - rule set tastes bad		Technical	Error	
45517	unable to determine route to host %s (TI concentrator).		Technical	Error	
45518	unable to determine route to host %s (SIS concentrator).		Technical	Error	
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
45526	mosquitto_new failed.		Technical	Error	
45527	mosquitto_threaded_set failed.		Technical	Error	
45528	mosquitto_subscribe failed.		Technical	Error	
45529	[SIGUSR1] unable to read/parse the configuration from %s		Technical	Error	
45530	[SIGUSR1] unable to read/parse the global XML configuration		Technical	Error	
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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
45539	Unable to send MQTT event VPNALERT/ONLINE		Technical	Error	
45540	Did NOT receive VPNALERT acknowledgement		Technical	Error	
45541	unable to create MQTT thread		Technical	Error	
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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
46012	Unable to establish new default gateway. This is fatal.		Technical	Fatal	
46013	Unable to execute iproute2 command because command not defined (INTERNAL ERROR).	Konfiguration fehlerhaft	Technical	Fatal	Konfiguration prüfen und neu laden

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
46015	Unable to purge old default gateway. This is fatal.		Technical	Fatal	
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
46017	Unable to set host name '%s' of connector. EXIT.		Technical	Fatal	
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
46021	Unable to unwind rule stack 'lektr_intranet_routes'. This is fatal.		Technical	Fatal	
46022	Unable to unwind rule stack 'services'. This is fatal.	Regelsatz 'SERVICES' kann nicht entfernt werden (netfilter/routing-Problem)	Technical	Fatal	Konnektor neu starten

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
46037	Unable to set host name '%s' of connector. EXIT.		Technical	Fatal	
46038	Unable to uninstall LEKTR intranet routes'. This is fatal.		Technical	Fatal	
46039	Unable to install LEKTR intranet routes'. This is fatal.		Technical	Fatal	
46040	Unable to enforce rule stack 'lektr_intranet_routes'. This is fatal.		Technical	Fatal	

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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 antwortet nicht	Technical	Error	Konnektor neustarten
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46508	Could not perform the UDP bind to socket %s.	bind() an UDP-Socket nicht möglich	Technical	Error	Konnektor neu starten
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46516	ERROR: Unable to set MQTT to threaded.	MQTT-Broker reagiert nicht	Technical	Error	Konnektor neu starten
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
46533	error retrieving application image ID: %d	Zugriff auf die Informationen zu den aktuellen Softwareständen nicht möglich	Technical	Error	Konnektor neu starten
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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.
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.

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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.

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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.
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.

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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.
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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.
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.

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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 any-more	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 wer-den.	Technical	Error	TSL aktualisieren
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 vali-diert 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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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.
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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.
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.

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
47902	creating new DHCP configuration failed (rc=%d)	Fehlkonfiguration	Technical	Error	Konfiguration des DHCP-Servers prüfen und korrigieren

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
48106	error synchronizing system time to hardware clock (rc=%d)	Programmfehler oder Hardware Schaden (vermutlich RTC)	Technical	Error	Operation wiederholen

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
48117	error initializing channel to DNS	DNS Problem	Technical	Error	Operation wiederholen

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
48122	error synchronizing system time via NTP	Netzwerk Problem	Technical	Error	Verbindung zur TI prüfen, ggf. herstellen und 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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
48205	error converting local to UTC time: %s	Programmfehler	Technical	Error	Operation wiederholen
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 ref-clock, exiting	Programmfehler oder Hardware Schaden (vermutlich RTC)	Technical	Error	Operation wiederholen
48209	error reading system time: %s, ex-iting	Programmfehler	Technical	Error	Operation wiederholen
48300	current system is unknown	Programmfehler	Technical	Fatal	Wenn nicht durch Neustart zu lö-sen, Konnektor einschicken
48301	activating LVM volume group konnektor failed (rc=%d)	Programmfehler oder Hardware Schaden (vermutlich SSD)	Technical	Fatal	Wenn nicht durch Neustart zu lö-sen, Konnektor einschicken
48302	deactivating LVM logical volume %s failed (rc=%d)	LVM Volume Group ist bei der Deak-tivierung 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 lö-sen, 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 lö-sen, Konnektor einschicken

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
48306	mounting CFS %s to %s failed: %s	Programmfehler oder Hardware Schaden (vermutlich SSD)	Technical	Fatal	Wenn nicht durch Neustart zu lösen, Konnektor einschicken
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
48405	could not subscribe to topic '%s' (rc=%d): %s	MQTT-Broker reagiert nicht	Technical	Error	Operation wiederholen
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
48504	NK-component exceeding disc space	Speicherplatz für NK nicht ausreichend	Technical	Error	Softwareaktualisierung erneut ausführen
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
48511	Firmware group IDs do not match: installed %s, uploaded %s	Es dürfen nur Firmware gleicher group IDs installiert werden.	Technical	Error	Firmwareupdate prüfen; die neue Firmware kann nicht auf dieses spezielle Gerät installiert werden; ggf Support kontaktieren
48512	Hardware versions do not match: installed %s, uploaded %s	Die Hardware-Version des Konnektors passt nicht zur Hardware-Version des Updatepaketes.	Technical	Error	Firmwareupdate prüfen, ob nicht zum Beispiel eine Einbox-konnektorfirmware versucht wurde, auf einem Rechenzentrumskonnektor zu installieren (oder umgekehrt).
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
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

Code	Beschreibung	Mögliche Ursache	Typ	Level	Fehlerbehebung/ Weitere Angaben
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
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

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

16.10 Für Clientsysteme erreichbare Dienste

Für Clientsysteme werden folgende Dienste bereitgestellt:

- Dienstverzeichnisdienst

  Stellt Informationen über die Dienste, der Versionen und die Endpunkte der Dienste zur Verfügung

- Kartenterminaldienst

  Regelt die Kommunikation mit den angeschlossenen Kartenterminals, beispielsweise das Pairing (siehe Kapitel 10.1)

- Kartendienst

  Verwaltet Informationen über die Karten, die in die vom Konnektor verwalteten Kartenterminals gesteckt sind und kapselt alle Ereignisse und Operationen, die sich auf Karten beziehen.

- Systeminformationsdienst

  Stellt Basisdiensten, Fachmodulen und Clientsystemen sowohl aktiv (Push-Mechanismus) wie passiv (Pull-Mechanismus) Informationen zur Verfügung (siehe Kapitel 9.4.5)

- Verschlüsselungsdienst

  Bietet Funktionen zur Ver- und Entschlüsseln von Dokumenten an (siehe Kapitel 2.2.9)

- Signaturdienst

  Bietet Funktionen zum Signieren von Dokumenten und zum Prüfen von Dokumentensignaturen (siehe Kapitel 2.2.8)

- Zertifikatsdienst

  Bietet Funktionen zur Überprüfung der Gültigkeit von Zertifikaten

- Authentifizierungsdienst

  Bietet Funktionen für die externe Authentisierung (siehe Kapitel 2.2.10)

- Fachmodul VSDM

  Bietet Funktionen für die Bereitstellung und Pflege der VSD (siehe Kapitel 9.7.1)

- Fachmodul NDFM

  Ermöglicht es dem PS, über den Modularen Konnektor auf eine eGK zuzugreifen um Informationen für die Notfallversorgung zu speichern

- Fachmodul eMP/AMTS

  Ermöglicht es Clientsystemen, einen eMP und AMTS-relevante Daten auf der eGK zu speichern

- LDAP-Proxy

  Ermöglicht es Clientsystemen und Fachmodulen Daten aus dem Verzeichnisdienst der TI-Plattform (VZD) abzufragen

16.11 Anzeigen bei Fehlerzuständen

Folgende Fehlerzustände werden von den Betriebsanzeigen 60 Sekunden lang angezeigt, anschließend fährt das System herunter (siehe Kapitel 4.4.4).

LED(s)	Signal	Fehlerzustand
Update System, Remote	An Blinken	EC_Random_Generator_Not_Reliable
Service System, Remote	An Blinken	EC_Software_Integrity_Check_Failed
Service, Update System, Remote	An Blinken	EC_Security_Log_Not_Writable
VPN, SIS System, Remote	An Blinken	EC_Secure_KeyStore_Not_Available
VPN, SIS, Update System, Remote	An Blinken	EC_Firewall_Not_Reliable
VPN, SIS, Service System, Remote	An Blinken	EC_OTHER_ ERROR_ STATE(1)

Tabelle 22: Anzeige von Fehlerzuständen

16.12 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)

16.13 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. Die Informationen zu den Lizenzen sind ebenfalls Online über den KSR-Dienst verfügbar sowie Bestandteil des Offline Updates.

16.14 Security Guidance Fachmodul NFDM

16.14.1 Anwendungshinweise

Bei der Nutzung des Fachmoduls müssen folgende Hinweise beachtet werden:

- Die Nutzung der Funktionen des Fachmoduls ist nur mit einem HBA der Produktivumgebung erlaubt.
- Dafür darf nur ein gültiger HBA verwendet werden, d. h. ein HBA mit abgelaufenen Zertifkat darf nicht verwendet werden.
- Das Fachmodul darf nur auf einem nach PP-0098 zertifizierten Konnektor in einer sicheren Umgebung genutzt werden. Die in diesem Handbuch beschriebenen Maßnahmen müssen beachtet werden.

  Diese Maßnahmen stellen sicher, dass nur spezifikationsgemäße Zugriffe auf die Dienstschnittstellen des Fachmoduls erfolgen.

16.14.2 Konfiguration des Fachmoduls

Das Fachmodul NFDM kann direkt über die Management-Oberfläche des Konnektors konfiguriert werden.

Die zu konfigurierenden Einstellungen befinden sich im Menü **Diagnose** im Bereich **Administration**.

▶ Klicken Sie **Einstellungen** und passen Sie die Konfiguration im Abschnitt **NFDM** an.

Folgende Parameter können konfiguriert werden:

- **Loglevel**

  Dieser Parameter legt den Mindestschweregrad der zu protokollierenden Ereignisse fest. Debug ist dabei der niedrigste Level, Fatal der höchste Level.

  Default-Wert: Warning

  Mögliche Werte:

  - Debug
  - Info
  - Warning
  - Error
  - Fatal

- **Speicherdauer der Protokolleinträge**

  Dieser Parameter legt fest, nach Ablauf welcher Zeit (in Tagen) die gespeicherten Protokolldaten automatisch gelöscht werden.

  Default-Wert: 180

  Mögliche Werte: 10 - 365

- **Performance-Log**

  Dieser Parameter legt fest, ob das Performance-Protokoll geschrieben werden soll oder nicht. Das Aktivieren (Schalter blau unterlegt) führt dazu, dass das Performance-Protokoll geschrieben wird. Das Deaktivieren (Schalter grau unterlegt) stoppt das Schreiben des Performance-Protokolls.

  Default-Wert: false

  Mögliche Werte:

  - true
  - false

Das Leeren des Performance-Protokolls NFDM kann im Menü **Diagnose** im Bereich **Administration** angestoßen werden.

16.14.3 Versionsprüfung

Die Version des installierten Fachmoduls kann in der Bedienoberfläche des Modularen Konnektors im Menü **System** im Bereich **Version** überprüft werden.

▶ Klicken Sie **Details**, um Einzelheiten anzuzeigen.

Um zu überprüfen, ob das installierte Fachmodul auch von der gematik zugelassen ist, können auf der Webseite der gematik die zugelassenen Fachmodule angezeigt werden lassen. Eine Auflistung der zugelassenen secunet Fachmodule befindet sich unter:

`https://fachportal.gematik.de/zulassungen`

Durch einen Vergleich der angezeigten Version des installierten Fachmoduls mit den bei der gematik gelisteten Versionen kann überprüft werden, ob das Fachmodul zugelassen ist.

16.15 Security Guidance Fachmodul AMTS

16.15.1 Anwendungshinweise

Bei der Nutzung des Fachmoduls müssen folgende Hinweise beachtet werden:

- Die Nutzung der Funktionen des Fachmoduls ist nur mit einem HBA der Produktivumgebung erlaubt.
- Dafür darf nur ein gültiger HBA verwendet werden, d. h. ein HBA mit abgelaufenen Zertifkat darf nicht verwendet werden.
- Das Fachmodul darf nur auf einem nach PP-0098 zertifizierten Konnektor in einer sicheren Umgebung genutzt werden. Die in diesem Handbuch beschriebenen Maßnahmen müssen beachtet werden.

  Diese Maßnahmen stellen sicher, dass nur spezifikationsgemäße Zugriffe auf die Dienstschnittstellen des Fachmoduls erfolgen.

16.15.2 Konfiguration des Fachmoduls

Das Fachmodul AMTS kann direkt über die Management-Oberfläche des Konnektors konfiguriert werden.

Die zu konfigurierenden Einstellungen befinden sich im Menü **Diagnose** im Bereich **Administration**.

▶ Klicken Sie **Einstellungen** und passen Sie die Konfiguration im Abschnitt **AMTS** an.

Folgende Parameter können konfiguriert werden:

- **Loglevel**

  Dieser Parameter legt den Mindestschweregrad der zu protokollierenden Ereignisse fest. Debug ist dabei der niedrigste Level, Fatal der höchste Level.

  Default-Wert: Warning

  Mögliche Werte:

  - Debug
  - Info
  - Warning
  - Error
  - Fatal

- **Speicherdauer der Protokolleinträge**

  Dieser Parameter legt fest, nach Ablauf welcher Zeit (in Tagen) die gespeicherten Protokolldaten automatisch gelöscht werden.

  Default-Wert: 180

  Mögliche Werte: 10 - 365

- **Performance-Log**

  Dieser Parameter legt fest, ob das Performance-Protokoll geschrieben werden soll oder nicht. Das Aktivieren (Schalter blau unterlegt) führt dazu, dass das Performance-Protokoll geschrieben wird. Das Deaktivieren (Schalter grau unterlegt) stoppt das Schreiben des Performance-Protokolls.

  Default-Wert: false

  Mögliche Werte:

  - true
  - false

Das Leeren des Performance-Protokolls AMTS kann im Menü **Diagnose** im Bereich **Administration** angestoßen werden.

16.15.3 Versionsprüfung

Die Version des installierten Fachmoduls kann in der Bedienoberfläche des Modularen Konnektors im Menü **System** im Bereich **Version** überprüft werden.

- ▶ Klicken Sie **Details**, um Einzelheiten anzuzeigen.

Um zu überprüfen, ob das installierte Fachmodul auch von der gematik zugelassen ist, können auf der Webseite der gematik die zugelassenen Fachmodule angezeigt werden lassen. Eine Auflistung der zugelassenen secunet Fachmodule befindet sich unter:

`https://fachportal.gematik.de/zulassungen`

Durch einen Vergleich der angezeigten Version des installierten Fachmoduls mit den bei der gematik gelisteten Versionen kann überprüft werden, ob das Fachmodul zugelassen ist.

16.16 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
Konstruktionsstand 2.0.0 / 2.1.0

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 das bzw. die Sicherheitssiegel (siehe umseitig).

	Von (Name)	Datum
Sicherheitssiegel geprüft		

4. Notieren Sie die Seriennummern des bzw. der Sicherheitssiegel(s).

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.

Sicherheitssiegel prüfen

Der Einboxkonnektor (Konstruktionsstand 2.0.0) ist mit zwei Sicherheitssiegeln ausgestattet, die in Vertiefungen an den beiden Gehäuseseiten angebracht sind. Der Rechenzentrumskonnektor (Konstruktionsstand 2.1.0) ist mit einem Sicherheitssiegel an der Vorderseite des Gehäuses ausgestattet.

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

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

Anhang zum Betriebshandbuch Modularer Konnektor
Konstruktionsstand 2.0.0 / 2.1.0

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 Google Chrome ab Version 80
- 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

Das Geheimnis (mindestens 6 Buchstaben) dient der Identifikation des Leistungserbringers gegenüber einem DVO. Es wird für den Fall benötigt, dass der Leistungserbringer aufgrund fehlender Zugangsdaten keinen Zugriff mehr auf die grafische Bedienoberfläche des Modularen Konnektors hat und wahlweise einen vollständigen Werksreset oder einen Werksreset der Benutzerkonten durchführen möchte (siehe Bedienhandbuch).

Geheimnis:	

Teilen Sie das Geheimnis dem IT-Dienstleister vor Ort (DVO) mit.

	Von (Name)	Datum
Geheimnis mitgeteilt		

Inbetriebnahme

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.

.

16.17 Dokumentensicherheit

16.17.1 Einleitung

Dieses Dokument beschreibt Maßnahmen zur Validierung der Eingangsdaten bei XAdES, PAdES und CAdES Dokumentensignaturen.

Mit der Signaturdirektive (siehe Kapitel 16.18) wird der Funktionsumfang an den Außenschnittstellen des Signaturdienstes festgelegt. Dabei werden die vom Konnektor zugelassenen Signaturvarianten bestimmt. In diesem Dokument wird die Härtung der Schnittstellen beschrieben, die den Funktionsumfang indirekt einschränken. Auf die Verarbeitung von nonQES XAdES Signaturen wird verzichtet. Somit wird der Konnektor auf die ausschließliche Bearbeitung von QES XML Dokumenten eingeschränkt.

16.17.2 Allgemein

Zu signierende Dokumente, mit einer Größe über 25 MB werden abgelehnt

16.17.3 XAdES

Für XAdES QES NFDM wurde eine Härtung der verwendeten Schemata vorgenommen. Hierdurch wurden nichtbenötigte, sicherheitskritische Elemente so weit wie möglich entfernt. Beispielsweise Any-Attribute, URLs oder XSLT. Details sind den gehärteten Schema-Dateien zu entnehmen.

Bei der Erstellung von XML-Signaturen wird Canonical XML Version 1.1 ohne Kommentare verwendet (http://www.w3.org/TR/2008/REC-xml-c14n11-20080502/). Für XAdES Dokumentsignaturen wurden der XML-Parser und die Validierung des übergebenen XML-Schemas mit Hilfe von Framework-Parametern wie folgt gehärtet.

Die DocumentBuilderFactory des Xerces ist folgendermaßen konfiguriert:

```
documentBuilderFactory.setExpandEntityReferences(false);
documentBuilderFactory.setNamespaceAware(true);
documentBuilderFactory.setXIncludeAware(false);
documentBuilderFactory.setFeature("http://xml.org/sax/features/e xternal-general-entities", false);
documentBuilderFactory.setFeature("http://xml.org/sax/features/e xternal-parameter-entities", false);
```

```
documentBuilderFactory.setFeature("http://apache.org/xml/fe
ature s/disallow-doctype-decl", true);
documentBuilderFactory.setFeature("http://apache.org/xml/fe
ature s/nonvalidating/load-external-dtd", false);
```

Die SchemaFactory ist wie folgt konfiguriert:

```
schemaFactory.setAttribute(XMLConstants.ACCESS_EXTERNAL_DTD
, "");
schemaFactory.setAttribute(XMLConstants.ACCESS_EXTERNAL_STY
LESHEET, "");
```

Der Konnekor nutzt als XSLT-, XPath- und XQuery-Prozessor Apache java-santuario (xmlsec) und net.sf.saxon. Die TransformerFactory für saxon ist wie folgt konfiguriert:

```
transformerFactory.setFeature(XMLConstants.FEATURE_SECURE_P
ROCESSING, t rue);
```

Für XAdES werden folgende Einschränkungen im XML-Parser umgesetzt. Diese gelten für nonQES und QES, sofern nicht durch eine Signaturrichtlinie (z.B. NFDM) explizit zugelassen.

Wenn ein an den Signaturdienst übergebenes XML-Dokument diesen Anforderungen nicht genügt, werden je nach Fall entsprechende Bestandteile der Anfrage ignoriert (z.B. XPath, s.u.) oder die gesamte Anfrage mit einem Fehlercode abgelehnt.

- Das XML Dokument muss der Signaturrichtlinie QES - Notfalldaten-Management (NFDM) in der Version 1.4.0 vom 28.06.2019 genügen.
- Aus dem vorherigen Punkt folgt insbesondere, dass zu verifizierende XML Dokumente im <Tranforms>-Teil ihrer Referenzen keine XSL-Transformationen enthalten dürfen.
- Dokumente mit XPath-Ausdrücken werdenzwecks Interoperabilität nicht komplett abgelehnt. Insb. im <Signature> Anteil können XPath Ausdrücke zur Referenzierung der signierten Daten verwenden werden. Zur Verhinderung von Angriffen werden im TOE solche XPath Ausdrücke ignoriert (statt sie mit Fehler zu quittieren), und für die Verifikationsdurchführung durch einen eigenen, unkritischen XPath-Ausdruck ersetzt.
- Es dürfen keine XML Entities im XML-Document vorkommen. Insbesondere werden Document Type Definitions (DTD) abgelehnt

- Externe Referenzen werden nicht aufgelöst. Es sind nur Referenzen innerhalb des Dokumentes erlaubt.
- Die XML-Struktur (Anzahl der Elemente, Tiefe, Breite) ist durch die folgenden Maximalwerte begrenzt:
  - Die Gesamtanzahl der Elemente im XML-Dokument: Max. 50.000
  - Die Tiefe eines Zweiges im XML-Dokument: Max. 500
  - Die Breite eines Zweiges im XML-Dokument: Max. 500

  Wird eine dieser Grenzen vom XML-Dokument überschritten, dann wird die Operation mit Fehlercode 4022 (Das XML-Dokument ist nicht wohlgeformt) abgebrochen
- Entity Expansion wird nicht unterstützt.
- Alle ID-Attribute werden zusätzlich ermittelt. Sollte der Wert eines ID-Attributes mehr als einmal auftreten, wird die Nachricht verworfen.
- XPointer im URI-Attribut des Reference-Elements sind nicht erlaubt. Nach [SigDir] muss das URI-Attribut leer sein. (Keine Teilbaum-Signaturen erlaubt.)
- Alle signierten Elemente sind Bestandteil desselben DOM-Baumes. (Keine Teilbaum- Signaturen erlaubt.)
- Das Feature ds:RetrievalMethod wird nicht unterstützt.
- Für QES ist die Anzahl der verwendeten und eingebetteten Schemata durch die Signaturrichtlinien festgelegt.
- XInclude wird nicht unterstützt. Die Features schemaLocation und noNamespaceSchemaLocation werden nicht unterstützt.
- Bei der Signaturverifikation wird das ds:Reference Element für die Signature erst validiert, wenn der Signaturschlüssel validiert wurde und das ds:SignedInfo Element validiert wurde.

16.17.4 PAdES

Um gegen die in [VulnRepPDFSig] definierten Angriffstypen

- Universal Signature Forgery (USF)
- Incremental Saving Attack (ISA)
- Signature Wrapping Attack (SWA)

bei der Verifikation von Signaturen geschützt zu sein, werden vom PDF-Parser die in [VulnRepPDFSig], Kapitel 5 vorgeschlagenen Gegenmaßnahmen umgesetzt. Einschränkungen auf den Funktionsumfang sind dadurch nicht zu erwarten.

Erläuterung aus [VulnRepPDFSig]:

The Signature object (5 0 obj) contains information regarding the applied cryptographic algorithms for hashing and signing the document. It additionally includes a Contents parameter containing a hex-encoded PKCS7 blob, holding the certificates used to sign the document as well as the signature value.The ByteRange parameter defines which bytes of the PDF file are used as the hash input for the signature calculation and defines two integer tuples:

(a;b) : Beginning at byte offset a, the following b bytes are used as input for the hash calculation. Typically, a = 0 is used to indicate that the beginning of the file is used while a + b is the byte offset where the PKCS#7 blob begins.

(c;d) : Typically, byte offset c is the end of the PKCS#7 blob, while c + d points to the last byte off the PDF file.

In [VulnRepPDFSig], Kapitel 5 wird ein Pseudocode dargestellt, der die im Dokument beschriebenen Angriffe verhindert.

16.17.5 CAdES

Es werden zurzeit keine besonderen Härtungsmaßnahmen für CAdES umgesetzt.

16.18 Signaturdirektive

16.18.1 Einleitung

Im vorliegenden Kapitel werden die SignDocument und VerifyDocument Schnittstellen genauer beschrieben. Der Konnektor setzt verschiedene Signaturtypen und Signaturvarianten um und erlaubt es, optional sogenannte Signaturrichtlinien in Operationsaufruf anzugeben, die sicherstellen, dass entsprechend erzeugte Dokumenten-Siganturen einem vorgegebenen Schema folgen. Dabei wird der Begriff „Signaturrichtlinie“ in Rahmen der Konnektorevaluierung unterschiedlich verwendet:

- Signaturrichtlinie als im Operationsaufruf angegebene Richtlinie für genau diese Dokumenten-Signatur. Das entspricht der oben beschriebenen Auffassung einer Signaturrichtlinie
- Signaturrichtlinie als allgemeine funktionale Einschränkung der Konnektor-Schnittstelle.

Dieses Kapitel beschreibt letztere „Signaturrichtlinie“. Zur Abgrenzung der Begrifflichkeiten wird im Folgenden von einer Signaturdirektive gesprochen.

In diesem Kapitel wird der Funktionsumfang an den Außenschnittstellen des Signaturdienstes beschrieben. Die Härtung der Schnittstellen (z.B. Härtung des XML-Parsers) wird in Kapitel 16.17 beschrieben.

Der Konnekor unterstützt zum Signieren und Verifizieren Algorithmen und Verfahren gemäß [gemSpec_Krypt].

16.18.2 Signaturdirektive SignDocument

16.18.2.1 Signaturtypen

Der Konnektor bietet die Erstellung folgender Signaturtypen an:

- XML-Signatur
- CMS-Signatur
- S/MIME-Signatur
- PDF-Signatur

Der Signaturtyp wird über folgenden Parameter bestimmt:

XML-Element oder –Attribut (XPath):	Beschreibung:	Werte:
/SIG:SignDocument/ SIG:SignRequest/ SIG:OptionalInputs/ SIG:SignatureType	Durch dieses in [OASIS-DSS] (Abschnitt 3.5.1) beschriebene Element kann der generelle Typ der zu erzeugenden Signaturen spezifiziert werden.	Siehe Tabelle 23: Signaturtypen

Signaturtyp	Wert
XML-Signatur	urn:ietf:rfc:3275
CMS-Signatur	urn:ietf:rfc:5652
S/MIME-Signatur	urn:ietf:rfc:5751
PDF-Signatur	http://uri.etsi.org/02778/3

Tabelle 23: Signaturtypen

Andere Signaturtyp-Angaben führen zu einer Fehlermeldung 4111 (Ungültiger Signatur-typ oder Signaturvariante). Insgesamt werden folgende Dokumentenformate je Signaturformate/-verfahren unterstützt:

Signaturformat / Signaturverfahren	Dokumentformat
XAdES	XML
PAdES	PDF/A (application/pdf-a gemäß [ISO 19005])
CAdES	XML PDF/A Text (text/pain) TIFF (image/tiff) Binär (nur bei nonQES)
S/MIME	MIME-Nachricht (nur bei nonQES) mit allen für CAdES zugelassenen Dokumentenformaten

Tabelle 24: Dokumentenformate

S/MIME Signaturen sind CMS-Signaturen mit einer entsprechenden S/MIME Vor- und Nachbehandlung. Ist das übergebene Dokument keine MIME-Nachricht, so wird der Fehler 4111 zurückgeliefert. Im S/MIME-Nachbereitungsschritt wird das erzeugte CMS-Objekt in eine MIME-Nachricht vom Typ „application/pkcs7-mime“ eingebettet.

Die im Folgenden beschriebenen allgemeinen Festlegungen gelten für die jeweiligen Signaturtypen und sind nicht auf eine Signaturvariante beschränkt.

CMS-Signaturen

Die SignDocument Operation erlaubt es, mit dem dss:properties Element im SOAP-Request für CMS-Signaturen zusätzliche signierte und unsignierte Eigenschaften (Properties) bzw. Attribute in die Signatur einzubringen (CMSAttribute), siehe [gemSpec_Kon].

Die folgenden Attribute werden dabei vom Konnektor nicht ausgewertet, sondern ignoriert. Dabei wird keine Fehlermeldung ausgegeben, sondern die Operation ausgeführt ohne diese Attribute im SOAP-Request zu berücksichtigen.

XML-Element oder –Attribut (XPath):	Werte:
/SIG:SignDocument/SIG:SignRequest/ SIG:OptionalInputs/dss:Properties/ SignedPropeties/Property/Value/CMSAttribute und /SIG:SignDocument/SIG:SignRequest /SIG:OptionalInputs/dss:Properties /UnsignedProperties/Property/Value /CMSAttribute	Siehe [gemSpec_Kon], TAB_KON_065. Folgende Attribute werden vom Konnektor ignoriert: ▪ ContentType ▪ SigningTime ▪ MessageDigest ▪ SigningCertificate ▪ SigningCertificateV2 ▪ CMSAlgorithmprotection

16.18.2.2 Signaturvarianten

Folgende Signaturvarianten sind zulässig:

Signaturvarianten				Einsatzbereich		
Signatur-verfahren	Signatur-variante	WAS wird signiert?	WO wird die Signatur abgelegt?	nonQES	QES Außenschnittstelle	QES Fachmodulschnittstelle
XAdES	detached	beliebiges (Binär)-Dokument	Außerhalb des Dokuments in der SignResponse	Nein	Nein	Nein
XAdES	detached	gesamtes Input XML-Dokument (=Root-Element mit Subelementen)	Außerhalb des Dokuments in der SignResponse	Nein	Nein	Nein
XAdES	detached	ausgewähltes nicht Root-Element mit Subelementen im Input XML-Dokument	Außerhalb des Dokuments in der SignResponse	Nein	Nein	Nein
XAdES	detached	ausgewähltes nicht Root-Element mit Subelementen im Input XML-Dokument	Innerhalb des Dokuments, aber Außerhalb des signierten Subbaums	Nein	Ja (NFDM)	Ja (NFDM)
XAdES	enveloped	gesamtes Input XML-Dokument (= Root-Element mit Subelementen)	Als direktes Child des Root-Elements	Nein	Nein (Bedingt aber keine Richtlinie)	Nein (Bedingt aber keine Richtlinie)
XAdES	enveloped	ausgewähltes nicht Root- Element mit Subelementen im Input XML-Dokument	Als direktes Child des ausgewählten Elements	Nein	Nein	Nein (Bedingt aber keine Richtlinie)
XAdES	enveloping	gesamtes Input XML-Dokument (=Root-Element mit Subelementen)	Im Dokument, das Root-Element umschließend	Nein	Nein (Bedingt aber keine Richtlinie)	Nein (Bedingt aber keine Richtlinie)
XAdES	enveloping	ausgewähltes nicht Root- Element mit Subelementen im Input XML-Dokument	Im Dokument, das ausgewählte Element umschließend	Nein	Nein	Nein
CAdES	detached	gesamtes Binärdokument	Außerhalb des Dokuments in der SignResponse	Ja	Ja	Ja

CAdES	enveloping	gesamtes Binärdokument	innerhalb des CMS- Dokuments	Ja	Ja	Ja
PAdES	-	Gesamtes PDF-Dokument	Im PDF-Dokument	Ja	Ja	ja

Tabelle 25: Signaturvarianten

Ja: Die Signaturvariante ist für den Einsatzbereich erlaubt.

Ja (NFDM): Die Signaturvariante ist für den Einsatzbereich erlaubt, da die im Konnektor integrierte Signaturrichtlinie NFDM diese Variante explizit fordert.

Nein: Die Signaturvariante ist für den Einsatzbereich nicht erlaubt.

Nein (Bedingt aber keine Richtlinie): Die Signaturvariante ist für den Einsatzbereich nicht erlaubt denn es existiert keine im Konnektor integrierte Signaturrichtlinie die diese Variante explizit fordert.

Die Spalten mit gelber Kopfzeile definieren die Signaturvarianten, die mit grauer, den Einsatzbereich. Beim Einsatzbereich wird zwischen nonQES und QES unterschieden und im Fall QES nach der Bereitstellung an der Außenschnittstelle oder intern für Fachmodule.

Die benötigten Signaturvarianten werden für XAdES über die Aufrufparameter `dss:IncludeObject` und `dss:SignaturePlacement` gemäß [OASIS-DSS] gesteuert. Für CAdES erfolgt die Steuerung welche Signaturvariante gewählt wird, über den Aufrufparameter `SIG:IncludeEContent`.

Signaturvarianten nonQES

Zusammengefasst reduziert sich die Tabelle aus Kapitel 2.2 für nonQES zu:

Signaturvarianten nonQES				**Einsatzbereich**
Signatur-verfahren	Signatur-variante	WAS wird signiert?	WO wird die Signatur abgelegt?	nonQES
CAdES	detached	gesamtes Binärdokument	Außerhalb des Dokuments in der SignResponse	Ja
CAdES	enveloping	gesamtes Binärdokument	innerhalb des CMS- Dokuments	Ja
PAdES	-	gesamtes PDF-Dokument	Im PDF-Dokument	Ja

Tabelle 26: Signaturvarianten nonQES

Signaturvarianten QES

Zusammengefasst reduziert sich die Tabelle aus Kapitel 2.2 für QES zu:

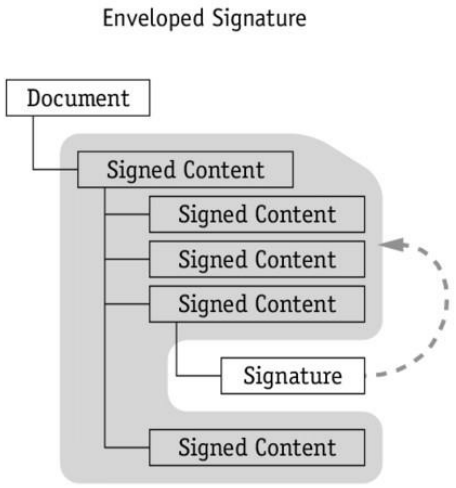
Signaturvarianten QES				**Einsatzbereich**
Signatur-verfahren	Signatur-variante	WAS wird signiert?	WO wird die Signatur abgelegt?	QES
XAdES	detached	Ausgewähltes nicht Root- Element mit Subelementen im Input XMLDokument	Innerhalb des Dokuments, aber außerhalb des signierten Subbaums	Ja (NFDM)
CAdES	detached	gesamtes Binärdokument	Außerhalb des Dokuments in der SignResponse	Ja
CAdES	enveloping	gesamtes Binärdokument	innerhalb des CMS-Dokuments	Ja
PAdES	-	gesamtes PDF-Dokument	Im PDF-Dokument	Ja

Tabelle 27: Signaturvarianten QES

Enveloped

XML Signature Syntax and Processing Version 1.1:

The signature is over the XML content that contains the signature as an element. The content provides the root XML document element. Obviously, enveloped signatures must take care not to include their own value in the calculation of the Signature Value.

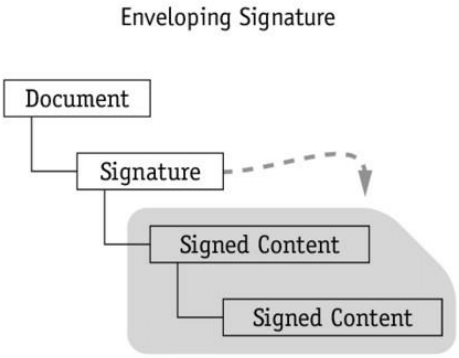


Im Modularen Konnektor wird diese Signaturvariante nicht erlaubt.

Enveloping

XML Signature Syntax and Processing Version 1.1:

> The signature is over content found within an Object element of the signature itself. The Object (or its content) is identified via a Reference (via a URI fragment identifier or transform).



Im Modularen Konnektor erlaubte Signaturvarianten sind:

Signatur-verfahren	Signatur-variante	Signaturinput	Signaturausgabe	**Einsatzbereich**
CAdES	enveloping	gesamtes Binärdokument	innerhalb des CMS- Dokuments	QES, nonQES

CAdES (QES, nonQES)

Die Steuerung der CAdES enveloping Signatur erfolgt über den Parameter `SIG:IncludeEContent`.

Die Verwendung dieses Parameters bei anderen Signaturtypen als CMS führt zu einem Fehler 4111.

Wird bei einer CAdES Signatur zusätzlich der Parameter dss:SignaturePlacement angegeben, wird die Operation ausgeführt ohne diesen Parameter auszuwerten. Im Ergebnis der Operation wird Warning 4197 zurückgegeben.

Enthält <SIG:Document> ein Attribut `RefURI` ungleich "", führt dies zu einem Fehler 4000.

Relevante Parameter:

XML-Element oder –Attribut (XPath):	Beschreibung:	Werte:
/SIG:SignDocument/SIG:SignRequest/ SIG:OptionalInputs/SIG:IncludeEContent	Durch dieses in [OASIS-DSS] (Abschnitt 3.5.7), definierte Element kann bei einer CMS-basierten Signatur das Einfügen des signierten Dokumentes in die Signatur angefordert werden.	true
/SIG:SignDocument/SIG:SignRequest/ SIG:Document /@RefURI	Referenziert den zu signierenden Teil des Dokumentes	RefURI="" oder kein RefURI Attribut

OCSP-Responses

OCSP-Responses können bei QES eingebettet werden.
Das Element `SIG:IncludeRevocationInfo` wird daher für QES ausgewertet.

Bei nonQES wird für `SIG:IncludeRevocationInfo = true` der Fehler 4000 geworfen.

XML-Element oder –Attribut (XPath):	Beschreibung:	Werte:
/SIG:SignDocument/SIG:SignRequest/ SIG:IncludeRevocationInfo	Durch diesen verpflichtenden Schalter kann der Aufrufer die Einbettung von zum Zeitpunkt der Signaturerstellung vorliegenden Sperrinformationen anfordern. Es wird ausschließlich die zu erstellende Signatur betrachtet, d.h. es erfolgt keine Einbettung von Sperrinformationen für bereits enthaltene Signaturen.	QES: false oder true nonQES: false

Parallel- und Gegensignaturen

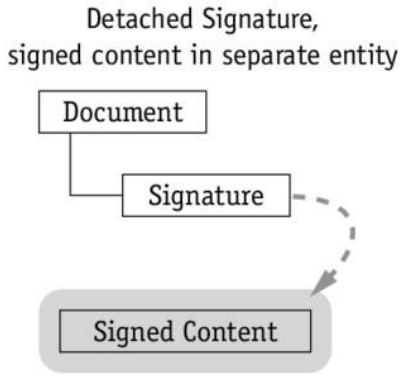
XML-Element oder –Attribut (XPath):	Beschreibung:	Werte:
/SIG:SignDocument/SIG:SignRequest/ SIG:OptionalInputs/ dss:ReturnUpdatedSignature	Durch dieses in [OASIS-DSS] (Abschnitt 4.5.8) definierte Element kann eine übergegebene XML- oder CMS-Signatur mit zusätzlichen Informationen und Signaturen (Parallel- und Gegensignaturen) versehen werden.	http://ws.gematik.de/ conn/sig/sigupdate/ parallel oder http://ws.gematik.de/ conn/sig/sigupdate/ counter/ documentexcluding

Bei anderen Werten wird der Fehler 4111 oder 4000 zurückgeliefert.

Detached

XML Signature Syntax and Processing Version 1.1:

The signature is over content external to the Signature element, and can be identified via a URI or transform. Consequently, the signature is "detached" from the content it signs. This definition typically applies to separate data objects, but it also includes the instance where the Signature and data object reside within the same



XML document but are sibling elements.

Die Signatur wird außerhalb des Dokuments in der `SignResponse` zurückgegeben.

Im EVG erlaubte Signaturvarianten sind:

Signatur-verfahren	Signatur-variante	Signaturinput	Signaturausgabe	**Einsatzbereich**
CAdES	detached	gesamtes Binärdoku-ment	Außerhalb des Doku-ments in der Sign-Response	QES, nonQES

CAdES (QES, nonQES)

Die Steuereung der CAdES Detached Signatur erfolgt über das Weglassen des Parameters `dss:IncludeEContent` (siehe auch Kapitel 2.2.3.2).

Enthält <SIG:Document> ein Attribut `RefURI` ungleich "" führt dies zu einem Fehler 4000.

OCSP-Responses

OCSP-Responses können bei QES eingebettet werden.
Das Element `SIG:IncludeRevocationInfo` wird daher für QES ausgewertet.

Bei nonQES wird für `SIG:IncludeRevocationInfo = true` der Fehler 4000 geworfen.

XML-Element oder –Attribut (XPath):	**Beschreibung:**	**Werte:**
/SIG:SignDocument/SIG:SignRequest/ SIG:IncludeRevocationInfo	Durch diesen verpflichtenden Schalter kann der Aufrufer die Einbettung von zum Zeitpunkt der Signaturerstellung vorlie-gendenSperrinformationen an-fordern. Es wird ausschließlich die zu erstel-lende Signatur betrachtet, d.h. es erfolgt keine Einbettung von Sperrinformationen für bereits enthaltene Signaturen.	QES: false oder true nonQES: false

Parallel- und Gegensignaturen

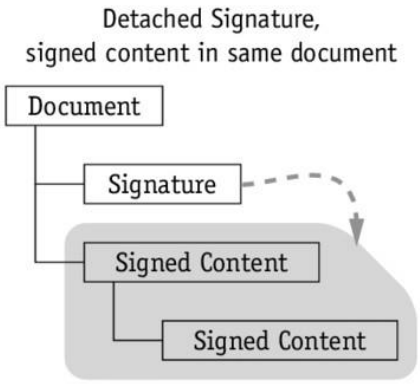
Parallel- und Gegensignaturen werden für CMS Detached Signaturen nicht unterstützt.

Wird ein `SIG:ReturnUpdatedSignature` Element übergeben, so wird der Fehler 4111 oder 4000 zurückgeliefert.

Detached in same document

XML Signature Syntax and Processing Version 1.1:

The signature is over content external to the Signature element, and can be identified via a URI or transform. Consequently, the signature is "detached" from the content it signs. This definition typically applies to separate data objects, but it also includes the instance where the Signature and data object reside within the same XML document but are sibling elements.



Im EVG erlaubte Signaturvarianten sind:

Signatur-verfahren	Signatur-variante	Signaturinput	Signaturausgabe	**Einsatzbereich**
XAdES	detached	ausgewähltes nicht Root-Element mit Subelementen im Input XML-Dokument	Innerhalb des Dokuments, aber außerhalb des signierten Subbaums	NFDM (QES)

XAdES (NFDM)

Die Steuereung der XAdES detached Signatur erfolgt über den Parameter dss:SignaturePlacement.

Diese Signaturvariante ist nur bei Angabe der NFDM Signturichtlinie erlaubt. Damit sind die erlaubten Paramter der SignDocument bzw. VerifyDocument Operation durch [gemRL_QES_NFDM] vorgegen.

Im Folgenden sind zum Vergleich mit den anderen Signaturvarianten relevante Paramter aufgeführt. Die Liste ist dabei nicht vollständig.

Relevante Parameter

XML-Element oder –Attribut (XPath):	Beschreibung:	Werte:
/SIG:SignDocument/SIG:SignRequest/ SIG:OptionalInputs/ sp:GenerateUnderSignaturePolicy/ sp:Sign aturePolicyIdentifier	Angabe der Signaturrichtlinie	urn:gematik:fa:sak:nf dm:r1:v1
/SIG:SignDocument/SIG:SignRequest/ SIG:Document/@ID	Dokumentbe-zeichner des zu signierdenden Dokumentes	Platzhalter für Dokument-bezeichner NFD_DOC_ID
/SIG:SignDocument/SIG:SignRequest/ SIG:Document/@RefURI	Angabe des zu Signierenden Teils.	Der Wert muss überein-stimmen mit dem Wert des Attributes ID des Elementes NFD:Notfalldaten
/SIG:SignDocument/SIG:SignRequest/ SIG:OptionalInputs/ dss:SignaturePlacement/ @WhichDocument	Identifies the in-put document which the signa-ture will be in-serted into	NFD_DOC_ID
/SIG:SignDocument/SIG:SignRequest/ SIG:OptionalInputs/ dss:SignaturePlacement/ @CreateEnvelopedSignature	If this is set to true a reference having an envel-oped signature transform is cre-ated.	false
/SIG:SignDocument/SIG:SignRequest/ SIG:OptionalInputs/ dss:SignaturePlacement/XPathFirstChild Of	Identifies an el-ement, in the XML input doc-ument, which the signature will be inserted as the first child of. The signature is placed immedi-ately after the start tag of the specified ele-ment.	"/*[local-name()='NFD_Docu ment']/*[local-Name()='SignatureAr zt']"

OCSP-Responses

OCSP-Responses müssen bei NFDM eingebettet werden.

XML-Element oder –Attribut (XPath):	Beschreibung:	Werte:
/SIG:SignDocument/ SIG:SignRequest/ SIG:IncludeRevocationInfo	Durch diesen verpflichtenden Schalter kann der Aufrufer die Einbettung von zum Zeitpunkt der Signaturerstellung vorliegenden Sperrinformationen anfordern. Es wird ausschließlich die zu erstellende Signatur betrachtet, d.h. es erfolgt keine Einbettung von Sperrinformationen für bereits enthaltene Signaturen.	true

Parallel- und Gegensignaturen

Parallel- und Gegensignaturen werden über das im Schnittstellenaufruf optionale Element `/SIG:SignDocument/SIG:SignRequest/SIG:OptionalInputs/dss:ReturnUpdatedSignature` angefragt.

Entsprechend [NFDM] ist dieses Element nicht vorgesehen und Parallel/-Gegensignaturen werden mit dem Fehler 4111 abgelehnt.

PDF Signaturen (QES, nonQES)

Signatur-verfahren	Signatur-variante	Signaturinput	Signaturausgabe	**Einsatzbereich**
PAdES	-	gesamtes PDF-Dokument	Im PDF-Dokument	nonQES, QES

Die Signatur wird als Incremental Update gemäß [PDF/A-2] Kapitel 7.5.6 an das Dokument angefügt.

OCSP-Responses

OCSP-Responses werden bei PAdES nicht eingebettet.

Bei `SIG:IncludeRevocationInfo = true` wird daher Fehler 4000 zurückgegeben.

XML-Element oder –Attribut (XPath):	Beschreibung:	Werte:
/SIG:SignDocument/ SIG:SignRequest/ SIG:IncludeRevocationInfo	Durch diesen verpflichtenden Schalter kann der Aufrufer die Einbettung von zum Zeitpunkt der Signaturerstellung vorliegenden Sperrinformationen anfordern. Es wird ausschließlich die zu erstellende Signatur betrachtet, d.h. es erfolgt keine Einbettung von Sperrinformationen für bereits enthaltene Signaturen. Für PDF-Signaturen werden keine Sperrinformationen eingebettet.	false

Parallel- und Gegensignaturen

Parallele Signaturen werden nicht angeboten. Gegensignaturen werden nicht angeboten.

Wird ein `dss:ReturnUpdatedSignature` Element angegeben, wird Fehler 4111 zurückgeliefert

S/MIME Signaturen (nonQES)

S/MIME Signaturen sind CMS-Signaturen mit einer entsprechenden S/MIME Vor- und Nachbehandlung. Für S/MIME ist folgende Signaturvariante erlaubt:

Signatur-format	Signatur-variante	Signaturinput	Signaturausgabe	**Einsatzbereich**
S/MIME	enveloping	gesamtes Binärdokument	innerhalb des CMS- Dokuments	nonQES

Ist das übergebene Dokument keine MIME-Nachricht, so wie der Fehlerf 4111 zurückgeliefert.

Wird im Aufruf kein `SIG:IncludeEContent` Element übergeben, so wird Fehler 4111 zurückgeliefert. Es gelten die gleichen Einschränkungen wie unter Kapitel 2.2.3.2.

16.18.3 Siganturderiktive VerifyDocument

Es werden für die Verifikation von Signaturen nur Signaturen mit Signaturtypen und Signaturvarianten unterstützt, die auch vom Konnektor erstellt werden können. Enthalten Signaturen zur Verifikation andere Signaturtypen oder Signaturvarianten, wird der Fehler 4000 zurückgeliefert.

Das Einbetten von OCSP-Responses wird für nonQES Signaturen und generell für PDF- Signaturen nicht unterstützt. Wird in diesem Fall ein Element `SIG:IncludeRevocationInfo = true` übergeben, wird die Warnung 4261 in die Antwort aufgenommen.

XML-Element oder –Attribut (XPath):	Beschreibung:	Werte:
/SIG:SignDocument/ SIG:SignRequest/ SIG:IncludeRevocationInfo	Durch diesen verpflichtenden Schalter kann der Aufrufer die Einbettung von zum Zeitpunkt der Signaturerstellung vorliegenden Sperrinformationen anfordern. Es wird ausschließlich die zu erstellende Signatur betrachtet, d.h. es erfolgt keine Einbettung von Sperrinformationen für bereits enthaltene Signaturen.	QES: false oder true nonQES: false PDF: false

16.19 Verschlüsselungsdirektive

16.19.1 Einleitung

Der Konnektor bietet durch den Verschlüsselungsdienst den Clientsystemen die Möglichkeit Dokumente hybrid zu ver- und entschlüsseln. In diesem Zusammenhang wird analog zur Signaturrichtlinie des Signaturdienstes (siehe Kapitel 16.18) der Begriff „Verschlüsselungsrichtlinie“ in Rahmen der Konnektorevaluierung unterschiedlich verwendet:

1. Verschlüsselungsrichtlinie als im Operationsaufruf angegebene Richtlinie für genau diese Dokumenten-Verschlüsselung.
2. Verschlüsselungsrichtlinie als allgemeine funktionale Einschränkung der Konnektor-Schnittstelle.

Eine Verschlüsselungsrichtlinie nach 1. ist in [gemSpec_Kon] nicht spezifiziert und wird von Konnektor nicht unterstützt. Es können keine solche Verschlüsselungsrichtlinien im Operationsaufruf angegeben werden.

Dieses Kapitel beschreibt letztere „Verschlüsselungsrichtlinie“. Zur Abgrenzung der Begrifflichkeiten wird im Folgenden von einer Verschlüsselungsdirektive gesprochen.

In diesem Kapitel wird der Funktionsumfang an den Außenschnittstellen des Verschlüsselungsdienstes beschrieben. Die Härtung der Schnittstellen (z.B. Härtung des XML-Parsers) wird in Kapitel 16.17 beschrieben.

Der Konnektor unterstützt zum hybriden Ver- und Entschlüsseln von Dokumenten die Algorithmen und Verfahren gemäß [gemSpec_Krypt], Kapitel 3.1.4 und 3.1.5.

16.19.2 Verschlüsselungsdirektive EncryptDocument

Der Konnektor bietet die Dokumentenverschlüsselung folgende Verschlüsselungsverfahren („EncryptionType“) an:

- CMS: hybride Ver-/Entschlüsselung nach CMS ([RFC5652])
- XMLEnc: hybride Ver-/Entschlüsselung von XML-Dokumenten ([XMLEnc])
- S/MIME: hybride Ver-/Entschlüsselung von MIME-Dokumenten ([S/MIME])

Das Verschlüsselungsverfahren wird über folgenden Parameter bestimmt:

XML-Element oder -Attribut (XPath)	Beschreibung	Werte
/CRYPT:EncryptDocument/ CRYPT:OptionalInputs/CRYPT: EncryptionType	Durch dieses Element kann das Verschlüsselungsver- fahren der zu verschlüs- selnden Dokumente spezifiziert werden.	Siehe Tabelle 28

Verschlüsselungsverfahren	Wert
XMLEnc	http://www.w3.org/TR/xmlenc-core/
CMS	urn:ietf:rfc:5652
S/MIME	urn:ietf:rfc:5751

Tabelle 28: Verschlüsselungsverfahren

Andere Angaben führen zu einer Fehlermeldung 4058 (Aufruf nicht zulässig).

Insgesamt werden folgende Dokumentenformate für die Verschlüsselungsverfahren unterstützt:

Verschlüsselungsverfahren	Dokumentformat
XMLEnc	XML
CMS	XML PDF/A Text (text/plain) TIFF (image/tiff) Binär
S/MIME	MIME-Nachricht (nur bei nonQES) mit allen für CAdES zugelassenen Dokumentenformaten

S/MIME Signaturen sind CMS-Signaturen mit einer entsprechenden S/MIME Vor- und Nachbehandlung. Ist das übergebene Dokument keine MIME-Nachricht, so wird der Fehler 4111 zurückgeliefert. Im S/MIME-Nachbereitungsschritt wird das erzeugte CMS-Objekt in eine MIME-Nachricht vom Typ „application/pkcs7-mime“ eingebettet.

Im Folgenden wird auf einzelne Punkte der Schnittstelle eingegangen. Dabei handelt es sich nicht um Abweichungen zu [gemSpec_Kon], sondern um Klarstellungen zur Umsetzung.

16.19.2.1 Allgemein

Die Schnittstelle EncryptDocument wird entsprechen [gemSpec_Kon] (inkl. Aller relevanten Errata) umgesetzt. Darüber hinaus gibt es keine weiteren Einschränkungen.

16.19.2.2 CRYPT:RecipientKeys

Das Element CRYPT:RecipientKeys gibt an, mit welchen Verschlüsselungszertifikat das Übergebene Dokument verschlüsselt werden soll:

XML-Element oder –Attribut (XPath):	Beschreibung:	Werte:
/SIG:EncryptDocument/ CRYPT:RecipientKeys	Das RecipientKeys-Element identifiziert die Empfänger der zu verschlüsselnden Nachricht über X.509-Zertifikate (öffentliche Schlüssel). Quelle für die Zertifikate kann eine gesteckte Karte sein, die per CertificateOnCard-Element referenziert wird, oder der Aufrufer, der X.509-Zertifikate im Certificate-Element übergibt.	Element CRYPT:CertificateOnCard oder Element CRYPT:Certificate

Für die Verschlüsselung werden die folgenden Karten unterstützt: HBAx und SM-B. Die Operation EncryptDocument erlaubt NICHT das Verschlüsseln mit der eGK.

16.19.2.3 CRYPT:Element

Dieses Element ist nur relevant für XML-Dokumente. Entsprechend gemErrata_2_Kon_PTV3 (C_6844) ist Teilbaumverschlüsselung nicht erlaubt. Für alle Dokumenttypen wird immer das gesamte Dokument verschlüsselt.

Der Parameter CRYPT:Element wird daher vom Konnektor nicht ausgewertet.

16.19.3 Verschlüsselungsdirektive DecryptDocument

Es werden für die Entschlüsselung von Dokumenten nur Verfahren unterstützt, die auch vom Konnektor bei der Verschlüsselung umgesetzt werden können, siehe dazu die Beschreibungen in Kapitel 16.19.2.1.

Im Folgenden wird auf einzelne Punkte der Schnittstelle eingegangen. Dabei handelt es sich nicht um Abweichungen zu [gemSpec_Kon], sondern um Klarstellungen zur Umsetzung.

16.19.3.1 Allgemein

Die Schnittstelle EncryptDocument wird entsprechen [gemSpec_Kon] (inkl. Aller relevanten Errata) umgesetzt. Darüber hinaus gibt es keine weiteren Einschränkungen.

16.19.3.2 CRYPT:PrivateKeyOnCard

Für die Entschlüsselung wird ein asymmetrischer Schlüssel zu einem X.509v3-Zertifikat genutzt. Dieses Zertifikat und der Schlüssel müssen von einer Karte kommen.

XML-Element oder –Attribut (XPath):	Beschreibung:	Werte:
/CRYPT:DecryptDocument/ CRYPT:PrivateKeyOnCard	Identifiziert die zu verwendende Karte mit dem (privaten) Schlüssel. Es werden die folgenden Karten unterstützt: HBAx und SM-B. Das Entschlüsseln mit der eGK wird NICHT unterstützen.	Child-Elemente CONN:Cardhande und CRYPT:KeyReference auf HBAx oder SM-B

Referenzliste

[gemSpec_Kon]	gematik: Spezifikation Konnektor, Version 5.4.0
[gemRL_QES_NFDM]	gematik: Signaturrichtlinie QES Notfalldaten-Management (NFDM), Version 1.2.0
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 2.11.0
[PDF/A-2]	ISO 19005-2:2011 – Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2)
[OASIS-DSS]	OASIS: Digital Signature Services
[ISO 19005]	ISO 19005-1:2005, Document management - Electronic document file format for long-term preservation
[BSI TR-03116-1]	Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur, Version 3.19, 04.12.2015, Bundesamt für Sicherheit in der Informationstechnik (BSI)
[RFC5652]	Internet Engineering Task Force (IETF) Request for Comments: 5652 Cryptographic Message Syntax (CMS), September 2009
[XMLEnc]	W3C Recommendation XML Encryption Syntax and Processing, Version 1.1
[S/MIME]	Internet Engineering Task Force (IETF) Request for Comments: 5751 Secure/Multipurpose Internet Mail Extensions (S/MIME), Version 3.2.
[VulnRepPDFSig]	Ruhr-Universität Bochum: Vulnerability Report - Attacks bypassing the signature validation in PDF, November 08, 2018 Chair for Network and Data Security
[PP-0097]	Common Criteria Schutzprofil (Protection Profile), Schutzprofil 1: Anforderungen an den Netzkonnektor, Version 1.6.4 vom 17.03.2020, Bundesamt für Sicherheit in der Informationstechnik
[PP-0098]	Common Criteria Schutzprofil (Protection Profile), Schutzprofil 2: Anforderungen an den Konnektor, Version 1.5.4 vom 17.03.2020,

Bundesamt für Sicherheit in der Informationstechnik

Glossar

A

Akteure	Personen oder Systeme, für die Zugriffsrechte zur TI definiert sind.
AMTS	Arzneimitteltherapiesicherheit
Anbieter	Rechtlich und wirtschaftlich verantwortliche Organisation für ein zentrales Produkt der TI. Anbieter können Aufgaben an einen Betreiber delegieren. Anbieter unterscheiden sich von den Herstellern von dezentralen Produkten der TI dadurch, dass das verantwortete Produkt kein physisches Gerät oder Software, sondern einen IT-Service darstellt.
Anbieter-Support	Supportfunktion, geleistet durch den produktverantwortlichen Anbieter. Die Koordination des Anbietersupports erfolgt durch die Service Provider.
Anbieterzulassung	Anbieter werden nach § 291b Abs. 1b Satz 5 SGB V von der gematik zugelassen. Die Anbieterzulassung ist Voraussetzung für die Durchführung des operativen Betriebs von Komponenten und Dienste im Rahmen der Telematikinfrastruktur.
Anbindungsmodus	Betriebsmodus des Modularen Konnektors, der bestimmt, ob der Betrieb am Übergangspunkt zum IAG oder innerhalb des lokalen Netzwerks erfolgt (siehe Kapitel 10.2.1.2).
Anwender	Natürliche Personen oder Organisationen, die TI-Services nutzen. Als Anwender werden dabei sowohl diejenigen Akteure bezeichnet, die tatsächlich mit dem IT-System arbeiten, als auch diejenigen, die eine Nutzung veranlassen und insofern für die bestimmungsgemäße Nutzung der Systeme verantwortlich sind.
Anwendung	Softwaresystem zur Unterstützung fachlicher Prozesse. Eine Fachanwendung zeichnet sich durch die Einhaltung der Vorgaben der Telematikinfrastruktur und die entsprechende Zulassung aus.
Anwendungskonnektor	Funktionaler Teil des Modularen Konnektors, der anwendungsnahe Basisdienste und Fachmodule zur Nutzung durch Clientsysteme bietet.

Aufrufkontext	Eindeutige Kombination aus Clientsystem, Mandant und Arbeitsplatz (siehe Kapitel 9.3.6)

B

Basisdienste	Leistungen der TI-Plattform zur Unterstützung der Fachanwendungen mit allen nötigen technischen und organisatorischen Anteilen.
Benutzerrolle	Typ des Benutzerkontos eines Administrators. Die Benutzerrolle bestimmt die Berechtigungen für den Zugriff auf den Modularen Konnektor (siehe Kapitel 9.1.3).
Berechtigtenkarte	Heilberufsausweis (HBA) und Praxisausweis (SMC-B). Mithilfe der Berechtigtenkarte kann ein Leistungserbringer (Berechtigter) Zugriff auf Daten der eGK eines Versicherten erhalten.
Berechtigter	Natürliche Person, die vom Eigentümer eines Objektes (z.B. Daten oder Fachanwendungen) zur Nutzung berechtigt wurde.
Bestandsnetz	Bestehende IT-Netzwerke von Leistungserbringern und Kostenträgern. Diese sind selbst kein Bestandteil der TI.
Betreiber	Falls der Modulare Konnektor durch eine Organisation betrieben wird, ist diese Organisation der Betreiber des Modularen Konnektors. Dies ist i. d. R. bei einem Rechenzentrumskonnektor der Fall. Der Betreiber ist in diesem Fall für die korrekte Durchführung der in diesem Handbuch beschriebenen Aufgaben der Rolle Leistungserbringer verantwortlich. Weiter übernimmt der Betreiber die Verantwortung der Rolle des Leistungserbringers für den Betrieb des Modularen Konnektors.
Betriebsanzeigen	Leuchtdioden am Gehäuse, die den aktuellen Betriebszustand signalisieren (siehe Kapitel 4.4).
BIOS	Basic input/output system; Software , die unmittelbar nach dem Einschalten des Geräts ausgeführt wird (Boot-Prozess).
BMP	Bundeseinheitlicher Medikationsplan (siehe Kapitel 110)
BNetzA	Bundesnetzagentur
Boot-Prozess	Ausführung des BIOS nach dem Einschalten des Geräts.
BSI	Bundesamt für Sicherheit in der Informationstechnik.

C

CE-Kennzeichnung	Erklärung des Herstellers, dass das Produkt den Anforderungen genügt, die in den Harmonisierungsrechtsvorschriften der Europäischen Gemeinschaft niedergelegt sind.
Certificate Authority	Zertifizierungsstelle der PKI, die digitale Zertifikate erstellt.
CETP	Connector Event Transport Protocol; Netzwerkprotokoll des Systeminformationsdienstes (siehe Kapitel 9.4.5)
Clientsystem	Ein dezentrales System, das mit der TI interagiert, ohne Bestandteil der TI zu sein (z.B. PVS-, AVS-, KIS-Systeme, E-Mail-Clients). .
CRL	Certificate Revocation List; eine Liste, die Informationen über gesperrte Zertifikate enthält(siehe Kapitel 2.2.4).

D

Dauerhafte Außerbetriebnahme	Prozess, durch den das Gerät gesperrt wird und nicht mehr in Betrieb genommen werden kann (siehe Kapitel 15).
Deregistrierung	Die Rücknahme der Freischaltung des Modularen Konnektors (siehe Kapitel 9.6.1.2).
DHCP	Dynamic Host Configuration Protocol, ein Kommunikationsprotokoll, das die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server ermöglicht.
DiffServ	Differentiated Services; ein Schema zur Klassifizierung von IP-Paketen
DNS	Domain Name System; System zur Auflösung von Domainnamen in IP-Adressen. Innerhalbs eines Netzwerkes wird diese Funktion vom DNS-Server ausgeführt, der entsprechende Anfragen beantwortet.
DNSSEC	Domain Name System Security Extensions; Sicherheitsmechanismen zur Gewährleistung der Authentizität der vom DNS bereitgestellten Daten.
DVO	Dienstleister vor Ort; Organisation, die den Administrator beim Betrieb des Netzwerks mit den darin befindlichen Komponenten unterstützt.

E

eGK	Elektronische Gesundheitskarte; Versichertenkarte für gesetzlich Krankenversicherte, die als Chipkarte im Scheckkartenformat ausgeführt ist.
eMP	Elektronischer Medikationsplan
ESP	Encapsulating Security Payload, ein IP-Protokoll

F

Fachanwendung	Eine Anwendung der TI mit allen nötigen technischen und organisatorischen Anteilen auf Anwendungsebene.
Fachdienst	Zentraler Anwendungsanteil der Fachanwendung innerhalb der TI mit Anbindung an die zentrale TI-Plattform. Fachdienste sind Bestandteil der TI, nicht Bestandteil der TI-Plattform.
Fachmodul	Ein dezentraler, auf einem Clientsystem betriebener Anwendungsanteil einer Fachanwendung mit sicherer Anbindung an die TI-Plattform.
Firewall	Funktion des Modularen Konnektors, die lokale Systeme vor unberechtigtem Zugriff aus dem Internet schützt, indem der Datenfluss anhand eines Regelwerks kontrolliert wird.

G

gematik	Die gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH) koordiniert die Einführung und Weiterentwicklung der elektronischen Gesundheitskarte (eGK) und ihrer Infrastruktur in Deutschland.
Gemeinschafts-praxis	Im Vertragsarztrecht festgelegte Kooperationsform von Ärzten oder Therapeuten, seit 2007 als Berufsausübungsgemeinschaft bezeichnet.
gSMC-K	Security Module Card Typ K; Internes Sicherheitsmodul, das die Identität des Modularen Konnektors beinhaltet.
gSMC-KT	Security Module Card Typ KT; Gerätekarte, die die Identität eines E-Health-Kartenterminals beinhaltet.

H

HBA	Heilberufsausweis; Berechtigungskarte, mit der sich Angehörige der Heilberufe (z.B. Ärzte und Apotheker) gegenüber der Telematikinfrastruktur ausweisen und vertraulich (verschlüsselt) kommunizieren können.
Hersteller	Hersteller der TI stellen ein Produkt gemäß den Spezifikationen der gematik her. Sie übernehmen die Produkthaftung gemäß den gesetzlichen Vorgaben und den Support gegenüber ihren Kunden. Hersteller von dezentralen Produkten der TI unterscheiden sich von Anbietern insbesondere dadurch, dass das verantwortete Produkt keinen IT-Service darstellt, sondern physische Geräte oder Software, welche in der Hoheit der Anwender betrieben werden.
Hybride Verschlüsselung	Verschlüsselung unter Verwendung einer Kombination aus asymmetrischer und symmetrischer Verschlüsselung

I

IAG	Internet Access Gateway; Gerät(e), die den Internetzugang ermöglichen und üblicherweise vom ISP zur Verfügung gestellt werden, z.B. DSL-Router und DSL-Modem.
ICMP	Internet Control Message Protocol, ein IP-Protokoll
Integrität	Die Unverfälschtheit von Informationsobjekten und Systemen, beispielsweise gespeicherten und übertragenen Daten, Anwendungen und Systemkomponenten.
Intermediär	Vermittler zwischen zwei Systemen, wobei beide Systeme jeweils dem Intermediär vertrauen, nicht jedoch zwangsweise einander.
Internetmodus	Betriebsmodus des Modularen Konnektors, der bestimmt, wie für das Internet bestimmte Datenpakete behandelt werden (siehe Kapitel 10.2.1.3).
IP	Internet Protocol, in Computernetzen verwendetes Netzwerkprotokoll für den Datenversand.
IP-Adresse	Adresse in Computernetzen, die auf IP basiert. Sie wird Schnittstellen zugewiesen, die an das Netz angebunden sind, und macht diese damit

	erreichbar.
IPComp	IP Payload Compression, ein IP-Protocol
IPsec	Internet Protocol Security; Protokoll-Suite, die eine gesicherte Kommunikation über potentiell unsichere IP-Netze wie das Internet ermöglicht.
ISP	Internet Service Provider; Anbieter von Diensten und technischen Leistungen, die für die Anbindung an das Internet erforderlich sind.
IT	Informationstechnik; Oberbegriff für die Datenverarbeitung.

K

Kartenterminal, eHealth-	LAN-fähiges Kartenterminal nach SICCT-Spezifikation, das das Lesen und Schreiben von Daten auf die eGK und die sichere Kommunikation mit der Telematikinfrastruktur ermöglicht.
KIM	Kommunikation im Medizinwesen
KSR	Konfigurations- und Software-Repository, Dienst für die Bereitstellung von Aktualisierungen für den Modularen Konnektor
Kostenträger	Im Kontext der Telematikinfrastruktur die gesetzlichen Krankenversicherungen.

L

LDAP	Lightweight Directory Access Protocol; Netzwerkprotokoll für die Kommunikation zwischen einem Clientsystem und einem Verzeichnisdienst.
Leistungserbringer	Erbringer von Leistungen des Gesundheitswesens für Versicherte, beispielsweise ein Arzt oder Therapeut. Der Leistungserbringer gehört zu einem zugriffsberechtigten Personenkreis nach § 291a Abs. 4 SGB V.

M

Mandant	Organisationseinheit, die sich mit dem Praxisausweis (SMC-B) ausweist (vgl. Berechtigter).
Meldung	Vom Konnektor erstelltes Protokoll eines Ereignisses während des Betriebs (siehe Kapitel 16.9).
Modularer Konnektor	Das Bindeglied zwischen der IT-Infrastruktur des Anwenders und der zentralen Telematikinfrastruktur (siehe Kapitel 2.1).

N

Netzkonnektor	Dezentrale Komponente der TI-Plattform zur sicheren Verbindung auf Netzwerkebene zwischen den dezentralen Systemen auf der einen Seite und den zentralen Diensten der TI-Plattform sowie den fachanwendungsspezifischen Diensten auf der anderen Seite.
NFDM	Notfalldatenmanagemen
NTP	Network Time Protocol; Standard zur Synchronisierung von Uhren in Computersystemen. Der Modulare Konnektor kann sich mit einem NTP-Server (Zeitdienst) in der zentralen TI synchronisieren und im lokalen Netzwerk einen NTP-server für die Synchronisation der Clientsysteme bereitstellen (siehe Kapitel 2.3.1).

O

OCSP	Online Certificate Status Protocol, Netzwerkprotokoll, mit dem der Modulare Konnektor den Status von Zertifikaten beim Validierungsdienst der TI abfragt (siehe Kapitel 2.2.4).
Offline-Modus	Betriebsmodus des Modularen Konnektors, in dem keine Verbindungen zu TI oder SIS aufgebaut werden. Der Modulare Konnektor stellt jedoch weiterhin lokale Funktionen zur Verfügung, wie z.B. die Ausführung von Fachmodulen.
Online-Modus	Betriebsmodus des Modularen Konnektors, in dem versucht wird, Verbindungen zu TI und optional SIS aufzubauen.

P

Pairing	Prozess der logischen Verknüpfung des Modularen Konnektors mit einem eHealth-Kartenterminal durch den Austausch geheimer Informationen (siehe Kapitel 6.3).
PIN	Personal Identification Number; Geheimzahl zur Authentifizierung. Beispielsweise muss zur Nutzung einer SMC-B durch einen Mandanten die zugehörige PIN an einem Kartenterminal eingegeben werden.
PKI	Public Key Infrastrukture; Sicherheitsinfrastruktur für die Erstellung, Verteilung und Prüfung von digitalen Zertifikaten.
Primärsystem	IT-System das bei einem Leistungserbringer eingesetzt wird, beispielsweise eine Praxisverwaltungssoftware (PVS). Das Primärsystem ist kein Bestandteil der TI-Plattform; es befindet sich unter der administrativen Hoheit des Leistungserbringers.
Protokollierung	Automatische Erfassung von sicherheitsrelevanten und operativen Ereignissen durch den Modularen Konnektor (siehe Kapitel 16.9).
PUK	Personal Unblocking Key; Geheimzahl mit der ein durch PIN geschütztes Gerät nach mehrmaliger Falscheingabe der PIN entsperrt werden und eine neue PIN zugeordnet werden kann.
PVS	Praxisverwaltungssystem; Software für den Betrieb von Arztpraxen.

R

REACH-Verordnung	EU-Chemikalienverordnung (Registration, Evaluation, Authorisation and Restriction of Chemicals).
Registrierung	Die Freischaltung des Modularen Konnektors (siehe Kapitel 9.6.1.1).
Remote Management	Betriebsmodus des Modularen Konnektors, in dem die Administrierung von einem entfernten System aus erfolgt (siehe Kapitel 11.12).
Remote-PIN	Funktion die es ermöglicht, für eine SMC-B, die in einem Kartenterminal steckt, an einem anderen Kartenterminal eine PIN einzugeben (siehe Kapitel 9.3.5).

REST	Representational State Transfer; Konzept für die Kommunikation zwischen Clientsystemen und Servern. Die REST-Schnittstelle des Modularen Konnektors ermöglicht die kommandozeilenbasierte Administrierung und die Durchführung eines Werksresets (siehe Kapitel 11.7.1.2).
RoHS-Richtlinien	EU-Richtlinien zur Verwendung bestimmter gefährlicher Stoffe in Elektrogeräten (Restriction of Hazardous Substances).

S

Schlüssel	Information für die Ver- oder Entschlüsselung von Daten mittels eines kryptographischen Algorithmus. Asymmetrische Verfahren der TI verwenden Schlüsselpaare, die aus einem öffentlichen Schlüssel und einem privaten Schlüssel bestehen. Der öffentliche Schlüssel ist nicht geheim und dient dazu, Nachrichten an den Besitzer zu verschlüsseln oder dessen digitale Signatur zu prüfen. Der private Schlüssel wird vom Besitzer geheim gehalten und dient dazu, Nachrichten zu entschlüsseln oder Dokumente zu signieren.
SICCT	Secure Interoperable Chip Card Terminal; Spezifikation des Kommunikationsstandards für die TI
Sicherheits-beiblätter	Im Lieferumfang enthaltene Dokumente mit sicherheitsrelevanten Hinweisen zu Empfang/Prüfung und Aufstellung/Inbetriebnahme des Modularen Konnektors.
Sicherheitssiegel	Sicherheitsmerkmal am Gehäuse des Modularen Konnektors zum Schutz vor Kompromittierung (siehe Kapitel 4.3.1).
Siegelband	Sicherheitsmerkmal an der Transportverpackung des Modularen Konnektors zum Schutz vor Kompromittierung (siehe Kapitel 3.1)
SIS	Sicherer Internetservice; Von der gematik zugelassener Zugangsdienst zum Internet.
SMC-B	Security Module Card Typ B; Praxisausweis (siehe Berechtigtenkarte)
Sperrung für den Versand	Die Sperrung für den Versand überschreibt ein Geheimnis, das zum Entschlüsseln des gesicherten Speichers notwendig ist. Der Modulare Konnektor ist danach nicht mehr funktionsfähig (siehe Kapitel 11.8).

SSL	Secure Socket Layer; Netzwerkprotokoll für die sichere Übertragung von Daten.
Standalone-Modus	Betriebsmodus, in dem keine Verbindungen zwischen dem Modularen Konnektor und Clientsystemen bestehen (siehe Kapitel 10.2.1.4).

T

TCP	Netzwerkprotokoll für die Aufteilung von Daten in Datenpakete. TCP beinhaltet Funktionen zur Empfangsquittierung, um die Übermittlung aller Datenpakete sicherzustellen.
TI	Telematikinfrastruktur; Privates Netzwerk für die Kommunikation zwischen den Akteuren des deutschen Gesundheitswesens.
TI-Services	Dienstleistungen der TI, die den Anwendern der TI bereitgestellt werden.
TLS	Transport Layer Security; Netzwerkprotokoll für die sichere Übertragung von Daten. TLS ist eine Weiterentwicklung von SSL.
TSL	Trust-Service Status List; Liste zulässiger Zertifikate (siehe Kapitel 2.2.4).

U

UDP	User Datagram Protocol; Netzwerkprotokoll für die Aufteilung von Daten in Datenpakete. UDP beinhaltet im Gegensatz zu TCP keine Quittierungsfunktionen; dadurch wird eine höhere Übertragungsgeschwindigkeit erzielt.

V

Versicherter	Natürliche Person, die in einem Versicherungsverhältnis mit einer gesetzlichen Krankenversicherung steht.
VPN	Virtual Private Network; Privates Netzwerk, dessen Systeme räumlich voneinander getrennt sind und über sichere Verbindungen kommunizieren.

VPN-Konzentrator	Zentraler Verbindungspunkt der zentralen TI (siehe Kapitel 2.2.1).
VPN-Zugangs-dienst.	Funktion für den sicheren Zugang zur zentralen TI (siehe Kapitel 2.2.1).

VSD	Versichertenstammdaten; Auf der eGK gespeicherte Verwaltungsdaten der Versicherten, zum Beispiel Name, Geburtsdatum und Angaben zur Krankenversicherung.
VSDM	Versicherten-stammdaten-management; Bereitstellung und Pflege der VSD in der Telematikinfrastruktur.
VZD	Verzeichnisdienst; Funktion der zentralen TI-Plattform zur Ablage von Daten und dem Zugriff auf Daten durch berechtigte Benutzer und fachanwendungsspezifische Dienste.

W

WAN	Wide Area Network; großräumiges Netzwerk, in diesem Handbuch Bezeichnung der Schnittstelle des Modularen Konnektors für die Verbindung mit der TI.
Werksreset der Benutzerkonten	Der Werksreset der Benutzerkonten setzt alle Benutzerkonten in den Auslieferungszustand zurück. Die Anmeldung ist anschließend nur noch mit den initialen Zugangsdaten möglich (siehe Kapitel 11.7.3).
Werksreset für Fail Safe	Der Werksreset für Fail Safe setzt die Konfiguration des Netzkonnektors in den Auslieferungszustand zurück und weist der LAN-Schnittstelle eine statische IP-Adresse zu (siehe Kapitel 11.7.2).
Werksreset, vollständiger	Der vollständige Werksreset setzt alle Parameter mit Ausnahme der aktuellen Firmware und Meldungen des Typs SECURITY in den Auslieferungszustand zurück (siehe Kapitel 11.7.1).

X

X.509	Standard für eine PKI, die digitale Zertifikate ausstellen, verteilen und prüfen kann.
XML	Extensible Markup Language, Standard zur Darstellung strukturierter Daten.

Z

Zeitdienst	Siehe NTP (Network Time Protocol)
Zentrales Netz	Das Zentrale Netz der TI ermöglicht den Transport von Daten zwischen den angeschlossenen Nutzern der TI. Es beinhaltet die Infrastruktur zur Kontrolle des Zugangs zum Zentralen Netz der TI und die eigentliche zentrale Transportplattform.
Zertifikat, digitales	Von der PKI erstellter Datensatz, der den Eigentümer und weitere Eigenschaften eines öffentlichen Schlüssels bestätigt.
Zugangsdienst	Siehe VPN-Zugangsdienst.