secunet Highspeedkonnektor

# Bedienungsanleitung

Für Administratoren von Konnektor-Instanzen

Version 2.0
Produkttypversion: 1.3.0-0
Firmwareversion: 2.0.2

30.08.2024

Diese Bedienungsanleitung bezieht sich auf den folgenden von der gematik zugelassenen und vom BSI zertifizierten Konstruktionsstand:

- Konstruktionsstand secunet Highspeedkonnektor 2.0.0

Weitere Versionshinweise finden Sie auf Seite 15.

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# Tabellenverzeichnis

# Vorwort

Dieses Dokument beschreibt den secunet Highspeedkonnektor, der zur sicheren Anbindung von Clientsystemen der Institutionen und Organisationen des Gesundheitswesens an die Telematikinfrastruktur dient. Der Highspeedkonnektor 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 folgenden von der gematik zugelassenen und vom BSI zertifizierten Konstruktionsstand:

- Konstruktionsstand secunet Highspeedkonnektor 2.0.0

Der Konstruktionsstand legt jeweils eine Firmware- und Hardwareversion fest. Informationen zu den zugelassenen Softwareversionen sind der Webseite des Herstellers zu entnehmen (www.secunet.com), Informationen zu den zugelassenen oder für den Betrieb in der TI genehmigten Software- und Hardwareversionen erhalten Sie von der gematik (www.gematik.de).

Dieses Handbuch bezieht sich auf folgende zugelassene Versionen:

- Produkttypversion 1.3.0-0
- Firmwareversion 2.0.2
- Hardwareversion 2.0.0

Diese Firmwareversion beinhaltet implizit folgende Fachmodule:

- secunet Fachmodul AMTS, Version 5.50.0
- secunet Fachmodul NFDM, Version 5.1.1
- secunet Fachmodul ePA, Version 5.50.0
- secunet Fachmodul VSDM, Version 5.50.0

Informationen über lizenzpflichtige Systemkomponenten finden Sie in Kapitel 8.8.2.1.

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/highspeedkonnektor).

Alle Anleitungen zu Browsern in diesem Dokument beziehen sich auf den Browser Google Chrome Version 87.

## Was beinhaltet dieses Dokument

In dieser Bedienungsanleitung ist die Administration von Instanzen des Highspeedkonnektors beschrieben.

Die Konnektor-Instanzen des secunet Highspeedkonnetors werden als virtuelle Maschinen vom Betreiber zur Verfügung gestellt. Die virtuellen Maschinen sind vollständig voneinander separiert und voreinander geschützt. Jede Konnektor-Instanz kann über eine eigenständige Bedienoberfläche bzw. REST-API angesprochen und verwaltet werden.

Im Folgenden werden die Bezeichnungen Konnektor-Instanz, Instanz und Konnektor als Synonyme verwendet.

## An wen ist diese Dokumentation gerichtet

Das Bedienhandbuch richtet sich an Personen, die in der folgenden Rolle auf eine Konnektor-Instanz zugreifen:

- Administrator von Konnektor-Instanzen (Instanz-Administrator)

  Der Instanz-Administrator (nachfolgend Administrator) besitzt dieselben Rechte wie der Administrator eines Einbox-Konnektors und ist für die Administrierung und Bedienung der Konnektor-Instanz zuständig.

Weitere Rollen:

- Betreiber (Basissystem-Administrator)

  Diese Benutzerrolle besitzt die folgenden Berechtigungen:

  - Verwaltung der instanzenübergreifenden Konfigurationen des Konnektors einschließlich Software-Aktualisierungen
  - Ressourcenkonfiguration von Konnektor-Instanzen
  - Leserechte auf das Logging des Basissystems ohne die Logs der Konnektor-Instanzen
  - Backup/Restore von Konnektor-Instanzen
  - Löschen von Konnektor-Instanzen

- Nutzer mit Rolle "Zugangsmodul" administrieren

- Zugangsmodul (technische Benutzerrolle)

  Diese Benutzerrolle besitzt die folgenden Berechtigungen:

  - Erzeugen und löschen von Konnektor-Instanzen
  - Zuordnen von IP-Adressen zu Konnektor-Instanzen
  - Backup/Restore von Konnektor-Instanzen
  - Ressourcenkonfiguration von Konnektor-Instanzen

- Dienstleister vor Ort (DVO)

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

- Arzt (Leistungserbringer) und Inhaber einer SMC-B

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

- Praxispersonal

  Personen, die dezentrale Produkte der Telematikinfrastruktur, z.B. die Instanz eines Highspeedkonnektors, im personalbedienten Bereich nutzen.

## Erforderliches Vorwissen

Die Administration der Instanz eines Highspeedkonnektors setzt Wissen über das Informationsmodell und die Funktionen der Telematikinfrastruktur voraus.

## Hinweis zu CC-Zertifizierung und gSMC-K aktualisieren

Die Zulassung des Highspeedkonnektors (HSK) umfasst die Evaluierung durch eine Common Criteria zertifizierte Prüfstelle sowie die Zertifizierung gemäß „Beschleunigter Sicherheitszertifizierung (BSZ)".

Zusätzlich basiert die Zulassung auf einer Begutachtung der Sicherheitsprozesse zur Personalisierung des Hardwaresicherheitsmoduls (HSM) sowie der Softwareentwicklungsprozesse sowie des gesamten Produkts durch von der gematik zugelassene Gutachter.

Zur Aufnahme der Geräteidentität verwendet der Highspeedkonnektor anstelle von Gerätekarten (gSMC-K) ein Hardwaresicherheitsmodul (HSM)

## 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

## 1.1 Bereitstellung durch den Betreiber

Die Instanz wurde Ihnen vom Betreiber des Highspeedkonnektors bereitgestellt (siehe Kapitel 2.5).

## 1.2 Prüfung der Zulassung

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

Unter dem Begriff „zugelassen“ werden alle Software- und Hardwareversionen zusammengefasst, für die entweder eine Zulassung oder eine Genehmigung zum Betrieb in der Telematikinfrastruktur seitens der gematik erteilt wurde.

Sie finden eine Auflistung aller Konnektoren unter:
https://fachportal.gematik.de/zulassungs-bestaetigungsuebersichten .

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

- Die Zulassung des Highspeedkonnektors beinhaltet die Beschleunigte Sicherheitszertifizierung (BSZ) des Highspeedkonnektors gemäß Anwendungshinweise und Interpretationen zum Schema (AIS), die für den Highspeedkonnektor relevant sind https://www.bsi.bund.de/bsz. Die Zulassung durch die gematik setzt eine Begutachtung der Sicherheitsprozesse zur Personalisierung des verwendeten Hardwaresicherheitsmodul (HSM) voraus.

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

https://www.secunet.com/highspeedkonnektor/

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

## 1.3 Was muss im Betrieb beachtet werden?

Die Konnektor-Instanz sowie der Zugang zur Konnektor-Instanz wurden vom Dienstleister vor Ort (DVO) für Ihre speziellen Bedürfnisse eingerichtet und benötigt im normalen Betrieb keine Bedienung.

- Kontaktieren Sie im Fall von Störungen oder sonstigen Auffälligkeiten den Betreiber.

## 1.4 Ansprechpartner für Fragen und bei Störungen

**Wenden Sie sich bei Störungen der Konnektor-Instanz oder Fragen zur sicheren Nutzung an Ihren Vertragspartner.**

# 2 Funktionsbeschreibung

## 2.1 Einsatzumgebung

Der Highspeedkonnektor kann in den Modi Eigenbetrieb und TI-Gateway betrieben werden. Die Konnektor-Instanzen übernehmen in beiden Modi die Funktionen der bisher dezentral eingesetzten Konnektoren, sodass kein Konnektor mehr vor Ort betrieben werden muss.

Im Eigenbetrieb können die Konnektor-Instanzen des Highspeedkonnektors dem Unternehmen oder der Unternehmensgruppe bereitgestellt werden.

Für die Eigennutzung eines Highspeed-Konnektors innerhalb einer Unternehmensgruppe muss ein lückenloser und einheitlicher Datenschutz gemäß den Anforderungen der DSGVO und des BDSG über die gesamte Unternehmensgruppe hinweg gewährleistet sein.

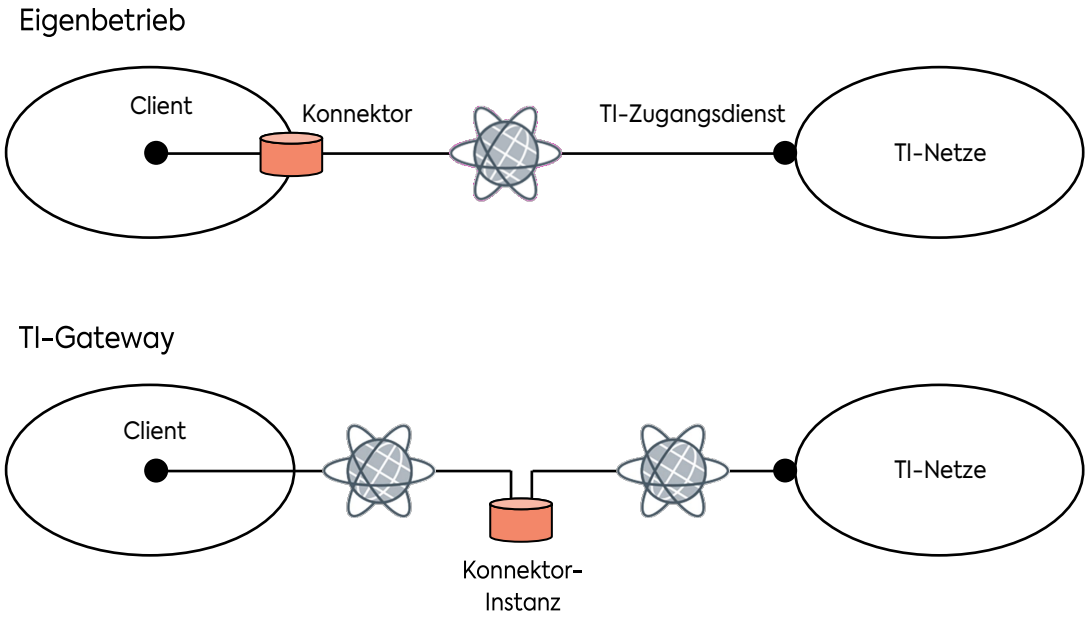



Abbildung 1: Einsatzumgebung Eigenbetrieb/TI-Gateway

## 2.2 Einsatzzweck

Der Highspeedkonnektor dient der sicheren Anbindung der IT-Systeme einer Praxis oder Praxisgemeinschaft an die Telematikinfrastruktur.

In diesem Dokument wird "Highspeedkonnektor" als Synonym für die jeweils verwendete Konnektor-Instanz verwendet.

Der Highspeedkonnektor stellt folgende Funktionen zur Verfügung:

- Anbindung an die Telematikinfrastruktur

  Der Highspeedkonnektor stellt über den Sicheren Zentralen Zugangspunkt (SZZP/SZZP-light) eine permanente, gesicherte Verbindung zur zentralen Telematikinfrastruktur her.

  Zugriffe der Clients aus dem lokalen Netz auf offene Fachdiensten und weitere Anwendungen (WANDA) erfolgen direkt über den Zugang zur TI und nicht über den Highspeedkonnektor.

Im Folgenden werden die Bezeichnungen SZZP sowie SZZP-light als Synonyme verwendet.

- Schutz auf Transportebene

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

- Protokollierung

  Der Highspeedkonnektor protokolliert automatisch sicherheitsrelevante und operative Ereignisse.

- Plattform für die Ausführung von Anwendungen (Fachmodule)

  Der Highspeedkonnektor 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 Highspeedkonnektor kann im lokalen Netzwerk einen NTP- und DNS-Server bereitstellen.

## 2.3 Sicherheitsfunktionen

### 2.3.1 Anbindung an die Telematikinfrastruktur

Der Betreiber des Highspeedkonnektors stellt sicher, dass der Highspeedkonnektor über einen Sicheren Zentralen Zugangspunkt (SZZP/SZZP-light) an die TI angebunden ist. Des Weiteren stellt dieser die Anbindung an einen VSDM-Intermediär und bei Bedarf an den HTTP-Forwarder der zentralen TI her.

### 2.3.2 Gültigkeitsprüfung von Zertifikaten

Der Zertifikatsdienst des Highspeedkonnektor überprüft die Gültigkeit von Zertifikaten. Dazu stellt die zentrale TI eine Trust-Service Status List (TSL) mit den Zertifikaten von zulässigen Dienstanbietern bereit.

Die Prüfung von Zertifikaten beinhaltet:

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

### 2.3.3 Kryptographische Verfahren in der Telematikinfrastruktur

Der Highspeedkonnektor verwendet z.B. zur Authentisierung externer Verbindungen kryptographische Verfahren in Form asymmetrischer Schlüssel und X.509-Zertifikaten.

Hierbei nutzt der Highspeedkonnektor ein internes Hardwaresicherheitsmodul (HSM) zur Abbildung der Geräteidentitäten. Das interne Hardwaresicherheitsmodul beinhaltet die Identität jeder Instanz eines Highspeedkonnektors, die untrennbar mit der Instanz verbunden ist.

Es kommen Identitäten auf Basis von ECC-Schlüsseln zum Einsatz.

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

### 2.3.4 Kryptografisch gesicherter Speicher

Die vom Betreiber des Highspeedkonnektors bereitgestellte Instanz 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 instanzindividuellen Schlüssels geschützt.

Die Instanz löscht nicht mehr benötigte Schlüssel (insbesondere Sitzungsschlüssel für 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.

### 2.3.5 Paketfilter

Zur Abwehr von Angriffen schränkt der Highspeedkonnektor den Datenaustausch mit Ausnahme der für den Verbindungsaufbau erforderlichen Kommunikation ein.

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.

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

Zudem akzeptiert der Highspeedkonnektor nur korrekte IP-Pakete.

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

### 2.3.6 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)

- Komfortsignatur

  Für die QES unterstützt der Konnektor die Komfortsignaturfunktion. In diesem Modus können für ein- und denselben HBA mehrere vom Clientsystem initiierte Signaturaufträge (Einzel- oder Stapelsignatur) abgearbeitet werden, ohne dass der Inhaber des HBA für jeden einzelnen dieser Signaturaufträge die PIN.QES am Kartenterminal eingegeben muss.

  Bei eingeschalteter Komfortsignaturfunktion können potentiell alle HBAs in der Umgebung, in der der Konnektor eingesetzt ist, Komfortsignaturen durchführen. Die eigentliche Aktivierung der Komfortsignatur muss separat für jeden einzelnen HBA erfolgen.

- Einfachsignaturmodus

  In diesem Betriebsmodus wird bei der qualifizierten Signatur eines einzelnen Dokumentes eine vereinfachte Sicherheitsumgebung ohne gegenseitige Authentisierung der Karte und des Highspeedkonnektors 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 12.14.2.1, 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 Highspeedkonnektor 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 Highspeedkonnektor 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.

### 2.3.7 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
- Ver- und Entschlüsselung mit HBA Vorläuferkarten

### 2.3.8 Authentifizierungsdienst

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

**Der Authentifizierungsdienst kann nur mit dem Authentisierungsschlüssel des HBAx oder des SM-B verwendet werden. Die Nutzung ist auf Dokumente (Hash-Werte) von maximal 512 Bit Länge beschränkt.**

### 2.3.9 Selbsttest

Der Highspeedkonnektor 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 6.4.1)

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

### 2.3.10 Client-Anwendungen für die Fachanwendung ePA

Das Fachmodul ePA (elektronische Patientenakte, siehe Kapitel 6.7.2) nutzt folgende lokale Anwendungen für die Kommunikation mit Diensten der TI:

- SGD-Client

  Client für die Verbindung mit Schlüsselgenerierungsdiensten (SGD) für die Ver- und Entschlüsselung von Dokumenten

- VAU-Client

  Client für die Verbindung mit einer vertrauenswürdigen Ausführungsumgebung (VAU), in der für Anfragen an das ePA- Aktensystem auf die Metadaten von Dokumenten zugegriffen wird

## 2.4 Weitere Dienste

### 2.4.1 Zeitdienst

Der Highspeedkonnektor stellt im lokalen Netzwerk einen NTP-Server der Stratum-Ebene 3 für Fachmodule und Clientsysteme bereit. Dieser synchronisiert sich 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.

### 2.4.2 DNS-Dienst

Der Highspeedkonnektor stellt im lokalen Netzwerk optional einen DNS-Server zur Verfügung.

## 2.5 Netzwerkschnittstellen

Der Highspeedkonnektor besitzt folgende Netzwerkschnittstellen:

- Die Schnittstelle jeder Konnektor-Instanz zu Client-Netzwerken und den darin befindlichen Clientsystemen und Kartenterminals.
- Die Schnittstelle zum SZZP-light für die Verbindung jeder Konnektor-Instanz mit der Telematikinfrastruktur.

Die Parameter zum Anschluss der Komponenten der Client-Netze erhalten Sie vom Betreiber des Highspeedkonnektors bei der Bereitstellung der Instanz. Details zu den unterstützten Netzwerkprotokollen finden Sie in Kapitel 12.1.

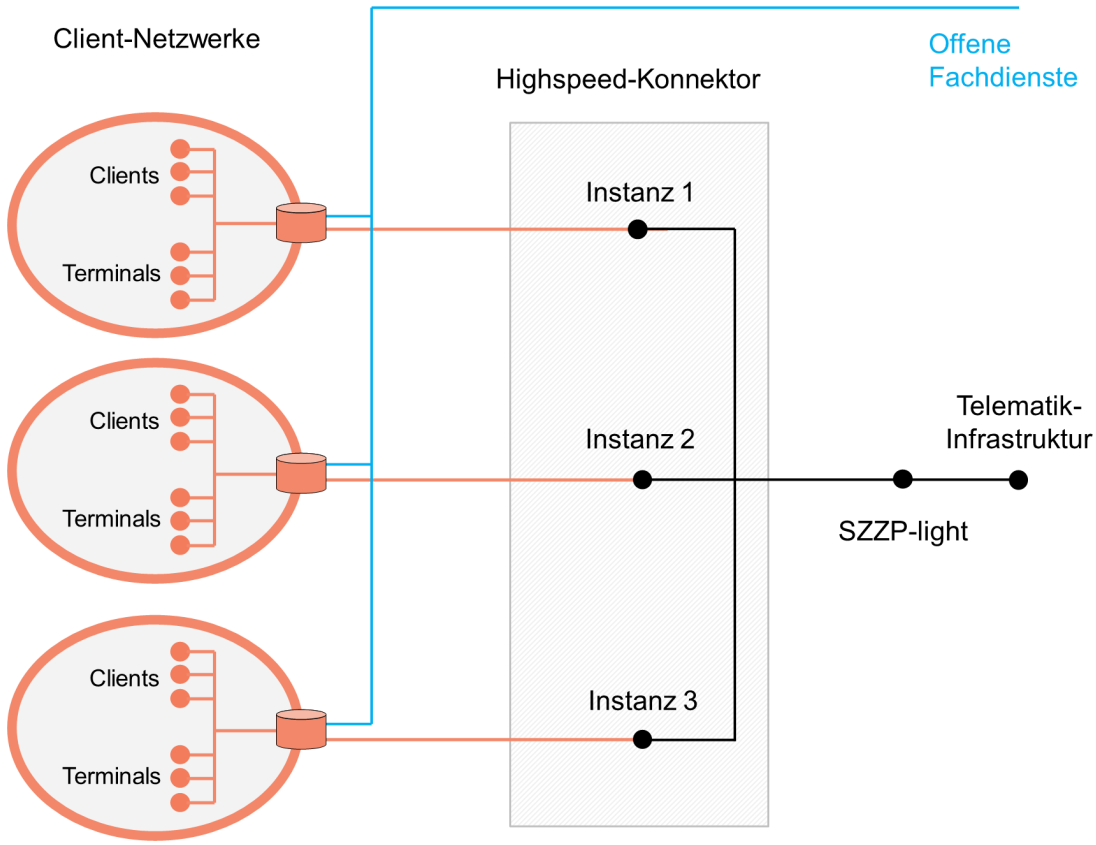



Abbildung 2: Netzwerkübersicht (vereinfachtes Beispiel)

Nachfolgend finden Sie eine Übersicht der verwendeten Ports:

| System | Protokolle | Ports |
|---|---|---|
| Client/PVS/KIS | HTTP/HTTPS | TCP 80/443/8500/9500 |
| | SOAP | TCP 80/443 |
| | LDAP | TCP/UDP 389/636 |
| | SMTP | TCP 25/465* |
| | POP3 | TCP 110/995* |
| | CETP | Vom PVS festgelegt** |
| Kartenterminal | SICCT | TCP/UDP 4742 |
| Modularer Konnektor | HTTP/HTTPS | TCP 80/443/8500/9500 |
| | DNS | TCP/UDP 53 |
| | SOAP | TCP 80/443 |
| | SICCT | TCP/UDP 4742 |
| | LDAP | TCP/UDP 389/636 |
| | CETP | Vom PVS festgelegt** |
| TI/VPNZugD (über Internet) | HTTP/HTTPS | TCP 80/443/8500/9500 |
| | DNS | TCP/UDP 53 |
| * Manuelle Änderung möglich<br>** Beachten Sie die Hinweise des PVS-Herstellers | | |

Tabelle 1: Verwendete Ports

Der Zugriff von Clients aus dem lokalen Netz auf offene Fachdienste erfolgt nicht über den Highspeedkonnektor. Stimmen Sie sich dazu mit Ihrem Vertragspartner ab.

**Der Highspeedkonnektor verwendet intern die Netzsegmente 169.254.77.0/24 und 169.254.88.0/24. Um eine Kommunikation des Highspeedkonnektor mit angeschlossenen Netzsegmenten zu ermöglichen, darf es keine Überschneidung mit dem intern verwendeten Netzsegment geben.**

# 3 Sicherheitshinweise

## 3.1 Sicherheitshinweise zu Benutzerpasswörtern

Ein Passwort, das für den Zugriff auf den Highspeedkonnektor festgelegt wird, muss mindestens 8 Zeichen lang sein und Zeichen aus drei der folgenden vier Zeichenarten enthalten:

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

Außerdem darf das Passwort den Benutzernamen weder vorwärts noch rückwärts, noch in Groß- oder Kleinschreibung beinhalten.

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 Highspeedkonnektor, 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.**

## 3.2 Sicherheitshinweise Sperrung bzw. Verlust des Zugangs

Es muss sichergestellt sein, dass für die Inbetriebnahme und Administration der Konnektor-Instanz des Highspeedkonnektors nur vertrauenswürdiges, mit der Benutzerdokumentation vertrautes, sachkundiges Personal eingesetzt wird.

Wenn der Zugang zum Highspeedkonnektor gesperrt oder in anderer Form nicht mehr möglich ist, muss der Betreiber informiert werden.

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

Verbindungen der Clients aus dem lokalen Netz zu offenen Fachdiensten und weiteren Anwendungen (WANDA) erfolgen direkt über den Zugang zur TI (SZZP-light) und nicht über den Highspeedkonnektor (siehe Kpaitel 2.1)

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

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

### 3.3.1 Anbindung an die TI

Der Highspeedkonnektors ist über einen Sicheren Zentralen Zugangspunkt (SZZP/ SZZP-light) an die TI angebunden.

### 3.3.2 Internet-Anbindung

**Die Anbindung des lokalen Netzwerks an das Internet kann zu erheblichen Sicherheitsrisiken führen. Alle Clientsysteme müssen entsprechende Sicherheitsmaßnahmen besitzen.**

### 3.3.3 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 Highspeedkonnektor kommunizieren, müssen vertrauenswürdig sein, d.h., es dürfen keine Angriffe aus den Clientsystemen erfolgen und es muss sichergestellt sein, dass sie die ihnen anvertrauten Daten / Informationen nicht missbrauchen. Sofern ein Clientsystem eine gesicherte Kommunikation mit dem Highspeedkonnektor 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 Highspeedkonnektor 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 Highspeedkonnektor. Es übermittelt die vom Leistungserbringer gewünschten Aufrufe an den Highspeedkonnektor.

**Ohne gesicherte beidseitig-authentisierte Verbindung zwischen dem Clientsystem und dem Highspeedkonnektor bestehen Sicherheitseinschränkungen. Beachten Sie die Hinweise zur Absicherung der Verbindung zu Clientsystemen in Kapitel 6.3.3.**

Bei Aktivierung des Komfortsignaturmodus (siehe Kapitel 2.3.6) ist die Authentifizierung des Nutzers vor Nutzung des Clientsystems zwingend erforderlich, da die

Authentifizierung des HBA-Inhabers für die Komfortsignatur durch das Clientsystem erfolgt.

**Bei Aktivierung des Komfortsignaturmodus wird im Aufrufkontext vom Clientsystem eine sogenannte User-Identifikationsnummer an den Highspeedkonnektor übermittelt. Nach erfolgreicher Aktivierung muss sich das Clientsystem mit dieser Identifikationsnummer in den nachfolgenden Signatur-Aufrufen gegenüber dem Highspeedkonnektor authentisieren. Diese Identifikationsnummer wird von der Clientsystem-Software vergeben und ist wie ein Passwort zu behandeln. Die Identifikationsnummer muss durch das Clientsystem ausreichend vor dem Zugriff durch unbefugte geschützt werden. Zudem ist das Clientsystem dafür verantwortlich, dass die Identifikationsnummern jeweils zufällig und für jede Aktivierung der Komfortsignaturfunktion unterschiedlich und unabhängig voneinander gewählt werden.**

Beim Aufruf des Highspeedkonnektors 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 Highspeedkonnektors 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 Highspeedkonnektor 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 Highspeedkonnektor angebotenen Abbruchfunktion der Stapelsignatur ermöglichen.

## 3.4 Sicherheitshinweise zur sicheren Administation

Der Leistungserbringer muss sicherstellen, dass administrative Tätigkeiten in Übereinstimmung mit der Dokumentation des Highspeedkonnektors 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 der angeschlossenen Kartenterminals zu konfigurieren und hat im Falle des manuellen Anwendens von Aktua-

lisierungen das Recht, das Update anzustoßen. Während des Updates müssen alle angeschlossenen (gepairten) Kartenterminals organisatorisch vor unberechtigtem Zugriff geschützt werden.

Der Administrator muss Authentisierungsinformationen und –token geheim halten bzw. darf diese nicht weitergeben (z. B. PIN bzw. Passwort oder Schlüssel-Token).

Der Betreiber des Highspeedkonnektors verantwortet die Installation von Firmwareupdates auf dem Highspeedkonnektor . Über ein bevorstehendes Update muss der Betreiber die Verantwortlichen der Instanzen informieren.

Der Leistungserbringer als Nutzer des Highspeedkonnektors hat die Verantwortung, die Eignung der aktuell genutzten Firmware-Version zu prüfen. Dies beinhaltet die Überprüfung, welche Firmware-Version aktuell eingesetzt wird (siehe Kapitel 9.1.4.2). 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.

Unter dem Begriff „zugelassen“ werden alle Software- und Hardwareversionen zusammengefasst, für die entweder eine Zulassung oder eine Genehmigung zum Betrieb in der Telematikinfrastruktur seitens der gematik erteilt wurde.

Für Informationen über die vorliegende Software- und Hardwareversion siehe Kapitel 6.5.6. Diese können mit den mit den Zulassungsobjekten der gematik abgeglichen werden..

Der Leistungserbringer muss sicherstellen, dass die Administrationskonsole (die Benutzerschnittstelle zur Administration des Highspeedkonnektors) 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.

## 3.5 Sicherheitshinweise zum Personal

Für den Zugriff befugt sind nur Personen, die vom Leistungserbringer namentlich autorisiert wurden.

Durch den Einsatz von qualifiziertem und vertrauenswürdigem Personal müssen Fehler und Manipulationen des Highspeedkonnektors ausgeschlossen werden.

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

Leistungserbringer und Praxispersonal müssen kontrollieren, ob die Konnektor-Instanz des Highspeedkonnektors sicherheitstechnische Veränderungen anzeigt. Der Highspeedkonnektor verfügt über einen Selbsttest, der die Integrität sicherheitsrelevanter Komponenten prüft und anzeigt (siehe Kapitel 2.3.9).

## 3.6 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 Highspeedkonnektor 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 Highspeedkonnektor verwendet werden.

Der Inhaber der SMC-B muss sicherstellen, dass diese nur freigeschaltet ist, wenn sie und die Konnektor-Instanz des Highspeedkonnektors 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).

## 3.7 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.

## 3.8 Hinweise zur Verarbeitung von XML-Dokumenten und PDF-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 Highspeedkonnektor werden durch den Verschlüsselungsdienst und den Signaturdienst XML-Dokumente verarbeitet. Es gelten die in den Kapiteln 12.13, 12.14 und 12.15 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.

Vom Highspeedkonnektor werden durch den Verschlüsselungsdienst und den Signaturdienst PDF-Dokumente verarbeitet. Es gelten die in den Kapiteln 12.13, 12.14 und 12.15 beschriebenen Einschränkungen. Der Konnektor schützt sich damit vor möglichen Angriffen auf die Verarbeitung von PDF-Dokumenten. Externe Komponenten, die solche PDF-Daten verarbeiten, müssen sich selbst vor möglichen PDF-Angriffen schützen. Insbesondere müssen sich externe Komponenten vor Angriffen beispielsweise auf die Anzeigekomponente (Viewer) schützen.

## 3.9 Hinweise zum Betrieb von offenen Fachdiensten

Informationen zur Nutzung offener Fachdienste stellt Ihnen Ihr Vertragspartner (Betreiber) zur Verfügung.

# 4 Erstmalige Inbetriebnahme

## 4.1 Was Sie für die Inbetriebnahme benötigen

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

- Eine SMC-B mit zugehöriger PIN/PUK ist vorhanden.
- Mindestens ein E-Health-Kartenterminal ist vorhanden.
- Das Praxisverwaltungssystem ist für die Verwendung mit der TI zugelassen.
- Die aktuelle TSL zum manuellen Hochladen liegen vor.
- Der Betreiber hat Ihnen die IP-Adresse für den Aufruf der webbasierten Benutzeroberfläche und das zugehörige TLS-Zertifikat bereitgestellt.
- Die vom Hersteller auf der Produktseite des Highspeedkonnektors bereitgestellten Informationen zur Prüfung des TLS-Zertifikats liegen Ihnen vor und wurden gemäß Anleitung in den Browser importiert.
- Auf dem System, das für die Administrierung der Konnektor-Instanz verwendet werden soll, sind Java 11 und der TI Gateway Client (siehe Kapitel 4.4.1) installiert

### 4.1.1 Unterstützte Browser

Um die webbasierte Bedienoberfläche des Highspeedkonnektors zu benutzen, ist die Verwendung des Browsers Google Chrome ab Version 87 empfohlen. Die aktuellen Versionen für Windows-, Linux- und Mac OS-Betriebssysteme sind auf der Webseite des Herstellers verfügbar (https://www.google.de/chrome).

## 4.2 Anforderungen an die Netzwerkumgebung

Wenn der Highspeedkonnektor im Eigenbetrieb hinter einer Firewall betrieben wird, müssen ausgehend alle Ports/Protokolle freigegeben sein.

### 4.2.1 An der LAN-Schnittstelle verwendete Ports

- Management: 8500 (primär), 9500 (sekundär)
- connector.sds: 80 (http), 443 (https)
- 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.

### 4.2.2 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 (DNS)
  - TCP: 80 (HTTP)
  - TCP: 443 (HTTPS)
  - TCP: 8443 (HTTPS)

### 4.2.3 Übersicht der verwendeten IP-Protokolle

| IP-Protokollnummer | Protokoll | Anmerkungen |
|---|---|---|
| 1 | ICMP | |
| 6 | TCP | |
| 17 | UDP | |
| 108 | IPComp | |

## 4.3 Geheimnis festlegen

Das Geheimnis dient der Identifikation des Leistungserbringers gegenüber einem Betreiber. Es wird für den Fall benötigt, dass der Leistungserbringer aufgrund fehlender Zugangsdaten keinen Zugriff mehr auf die grafische Bedienoberfläche des Highspeedkonnektors hat und wahlweise einen vollständigen Werksreset (siehe Kapitel 8.7.1) oder einen Werksreset der Benutzerkonten (siehe Kapitel 8.7.2) durchführen möchte.

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

## 4.4 Erstanmeldung

Für jede Instanz des Highspeedkonnektors erhalten Sie vom Betreiber die IP-Adresse für den Aufruf der webbasierten Benutzeroberfläche.

Die Administrationsschnittstelle zur Konnektor-Instanz wird über eine TLS-Verbindung abgesichert. Beim TLS-Verbindungsaufbau wird für die Authentisierung der Instanz ein TLS-Zertifikat verwendet, das im HSM des Highspeedkonnektors hinterlegt ist. Um sicherzustellen, dass bei der initialen und allen weiteren Verbindunganfragen zur Instanz das korrekte Zertifikat verwendet wird, muss initial eine Validierung des Zertifikates der Konnektor-Instanz durchgeführt werden.

**Wenn die Validierung des des Zertifikates der Konnektor-Instanz nicht korrekt durchgeführt wird, kann der Schutz von sensiblen Informationen wie Zugangsdaten nicht sichergestellt werden. Vor der Validierung des des Zertifikates der Konnektor-Instanz dürfen keine Zugangsdaten an der Administrationsschnittstelle eingegeben werden.**

Die erstmalige Anmeldung an einer Instanz geschieht in folgenden Schritten:

- **TI-Gateway Modus**: Prüfen Sie das TLS-Zertifikat der Konnektor-Instanz mithilfe des TI Gateway Clients (siehe Kapitel 4.4.1).

  Wenn die Prüfung erfolgreich ist, können Sie das TLS-Zertifikat der HSK-Instanz lokal speichern.

- **Eigenbetrieb**: Rufen Sie die Bedienoberfläche des Highspeedkonnektors auf und laden Sie das TLS-Zertifikat der Konnektor-Instanz herunter (siehe Kapitel 4.4.2).

- Importieren Sie das TLS-Zertifikat der Konnektor-Instanz im Browser (siehe Kapitel 4.4.3).

- Melden Sie sich an der Bedienoberfläche des Konnektors an und ändern Sie das Initialpasswort (siehe Kapitel 4.4.4).

  Der Aufruf der Bedienoberfläche ist bei Verwendung des heruntergeladenen TLS-Zertifikats der Konnektor-Instanz über die Ports 8500 oder 9500 möglich.

- Falls Sie ein eigenes TLS-Zertifikat für die Verbindung zum Konnektor verwenden möchten, können sie dieses nun hochladen und für zukünftige Verbindungen verwenden (siehe Kapitel 6.3.3.2).

  Beachten Sie, dass bei der Verwendung eines eigenen TLS-Zertifikates die Anmeldung an der Bedienoberfläche des Highspeedkonnektors nur über den Port 8500 möglich ist.

### 4.4.1 Konnektor-Instanz mittels TI Gateway Client verifizieren

Der TI Gateway Client ist eine Anwendung zur Überprüfung der Authentizität einer Konnektor-Instanz. Der TI Gateway Client kann sowohl über eine grafische Benutzeroberfläche (GUI-Mode) als auch per Kommandozeile (CLI-Mode) bedient werden.

**Falls das Zertifikat Ihrer Konnektor-Instanz nicht verifiziert werden kann, wenden Sie sich bitte umgehend an den Betreiber.**

#### 4.4.1.1 Installation

Der TI Gateway Client wird als Zip-Archiv ausgeliefert.

- Entpacken Sie die Archivdatei, ohne die darin befindlichen Dateien und Ordner umzubenennen oder zu verschieben.

#### 4.4.1.2 Aufruf im CLI-Mode

Starten Sie das Programm mittels Eingabeaufforderung/Shell.

- Geben Sie dazu den folgenden Befehl ein:

```
java -jar ti_gateway_client.jar -i <IP-Adresse der Instanz> -p 9500
```

Der TI Gateway Client baut beim Start eine TLS-Verbindung zur HSK-Instanz auf und überprüft anschließend das Zertifikat.

Wenn die Prüfung erfolgreich ist, können Sie das Zertifikat der HSK-Instanz lokal speichern und den Fingerprint in die Zwischenablage kopieren.

**Tipp**

Erstellen Sie für wiederholte Aufrufe eine Verknüpfung.

Nachfolgend finden Sie eine übersicht der Parameter beim Aufruf.

| Parameter | Funktion |
|---|---|
| `-i, --ip-address` | IP-Adresse der HSK-Instanz |
| `-p, --port` | Port der HSK-Instanz (geben Sie den Port 9500 an) |

| | |
|---|---|
| `-w, --write-file <file>` | Schreibt optional das Instanz-Zertifikat sowie dessen Fingerprint als Zeichenfolge in die angegebene Datei. Die Datei wird neu angelegt. Eine bereits vorhandende Datei wird nicht überschrieben, das Programm brichtin diesem Fall mit einer entsprechenden Meldung ab. |

#### 4.4.1.3 Aufruf im GUI-Mode

- Rufen Sie die grafische Bedienoberfläche entweder mit doppeltem Mausklick auf die .jar-Datei auf, oder geben Sie mittels Eingabeaufforderung/Shell den folgenden Befehl ein:

```
java -jar ti_gateway_client.jar
```


Abbildung 3: TI Gateway Client GUI-Mode

- Geben Sie die IP-Adresse der HSK-Instanz ein und klicken Sie auf **TLS-Zertifikat prüfen**.

  Das Ergebnis der Prüfung wird angezeigt.

- Vergleichen Sie zusätzlich den Fingerprint (SHA-256 Wert) des im Browser bei der Verbindung zur Management-Schnittstelle der Konnektor-Instanz mit einer Sicherheitswarnung angezeigten Zertifikats mit dem durch den TI Gateway Client angezeigten SHA-256 Wert.

- Nach einer erfolgreichen Prüfung können Sie über **Zertifikat downloaden** das Zertifikat der HSK-Instanz lokal speichern.

### 4.4.2 Zertifikat des Konnektors herunterladen

Alle Anleitungen zu Browsern in diesem Dokument beziehen sich auf den Browser Google Chrome Version 87.

Gehen Sie wie folgt vor, um das TLS-Zertifikat des Highspeedkonnektors herunterzuladen und zu exportieren:

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

```
https://<IP-Adresse der Konnektor-Instanz>:9500/management
```

Es sollte nun eine entsprechende Fehlermeldung im Browser angezeigt werden:

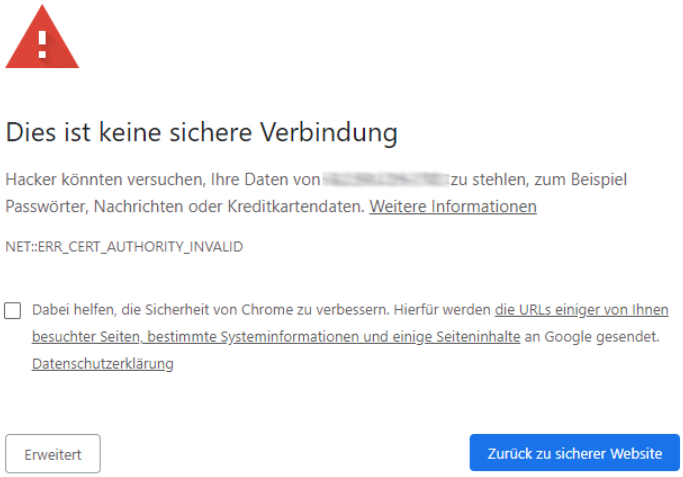



Abbildung 4: Zertifikatsfehler (Beispiel)

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

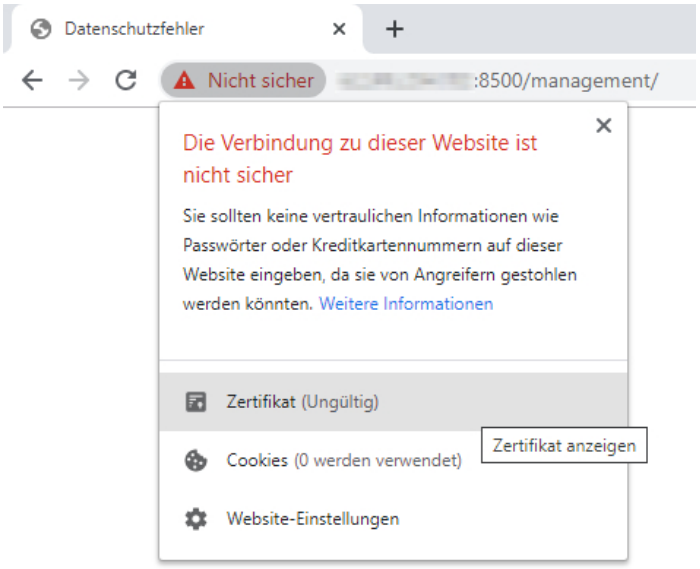



Abbildung 5: Informationen zu unsicherer Verbindung (Beispiel)

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

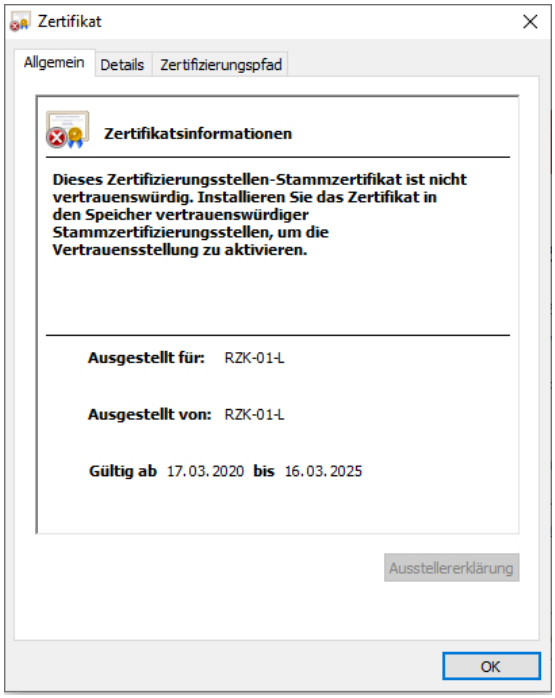



Abbildung 6: Zertifikatsinformationen

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

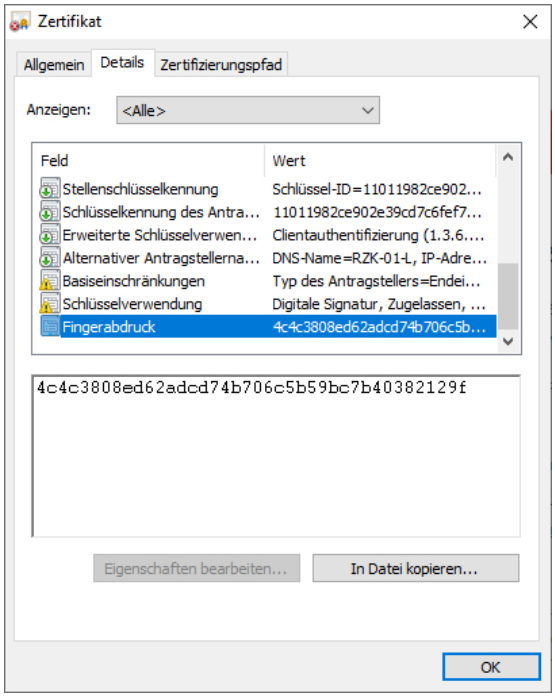



Abbildung 7: Zertifikatsdetails (Beispiel)

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

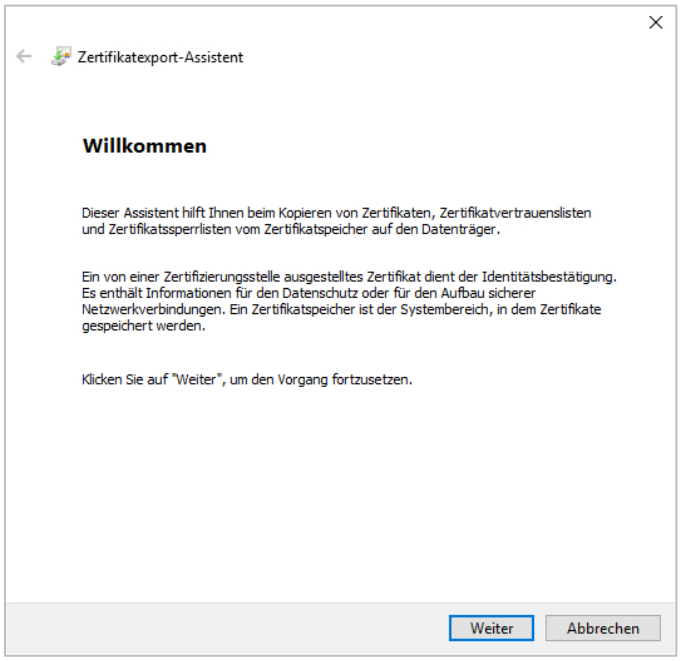



Abbildung 8: Zertifikatexport-Assistent

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

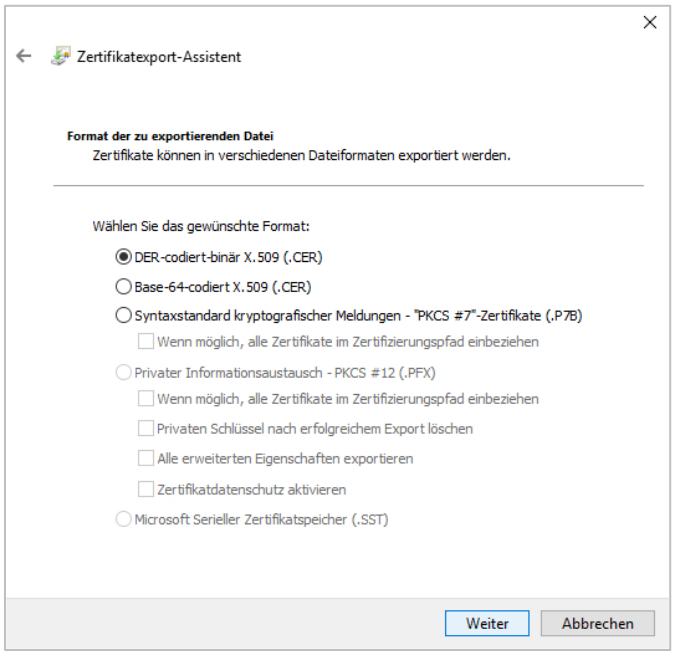



Abbildung 9: Zertifikatsformat

- Folgen Sie den Anweisungen des Zertifikatexport-Assistenten.

### 4.4.3 Zertifikat des Konnektors im Browser importieren

Die Administrationsschnittstelle zum Highspeedkonnektor wird über eine TLS-Verbindung abgesichert. Beim TLS-Verbindungsaufbau wird für die Authentisierung des Konnektors ein TLS-Zertifikat verwendet, das im Highspeedkonnektor hinterlegt ist. Um sicherzustellen, dass bei der initialen und allen weiteren Verbindunganfragen zum Highspeedkonnektor 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 korrekt durchgeführt wird, kann der Schutz von sensiblen Informationen wie Zugangsdaten nicht sichergestellt 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**.

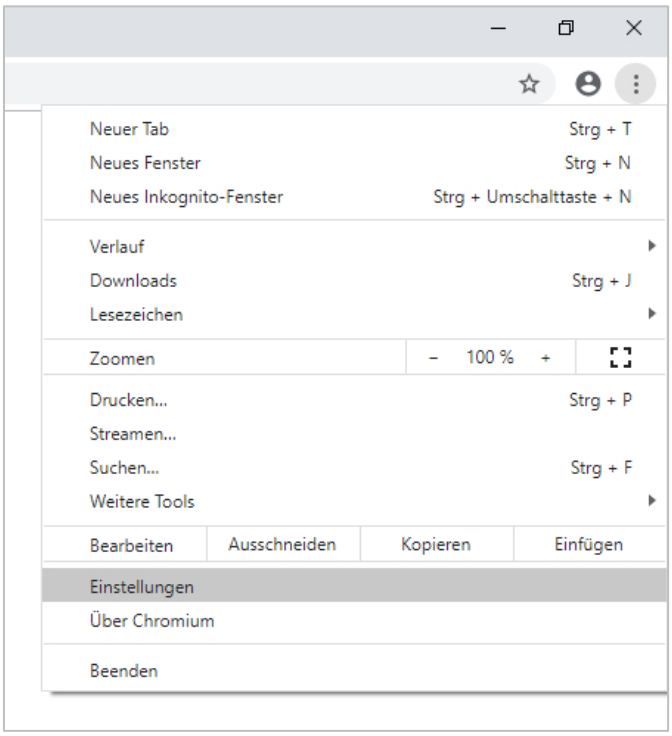



Abbildung 10: Browser-Einstellungen

- Öffnen Sie unter **Datenschutz und Sicherheit** den Bereich **Sicherheit**.

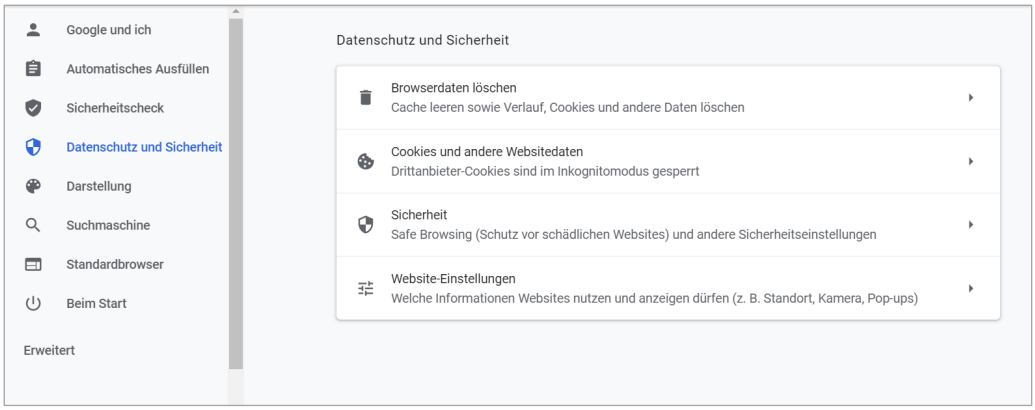



Abbildung 11: Bereich Sicherheit öffnen

- Klicken Sie **Zertifikate verwalten**.

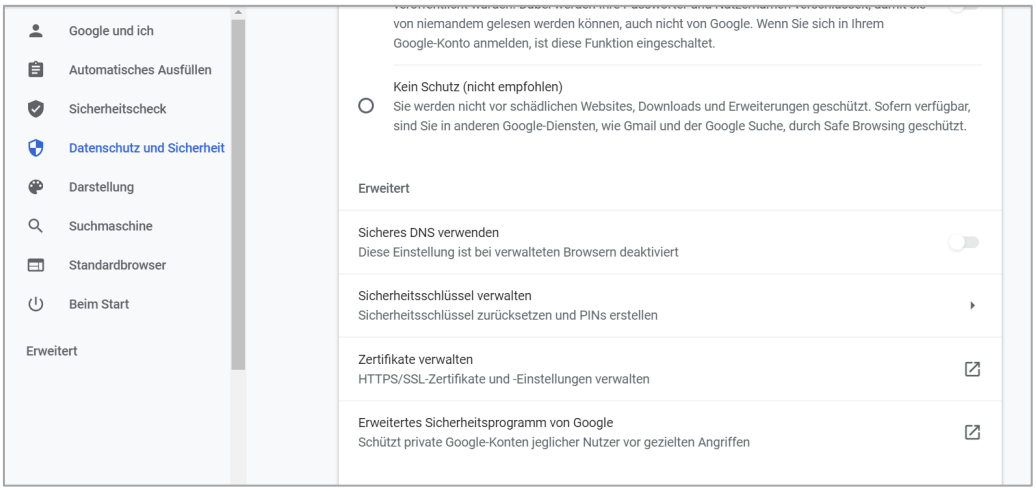



Abbildung 12: Zertifikate verwalten

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

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

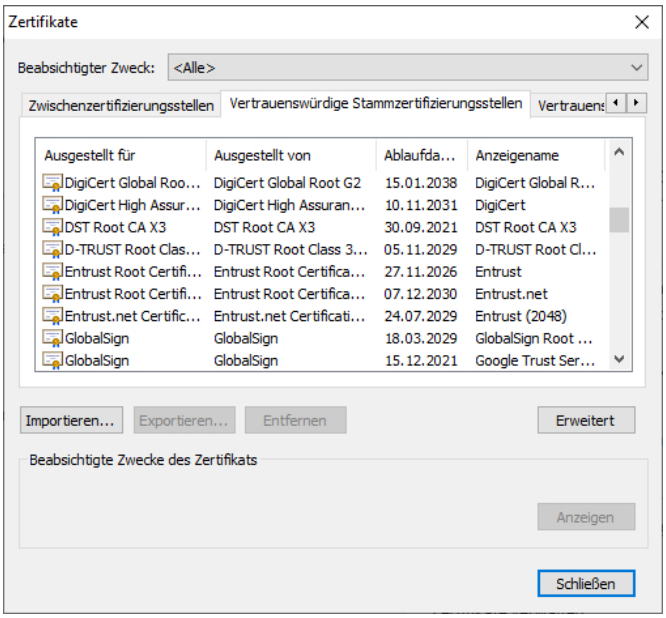



Abbildung 13: Importierte Zertifikate (Beispiel)

Der Zertifikatimport-Assistent öffnet sich:

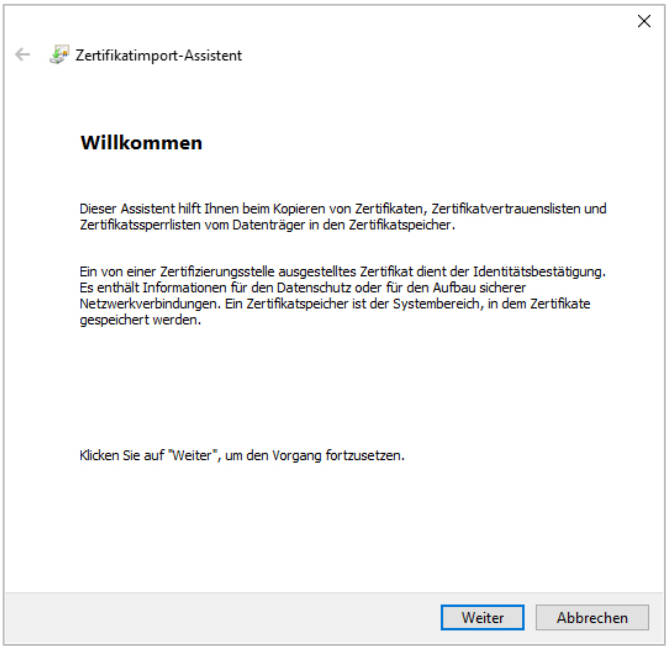



Abbildung 14: Zertifikatimport-Assistent

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

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

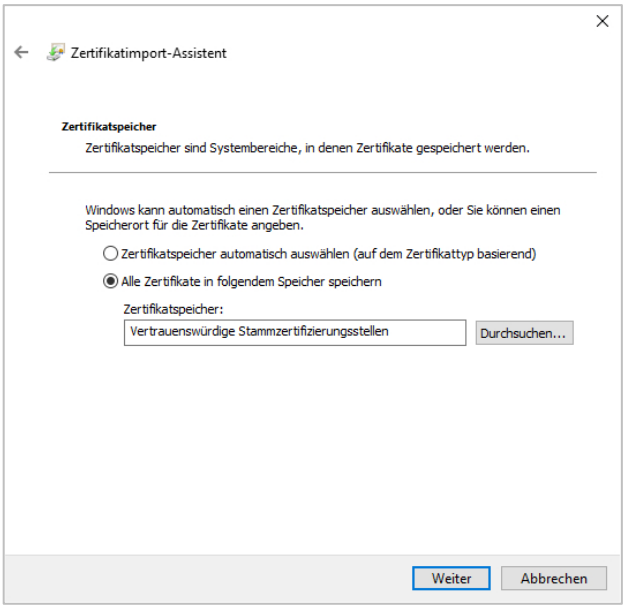



Abbildung 15: Zertifikatsspeicher

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

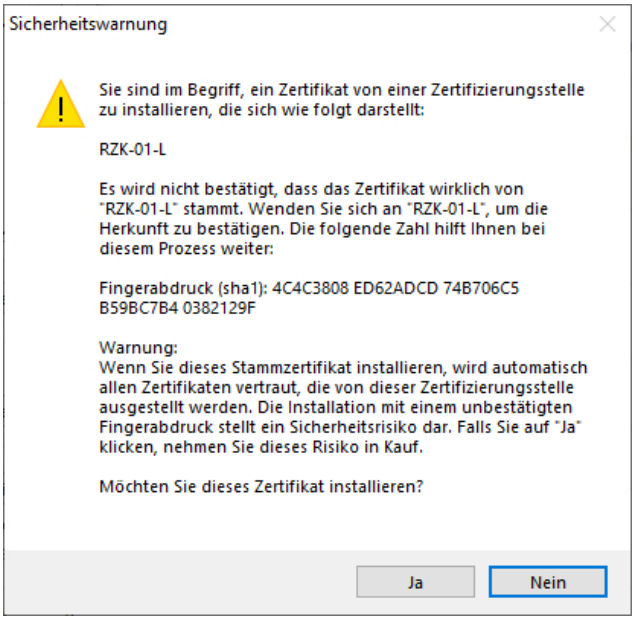



Abbildung 16: Sicherheitswarnung bei Import

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

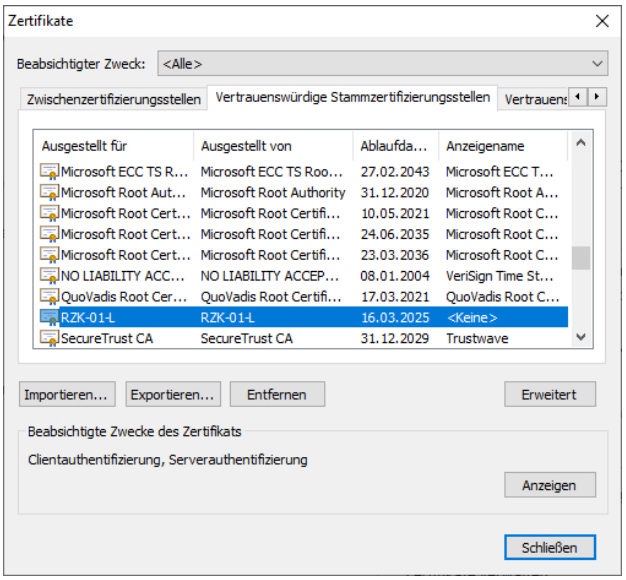



Abbildung 17: Importiertes Zertifikat des Highspeedkonnektors

- Starten Sie den Browser neu.

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

Sobald Sie einmal das Zertifikat in einem Clientsystem importiert haben, können Sie die Zertifikatsvalidierung für weitere Clientsysteme im lokalen Netzwerk durchführen, ohne eine direkte Verbindung zwischen dem Clientsystem und dem Highspeedkonnektor 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 Highspeedkonnektors im Browser weiterhin eine Sicherheitswarnung 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 nicht übereinstimmt, wenden Sie sich an den Betreiber.**

Falls Sie Remote Management zulassen wollen, muss das Zertifikat des 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 5.1).

Nach dem Import des Zertifikats des 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.**

**Nach der Durchführung einer Laufzeitverlängerung ändert sich das Zertifikat und entsprechend auch der Fingerprint. Es muss daher unbedingt eine erneute Validierung durchgeführt werden.**

### 4.4.4 Erstmalige Anmeldung

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

```
https://<IP-Adresse der Konnektor-Instanz>:9500/management
```

Die Bedienoberfläche des Konnektors öffnet sich.

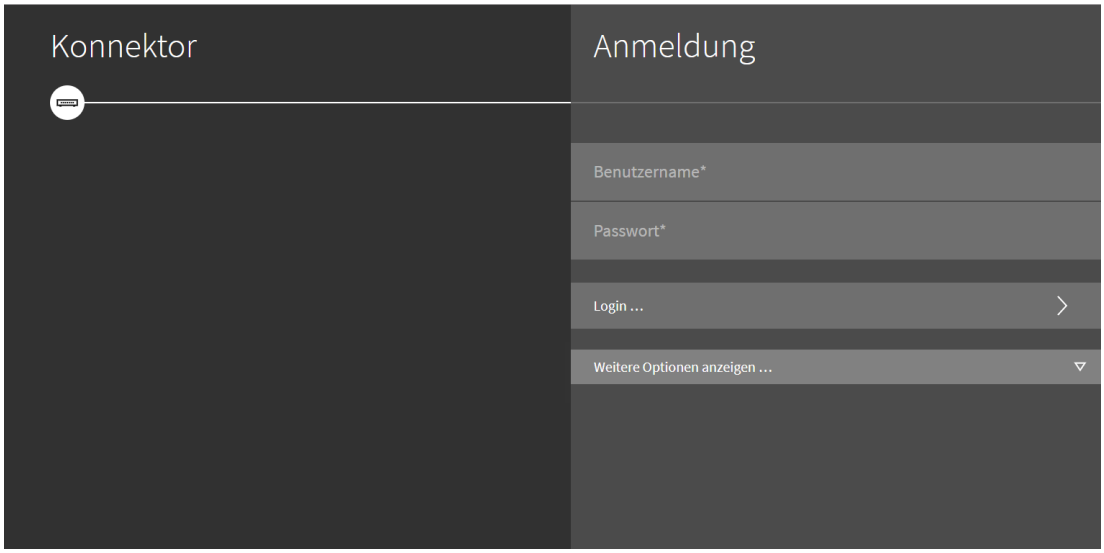



Abbildung 18: Anmeldedialog

- Melden Sie sich mit folgenden initialen Zugangsdaten an:

| | |
|---|---|
| Benutzername: | `super` |
| Passwort: | `konnektor` |

Sie werden aufgefordert, ein neues Passwort einzugeben.

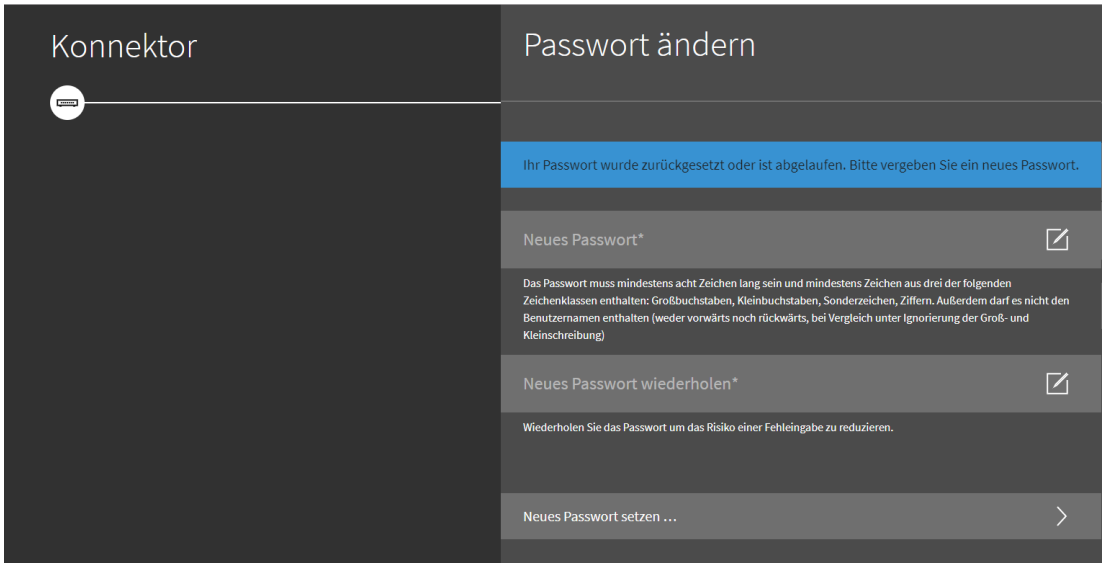



Abbildung 19: Passwort ändern

**Falls Sie bei der ersten Anmeldung nicht zum Passwortwechsel aufgefordert werden, darf der Highspeedkonnektor nicht in Betrieb genommen werden. Es besteht die Gefahr einer möglichen Kompromittierung. Benachrichtigen Sie in diesem Fall den Betreiber.**

- Geben Sie ein neues Passwort ein. Beachten Sie die Hinweise zu Passwörtern in Kapitel 3.1.
- Klicken Sie **Neues Passwort setzen**.

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

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

**Prüfen Sie bei der Inbetriebnahme die Systemzeit (siehe Kapitel 6.5.3) und passen Sie diese wenn notwendig an.**

**Prüfen Sie, dass keine weiteren administrativen Nutzer in der Konnektor-Instanz angelegt sind.**

**Verifizieren Sie, dass das Informationsmodell der Konnektor-Instanz bei der Ersteinrichtung leer/unkonfiguriert ist.**

Nach der Erstanmeldung können Sie auch das Zertifikat für den Port 8500 abrufen und im Browser hinterlegen, oder ein eigenes Zertifikat für den Port 8500 erzeugen oder hinterlegen. Danach ist je nach Wunsch die Nutzung der Ports 9500 oder 8500 möglich.

## 4.5 Übersicht der Verbindungswege (Management, SOAP, CETP) sowie die genutzten Zertifikate und Zertifikatsketten

Varianten und Optionen der Zertifikate und Zertifikatskette:

- Auslieferung:
  - TLS-Zertifikat des Konnektors (Management 8500, 8501)
  - TLS-Zertifikat des gSMC-K Objekts des Konnektors (Management 9500) & connector.sds
- Intern neu erzeugt
- Extern erzeugt und importiert

## 4.6 Vorgehensweise bei der ersten Konfiguration

Die Konfiguration des Highspeedkonnektors ist in Kapitel 5 beschrieben. Passen Sie die Konfiguration in folgender Reihenfolge an:

1. Prüfen Sie die Systemzeit (siehe Kapitel 6.5.3).
2. Legen Sie im Menü **System** die grundlegenden Betriebsbedingungen fest (siehe Kapitel 6.5).
3. Legen Sie Benutzer für die Personen an, die den Highspeedkonnektor über die Bedienoberfläche administrieren (siehe Kapitel 6.1).

   Falls die Administration mit Remote Management erfolgen soll, ist hierfür ein eigener Benutzer mit der Rolle Remote-Admin erforderlich. Aktivieren Sie bei Bedarf die Remote Management-Schnittstelle (siehe Kapitel 6.5.1).

   Falls Sie Remote Management zulassen wollen, muss das Zertifikat des Highspeedkonnektors 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.

   Nach dem Import des Zertifikats des 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.

4. Konfigurieren Sie die Dienste für die Anbindung an das lokale Netzwerk.

**Der Highspeedkonnektor verwendet intern die Netzsegmente 169.254.77.0/24 und 169.254.88.0/24. Um eine Kommunikation des Highspeedkonnektor mit angeschlossenen Netzsegmenten zu ermöglichen, darf es keine Überschneidung mit dem intern verwendeten Netzsegment geben.**

5. Verbinden Sie die Kartenterminals des lokalen Netzwerks (siehe Kapitel 7.1).
6. Legen Sie die weiteren Komponenten der Betriebsumgebung, wie Mandanten, Arbeitsplätze und Clientsysteme an (siehe Kapitel 6.3).

   Erstellen Sie für den Zugriff der Fachmodule auf die TI Aufrufkontexte.
7. Prüfung der bei der Produktion installierten TSL. Aufgrund der begrenzten zeitlichen Gültigkeit der TSL sowie den durch Produktion und Transport gegebenen Zeiträumen kann es dazu kommen, dass die in der Produktion eingebrachten TSL nicht mehr gültig sind. Bei Bedarf können Sie eine TSL über die Managementschnittstelle hochladen. Im Menü **System** können Sie im Bereich **Zertifikate** das jeweilige Ablaufdatum anzeigen lassen sowie eine TSL hochladen (siehe Kapitel 6.5.2).

   URL für den Abruf der aktuellen TSL:

   ```
   https://download.tsl.ti-dienste.de/TSL.xml
   ```
8. Konfigurieren Sie nach Bedarf die Fachmodule (siehe Kapitel 6.7).

# 5 Grundlagen zur Bedienoberfläche

Der Highspeedkonnektor wird über eine webbasierte Bedienoberfläche konfiguriert, die Sie im Browser aufrufen können. Beachten Sie die Hinweise zu empfohlenen Browsern in Kapitel 4.1.

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

## 5.1 An- und Abmeldung

Sie benötigen für die Anmeldung einen unterstützten Browser (siehe Kapitel 4.1.1). In Kapitel 12.2 finden Sie eine Übersicht der unterstützten Algorithmen.

### Anmeldung

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

```
https://<IP-Adresse der Konnektor-Instanz>:8500/management
```

Der Aufruf der Bedienoberfläche ist bei Verwendung des heruntergeladenen TLS-Zertifikats des Konnektors sowhl über die Ports 8500 oder 9500 möglich.

Verwenden Sie für Remote Management (siehe Kapitel 10) folgende Adresse:

```
https://<IP-Adresse der Konnektor-Instanz>:8501/management
```

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

**Tipp**

Erstellen Sie für den wiederholten Aufruf eine Verknüpfung.

### 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.**

## 5.2 Die Ansicht „Home“

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

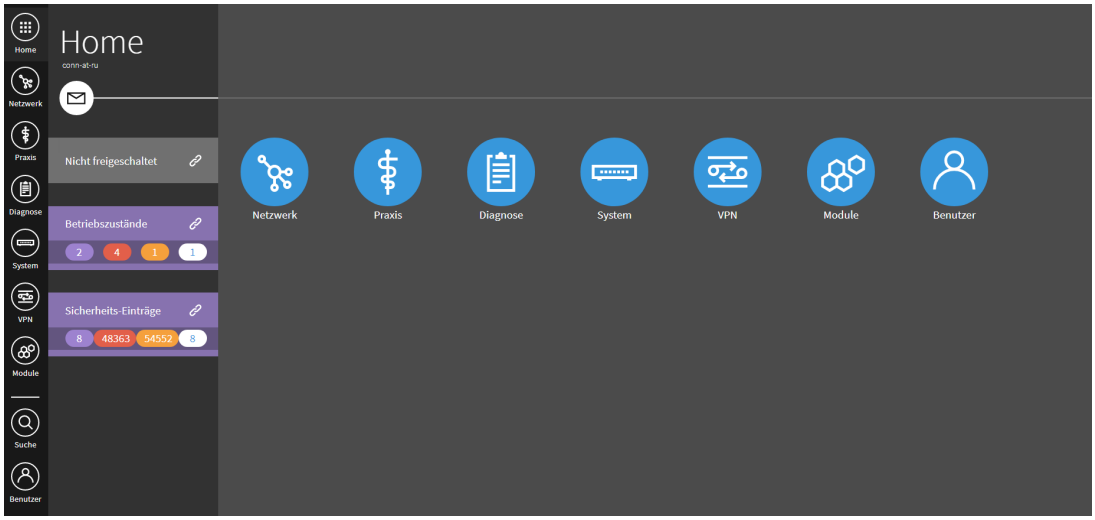



Abbildung 20: Ansicht „Home“

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

- Verbindungsstatus der TI
- Betriebszustände
- Meldungen, die seit dem letzten Ausloggen des aktuellen Administrators ausgegeben wurden (siehe Kapitel 12.4)

  Abhängig von der Schwere werden folgende Farbzuweisungen verwendet:

  - Gelbe (Warning)
  - Orange (Error)
  - Rot (Fatal)
  - Ohne (Info)

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

## 5.3 Übersicht der Menüs

In den Menüs konfigurieren Sie die Einstellungen für den Betrieb und die Wartung des Highspeedkonnektors. Die Namen der Menüs in der seitlichen Menüleiste können Sie über Ihre Profileinstellungen ein- und ausblenden (siehe Kapitel 6.1.1).

**Home**

Zur Ansicht **Home** zurückkehren.

**Benutzer**

In diesem Menü können Sie Ihr Profil einsehen, sich abmelden und die Administratoren des Highspeedkonnektors verwalten (siehe Kapitel 6.1).

**Netzwerk**

In diesem Menü konfigurieren Sie die Netzwerkschnittstellen und Netzwerkdienste (siehe Kapitel 6.2).

**Praxis**

In diesem Menü verwalten Sie Clientsysteme, Mandanten, Arbeitsplätze, Karten und Terminals (siehe Kapitel 6.3).

**Diagnose**

In diesem Menü haben Sie Zugriff auf Meldungen (siehe Kapitel 6.4).

**System**

In diesem Menü treffen Sie allgemeine Einstellungen zum System und verwalten Backups (siehe Kapitel 6.5).

**VPN**

In diesem Menü konfigurieren Sie die Anbindung an die TI (siehe Kapitel 6.6).

**Module**

In diesem Menü verwalten Sie die auf dem Highspeedkonnektor betriebenen Fachanwendungen (siehe Kapitel 6.7) und Lizenzen für lizenzierbare Funktionen (siehe Kapitel 8.9.1).

## 5.4 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

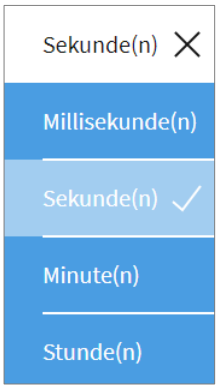

Eingabe in untergeordnetem Formular abschließen; Beachten Sie: Die Eingaben werden erst durch nochmaliges bestätigen mit ✓ gespeichert.


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:

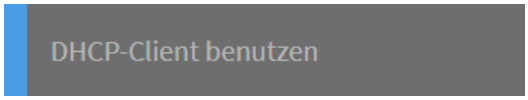
Seite lädt

Aktion wird durchgeführt

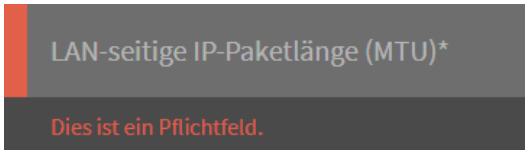
### 5.4.1 Die Prüfung von Eingaben

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




### 5.4.2 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 Highspeedkonnektors) werden in einem farbigen Hinweis am oberen Bildschirmrand angezeigt.

### 5.4.3 Die Suchfunktion

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

#### 5.4.3.1 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**.

#### 5.4.3.2 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.

#### 5.4.3.3 In den Suchergebnissen navigieren

Neben dem manuellen Anklicken von Suchergebnissen, um die betreffenden Dialogfenster 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.

## 5.5 Konfigurationsänderungen, die einen Neustart erfordern

Manche Konfigurationsänderungen erfordern bei der Administration des Highspeedkonnektors einen Neustart. Wenn Einstellungen vorgenommen werden, die einen Neustart des Highspeedkonnektors erfordern, wird ein Warnhinweis angezeigt. Bestätigen Sie diesen, um die Aktion durchzuführen.

Darüberhinaus ist ein Neustart nach der Aktualisierung der Firmware erforderlich. Der Betreiber wird Sie über die Firmwareupdates informieren.

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 | Erweiterte TLS-Einstellungen | Alle Einstellungen |
| Menü **Praxis** | | |
| Karten | Einstellungen | Timeout für Kartenoperationen |
| Karten | Einstellungen | Timeout für PIN-Kommandos |
| Terminals | Einstellungen | Service Discovery Zyklus |
| Terminals | Einstellungen | Service Announcement Port |
| Terminals | Einstellungen | Anzahl Keep-Alive Versuche |
| Terminals | Einstellungen | TLS Handshake Timeout |
| Terminals | Einstellungen | Display Anzeigedauer |
| Terminals | Einstellungen | Timeout für Pairing-Kommandos |
| Clientsysteme | Clientsystem-Einstellungen | TLS-Pflicht |
| Clientsysteme | Clientsystem-Einstellungen | Authentifizierung |
| Clientsysteme | Clientsystem-Einstellungen | Ungesicherter Zugriff auf Dienstverzeichnisdienst |
| Clientsysteme | Clientsystem-Einstellungen | Software-Server-Zertifikat |
| Menü **System** | | |
| Backup | Backup einspielen | |
| Menü **Module** | | |

| | | |
|---|---|---|
| Lizenz | Lizenz hochladen | |
| VSDM | Einstellungen | Intermediär-Servicename |

Tabelle 2: Konfigurationsänderungen, die einen Neustart erfordern

# 6 Menüs und Einstellungen

Nachfolgend sind die einzelnen Einstellungen zum Konfigurieren einer Instanz des Highspeedkonnektors beschrieben. Standardwerte und Wertebereiche für die einzelnen Konfigurationsparameter finden Sie in Kapitel 12.2.

Für den Highspeedkonnektor sind nicht alle Konfigurationsoptionen des Modularen Konnektors relevant. Diese Einstellungen sind nachfolgend gekennzeichnet (*). Bei nicht relevanten Einstellungen werden Eingaben vom System ignoriert.

## 6.1 Das Menü „Benutzer“

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


Abbildung 21: Menü „Benutzer“

### 6.1.1 Bereich „Mein Profil“

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

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

### 6.1.2 Bereich „Verwaltung“

Sie haben folgende Möglichkeiten:

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

  Für ein neues Benutzerkonto müssen der Benutzername und das initiale Passwort eingegeben sowie eine Benutzerrolle ausgewählt werden (siehe Kapitel 6.1.3). Beachten sie die Hinweise zu Passwörtern in Kapitel 3.1.

**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. Ausnahmen sind die initialen Passwörter von Remote-Administratoren. Diese dürfen nur an die vom Leistungserbringer beauftragten Remote-Administratoren persönlich weitergegeben werden.**

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

### 6.1.3 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 5.1) | Ja | Ja | Nein |
| Administrationszugriff über Remote Management | Nein | Nein | Ja |
| Werksreset durchführen (siehe Kapitel 8.5) | Ja | Ja | Nein |
| Verwaltung von Benutzerkonten (siehe Kapitel 6.1.2) | Ja | Nein | Nein |
| Passwörter zurücksetzen (siehe Kapitel 6.1.4) | Ja | Nein | Nein |
| Zeitintervall für den Passwortwechsel konfigurieren (siehe Kapitel 6.1.2) | Ja | Nein | Nein |
| Backup exportieren (siehe Kapitel 6.5.5) | Ja | Ja | Ja |
| Backup importieren (siehe Kapitel 6.5.5) | Ja | Nein | Nein |
| Remote Management initialisieren (siehe Kapitel 6.5.1, Einstellung „Remote-Management aktivieren“) | Ja | Ja | Nein |
| Remote Mangement konfigurieren (siehe Kapitel 6.5.1, Einstellung „Remote-Management erlauben“) | Ja | Nein | Nein |
| Verwaltung aller übrigen Konfigurationsdaten | Ja | Ja | Ja |

Tabelle 3: 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 SMBs für den Administrator
- Einsichtnahme in personenbezogene Daten in den Protokollen

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

### 6.1.4 Passwort eines Benutzers zurücksetzen

▶ Wählen Sie im Bereich **Benutzerverwaltung** das gewünschte Konto und Klicken Sie **Benutzer bearbeiten**.

▶ Geben Sie in den Feldern **Passwort** und **Passwort wiederholen** ein neues initiales Passwort ein. Der Benutzer wird beim nächsten Einloggen mit dem initialen Passwort automatisch aufgefordert, ein neues Passwort einzugeben.

## 6.2 Das Menü „Netzwerk“

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

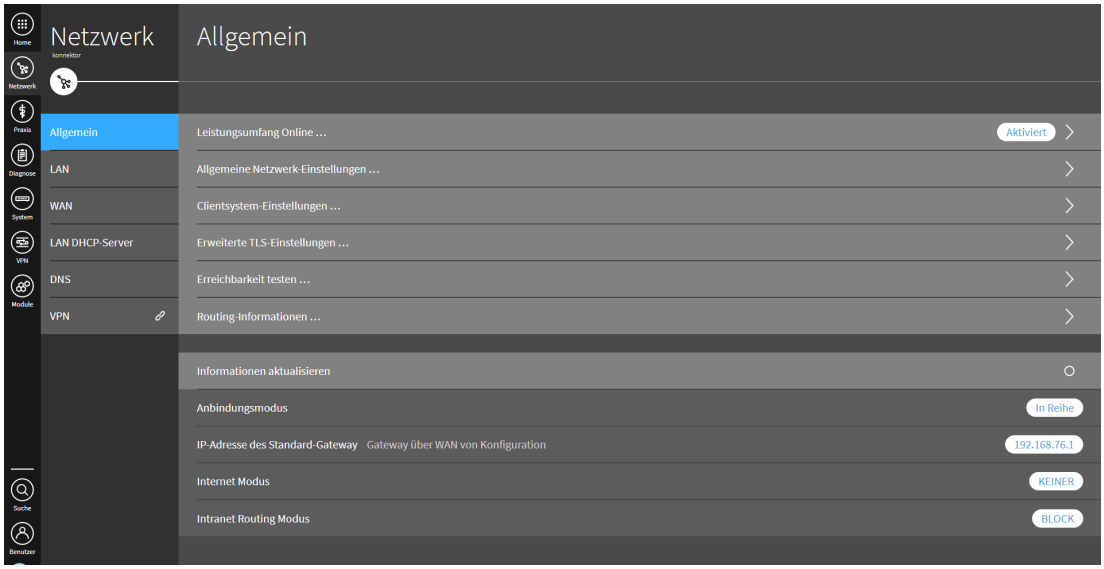



Abbildung 22: Menü „Netzwerk“

### 6.2.1 Bereich „Allgemein“

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

- Unter **Leistungsumfang Online ...** * legen Sie fest, ob der Konnektor online oder offline betrieben wird. Diese Einstellung wird vom Highspeedkonnektor nicht unterstützt.
- Unter **Allgemeine Netzwerk-Einstellungen ...** konfigurieren Sie die grundlegende Infrastruktur der Einsatzumgebung:
  - **Internet Modus** *
  - **Intranet Routing Modus** *

    Die Weiterleitung oder Blockade von Datenpaketen aus den internen Netzwerken
  - **Routen / Netzwerk-Segmente**

    Konfigurieren Sie Netzwerk-Segmente der Einsatzumgebung und bei Bedarf Routeradressen innerhalb der Segmente (Next Hop).

Wenn der Highspeedkonnektor im Betriebsmodus **In Reihe** verwendet wird, ist auch beim Standard-Gateway für alle Netzwerk-Segmente die Konfiguration einer Next Hop Adresse zwingend erforderlich.

- Unter **Clientsystem-Einstellungen ...** legen Sie Einstellungen zur Verbindung mit Clientsystemen konfiguriert werden (siehe Kapitel 6.3.3).

  **Beachten Sie die Sicherheitshinweise in Kapitel 6.3.3.**

- Unter **Erweiterte TLS-Einstellungen ...** konfigurieren Sie Einstellungen zum Transport Layer Security Protokoll (TLS), siehe Kapitel 12.3.2.1.
- 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.

### 6.2.2 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 Highspeedkonnektor im lokalen Netzwerk als DHCP-Client betrieben wird, kann mit **DHCP-Client Lease erneuern ...** eine neue IP-Adresse vom DHCP-Server angefordert werden.

### 6.2.3 Bereich „WAN“ *

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

### 6.2.4 Bereich „LAN DHCP-Server“ *

Der Highspeedkonnektor 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 Highspeedkonnektor selbst oder ein externer Server)
  - Default-Gateway (der Highspeedkonnektor selbst oder ein anderes gateway)
  - Netzmaske und Domain-Name
  - Lease-Dauer, nach der regelmäßig eine neue IP-Adresse angefordert wird
  - Routen
  - DHCP-Optionen

Unter **DHCP-Optionen** können Sie den DHCP-Dienst des Konnektors entsprechend [RFC2132] konfigurieren. Ändern Sie die vorgegebene Konfiguration nur, wenn Sie mit den DHCP-Optionen gut vertraut sind. Wenn Sie Einstellungen an den DHCP-Optionen vornehmen, sind Sie für den korrekten Betrieb des DHCP-Dienstes verantwortlich.

### 6.2.5 Bereich „DNS“ *

Hier werden Informationen über das lokale Netzsegment LE/KTR (Leistungserbringer/Kostenträger) angezeigt.

### 6.2.6 Verknüpfung „VPN“ *

Der Menüpunkt **VPN** öffnet das verknüpfte Menü **VPN** (siehe Kapitel 6.6).

## 6.3 Das Menü „Praxis“

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


Abbildung 23: Menü „Praxis“

### 6.3.1 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.
- Zertifikat der gSMC-K herunterladen

  Klicken Sie dazu auf das Zertifikat der gSMC-K. Es werden Informationen zum Zertifikat und zum Kartenhalter angezeigt und Sie haben folgende Optionen zum Herunterladen des Zertifikats:

  - **RSA Authentifizierungs-Zertifikat der primären SMCK ... ***
  - **ECC Authentifizierungs-Zertifikat der primären SMCK ...**

- Die im Konnektor verbauten gSMC-Ks können Sie anhand der Identifikationsnummer (ICCSN) ermitteln. Die ICCSN der Karten besteht aus 20 Stellen. Die elfte Stelle der ICCSN gibt dabei den Typ der verbauten Karten an. Im Highspeedkonnektor wird nur ein Kartentyp verwendet:

| Wert | Kartentyp |
|---|---|
| 9 | Hardwaresicherheitsmodul (HSM) |

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 Highspeedkonnektor 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).**

### 6.3.2 Bereich „Terminals“

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

Sie haben folgende Möglichkeiten:

- Unter **Einstellungen ...** können Einstellungen zum Verbindungsaufbau mit Kartenterminals sowie zur Behandlung von Fehlerfällen konfiguriert werden.

  Einstellungen der Fehlerbehandlung sollten nur im Rahmen eines Support-Falls nach Aufforderung des Herstellers geändert werden.

- Mit **Liste der Kartenterminals aktualisieren** wird die angezeigte Liste der Kartenterminals aktualisiert.

- Unter **Unterstützte Versionen** wird angezeigt, welche Versionen von eHealth-Kartenterminals vom Highspeedkonnektor 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 Highspeedkonnektor Updates für das Kartenterminal durchführen zu können (siehe Kapitel 9). 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 Verbindungseinstellungen an.

- **Kartenterminal dem Konnektor zuweisen ...**

  Bevor ein Kartenterminal genutzt werden kann, muss es dem Highspeedkonnektor durch Pairing zugeordnet werden (siehe Kapitel 7.1.1).

**Der Administrator ist für die korrekte Zuordnung von Kartenterminals verantwortlich.**

Nach dem Pairing sind weitere Zuordnungen des Kartenterminals erforderlich (siehe Kapitel 7.1.2).

- **Kartenterminal entfernen**

### 6.3.3 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 Highspeedkonnektors 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 Highspeedkonnektor und die Clientsysteme tauschen Daten über die SOAP/HTTP-Schnittstelle aus; zudem werden optional Benachrichtigungen über Ereignisse des Systeminformationsdienstes vom Highspeedkonnektor über das CETP-Protokoll an die Clientsysteme versendet (siehe Kapitel 6.4.5).

Um einen unbefugten Zugriff auf medizinische Informationen auszuschließen, ist eine sichere Installation in den Leistungserbringerinstitutionen unerlässlich, insbesondere mit der Einführung der elektronischen Patientenakte. Die LAN-Schnittstellen müssen vor unbefugten Zugriffen mit TLS und Client-Authentisierung geschützt werden, da ohne eine vom Konnektor erzwungene Client-Authentisierung ohne weitere Schutzmaßnahmen für einen Angreifer (auch über das Internet) mit geringem Aufwand beispielsweise ein Zugriff auf alle elektronischen Patientenakten möglich ist, die für die Leistungserbringerinstitution freigegeben sind.

Aus diesem Grund bietet der Highspeedkonnektor mehrere Möglichkeiten, um die Verbindung zum Client-System per TLS zu schützen. Dies erfolgt über die Option **TLS-Pflicht** in den Clientsystem-Einstellungen.

Wenn **TLS-Pflicht** aktiviert ist, werden HTTP-Nachrichten und CETP-Ereignisse nur über eine TLS-gesicherte Verbindung gesandt. In diesem Fall authentifiziert sich der Konnektor gegenüber dem Clientsystem mit dem Konnektor-Zertifikat, falls dies im Rahmen des TLS-Handshakes vom Clientsystem angefordert wird.

Als alternative Möglichkeit bietet der Highspeedkonnektor darüber hinaus die Option Software-Server-Zertifikat an (siehe Kapitel 6.3.3.2), mit der die Verbindung zum Clientsystem mit einem eigenen, selbsterzeugten Zertifikat abgesichert werden kann.

**Wenn die Option Software-Server-Zertifikat gewählt wird, beruht die Sicherheit der Verbindung vor allem auf der Vertraulichkeit des zugehörigen privaten Schlüssels. Dieser muss vom Administrator geschützt werden.**

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

1. TLS deaktiviert (keine Absicherung auf Transportebene, nur im Eigenbetrieb verwendbar)

- 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 (nur im Eigenbetrieb verwendbar)

   - 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 Highspeedkonnektors herunter und importieren Sie es im PVS.

3. TLS aktiviert, mit Server-Authentisierung und Client-Authentisierung mittels Benutzername und Passwort (nur im Eigenbetrieb verwendbar)

   - 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 Highspeedkonnektor besteht. Beachten Sie die Hinweise des PVS-Herstellers.
- Laden Sie für die Server-Authentifizierung mit **Konnektor-Zertifikat herunterladen ...** das Zertifikat des Highspeedkonnektors herunter und importieren Sie es im PVS.

4. TLS aktiviert, mit Server-Authentisierung und Client-Authentisierung per Zertifikat (im TI-Gateway modus verpflichtend)

   - 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. Beachten Sie die Hinweise des PVS-Herstellers.

     Folgende Zertifikate können für die Authentisierung verwendet werden:

     - Das Zertifikat der gSMC-K, das Sie im Bereich **Karten** herunterladen können (siehe Kapitel 6.3.1).
     - Ein neu erzeugtes oder ein anderes bereits bestehendes Zertifikat (siehe Kapitel 6.3.3.2).

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 Highspeedkonnektor im Rahmen des TLS-Verbindungsaufbaus anfordert, authentisiert sich der Highspeedkonnektor, 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 Highspeedkonnektor bestehen Sicherheitseinschränkungen. Ohne Authentisierung des Highspeedkonnektors 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 Highspeedkonnektor bietet keinen Schutz gegen Man-in-the-Middle Attacken.

Eine einseitige TLS-Authentisierung des Highspeedkonnektors 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.

#### 6.3.3.1 Sichere Anbindung des Clientsystems

Das Clientsystem kommuniziert mit dem Highspeedkonnektor über verschiedene Protokolle (SOAP, CETP, LDAP). Wie in Kapitel 6.3.3 beschrieben, kann die Kommunikation dabei durch einen TLS-Kanal abgesichert werden (siehe dazu Warnhinweis zu TLS in Kapitel 6.3.3).

In der folgenden Tabelle sind die verschiedenen Konfigurationsmöglichkeiten zusammengefasst:

| Protokoll | Clientsystem | Highspeedkonnektor |
|---|---|---|
| **TLS-Pflicht deaktiviert** (ANCL_TLS_MANDATORY=Disabled, ANCL_CAUT_MANDATORY=Disabled) | | |
| SOAP | TLS ist optional.<br>Wenn TLS verwendet wird, dann:<br>[ANCL_CAUT_MODE=CERTIFICATE<br>oder<br>ANCL_CAUT_MODE=PASSWORD<br>oder<br>NOAUTH] | TLS ist optional.<br>Wenn TLS verwendet wird, dann:<br>CERTIFICATE |
| CETP | Kein TLS | Kein TLS |
| LDAP-Proxy | TLS ist optional.<br>Wenn TLS verwendet wird, dann:<br>[ANCL_CAUT_MODE=CERTIFICATE<br>or<br>NOAUTH] | TLS ist optional.<br>Wenn TLS verwendet wird, dann:<br>CERTIFICATE |
| **TLS-Pflicht aktiviert** (ANCL_TLS_MANDATORY=Enabled<br>**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)<br>**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)<br>**Authentifizierungsmethode: Keine Authentifizierung** (ANCL_CAUT_MANDATORY=Disabled) | | |
| SOAP | NOAUTH | CERTIFICATE |
| CETP | CERTIFICATE | Optional CERTIFICATE (wenn vom Clientsystem angefordert) |
| LDAP-Proxy | NOAUTH | CERTIFICATE |

Tabelle 4: Konfigurationsmöglichkeiten für die Anbindung des Clientsystems

Dabei gelten folgende Festlegungen:

CERTIFICATE = Zertifikatsbasierte Authentisierung

PASSWORD = Authentifizierung mit Benutzername/Passwort

NOAUTH = Keine Authentisierung des Clientsystems

#### 6.3.3.2 Software-Server-Zertifikat verwenden

Die Zertifikatsbasierte Server-Authentisierung des Highspeedkonnektors basiert auf dem in der Gerätekarte des Konnektors (gSMC-K) sicher gespeicherten privaten Schlüssel und dem zugehörigen Zertifikat. Die gSMC-K als internes Sicherheitsmodul beinhaltet damit die Identität des Highspeedkonnektors.

Sollte die Verwendung dieses Konnektor-Zertifikates in Ihrer Netzwerkinfrastruktur zu Problemen führen, kann mit der Option Software-Server-Zertifikat ein alternatives Server-Zertifikat verwendet werden um die TLS-Verbindung zu den Clientsystemen abzusichern.

**Bei Verwendung eines durch den Administrator selbst erzeugten Zertifikates ist der Administrator für die Vertraulichkeit des privaten Schlüssels und die Inhalte des Zertifikates verantwortlich. Bei Problemen mit dem Zertifikat der Gerätekarte ist die Option Software-Server-Zertifikat aber immer einer Deaktivierung der TLS-Absicherung vorzuziehen, siehe dazu den entsprechenden Warnhinweis in Kapitel 6.3.3.**

Das verwendete Software-Server-Zertifikat können Sie durch die folgenden Schritte konfigurieren.

Um ein bestehendes Zertifikaz hochzuladen:

- Aktivieren Sie im Bereich **Clientsysteme** die Option **Software-Server-Zertifikat**.
- Wählen Sie **Zertifikat (als p12 Keystore-Datei) hochladen ...** .
- Geben Sie den Speicherort der Zertifikatsdatei und das zugehörige Passwort an.

Beachten Sie, dass bei der Verwendung eines eigenen TLS-Zertifikates die Anmeldung an der Bedienoberfläche des Konnektors nur über den Port 8500 möglich ist.

Um ein Zertifikat neu zu erstellen:

- Aktivieren Sie im Bereich **Clientsysteme** die Option **Software-Server-Zertifikat**.
- Klicken Sie **Zertifikat erstellen...** .
- Wählen Sie aus dem ausklappenden Menü das zu verwendende kryptografische Verfahren aus.
- Geben Sie im Feld **Hostnamen** optional den gewünschten Hostnamen ein.

  Wenn Sie keinen Hostname festlegen, wird der Konnektorname aus den Einstellungen verwendet.

- Geben Sie nach Aufforderung ein Passwort ein.

  Dadurch wird ein neues Zertifikat erstellt und im Bereich **Clientsysteme** angezeigt.

- Um das erstellte Zertifikat zu exportieren, klicken Sie auf  und wählen Sie anschließend **Zertifikat herunterladen …** .

Nutzen Sie zur Client-Authentisierung nach einem Werksreset ggf. das im Highspeedkonnektor erzeugte und heruntergeladene X.509-Zertifikat. Dieses können Sie mit der Option **Zertifikat hochladen …** in den Highspeedkonnektor einspielen. Gehen Sie dazu wie im Kapitel 8.4.2 beschrieben vor.

### 6.3.4 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.

### 6.3.5 Bereich „Mandanten“

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

Das Handbuch ist so formuliert, dass es den Leistungserbringer bzw. Administrator als eine Partei betrachtet, die alle notwendigen Entscheidungen zur Konfiguration des Gerätes trifft.

Wenn der Highspeedkonnektor für eine Gemeinschaft mehrerer Mandanten betrieben wird, wird dabei vorausgesetzt, dass für jede Administratoraktivität, die alle Mandanten betrifft (grundlegende Einstellungen am Gerät) auf geeignete Art ein Konsens herbeigeführt bzw. das Einverständnis aller Mandanten erteilt wurde. Das Handbuch geht daher in der Darstellung davon aus, dass es nur eine Partei gibt, die die Administration verantwortet.

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.
- 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.

### 6.3.6 Bereich „Aufrufkontexte“

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

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 einen Arbeitsplatz aus. Da jeder Aufrufkontext aus einer eindeutigen Kombination aus Mandant, Clientsystem und Arbeitsplatz bestehen muss, sind nicht zulässige Auswahlmöglichkeiten automatisch gesperrt und mit dem Symbol 🔒 gekennzeichnet.

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

## 6.4 Das Menü „Diagnose“

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

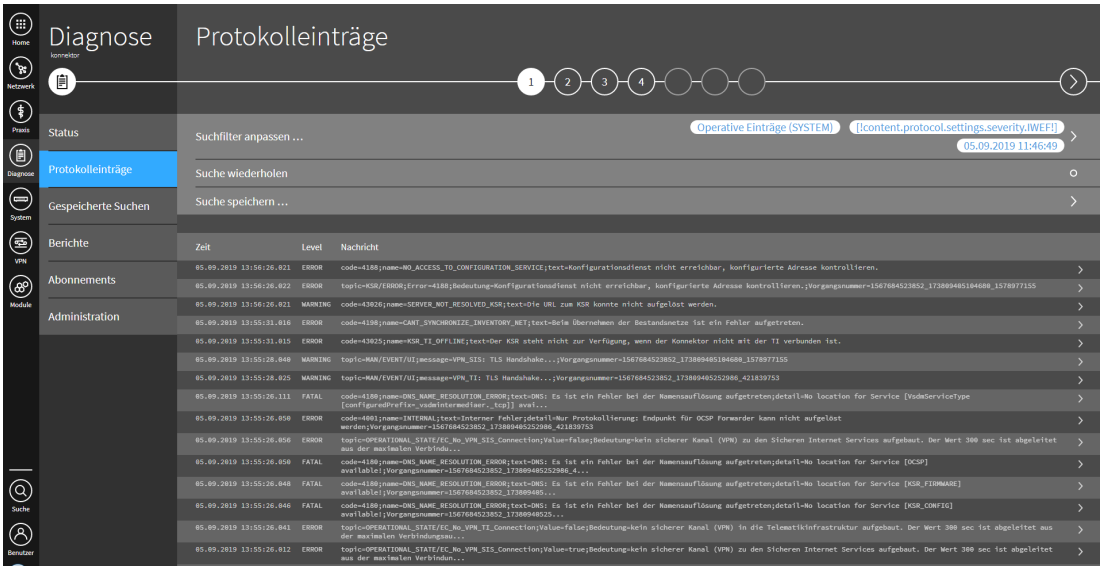



Abbildung 24: Menü „Diagnose“

### 6.4.1 Bereich „Protokolle“

Im diesem Bereich 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 12.4.

Mit **Suche speichern ...** können Sie die Suchfilter-Einstellungen abspeichern. Geben Sie dazu einen Namen ein und aktivieren Sie ggf. die Einstellung **Private Suche**, um den Zugriff auf die gespeicherte Suche einzuschränken; andere Benutzer können die gespeicherte Suche dann nicht verwenden oder verändern. Die Suche kann im Bereich **Gespeicherte Suchen** aufgerufen werden (siehe Kapitel 6.4.3).

Optional können Sie Meldungen exportieren und herunterladen:

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

### 6.4.2 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 2.3.9).

Mit **TI-Diagnose** können Sie die Erreichbarkeit der TI-Dienste prüfen.

### 6.4.3 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.

### 6.4.4 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 6.4.6) erstellten Einträge erfasst:

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

### 6.4.5 Bereich „Abonnements“

Benachrichtigungen über Ereignisse werden vom Highspeedkonnektor 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 Highspeedkonnektors registriert haben. Abonnenten können bei Bedarf gelöscht werden.

### 6.4.6 Bereich „Administration“

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

- Unter **Protokoll-Einstellungen ...** können Sie für die verschiedenen Protokolle (siehe Kapitel 12.4.1) festlegen, welche Ereignisse protokolliert werden und wie lange Protokolleinträge gespeichert bleiben.

Die Änderung der Vorhaltedauer um einen größeren Wert kann zu einer langen Verzögerung führen, während der die Bedienoberfläche des Highspeedkonnektors nicht auf Eingaben reagiert. Es wird empfohlen, den Wert um nicht mehr als 40 Tage auf einmal und ggf. in mehreren Schritten zu verändern.

  - 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.

  Klicken Sie dazu entweder auf **Alle Protokolle leeren** oder wählen Sie aus, welche Protokoll-Einträge geleert werden sollen. Es können nur operative Einträge und Performance-Einträge geleert werden.

**Wenn der Highspeedkonnektor für den Versand zum Hersteller vorbereitet werden soll, sichern Sie bitte vor der Ausführung dieser Aktion alle Logs des gesamten Betriebszeitraumes. Im Fall einer Gewährleistungsprüfung stehen somit alle Logs zur Verfügung.**

Das Sicherheitsprotokoll kann nicht geleert werden und bleibt auch bei einem vollständigen Werksreset erhalten (siehe Kapitel 8.5).

### 6.4.7 Bereich „Diagnose-Kit“

Dieser Bereich dient zur Analyse von Verbindungsproblemen zu Diensten in der TI. Wenn der Verdacht auf Verbindungsprobleme zur TI besteht, können Sie mit dem Diagnose-Kit eine Überprüfung durchführen, um das Problem einzugrenzen.

- Klicken Sie dazu in den Abschnitten **Erreichbarkeitstest** und **Funktionstest** jeweils auf **Test starten**.

  Sollte es Verbindungsprobleme geben, werden diese mit entsprechenden Hinweisen aufgeführt, die dann an den DVO oder Support übermittelt werden können.

## 6.5 Das Menü „System“

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

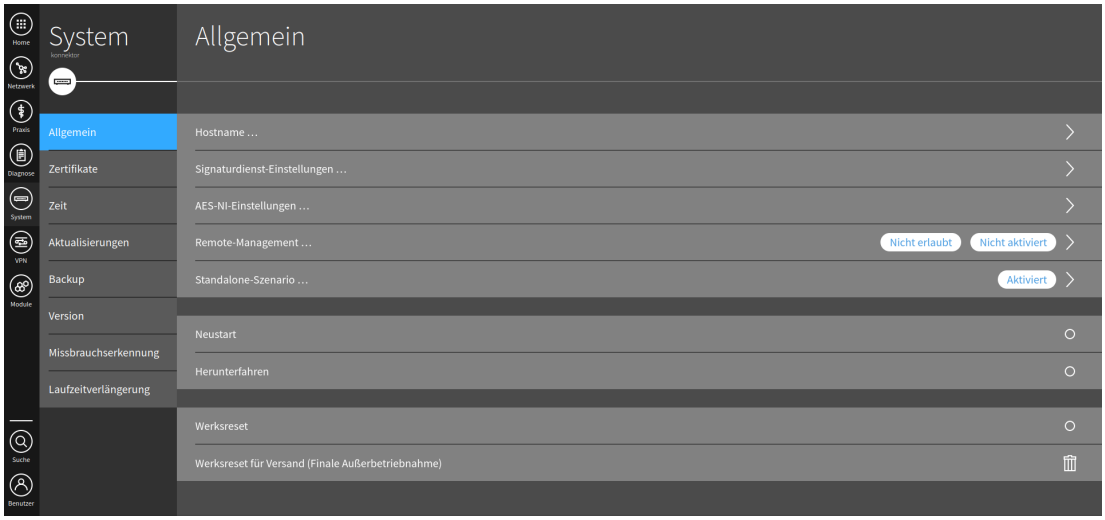



Abbildung 25: Menü „System“

### 6.5.1 Bereich „Allgemein“

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

Sie haben folgende Möglichkeiten:

- **Name … ***

  Legt den Hostnamen des Highspeedkonnektors fest.

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

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

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

- **Signaturdienst-Einstellungen** (siehe Kapitel 2.3.6)
  Legt fest, ob die Signaturanwendungskomponente aktiv ist und steuert den Einfachsignaturmodus sowie die Funktion Komfortsignatur (siehe Kapitel 6.5.1.1).

- **AES-NI-Einstellungen** *
  Steuert die Hardwareunterstützung AES-NI.

**Nach jeder Änderung der Hardwareunterstützung AES-NI ist der Neustart des Highspeedkonnektors erforderlich.**

- **Remote-Management ...**
  Wenn Remote Management erlaubt und aktiviert ist, kann der Highspeedkonnektor über das öffentliche Netzwerk administriert werden.

- **Standalone-Szenario ...** *
  Wenn aktiviert, arbeitet der Highspeedkonnektor ohne angeschlossene Clientsysteme.

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

- **Herunterfahren**
  Ein Herunterfahren des Konnektors wird beim Highspeedkonnektor/TI-Gateway nicht mehr angeboten. Führen Sie im Bedarfsfall einen Neustart durch. Falls ein Neustart nicht ausreicht, wenden Sie sich bitte an den Betreiber.

- **Werksreset** *
  Führt einen vollständigen Werksreset aus; beachten Sie das Kapitel 8.5.

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

#### 6.5.1.1 Komfortsignatur

Die Konfigurationseinstellungen zur Komfortsignatur sind, unabhängig von der Lizenzierung, ab Firmware PTV4 immer sichtbar. Gleiches gilt für die SOAP-Endpunkte des SignatureServices. Wenn die vorgenannten Voraussetzungen nicht erfüllt sind, führt deren Aufruf zu einer Fehlermeldung (SOAP-Fault) mit der Aussage, dass kein passender Endpunkt gefunden werden konnte.

Zusätzlich wird die Info-Meldung "Die Komfortsignatur-Funktionalität steht aufgrund fehlender Lizenzierung nicht zur Verfügung." in das Protokoll geschrieben.

Bei aktivierter Komfortsignatur muss der Inhaber des HBA die PIN nicht mehr für jeden Signaturauftrag einzeln eingeben. Stattdessen bleibt die PIN für eine konfigurierbare Zeit und eine konfigurierbare Zahl an Signaturaufträgen gültig (siehe Kapitel 2.3.6).

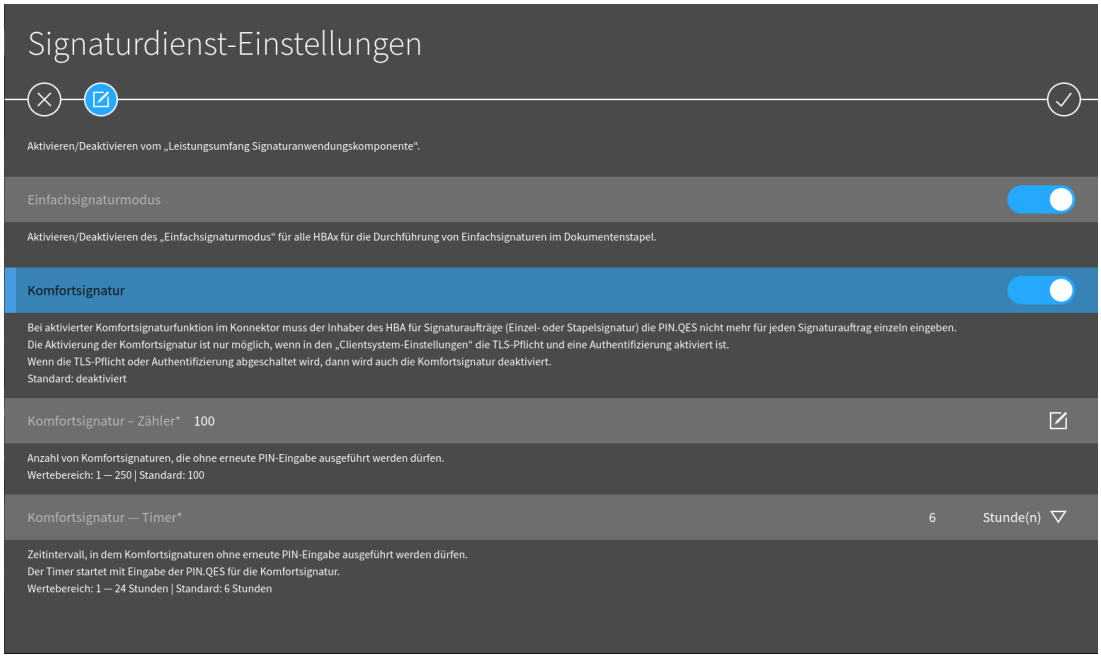



Abbildung 26: Komfortsignatur aktivieren

- Aktivieren Sie dazu die Einstellung **Komfortsignatur**.

**Beachten Sie: Wenn die Funktionen „TLS-Pflicht" oder „Clientauthentifizierung" (siehe Kapitel 6.3.3.1) deaktiviert sind, ist die Verwendung der Komfortsignatur nicht zulässig. Es wird eine entsprechende Warnmeldung angezeigt. Wenn eine dieser Funktionen deaktiviert wird, dann wird automatisch auch die Komfortsignatur deaktiviert.**

- Passen Sie optional die Einstellung **Komfortsignatur-Zähler** an.

Diese legt die maximale Anzahl von Signaturaufträgen fest, die ohne erneute Eingabe der PIN durchgeführt werden können.

- Passen Sie optional die Einstellung **Komfortsignatur-Timer** an.
  Diese legt fest, wie lange Signaturaufträge ohne erneute Eingabe der PIN durchgeführt werden können.

### 6.5.2 Bereich „Zertifikate“

Der Zertifikatsdienst stellt Funktionen zur Validierung von Zertifikaten zur Verfügung (siehe Kapitel 2.3.2).

Sie haben folgende Möglichkeiten:

- **ECC-Migration ...** *
  Hier können Sie die für die Migration der kryptographischen Verfahren auf ECC-basierte Schlüssel (siehe Kapitel 2.3.3) erforderliche TSL-Datei und die zugehörigen Zertifikate manuell hochladen.
- Unter **Einstellungen ...** können Zeitfristen für Aktualisierungen und OCSP-Abfragen sowie eine Downloadadresse für die TSL konfiguriert werden.
- Unter **Missbrauchserkennung-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 **Zusätzliche CA-Zertifikate für die Verschlüsselung ...** können CA-Zertifikate importiert werden und stehen dann für den Verschlüsselungsdienst zur Verfügung (siehe Kapitel 8.4).

  **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.**
- Das manuelle Hochladen von TSL und BNetzA-VL (Vertrauensliste der BNetzA) wird vom Highspeedkonnektor nicht unterstützt.

Bei einer bestehenden Verbindung zur TI werden diese Dateien normalerweise automatisch aktualisiert.

- 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.

### 6.5.3 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 12.1.3).

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

**Beachten Sie: Die im Konnektor eingestellte Zeit darf nicht mehr als 30 Sekunden von der in der TI gültigen Zeit abweichen, andernfalls ist eine Verbindung zur TI nicht möglich. Prüfen Sie die Zeit mindestens bei der Inbetriebnahme und passen Sie sie wenn notwendig an.**

### 6.5.4 Bereich „Aktualisierungen“

In diesem Bereich verwalten Sie Aktualisierungen für Kartenterminals (siehe auch Kapitel 9):

- Unter **Einstellungen ...** können Sie die Einstellungen für automatische Update konfigurieren (siehe Kapitel 9.1.2).
- 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.

### 6.5.5 Bereich „Backup“

In diesem Bereich können Sie Systemsicherungen (Backups) erstellen und importieren (siehe Kapitel 8.8).

### 6.5.6 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.

### 6.5.7 Bereich „Missbrauchserkennung“

In diesem Bereich 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.

### 6.5.8 Bereich „Laufzeitverlängerung“ *

Der Bereich "Laufzeitverlängerung" unterstützt Sie bei der Durchführung der Laufzeitverlängerung bei Ihrem Konnektor. Beachten Sie die Hinweise zur Laufzeitverlängerung in Kapitel 8.6. Zur Laufzeitverlängerung muss der Konnektor beim Zugangsdienst der TI freigeschaltet sein.

Nachfolgend aufgeführte Schritte sind für die Verlängerung der Zertifikatslaufzeiten erforderlich, wobei die angegebene Reihenfolge eingehalten werden muss. Die Durchführung der Backups ist optional, wird aber dringend empfohlen. Alle anderen Schritte sind verpflichtend für die vollständige Durchführung der Laufzeitverlängerung. Für verpflichtende Schritte wird der jeweilige Status ("Offen" bzw. "Erledigt") in der Konnektoroberfläche angezeigt. Zudem führen Verlinkungen (graue Schaltflächen) bei den einzelnen Schritten zu den zugehörigen Untermenüs, bei denen die Einstellungen vorgenommen werden müssen.

1. Rufen Sie die neuen Zertifikate mit verlängerter Laufzeit ab.

   Falls es beim Download der Zertifikate zu Fehlern kommt, werden diese angezeigt und der Vorgang abgebrochen.

   Importieren Sie alternativ Zertifikate aus einer lokalen Quelle, beispielsweise wenn aufgrund abgelaufener Zertifikate keine Verbindung zur TI möglich ist.

   Anschließend werden die importierten Zertifikate angezeigt.

2. Es wird empfohlen, ein Backup des aktuellen Systemzustandes zu erstellen (siehe Kapitel 8.88.8).

3. Schalten Sie den Konnektor anschließend beim VPN-Zugangsdienst mit den neuen Zertifikaten frei (siehe Kapitel 6.6.2.3).

4. Legen Sie in den Clientsystem-Einstellungen (siehe Kapitel 6.3.3) die neuen Zertifikate für die Authentifizierung gegenüber dem Clientsystem fest.

   Aktivieren Sie dafür unter **Praxis** > **Clientsysteme** > **Clientsystem-Einstellungen** den Schalter bei **Laufzeitverlängerung: Erneuerte ID.AK.Aut für Authentisierung des Konnektors gegenüber Clientsystemen verwenden**.

5. Es wird empfohlen, nun erneut ein Backup mit den neuen Zertifikaten zu erstellen.

6. Nach Abschluss wird Ihnen am Ende der Anleitung eine Übersicht der verwendeten Zertifikate angezeigt.

7. Legen Sie schließlich in den Einstellungen der einzelnen Clientsysteme das zu verwendende Zertifikat fest. Beachten Sie dazu die Hinweise des PVS-Herstellers.

## 6.6 Das Menü „VPN“

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


Abbildung 27: Menü „VPN“

### 6.6.1 Bereich „TI-Status“ *

Nach erfolgreicher Freischaltung stellt der Highspeedkonnektor die Verbindungen zur TI her. In diesem Bereich werden Informationen zum aktuellen Verbindungsstatus angezeigt.

Unter **VPN-Verbindung TI ...** können Sie Details zur Verbindungen prüfen sowie die Verbindung bei Bedarf manuell trennen und wiederherstellen.

Die Einstellung **VPN-Verbindung SIS ...** * wird vom Highspeedkonnnektor nicht unterstützt.

Unter **Einstellungen** können Netzwerkeinstellungen für den Zugang zur TI angepasst werden:

- Die Zeitdauer innerhalb der ein Netzwerkdienst antworten muss, bevor das System einen Timeout-Fehler meldet (TI Service Timeout)
- Bandbreitenbeschränkung des ausgehenden Datenverkehrs für die Kommunikation mit der TI

### 6.6.2 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 Highspeedkonnektor hinter dem NAT-Gateway ermittelt werden kann.**

Unter **VPN-Einstellungen ...** können Netzwerkeinstellungen für den Zugang zur TI 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 (siehe Kapitel 6.6.2.5)

Unter **VPN-Zugangsdienstanbieter ...** legen Sie den DNS-Server und die DNS-Domain für den Zugangsdienst fest, um die Verbindung zur TI zu ermöglichen. Der DNSSEC Trustanchor ist bis zu 5 Jahre gültig und bedarf keiner Administrierung.

Legen Sie einen DNS-Server im Transportnetz fest und konfigurieren Sie die Einstellungen des DNS-Servers.

**Bitte achten Sie stets darauf, dass mindestens ein DNS-Server für das Transportnetz eingetragen ist, bevor Sie die Konfiguration speichern.**

Wenn der Highspeedkonnektor als DHCP-Server betrieben wird, wird die Adresse des DNS-Servers automatisch den Clientsystemen mitgeteilt, sofern in den Clientgroups kein externer DNS-Server konfiguriert ist.

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

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

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

### 6.6.2.1 Highspeedkonnektor 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).
- Wählen Sie den Typ des SMC-K Zertifikats für die Freischaltung (ECC).

Bitte informieren Sie sich vor der Registrierung mit ECC-Zertifikat, ob ihr VPN-Zugangsanbieter diesen Zertifikatstyp unterstützt. Zur Drucklegung dieser Bedienungsanleitung unterstützten nicht alle Anbieter diesen Zertifikatstyp.

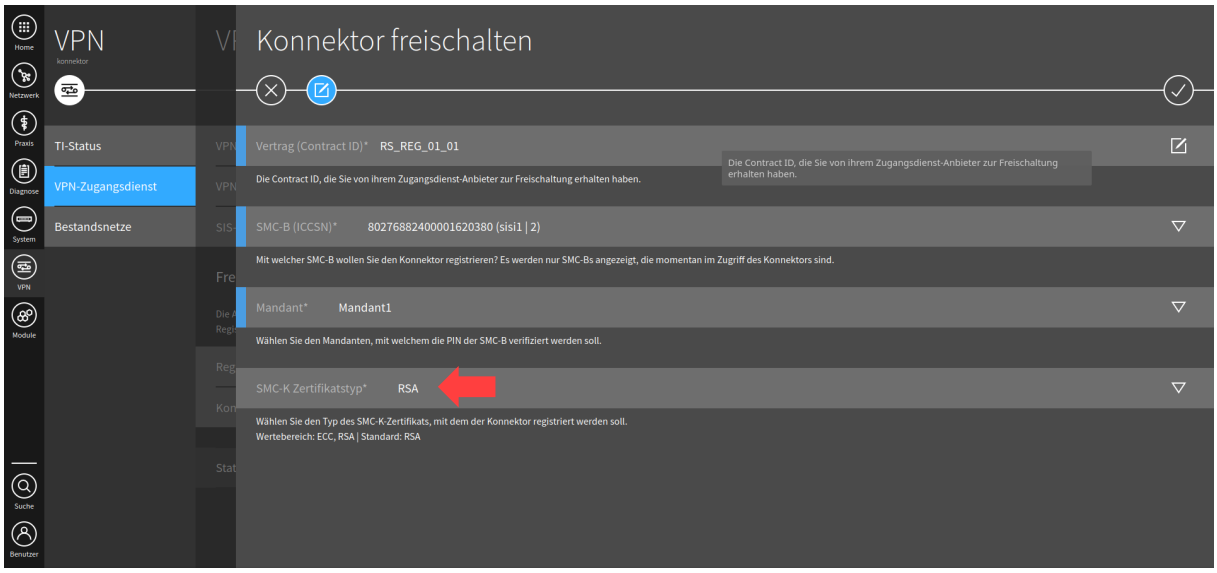



Abbildung 28: Auswahl des Zertifikatstyps für die Freischaltung

Bei jeder Freischaltung kann nur ein einziger Zertifikatstyp ausgewählt werden.

Falls der Zugangsdienst eine Mehrfachregistrierung unterstützt, können Sie die Freischaltung anschließend mit dem jeweils anderen Zertifikatstyp wiederholen.

- Geben Sie die zugehörige Vertragsnummer ein.

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

#### 6.6.2.2 Freischaltung des Highspeedkonnektors zurücknehmen

**Im Fall einer Mehrfachregistrierung wird hierdurch die Freischaltung aller Zertifikate zurückgenommen.**

- Klicken Sie **Konnektorfreischaltung zurücknehmen**.
- Um eine zurückgenommene Freischaltung wieder Herzustellen, klicken Sie bei Bedarf **Konnektor erneut freischalten**.

#### 6.6.2.3 Freischaltung des Konnektors nach Laufzeitverlängerung

Der Highspeedkonnektor bietet eine Funktion zur Verlängerung der Laufzeit der Konnektorzertifikate (siehe Kapitel 6.5.8).

**Möglicherweise ist vor der erneuten Registrierung mit den verlängerten Zertifikaten die Deregistrierung der alten Zertifikaten nötig. Halten Sie diesbezüglich Rücksprache mit Ihrem Zugangsdienstanbieter, bevor Sie eine Deregistrierung vornehmen.**

Nach dem Bezug neuer Zertifikate muss der Konnektor beim VPN-Zugangsdienst erneut freigeschaltet werden.

Sie können dabei festlegen, ob die erneute Freischaltung mit neuen Zertifikaten automatisch geschehen soll, und ob dabei die Migration der kryptographischen Verfahren auf ECC-basierte Schlüssel erfolgen soll.

#### 6.6.2.4 Freigeschaltetes Zertifikat ändern

Wenn das freigeschaltete Zertifikat geändert werden soll und der Zugangsdienst keine Mehrfachregistrierung unterstützt, muss die Freischaltung zuerst zurückgenommen werden:

- Klicken Sie **Konnektorfreischaltung zurücknehmen**.
- Klicken Sie anschließend **Konnektor freischalten ...** und führen Sie die Freischaltung mit dem gewünschten Zertifikat durch.

#### 6.6.2.5 Konfiguration der Paketgröße (MTU)

Der Highspeedkonnektor ermöglicht im Bereich **VPN-Einstellungen** die Konfiguration der maximalen Paketgröße (MTU) für die VPN-Kanäle zur TI.

Beachten Sie, dass der Wert bei der Konfiguration eine bestimmte Schwelle nicht überschreiten darf, damit die Pakete auf dem Transportweg nicht unerwartet verworfen werden. Diese Schwelle wird maßgeblich durch die MTU der ausgehenden Transportschnittstelle bestimmt.

Die Transportschnittstelle ist dabei durch den Anbindungsmodus vorgegeben:

- Im Anbindungsmodus Reihe ist die Transportschnittstelle die WAN-Schnittstelle
- Im Anbindungsmodus Parallel ist die Transportschnittstelle die LAN-Schnittstelle

Wenn Sie die MTU der Transportschnittstelle auf einen Wert oberhalb des Schwellwertes einstellen, wird eine Fehlermeldung generiert. Diese Meldung tritt ebenfalls auf, wenn die MTU der Transportschnittstelle heruntergesetzt wird und die voreingestellte MTU des VPN daraufhin den Schwellwert verletzt.

Die Fehlermeldung kann beispielhaft wie folgt lauten:

```
Fehler beim Speichern: Fehler (VPN/Einstellungen), der maximale TI
Paketgröße-Wert ist ungültig (1500 > 1422 [WAN MTU - ESP Overhead])
```

Wenn der Highspeedkonnektor beim Verbindungsaufbau zur TI feststellt, dass für das VPN ein zu hoher MTU-Wert konfiguriert ist, wird dieser automatisch angepasst.

### 6.6.3 Regelwerk des Paketfilters konfigurieren *

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

### 6.6.4 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 Highspeedkonnektor 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 Highspeedkonnektor entsprechend der aktuellen Paketfilter-Regeln behandelt (siehe Kapitel 6.6.3). Für die Clientsysteme ist sicherzustellen, dass alle angebundenen Bestandsnetze auch in der aktuellen Liste des Highspeedkonnektors 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.
- Sie können alternativ festlegen, dass neue verfügbare Bestandsnetze automatisch aktiviert werden.

## 6.7 Das Menü „Module“

Im Menü **Module** werden alle lizenzierten Fachmodule angezeigt (siehe Kapitel 8.8.2.1). Für manche Fachmodule können weitere Einstellungen vorgenommen werden.

Im Bereich **Lizenz** können Sie die Lizenzen des Highspeedkonnektors verwalten (siehe Kapitel 6.7.5).

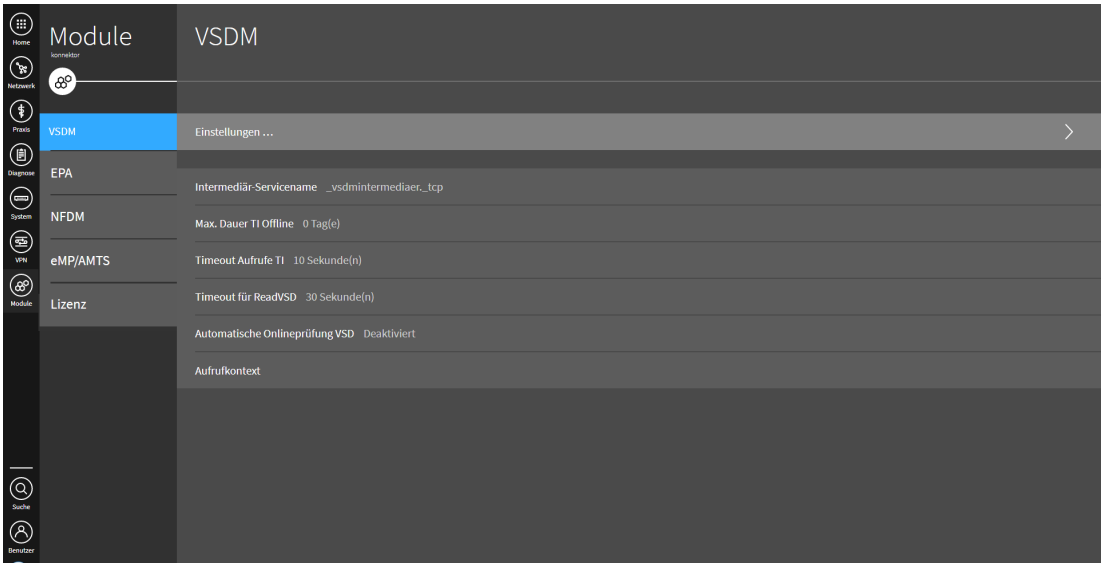



Abbildung 29: Menü „Module“

### 6.7.1 Hinweise zum 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 Highspeedkonnektor automatisch eine neue zufällige Zeichenkette.

### 6.7.2 Hinweise zum Fachmodul ePA

Das Fachmodul ePA bietet dem Primärsystem Funktionen für die Archivierung und Verwaltung von medizinische Dokumenten von Versicherten. Die Ablage der Dokumente geschieht im zentralen Fachdienst ePA-Aktensystem der TI in verschlüsselter Form.

Die Verschlüsselung der Dokumente für die Ablage im ePA-Aktensystem und die Entschlüsselung archivierter Dokument für den Abruf durch das Primärsystem führt das Fachmodul ePA unter Nutzung zweier voneinander unabhängiger Schlüsselgenerierungsdienste (SGD) der TI aus. Der Prozess stellt dabei sicher, dass die abgeleiteten Schlüssel für Versicherte auch bei einem Wechsel ihrer eGK stets gleich bleiben und die Weiterverarbeitung ihrer Patientenakten möglich ist.

Um eine im ePA-Aktensystem eingehende Anfrage verarbeiten zu können, wird für jedes Dokument zusätzlich ein Satz an Metadaten gespeichert. Diese umfassen beispielsweise das Dokumentenformat (z. B. PDF), den Dokumententyp (z. B. Notfalldatensatz), den Erstellungszeitpunkt und den Autoren. Der Zugriff auf die Metadaten geschieht in unverschlüsselter Form ausschließlich in einer abgesicherten Laufzeitumgebung (sog. Vertrauenswürdige Ausführungsumgebung, VAU).

- **Aktivierung/Deaktivierung der mandantenübergreifenden Akten-Ermittlung (AMCRE)**

  Default-Wert: Wahr

  Diese Einstellungen sollte nur im Rahmen eines Support-Falls nach Aufforderung des Herstellers geändert werden.

Die weitere Bedienung ist der Security Guidance Fachmodul ePA beschrieben (siehe Anhang 12.12).

### 6.7.3 Hinweise zum Fachmodul NFDM

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

Die Bedienung ist der Security Guidance Fachmodul NFDM beschrieben (siehe Anhang 12.10).

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

### 6.7.4 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 12.11).

### 6.7.5 Bereich „Lizenz“ *

In diesem Bereich wird der Status der lizenzierbaren Funktionalitäten angezeigt (siehe Kapitel 8.8.2.1).

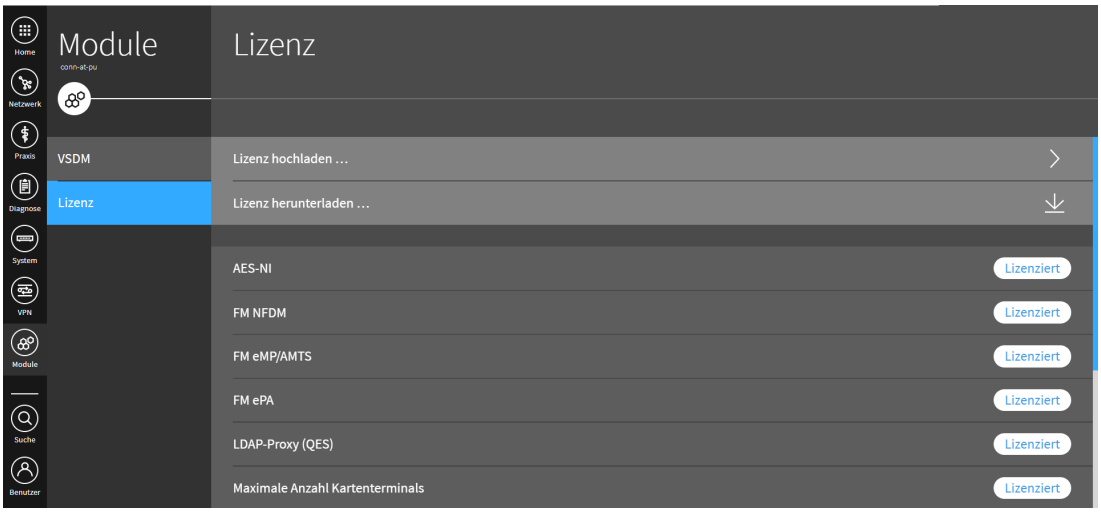



Abbildung 30: Bereich „Lizenz“

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

# 7 Den Highspeedkonnektor für die Einsatzumgebung konfigurieren

## 7.1 Kartenterminals anbinden und benutzen

**Es dürfen nur zugelassene, zertifizierte Kartenterminals verwendet werden.**

### 7.1.1 Kartenterminal verbinden (Pairing)

Beim Pairing wird ein Kartenterminal dem Highspeedkonnektor 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 vorliegt. Aktualisieren Sie diese ggf. vorher (siehe Kapitel 8.3).

- 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**.

  In Abhängigkeit von der individuellen Anbindung einer Leistungserbringerumgebung an den Highspeedkonektor können neue Kartenterminal automatisch erkannt werden. Bei der automatischen Erkennung wird ein neu angeschlossenes Kartenterminal anschließend mit dem Status *Bekannt* angezeigt.

  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 Highspeedkonnektor Updates für das Kartenterminal durchführen zu können (siehe Kapitel 9).

  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 Highspeedkonnektors angezeigt und in der Bedienoberfläche des Highspeedkonnektors wird das Kartenterminal nun mit dem Status *Aktiv* angezeigt.

### 7.1.2 Kartenterminal zuordnen

Nach dem Pairing sind folgende Zuordnungen des Kartenterminals erforderlich:

- Einem Arbeitsplatz (siehe Kapitel 6.3.3.1)
- Mindestens einem Mandanten (siehe Kapitel 6.3.5)

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 Kartenterminal. Ein entferntes Kartenterminal befindet sich an einem beliebigen Ort im lokalen Netzwerk, die zugehörige PIN wird vom Arbeitsplatz aus über ein lokales Kartenterminal eingegeben.

- 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.

### 7.1.3 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.

### 7.1.4 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.

### 7.1.5 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 Highspeedkonnektor im Menü **Praxis** aus der Liste der Kartenterminals (siehe Kapitel 6.3.2).

## 7.2 Updates für Kartenterminals

Der Highspeedkonnektor kann vom KSR (Konfigurations- und Software-Repository) oder über ein Clientsystem Updates (Firmware-Aktualisierungen) für Kartenterminals durchführen (siehe Kapitel 9). Der Highspeedkonnektor überprüft die Signatur aller Updatepakete. Wenn die Signatur nicht korrekt ist, wird das Update nicht eingespielt und die Firmware verbleibt auf dem bisherigen Stand.

# 8 Den Highspeedkonnektor administrieren

## 8.1 Hinweise zur Fehlersuche

- Prüfen Sie die vorliegenden Fehlermeldungen (siehe Kapitel 6.4.1).
- Prüfen Sie, ob die TSL noch gültig ist (siehe Kapitel 6.5.2) und laden Sie diese ggf. manuell hoch (siehe Kapitel 8.3).
- Wenn der Highspeedkonnektor hinter einer Firewall betrieben wird, prüfen Sie, ob die Anforderungen an die freigegebenen Ports/Protokolle erfüllt sind (siehe Kapitel 4.2)

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

## 8.2 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.

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 erreichbar ist und korrekt funktioniert, werden Datum und Zeit der erfolgreichen Prüfung angezeigt. Im Fehlerfall wird eine Fehlermeldung angezeigt.

## 8.3 TSL hochladen

Aufgrund der begrenzten zeitlichen Gültigkeit der TSL sowie den durch Produktion und Transport gegebenen Zeiträumen kann es dazu kommen, dass die in der Produktion eingebrachte TSL nicht mehr gültig ist.

Bei Bedarf können Sie eine aktuelle TSL hochladen.

- Im Menü **System** können Sie im Bereich **Zertifikate** das jeweilige Ablaufdatum anzeigen lassen sowie eine TSL hochladen.

- Deaktivieren Sie dazu vorübergehend den Leistungsumfang Online (siehe Kapitel 6.2.1).

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

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

### 8.3.1 Import aktueller TSL nach Wechsel des TSL-Vertrauensankers

Wenn der Highspeedkonnektor über einen längeren Zeitraum offline war, 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 6.5.2). Spielen Sie dabei die TSL in zeitlichen aufsteigender Abfolge ein, beginnend mit der ältesten TSL.

Weiterführende Supportinformationen werden im Bedarfsfall über die Wissensdatenbank bereitgestellt.

## 8.4 TLS-Zertifikate für Clientsysteme verwalten

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

### 8.4.1 TLS-Zertifikat generieren und im Browser importieren

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

- Öffnen Sie im Menü **Praxis** den Bereich **Clientsysteme**.
- Falls nicht bereits erfolgt, erstellen Sie das Clientsystem (siehe Kapitel 6.3.3).
- 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 dem 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 4.4.1 beschrieben.

### 8.4.2 TLS-Zertifikat in den Highspeedkonnektor importieren

**Diese Funktion darf nur dazu verwendet werden, um nach einem vollständigen Werksreset ein zuvor vom Highspeedkonnektor 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.

## 8.5 Selbst-Test durchführen

Im Menü **Diagnose** können Sie im Bereich **Status** mit **Selbst-Test ...** eine Prüfung der Integrität sicherheitsrelevanter Komponenten anstoßen (siehe Kapitel 2.3.9).

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

## 8.6 Laufzeit der Konnektor-Zertifikate verlängern

Die bereitgestellten Zertifikate besitzen eine befristete Laufzeit. Um eine unterbrechungsfreie Nutzung der TI zu gewährleisten, müssen die Zertifikate rechtzeitig vor Ablauf der Zertifikatslaufzeit erneuert werden.

Wenden Sie sich dazu an den Betreiber.

## 8.7 Werksreset durchführen

Mit den verschiedenen Arten von Werksreset können bestimmte oder alle Parameter der Instanz des Highspeedkonnektors in den Auslieferungszustand zurückversetzt werden.

| | Konfigurationsdaten | Netzwerkeinstellungen | Benutzerkonten |
|---|---|---|---|
| Vollständiger Werksreset (siehe Kapitel 8.7.1) | x | x | x |
| Werksreset der Instanz durch den Betreiber (siehe Kapitel 8.7.2) | - | - | x |

Tabelle 5: Werksreset – Übersicht

### 8.7.1 Vollständiger Werksreset

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 die Konnektor-Instanzim Auslieferungszustand, die Anmeldung erfolgt analog der Erstanmeldung (siehe Kapitel 4.4). Beachten Sie bei Client-Authentisierung per Zertifikat die Hinweise zur Client-Authentisierung nach einem Werksreset (siehe Kapitel 6.3.3).

**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.**

Der vollständige Werksreset wird über das Menü ⊜ **System** im Bereich **Allgemein** durchgeführt (siehe Kapitel 6.5.1).

Danach wird die Instanz des Highspeedkonnektors heruntergefahren.

### 8.7.2 Werksreset der Instanz durch den Betreiber

Falls Sie sich nicht mehr an der Bedienoberfläche anmelden können, wenden sie sich an den Betreiber. Dieser kann die Instanz auf den Ausgangszustand zurücksetzen.

## 8.8 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.

### 8.8.1 Backup erstellen

Gehen Sie wie folgt vor:

- Klicken Sie **Backup erstellen ...**
- Wählen Sie den Umfang der Sicherung aus:
  - **Gesamtexport**

    Alle Einstellungen des Highspeedkonnektors sowie alle angelegten Objekte und Benutzerkonten werden exportiert. 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 Highspeedkonnektors.

- **Anwendungskonnektor.**

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

- **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`)

Außerdem darf das Passwort den Benutzernamen weder vorwärts noch rückwärts, noch in Groß- oder Kleinschreibung beinhalten.

**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.

### 8.8.2 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 Highspeedkonnektors durchzuführen.**

**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 6).**

#### 8.8.2.1 Wartungspairing

Um zu verhindern, dass bei Ausfall eines Konnektors alle Kartenterminals eingesammelt und erneut dem initialen Pairing-Prozess unterzogen werden müssen, kann eine Sicherungskopie der Pairing-Geheimnisse in den neuen Konnektor eingespielt und mit deren Hilfe automatisiert ein neuerliches Pairing mit derselben Pairing-Information durchgeführt werden. Im Gegensatz zum initialen Pairing muss der Administrator beim Wartungspairing nicht sicherstellen, dass sich alle Kartenterminals in seiner organisatorischen Hoheit befinden.

Das Bekanntmachen eines neuen Konnektors unter Verwendung bereits bestehender Pairing-Information läuft in zwei Phasen ab:

- Nach dem TLS-Verbindungsaufbau ruft der Konnektor in der ersten Phase vom Kartenterminal eine Challenge (eine vom Kartenterminal generierte Zufallszahl) ab.
- Der Konnektor bildet aus der Challenge und dem Shared Secret den SHA256-Hash-Wert. Diesen Hash-Wert sendet der Konnektor in der zweiten Phase als Response auf die Challenge.

  Das Kartenterminal bildet für jeden genutzten Pairing-Block ebenfalls den Hash-Wert aus Challenge und jeweiligem Shared Secret und vergleicht alle generierten Hash-Werte mit der Response des Konnektors.

Falls das Kartenterminal die Response erfolgreich validieren und eindeutig einem Pairing-Block zuordnen kann, trägt das Kartenterminal den öffentlichen Schlüssel in den korrespondierenden Pairing-Block ein.

Mögliche Fehlerzustände und Lösungen:

- Wartungspairing kann nicht durchgeführt werden, weil das KT nicht an/im Netzwerk verfügbar ist.

  Schalten Sie ggf. das Kartenterminal an.
- Unerwartete Fehler

  Entfernen Sie das Pairing des Terminals und führen Sie das Pairing erneut durch.

## 8.9 Lizenzen verwalten

Eine Lizenzierung erfolgt individuell für einen Highspeedkonnektor, identifiziert anhand seiner Seriennummer, und gilt für alle Instanzen mit identischem Unfang. Der Umfang der zu lizenzierenden Funktionen wird vom Hersteller je Release definiert.

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

### 8.9.1 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

- ENCSERVICE

  Ver- und Entschlüsselung

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

- Fachmodule

  Die Lizenzierung der nachfolgend aufgeführten Fachmodule erfolgt zusammenhängend; eine separate Lizenzierung ist nicht möglich. Standardmäßig werden alle Fachmodule für alle Konnektor-Instanzen eines Highspeedkonnektors lizenziert.

  - AMTS: Fachmodul eMP/AMTS
  - NFDM: Fachmodul NFDM (inkl. Signaturrichtlinie NFDM)
  - ePA2: Fachmodul ePA2 - Funktionalitäten gemäß ePA Stufe 2.0

### 8.9.2 Lizenzfreie Verwendung

Zur lizenzfreien Verwendung sind die folgenden Funktionen verfügbar:

- QES/nonQES
- LDAP
- Ver-/Entschlüsselung
- Die Anzahl der Betriebsstätten (BSNR bzw. SMC-B) und Kartenterminals ist nicht begrenzt.
- Komfortsignatur

# 9 Updates für Kartenterminals durchführen

Der Highspeedkonnektor nutzt den KSR, um Updates (Systemaktualisierungen) für Kartenterminals zu laden und auf angeschlossenen Kartenterminals zu installieren. Die Software des Highspeedkonnektors selbst wird nicht über den KSR aktualisiert, sondern offline durch den Betreiber.

Es besteht die Möglichkeit, sich per Event (CETP-Protokoll) über die Verfügbarkeit von Aktualisierungen 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 Highspeedkonnektor bereits vorliegenden.

**Beachten Sie die Sicherheitshinweise zur sicheren Administrierung in Kapitel 3.4. Führen Sie ein Update nur dann durch, wenn Sie ausreichend Informationen über dessen Inhalt haben. Prüfen Sie den Status der Zulassung und Zertifizierungsinformationen. Informationen über zugelassene oder für den Betrieb in der TI genehmigte Softwareversionen erhalten Sie von der gematik unter `www.gematik.de`.**

**Sobald dem Administrator bekannt wird, dass ein kryptografischer Algorithmus für die Verarbeitung von qualifizierten elektronischen Signaturen (siehe Kapitel 2.3.7) nicht mehr geeignet ist, muss er die Anwender umgehend darüber informieren und den Betreiber kontaktieren, um ein Update durchführen, sobald dieses verfügbar ist.**

**Nach der Durchführung eines Updates muss der Administrator prüfen, ob die Installation der von ihm ausgewählten Version erfolgreich war. Insbesondere bei auftretenden Fehlern oder Stromausfällen während der Installation muss die Firmware-Version geprüft werden.**

### 9.1.1 Übersicht

Der Konfigurationsdienst (KSR) der Telematikinfrastruktur (TI) stellt für Kartenterminals eine Schnittstelle für Softwareupdatepakete zur Verfügung.

### 9.1.2 Automatische Updates durchführen

Die Spezifikationen der gematik fordern, dass diese Funktion standardmäßig aktiviert ist. Die automatische Durchführung von Updates können Sie bei einem Highspeedkonnektor nur im Eigenbetrieb manuell wieder deaktivieren. Bei aktiven automatischen Updates werden bereitstehende Updates automatisch heruntergeladen und installiert.

Für einzelne Updates kann die automatische Durchführung vom Hersteller deaktiviert sein. Das Update ist dann nur manuell möglich.

Beachten Sie die Sicherheitshinweise zur sicheren Administrierung in Kapitel 3.4. Vergewissern Sie sich vor der Ausführung eines automatischen Updates, dass Sie ausreichend Informationen über dessen Inhalt haben.

Informationen über zugelassene oder für den Betrieb in der TI genehmigte Softwareversionen erhalten Sie von der gematik unter `www.gematik.de`.

#### 9.1.2.1 Konfigurationswerte

Im Menü **System** können Sie im Bereich **Aktualisierungen** (siehe Kapitel 6.5.4) folgende Einstellungen für automatische Updates konfigurieren:

- **Automatische Prüfung**

  Wenn aktiv, sucht der Highspeedkonnektor automatisch nach verfügbaren Updates.

- **Automatischer Download**

  Wenn aktiv, werden erkannte verfügbare Updates automatisch heruntergeladen.

- **Automatische Installation**

  Wenn aktiv, werden heruntergeladene Updates automatisch installiert.

- **Wochentag** und **Uhrzeit** für die Durchführung des automatischen Updates

  Zu diesem Zeitpunkt muss der organisatorische Schutz der mit dem Highspeedkonnektor gepairten Kartententerminals sichergestellt sein.

Die festgelegte Zeit wird als Koordinierte Weltzeit (UTC) interpretiert und für den Standort Deutschland automatisch umgerechnet. Je nach Winter- oder Sommerzeit ergibt sich dadurch ein Zeitversatz um eine oder zwei Stunden.

Beispiel: Wenn Sie den Zeitpunkt 22:30 Uhr für das Update festlegen, ergibt sich für Deutschland bei Winterzeit der Zeitpunkt 23:30 Uhr desselben Tages, bei Sommerzeit hingegen 00:30 Uhr des Folgetages.

#### 9.1.2.2 Hinweise auf Aktivierung Auto-Update

Über die Aktivierung der Auto-Update Funktionalität werden Sie durch einen Hinweis auf der Benutzeroberfläche des Konnektors informiert. Der Hinweis gibt Auskunft darüber, welche Uhrzeit und welcher Wochentag zur Durchführung des automatischen Softwareupdates vorkonfiguriert sind.

#### 9.1.2.3 Signalisierung und Protokollierung

Es werden Events (siehe Kapitel 12.4.3.3) sowie Protokolleinträge erzeugt. Hierbei werden die folgenden Protokolleinträge erzeugt, bei denen in Teilen nicht zwischen der Anwendung eines manuellen Updates oder einem Auto-Update unterschieden wird:

- Verfügbarkeit Auto-Update: Warning-Eintrag ins Systemprotokoll
- Start Auto-Update: Info-Eintrag ins Systemprotokoll
- Erfolgreicher Abschluss Auto-Update: Info-Eintrag ins Sicherheitsprotokoll
- Fehlerfälle: Error-Eintrag ins Sicherheitsprotokoll
  - Fehlschlag eines KT-Updates

#### 9.1.2.4 Durchführung eines automatischen Updates

Nach der erstmaligen Aktivierung des Auto-Updates werden zukünftige Firmwareversionen automatisch zu den konfigurierten Zeitpunkten eingespielt.

### 9.1.3 Automatische Updates deaktivieren

Die automatische Durchführung von Updates können Sie bei einem Highspeedkonnektor im Eigenbetrieb auf Wunsch unterdrücken. Im TI-Gateway Modus sind automatische Updates nicht deaktivierbar.

Deaktivieren Sie dazu im Menü **System** im Bereich **Aktualisierungen** unter **Einstellungen ...** folgende Funktion:

- **Automatische Installation**

  Nachdem Sie die Deaktivierung mit ✓ bestätigt haben, werden heruntergeladene Updates nicht mehr automatisch installiert.


Abbildung 31: Automatische Updates deaktivieren

Optional können Sie zusätzlich folgende Funktion deaktivieren:

- **Automatischer Download**

  Wenn deaktiviert, werden Updates nicht mehr automatisch heruntergeladen.

### 9.1.4 Update von Kartenterminals 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.

#### 9.1.4.1 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 Highspeedkonnektor 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 Highspeedkonnektor Updates für das Kartenterminal durchführen zu können (siehe Kapitel 6.3.2).

#### 9.1.4.2 Aktuelle Firmware-Version prüfen

Sie haben folgende Möglichkeiten, um die Firmware-Version zu prüfen:

- Firmware-Version in der Bedienoberfläche des Highspeedkonnektors 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.
- Firmware-Version im PVS prüfen

  Die genutzte Firmware-Version wird auch im Primärsystem angezeigt.

  Lassen Sie sich die installierte Version über das Primärsystem anzeigen; beachten Sie dazu die Hinweise des Primärsystem-Herstellers.

### 9.1.4.3 Update durchführen

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

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

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

#### 9.1.4.4 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.

# 10 Remote Management

Das Remote Management des Highspeedkonnektors erfolgt über die LAN-Schnittstelle. Die Nutzung des Remote-Managements muss über die Management-Oberfläche des Highspeedkonnektors aktiviert werden (siehe Kapitel 6.5.1).

- Legen Sie einen Benutzer mit der Rolle *Remote-Admin* an (siehe Kapitel 6.1).

  Der Administrator des Konnektors muss das initiale Passwort dem Remote-Administrator auf sicherem Wege mitteilen. Beachten Sie dazu die Warnhinweise in Kapitel 6.1.2.

- Validieren Sie das TLS-Zertifikat des Highspeedkonnektors und Importieren Sie das Zertifikat in den Browser. Führen Sie dazu die in Kapitel 4.4.1 beschriebenen Schritte durch.

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

  ```
  https://<IP-Adresse der Konnektor-Instanz >:8501/management
  ```

- Nach erfolgreicher Verbindung zum Highspeedkonnektor erscheint der Anmeldedialog und fordert den Remote-Administrator zur Eingabe von Benutzernamen und Passwort auf. Bei der Erstanmeldung des Remote-Administrators muss das erstellte initiale Passwort verwendet werden. Anschließend wird der Remote-Administrator aufgefordert, ein neues Passwort zu erstellen. Beachten Sie dabei die Hinweise zu Passwörtern im Kapitel 3.1.

- Beachten Sie die eingeschränkten Rechte des Remote-Administrators (siehe Kapitel 6.1.3)

**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.**

# 11 Meldung von möglichen Schwachstellen

Sie können mögliche Schwachstellen des Highspeedkonnektors über den Betreiber an den Hersteller melden. Eine mögliche Schwachstelle liegt beispielsweise vor, wenn sich der Highspeedkonnektor anders verhält, als im Handbuch beschrieben.

Beschreiben Sie dem Betreiber das Verhalten des Highspeedkonnektors, welches eine mögliche Schwachstelle anzeigt. Der Betreiber leitet diese Meldung zwecks Klärung an den Hersteller weiter.

# 12 Anhang

## 12.1 Unterstützte Netzwerkprotokolle

### 12.1.1 TCP/IP

Der Highspeedkonnektor unterstützt TCP-/IPv4-Pakete gemäß RFC 793 /RFC 791 (siehe Kapitel 4.2.3 für eine Übersicht der verwendeten IP-Protokolle).

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

### 12.1.2 TLS

Der Highspeedkonnektor 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 Highspeedkonnektor 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

  Für die unterstützen Werte siehe Kapitel 12.2, Tabelle 6: Bei TLS unterstützte Cipher suites.
- 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 Highspeedkonnektor ein eigenes Zertifikat für die Authentisierung.

Für die Nachricht CertificateRequest (RFC 5246 Abschnitt 7.4.4) sendet der Highspeedkonnektor folgende Parameter:

- certificate_types
- supported_signature_algorithms
- certificate_authorities

### TLS-Handshake

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

### 12.1.3 NTP

#### NTP-Server

Der Highspeedkonnektor nutzt NTP für die Bereitstellung von Zeitinformationen für die angeschlossenen Clientsysteme.

Der Highspeedkonnektor 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 Highspeedkonnektors arbeitet im Modus secondary server gemäß RFC 5905 Abschnitt 2. Fehlermeldungen werden gemäß RFC 5905 Abschnitt 9.2 generiert.

#### NTP-Client

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

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

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

### 12.1.4 DHCP-Client

Der Highspeedkonnektor 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 Highspeedkonnektor wertet folgende Parameter aus:

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

Weitere Parameter werden nicht berücksichtigt.

### 12.1.5 DNS

Der Highspeedkonnektor bietet einen Domain Name Server (DNS) zur Auflösung von DNS-Anfragen von Clientsystemen im lokalen Netzwerk und unterstützt DNS-Abfragen gemäß RFC 1035.

### 12.1.6 Aktualisierung der TSL

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

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

#### 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 6.5.2).

## 12.2 Unterstützte Algorithmen

| Algorithmen | Instanz MGMT | Instanz SOAP | LDAP | Instanz Client |
|---|---|---|---|---|
| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 | x | x | x | x |
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 | x | x | x | x |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | x | x | x | x |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | x | x | x | x |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | x | x | x | x |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | x | x | x | x |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA | x | x | x | x |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA | x | x | x | x |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | | | | |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | | | | |

Tabelle 6: Bei TLS unterstützte Cipher suites

| | RSA-2048 | RSA-3072 | SECP-256 | SECP-384 | Brainpool-P256 |
|---|---|---|---|---|---|
| **Instanz MGMT** | | | | | |
| generiert | x | | | | |
| AK.AUT | x | | | | |
| **Instanz SOAP** | | | | | |
| generiert | | x | x | | x |
| Upload | x | x | x | | x |

Tabelle 7: Algorithmen und Schlüssellängen der Außenschnittstellen einer Konnektor-Instanz

## 12.3 Standardwerte bei Auslieferung

Der Highspeedkonnektor unterstützt nicht alle Konfigurationsoptionen des Modularen Konnektors. Bei nicht unterstützten Einstellungen werden manuelle Eingaben vom System ignoriert.

### 12.3.1 Menü „Benutzer“

| Wert | Standardeinstellung | Wertebereich |
|---|---|---|
| Ablaufzeit Passwörter | 120 Tage | - |

### 12.3.2 Menü „Netzwerk“

#### 12.3.2.1 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 | - |

| Wert | Standardeinstellung | Wertebereich |
|---|---|---|
| Intranet Routen | - | - |
| Bandbreitenbeschränkung | 100 Mbit/s | 1-1000 Mbit/s |

### 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

Mit dem Wert für **Permanente Verbindungen** wird die Anzahl der TLS-Verbindungen definiert, die der Konnektor versucht, proaktive in die TI zum VSDM-Intermediär aufzubauen.

Werte größer **1** können dabei zu einer sehr starken Belastung des VSDM-Intermediär führen.

Der standardmäßig eingestellte Wert **0** deaktiviert diese Funktionalität und TLS-Verbindungen zum Intermediär werden ausschließlich anlassbezogen aufgebaut.

Beim Wert **0** kann sich die Laufzeit bzgl. nicht direkt aufeinanderfolgender Abfragen der Versichertenstammdaten (ReadVSD) minimal verlängern, da einer Anfrage nun immer ein TLS-Verbindungsaufbau vorausgeht.

Standardmäßig verwendet der Highspeedkonnektor ECC-Algorithmen für alle TLS-Verbindungen (Verbindungen zu Kartenterminals, zu den Fachdiensten, zum Registrationsserver und zum KSR-Dienst), mit Ausnahme der Verbindung zum Primärsystem bzw. Clientsystem.

Wenn auch die Verbindung zum Primärsystem mit ECC-Algorithmen abgesichert werden soll, dann muss vorher geprüft werden, ob das Primärsystem ECC-Algorithmen unterstützt. Wenn dies der Fall ist, kann die Authentisierung gegenüber dem Clientsystem mittels ECC-Zertifikat in den erweiterten TLS-Einstellungen aktiviert werden.

- Klicken Sie dazu im Menü **Netzwerk** im Bereich **Allgemein** auf **Erweiterte TLS-Einstellungen ...**
- Aktivieren Sie die Option **ECC-Zertifikat zur Authentisierung gegenüber dem Clientsystemen nutzen**.

  Wenn die Nutzung des ECC-Zertifikats aktiviert ist, wird dieses auch für die Authentisierung an der CETP-Schnittstelle verwendet.

Diese Funktion ist nur dann nutzbar, wenn auch ein ECC-Zertifikat zur Authentisierung gegenüber Clientsystemen im Konnektor existiert oder zu einem früheren Zeitpunt existiert hat und die Verwendung des ECC-Zertifikats noch aktiviert ist. (Standard: deaktiviert").

Über **Maximale Verbindungen** kann definiert werden, wie viele Verbindungen der Konnektor im Lastfall aufbaut und für die angegebene Lebensdauer offen behält.

Beispiel:

Kommen zwei ReadVSD Anfragen zeitgleich rein, so muss der Konnektor zwei Verbindungen zum VSDM-Intermediär aufbauen, da die Anfragen über getrennte TLS-Verbindungen übermittelt werden müssen. Beide Verbindungen werden nach der Nutzung für die eingestellte Lebensdauer beibehalten, sofern der Wert für **Maximale Verbindungen** nicht überschritten wurde.

Werden Verbindungen nach Ablauf der Lebensdauer abgebaut, wird geprüft, ob die in **Permanente Verbindungen** definiert Anzahl unterschritten wurde, worauf eine entsprechende Anzahl von Verbindungen wieder aufgebaut wird.

| Wert | Standardeinstellung | Wertebereich |
|---|---|---|
| Permanente Verbindungen | 0 | 0 - 100 |
| Maximale Verbindungen | 1 | 0 - 100 |
| Lebensdauer Verbindungen | 5 Minuten | Mind. 1 Millisekunde |
| Aufräum-Intervall | 5 Minuten | Mind. 1 Millisekunde |

| Wert | Standardeinstellung | Wertebereich |
|---|---|---|
| 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 |
| ECC-Ciphersuiten verwenden | An | An/Aus |
| ECC-Zertifikat zur Authentifizierung gegenüber Clientsystemen nutzen | Aus | An/Aus |

**Erreichbarkeit testen**

| Wert | Standardeinstellung | Wertebereich |
|---|---|---|
| Test-Quelle | Netzkonnektor | - |
| IP-Adresse/FQDN | - | - |
| Port | - | - |
| Anzahl zusätzlicher Versuche | 0 | - |
| Timeout | 2000 Millisekunden | - |

#### 12.3.2.2 Bereich „LAN“

| Wert | Standardeinstellung | Wertebereich |
|---|---|---|
| DHCP-Client benutzen | An | An/Aus |
| LAN-Netzwerk | - | - |

| Wert | Standardeinstellung | Wertebereich |
|---|---|---|
| LAN-seitige IP-Paketlänge (MTU) | 1400 | - |
| Weitere Parameter | - | - |

#### 12.3.2.3 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 |

#### 12.3.2.4 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 | - |

#### 12.3.2.5 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> | - |

### 12.3.3 Menü „Praxis“

#### 12.3.3.1 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<br>(0 = Keine Warnung) |
| Timeout für Kartenreservierung | 5 Sekunden | 500 Millisekunden - 10 Sekunden |

#### 12.3.3.2 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<br>(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 |
| Timeout für Update-Kommandos | 60 Sekunden | 10 - 600 Sekunden |

### 12.3.4 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 |

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

### 12.3.5 Menü „System“

#### 12.3.5.1 Bereich „Allgemein“

| Wert | Standardeinstellung | Wertebereich |
|---|---|---|
| Name | conn-at-pu | - |
| Leistungsumfang Signatur-anwendungskomponente | Aus | An/Aus |
| Einfachsignaturmodus | An | An/Aus |
| Remote-Management erlauben | Aus | An/Aus |
| Remote-Management aktivieren | Aus | An/Aus |
| Standalone-Szenario | Aus | An/Aus |
| Komfortsignatur | Aus | An/Aus |
| Komfortsignatur-Zähler | 100 | 1-250 |
| Komfortsignatur-Timer | 6 Stunden | 1-24 Stunden |

#### 12.3.5.2 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<br>(0 = deaktiviert) |

#### 12.3.5.3 Bereich „Zeit“

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

#### 12.3.5.4 Bereich „Aktualisierungen“

| Wert | Standardeinstellung | Wertebereich |
|---|---|---|
| Automatische Prüfung | An | An/Aus |
| Automatischer Download | An | An/Aus |

| Wert | Standardeinstellung | Wertebereich |
|---|---|---|
| Automatische Installation | An | An/Aus |
| Frühester Zeitpunkt für den Beginn der automatischen Aktualisierung | Automatische Vorbelegung nach Seriennummer | Früheste automatische Installation / Späteste automatische Installation |
| Wochentag | Der Tag wird beim Update bestimmt, und ist ein zufälliger Tag von Montag-Freitag. | Montag - Sonntag |
| Uhrzeit | 01:00 | 00:00 - 23:59 |
| Erprobung-Update-Pakete anzeigen | Aus | An/Aus |
| Neue Bestandsnetze automatisch aktivieren | An | An/Aus |

### 12.3.6 Menü „Fachmodule“

#### 12.3.6.1 Bereich „VSDM“

| Wert | Standardeinstellung | Wertebereich |
|---|---|---|
| Intermediär-Servicename | _vsdmintermediaer._tcp | |
| Max. Dauer TI Offline | 0 Tage (keine Prüfung) | -<br>(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) |

## 12.4 Meldungen und Protokolle

Der Highspeedkonnektor erzeugt im Betrieb für jede Instanz Meldungen und protokolliert diese im Protokollspeicher. Sie können über die Bedienoberfläche ausgelesen werden (siehe Kapitel 6.4). 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 5.2).

### 12.4.1 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

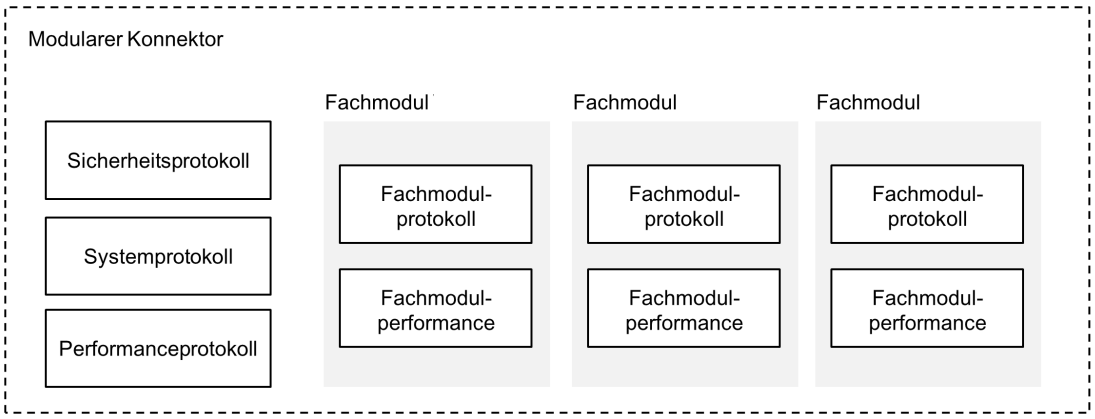



Abbildung 32: Übersicht der Protokolle für eine Instanz

Welche Ereignisse protokolliert werden, können Sie im Menü **Diagnose** im Bereich **Administration** festlegen (siehe Kapitel 6.4.6).

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 Highspeedkonnektors ausgeführt werden.

### 12.4.2 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 „severi-ty“. 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.

### 12.4.3 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

#### 12.4.3.1 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; Vorgangsnummer=9e49ad88-9fd2-4e4f-
8c3e-a4a620480bac

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

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

#### 12.4.3.2 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 12.4.6.

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 ungül-
tig;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.

#### 12.4.3.3 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 Events 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;LastUpd
ateTSL=25.05.2018 08:18:58.749;Bedeutung=das letzte Update der TSL
war nicht erfolgreich.;Vorgangsnummer=
1527232951219_92625886727_662519268
```

#### 12.4.3.4 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 geschrieben 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.

#### 12.4.3.5 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“ lautet bei diesen Einträgen immer „MGM/ADMINCHANGES“. Die Einträge werden ins Systemprotokoll mit der Severity-Stufe „info“ geschrieben. 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“.

### 12.4.3.6 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 6.4.6).

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
```

### 12.4.4 Abruf der Protokolle

In der Bedienoberfläche des Highspeedkonnektors können Administratoren im Menü **Diagnose** im Bereich **Protokolleinträge** die vorhandenen Meldungen abrufen (siehe Kapitel 6.4.1).

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.

### 12.4.5 Löschen von Protokolleinträgen

In der Bedienoberfläche des Highspeedkonnektors können Sie im Menü **Diagnose** im Bereich **Administration** Protokolleinträge löschen (siehe Kapitel 6.4.6). 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 Highspeedkonnektor 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.

### 12.4.6 Übersicht der Meldungen

| | |
|---|---|
| Code | Fehler-ID (dient als Referenz der gematik) |
| Beschreibung | Kurze Zusammenfassung |
| Typ | Art der Meldung; diese bestimmt, in welche Protokolldatei die Meldung geschrieben wird.<br>SECURITY: Sicherheitsprotokoll<br>TECHNICAL, INFRASTRUCTURE, BUSINESS und OTHER: Systemprotokoll bzw. Fachmodulprotokoll |
| Level | Einstufung nach Schwere des Vorfalls (FATAL, ERROR, WARNING, INFO, DEBUG) |
| PVS | Gekennzeichnete Meldungen werden zusätzlich an die Praxisverwaltungssoftware gemeldet. |
| Fehlerbehebung/<br>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 Highspeedkonnektors 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.<br>▶ Wiederholen Sie den Vorgang.<br>Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 101 | Kartenfehler | SECURITY | FATAL | PVS | Eine Karte reagiert nicht oder nicht wie vorgesehen.<br>▶ Stecken Sie die Karte erneut ein und wiederholen Sie den Vorgang.<br><br>Wenn das Problem nur bei einer bestimmten Karte auftritt, ist möglicherweise die Karte defekt.<br>▶ Verweisen Sie den Versicherten mit den entsprechenden Fehlerinformationen an seine Krankenkasse, wenn der Fehler bei einer eGK auftritt.<br><br>▶ Verfahren Sie entsprechend der Vereinbarung zum Inhalt und zur Anwendung der elektronischen Gesundheitskarte (*Anlage 4a BMV-Ä*), wenn eine Karte nicht verwendet werden kann<br><br>Wenn der Fehler häufiger bzw. bei verschiedenen eGKs auftritt, wenden Sie sich an den DVO.<br><br>Fehlerbehebung durch DVO:<br>▶ Wenn der Fehler bei verschiedenen eGKs auftritt, überprüfen Sie anhand der Protokolle des Highspeedkonnektors bzw. des Fachmoduls VSDM, in welchem Kontext der Fehler auftritt bzw. von welcher Krankenkasse und von welchem Fachdienstbetreiber die betroffenen Karten stammen.<br>▶ Stellen Sie für den betroffenen Fachdienstbetreiber ein Ticket ein. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 102 | Gerätefehler | SECURITY | FATAL | PVS | Der Konnektor reagiert nicht oder nicht wie vorgesehen.<br>▶ Wenden Sie sich an den DVO. |
| 103 | Softwarefehler | SECURITY | FATAL | PVS | Der Konnektor reagiert nicht oder nicht wie vorgesehen.<br>▶ Wenden Sie sich an den DVO. |
| 104 | Fachmodul reagiert nicht | SECURITY | FATAL | PVS | Der Konnektor reagiert nicht oder nicht wie vorgesehen.<br>▶ Wenden Sie sich an den DVO. |
| 105 | eGK nicht lesbar | SECURITY | FATAL | PVS | Ein technisches Problem ist beim Auslesen der eGK aufgetreten.<br>▶ Stecken Sie die Karte erneut ein und versuchen Sie sie einzulesen.<br>▶ 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. Verfahren Sie entsprechend der Vereinbarung zum Inhalt und zur Anwendung der elektronischen Gesundheitskarte (*Anlage 4a BMV-Ä*), wenn eine Karte nicht verwendet werden kann.<br>▶ Wenn der Fehler häufiger bzw. bei verschiedenen eGKs auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 106 | Zertifikat auf eGK ungültig | SECURITY | FATAL | PVS | Die eGK ist kein gültiger Leistungsanspruchsnachweis.<br>▶ Fragen Sie den Versicherten, ob er in der Zwischenzeit eine neuere eGK von der Krankenkasse zugeschickt bekommen hat.<br>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.<br>▶ 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.<br>▶ Fragen Sie den Versicherten, ob er in der Zwischenzeit eine neuere eGK von der Krankenkasse zugeschickt bekommen hat.<br>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.<br>▶ Verweisen Sie den Versicherten mit Verweis auf die Meldung (z.B. Zertifikat ungültig) an seine Krankenkasse. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 108 | Protokollierung auf eGK nicht möglich | TECHNICAL | FATAL | PVS | Ein technisches Problem ist beim Schreiben auf die eGK aufgetreten.<br>▶ Stecken Sie die Karte erneut ein und wiederholen Sie den Vorgang.<br>▶ 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. Verfahren Sie entsprechend der Vereinbarung zum Inhalt und zur Anwendung der elektronischen Gesundheitskarte (*Anlage 4a BMV-Ä*), wenn eine Karte nicht verwendet werden kann.<br>▶ 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.<br>▶ Stecken Sie die Karte erneut ein und wiederholen Sie die Freischaltung.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 110 | Fehler beim Verarbeiten von Befehlen auf der eGK | TECHNICAL | FATAL | PVS | Ein technisches Problem ist beim Lesen der eGK aufgetreten.<br>▶ Stecken Sie die Karte erneut ein und wiederholen Sie den Vorgang.<br>▶ 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. Verfahren Sie entsprechend der Vereinbarung zum Inhalt und zur Anwendung der elektronischen Gesundheitskarte (*Anlage 4a BMV-Ä*), wenn eine Karte nicht verwendet werden kann.<br>▶ 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.<br>▶ Stecken Sie die Karte erneut ein und wiederholen Sie den Vorgang.<br>▶ 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. Verfahren Sie entsprechend der Vereinbarung zum Inhalt und zur Anwendung der elektronischen Gesundheitskarte (*Anlage 4a BMV-Ä*), wenn eine Karte nicht verwendet werden kann.<br>▶ Wenn der Fehler häufiger bzw. bei verschiedenen eGKs auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 112 | Fehler beim Schreiben von Daten der eGK | TECHNICAL | FATAL | PVS | Ein technisches Problem ist beim Schreiben auf die eGK aufgetreten.<br>▶ Stecken Sie die Karte erneut ein und wiederholen Sie die Freischaltung.<br>▶ 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. Verfahren Sie entsprechend der Vereinbarung zum Inhalt und zur Anwendung der elektronischen Gesundheitskarte (*Anlage 4a BMV-Ä*), wenn eine Karte nicht verwendet werden kann.<br>▶ 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.<br>▶ Fragen Sie den Versicherten, ob er in der Zwischenzeit eine neuere eGK von der Krankenkasse zugeschickt bekommen hat.<br>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.<br>▶ Verweisen Sie den Versicherten mit Verweis auf die Meldung (veraltete eGK) an seine Krankenkasse. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 114 | Gesundheits-anwendung auf eGK gesperrt | TECHNICAL | FATAL | PVS | Die eGK ist kein gültiger Leistungsanspruchsnachweis.<br>▶ Fragen Sie den Versicherten, ob er in der Zwischenzeit eine neuere eGK von der Krankenkasse zugeschickt bekommen hat.<br>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.<br>▶ Verweisen Sie den Versicherten mit Verweis auf die Meldung (Gesundheitsanwendung gesperrt) an seine Krankenkasse. |
| 115 | Leseversuch von eGK älter als Generation 2 | TECHNICAL | FATAL | PVS | Die Durchführung der Operation ist mit der eGK kleiner der Generation G2 nicht möglich.<br>▶ Fragen Sie den Versicherten, ob er in der Zwischenzeit eine neuere eGK von der Krankenkasse zugeschickt bekommenhat. |
| 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 Leistungsanspruchs-nachweis. VSD können mit Prüfungsnachweis 3 („Aktualisierung VSD auf eGK technisch nicht möglich") eingelesen werden.<br>▶ Wenn der Fehler über einen längeren Zeitraum häufiger auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 1006 | TSL-Downloadad-ressen wieder-holt nicht erreichbar | TECHNICAL | ERROR | PVS | - |
| 1007 | Vergleich der ID und Se-quenceNumber entspricht nicht der Vergleichs-variante 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 | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für 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 | | - |

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

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 1026 | Das Element „ServiceSupply-Point“ 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 durchgeführt werden (2) | TECHNICAL | ERROR | | - |
| 1030 | OCSP-Zertifikat nicht in TSL Informationen enthalten | SECURITY | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 1039 | Warnung, dass Offline-Modus aktiviert ist und keine OCSP-Statusabfrage durchgeführt wurde | SECURITY | WARNING | | - |
| 1040 | Bei der Online-statusprüfung ist ENFORCE_ CERTHASH_ CHECK auf ´true´ gesetzt, die OCSP-Response ent-hält jedoch kei-ne certHash Erweiterung | SECURITY | ERROR | | - |

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

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 1044 | Warnung, dass zum angefragten Zertifikat keine Statusinformationen verfügbar sind. | TECHNICAL | WARNING | | - |
| 1047 | Das Zertifikat wurde vor oder zum Referenzzeitpunkt widerrufen. | SECURITY | WARNING | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 1048 | Es ist ein Fehler bei der Prüfung des QCStatements aufgetreten (z. B. nicht vorhanden, obwohl gefordert). | TECHNICAL | ERROR | | - |
| 1050 | Die einem TUC zur Zertifikatsprüfung beigefügte OCSP-Response zu dem zu prüfenden Zertifikat kann nicht erfolgreich gegen das Zertifikat validiert werden. | TECHNICAL | WARNING | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 1051 | Die in einem OCSP-Response zurückgelieferte Nonce stimmt nicht mit der Nonce des OCSP-Requests überein. | SECURITY | ERROR | | - |
| 1052 | Attribut-Zertifikat kann dem übergebenen Basis-Zertifikat nicht zugeordnet werden. | SECURITY | ERROR | | - |
| 1053 | Die CRL kann nicht heruntergeladen werden. | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 verwendete HBA auf ihre Gültigkeit. |
| 4000 | Syntaxfehler | TECHNICAL | ERROR | PVS | Beim Aufruf einer Operation ist ein Syntaxfehler aufgetreten.<br>▶ Wiederholen Sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4001 | Interner Fehler | TECHNICAL | ERROR | PVS | Ein technisches Problem ist aufgetreten.<br>▶ Wiederholen Sie den Vorgang.<br>▶ 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.<br>▶ Starten Sie den Highspeedkonnektor neu.<br>▶ 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.<br>▶ Wiederholen Sie den Vorgang.<br>▶ 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 Highspeedkonnektor und dem Primärsystem vor. Die Mandanten-ID aus dem Aufrufkontext ist dem Highspeedkonnektor nicht bekannt. Die Konfiguration muss überprüft werden.<br>▶ Wenden Sie sich an den DVO. |

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

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

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4013 | SM-B_Verwaltet ist dem Mandanten nicht zugeordnet | SECURITY | ERROR | PVS | Es liegt eine Inkonsistenz im Informationsmodell zwischen dem Highspeedkonnektor und dem Primärsystem vor. Die SMC-B aus dem Aufrufkontext ist dem Mandanten nicht zugeordnet. Die Konfiguration muss überprüft werden.<br>▶ 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 Highspeedkonnektor und dem Primärsystem vor. Der Arbeitsplatz aus dem Aufrufkontext ist für diesen Mandanten nicht dem Clientsystem zugeordnet. Die Konfiguration muss überprüft werden.<br>▶ 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 Highspeedkonnektor und dem Primärsystem vor. Das Kartenterminal aus dem Aufrufkontext ist vom Arbeitsplatz nicht zugreifbar. Die Konfiguration muss überprüft werden.<br>▶ 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 Highspeedkonnektor und dem Primärsystem vor. Das Kartenterminal aus dem Aufrufkontext ist vom Arbeitsplatz nicht zugreifbar. Die Konfiguration muss überprüft werden.<br>▶ Wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4017 | Die eGK hat bereits eine Kartensitzung, die einem anderen Arbeitsplatz zugeordnet ist. | SECURITY | ERROR | PVS | Fehler beim Zugriff auf eine eGK. Die eGK wird derzeit von einem anderen Arbeitsplatz verwendet.<br>▶ 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.<br>▶ 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.<br>▶ Wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4020 | Kartenterminal ist weder lokal noch entfernt über irgendeinen dem Clientsystem zugeordneten Arbeitsplatz aus zugreifbar | SECURITY | ERROR | PVS | Es liegt eine Inkonsistenz im Informationsmodell zwischen Konnektor und Primärsystem vor. Das Kartenterminal aus dem Aufrufkontext ist von keinem Arbeitsplatz zugreifbar. Die Konfiguration muss überprüft werden.<br>▶ 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.<br>▶ Wenden Sie sich an den DVO. |
| 4022 | XML-Dokument nicht wohlgeformt | SECURITY | ERROR | PVS | Das verwendete Dokument ist nicht wohlgeformt.<br>▶ Wiederholen Sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4023 | XML-Dokument nicht valide in Bezug auf XML-Schema | SECURITY | ERROR | PVS | Das verwendete Dokument ist nicht valide.<br>▶ Wiederholen Sie den Vorgang.<br>▶ 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.<br>▶ Wiederholen Sie den Vorgang.<br>▶ 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.<br>▶ Wiederholen Sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4027 | Die Endpunkt-informationen konnten nicht übernommen werden. | TECHNICAL | ERROR | PVS | Es ist ein technischer Fehler während der Bootup-Phase aufgetreten.<br>▶ Starten Sie den Highspeedkonnektor neu.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |
| 4028 | Fehler beim Versuch eines Verbindungs-aufbaus zum KT | TECHNICAL | ERROR | PVS | Es ist ein technischer Fehler beim Aufbau einer Kartenterminal-Sitzung aufgetreten.<br>▶ 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.<br>▶ 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.<br>▶ Wenden Sie sich an den DVO. |
| 4031 | Interner Fehler | TECHNICAL | ERROR | PVS | Es ist ein technischer Fehler im Kartenterminaldienst aufgetreten.<br>▶ Wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4032 | Verbindung zu HSM konnte nicht aufgebaut werden | TECHNICAL | ERROR | PVS | Es ist ein technischer Fehler beim Aufbau einer Kartenterminal-Sitzung aufgetreten.<br>▶ Wenden Sie sich an den DVO. |
| 4033 | Kartenterminal antwortet nicht, Zufügen fehlgeschlagen | TECHNICAL | ERROR | PVS | Es ist ein technischer Fehler beim Hinzufügen eines Kartenterminals aufgetreten.<br>▶ Wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4034 | Kartenterminal mit gleichem Hostnamen 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.<br>▶ Wenden Sie sich an den DVO. |
| 4035 | Angegebene IP-Adresse gehört zu einer anderen MAC-Adresse als die, die übergeben wurde. Angaben zur MAC-Adresse prüfen | TECHNICAL | ERROR | PVS | Es ist ein technischer Fehler beim Hinzufügen eines Kartenterminals aufgetreten.<br>▶ Wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4036 | Angegebene IP-Adresse gehört zu einem anderen Hostnamen als der, der übergeben wurde. Angaben zum Hostnamen prüfen | TECHNICAL | ERROR | PVS | Es ist ein technischer Fehler beim Hinzufügen eines Kartenterminals aufgetreten.<br>▶ Wenden Sie sich an den DVO. |
| 4037 | Verwaltung der Kartenterminals inkonsistent | TECHNICAL | ERROR | PVS | Es ist ein technischer Fehler beim Hinzufügen eines Kartenterminals aufgetreten.<br>▶ 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 Highspeedkonnektor ablaufenden Vorgang reserviert.<br>▶ Wiederholen Sie den Vorgang. |
| 4040 | Fehler beim Versuch eines Verbindungsaufbaus zum KT | SECURITY | ERROR | PVS | Es ist ein Fehler beim Pairing eines Kartenterminals aufgetreten.<br>▶ Wenden Sie sich an den DVO. |

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

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4046 | Kartenapplikation existiert nicht | TECHNICAL | ERROR | PVS | Fehler beim Aufruf einer Kartenapplikation der verwendeten Karte.<br>▶ Stecken Sie die Karte erneut ein und wiederholen Sie den Vorgang.<br>Falls das Problem nur bei einer bestimmten Karte auftritt, ist die Karte ggf. defekt oder falsch personalisiert.<br>▶ Tritt der Fehler bei einer eGK auf, verweisen Sie den Versicherten mit den entsprechenden Fehlerinformationen an seine Krankenkasse. Verfahren Sie entsprechend der Vereinbarung zum Inhalt und zur Anwendung der elektronischen Gesundheitskarte (*Anlage 4a BMV-Ä*), wenn eine Karte nicht verwendet werden kann.<br>▶ 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.<br>▶ Stecken Sie die Karte erneut ein und wiederholen Sie den Vorgang.<br>▶ Wenn der Fehler erneut auftritt, wenden Sie sich an den DVO. |
| 4048 | Fehler bei der C2C-Authentisierung | TECHNICAL | ERROR | PVS | Es ist ein Fehler bei C2C-Prüfung aufgetreten. Es sollte überprüft werden, ob die eGK und die SMC-B bzw. der HBA korrekt gesteckt sind.<br>▶ Stecken Sie die Karte erneut ein und wiederholen Sie den Vorgang.<br>▶ Wenn der Fehler erneut auftritt, wenden Sie sich an den DVO. |

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

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4055 | Fehler beim Secure Messaging, Quellkarte | SECURITY | ERROR | | - |
| 4056 | Fehler bei der C2C-Authentisierung, Quellkarte | TECHNICAL | ERROR | | Die Onlineabfrage einer eGK lässt sich nicht erfolgreich durchführen.<br>Die verwendete SMC-B ist anscheinend nicht freigeschaltet.<br>▶ Überprüfen Sie darum den Status der SMC-B unter Praxis > Karten > SMC-B X > PIN-Status abfragen ...<br>Hier sollte für den Mandanten der Status „Verifiziert“ angezeigt werden. Ist dies nicht der Fall, schalten Sie die SMC-B frei. |
| 4057 | Fehler bei der C2C-Authentisierung, Zielkarte | TECHNICAL | ERROR | | - |
| 4058 | Aufruf nicht zulässig | SECURITY | ERROR | | - |
| 4060 | Ressource belegt | TECHNICAL | ERROR | | - |

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

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4067 | Neue PIN nicht identisch | SECURITY | ERROR | | - |
| 4068 | Neue PIN zu kurz/lang | SECURITY | ERROR | | - |
| 4069 | Korruptes Chiffrat bei asymmetrischer Entschlüsselung | TECHNICAL | ERROR | | - |
| 4070 | Autorisierende Karte oder Kartensitzung fehlt | TECHNICAL | ERROR | | - |
| 4071 | Keine Karte für C2C Auth gesetzt | TECHNICAL | ERROR | | - |
| 4072 | Ungültige PIN-Referenz | TECHNICAL | ERROR | | - |
| 4073 | Adressiertes Passwort konnte nicht gefunden werden | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4074 | Formatfehler der übergebenen PIN | TECHNICAL | ERROR | | - |
| 4075 | Formatfehler der übergebenen neuen PIN | TECHNICAL | ERROR | | - |
| 4076 | Formatfehler im übergebenen PUK | TECHNICAL | ERROR | | - |
| 4077 | Setzen der neuen PIN nicht zulässig | SECURITY | ERROR | | - |
| 4078 | PIN-Eingabe über das Clientsystem ist nicht zugelassen | SECURITY | ERROR | | - |
| 4079 | Schlüsseldaten fehlen | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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.<br>▶ Stecken Sie die Karte erneut ein und wiederholen Sie den Vorgang.<br>▶ Wenn der Fehler erneut auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4104 | XML-Element nicht eindeutig identifiziert (Überschneidung) | TECHNICAL | ERROR | | - |
| 4105 | Hybride Verschlüsselung konnte nicht durchgeführt werden | TECHNICAL | ERROR | | - |
| 4106 | Falscher Schlüssel | TECHNICAL | ERROR | | - |
| 4107 | Hybride Entschlüsselung konnte nicht durchgeführt werden | TECHNICAL | ERROR | | - |
| 4108 | Symmetrische Verschlüsselung konnte nicht durchgeführt werden | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4109 | Symmetrische Entschlüsselung konnte nicht durchgeführt werden | TECHNICAL | ERROR | | - |
| 4110 | Ungültiges Dokumentformat | TECHNICAL | ERROR | PVS | Der Aufruf der Operation ist nicht gültig in Bezug auf das verwendete Dokument.<br>▶ Wiederholen Sie den Vorgang.<br>▶ 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.<br>▶ Wiederholen Sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |

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

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4123 | Fehler bei Signaturerstellung | SECURITY | ERROR | | Die Signatur konnte nicht erstellt werde.<br>▶ Wiederholen Sie den Vorgang.<br>▶ 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.<br>▶ Wiederholen Sie den Vorgang.<br>▶ 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.<br>▶ 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 Ablaufdatums schlägt fehl | SECURITY | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4133 | Import der BNetzA-Vertrauensliste fehlgeschlagen | SECURITY | ERROR | | - |
| 4146 | Kartenhandle existiert nicht | TECHNICAL | ERROR | | - |
| 4147 | Zertifikat nicht vorhanden (z. B. kein QES-Zertifikat in SM-B) | TECHNICAL | ERROR | | - |
| 4148 | Fehler beim Extrahieren von Zertifikatsinformationen | TECHNICAL | ERROR | | - |
| 4149 | Ungültige Zertifikatsreferenz | TECHNICAL | ERROR | | - |
| 4150 | Fehler beim Schreiben des Systemprotokolls | TECHNICAL | FATAL | | - |

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

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4156 | Server konnte bei TLS-Verbindungs-aufbau nicht authentisiert werden | SECURITY | ERROR | | - |
| 4157 | Clientauthenti-sierung bei TLS-Verbindungs-aufbau fehlge-schlagen | SECURITY | ERROR | | - |
| 4158 | Adressierte TLS-Verbin-dung nicht vorhanden | TECHNICAL | ERROR | | - |
| 4159 | Public-IP: DNS Server antwor-tet nicht | TECHNICAL | FATAL | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4173 | Die CRL ist nicht mehr gültig (outdated). | TECHNICAL | FATAL | | Im Protokoll des Konnektors wird diese Fehlermeldung angezeigt, sofern ein Problem mit der eingespielten TSL vorliegt. Dieser Fehler ist ein Folgefehler von 46552. |
| 4174 | TI VPN-Tunnel: Verbindung konnte nicht aufgebaut werden | TECHNICAL | FATAL | PVS | Die Verbindung zum VPN-Zugangsdienst konnte nicht aufgebaut werden.<br>▶ Überprüfen Sie den Internetzugang<br>▶ 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4178 | Das Fachmodul konnte die aktuelle Systemzeit des Konnektors nicht abrufen. | TECHNICAL | ERROR | | - |
| 4179 | DNS: Anfrage wurde abgebrochen, da der Timeout von ANLW_SERVICE_TIMEOUT Sekunden überschritten wurde. | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4180 | DNS: Es ist ein Fehler bei der Namensauflösung aufgetreten | TECHNICAL | FATAL | | Die folgenden Variationen sind zu unterscheiden:<br>1. No location for Service [VPN_REGISTRATION] available!<br>Der im Konnektor hinterlegte Registrierungsserver kann nicht erreicht werden.<br>▶ Überprüfen Sie die Schreibweise der DNS-Domain, die im Konnektor eingetragen wurde: Netzwerk > DNS > Einstellungen > DNS-Domain Zugangsdienst<br>2. No location for Service [KSR_FIRMWARE] available!<br>Der vom Konnektor angefragte KSR kann nicht erreicht werden.<br>Hierbei handelt es sich um kein Problem mit dem Konnektor, sondern um ein temporäres Problem in der Infrastruktur.<br>3. No location for Service [OCSP] available!<br>Der vom Konnektor angefragte OCSP kann nicht erreicht werden.<br>Hierbei handelt es sich um kein Problem mit dem Konnektor, sondern um ein temporäres Problem in der Infrastruktur.<br>4. Fehler bei der Namensauflösung von '_regserver._tcp.[URL des Registrierungsservers]'<br>Der im Konnektor hinterlegte Registrierungsserver kann nicht erreicht werden.<br>▶ Sofern dieser Fehler auch nach Lösung der im Fehler 43027 beschriebenen möglichen Ursachen weiterhin auftritt, sollte der Status der Freischaltung der verwendeten SMC-B beim Herausgeber überprüft werden. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 Firmware-Gruppe | SECURITY | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4186 | Download aller Update Files nicht 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 Be-ziehen der Up-datelisten | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 Übernehmen der Bestandsnetze ist ein Fehler aufgetreten | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 eingesteckt. | TECHNICAL | ERROR | | - |
| 4203 | Karte deaktiviert, aber nicht entnommen. | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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-Performanceprotokolls | TECHNICAL | FATAL | | - |
| 4218 | Zugriff auf Konnektor-Performanceprotokoll nicht möglich | TECHNICAL | FATAL | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 vorhan-den | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4252 | Jobnummer wurde in den letzten 1.000 Aufrufen bereits verwendet und ist nicht zulässig | TECHNICAL | ERROR | | - |
| 4253 | Keine Signatur im Aufruf | TECHNICAL | ERROR | | - |
| 4254 | Keine Display-größe für das Kartenterminal definiert | SECURITY | ERROR | | - |
| 4255 | Fehler beim Import des TSL-Signer-CA CrossZertifikats | TECHNICAL | ERROR | | - |
| 4259 | Verschlüsselung für Zertifikat <x> nicht mög-lich | TECHNICAL | WARNING | PVS | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4261 | Das Einbetten von OCSP-Responses wird für Signaturen nicht Unterstütz. | TECHNICAL | WARNING | PVS | - |
| 4262 | Signatur umfasst nicht das gesamte Dokument | TECHNICAL | ERROR | PVS | Die Dokumentensignatur entspricht nicht den Vorgaben.<br>▶ Wiederholen Sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |
| 4263 | Komfortsignaturfunktion nicht aktiviert | TECHNICAL | ERROR | PVS | Um die Komfortsignaturfunktion nutzen zu können, muss diese erst in den Einstellungen des Konnektors aktiviert werden. Wenden Sie sich an den DVO. |
| 4264 | Ein oder mehrere Zertifikate ignoriert | TECHNICAL | WARNING | PVS | - |
| 4265 | Karten-Handle ungültig | TECHNICAL | WARNING | PVS | Der Aufruf der Operation ist nicht gültig.<br>▶ Wiederholen Sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4266 | Keine Kartensitzung vorhanden | TECHNICAL | WARNING | PVS | Der Aufruf der Operation ist nicht gültig.<br>▶ Wiederholen Sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |
| 4267 | Fehler beim Aktivieren des Komfortsignaturmodus | TECHNICAL | ERROR | PVS | Die Komfortsignatur konnte nicht aktiviert werde.<br>▶ Wiederholen Sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |
| 4268 | Fehler beim Deaktivieren des Komfortsignaturmodus | TECHNICAL | ERROR | PVS | Die Komfortsignatur konnte nicht deaktiviert werde.<br>▶ Wiederholen Sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |
| 4269 | Fehler beim Ermitteln des Signaturmodus | TECHNICAL | ERROR | PVS | Die Komfortmoduf konnte nicht ermittelt werde.<br>▶ Wiederholen Sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4270 | UserId wurde in den letzten 1.000 Vorgängen bereits verwendet | TECHNICAL | ERROR | PVS | Der Aufruf der Operation ist nicht gültig in Bezug auf die übergebene UserId.<br>▶ Wiederholen Sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |
| 4271 | Komfortsignaturmodus abgebrochen | TECHNICAL | ERROR | PVS | Die Komforsignatur-Sitzung ist nicht mehr aktiv. Aktivieren sie die Komforsignatur für die Karte erneut. |
| 4272 | UserId nicht zulässig | TECHNICAL | ERROR | PVS | Der Aufruf der Operation ist nicht gültig in Bezug auf die übergebene UserId.<br>▶ Wiederholen Sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO.” |
| 4273 | Attribute im Parameter dss:Properties wurden ignoriert | TECHNICAL | WARNING | PVS | - |
| 4274 | Komfortsignaturen werden nur für den HBA unterstützt | TECHNICAL | ERROR | PVS | Der Aufruf der Operation ist nicht gültig in Bezug auf verwendete Karte.<br>▶ Verwenden sie eine HBA und wiederholen Sie den Vorgang.” |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 4275 | Security Error PIN jetzt gesperrt (BLOCKED) | TECHNICAL | ERROR | PVS | |
| 4276 | Security Error PIN falsch (REJECTED) | TECHNICAL | ERROR | PVS | |
| 4412 | NonQES XAdES Signatur gefunden | TECHNICAL | ERROR | | - |
| 41000 | Karte/ Kartenterminal antwortet mit einer spezifischen Fehlermeldung, Fehlercode: | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 41016 | Keine SMC-B für den TLS-Verbindungsaufbau gesteckt oder freigeschaltet. | TECHNICAL | ERROR | | - |
| 41017 | C2C-Authentisierung durch den Konnektor abgebrochen. | TECHNICAL | INFO | | - |
| 41018 | Fehler beim Schreiben des PN. | TECHNICAL | ERROR | | - |
| 42000 | Import einer Backup Datei ist fehlgeschlagen. | TECHNICAL | ERROR | | - |
| 42001 | Import einer Backup Datei ist beim Entschlüsseln fehlgeschlagen. | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 42005 | Ein Import kann nicht eingespielt werden, da die Version nicht festgestellt werden kann. | TECHNICAL | ERROR | | - |
| 42010 | Export einer Backup Datei ist fehlgeschlagen. | TECHNICAL | ERROR | | - |
| 42011 | PublicKey für Backup-Erstellung nicht lesbar. | TECHNICAL | ERROR | | - |
| 42012 | Rolle stimmt nicht mit der Vorgabe überein. | TECHNICAL | ERROR | | - |
| 42013 | Interner Fehler bei der OCSP-Prüfung | TECHNICAL | ERROR | | - |

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

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 42018 | Das Zertifikat des Clientsystems für den TLS-Verbindungsaufbau ist nicht gültig. | TECHNICAL | ERROR | | - |
| 42019 | Die OCSP-Response enthält eine certHashErweiterung, diese kann aber nicht verarbeitet werden. | TECHNICAL | WARNING | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 42020 | Der TLS-Dienst konnte mit einer Gegenstelle [x] in der Telematikinfrastruktur keine TLS-Verbindung aufbauen. | TECHNICAL | ERROR | | Hierbei handelt es sich um kein Problem mit dem Konnektor, sondern um ein temporäres Problem der TI-Infrastruktur oder um ein generelles Problem mit der lokalen Netzwerkinfrastruktur.<br>Sofern der bereitgestellte Internetanschluss über ein Internat-Access-Gateway (IAG) mit VoIP-Integration oder komplexer Firewall umgesetzt wird, kann es trotz einer bestehenden VPN-Verbindung zu Problemen bei dem Abgleich der Versichertenstammdaten kommen. Das IAG könnte die aus der TI kommenden Rückantworten an den Konnektor blockieren oder durch eine hohe Fragmentierung der Pakete (im Zusammenhang mit VoIP) die Kommunikation stören.<br>Sollten IAGs mit VoIP-Integration oder komplexen Firewallmechanismen verwendetet werden, gilt es die Einstellungen dieser Geräte überprüfen zu lassen:<br>▶ Die Freigabe der für den Betrieb notwendigen Ports muss gewährleistet sein.<br>▶ Die Fragmentierung der Pakete (MTU-Size) darf den für den Betrieb minimal zulässigen Wert von 576 Byte nicht unterschreiten. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 neuen Vertrauens-Anker. | TECHNICAL | INFO | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 42034 | Über BasicAuth wurde für ein Clientsystem-User das Passwort wiederholt falsch angegeben. Dieser User kann sich erst wieder in <x> ms anmelden. | TECHNICAL | WARNING | | Prüfen sie die Hinterlegten Clientsystem-Daten im verwendeten Primärsystem |
| 42035 | Neuer Vertrauensanker ist kein ECC-Zertifikat | TECHNICAL | WARNING | | Prüfen sie das verwendete Vertrauensanker-Zertifikat |
| 42036 | TSL-Downloadadresse im Internet nicht erreichbar | TECHNICAL | ERROR | | - |
| 42037 | Die Signatur aus dem Internet konnte nicht gelesen werden | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 42038 | Die OCSP-Response aus dem Internet ist veraltet | TECHNICAL | ERROR | | - |
| 42039 | Signatur der Internet-TSL ist ungültig bzw. konnte nicht erfolgreich geprüft werden | TECHNICAL | ERROR | | - |
| 42040 | Signatur der Internet-TSL stimmt nicht mit TSL-Signer-Zertifikat überein | TECHNICAL | ERROR | | - |
| 42100 | VAU-Nachricht konnte nicht erzeugt werden | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 42101 | Der PublicKey aus der VAUServerHello-Nachricht konnte nicht verarbeitet werden | TECHNICAL | ERROR | | - |
| 42102 | Die VAU-Nachricht vom Server enthält ungültige Daten | TECHNICAL | ERROR | | - |
| 42103 | Die VAU-Nachricht vom Server konnte nicht entschlüsselt werden | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 42104 | Das Server-Zertifikat aus der VAUServer-Hello-Nachricht konnte nicht verarbeitet werden | TECHNICAL | ERROR | | - |
| 42105 | Die Signatur der VAUServer-Hello-Nachricht ist ungültig | TECHNICAL | ERROR | | - |
| 42106 | Fehler vom VAU-Server | TECHNICAL | ERROR | | - |
| 42107 | Fehler bei der VAU Schlüssel-ableitung | TECHNICAL | ERROR | | - |
| 42108 | Timeout bei der Kommunikation mit dem VAU-Server | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 42109 | Fehler bei der TCP-Verbindung mit dem VAU-Server | TECHNICAL | ERROR | | - |
| 42110 | Fehler beim TLS-Handshake mit dem VAU-Server | TECHNICAL | ERROR | | - |
| 42111 | Timeout beim TLS-Handshake mit dem VAU-Server | TECHNICAL | ERROR | | - |
| 42200 | Die Signatur ist ungültig. | TECHNICAL | ERROR | | - |
| 42201 | Das SGD-HSM Zertifikat ist ungültig. | TECHNICAL | ERROR | | - |
| 42202 | Der Hashwert für PublicKeyE-cies konnte nicht ermittelt werden. | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 42203 | Die ECIES-Verschlüsselung ist fehlgeschlagen. | TECHNICAL | ERROR | | - |
| 42204 | Die ECIES-Entschlüsselung ist fehlgeschlagen. | TECHNICAL | ERROR | | - |
| 42205 | Die SGD-Nachricht vom Server enthält ungültige Daten. | TECHNICAL | ERROR | | - |
| 42206 | Lokalisierung des Schlüsselgenerierungsdienstes fehlgeschlagen. | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 42207 | TCP-Verbindung zum Schlüssel-generierungs-dienst fehlgeschlagen. | TECHNICAL | ERROR | | - |
| 42208 | Fehler im Schlüsselgene-rierungsdienst - Die Operation konnte nicht durchgeführt werden. | TECHNICAL | ERROR | | - |
| 42209 | Zertifikat auf SMC-B ungül-tig. | TECHNICAL | ERROR | | - |
| 42210 | Keine Berechti-gung für den Schlüsselgene-rierungsdienst vorhanden. | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 42211 | Verbindungs-aufbau zum Schlüsselgene-rierungsdienst fehlgeschlagen. | TECHNICAL | ERROR | | - |
| 42212 | Timeout beim TLS-Handshake mit dem Schlüsselgene-rierungsdienst | TECHNICAL | ERROR | | - |
| 42213 | Timeout bei der Kommunikation mit dem Schlüsselgene-rierungsdienst | TECHNICAL | ERROR | | - |
| 43000 | Fehler bei der Kommunikation mit dem Fach-dienst. | TECHNICAL | ERROR | | - |
| 43001 | Ein Download für das Termi-nalupdate läuft bereits. | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 43012 | Das zu aktualisierende Terminal ist aktuell nicht erreichbar und wird bei Wiedererreichbarkeit aktualisiert. | TECHNICAL | INFO | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 43013 | Fehler bei Registrierung des Konnektors im Registrierungsserver.<br>Fehler: <x> | TECHNICAL | ERROR | | Die folgenden Variationen sind zu unterscheiden:<br>1. Fehler: HTTP transport error: org.bouncycastle.tls.TlsFatalAlert: internal_error(80) ( - )<br>Die SMC-B kann nicht ordnungsgemäß verwendet werden.<br>▶ Ziehen Sie die SMC-B aus dem Kartenterminal und stecken Sie sie dann erneut. Alternativ können Sie das Kartenterminal aus- und anschließend wieder anschalten.<br>2. Fehler: HTTP transport error: java.net.SocketExection: Broken pipe (Write failed) ( - )<br>Das Zertifikat der verwendeten SMC-B ist beim Registrierungsdienst unbekannt. Die SMC-B wurde nach Erhalt nicht oder sehr kurzfristig vor der Registrierung aktiviert.<br>▶ Wenden Sie sich entsprechend an den Hersteller der SMC-B.<br>3. Der Timestamp im Request weicht mehr als 300 Sekunden von der aktuellen Zeit im Registrierungsserver ab<br>Der Konnektor lässt sich nicht beim Registrierungsserver freischalten. Bei der manuellen Einstellung der Zeit wurde durch den Browser (beziehungsweise das Betriebssystem) die Sommerzeit nicht berücksichtigt. Dadurch kommt es zu einer Diskrepanz zwischen der angezeigten und der internen Zeit des Konnektors.<br>▶ Überprüfen Sie die im Konnektor eingestellte Zeit unter: System > Zeit > Konnektorzeit<br>▶ Vergleichen Sie die Angabe mit den Zeitstempeln der aktuellen Protokolleinträge: Diagnose > Protokolleinträge<br>▶ Sofern sich eine Abweichung feststellen lässt, überprüfen Sie ob an dem zur Administration verwendeten Gerät die automatische Synchronisation der Zeit und die automatische Umstellung auf Sommerzeit aktiv ist. Korrigieren Sie dies, sofern eine oder beide dieser Einstellungen nicht aktiv sind. Stellen Sie anschließend erneut manuell die Zeit des Konnektors ein: System > Zeit > Zeit einstellen |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 43014 | Fehler bei Registrierung des Konnektors im Konnektor. | TECHNICAL | ERROR | | Dieser Fehler ist eine Folgefehler von 43027 SERVER_NOT_RESOLVED_REGSERVER – Die URL zum Registrierungsserver konnte nicht aufgelöst werden. |
| 43015 | Fehler bei Deregistrierung des Konnektors im Registrierungsserver. Fehler: <x> | TECHNICAL | ERROR | | - |
| 43016 | Fehler bei Deregistrierung des Konnektors im Konnektor. | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 43017 | Fehler bei Statusabfrage beim Registrierungsserver im Registrierungsserver.<br>Fehler: <x> | TECHNICAL | ERROR | | Die folgenden Variationen sind zu unterscheiden:<br>1. Fehler: HTTP transport error: java.net.SocketExection: Broken pipe (Write failed) ( - )<br>Das Zertifikat der verwendeten SMC-B ist beim Registrierungsdienst unbekannt. Die SMC-B wurde nach Erhalt nicht oder sehr kurzfristig vor der Registrierung aktiviert.<br>▶ Wenden Sie sich entsprechend an den Hersteller der SMC-B.<br>2. HTTP transport error: org.bouncycastle.tls.TlsFatalAlert: internal_error(80) ( - )<br>Die SMC-B kann nicht ordnungsgemäß verwendet werden.<br>▶ Ziehen Sie die SMC-B aus dem Kartenterminal und stecken Sie sie dann erneut. Alternativ können Sie das Kartenterminal aus- und anschließend wieder anschalten. |
| 43018 | Fehler bei Statusabfrage beim Registrierungsserver im Konnektor. | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 43019 | Beim Hochladen einer Update-XML-Datei ist ein Fehler aufgetreten. Datei nicht lesbar. | TECHNICAL | ERROR | | - |
| 43020 | Fehler beim Senden der OperatingData im Registrierungsserver. Fehler: <x> | TECHNICAL | ERROR | | - |
| 43021 | Fehler beim Senden der OperatingData im Konnektor. | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 43022 | Beim Laden der öffentlichen Schlüssel für den KSR ist ein Fehler aufgetreten. Ein Update über KSR ist daher nicht möglich. | TECHNICAL | ERROR | | - |
| 43023 | Das zu aktualisierende Terminal wurde nicht gefunden. | TECHNICAL | ERROR | | - |
| 43024 | Die Zugangsdaten für die Admin-Session am Terminal wurden noch nicht komplett hinterlegt. | TECHNICAL | ERROR | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 43027 | Die URL zum Registrierungs-server konnte nicht aufgelöst werden. | TECHNICAL | WARNING | | Es gibt mehrere mögliche Ursachen für diesen Fehler:<br>- Sofern DHCP verwendet wird, überprüfen Sie ob der Konnektor vom Router Informationen zum Gateway erhalten hat.<br>- Eine mögliche Ursache für dieses Problem kann die Verwendung von DS-Lite sein. Es gilt darum die Einstellungen für MTU anzupassen. Dafür muss zwingend die Version 2.0.37 (oder höher) in-stalliert sein.<br>- Möglicherweise kann DNSSEC nicht verwendet werden. Überprüfen Sie ob der Port 53 (TCP/UDP) ausgehend für den Konnektor freigeschaltet ist.<br>- Dieser Fehler kann in Kombination mit dem Fehler 4180 DNS: Es ist ein Fehler bei der Na-mensauflösung aufgetreten. No location for Service [VPN_REGISTRATION] available! auftreten. Überprüfen Sie dahingehend das Protokoll des Konnektors. Sofern dieser Fehler in Kombination mit dem Fehlern 43014 und 43027 auftritt, beheben Sie zunächst den Fehler 4180.<br>▶ Gateway überpüfen<br>Die Überprüfung des Gateways geschieht unter: Netzwerk > Allgemein > IP-Adresse des Standard-Gateway<br>Hier sollte, sofern dem Konnektor das Gateway bekannt ist, eine IP-Adresse angezeigt werden.<br>▶ MTU anpassen<br>Um den optimalen Wert für MTU zu ermitteln, können Sie unter Windows einen Ping absetzen: ping -f -l 1500<br>Reduzieren Sie den Wert 1500 solange (in Zehnerschritten), bis der Ping die Webseite erreichen kann. Dadurch ergibt sich der höchstmögliche Wert für die Einstellung der MTU.<br>Die anschließende Einstellung des Werts im Konnektors wird folgendermaßen durchgeführt:<br>Im Parallelbetrieb geschieht dies unter: Netzwerk > LAN > Einstellungen > LAN-seitige IP-Paketlänge (MTU)<br>Im Reihenbetrieb geschieht dies unter: Netzwerk > WAN > Einstellungen > WAN-seitige IP-Paketlänge (MTU) |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 43028 | Beim Hochladen einer Firmware-Datei ist ein Fehler aufgetreten. Datei nicht in UpdateInfo.xml enthalten. | TECHNICAL | ERROR | | - |
| 43029 | Eine Aktualisierung wird gerade heruntergeladen. Ein Zurücksetzen des Bereiches 'Aktualisierung' ist derzeit nicht möglich. | TECHNICAL | ERROR | | - |

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

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

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

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 43038 | Eine Aktualisierung konnte nicht installiert werden. 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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 | | - |

#### 12.4.6.1 Fachmodul VSDM

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 3001 | VSD nicht konsistent | TECHNICAL | ERROR | PVS | Die Versichertendaten sind aufgrund eines Fehlers bei einer vorangegangenen Aktualisierung nicht mehr konsistent und können nicht eingelesen werden.<br>▶ Versuchen Sie, die Karte erneut zu aktualisieren.<br>Falls nach 2-3 Versuchen die Karte immer noch denselben Fehler aufweist, ist die eGK ggf. defekt.<br>▶ Verweisen Sie den Versicherten mit Verweis auf die Meldung an seine Krankenkasse. Verfahren Sie entsprechend der Vereinbarung zum Inhalt und zur Anwendung der elektronischen Gesundheitskarte (*Anlage 4a BMV-Ä*), wenn eine Karte nicht verwendet werden kann. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 3011 | Verarbeiten der Versicherten-daten gescheitert | TECHNICAL | ERROR | PVS | Beim Einlesen der Versichertendaten von der eGK ist ein Fehler aufgetreten.<br>▶ Stecken Sie die Karte erneut ein und wiederholen Sie den Vorgang.<br>▶ Wenn das Problem nur bei einer bestimmten Karte auftritt, ist ggf. die Karte defekt. Verweisen Sie den Versicherten an seine Krankenkasse. Verfahren Sie entsprechend der Vereinbarung zum Inhalt und zur Anwendung der elektronischen Gesundheitskarte (*Anlage 4a BMV-Ä*), wenn eine Karte nicht verwendet werden kann.<br>▶ Wenden Sie sich ansonsten an den DVO. |
| 3020 | Lesen KVK gescheitert | TECHNICAL | ERROR | PVS | Beim Einlesen der Krankenversichertenkarte (KVK) ist ein Fehler aufgetreten.<br>▶ Stecken Sie die Karte erneut ein und wiederholen Sie den Vorgang.<br>▶ Wenn das Problem nur bei einer bestimmten Karte auftritt, ist ggf. die Karte defekt.<br>▶ Wenden Sie sich ansonsten an den DVO.<br>Hinweis: Die KVK ist seit 01.01.2015 nur noch für Versicherte sogenannter sonstiger Kostenträger (z.B. Heilfürsorge) sowie im Rahmen der Privatversicherung zulässig. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 3021 | KVK-Prüfsumme falsch, Daten korrupt | TECHNICAL | ERROR | PVS | Beim Einlesen der Krankenversichertenkarte (KVK) ist ein Fehler aufgetreten. Die KVK ist ungültig oder defekt.<br>▶ 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.<br>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.<br>▶ Wiederholen Sie die Onlineprüfung für die eGK am Online-Konnektor und lesen Sie die Karte erneut ein.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 3040 | Es ist kein Prüfungsnachweis auf der eGK vorhanden | TECHNICAL | ERROR | PVS | Es ist kein Prüfungsnachweis auf der eGK vorhanden.<br>Beim Einlesen einer eGK kommt es zum Fehler, der Prüfungsnachweis lässt sich nicht auslesen.<br>Eine eGK ohne Prüfungsnachweis wird vom PVS mit den ReadVSD Parametern ReadOnlineReceipt = true und PerformOnlineCheck = false (MODE_ONLINE_CHECK = NEVER) an einem Online-Konnektor aufgerufen. Dieser Aufruf ist nur für einen Offline-Konnektor im Standalone-Szenario vorgesehen und führt folglich zu einem Fehler beim Online-Konnektoren.<br>▶ Vorgehen bei einem Online-Konnektor (gilt auch für das Standalone-Szenario): Konfigurieren Sie das PVS so, dass die ReadVSD Parameter entsprechen den Modi MODE_ONLINE_CHECK = USER / ALWAYS / FIRST aufgerufen werden.<br>▶ Vorgehen bei einem Offline-Konnektor (Standalone-Szenario): Stellen Sie organisatorisch sicher, dass die am Offline-Konnektor einzulesende eGK vorher an dem Online-Konnektor der Praxis auf die Aktualität hin überprüft wurde. |
| 3041 | SM-B nicht freigeschaltet | TECHNICAL | ERROR | PVS | Die verwendete SMC-B ist nicht freigeschaltet.<br>▶ Schalten Sie die entsprechende SMC-B frei. |
| 3042 | HBA nicht freigeschaltet | TECHNICAL | ERROR | PVS | Der verwendete HBA ist nicht freigeschaltet.<br>▶ Schalten Sie den entsprechenden HBA frei. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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.<br>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.<br>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.<br>Die eGK ist gültiger Leistungsanspruchsnachweis. VSD können mit Prüfungsnachweis 3 („Aktualisierung VSD auf eGK technisch nicht möglich") eingelesen werden. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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<br>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.<br>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, kartenindividuellen symmetrischen Schlüssels ist fehlgeschlagen. | SECURITY | FATAL | PVS | Fehler bei der Onlineprüfung der eGK. Der Aufbau der gesicherten Verbindung zwischen Karte und Fachdienst ist fehlgeschlagen. Die Fehlerursache muss vom Fachdienstbetreiber analysiert werden.<br>Die eGK ist gültiger Leistungsanspruchsnachweis. VSD können mit Prüfungsnachweis 3 („Aktualisierung VSD auf eGK technisch nicht möglich") eingelesen werden.<br>▶ Wenn der Fehler mehrfach bei verschiedenen eGKs auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 12105 | Die eGK ist defekt. | TECHNICAL | FATAL | PVS | Abbruch des Anwendungsfalles der Onlineprüfung der eGK, kein Einlesen der Versichertendaten möglich.<br>▶ Stecken Sie die Karte erneut ein.<br>▶ 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. Verfahren Sie entsprechend der Vereinbarung zum Inhalt und zur Anwendung der elektronischen Gesundheitskarte (*Anlage 4a BMV-Ä*), wenn eine Karte nicht verwendet werden kann.<br>▶ 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.<br>Die eGK ist gültiger Leistungsanspruchsnachweis. VSD können mit Prüfungsnachweis 3 („Aktualisierung VSD auf eGK technisch nicht möglich") eingelesen werden. |

### 12.4.6.2 Fachmodul NFDM

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 5000 | Die eGK ist defekt. | TECHNICAL | FATAL | PVS | Ein technisches Problem ist beim Nutzen der eGK aufgetreten.<br>▶ Stecken Sie die Karte erneut ein und wiederholen sie den Vorgang.<br>▶ 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.<br>▶ 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 Operation durchzuführen.<br>▶ Verwenden Sie ggf. eine andere Karte. |
| 5003 | Notfalldaten-satz nicht kon-sistent | TECHNICAL | ERROR | PVS | Die Notfalldaten auf der Karte sind nicht konsistent geschrieben wor-den und können daher nicht gelesen werden.<br>▶ Die Notfalldaten müssen neu geschrieben werden. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 5004 | Unbekannte Version der Speicherstruktur für den Notfalldatensatz auf der eGK | TECHNICAL | FATAL | PVS | Ein technisches Problem ist beim Nutzen der eGK aufgetreten.<br>▶ Stecken Sie die Karte erneut ein und wiederholen sie den Vorgang.<br>▶ 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. Verfahren Sie entsprechend der Vereinbarung zum Inhalt und zur Anwendung der elektronischen Gesundheitskarte (*Anlage 4a BMV-Ä*), wenn eine Karte nicht verwendet werden kann. |
| 5006 | Dekomprimierung des Notfalldatensatzes gescheitert | TECHNICAL | ERROR | PVS | - |
| 5007 | Decodierung des Notfalldatensatzes gescheitert | TECHNICAL | ERROR | PVS | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 5008 | Die Versicherten-ID des Notfalldatensatzes stimmt nicht mit der Versicherten-ID der eGK überein. | SECURITY | ERROR | PVS | Die Notfalldaten, die auf die Karte geschrieben werden sollen, passen nicht zur verwendeten Karte.<br>▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang.<br>▶ 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 | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 5012 | Das Löschen des Notfalldatensatzes ist gescheitert. | TECHNICAL | ERROR | PVS | Ein technisches Problem ist beim Nutzen der eGK aufgetreten.<br>▶ Stecken Sie die Karte erneut ein und wiederholen sie den Vorgang.<br>▶ 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. Verfahren Sie entsprechend der Vereinbarung zum Inhalt und zur Anwendung der elektronischen Gesundheitskarte (*Anlage 4a BMV-Ä*), wenn eine Karte nicht verwendet werden kann. |
| 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.<br>▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |
| 5014 | Das Primärsystem hat keine Zugriffsberechtigung auf die eGK. | SECURITY | ERROR | PVS | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für 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.<br>▶ Stecken Sie die Karte erneut ein und wiederholen sie den Vorgang.<br>▶ 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. Verfahren Sie entsprechend der Vereinbarung zum Inhalt und zur Anwendung der elektronischen Gesundheitskarte (*Anlage 4a BMV-Ä*), wenn eine Karte nicht verwendet werden kann. |
| 5017 | Der Notfalldatensatz ist nicht valide. | SECURITY | ERROR | PVS | Die Notfalldaten, die auf die Karte geschrieben werden sollen, sind ungültig.<br>▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 5018 | Die Signaturprüfung konnte nicht durchgeführt werden. | SECURITY | ERROR | PVS | Die Notfalldaten, die auf die Karte geschrieben werden sollen, sind ungültig.<br>▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang.<br>▶ 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.<br>▶ 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 | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 5103 | Datensatz „Persönliche Erklärungen“ nicht konsistent | TECHNICAL | ERROR | PVS | Der Datensatz „Persönliche Erklärungen“ auf der Karte ist nicht konsistent geschrieben worden und kann daher nicht gelesen werden.<br>▶ 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.<br>▶ Stecken Sie die Karte erneut ein und wiederholen sie den Vorgang.<br>▶ 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. Verfahren Sie entsprechend der Vereinbarung zum Inhalt und zur Anwendung der elektronischen Gesundheitskarte (*Anlage 4a BMV-Ä*), wenn eine Karte nicht verwendet werden kann. |
| 5106 | Dekomprimierung des Datensatz „Persönliche Erklärungen“ gescheitert | TECHNICAL | ERROR | PVS | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für 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 soll, passt nicht zur verwendeten Karte.<br>▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |
| 5109 | Die Kodierung (base64) des Datensatz „Persönliche Erklärungen“ ist gescheitert. | TECHNICAL | ERROR | PVS | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für 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.<br>▶ Stecken Sie die Karte erneut ein und wiederholen sie den Vorgang.<br>▶ 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. Verfahren Sie entsprechend der Vereinbarung zum Inhalt und zur Anwendung der elektronischen Gesundheitskarte (*Anlage 4a BMV-Ä*), wenn eine Karte nicht verwendet werden kann. |
| 5113 | Der Datensatz „Persönliche Erklärungen“ überschreitet die maximal zulässige Größe. | BUSINESS | ERROR | PVS | Der Datensatz „Persönliche Erklärungen“, der auf die Karte geschrieben werden soll, ist zu groß für die Karte.<br>▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 5114 | Der Datensatz „Persönliche Erklärungen“ ist nicht valide. | SECURITY | ERROR | PVS | Der Datensatz „Persönliche Erklärungen“, der auf die Karte geschrieben werden soll, ist ungültig.<br>▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang.<br>▶ 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.<br>▶ 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 | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für 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.<br>▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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.<br>▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |
| 5500 | Interner Fehler | TECHNICAL | FATAL | PVS | - |

### 12.4.6.3 Fachmodul AMTS

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 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.<br>▶ Schalten Sie die entsprechende SMC-B frei. |
| 6051 | eGK-Generation 1 und 1+ nicht unterstützt | TECHNICAL | ERROR | PVS | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 6052 | Verbindungs-fehler zwischen Karten | SECURITY | ERROR | PVS | - |
| 6054 | eMP/AMTS-Daten sind inkonsistent. Bitte Daten er-neut schreiben. | TECHNICAL | ERROR | PVS | Die eMP/AMTS-Daten auf der Karte sind nicht konsistent geschrieben worden und können daher nicht gelesen werden.<br>▶ Die eMP/AMTS-Daten müssen neu geschrieben werden. |
| 6056 | Einverständnis nicht erteilt | TECHNICAL | ERROR | PVS | - |
| 6057 | Versicherten-ID von eGK und zu speichernde Daten unter-scheiden sich | BUSINESS | ERROR | PVS | Die eMP/AMTS-Daten, die auf die Karte geschrieben werden sollen, passen nicht zur verwendeten Karte.<br>▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang.<br>▶ Wenn der Fehler weiterhin auftritt, wenden Sie sich an den DVO. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 6058 | eMP/AMTS-Daten konnten nicht validiert werden | TECHNICAL | ERROR | PVS | Die eMP/AMTS-Daten, die auf die Karte geschrieben werden sollen, sind ungültig.<br>▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang.<br>▶ 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.<br>▶ Kontrollieren sie die Daten und wiederholen sie den Vorgang.<br>▶ 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 | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 6063 | eGK gesperrt | SECURITY | ERROR | PVS | Die eGK ist kein gültiger Leistungsanspruchsnachweis.<br>▶ Fragen Sie den Versicherten, ob er in der Zwischenzeit eine neuere eGK von der Krankenkasse zugeschickt bekommen hat.<br>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.<br>▶ 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.<br>▶ Aktivieren sie mit dem Versicherten die Anwendung AMTS. |
| 6065 | Löschung der AMTS-Daten nicht zugestimmt | BUSINESS | ERROR | PVS | - |
| 6072 | Operation durch Ziehen der eGK vorzeitig beendet | TECHNICAL | ERROR | PVS | - |

#### 12.4.6.4 Fachmodul ePA

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 7200 | Lokalisierung des Aktensystems fehlgeschlagen | TECHNICAL | ERROR | PVS | Die Lokalisierung des Aktensystems funktioniert in der TI momentan nicht.<br>▶ Versuchen Sie, erneut die Operation durchzuführen<br>Falls nach 2-3 Versuchen die Operation immer noch denselben Fehler aufweist ist der Dienst aktuell nicht erreichbar.<br>Verweisen Sie den Versicherten mit Verweis auf die Meldung an seine Krankenkasse/seinen Aktenanbieter. |
| 7202 | Verbindung zum Aktensystem fehlgeschlagen | SECURITY | ERROR | PVS | Der Verbindungsaufbau zum Aktensystems funktioniert im Momentan nicht.<br>▶ Versuchen Sie, erneut die Operation durchzuführen<br>Falls nach 2-3 Versuchen die Operation immer noch denselben Fehler aufweist ist der Dienst aktuell nicht erreichbar.<br>Verweisen Sie den Versicherten mit Verweis auf die Meldung an seine Krankenkasse/seinen Aktenanbieter. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 7203 | Die gegenseitige Authentisierung von eGK und SMC-B (Card-to-Card-Authentisierung) ist gescheitert. | SECURITY | ERROR | PVS | Ein technisches Problem ist beim Nutzen der eGK aufgetreten.<br>▶ Stecken Sie die Karte erneut und wiederholen sie den Vorgang.<br>▶ 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. Verfahren Sie entsprechend der Vereinbarung zum Inhalt und zur Anwendung der elektronischen Gesundheitskarte (*Anlage 4a BMV-Ä*), wenn eine Karte nicht verwendet werden kann. |
| 7205 | Es konnte kein freigeschaltetes SM-B mit einem zulässigen Institutionstyp gefunden werden. | TECHNICAL | ERROR | PVS | Aktuell steckt keine freigeschaltet SMC-B im System .<br>▶ Schalten Sie eine entsprechende SMC-B frei. |
| 7206 | Prüfung der Zugriffsberechtigung fehlgeschlagen | TECHNICAL | ERROR | PVS | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 7207 | PIN-Verifikation gescheitert | TECHNICAL | ERROR | PVS | - |
| 7208 | Es konnte kein freigeschaltetes SM-B des Mandanten gefunden werden. | TECHNICAL | ERROR | PVS | Aktuel steckt keine freigeschaltet SMC-B im System.<br>▶ Schalten Sie eine entsprechende SMC-B frei. |
| 7209 | Keine Berechtigung für das Aktenkonto vorhanden | TECHNICAL | ERROR | PVS | Der Versicherte bzw. der Leistungserbringer hat keinen Zugriff auf das Angefragte Aktenkonto.<br>▶ Prüfen sie ob das richtige Aktenkonto verwendet wurde und ob noch Zugriffberechtigungen exestieren |
| 7210 | Die Berechtigung kann nicht hinterlegt werden. | TECHNICAL | ERROR | PVS | Es ist ein Fehler beim Hinterlegen der Berechtigungen aufgetretten.<br>▶ Versuchen Sie, erneut die Operation durchzuführen |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 7211 | Dokument überschreitet maximal zulässige Größe von 25 MB | TECHNICAL | ERROR | PVS | Das verwendete Dokument ist zu Groß um es im Aktensystem abzulegen.<br>▶ Verringern sie die Größe des Dokuments |
| 7212 | Summe der Dokumente überschreitet maximal zulässige Größe von 250 MB | TECHNICAL | ERROR | PVS | Die verwendeten Dokumente überschreiten die maximal zulässige Größe für einen Aufruf beim Aktensystem.<br>▶ Verschicken sie die Dokumente in einzelnen kleineren Aufrufen |
| 7213 | Sperrstatus des Zertifikats der eGK nicht ermittelbar | TECHNICAL | ERROR | PVS | Fehler bei der Online-Prüfung der eGK.<br>▶ Versuchen Sie, erneut die Operation durchzuführen.<br>Falls nach 2-3 Versuchen die Operation immer noch denselben Fehler aufweist ist der Online-Dienst für die Zertifikatsprüfung aktuell nicht erreichbar.<br>▶ Verweisen Sie den Versicherten mit Verweis auf die Meldung an seine Krankenkasse/seinen Aktenanbieter. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 7214 | Das Schlüsselmaterial der Akte entspricht nicht den Sicherheitsanforderungen. | SECURITY | ERROR | PVS | - |
| 7215 | Fehler im Aktensystem - Die Operation konnte nicht durchgeführt werden. | TECHNICAL | ERROR | PVS | Ein technisches Problem ist beim Nutzen des Aktensystems aufgetreten.<br>▶ Wiederholen sie den Vorgang.<br>▶ Falls nach 2-3 Versuchen die Operation immer noch denselben Fehler aufweist, verweisen Sie den Versicherten mit Verweis auf die Meldung an seine Krankenkasse/seinen Aktenanbieter. |
| 7217 | Die Operation wurde am Kartenterminal abgebrochen. | TECHNICAL | ERROR | PVS | - |
| 7220 | Aktensystem nicht erreichbar | INFRASTRUCTURE | ERROR | PVS | Der Verbindungsaufbau zum Aktensystems funktioniert im Momentan nicht.<br>▶ Versuchen Sie, erneut die Operation durchzuführen<br>Falls nach 2-3 Versuchen die Operation immer noch denselben Fehler aufweist ist der Dienst aktuell nicht erreichbar.<br>▶ Verweisen Sie den Versicherten mit Verweis auf die Meldung an seine Krankenkasse/seinen Aktenanbieter. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 7221 | Zertifikat auf SMC-B ungültig | SECURITY | ERROR | PVS | Die verwendete SMC-B ist nicht mehr gültig.<br>▶ Verwende sie eine andere SMC-B |
| 7230 | Die Liste der Berechtigungen ist möglicherweise unvollständig, da nicht alle bekannten Aktensysteme abgefragt werden konnten. | TECHNICAL | WARNING | PVS | - |
| 7231 | Die Abfrage getAuthorizationList wurde zu häufig gestellt. | TECHNICAL | ERROR | PVS | - |
| 7290 | Die Patientenakte konnte nicht gefunden werden. | TECHNICAL | ERROR | PVS | Für die Angaben konnte bei keinem Aktenanbieter ein Aktenkonte gefunden werden.<br>▶ Verweisen Sie den Versicherten mit Verweis auf die Meldung an seine Krankenkasse/seinen Aktenanbieter. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 7291 | Die Patientenakte konnte nicht eindeutig identifiziert werden. | TECHNICAL | ERROR | PVS | Für die Angaben konnte kein eindeutiger Aktenanbieter identifiziert werden.<br>▶ Verweisen Sie den Versicherten mit Verweis auf die Meldung an seine Krankenkasse/seinen Aktenanbieter. |
| 7400 | Fehler - Die Operation konnte nicht durchgeführt werden. | TECHNICAL | ERROR | PVS | Der Operation mit dem Aktensystem konnte nicht durchgeführt werden.<br>▶ Versuchen Sie, erneut die Operation durchzuführen<br>Falls nach 2-3 Versuchen die Operation immer noch denselben Fehler aufweist ist eine Kommunikation mit dem Dienst aktuell nicht möglich.<br>▶ Verweisen Sie den Versicherten mit Verweis auf die Meldung an seine Krankenkasse/seinen Aktenanbieter. |
| 7401 | Operation konnte nicht durchgeführt werden - Akte vorübergehend nicht verfügbar. | TECHNICAL | ERROR | PVS | Der Operation mit dem Aktensystem konnte nicht durchgeführt werden.<br>▶ Versuchen Sie, erneut die Operation durchzuführen<br>Falls nach 2-3 Versuchen die Operation immer noch denselben Fehler-Aufweist, ist eine Kommunikation mit dem Dienst aktuell nicht möglich. Verweisen Sie den Versicherten mit Verweis auf die Meldung an seine Krankenkasse/seinen Aktenanbieter. |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 7402 | Das Aktenkonto ist bereits eingerichtet. | TECHNICAL | WARNING | PVS | - |
| 7403 | Das Aktenkonto kann noch nicht verwendet werden. | TECHNICAL | ERROR | PVS | Der Status des Status des Aktenkontos entspricht nicht den Vorraussetzungen für diese Operation.<br>▶ Prüfen sie, ob das Aktenkonto ggf. noch Aktiviert werden muss.<br>▶ Ansonsten Verweisen Sie den Versicherten mit Verweis auf die Meldung an seine Krankenkasse/seinen Aktenanbieter. |
| 7404 | Das Aktenkonto existiert nicht (mehr) in diesem ePA-Aktensystem. | TECHNICAL | ERROR | PVS | - |
| 7405 | Das Aktenkonto wurde bei diesem ePA-Aktensystem gekündigt, kann aber aktuell noch benutzt werden. | TECHNICAL | WARNING | PVS | - |

| Code | Beschreibung | Typ | Level | PVS | Fehlerbehebung/Weitere Angaben für PVS |
|---|---|---|---|---|---|
| 7406 | Das Aktenkonto wurde bei diesem ePA-Aktensystem gekündigt und ist nur noch für einen Kontowechsel lesend zugreifbar. | TECHNICAL | WARNING | PVS | - |

### 12.4.7 Weitere Meldungen zu Verbindungsproblemen

Legende:

| | |
|---|---|
| Code | Fehler-ID (dient als Referenz der gematik) |
| Beschreibung/<br>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/<br>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 |
| 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 |
| 45012 | no answer from charon after sending command | charon Dämon läuft nicht | Technical | Error | Operation wiederholen |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 45013 | SIS cannot be initiated while TI is down | Anwenderfehler (kein SIS ohne TI!) | Technical | Error | Manuelle 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 connection | Laufzeitfehler in der VICI-Bibliothek aufgetreten | Technical | Error | Konnektor neu starten |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 45031 | poll() failed | Kommunikationsfehler zwischen dem connector-vpnman und dem charon-Daemon (strongSwan VPN) aufgetreten | Technical | Error | Konnektor neu starten |
| 45033 | failed reading from file | Multiple Fehlerursachen:<br>• Korruptes Dateisystem (HW-Fehler)<br>• Dateisystem voll<br>• HW-Fehler des Hintergrundspeichers<br>• Fehlkonfiguration | Technical | Error | Konnektor neu starten; wenn sich nach dem Neustart keine Veränderung ergibt, den Support kontaktieren |
| 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 Hintergrundspeichers aufgetreten | Technical | Error | Logdateien auf dem Konnektor löschen und neu starten |
| 45038 | unable to connect to MQTT broker | MQTT Broker nicht erreichbar | Technical | Fatal | Konnektor neu starten |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 certificate 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 certificate 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 certificate 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 | public key of concentrator's certificate uses unexpected elliptic curve | Das X.509v3-Zertifikat des VPN-Zugangsdienstes ist fehlerhaft. | 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 |
|---|---|---|---|---|---|
| 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. |
| 45057 | Unable to create VPN device | Netzwerkstack-Fehler | Technical | Error | Konnektor neu starten |
| 45100 | Internal error (configuration bad) occurred. | Nicht behebbarer Laufzeitfehler | Technical | Error | Mit Log-Dateien an Hersteller wenden |
| 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 | |
| 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) |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 Zentraldienstenetz und dem lokalen Netz | Technical | Error | Interne IT-Infrastruktur anpassen und DHCP-Server umkonfigurieren |
| 45110 | IPv4 address %s overlaps with net 'TI Dezentral (Konnektoren)' | IP-Überlappung zwischen dem Netz der TI und dem lokalen Netz | Technical | Error | Interne IT-Infrastruktur anpassen und DHCP-Server umkonfigurieren |
| 45111 | IPv4 address %s overlaps with net 'TI Dezentral SIS (Konnektoren)' | IP-Überlappung zwischen dem SIS-Netz und dem lokalen Netz | Technical | Error | Interne IT-Infrastruktur anpassen und DHCP-Server umkonfigurieren |
| 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 |
| 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 |
| 45314 | Unable to create VBOX virtual machine (4/6) | SSD-Kapazität erschöpft | Technical | Error | Log-Dateien löschen oder Werksreset durchführen |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 45509 | Unable to enforce rule set '%s' because it is UNKNOWN. | Konfiguration fehlerhaft | Technical | Error | Konfiguration prüfen, ggf. Konnektor neu starten |
| 45510 | insufficient memory available. | RAM-Speicherkapazität erschöpft | Technical | Error | Konnektor neu starten |
| 45511 | Unable to purge limit rule - rule set tastes bad | Konfiguration fehlerhaft | Technical | Error | Konfiguration prüfen, ggf. Konnektor neu starten |
| 45512 | Unable to determine route to host %s (TI concentrator). | Routing-Konfiguration fehlerhaft | Technical | Error | Konfiguration prüfen und neu laden |
| 45513 | Unable to determine route to host %s (SIS concentrator). | Routing-Konfiguration fehlerhaft | Technical | Error | Konfiguration prüfen und neu laden |
| 45514 | unknown substitution prefix found. | Konfiguration fehlerhaft | Technical | Error | Konfiguration prüfen, ggf. Konnektor neu starten |
| 45515 | expected exit code is %i, returned exit code is %i. | Netfilter-Problem im Kernel | Technical | Error | Konnektor neu starten |
| 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 | |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 45519 | (UNWIND) expected exit code is %i, returned exit code is %i. | Netfilter-Problem im Kernel | Technical | Error | Konnektor neu starten |
| 45520 | unable to perform global (initial) main configuration. | Netfilter-Problem im Kernel | Technical | Error | Konnektor neu starten |
| 45521 | unable to perform global (initial) ip configuration. | Netzwerkstack-Problem im Kernel | Technical | Error | Konnektor neu starten |
| 45522 | unable to perform global (initial) xfrm configuration. | XFRM-Problem im Kernel | Technical | Error | Konnektor neu starten |
| 45523 | unable to perform global (initial) iptables 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 | |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 |
| 45533 | Unable to establish a new default gateway (%s 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 |
| 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 | |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 45542 | mosquitto_new | Mosquitto Service nicht erreichbar | Technical | Error | Konnektor neu starten |
| 45543 | mosquitto_threaded_set | Mosquitto Service nicht erreichbar | Technical | Error | Konnektor neu starten |
| 45544 | mosquitto_subscribe | Mosquitto Service nicht erreichbar | Technical | Error | Konnektor neu starten |
| 45545 | Unable to flush XFRM policies | Netzwerkstack-Fehler | Technical | Error | Konnektor neu starten |
| 45546 | Unable to set host name '%s' of connector. EXIT | Netzwerkstack-Fehler | Technical | Error | Konnektor neu starten |
| 46000 | Enforcement of initial (static) rules failed. EXIT. | Netzwerkstack-Fehler | Technical | Fatal | Konnektor neu starten |
| 46001 | Unable to apply ANLW_LEKTR_INTRANET_ROUTES routes; current route is %s via %s (exitcode of route command is %i). | ANLW_LEKTR_INTRANET_ROUTES (siehe [gemSpec]) konnten 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]) konnten nicht gesetzt werden | Technical | Fatal | Konfiguration prüfen und neu laden |
| 46003 | Unable to enforce rule stack '%s'. This is fatal. | Regelsatz 'AK' kann nicht eingesetzt werden (netfilter/routing-Problem) | Technical | Fatal | Konnektor neu starten |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 |
| 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 '%s'. This is fatal. | Regelsatz 'AK' 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 |
| 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 (%s) IPv4 address / netmask combination. | Regelsatz WAN kann nicht gesetzt 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 |
| 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 | |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 46040 | Unable to enforce rule stack 'lektr_intranet_routes'. This is fatal. | | Technical | Fatal | |
| 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 neu starten |
| 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 46506 | Failed to send SIGHUP for event with ID='%s', pid=%lu | Connector-Service kann bei einer Änderung der Konfiguration kein SIGHUP-Signal an einen nachgeschalteten Prozess senden | Technical | Error | keine Aktion |
| 46507 | Could not compute the broadcast IP address (SICCT). | SICCT-Konfiguration fehlerhaft | Technical | Error | Konfiguration prüfen und neu laden |
| 46508 | Could not perform the UDP bind to socket %s. | bind() an UDP-Socket nicht möglich | Technical | Error | Konnektor neu starten |
| 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 |
| 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 46514 | ERROR: Unable to create MQTT thread. | Thread kann nicht erstellt werden | Technical | Error | Konnektor neu starten |
| 46515 | ERROR: Unable to create new MQTT client instance. | MQTT-Broker reagiert nicht | Technical | Error | Konnektor neu starten |
| 46516 | ERROR: Unable to set MQTT to threaded. | MQTT-Broker reagiert nicht | Technical | Error | Konnektor neu starten |
| 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 46523 | Mosquitto loop returned error: %i (MOSQ_ERR_CONN_LOST). | MQTT-Broker reagiert nicht | Technical | Error | keine Aktion; der Service versucht stetig, die Verbindung neu aufzubauen |
| 46524 | Mosquitto loop returned error: %i (MOSQ_ERR_UNKNOWN). | MQTT-Broker reagiert nicht | Technical | Error | keine Aktion; der Service versucht stetig, die Verbindung neu aufzubauen |
| 46525 | Mosquitto loop returned error: %i (MOSQ_ERR_ERRNO). | MQTT-Broker reagiert nicht | Technical | Error | keine Aktion; der Service versucht stetig, die Verbindung neu aufzubauen |
| 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 46530 | error locking system state information (rc=%d) | Zugriff auf die Informationen zu den aktuellen Softwareständen nicht möglich | Technical | Error | Konnektor neu starten |
| 46531 | error retrieving system state information: %d | Zugriff auf die Informationen zu den aktuellen Softwareständen nicht möglich | Technical | Error | Konnektor neu starten |
| 46532 | error retrieving system ID: %d | Zugriff auf die Informationen zu den aktuellen Softwareständen nicht möglich | Technical | Error | Konnektor neu starten |
| 46533 | error retrieving application image ID: %d | Zugriff auf die Informationen zu den aktuellen Softwareständen nicht möglich | Technical | Error | Konnektor neu starten |
| 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 |

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

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 46542 | Download CRL : unable to download CRL (network error). | Die CRL kann aufgrund eines Netzwerkfehlers nicht heruntergeladen werden (z.B. findet aktuell eine Umkonfigurierung statt oder der Server ist tatsächlich "down"). | Technical | Error | Auto-Download der CRL in der MGMT-UI erneut anstoßen; bei wiederholtem Fehler: Support kontaktieren |
| 46543 | Download CRL : unable to ASN.1 parse the CRL. | Die CRL ist syntaktisch nicht korrekt. Dies ist ein Fehler der Telematikinfrastruktur. | Technical | Error | Auto-Download der CRL in der MGMT-UI erneut anstoßen; bei wiederholtem Fehler: Support kontaktieren |
| 46544 | Download CRL : downloaded CRL is not valid anymore. | Die CRL wurde soeben aktualisiert aber ist nicht mehr gültig. Dies ist entweder ein Fehler der Telematikinfrastruktur oder die Zeitsynchronisation des Konnektors ist fehlgeschlagen, und der Konnektor arbeitet mit einer falschen Systemzeit. | Technical | Error | Auto-Download der CRL in der MGMT-UI erneut anstoßen; bei wiederholtem Fehler: Support kontaktieren oder Konnektor neu starten |
| 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 |

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

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 46550 | parseTSL: Invalid CPU architecture detected (only 64bit supported). | Dies ist ein so genannter "sanity check" innerhalb der Quellcodes und kann als Fehler nur auftreten, wenn der Konnektor in einer 32bit-Firmware betrieben wird, was nicht geplant ist. | Technical | Error | Keine Aktion, siehe Beschreibung links. |
| 46551 | parseTSL: Invalid parameters passed (please contact the soft-ware vendor). | Interner Software-Fehler (sanity check) | Technical | Error | Support kontaktieren |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 46552 | parseTSL: TSL not readable (I/O error). | Die TSL (als Datei) kann nicht vom Hintergrundspeicher (SSD) gelesen werden.<br>Im Protokoll des Konnektors wird diese Fehlermeldung angezeigt, sofern ein Problem mit der eingespielten TSL vorliegt.<br>Eine neue TSL wird spätestens sieben Tage vor Ablauf der Gültigkeit der aktuellen TSL, i.d.R. jedoch ca. alle zwei Wochen, durch die gematik bereitgestellt | Technical | Error | Zunächst prüfen, welche TSL aktuell im Konnektor eingespielt ist:<br>System > Zertifikate > TSL Information > Sequenznummer<br>Sofern durch die gematik eine neuere TSL bereitgestellt wurde, kann diese manuell eingespielt werden. Dazu deaktivieren Sie zunächst den Leistungsumfang Online: Netzwerk > Allgemein > Leistungsumfang Online<br>Laden Sie anschließend die aktuelle TSL manuell herunter (z. B. via Support-Kit). Support-Kit laden ><br>Alternativ können Sie die aktuelle TSL von „https://download.tsl.ti-dienste.de/TSL.xml“ und den zugehörigen Hashwert von „https://download.tsl.ti-dienste.de/TSL.sha2“ herunterladen.<br>Spielen Sie die TSL am Konnektor ein:<br>System > Zertifikate > TSL hochladen ...<br>Aktivieren Sie Leistungsumfang Online:<br>Netzwerk > Allgemein > Leistungsumfang Online<br>Starten Sie abschließend den Konnektor neu: System > Allgemein > Neustart<br>Sollte der Fehler weiterhin auftreten, kontaktieren Sie den Support. |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 46553 | parseTSL: Trust store (compiled TSL) not writable (I/O error). | Die TSL kann als binarisierte Version nicht im Hintergrundspeicher abgelegt werden. | Technical | Error | TSL über die MGMT-UI erneut einbringen. Bei wiederholtem Fehler, Support kontaktieren. |
| 46554 | parseTSL: Insufficient memory available. | Nicht genügend RAM-Speicher verfügbar | Technical | Error | TSL über die MGMT-UI erneut einbringen. Bei wiederholtem Fehler, Support kontaktieren. |
| 46555 | parseTSL: Unable to parse TSL XML. | Die TSL sind syntaktisch nicht korrekt. Dies ist ein Fehler der TI. | Technical | Error | TSL über die MGMT-UI erneut einbringen. Bei wiederholtem Fehler, TI kontaktieren |
| 46556 | parseTSL: Unable to parse X.509 (DER encoded) certificate(s) from the TSL. | Die in der TSL gespeicherten Zertifikate (oder mindestens eines davon) sind nicht korrekt (binär) formatiert. | Technical | Error | TSL über die MGMT-UI erneut einbringen. Bei wiederholtem Fehler, TI kontaktieren |
| 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 46560 | parseTSL: Trust store (compiled TSL) is corrupt. | Der binarisierte Trust-Store (aus TSL hervorgegangen) ist korrupt. Dies deutet auf einen I/O-Fehler des Hintergrundspeichers hin. | Technical | Error | TSL über die MGMT-UI erneut einbringen. Bei wiederholtem Fehler, Support kontaktieren. |
| 46561 | parseTSL: No CRL download URL found in the TSL. | Die TSL enthält keine CRL-Download-URL. | Technical | Error | TSL über die MGMT-UI erneut einbringen. Bei wiederholtem Fehler, TI kontaktieren. |
| 46562 | I/O error: unable to open file '%s' | Eine Datei kann nicht vom Hintergrundspeicher gelesen werden. | Technical | Error | Konnektor neu starten |
| 46563 | I/O error: file '%s' has zero length | Eine Datei wurde auf Länge 0 gekürzt (fälschlicherweise). | Technical | Error | Konnektor neu starten |
| 46564 | I/O error: reading file '%s' - insufficient memory available | Es ist nicht genug RAM-Speicher verfügbar. | Technical | Error | Konnektor neu starten |
| 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 wird aber noch nicht vorhanden ist (und auch keine manuelle CRL im Konnektor vorliegt) | Technical | Error | Konnektor neu starten |
| 46567 | writeCRL: CRL not returned from server (error response received) | Der Web-Server, der die CRL anbietet, hat einen HTTP-Fehlercode geliefert, anstatt die CRL anzubieten. | Technical | Error | Auto-Download der CRL in MGMT-UI neu anstoßen. Bei wiederholtem Fehler: ggf. auf manuelle CRL ausweichen. Bei immer noch bestehender Fehlerursache: TI informieren. |
| 46568 | writeCRL: Invalid function parameters passed | Software-Fehler | Technical | Error | Support informieren |
| 46569 | writeCRL: unable to parse X.509v3 certificate | Ein CRL-Signer-Zertifikat (Teil der CRL-Prüfung ist die Signaturprüfung der CRL) ist syntaktisch nicht korrekt. | Technical | Error | Auto-Download der CRL in MGMT-UI neu anstoßen. Bei wiederholtem Fehler: ggf. auf manuelle CRL ausweichen. Bei immer noch bestehender Fehlerursache: TI informieren. |

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

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 |
| 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 |

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

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 |
| 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 |
| 46601 | STARTUP] Unable to initialize TSL/CRL facility (unable to lock down TSL/CRL facility). | Interner Verarbeitungsfehler | Technical | Error | Konnektor neu starten |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 46617 | writeCRL: no valid CRL returned from server (error response re-ceived) | CRL Download fehlgeschlagen. Download-Server meldet Fehler. | Technical | Error | CRL manuell einbringen |
| 46618 | [CRL logic] Unable to lock mutex | Interner Verarbeitungsfehler | Technical | Error | Konnektor neu starten |
| 46619 | [UpdateCRL REST] Unable to lock mutex | Interner Verarbeitungsfehler | Technical | Error | Konnektor neu starten |
| 46620 | [UpdateCRL REST] Unable to lock global mutex | Interner Verarbeitungsfehler | Technical | Error | Konnektor neu starten |
| 46621 | [Force automatic CRL download] Unable to lock mutex | Interner Verarbeitungsfehler | Technical | Error | Konnektor neu starten |
| 46622 | [Force automatic CRL download] : internal parameter error | Interner Verarbeitungsfehler | Technical | Error | Konnektor neu starten |
| 46623 | [Force automatic CRL download] : internal error | Interner Verarbeitungsfehler | Technical | Error | Konnektor neu starten |
| 46624 | [Force automatic CRL download] : unable to read trust store | Interner Verarbeitungsfehler | Technical | Error | Konnektor neu starten |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 46625 | [Force automatic CRL download] : generic error | Interner Verarbeitungsfehler | Technical | Error | Im Protokoll des Konnektors wird diese Fehlermeldung angezeigt, sofern ein Problem mit der eingespielten TSL vorliegt. Dieser Fehler ist eine Folgefehler von 46552 parseTSL: TSL not readable (I/O error). |
| 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 werden. | Technical | Error | Konnektor neu starten |
| 46628 | [Force automatic CRL download] : unable to ASN.1 parse the CRL | CRL konnte nicht dekodiert werden (ASN.1) | Technical | Error | Konnektor neu starten |
| 46629 | [Force automatic CRL download] : downloaded CRL is not valid anymore | Die heruntergeladene 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 46631 | [Force automatic CRL download] : CRL signer not found - unable to verify digital signature of CRL | Es konnte kein gültiger CRL Signer in der aktuellen TSL gefunden werden. | Technical | Error | TSL aktualisieren |
| 46632 | [Force automatic CRL download] : CRL signer found but expired - unable to verify digital signature of CRL | CRL Signer ist ungültig. Die SIgnatur der CRL konnte nicht verifiziert werden. | Technical | Error | TSL aktualisieren |
| 46633 | [Force automatic CRL download] : unknown error code reported. Please contact software vendor | Interner Verarbeitungsfehler | Technical | Error | Konnektor neu starten |
| 46634 | Resolving CRL server name failed | CRL-Hostname konnte nicht aufgelöst werden. | Technical | Error | |
| 47500 | Refusing update package | Das Update-Paket konnte nicht validiert werden (z.B. inkorrekte digitale Signatur) | Technical | Error | Support kontaktieren |
| 47501 | Unable to switch to update | Der aktuelle Konnektor-Laufzeitzustand verhindert, dass zum Updater gewechselt wird. | Technical | Error | Konnektor neu starten |

| 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 |
| 47701 | I/O error: unable to read or write a file | Der Zugriff auf den Hintergrundspeicher ist fehlgeschlagen. | Technical | Error | Konnektor neu starten |
| 47704 | I/O error: unable to resolve IP of network interface '%s' | Der Platzhalter '%s' kann entweder (eth0=WAN) oder (eth1=LAN) sein: Die IP-Adresse des Interfaces ist nicht abrufbar (dies ist z.B. möglich, wenn der Adapter aktuell "down" ist, weil eine DHCP-Rekonfiguration stattfindet). | Technical | Error | Konnektor neu starten |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 es befindet sich keine TSL auf dem Konnektor. | Technical | Error | In der MGMT-UI eine neue TSL einbringen; bei wiederholtem Fehler: TI und/oder Support kontaktieren |
| 47711 | I/O error: TSL lacks DNSSEC trust-anchor element | In der TSL muss der DNSSEC-Trust-Anchor der TI-Zone verzeichnet sein. Dieses Element fehlt. | Technical | Error | In der MGMT-UI eine neue TSL einbringen; bei wiederholtem Fehler: TI und/oder Support kontaktieren |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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. |
| 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. |
| 47733 | I/O error: trust anchor key digest lacks key tag element | Eingabedaten (Trust Anchor/TSL) sind fehlerhaft. | Technical | Error | Konfiguration prüfen |
| 47734 | I/O error: trust anchor key digest lacks algorithm element | Eingabedaten (Trust Anchor/TSL) sind fehlerhaft. | Technical | Error | Konfiguration prüfen |
| 47735 | I/O error: trust anchor key digest lacks digest type element | Eingabedaten (Trust Anchor/TSL) sind fehlerhaft. | Technical | Error | Konfiguration prüfen |
| 47736 | I/O error: trust anchor key digest lacks digest element | Eingabedaten (Trust Anchor/TSL) sind fehlerhaft. | Technical | Error | Konfiguration prüfen |
| 47740 | I/O error: data-structure lacks element '%s' | Eingabedaten sind fehlerhaft. | Technical | Error | Konfiguration prüfen |
| 47750 | insufficient memory | Arbeitsspeicher erschöpft | Technical | Error | Konnektor neu starten |
| 47800 | failed to configure DNS (phase %) | DNS Server startet nicht | Technical | Error | Konnektor neu starten |
| 47801 | failed to configure or fetching DNS trusted keys | TI DNS Server wird nicht erreicht | Technical | Error | Operation wiederholen |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 |
| 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 |
| 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 wiederholen |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 |
| 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 for-mat | 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. wiederherstellen und Operation wiederholen |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 48124 | CRITICALTIMEDEVIATION: local clock offset to NTP reference clock exceeds limit | Zeitabweichung von mehr als einer Stunde entdeckt und Übergang in den kritischen Betriebszustand | Technical | Fatal | Zeitsynchronisation durchführen oder Zeit einstellen |
| 48200 | error locking RTC | Programmfehler oder RTC aktuell in Verwendung | Technical | Error | Operation wiederholen |
| 48201 | error reading RTC: %s | Programmfehler oder Hardware Schaden (vermutlich RTC) | Technical | Error | Operation wiederholen |
| 48202 | error setting RTC | Programmfehler oder Hardware Schaden (vermutlich RTC) | Technical | Error | Operation wiederholen |
| 48203 | error reading system time: %s | Programmfehler | Technical | Error | Operation wiederholen |
| 48204 | error setting system time: %s | Programmfehler | Technical | Error | Operation wiederholen |
| 48205 | error converting local to UTC time: %s | Programmfehler | Technical | Error | Operation wiederholen |
| 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 48209 | error reading system time: %s, exiting | Programmfehler | Technical | Error | Operation wiederholen |
| 48300 | current system is unknown | Programmfehler | Technical | Fatal | Wenn nicht durch Neustart zu lösen, Konnektor einschicken |
| 48301 | activating LVM volume group konnektor failed (rc=%d) | Programmfehler oder Hardware Schaden (vermutlich SSD) | Technical | Fatal | Wenn nicht durch Neustart zu lösen, Konnektor einschicken |
| 48302 | deactivating LVM logical volume %s failed (rc=%d) | LVM Volume Group ist bei der Deaktivierung noch in Verwendung | Technical | Error | keine Aktion |
| 48303 | mapping CFS failed (rc=%d) | Programmfehler oder Hardware Schaden (vermutlich SSD oder gSMC-K) | Technical | Fatal | Wenn nicht durch Neustart zu lösen, Konnektor einschicken |
| 48304 | unmapping CFS failed (rc=%d) | Verschlüsseltes Dateisystem ist beim Aushängen noch in Verwendung | Technical | Error | keine Aktion |
| 48305 | mounting %s to %s failed: %s | Programmfehler oder Hardware Schaden (vermutlich SSD) | Technical | Fatal | Wenn nicht durch Neustart zu lösen, Konnektor einschicken |
| 48306 | mounting CFS %s to %s failed: %s | Programmfehler oder Hardware Schaden (vermutlich SSD) | Technical | Fatal | Wenn nicht durch Neustart zu lösen, Konnektor einschicken |
| 48307 | bind mount %s to %s failed: %s | Programmfehler oder Hardware Schaden (vermutlich SSD) | Technical | Fatal | Wenn nicht durch Neustart zu lösen, Konnektor einschicken |

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

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

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 48505 | Update-package exceeding disc-space | Speicherplatz für Zwischenablage Update nicht ausreichend | Technical | Error | Softwareaktualisierung erneut ausführen |
| 48506 | Uploaded firmware does not correspond to intended version | Firmwareversion des Updates stimmt nicht mit dem übergebenen Wert überein | Technical | Error | Support kontaktieren |
| 48507 | Uploaded firmware not listed in latest firmware-group-info | Firmware-Gruppen-Information des Updates ist kleiner als die im Konfigurationsbereich gespeicherte 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 |
| 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 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 erschöpf, 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 |

| Code | Beschreibung | Mögliche Ursache | Typ | Level | Fehlerbehebung/ Weitere Angaben |
|---|---|---|---|---|---|
| 49816 | reading WAN IP address failed: %s | Programmfehler oder Netzwerk Problem | Technical | Error | WAN-Verbindung prüfen, ggf. herstellen und Operation wiederholen |
| 49817 | reading WAN MAC address failed: %s | Programmfehler oder Hardware Schaden (vermutlich WAN Interface) | Technical | Error | Operation wiederholen |
| 49818 | error parsing xml configuration file %s | Fehlkonfiguration | Technical | Error | Konfiguration prüfen, korrigieren und Operation wiederholen |
| 49819 | parameter %s could not be read from configuration (rc=%d) | Fehlkonfiguration | Technical | Error | Konfiguration prüfen, korrigieren und Operation wiederholen |
| 49820 | error running command %s: %s | Programmfehler | Technical | Error | Operation wiederholen |
| 49821 | finished with error (rc=%d) | Programmfehler | Technical | Error | Operation wiederholen |
| 49822 | unexpected argument | Programmfehler | Technical | Error | Operation wiederholen |
| 49823 | error running command %s (rc=%d) | Programmfehler | Technical | Error | Operation wiederholen |
| 49824 | unable to rename file %s to %s: %s | Programmfehler oder Hardware Schaden (vermutlich SSD) | Technical | Error | Operation wiederholen |

## 12.5 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 7.1)

- 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 6.4.5)

- Verschlüsselungsdienst

  Bietet Funktionen zur Ver- und Entschlüsseln von Dokumenten an (siehe Kapitel 2.3.7)

- Signaturdienst

  Bietet Funktionen zum Signieren von Dokumenten und zum Prüfen von Dokumentensignaturen (siehe Kapitel 2.3.6)

- Zertifikatsdienst

  Bietet Funktionen zur Überprüfung der Gültigkeit von Zertifikaten

- Authentifizierungsdienst

  Bietet Funktionen für die externe Authentisierung (siehe Kapitel 2.3.8)

- Fachmodul VSDM

  Bietet Funktionen für die Bereitstellung und Pflege der VSD (siehe Kapitel 6.7.1)

- Fachmodul NDFM

  Ermöglicht es dem PS, über den Highspeedkonnektor 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

- Fachmodul ePA

  Ermöglicht Clientsystemen die Verwaltung von medizinische Dokumenten von Versicherten durch das ePA-Aktensystem der TI.

- LDAP-Proxy

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

## 12.6 Übersicht der Fehlerzustände

**Hinweis zur Spalte ErrorCondition**: Jeder Fehlerzustand wird durch einen eindeutigen „ErrorCondition“ identifiziert. Dieser kann einen Parameter enthalten. Sind etwa die Kartenterminals mit ctId=47 und das mit ctId=93 nicht erreichbar, so lauten die ErrorCondition:

- EC_CardTerminal_Not_Available(47)

  und

- EC_CardTerminal_Not_Available(93)

**Hinweis zur Spalte Parameterlist**: „EC.description“ referenziert den Text, der in der Spalte „Beschreibung“ des Zustandes spezifiziert wurde.

| ErrorCondition | Beschreibung | Type | Severity | max. Feststellungszeit | Parameterlist |
|---|---|---|---|---|---|
| EC_CardTerminal_ Software_Out_Of_ Date ($ctId) | Software auf Kartenterminal ($ctId) ist nicht aktuell | Op | Info | 1 Tag | CtID=$ctId; Bedeutung= $EC.description |
| EC_CardTerminal_ gSMCKT_Certificate_ Expires_Soon ($ctId) | Das Zertifikat der gSMC-KT im Kartenterminal($ctId) läuft in weniger als 5 Wochen ab | Op | Info | 7 Tage | CtID=$ctId; Bedeutung= $EC.description |
| EC_Connector_ Software_Out_ Of_Date | I_KSRS_Download::list_ Updates liefert mindestens eine Upda-teInformation mit einer Upda-teInformation/Firmware/ FWVersion > aktuelle Version der Konnektorsoftware, deren Up-dateInformation/Firmware/ FWPriority = „Kritisch“ | Op | Info | 1 Tag | Bedeutung= $EC.description |

| | | | | | |
|---|---|---|---|---|---|
| EC_FW_Update_Available | I_KSRS_Download::list_ Updates liefert mindestens eine UpdateInformation mit einer UpdateInformation/Firmware/FWVersion > aktuelle Version der Konnektor- oder Kartenterminalsoftware | Op | Info | 1 Tag | Bedeutung= $EC.description |
| EC_FW_Not_Valid_Status_Blocked | Konnektor Firmware muss aktualisiert werden. Zugang zur TI momentan nicht erlaubt. | Sec | Fatal | 1 Tag | Bedeutung= $EC.description |
| EC_Time_Sync_Not_Successful | der letzte Synchronisationsversuch der Systemzeit war nicht erfolgreich. | Op | Info | 1 Sek | LastSyncAttempt= $lastSyncAttempt Timestamp; LastSyncSuccess =$lastSyncSuccess Timestamp; Bedeutung= $EC.description |
| EC_TSL_Update_Not_Successful | das letzte Update der TSL war nicht erfolgreich. | Op | Info | 1 Sek | Bedeutung= $EC.description; LastUpdateTSL= $lastUpdateTSL Timestamp |
| EC_TSL_Expiring | Systemzeit t mit t > NextUpdate-Element der TSL – 7 Tage und t <= NextUpdate-Element der TSL | Sec | Info | 1 Tag | NextUpdateTSL =$NextUpdate-Element der TSL; Bedeutung= $EC.description |
| EC_BNetzA_VL_Update_Not_Successful | Das letzte Update der BNetzA-VL war nicht erfolgreich | Op | Info | 1 Sek | LastUpdateBNetz AVL= $lastUpdateBNetz AVLTimestamp; Bedeutung= $EC.description |

| | | | | | |
|---|---|---|---|---|---|
| EC_ BNetzA_VL_ not_valid | Systemzeit t mit t > NextUpdate-Element der BNetzA-VL | Sec | Warning | 1 Tag | NextUpdateBNetzAVL =$NextUpdate-Element der BNetzA-VL; Bedeutung= $EC.description |
| EC_TSL_Trust_ Anchor_Expiring | Gültigkeit des Vertrauensankers ist noch nicht abgelaufen, läuft aber innerhalb von 30 Tagen ab. | Sec | Info | 1 Tag | ExpiringDateTrustAnchor= Ablaufdatum der Vertrauensanker gültigkeit; Bedeutung= $EC.description |
| EC_LOG_ OVERFLOW | Wenn im Rahmen der Regeln für die rollierende Speicherung von Logging-Einträgen Einträge gelöscht werden, die nicht älter als SECURITY_LOG_DAYS, LOG_DAYS bzw. FM_ <fmName>_LOG_DAYS sind, tritt der Fehlerzustand ein. Der Fehlerzustand kann nur durch einen Administrator wieder zurückgesetzt werden. Unter Protokoll wird die Liste der auslösenden Protokolle angegeben. | Op | Warning | 1 Sek | Protokoll=$Protokoll; Bedeutung= $EC.description |
| EC_CRL_Expiring | Systemzeit t > NextUpdate der CRL – 3 Tage | Sec | Warning | 1 Tag | ExpiringDateCRL= NextUpdate der CRL; Bedeutung= $EC.description |

| | | | | | |
|---|---|---|---|---|---|
| EC_Time_Sync_ Pending_Warning | MGM_LU_ONLINE=Enabled und keine erfolgreiche Synchronisation der Systemzeit seit d Tagen und d > NTP_WARN_PERIOD und d <= NTP_GRACE_PERIOD. Nach einer Korrektur oder Bestätigung der Systemzeit durch einen Administrator muss der Konnektor wie nach einer erfolgreichen Zeitsynchronisation verfahren, d.h., der Tagezähler wird auf 0 zurückgesetzt. | Sec | Warning | 1 Tag | LastSyncSuccess= $lastSyncSuccess Timestamp; Bedeutung= $EC.description |
| EC_TSL_Out_ Of_Date_Within_ Grace_Period | Systemzeit t mit t > NextUpdate-Element der TSL und t <= NextUpdate-Element der TSL + CERT_TSL_ DEFAULT_GRACE_ PERIOD_DAYS und eine neue TSL ist nicht verfügbar | Sec | Warning | 1 Tag | NextUpdateTSL =$NextUpdate-Element der TSL; GracePeriodTSL =CERT_TSL_ DEFAULT_ GRACE_PERIOD_ DAYS; Bedeutung= $EC.description |
| EC_CardTerminal_ Not_Available ($ctId) | Kartenterminal($ctId) ist nicht verfügbar. Dieser Betriebszustand bezieht sich auf die als „aktiv“ gekennzeichneten KTs. | Op | Error | 1 Sek | CtID=$ctId; Bedeutung= $EC.description |
| EC_No_VPN_TI_ Connection | Kein sicherer Kanal (VPN) in die Telematikinfrastruktur aufgebaut.<br>Der Wert 300 sec ist abgeleitet aus der maximalen Verbindungsaufbauzeit bei einem Standortausfall des VPN-Zugangsdienstes. | Op | Error | 300 Sek | Bedeutung= $EC.description |

| | | | | | |
|---|---|---|---|---|---|
| EC_No_VPN_ SIS_Connection | Kein sicherer Kanal (VPN) zu den Sicheren Internet Services aufgebaut. Der Wert 300 sec ist abgeleitet aus der maximalen Verbindungsaufbauzeit bei einem Standortausfall des VPN-Zugangsdienstes. | Op | Error | 300 Sek | Bedeutung= $EC.description |
| EC_No_Online_ Connection | Konnektor kann Dienste im Transportnetz nicht erreichen. | Op | Error | 10 Sek | Bedeutung= $EC.description |
| EC_IP_Adresses_ Not_Available | Die IP-Adressen des Netzkonnektors sind nicht oder falsch gesetzt. | Sec | Error | 1 Sek | Bedeutung= $EC.description |
| EC_CRL_Out_Of_ Date | Systemzeit t > Next Update der CRL | Sec | Fata l | 1 Tag | NextUpdateCRL= $NextUpdate der CRL; Bedeutung= $EC.description |
| EC_Firewall_Not_ Reliable | Firewall-Regeln konnten nicht fehlerfrei generiert werden oder beim Laden der Firewall-Regeln ist ein Fehler aufgetreten. | Sec | Fatal | 1 Sek | Bedeutung= $EC.description |
| EC_Random_ Generator_ Not_Reliable | Der Zufallszahlengenerator kann die Anforderungen an die zu erzeugende Entropie nicht erfüllen. | Sec | Fatal | 1 Sek | Bedeutung= $EC.description |
| EC_Secure_ KeyStore_ Not_Available | Sicherer Zertifikats- und Schlüsselspeicher des Konnektors (gSMC-K oder Truststore) nicht verfügbar | Sec | Fatal | 1 Sek | Bedeutung= $EC.description |

| | | | | | |
|---|---|---|---|---|---|
| EC_Security_ Log_ Not_Writable | Das Sicherheitslog kann nicht geschrieben werden. | Op | Fatal | 1 Sek | Bedeutung= $EC.description |
| EC_Software_ Integrity_ Check_Failed | Eine oder mehrere konnektorinterne Integritätsprüfungen der aktiven Konnektorbestandteile sind fehlgeschlagen. | Sec | Fatal | 1 Tag | Bedeutung= $EC.description |
| EC_Time_ Difference_ Intolerable | Abweichung zwischen der lokalen Zeit und der per NTP empfangenen Zeit bei der Zeitsynchronisation größer als NTP_MAX_ TIMEDIFFERENCE. Nach einer Korrektur oder Bestätigung der Systemzeit durch einen Administrator muss der Konnektor den Fehlerzustand zurücksetzen. | Sec | Fatal | 1 Sek | NtpTimedifference= Zeitabweichung; NtpMaxAllowed Timedifference =NTP_MAX_ TIMEDIFFERENCE; Bedeutung= $EC.description |
| EC_Time_Sync_ Pending_Critical | MGM_LU_ONLINE= Enabled und keine erfolgreiche Synchronisation der Systemzeit seit d Tagen und d > NTP_GRACE_PERIOD Nach einer Korrektur oder Bestätigung der Systemzeit durch einen Administrator muss der Konnektor wie nach einer erfolgreichen Zeitsynchronisation verfahren, d.h., der Tagezähler wird auf 0 zurückgesetzt. | Sec | Fatal | 1 Tag | LastSyncSuccess =$lastSync Success-Timestamp; NtpGracePeriod= NTP_GRACE_ PERIOD; Bedeutung= $EC.description |

| | | | | | |
|---|---|---|---|---|---|
| EC_TSL_Trust_ Anchor_ Out_Of_Date | Gültigkeit des Vertrauens-ankers ist abgelaufen | Sec | Fatal | 1 Tag | ExpiringDateTrust Anchor= Ablauf-datum der Ver-trauensanker gültigkeit; Bedeu-tung= $EC.description |
| EC_TSL_Out_ Of_Date_ Be-yond_Grace_ Pe-riod | Systemzeit t mit t > NextUpdate-Element der TSL + CERT_TSL_DEFAULT_ GRACE_ PERIOD_DAYS und eine neue TSL ist nicht verfügbar | Sec | Fatal | 1 Tag | NextUpdateTSL =$NextUpdate-Element der TSL; GracePeriodTSL =CERT_TSL_ DEFAULT_ GRACE_PERIOD_ DAYS; Bedeutung= $EC.description |
| EC_ CRYPTOP ERATION_ ALARM | Gemäß TIP1-A_4597 wurde ein potentieller Missbrauch einer Kryptooperation erkannt. Nur der Administrator kann die Alarmmeldung zurücksetzen. | Sec | Warning | 1 Min | Operation= $Operationsname; Count=$Summenwe rt; Arbeitsplatz= $<Liste operations-aufrufend en workplaceIDs>; Meldung= 'Auffälli-ge Häufung von Operationsaufrufen in den letzten 10 Minuten' |
| EC_OTHER_ERROR_ STATE(1) | Die herstellerspezifischen Selbsttests des Konnektors sind fehlgeschlagen. | Op | Info | <= 1 Tag | |
| EC_OTHER_ERROR_ STATE(2) | Diese Meldung wird an der SOAP-Schnittstelle ausgegeben, um zu signalisieren, dass der Neustart des Konnektors notwendig ist. | Op | Info | <= 1 Tag | |

## 12.7 Die Notation von IP-Adressen

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

Eine CIDR-Adressangabe besteht aus zwei Teilen:

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

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

Beispiele für IP-Adressen:

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

## 12.8 Lizenzinformationen

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

Informationen zu Lizenzen der jeweiligen Version des Highspeedkonnektors finden Sie auf der folgenden Webseite von secunet:

https://www.secunet.com/highspeedkonnektor

Die Informationen zu den Lizenzen sind Bestandteil des Offline Updates.

## 12.9 Versionsprüfung von Fachmodule

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

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

Fachmodule sind ein Bestandteil der Konnektorsoftware und können nur durch ein Update des Highspeedkonnektors aktualisiert werden. Für einen von der gematik zugelassenen oder für den Betrieb in der TI genehmigten Highspeedkonnektor (siehe Kapitel 1.1 Prüfung der Zulassung) können Sie die Versionen der darin enthaltenen Fachmodule den Versionshinweisen auf Seite 15 entnehmen. Vergleichen Sie die dort für jedes Fachmodul angegebene Version mit der Version des Fachmoduls, dass über die Bedienoberfläche angezeigt wird. Für einen von der gematik zugelassenen Highspeedkonnektor können Sie die Versionen der Fachmodule bei Bedarf auch dem Security Target des Highspeedkonnektors entnehmen, dass Sie auf den Webseiten des BSI unter https://www.bsi.bund.de finden.

## 12.10 Security Guidance Fachmodul NFDM

### 12.10.1 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 abgelaufenem Zertifikat darf nicht verwendet werden.
- Das Fachmodul darf nur auf einem nach PP-0098 zertifizierten Konnektor[1] 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.

### 12.10.2 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:

- **Protokollierungslevel**

  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

[1] Dies umfasst ebenso Konnektoren mit einer durch die gematik nach dem Minor Release Verfahren (gemäß Anhang C aus [gemZUL_Prod_Kon]) zugelassenen Firmware.

- Error
- Fatal

- **Vorhaltedauer**

  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.

### 12.10.3 Versionsprüfung

Beachten Sie die Hinweise in Kapitel 12.9.

## 12.11 Security Guidance Fachmodul AMTS

### 12.11.1 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 abgelaufenem Zertifikat darf nicht verwendet werden.
- Das Fachmodul darf nur auf einem nach PP-0098 zertifizierten Konnektor[2] 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.

### 12.11.2 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:

- **Protokollierungslevel**

  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

[2] Dies umfasst ebenso Konnektoren mit einer durch die gematik nach dem Minor Release Verfahren (gemäß Anhang C aus [gemZUL_Prod_Kon]) zugelassenen Firmware.

- Error
- Fatal

- **Vorhaltedauer**

  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.

### 12.11.3 Versionsprüfung

Beachten Sie die Hinweise in Kapitel 12.9.

## 12.12 Security Guidance Fachmodul ePA

### 12.12.1 Anwendungshinweise

Bei der Nutzung des Fachmoduls müssen folgende Hinweise beachtet werden:

- Das Fachmodul darf nur auf einem nach PP-0098 zertifizierten Konnektor[3] in einer sicheren Umgebung genutzt werden. Die in diesem Handbuch beschriebenen Maßnahmen müssen beachtetwerden.
- Diese Maßnahmen stellen sicher, dass nur spezifikationsgemäße Zugriffe auf die Dienstschnittstellen des Fachmodulserfolgen.

### 12.12.2 Konfiguration des Fachmoduls

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

Die zu konfigurierenden Parameter befinden sich im Menü **Diagnose** → **Administration** → **Einstellungen** unter dem Eintrag **ePA** und im Menü **Module** → **Fachmodul ePA** → **Einstellungen**.

### 12.12.3 Logging und Protokollierung

Folgende Parameter können konfiguriert werden:

- **Protokollierungslevel**

  Dieser Parameter legt den Mindestschweregrad der zu protokollierenden Ereignisse fest.

  Mögliche Werte:

  - Debug,
  - Info,
  - Warning,
  - Error,
  - Fatal

  **Debug** ist dabei der niedrigste Level; **Fatal** der höchste Level.

[3] Dies umfasst ebenso Konnektoren mit einer durch die gematik nach dem Minor Release Verfahren (gemäß Anhang C aus [gemZUL_Prod_Kon]) zugelassenen Firmware.

Default-Wert: Warning

- **Vorhaltedauer**

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

  Wertebereich: Zwischen 10 - 365

  Default-Wert: 180

- **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.

  Mögliche Werte:

  - true
  - false

  Default-Wert: false

  Das Leeren des Performance-Protokolls (ePA) kann im Menü **Diagnose** → **Administration** angestoßen werden.

- **TLS Timeout**

  Der Parameter legt die Anzahl Sekunden fest, die der Highspeedkonnektor auf den TLS- Verbindungsaufbau zum Aktensystem wartet (Handshake-Timeout).

  Default-Wert: 10

  Wertebereich: 5 – 30

- **Anzahl Keep-Alive Versuche**

  Der Parameter legt die Anzahl aufeinander folgenden, nicht beantworteten Keep-Alive- Nachrichten, fest nach denen ein Timeout der TLS-Verbindung festgestellt wird.

  Default-Wert: 10

  Wertebereich: 5 – 30

- **Server Timeout**

  Der Parameter legt die Anzahl Sekunden fest, die der Highspeedkonnektor maximal auf den TCP- Verbindungsaufbau zum Aktensystem/SGD wartet.

  Default-Wert: 10

  Wertebereich: 5 - 30

- **Standart-Aufrufkontext**

Der Parameter legt den Aufrufkontext fest der bei für die Nutzung des Webservices PHRService verwendet werden soll, wenn kein Aufrufkontext übergeben wird.

- **Timeout bei Inaktivität**

  Der Parameter legt die maximale Zeitdauer für Inaktivität bei Nutzung einer Aktensesseion fest.

  Default-Wert: 20

  Wertebereich: 0 - 20

- **Timeout für eine VAU-Anfrage**

  Der Parameter legt die Anzahl Sekunden fest, die der Konnektor maximal auf die Antwort für einen VAU-Anfrage wartet.

  Default-Wert: 120

  Wertebereich: 5 – 1800

### 12.12.4 Versionsprüfung

Beachten Sie die Hinweise in Kapitel 12.9.

## 12.13 Dokumentensicherheit

### 12.13.1 Einleitung

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

Mit der Signaturdirektive (siehe Kapitel 12.14) 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.

### 12.13.2 Allgemein

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

### 12.13.3 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/external-general-entities", false);
documentBuilderFactory.setFeature("http://xml.org/sax/features/external-parameter-entities", false);
```

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

Die SchemaFactory ist wie folgt konfiguriert:

```
schemaFactory.setAttribute(XMLConstants.ACCESS_EXTERNAL_DTD, "");
schemaFactory.setAttribute(XMLConstants.ACCESS_EXTERNAL_STYLESHEET, "");
```

Der Konnektor 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_PROCESSING, 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 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 werden abgelehnt.
- Dokumente mit XSLT-Transformationen werden abgelehnt.
- 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
- Ein Element darf nicht mehr als 20 Attribute haben.
- Namen von Elementen und Attrubten dürfen nicht länger als 200 Zeichen sein.
- Es dürfen maximal 64 Transforms verwendet werden.
- Ein Reference Element darf maximal 10 Transforms enthalten.

Wird eine dieser Grenzen vom XML-Dokument überschritten, dann wird die Operation mit Fehlercode 4280 (Dimensionierung des Dokuments nicht unterstützt) 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.

### 12.13.4 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.

### 12.13.5 CAdES

Es werden zurzeit keine besonderen Härtungsmaßnahmen für CAdES umgesetzt.

## 12.14 Signaturdirektive

### 12.14.1 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-Signaturen 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 12.13 beschrieben.

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

### 12.14.2 Signaturdirektive SignDocument

#### 12.14.2.1 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 8: 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 8: 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<br>PDF/A<br>Text (text/pain)<br>TIFF (image/tiff)<br>Binär (nur bei nonQES) |
| S/MIME | MIME-Nachricht (nur bei nonQES) mit allen für CAdES zugelassenen Dokumentenformaten |

Tabelle 9: 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/ SignedProperties/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:<br>■ ContentType<br>■ SigningTime<br>■ MessageDigest<br>■ SigningCertificate<br>■ SigningCertificateV2<br>■ CMSAlgorithmprotection |

### 12.14.2.2 Signaturvarianten

Folgende Signaturvarianten sind zulässig:

| Signaturvarianten | | | | Einsatzbereich | | |
|---|---|---|---|---|---|---|
| Signatur-verfahren | Signatur-variante | WAS wird signiert? | WO wird die Signatur abgelegt? | nonQES | QES Außenschnitt stelle | 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 Dokumentes in der SignResponse | Ja | Ja | Ja |
| CAdES | enveloping | gesamtes Binärdokument | innerhalb des CMS- Dokumentes | Ja | Ja | Ja |
| PAdES | - | Gesamtes PDF-Dokument | Im PDF-Dokument | Ja | Ja | Ja |

Tabelle 10: 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 Dokumentes in der SignResponse | Ja |
| CAdES | enveloping | gesamtes Binärdokument | innerhalb des CMS- Dokumentes | Ja |
| PAdES | - | gesamtes PDF-Dokument | Im PDF-Dokument | Ja |

Tabelle 11: Signaturvarianten nonQES

### Signaturvarianten QES

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

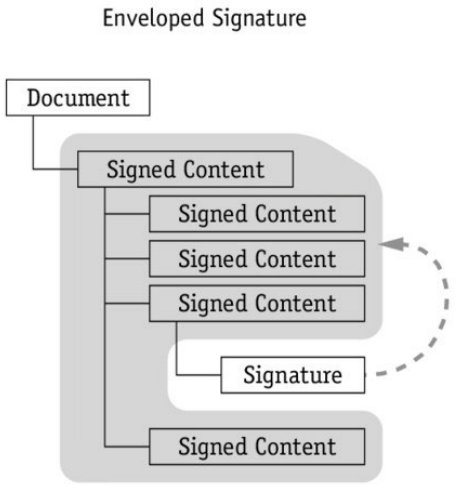
| Signaturvarianten QES | | | | Einsatzbereich |
|---|---|---|---|---|
| Signatur-verfah- | Signatur-variante | WAS wird signiert? | WO wird die Signatur abge-legt? | QES |
| XAdES | detached | Ausgewähltes nicht Root- Element mit Subelementen im Input XMLDokument | Innerhalb des Dokumentes, aber außerhalb des signier-ten Subbaums | Ja (NFDM) |
| CAdES | detached | gesamtes Binärdokument | Außerhalb des Dokumentes in der SignResponse | Ja |
| CAdES | enveloping | gesamtes Binärdokument | innerhalb des CMS-Dokumentes | Ja |
| PAdES | - | gesamtes PDF-Dokument | Im PDF-Dokument | Ja |

Tabelle 12: 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.

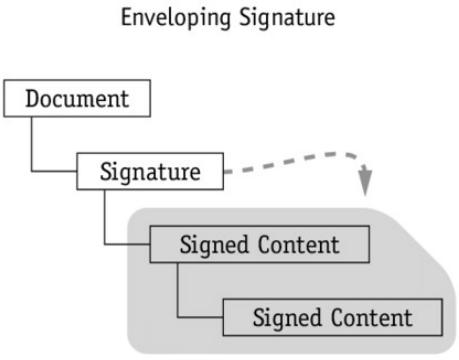



Im Highspeedkonnektor wird diese Signaturvariante nicht erlaubt.

### 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 Highspeedkonnektor erlaubte Signaturvarianten sind:

| Signatur- ver-fahren | Signatur-variante | Signaturinput | Signaturausgabe | Einsatzbereich |
|---|---|---|---|---|
| CAdES | enveloping | gesamtes Binärdokument | innerhalb des CMS- Dokumentes | 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

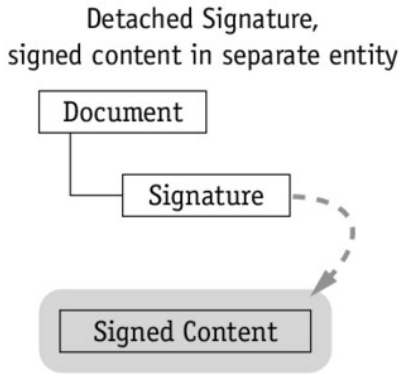
| XML-Element oder –Attribut (XPath): | Beschreibung: | Werte: |
|---|---|---|
| /SIG:SignDocument/SIG:SignRequest/ SIG:OptionalInputs/ dss:ReturnUpdatedSignature | Durch dieses in [OASIS-DSS] (Abschnitt 4.5.8) definierte Element kann eine übergegebene XML- oder CMS-Signatur mit zusätzlichen Informationen und Signaturen (Parallel- und Gegensignaturen) versehen | http://ws.gematik.de/conn/sig/sigupdate/parallel<br>oder<br>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-verfah- | Signatur-variante | Signaturinput | Signaturausgabe | Einsatzbereich |
|---|---|---|---|---|
| CAdES | detached | gesamtes Binärdoku-ment | Außerhalb des Doku-ments in der SignRespon-se | 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 anfordern. Es wird ausschließ-lich die zu erstellende Signatur betrachtet, d.h. es erfolgt kei-ne Einbettung von Sperrinfor-mationen für bereits enthaltene Signaturen. | QES: false oder true nonQES: false |

### Parallel- und Gegensignaturen

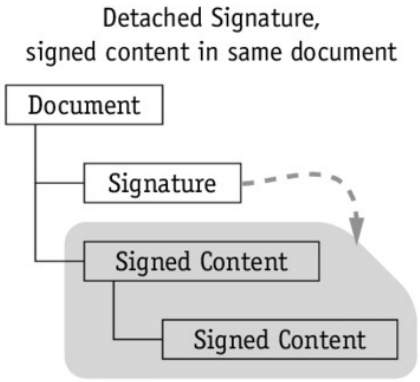
Parallel- und Gegensignaturen werden für CMS Detached Signaturen nicht unterstützt.

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-verfah- | 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/XPathFirstChildOf | Identifies an ele-ment, in the XML input document, which the signa-ture will be insert-ed as the first child of. The signature is placed immedi-ately after the start tag of the specified element. | ”/*[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.<br>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- Dokumentes | 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.

### 12.14.3 Signaturdirektive 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 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<br>nonQES: false<br>PDF: false |

## 12.15 Verschlüsselungsdirektive

### 12.15.1 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 12.14) der Begriff „Verschlüsselungsrichtlinie“ im Rahmen der Konnektorevaluierung unterschiedlich verwendet:

8. Verschlüsselungsrichtlinie als im Operationsaufruf angegebene Richtlinie für genau diese Dokumenten-Verschlüsselung.
9. 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 12.13 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.

### 12.15.2 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 Verschlüsselungsverfahren der zu verschlüsselnden Dokumente spezifiziert werden. | Siehe Tabelle 13 |

| Verschlüsselungsverfahren | Wert |
|---|---|
| XMLEnc | http://www.w3.org/TR/xmlenc-core/ |
| CMS | urn:ietf:rfc:5652 |
| S/MIME | urn:ietf:rfc:5751 |

Tabelle 13: 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<br>PDF/A<br>Text (text/plain)<br>TIFF (image/tiff)<br>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.

#### 12.15.2.1 Allgemein

Die Schnittstelle EncryptDocument wird entsprechend [gemSpec_Kon] (inkl. Aller relevanten Errata) umgesetzt. Darüber hinaus gibt es keine weiteren Einschränkungen.

#### 12.15.2.2 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:Certificate OnCard<br>oder<br>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.

#### 12.15.2.3 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.

### 12.15.3 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 12.15.2.1.

Im Folgenden wird auf einzelne Punkte der Schnittstelle eingegangen. Dabei handelt es sich nicht um Abweichungen zu [gemSpec_Kon], sondern um Klarstellungen zur Umsetzung.

#### 12.15.3.1 Allgemein

Die Schnittstelle EncryptDocument wird entsprechend [gemSpec_Kon] (inkl. Aller relevanten Errata) umgesetzt. Darüber hinaus gibt es keine weiteren Einschränkungen.

#### 12.15.3.2 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.<br>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 |

## 12.16 An den VPN-Zugangsdienst übermittelte Betriebsdaten

Entsprechend [gemSpec_Kon] werden Betriebsdaten an die Betriebsdatenerfassung der TI übermittelt. Die Betriebsdaten aller Konnektor-Instanzen werden zentral pro Highspeedkonnektor aggregiert und dann zusammen übertragen.

Übermittelte Betriebsdaten:

- **Product Information**

  Produkttypversion, Informationen über den Hersteller, Produktbezeichnung, Version des Konnektorprodukts (Hardware und Firmware).

- **Configuration**
  - **Client Connection Mode**

    Einstellungen, die sich auf die technische Anbindung der Primärsysteme beziehen:
    - Verschlüsselte Verbindung über Transport Layer Security (TLS)
    - Art der Authentisierung der Primärsysteme

- **Connector**

  Der Verbindungsstatus TI wird immer mit dem Wert Online und dem Bootzeitpunkt versendet. Der Verbindungsstatus SIS wird immer mit dem Wert Offline und dem Bootzeitpunkt versendet.

  Liste der Fehlerzustände des Konnektors.

- **Trust Status**

  Informationen über aktuelle Vertrauens- und Sperrlisten im Konnektor:
  - Trust Service Status List (TSL)
  - Vertrauensliste der Bundesnetzagentur (BNetzA-VL)

  Die Informationen umfassen Nummer der Liste, Gültigkeitsbeginn bzw. Erstellungsdatum und Zeitpunkt der nächsten Aktualisierung.

- **Connector Certificates**

  Ablaufdaten der Kartenzertifikate der gSMC-K.

  Stellvertretend für alle Zertifikate wird nur ein Zertifikat der gSMC-K übermittelt (gleicher Gültigkeitszeitraum aller Zertifikate einer gSMC-K).

- **Card Terminals**

Produktinformationen der angeschlossenen Kartenterminals (Produkttypversion, Informationen über den Hersteller, Produktbezeichnung, Version von Hardware und Firmware des KT-Produkts).

Ablaufdaten der Kartenzertifikate der gSMC-KT.

- **Operating Site**

  Die Instanz ermittelt die Betriebsstättenart über mit dem Konnektor eingesetzten SMC-Bs.

  Ddabei wird eine der folgenden Betriebsstättenarten ermittelt:

  - KRANKENHAUS
  - ARZTPRAXIS
  - ZAHNARZTPRAXIS
  - APOTHEKE
  - SONSTIGE

  Wenn mehrere SMC-Bs eingesetzt werden, werden die Betriebsstätte nach Priorisierung ausgewählt. Die obenstehende Liste der Betriebsstättenarten ist dabei mit absteigender Priorität sortiert.

# Referenzliste


| | |
|---|---|
| [gemProdT_Kon_ Highspeed] | gematik: Produkttypsteckbrief Konnektor - Prüfvorschrift, Produkttyp Version 1.3.0-0, Version 1.0.0 vom 10.07.2023 |
| [gemSpec_Kon] | gematik: Spezifikation Konnektor, Version gemäß [gemProdT_Kon_ Highspeed] |
| [gemRL_QES_NFDM] | gematik: Signaturrichtlinie QES Notfalldaten-Management (NFDM), Version gemäß [gemProdT_Kon_ Highspeed] |
| [gemSpec_Krypt] | gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version gemäß [gemProdT_Kon_ Highspeed] |
| [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 3.20, 21.09.2018, 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

# 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.<br>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. |
| 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.<br>Eine Fachanwendung zeichnet sich durch die Einhaltung der Vorgaben der Telematikinfrastruktur und die entsprechende Zulassung aus. |
| Anwendungskonnektor | Funktionaler Teil des Highspeedkonnektors, der anwendungsnahe Basisdienste und Fachmodule zur Nutzung durch Clientsysteme bietet. |
| Aufrufkontext | Eindeutige Kombination aus Clientsystem, Mandant und Arbeitsplatz (siehe Kapitel 6.3.6) |

## 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 Highspeedkonnektor (siehe Kapitel 6.1.3). |
| 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 Highspeedkonnektor durch eine Organisation betrieben wird, ist diese Organisation der Betreiber des Highspeedkonnektors. 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 Highspeedkonnektors. |
| BIOS | Basic input/output system; Software , die unmittelbar nach dem Einschalten des Geräts ausgeführt wird (Boot-Prozess). |
| BMP | Bundeseinheitlicher Medikationsplan (siehe Kapitel 108) |
| BNetzA | Bundesnetzagentur |
| 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 6.4.5) |
| 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 2.3.2). |

## D

| | |
|---|---|
| Deregistrierung | Die Rücknahme der Freischaltung des Highspeedkonnektors (siehe Kapitel 6.6.2.2). |
| DHCP | Dynamic Host Configuration Protocol, ein Kommunikationsprotokoll, das die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server ermöglicht. |
| 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

| | |
|---|---|
| ECC | Kryptografisches Verfahren basierend auf elliptischen Kurven (eng. Abk.: Elliptic Curve Cryptography) |
| eGK | Elektronische Gesundheitskarte; Versichertenkarte für gesetzlich Krankenversicherte, die als Chipkarte im Scheckkartenformat ausgeführt ist. |
| eMP | Elektronischer Medikationsplan |
| ePA | Elektronische Patientenakte |

## 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 die lokale Systeme vor unberechtigtem Zugriff aus anderen Netzwerken 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. |
| gSMC-K | Security Module Card Typ K; Internes Sicherheitsmodul, das die Identität des Highspeedkonnektors 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.<br>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. |
| 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 |
| 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 Highspeedkonnektor |
| 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.<br>Der Leistungserbringer gehört zu einem zugriffsberechtigten Personen- |

| | |
|---|---|
| | kreis 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 12.4). |

## N

| | |
|---|---|
| NFDM | Notfalldatenmanagemen |
| NTP | Network Time Protocol; Standard zur Synchronisierung von Uhren in Computersystemen. Der Highspeedkonnektor 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 2.4.1). |

## O

| | |
|---|---|
| OCSP | Online Certificate Status Protocol, Netzwerkprotokoll, mit dem der Highspeedkonnektor den Status von Zertifikaten beim Validierungsdienst der TI abfragt (siehe Kapitel 2.3.2). |

## P

| | |
|---|---|
| Pairing | Prozess der logischen Verknüpfung des Highspeedkonnektors 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 Highspeedkonnektor (siehe Kapitel 12.4). |
| 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 Highspeedkonnektors (siehe Kapitel 6.6.2.1). |
| Remote Management | Betriebsmodus des Highspeedkonnektors, in dem die Administrierung von einem entfernten System aus erfolgt. |
| Remote-PIN | Funktion, die es ermöglicht, für eine SMC-B, die in einem Kartenterminal steckt, an einem anderen Kartenterminal eine PIN einzugeben (siehe Kapitel 6.3.5). |
| REST | Representational State Transfer; Konzept für die Kommunikation zwischen Clientsystemen und Servern. Die REST-Schnittstelle des Highspeedkonnektors ermöglicht die kommandozeilenbasierte Administrierung. |
| 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.<br>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. |
| SGD | Schlüsselgenerierungsdienst |
| SICCT | Secure Interoperable Chip Card Terminal; Spezifikation des Kommunikationsstandards für die TI |
| SMC-B | Security Module Card Typ B; Praxisausweis (siehe Berechtigtenkarte) |
| SSL | Secure Socket Layer; Netzwerkprotokoll für die sichere Übertragung von Daten. |

## 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 2.3.2). |

## 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

| | |
|---|---|
| VAU | Vertrauenswürdige Ausführungsumgebung, in der für Anfragen an das ePA-Aktensystem auf die Metadaten von Dokumenten zugegriffen wird. |
| 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. |
| 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

| | |
|---|---|
| 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 8.7.2). |
| Werksreset, vollständiger | Der vollständige Werksreset setzt alle Parameter mit Ausnahme der aktuellen Firmware und Meldungen des Typs SECURITY in den Auslieferungszustand zurück (siehe Kapitel 8.7.1). |

## 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. |