



Administratorhandbuch

KoCoBox MED+

Version 5

KoCo Connector GmbH
Dessauer Straße 28-29
10963 Berlin
Tel.: +49 (0) 30 24 64 90-0
Fax: +49 (0) 30 24 64 90-199
info@kococonnector.com
www.kococonnector.com

© Copyright 2024, KoCo Connector GmbH, alle Rechte vorbehalten.

Dieses Administratorhandbuch für die KoCoBox MED+ darf weder auszugsweise noch vollständig, in keiner weiteren Form und auf keine andere Weise reproduziert werden. Ferner darf es ohne vorherige schriftliche Erlaubnis durch die KoCo Connector GmbH nicht als Grundlage für Übersetzungen, Transformationen oder Anlehnungen genutzt werden.

Aus Gründen der Lesbarkeit wurde im Text die männliche Form gewählt; nichtsdestoweniger beziehen sich die Ausführungen auf Angehörige aller Geschlechter.

Die Firmware-Versionsnummer rufen Sie am Display der KoCoBox MED+ ab über:
Hauptmenü > Versionen

Dokumentenversion: 5
Dokumentensprache: deutsch (de)
zuletzt geändert: 17. Juli 2024

Inhaltsverzeichnis

| | |
|---|----|
| Allgemeine Informationen..... | 6 |
| Lieferumfang..... | 8 |
| 1 Einleitung | 9 |
| 2 Allgemeine Sicherheitshinweise | 11 |
| 3 Sicherheitsziele für den Einsatz der KoCoBox MED+ | 13 |
| 3.1 Sichere Einsatzumgebung | 14 |
| 3.2 Sichere Clientsystemanbindung..... | 16 |
| 3.3 Sichere Ersatzverfahren | 17 |
| 4 Allgemeines zur KoCoBox MED+..... | 18 |
| 4.1 Technische Daten und Betriebsbedingungen..... | 18 |
| 4.2 Sicherheitssiegel und Design | 19 |
| 5 Sicherer Anschluss der KoCoBox MED+ | 28 |
| 6 Display | 32 |
| 6.1 Standardansicht | 32 |
| 6.1.1 Menüstruktur..... | 33 |
| 6.1.2 Navigationslogik des Steuermenüs..... | 36 |
| 6.2 Fehlerzustandsanzeige | 37 |
| 7 Inbetriebnahme des Konnektors..... | 38 |
| 7.1 Vorbereitungen | 40 |
| 7.2 Administrator-Passwort..... | 44 |
| 7.3 Aufbau und Semantik der Managementschnittstelle | 49 |
| 7.4 Grundkonfiguration des Konnektors..... | 54 |
| 7.4.1 Status | 54 |
| 7.4.2 Zusammenfassende Übersicht zur Initialkonfiguration | 56 |
| 7.4.3 Konfiguration des Netzkonnektors | 60 |
| 7.4.3.1 LAN / WAN..... | 61 |
| 7.4.3.2 DHCP | 66 |
| 7.4.3.3 VPN (Virtual Private Network)..... | 71 |
| 7.4.3.4 Zeitdienst..... | 75 |
| 7.4.3.5 DNS (Domain Name Server)..... | 78 |
| 7.4.4 Verbindung in die Telematikinfrastruktur | 79 |
| 7.4.4.1 Anschluss von Kartenterminals | 82 |
| 7.4.4.2 Import von TSL/CRL..... | 83 |
| 7.5 Konfiguration des Anwendungskonnektors | 84 |
| 7.5.1 Verwaltung | 84 |
| 7.5.1.1 Clientsysteme..... | 88 |
| 7.5.1.2 Ex-/Import | 95 |

| | | |
|----------|--|------------|
| 7.5.1.3 | Telematikdienste..... | 102 |
| 7.5.2 | Kartendienst..... | 103 |
| 7.5.3 | Kartenterminaldienst..... | 105 |
| 7.5.4 | Systeminformationsdienst | 113 |
| 7.5.5 | Zertifikatsdienst | 115 |
| 7.5.5.1 | CA-Import..... | 119 |
| 7.5.5.2 | Status verwendeter Zertifikate..... | 120 |
| 7.5.5.3 | Laufzeitverlängerung | 121 |
| 7.5.6 | Protokollierungsdienst | 122 |
| 7.5.7 | Signaturdienst..... | 125 |
| 7.5.8 | LDAP-Proxy..... | 131 |
| 7.5.9 | Verschlüsselungsdienst | 132 |
| 7.6 | Konnektormanagement | 133 |
| 7.6.1 | Benutzerverwaltung | 133 |
| 7.6.2 | Infomodell..... | 137 |
| 7.6.3 | Aktualisierung..... | 141 |
| 7.6.4 | Werksreset | 155 |
| 7.7 | Fachmodule..... | 158 |
| 7.7.1 | Fachmodulspezifische Sicherheitsmaßnahmen..... | 158 |
| 7.7.2 | Versichertenstammdatenmanagement (VSDM) | 160 |
| 7.7.3 | Arzneimitteltherapiesicherheit (AMTS) | 165 |
| 7.7.4 | Elektronische Patientenakte (ePA)..... | 168 |
| 7.7.5 | Notfalldaten-Management (NFDM)..... | 175 |
| 8 | Sicherheitsrelevante Szenarien | 178 |
| 8.1 | Einsatzumgebung..... | 178 |
| 8.2 | Sicherheitskritische Fehlerzustände..... | 180 |
| 8.3 | Selbsttest..... | 185 |
| 8.4 | Sperrprozess und Außerbetriebnahme..... | 187 |
| 9 | Anhang | 188 |
| 9.1 | Weitere Konfigurationsoptionen..... | 188 |
| 9.1.1 | Alternative Netzwerkkonfigurationen | 188 |
| 9.1.1.1 | Anbindungsmodus Internet..... | 188 |
| 9.1.1.2 | Routingmodus Intranet..... | 188 |
| 9.1.1.3 | WAN Adapter Modus..... | 188 |
| 9.1.2 | Konfiguration ohne Internetanbindung..... | 190 |
| 9.1.3 | Standalone-Szenario mit physischer Trennung..... | 191 |
| 9.2 | Fehlermeldungen..... | 193 |
| 9.2.1 | Herstellerspezifische Fehlermeldungen | 193 |
| 9.2.2 | Betriebszustandsmeldungen..... | 209 |
| 9.2.3 | Sicherheitsrelevante Fehlermeldungen der Fachmodule..... | 214 |
| 9.3 | Ergänzende technische Informationen | 217 |
| 9.3.1 | Startverhalten | 217 |
| 9.3.2 | Versionsangaben zu gesteckten Karten im CETP-Event..... | 217 |
| 9.3.3 | Infomodell und XML-Schema..... | 218 |
| 9.3.4 | Gehärtete Schemata für XAdES-NFD..... | 222 |
| 9.4 | Datenschutzerklärung..... | 238 |
| 9.5 | Lizenzinformationen | 243 |
| 9.6 | Tabellenverzeichnis | 244 |

| | | |
|------|----------------------------|-----|
| 9.7 | Stichwortverzeichnis..... | 245 |
| 9.8 | Glossar | 259 |
| 9.9 | Abkürzungsverzeichnis..... | 280 |
| 9.10 | Abbildungsverzeichnis..... | 284 |
| 9.11 | Referenzen..... | 287 |

Allgemeine Informationen

Dieses Administratorhandbuch beschreibt die KoCoBox MED+ inklusive ihrer Fachmodule und Dienste. Es referiert auf die KoCoBox MED+, Version 5.

Die Ausführungen zum Konnektor¹ erläutern Einsatzumgebung, Installation, Konfigurationen und Bedienung mittels Managementschnittstelle sowie die in diesem Zusammenhang einzuhaltenden Sicherheitsanforderungen.

Semantik des Handbuchs

Zum Verdeutlichen wichtiger Aspekte und zur Steuerung der Aufmerksamkeit werden im Handbuch folgende Icons verwendet:



Sicherheitshinweis



Hinweis



Tipp



Störung



Fehlermeldung



Handlungsanweisung



vorhanden / in Ordnung



Frage / Prüfung



Sicherheitsgefahr



Warnung



Information

¹ Der Konnektor setzt sich insgesamt aus dem Netzkonnektor (NK), dem Anwendungskonnektor (AK), den Fachmodulen (FM) und der Security Module Card Konnektor (gSMC-K) zusammen. Ausführliche Informationen dazu: [PP-0097], S. 9 und S. 11 sowie [PP-0098], S. 17 ff., ferner für die Fachmodule: [TR-03154], S. 10 ff. sowie [TR-03155], S. 10 ff. und [TR-03157], S. 12 ff.

Schriftkonventionen

Bedeutungen:

- Schmalschrift: im technischen Kontext Funktions- und Button-Bezeichnungen
- Halbfettschrift: Teilüberschrift
- **Fettschrift:** Hervorhebung
- *Kursivschrift:* Namen, Titel, Überschriften, Pfadbeschreibungen oder Meldungstexte (z.B. im Dialogfenster)
- Courier New: Displaytext/Displaymenü der KoCoBox MED+
- elektronische Gesundheitskarte (eGK): wird eine Abkürzung erstmals verwendet, steht sie in Klammern neben dem vollständigen, ausgeschriebenen Begriff; sämtliche Abkürzungen sind im Abkürzungsverzeichnis dokumentiert

Lesehinweis

Zum fachlich tieferen Verständnis der Ausführungen in diesem Handbuch können Sie bei Bedarf während der Lektüre auch die im Literaturverzeichnis angegebenen Dokumente heranziehen. Auf diese wird stellenweise in Fußnoten referiert.

Lieferumfang

Die Verpackung der KoCoBox MED+ besteht aus einer rechteckigen Pappbox. Diese ist an der vorderen Längsseite mit einem Verpackungssiegel sowie rechts daneben zusätzlich mit einem Sicherheitssiegel verschlossen. Auf dieser Verpackung befinden sich zudem seitlich zwei Aufkleber zur Identifikation des Geräts.²



Prüfen Sie, ob die beiden Siegel der Verpackung³ sowie das Paket insgesamt äußerlich unversehrt sind, bevor Sie es öffnen.



Die Box muss die unten aufgelisteten Teile beinhalten.

Packen Sie den gesamten Inhalt aus und prüfen Sie den Lieferumfang auf Vollständigkeit:

- KoCoBox MED+ (Konnektor)
- Steckernetzteil
- Allgemeine Gebrauchsanleitung
- 4 Gehäusefüße (selbstklebend)



Verwenden/Installieren Sie bitte nur einen Konnektor, der von einem **autorisierten Lieferanten** bereitgestellt wird.



Ist die Verpackung des Geräts äußerlich beschädigt und / oder eines der aufgeführten Teile nicht vorhanden oder beschädigt, kontaktieren Sie den Lieferanten. Nehmen Sie das Gerät nicht in Betrieb!



Verwenden Sie nur vom Hersteller zugelassene Zubehörteile. Steckernetzteile mit abweichenden Werten können das Gerät beschädigen. Dadurch erlischt die Garantie!



Das Administratorhandbuch steht dem Servicepartner (Lieferanten) über das Service-Portal der KoCo Connector GmbH (<https://www.kococonnector.com>) jeweils in der aktuellen Version zur Verfügung.



Der Servicepartner ist verpflichtet, diese dem Endkunden auf Anforderung bereit zu stellen.

² Zur Optik der beiden Siegel auf der Verpackung sowie der beiden Aufkleber siehe das Kapitel Sicherheitssiegel und Design.

³ Zur Optik der Sicherheitssiegel im originalen und manipulierten Zustand siehe das Kapitel Sicherheitssiegel und Design.

1 Einleitung

Der Konnektor (to connect = verbinden) hat im Rahmen der Nutzung der elektronischen Gesundheitskarte (eGK) die Aufgabe, die sichere Verbindung zwischen dezentralen und zentralen Komponenten der Telematikinfrastruktur (TI)⁴ des Gesundheitswesens zu gewährleisten.

Dieses Administratorhandbuch⁵ beschreibt die initiale sowie weiterführende Konfiguration der KoCoBox MED+ zur sicheren Einbindung in die TI.

Die KoCoBox MED+ ist eine sogenannte ‚Einbox-Lösung‘: Netz- und Anwendungskonnektor sowie die Fachmodule (NK, AK, FM) sind in einer Box integriert. Die gSMC-K als Sicherheitsmodul des Konnektors ist sicher mit dem NK und AK verbunden.⁶ Der Bestandteil NK erfüllt die Sicherheitsfunktionen einer Firewall, eines VPN-Clients sowie von Servern für einen Zeitdienst, einen Namensdienst (Domain Name Server, DNS) und einen DHCP-Dienst.

Der Konnektor muss sehr hohen Sicherheitsstandards Rechnung tragen. Die KoCoBox MED+⁷ erfüllt diese. Insofern sind die Sicherheitsvorgaben mit besonderer Sorgfalt einzuhalten.



Die KoCoBox MED+ wird in mehreren Hardwaregenerationen (G3-Konnektor, G4-Konnektor⁸) ausgeliefert. Diese sind nachfolgend beschrieben. Sofern Unterschiede zwischen den Generationen bestehen, sind diese explizit dargestellt.

Zielgruppe

Zielgruppe dieses Handbuchs sind die Administratoren der KoCoBox MED+. Administratoren sind vom Besitzer der KoCoBox MED+ autorisierte, vertrauenswürdige und fachlich kompetente Personen, die das Gerät über die passwortgeschützte Managementschnittstelle konfigurieren und verwalten.



Eine nicht-autorisierte, nicht fachlich geschulte bzw. nicht vertrauenswürdige Person darf die KoCoBox MED+ aus Sicherheitsgründen nicht administrieren!

Weitere Dokumente

Mit diesem Handbuch sind für eine Einrichtung der vollständigen Betriebsumgebung der KoCoBox MED+ weitere ergänzende Dokumente wichtig:

- Für die Konfiguration und Verwendung des Clientsystems durch den Arzt/Apotheker gilt die Dokumentation des Clientsystemherstellers.
- Für die Konfiguration und Verwendung der Kartenterminals gilt die Dokumentation des Kartenterminal-Herstellers.

⁴ Synonym auch: Produkte der TI

⁵ Der besseren Lesbarkeit halber werden nur männliche Formen verwendet.

⁶ Siehe [PP-0097], S. 13 ff.

⁷ Synonym auch nur *Gerät* oder *Konnektor* genannt

⁸ Abgekürzt: G3, G4

- Für die Verwendung der in der Praxis einzusetzenden Karten (Betriebsstättenkarte SM-B und Heilberufsausweis HBA) gelten die Informationen der herausgebenden Organisation der jeweiligen Karte.
- Für die Nutzung der Signaturfunktionalität und der damit verbundenen Signatur- und Verschlüsselungsrichtlinien gelten die umgesetzten Anforderungen aus den gematik-Implementierungsrichtlinien⁹. Entsprechende Hinweise sind der Benutzerdokumentation des Clientsystems zu entnehmen.

Support

Für die KoCoBox MED+ gibt es drei Support-Instanzen.¹⁰

- First-Level-Support: Support-Hotline des Servicepartners.¹¹
- Second-Level-Support: Support-Instanz des Resellers bzw. des Clientsystem-Herstellers
- Third-Level-Support: Support des Herstellers, der KoCo Connector GmbH

⁹ betrifft [gemILF_PS], [gemILF_PS_NFDM, gemILF_PS_AMTS]

¹⁰ Vereinfacht wird im Text nur der Begriff *Support* verwendet. Es wird vorausgesetzt, dass der Leser des Administratorhandbuchs seinen zuständigen Support kennt.

¹¹ Synonym auch: Systempartner; Nutzern, die die KoCoBox MED+ im KoCo-Shop erworben haben, stehen die in den auf der Webseite www.koco-shop.de im Bereich FAQ aufgeführten Support-Optionen zur Verfügung.

2 Allgemeine Sicherheitshinweise

- Lesen Sie vor Inbetriebnahme des Geräts dieses Administratorhandbuch sorgfältig durch und bewahren Sie es gut auf.
- Der Bestell-/Lieferprozess sollte problemlos wie folgt abgelaufen sein: Bestellung des Konnektors beim Servicepartner und Erhalt der Bestellnummer; Vereinbarung des Installationstermins und Bestimmung eines Identifikationsverfahrens für den Service-Techniker (z.B. PIN-Nummer, Lichtbildausweis); Eintreffen des Service-Technikers beim Installationstermin mit dem Konnektor sowie der entsprechenden Bestellnummer, Authentifizierung mittels vereinbartem Identifikationsverfahren. Bei Unstimmigkeiten im Ablauf ist unverzüglich der Servicepartner zu kontaktieren.
- Notieren Sie an einem geschützten Ort die Seriennummer des Konnektors, um sie bei Verlust des Geräts, z.B. durch Diebstahl, für den Support griffbereit zu haben. Diese finden Sie auf dem Typenschild am Boden der Box sowie auf der Verpackung.
- An einem geeigneten, geschützten Ort sind die Vertragsnummer (ContractID) sowie die Kontaktdaten des Zugangsdienstproviders (ZGDP) bereitzuhalten.
- Nutzen Sie TLS-Cipher-Suites mit AES-GCM bei der Datennetz-Verbindung mit der KoCoBox MED+. Vermeiden Sie die Verwendung von AES-CBC bei jeglichen Verbindungen.
- Halten Sie als Administrator die Authentisierungsinformationen und die Admin-PIN bzw. das Admin-Passwort unbedingt geheim und geben sie diese niemals weiter.
- Speichern Sie entsprechende Passwörter niemals im Browser.
- Beachten Sie bei späteren Wartungsaktivitäten immer das aktuelle Administratorhandbuch.
- Berücksichtigen Sie bei der Konfiguration das Betriebsführungsbuch.¹²
- Achten Sie darauf, dass Sie generell vor Beginn der administrativen Tätigkeiten an der KoCoBox MED+ den dafür verwendeten Browser neu starten und den Zugang zum Konnektor als einzige Sitzung ausführen, um die Gefahr unerkannter Angriffe aus anderen Browsersitzungen zu vermindern.
- Fachmodule verwenden keine ECN Bits im IP V4 Header. Daher erfolgt kein Leaking von Informationen. Bitte stellen Sie sicher, dass Anwendungen im LAN, die auf Bestandsnetze¹³ oder Fachdienste zugreifen, ebenfalls keine ECN Bits benutzen.
- Zur Verfügung gestellte Software-Updates für die KoCoBox MED+ sind zeitnah einzuspielen, um stets die aktuellen Versionen der Sicherheitstechnologien zu verwenden. Sicherheitsinformationen finden Sie unter www.gematik.de, www.bundesnetzagentur.de, www.bsi.bund.de.
- Verwenden Sie die KoCoBox MED+ nur für den vorgesehenen Zweck.
- Stellen Sie sicher, dass das Gerät nur in einer zugriffsgeschützten bzw. zugriffsbeschränkten Umgebung eingesetzt wird.¹⁴
- Ist eines / sind beide Siegel an der Verpackung äußerlich beschädigt, kontaktieren Sie bitte Ihren Servicepartner. Nehmen Sie das Gerät bis zu dessen Freigabe nicht in Betrieb!

¹² Da der Konnektor bspw. den Import/Export der Konfigurationsdaten nicht personenbezogen/namentlich protokolliert, etwaige Änderungen jedoch auf eine natürliche Person zurückzuführen sein müssen, ist die Dokumentation mittels Betriebsführungsbuch erforderlich.

¹³ Der Begriff „Bestandsnetze“ bezeichnet hierbei andere Anwendungen des Gesundheitswesens ohne Zugriff auf Dienste der TI in angeschlossenen Netzen des Gesundheitswesens (aAdG-NetG).

¹⁴ Zur Definition der zugriffsgeschützten bzw. zugriffsbeschränkten Umgebung siehe das folgende Kapitel.

- Nehmen Sie die KoCoBox MED+ nur mit unverletzten Sicherheitssiegeln in Betrieb.¹⁵
- Sind die Sicherheitsschrauben¹⁶ am Boden des Geräts gelöst oder fehlen diese, so nehmen Sie das Gerät nicht in Betrieb. Kontaktieren Sie bitte umgehend Ihren Servicepartner.
- Schließen Sie das Gerät ausschließlich an eine vorschriftsmäßig installierte Steckdose an und achten Sie auf seinen sicheren Stand.
- Beachten Sie beim Anschluss an das Stromnetz die Anschlusswerte und verlegen Sie die Netz- und CAT5a-Kabel unfallsicher.
- Zum Netzanschluss dieses Gerätes ist eine geprüfte Leitung mit einem zulässigen Nennstrom von mindestens 6 Ampere zu verwenden.
- Öffnen Sie niemals das Gehäuse der KoCoBox MED+.
- Sorgen Sie dafür, dass die Lüftungsschlitze ausreichend Abstand zu Umbauten haben und niemals abgedeckt sind.
- Es dürfen niemals durch die Lüftungsschlitze Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte Fehlfunktionen des Konnektors oder einen Brand auslösen.
- Schützen Sie das Gerät vor extremen Temperaturschwankungen.
- Bedienen Sie die Steuer-Buttons des Geräts nicht mit Woll- oder Lederhandschuhen. Dies kann zu Funktionsstörungen führen.
- Sofern Sie während des Betriebs des Konnektors Meldungen bekommen, die Sie im Rahmen Ihrer Tätigkeit nicht erwarten, könnte dies auf eine Manipulation hindeuten. Kontaktieren Sie sicherheitshalber Ihren Support.
- Führen Sie vor der Weitergabe der KoCoBox MED+ an einen anderen Betriebsstättenverantwortlichen einen Werksreset aus. Sollte dieser fehlschlagen, ist der Konnektor auszutauschen und an den Hersteller zurückzuführen.
- Prüfen Sie die Unversehrtheit von Kartenterminals, bevor Sie sie im Netzwerk mit der KoCoBox MED+ verbinden. Verwenden Sie ausschließlich Geräte mit unverletzten Sicherheitssiegeln. Weiterführende Information zu Aussehen und Position der Siegel finden Sie in der Dokumentation der Kartenterminals.
- Wenden Sie sich bei allen Fragen, die den sicheren Betrieb oder die Vertrauenswürdigkeit der KoCoBox MED+ betreffen, an Ihren Support.
- Für den Fall, dass Sie vom Hersteller oder Ihrem Support telefonisch oder per E-Mail Sicherheitshinweise bekommen oder über eine Kompromittierung der TI informiert werden, folgen Sie bitte unverzüglich den Anweisungen!
- Versichern Sie sich bei entsprechenden Anrufen oder E-Mails dabei auf geeignete Weise, dass es sich tatsächlich um den Hersteller bzw. Ihren Support handelt (z.B. durch Namensnennung eines Ihnen bekannten Mitarbeiters oder mittels telefonischen Rückrufs Ihrerseits).
- Beachten Sie sorgfältig die speziellen Sicherheitshinweise in den folgenden Abschnitten.

¹⁵ Bitte beachten Sie: Es muss sich dabei ausschließlich um das im Abschnitt Sicherheitssiegel und Design beschriebene und dargestellte Sicherheitssiegel – und kein anderes – handeln. Die beiden Sicherheitssiegel der Box müssen regelmäßig auf ihre Integrität überprüft werden.

¹⁶ Die KoCoBox MED+ wird mit 1 bis 6 Sicherheitsschrauben ausgestattet. Die angestrebte Schutzwirkung wird bereits durch eine Sicherheitsschraube erzielt.

3 Sicherheitsziele für den Einsatz der KoCoBox MED+

Das folgende Kapitel beschreibt ausführlich die Rahmenbedingungen, unter denen die KoCoBox MED+ – etwa in der Arztpraxis oder in der Apotheke – eingesetzt werden darf und dabei die vorgegebenen Sicherheitsziele erfüllt.

Es gliedert sich in die Beschreibung

- der sicheren Einsatzumgebung (Wie muss der Raum, in dem das Gerät aufgestellt wird, vor Zugriffen Unbefugter geschützt sein?),
- der sicheren Clientsystemanbindung (Welche Sicherheitsstandards muss die IT-Umgebung/müssen die IT-Systeme erfüllen, an die der Konnektor angeschlossen ist?),
- sowie der sicheren Ersatzverfahren (Wie kann der Praxisbetrieb auf sichere Art und Weise aufrechterhalten werden, etwa bei Ausfall der TI?).

3.1 Sichere Einsatzumgebung

Die KoCoBox MED+ – sowie die Netzwerkkomponenten Switch und Internet Access Gateway (IAG), z.B. Router mit DSL-/Kabelmodem – darf gemäß Sicherheitskonzept nur in einem **zugriffsgeschützten** oder **zugriffsbeschränkten** Bereich eingesetzt werden.¹⁷

Zugriffsschutz

Der **zugriffsgeschützte Bereich** muss den physischen Schutz des Geräts gegen Angreifer mit hohem Angriffspotenzial¹⁸ gewährleisten und den unberechtigten Zugang während der aktiven Datenverarbeitung im Konnektor verhindern.¹⁹: Erfolgt dennoch ein unberechtigter physischer Zugriff auf das Gerät, muss dieser erkannt werden. Zugang zu dieser sicheren Einsatzumgebung haben nur die Ärzte / Apotheker und autorisierte Personen (z.B. das Fachpersonal).

Beispiele für diesen zugriffsgeschützten Bereich sind:

- ein Rechenzentrum oder abschließbare Räume, in denen sich weitere schützenswerte Güter, wie die Praxis-EDV, verschreibungspflichtige Medikamente, die unter das Betäubungsmittelgesetz fallen, sowie medizintechnische Geräte, Formulare, Praxisstempel usw. befinden können
- ein verschließbarer Schrank oder ein gesichertes Behältnis (z.B. ein im Boden oder an der Wand verankerter Metallkasten mit Sicherheitsschloss)



Die Reglementierung erfolgt bspw. mittels Hinweisschilds (z.B. *Zutritt für Unbefugte nicht gestattet!*) und Türschloss.



Diese Sicherungsmaßnahmen **müssen** den Zugriff auf das Gerät durch nicht-autorisierte Personen verhindern.²⁰

Überwachung

Das Gerät sollte in seiner geschützten Einsatzumgebung durch weitere organisatorische und technische Maßnahmen gesichert werden, wie z.B. (wenn vorhanden) eine Alarmanlage, Sicherheitsschlösser, Fenstergitter.

Für die Überwachung sämtlicher Schutzmaßnahmen ist ein eindeutig identifizierbarer Verantwortlicher (mit Vertreter) zu bestimmen, der sich zuverlässig und regelmäßig um diese Aufgabe kümmert. Hierbei prüft er zum Beispiel die Funktionsfähigkeit der technischen Sicherungsvorrichtungen, kontrolliert den Raum, in dem sich das Gerät befindet, prüft die Räume auf Einbruch sowie die Sicherheitssiegel der KoCoBox MED+ auf Unversehrtheit.

¹⁷ Vgl. [gemSpec_Kon], S. 527

¹⁸ Diesen Personen wird eine hohe Motivation unterstellt, die TI zu kompromittieren.

¹⁹ In der Regel findet die Datenverarbeitung in den Öffnungszeiten z.B. der Arztpraxis oder der Apotheke statt.

²⁰ Die konkreten Maßnahmen dafür hängen von den individuellen Gegebenheiten vor Ort ab, der Servicepartner kann hierfür entsprechende Hinweise geben.

Sicherheitshinweise



Zusammenfassend sind zur sicheren Inbetriebnahme und für den sicheren Betrieb der KoCoBox MED+ folgende Sicherheitsanforderungen zu erfüllen:

- Die KoCoBox MED+ kommt nur in einer Umgebung zum Einsatz, die laut Definition **zugriffsgeschützt** bzw. **zugriffsbeschränkt** ist.
- Es ist sichergestellt, dass nur der Endkunde bzw. von ihm autorisierte Personen Zugriff haben.
- Der Endkunde sorgt dafür, dass administrative Tätigkeiten immer in Übereinstimmung mit dem vorliegenden Handbuch (aktuelle Version) und von autorisierten, vertrauenswürdigen und ausgebildeten Administratoren durchgeführt werden.
- Verbindungen mit dem Konnektor nutzen TLS-Cipher-Suites mit AES-GCM und **vermeiden** die Verwendung von **AES-CBC**.
- Die Administratoren halten Authentisierungsinformationen und -token geheim bzw. geben diese nicht weiter (z.B. PIN bzw. Passwort oder Schlüssel-Token).
- PINs oder Passwörter werden nicht im Webbrowser gespeichert.
- Die gesamte Einsatzumgebung ist durch organisatorische und technische Maßnahmen zu schützen.
- Sofern sich ein Unbefugter widerrechtlichen Zugang / Zugriff verschafft und / oder das Gerät gestohlen wurde, wird dies unverzüglich erkannt.
- Eine Manipulation der KoCoBox MED+, indiziert durch ein gebrochenes Sicherheitssiegel und / oder zerstörte Sicherheitsschrauben, wird sofort sicher erkannt.²¹
- Es ist ein eindeutig identifizierbarer Verantwortlicher benannt, der das fehlerfreie Funktionieren aller Sicherheitsmaßnahmen zuverlässig überwacht.
- Falls der Konnektor manipuliert oder gestohlen wurde, ist unverzüglich der Servicepartner zu informieren und dabei die Seriennummer (SN) des Geräts zu übermitteln.



Wir empfehlen weitere Maßnahmen zur Sicherung der KoCoBox MED+:

- Anschluss der KoCoBox MED+ mittels Kensington-Schloss an eine Verankerung vor Ort
- regelmäßige Information / Schulung des Endkunden und seines (Fach-)Personals in der sorgfältigen Beachtung der räumlichen und organisatorischen Schutzmaßnahmen

²¹ Der Konnektor ist als Tischgerät konzipiert und sollte, im Rahmen der Beweglichkeit von Spannungsversorgung und Netzwerkanschlüssen, für eine Inspektion angehoben und seitlich gedreht werden können. Dies ist besonders beim Einstellen in ein Rack zu berücksichtigen. Die Sichtprüfung von Sicherheitssiegel, Geräteetikett und Verschraubung erfolgt durch Anheben bzw. seitliches Drehen des Konnektors um bis zu 90°.

3.2 Sichere Clientsystemanbindung

Bei der Einbindung der KoCoBox MED+ in das lokale Netz muss sichergestellt sein, dass das Gerät das Clientsystem / die Clientsysteme des Arztes / Apothekers – z.B. das Praxisverwaltungssystem (PVS), Arztinformationssystem (AIS) oder das Apothekenverwaltungssystem (AVS) – korrekt, d.h. auf sichere Art und Weise nutzt.²²

- Prüfen Sie jeweils, ob es sich beim anzubindenden Clientsystem / den anzubindenden Clientsystemen jeweils um ein sicheres Produkt handelt, das durch die Gematik für den Einsatz in der Telematikinfrastruktur bestätigt wurde.²³
- Stellen Sie sicher, dass es in sicherer Art und Weise administriert wird (z.B. mittels geschütztem Passwort und PIN).
- Achten Sie sorgsam darauf, dass keine Schadsoftware auf das Clientsystem / die Clientsysteme (oder ggf. andere IT-Systeme im LAN) aufgebracht werden, z.B. beim Einspielen von ausführbaren Dateien per Laufwerk oder USB-Stick oder durch Öffnen von E-Mail-Anhängen).
- Stellen Sie durch entsprechende Konfigurationen in der Managementschnittstelle der KoCoBox MED+ sicher, dass das Clientsystem / die Clientsysteme nicht oder nur auf sichere Art und Weise mit dem Internet verbunden sind – wie etwa durch Nutzung des Sicheren Internet Service (SIS).
- Vergewissern Sie sich, dass es sich bei der verwendeten Version des Konnektors um eine **zugelassene** Version handelt. Der Konnektor stellt dem Clientsystem seine Versionsinformation mit Hilfe der Datei `connector.sds` zur Verfügung. Kontaktieren Sie Ihren Clientsystem-Hersteller, wie Sie in der Clientsystem-Software diese Information erhalten können.²⁴ Prüfen Sie die erhaltenen Informationen gegen die, die Sie im Gematik-Fachportal unter <https://fachportal.gematik.de/zulassungen/online-produktivbetrieb/> aufgelistet finden. Wählen Sie hierzu den Produkttyp Konnektor und den Status zugelassen aus. In der Ergebnisliste muss die KoCoBox MED+ mit den Informationen *Produktversion* und *Produkttypversion* vorliegen. Diese **müssen** mit den aus dem Konnektor ausgelesenen Informationen übereinstimmen. Sollte dies nicht der Fall sein, nehmen Sie den Konnektor nicht in Betrieb und wenden sich umgehend an Ihren Servicepartner.



Beachten Sie, dass bei Verwendung des SIS Angriffe aus dem Internet **nicht** ausgeschlossen werden können. Sorgen Sie daher im Praxisnetz für eine **stets aktuell gehaltene Absicherung** der genutzten Clientsysteme, z.B. mittels **Systemupdates und Virenschnern**, sowie die Verwendung **sicherer Grundeinstellungen und Zugangsdaten** der entsprechenden Arbeitsstationen.

²² Generell liegt die Verantwortung für die Sicherheit der Clientsysteme sowohl beim Endkunden als auch beim Hersteller des Clientsystems. Er muss sein Produkt nach dem aktuellen Stand der Technik und so gestaltet haben, dass es den Konnektor für Dienste gemäß § 291a SBG V korrekt aufruft. Vgl. [PP-0097], S. 55 und S. 57 f. bzw. [PP-0098], S. 97 und S. 100 f.

²³ Die genauere Beschreibung eines sicheren Clientsystems findet sich in [PP-0098], S. 108 sowie die Liste der bestätigten Clientsysteme unter <https://fachportal.gematik.de/service/konnektorsimulator-fuer-primarsysteme/liste-der-bestaetigten-primarsysteme/>

²⁴ Dies beinhaltet die Informationen `ProductName`, `FWVersion`, `HWVersion`, und `ProductTypeVersion`.

3.3 Sichere Ersatzverfahren

Es besteht die Möglichkeit, dass die Telematikinfrastruktur oder Teile davon ganz oder teilweise ausfallen oder auch Schwächen in den verwendeten kryptographischen Algorithmen, die eine zentrale Sicherheitsfunktion erfüllen, bekannt werden.²⁵

- Informieren Sie den Endkunden sowie ggf. das Fachpersonal darüber, dass der Konnektor nur noch offline genutzt wird; die eGK kann weiterhin ausgelesen werden. Onlinedienste wie zum Beispiel der Abgleich der Versichertenstammdaten (VSDM) oder SIS sind nicht verfügbar.
- Halten Sie gegebenenfalls ein mobiles Kartenterminal in Reserve. Die Datensätze können darüber per Batch-Verfahren ins Clientsystem eingelesen werden.
- Der Arzt soll die Behandlung der Patienten (und eventuelle Änderungen der Versichertenstammdaten) auf Papier dokumentieren und die Daten nach der Wiederherstellung des sachgerechten Betriebs nachtragen.

²⁵ Siehe [PP-0097], S. 58

4 Allgemeines zur KoCoBox MED+

4.1 Technische Daten und Betriebsbedingungen

Die KoCoBox MED+ wird in zwei verschiedenen Hardwaregenerationen (G3 und G4) ausgeliefert. Beide weisen die gleiche Funktionalität auf. Unterschiede in den technischen Daten stellt die nachfolgende Übersicht dar.

| | KoCoBox MED+ G3 | KoCoBox MED+ G4 |
|--------------------------------|---|--|
| Abmessungen (B x T x H) | 220 x 165 x 50 mm | 130 x 130 x 42 mm |
| Gehäusematerial | Acrylnitril-Butadien-Styrol (ABS) | pulverbeschichteter Aluminiumdruckguss |
| Masse | ca. 580 g | ca. 592 g |
| Display | Grafik-Display mit 128 x 64 Pixeln und 1,7 Zoll Bildschirmdiagonale | Grafik-Display RGB mit 320 x 240 Pixeln und 2 Zoll Bildschirmdiagonale |
| Bedienelemente | sechs kapazitive Sensoren | Keypad mit sechs Feldern |
| Hauptprozessor | i.MX6 Quad (NXP) | i.MX8 QuadMax (NXP) |
| Arbeitsspeicher | 2 GByte DDR3 | 8 GByte DDR4 |
| Festspeicher | 4 MByte Boot-NOR-Flash 2 GByte eMMC-Flash | 10 GByte eMMC-Flash |

Tabelle 1: Technische Daten der KoCoBox MED+



Die KoCoBox MED+ besitzt **keinen** On-/Off-Schalter. Das Gerät wird durch den Anschluss an das Stromnetz eingeschaltet.



Das Gerät ist für den Einsatz unter Umgebungsbedingungen vorgesehen, wie sie in Büro- und Praxisräumen herrschen: Sie sollten trocken, sauber und weitgehend staubfrei sein. Die KoCoBox MED+ sollte zudem auf einem erschütterungsfreien, ebenen Untergrund stehen. Dies vermeidet technische Störungen und gewährleistet den sicheren Einsatz der KoCoBox MED+.

- **Betriebstemperatur:** Zimmertemperatur (empfohlen):
Temperaturspanne von 5° bis 40° C
- **Luftfeuchtigkeit:** maximal 90% relative Luftfeuchtigkeit,
nicht kondensierend
- **Pflege:** leicht angefeuchtetes antistatisches, fusselfreies Tuch,
keine flüssigen, gasförmigen oder leicht entflammbaren Reinigungsmittel
keine Sprays, Scheuermittel, Alkohol oder Polituren

4.2 Sicherheitssiegel und Design

Die Verpackung der KoCoBox MED+ ist mit einem runden, transparenten Verpackungssiegel verschlossen. Zudem befindet sich daneben ein Sicherheitssiegel (siehe unten). An der rechten Seite gibt es zwei Verpackungsaufkleber mit der Seriennummer sowie mit Barcodes.

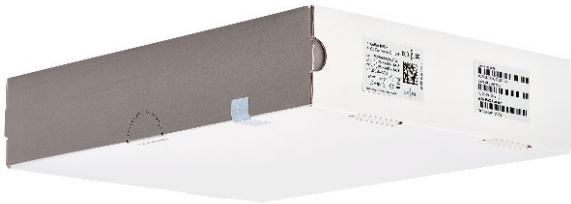


Abbildung 1: Geräteverpackung mit Siegeln und Verpackungsaufklebern (G3)



Abbildung 2: Geräteverpackung mit Siegeln und Verpackungsaufklebern (G4)



Abbildung 3: Verpackungssiegel der KoCoBox MED+

Der Durchmesser des Verpackungssiegels (G3 und G4-Konnektor) beträgt 3,7 cm.

Darüber hinaus befinden sich seitlich auf der Verpackung zwei Aufkleber zur Identifikation des Geräts.

Ein Aufkleber zeigt die Seriennummer des Geräts, WAN und LAN-Adresse sowie das Feld SMC-K exp.: Das darin angezeigte Datum entspricht dem Ablaufdatum der für den Zugang zur Telematik-Infrastruktur benötigten Zertifikate.

Das Maß des Aufklebers (G3- und G4-Konnektor) ist: Breite 51 mm, Höhe 32 mm.

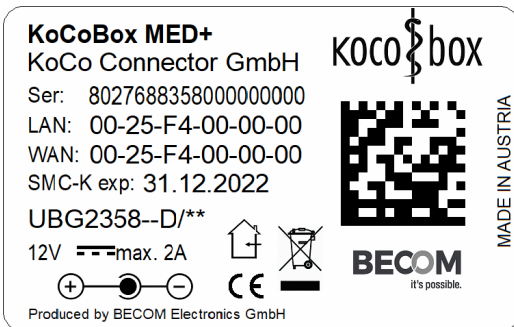


Abbildung 4: Verpackungsaufkleber mit Seriennummer (G3)

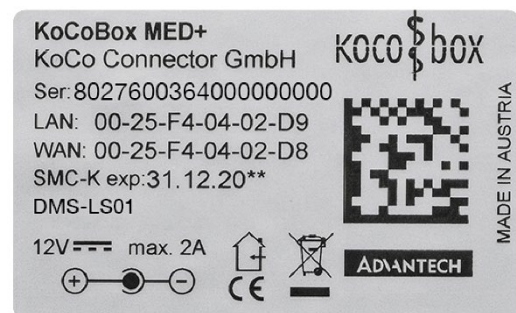


Abbildung 5: Verpackungsaufkleber mit Seriennummer (G4)

Der zweite Verpackungsaufkleber enthält Barcodes für die Seriennummer sowie die WAN- und LAN-MAC-Adresse.

Das Maß des Aufklebers (G3- und G4-Konnektor) ist: Breite 51 mm, Höhe 32 mm.

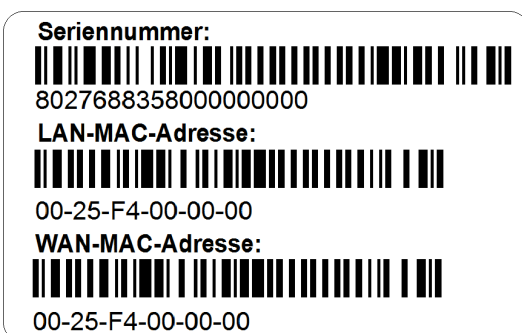


Abbildung 6: Verpackungsaufkleber mit Barcodes (G3)

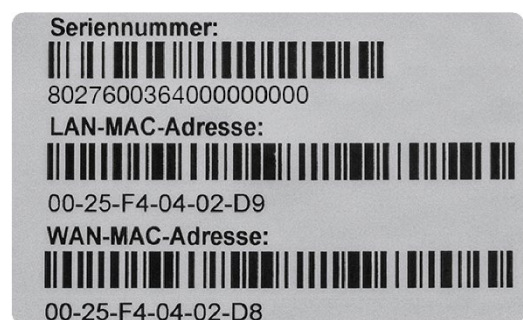


Abbildung 7: Verpackungsaufkleber mit Barcodes (G4)

Daneben ist die KoCoBox MED+ selbst durch zwei identische Sicherheitssiegel geschützt. Diese haben ein Hologramm, sodass sie nur sehr schwer zu kopieren sind.

Die folgenden Abbildungen zeigen das Sicherheitssiegel für die KoCoBox MED+ (und ihre Verpackung) im originalen bzw. manipulierten Zustand.



Abbildung 8: Optik des Sicherheitssiegels im Originalzustand (G3)



Abbildung 9: Ansicht nach Manipulation (G3)



Abbildung 10: Optik des Sicherheitssiegels im Originalzustand (G4)



Abbildung 11: Ansicht nach Manipulation (G4)

Die Maße des Sicherheitssiegels am Gerät sind

- 30 x 15 mm für die KoCoBox MED+ (G3-Konnektor),
- 32 x 13,5 mm für die KoCoBox MED+ (G4-Konnektor).



Sofern Sie nach Sichtprüfung eine Manipulation an einem oder beiden Sicherheitssiegeln der KoCoBox MED+ feststellen, nehmen Sie das Gerät **nicht** in Betrieb und informieren Sie unverzüglich Ihren Support.

Platzierung der Sicherheitssiegel KoCoBox MED+ G3



Abbildung 12: KoCoBox MED+ (G3) - Seitenansicht rechts mit Sicherheitssiegel

- 1** Front mit Display und Steuer-Buttons **2** Lüftungsschlitze **3** Sicherheitssiegel rechts

Von vorn betrachtet klebt ein Sicherheitssiegel mittig auf der Trennlinie zwischen Gehäuseunter- und Gehäuseoberteil, jeweils in der Mitte an beiden Seiten.



Abbildung 13: KoCoBox MED+ (G3) - Seitenansicht links mit Sicherheitssiegel

- 1** Lüftungsschlitze **2** Sicherheitssiegel links

Platzierung der Sicherheitssiegel KoCoBox MED+ G4



Abbildung 14: KoCoBox MED+ (G4) Ansicht rechts mit Sicherheitssiegel

- 1** Front mit Display und Steuer-Buttons **2** Sicherheitssiegel rechts

Von vorn betrachtet klebt ein Sicherheitssiegel mittig in einer Mulde zwischen Gehäuseunter- und Gehäuseoberteil, jeweils in der Mitte an beiden Seiten.



Abbildung 15: KoCoBox MED+ (G4) Ansicht links mit Sicherheitssiegel

- 1** Sicherheitssiegel links **2** Front mit Display und Steuer-Buttons

Steuerelemente



Abbildung 16: Front der KoCoBox MED+ (G3) mit Display und Steuer-Buttons

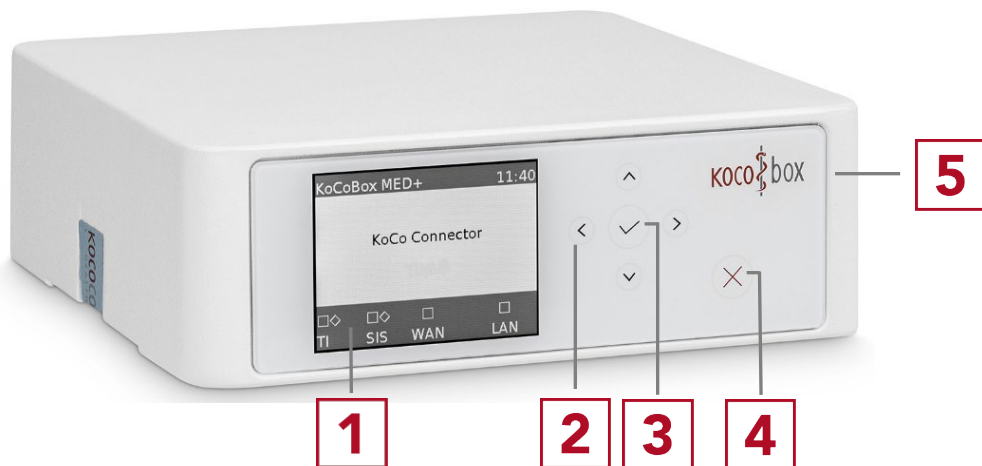


Abbildung 17: Front der KoCoBox MED+ (G4) mit Display und Steuer-Buttons

- 1** Display **2** Steuer-Buttons zur Navigation im Steuermenü

- ⬆️ oben: um jeweils eine Zeile nach oben navigieren
⬇️ unten: um jeweils eine Zeile nach unten navigieren

- ⬅️ ➡️ links / rechts: zwischen menü-externen kritischen Fehlerzustandsmeldungen navigieren

- 3** Button OK: Bestätigen einer Auswahl / Hauptmenü öffnen/ Untermenü öffnen bzw. Befehl bestätigen

- 4** Button Abbrechen: Auswahl abbrechen / Menü schließen bzw. zum vorherigen Menüpunkt oder zur vorherigen Ansicht zurückgehen

- 5** Logo

Anschlüsse



Abbildung 18: Rückseite der KoCoBox MED+ (G3) mit Anschlüssen

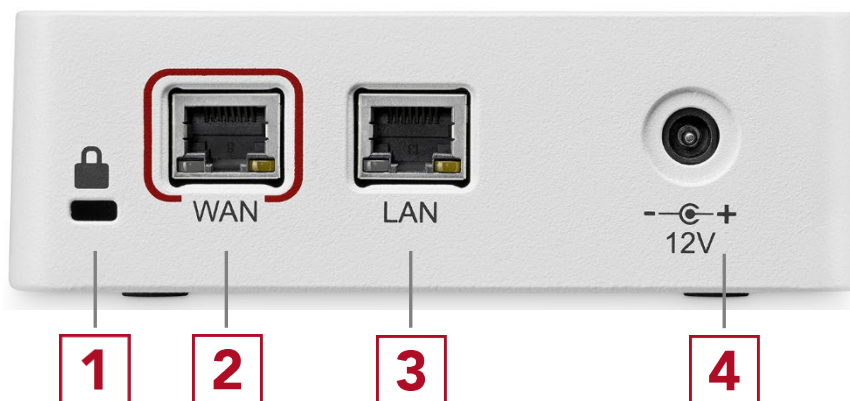


Abbildung 19: Rückseite der KoCoBox MED+ (G4) mit Anschlüssen

- 1** Kensington Lock: für Kensington-Schloss, Diebstahlsicherung für mobile Hardware
- 2** WAN: 10 / 100 / 1000 Base-T Gigabit Ethernet (RJ-45 Connector) zum Anschluss an einen Router mit DSL-/Kabelmodem
- 3** LAN: 10 / 100 / 1000 Base-T Gigabit Ethernet (RJ-45 Connector)
- 4** Stromanschluss (Spannungsversorgung)

Unterseite



Abbildung 20: Bodenansicht der KoCoBox MED+ (G3)



Abbildung 21: Bodenansicht der KoCoBox MED+ (G4)

1 Typenschild und Aufkleber mit Barcode

2 GummifüÙe

3 Sicherheitsiegel

4 Schraublöcher mit 1-6 Sicherheitsschrauben



Verwenden Sie die GummifüÙe zum sicheren Aufstellen des Geräts.

Typenschild

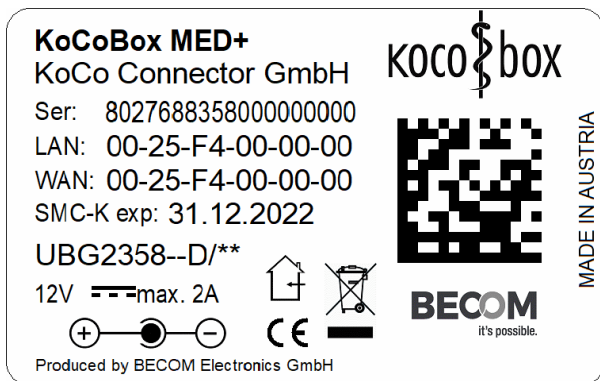


Abbildung 22: Typenschild am Boden der KoCoBox MED+ (G3)

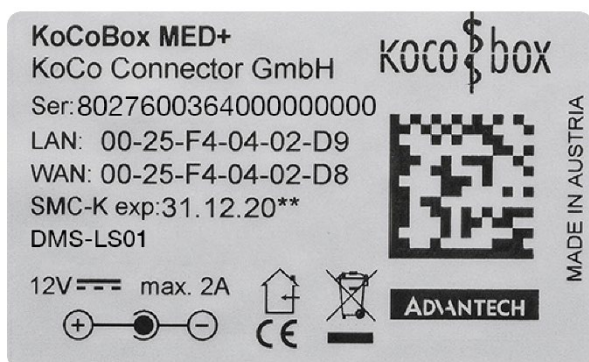


Abbildung 23: Typenschild am Boden der KoCoBox MED+ (G4)

Ein Aufkleber zeigt die Seriennummer des Geräts, WAN und LAN-Adresse sowie das Feld SMC-K exp. Das darin angezeigte Datum entspricht dem Ablaufdatum der für den Zugang zur Telematik-Infrastruktur benötigten Zertifikate.

Die Maße des Typenschildes sind Breite: 51 mm, Höhe: 32 mm.



Halten Sie zur Authentisierung im Supportfall die Vertragsnummer (ContractID) an einem geeigneten, geschützten Ort bereit.



Notieren Sie an einer geeigneten Stelle die auf dem Typenschild aufgedruckte Seriennummer (Ser) des Geräts für den Supportfall/die Registrierung und informieren Sie weitere autorisierte Personen (z.B. das Fachpersonal) darüber.

5 Sicherer Anschluss der KoCoBox MED+

Bevor Sie den Konnektor vor Ort anschließen, versichern Sie sich der Integrität der KoCoBox MED+ sowie sämtlicher für ihren sicheren Einsatz geforderten Voraussetzungen.

Integritätsprüfung



Untersuchen Sie sorgfältig:

- ob Verpackungssiegel sowie Sicherheitssiegel auf der Verpackung der KoCoBox MED+ (in Form einer Pappbox) sowie sämtliche Bestandteile des Lieferumfangs intakt sind;²⁶
- ob die Sicherheitsschrauben, mit denen das Gehäuse der KoCoBox MED+ verschraubt ist, intakt sind;
- ob die beiden Sicherheitssiegel an der KoCoBox MED+ exakt der oben dargestellten Abbildung entsprechen, es muss sich nach intensiver augenscheinlicher Prüfung jeweils **genau** um diese Sicherheitssiegel handeln – und keine anderen;
- ob beide Sicherheitssiegel unbeschädigt sind: Sie dürfen nach genauer augenscheinlicher und haptischer Prüfung (Hologramm und Oberfläche) weder zerschnitten noch zerkratzt oder geknittert sein und somit absolut keine Anzeichen von Manipulation aufweisen;
- ob das Typenschild der KoCoBox MED+ unbeschädigt ist und exakt der Abbildung entspricht; es darf nach augenscheinlicher und haptischer Prüfung weder zerkratzt noch geknittert sein oder Löcher verdecken und somit keine Anzeichen von Manipulation haben;
- ob nur die beiden Sicherheitssiegel und das Typenschild – und keine weiteren Applikationen – auf der KoCoBox MED+ angebracht sowie keine Löcher, Kratzer oder sonstigen Beschädigungen festzustellen sind;
- ob die räumlichen und organisatorischen Sicherheitsanforderungen an die Einsatzumgebung der KoCoBox MED+ erfüllt sind;



Nur wenn Sie bei der Integritätsprüfung zum Ergebnis kommen, dass keine Manipulation vorliegt, dürfen Sie das Gerät in Betrieb nehmen.



Bei Zweifeln an der Integrität des Verpackungs- und/oder Sicherheitssiegels, eines oder beider Sicherheitssiegel am Gerät, des Typenschildes, des Geräts oder Ihrer Maßnahmen zum Zugriffsschutz kontaktieren Sie den Support. Nehmen Sie es **nicht** in Betrieb.



Führen Sie im laufenden Betrieb der KoCoBox MED+ in regelmäßigen Zeitabständen eine sorgfältige Sichtkontrolle des Geräts durch.

²⁶ Ein beschädigtes Verpackungs-/und oder Sicherheitssiegel kann ein Hinweis auf unbefugtes Öffnen der Box während des Transports sein und muss weitere Sichtkontrollen (Gehäusesiegel, Verschraubung) durch den Empfänger nach sich ziehen.

Technische Voraussetzungen für den Anschluss der KoCoBox MED+ vor Ort sind:

- Breitband-Internet-Anschluss und Router mit DSL-/Kabelmodem
- netzwerkfähiger Rechner (für den Zugang zur Managementschnittstelle)

Anbindungsmodi

Mit dem Konnektor können unterschiedliche netzseitige Einsatzszenarien²⁷ umgesetzt werden, die in diesem Handbuch aus Gründen der Übersichtlichkeit nicht allumfassend dargestellt werden können. Abhängig davon bietet der Konnektor jeweils entsprechende Konfigurationsparameter.

Der Konnektor kann in zwei Anbindungsmodi genutzt werden, seriell (,in Reihe') oder parallel.

- Seriell (,in Reihe'): Der Konnektor fungiert als Gateway für das Netz des Endkunden, indem er zwischen das lokale Netz und den Router mit DSL-/Kabelmodem geschaltet wird.²⁸



Hier muss der Secure Internet Service (SIS) genutzt werden, wenn Internet zur Verfügung stehen soll.

- Parallel: Der Konnektor wird als weiteres Gerät in die bestehende Netzwerkinfrastruktur integriert. Hier können wahlweise der Internetzugang via IAG oder SIS genutzt werden.



Bitte beachten Sie: Das lokale Netz (LAN) ist mit geeigneten Maßnahmen außerhalb der KoCoBox MED+ vor Angriffen aus dem Internet zu schützen (Firewall, aktuelle Antivirensoftware etc.). Der für das Praxisnetzwerk zuständige Administrator ist für den Schutz des Praxisnetzwerks verantwortlich.

Die folgenden Abbildungen zeigen die Anbindungsmodi exemplarisch.²⁹

²⁷ Eine beispielhafte Darstellung der verschiedenen Einsatzszenarien findet sich in den Konnektor-Spezifikationen, Anhang K.

²⁸ Eine Illustration für diese einfache Installation sowie die Konfiguration des Konnektors für die serielle Anbindung (,in Reihe') finden Sie im Anhang unter Alternative Netzwerkkonfigurationen.

²⁹ Die Skizzen zeigen die Einbindung der KoCoBox MED+ in das lokale Netz, beispielhaft erweitert um einen Switch.

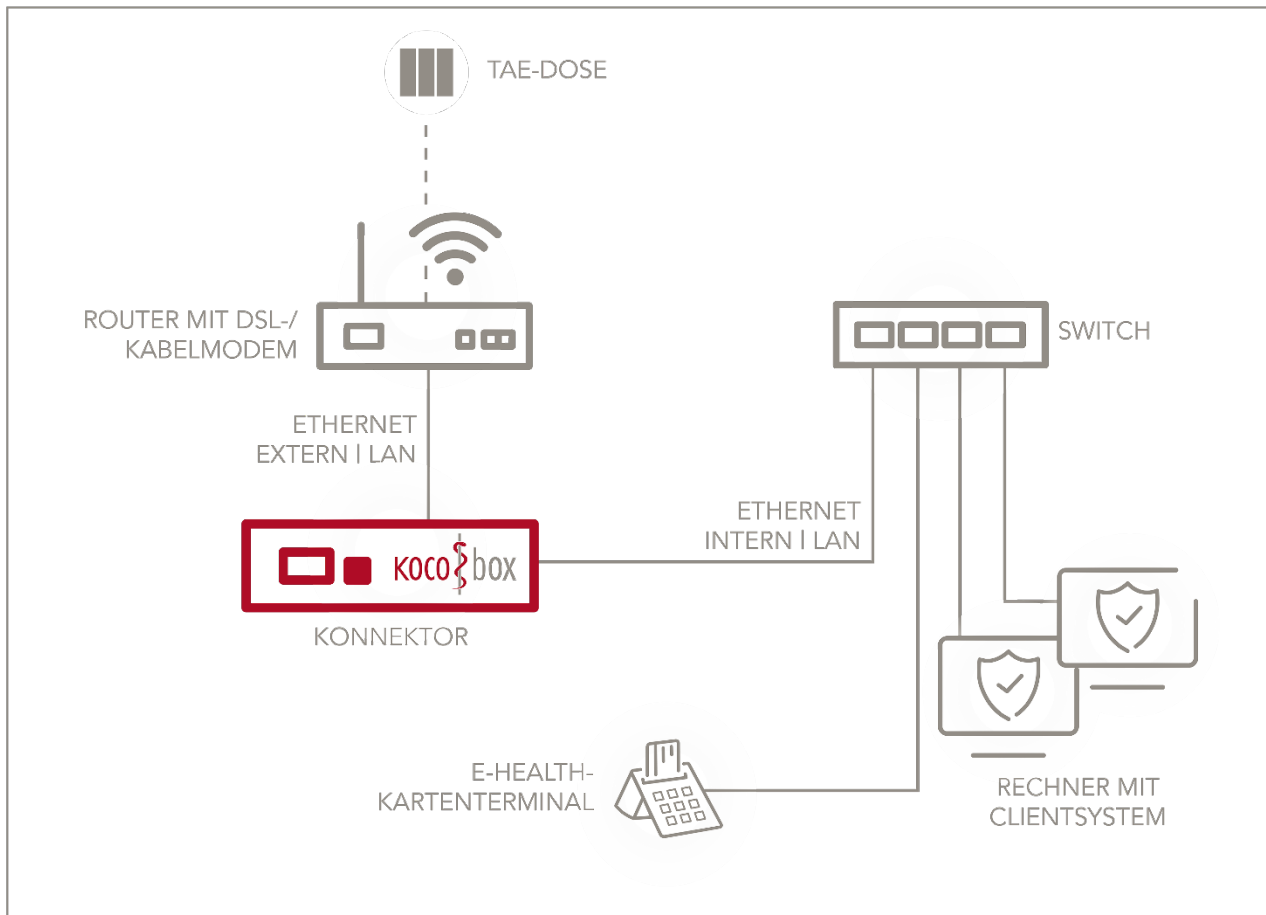


Abbildung 24: Serielle („in Reihe“) Anbindung der KoCoBox MED+

Technische Anbindung der KoCoBox MED+ „in Reihe“:

- Verbinden Sie die WAN-Schnittstelle der KoCoBox MED+ mittels CAT5e Netzwerkkabel mit Ihrer Internetanbindung.
- Verbinden Sie die LAN-Schnittstelle der KoCoBox MED+ mittels CAT5e Netzwerkkabel mit dem lokalen Netz, in dem sich Clientsystem und Kartenterminal befinden.
- Schalten Sie die miteinander verbundenen Geräte ein, indem Sie sie an das Stromnetz anschließen. Das System der KoCoBox MED+ fährt hoch.

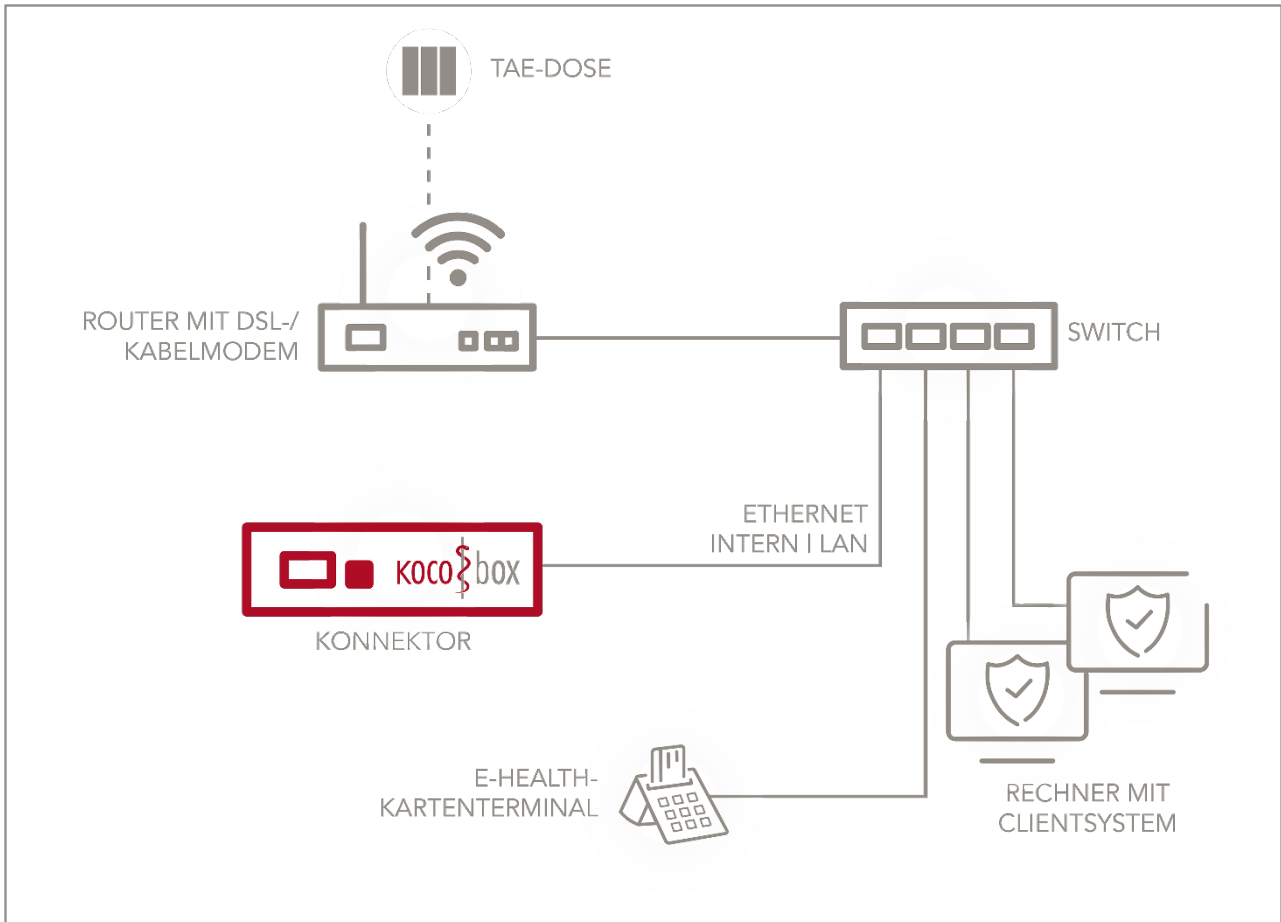


Abbildung 25: Parallele Anbindung der KoCoBox MED+

Technische Anbindung der KoCoBox MED+ ‚parallel‘:

- Verbinden Sie die LAN-Schnittstelle der KoCoBox MED+ mittels Netzkabel mit dem Netz, das als lokales Netz des Endkunden verwendet wird (Clientsystem, Kartenterminals).
- Schalten Sie die miteinander verbundenen Geräte ein, indem Sie sie an das Stromnetz anschließen. Das System der KoCoBox MED+ fährt hoch.



Hinweise:

- Der Systemstart nach dem ersten Einschalten der KoCoBox MED+ dauert ca. 10 Minuten.
- Wenn andere Kabel/Stecker, wie z.B. ein ISDN-Kabel, oder ein falsches Endgerät verwendet werden, kann keine Verbindung aufgebaut werden.
- Ob eine Verbindung steht (ein Port belegt ist), kann man am Display³⁰ erkennen.
- Falsche Anschlüsse werden nicht erkannt / angezeigt. Sofern die inkorrekte Netzwerkverbindung nicht Annahmen der Sicherheit der Umgebung umgehen (z.B. keine Verbindung zwischen WAN und LAN neben dem Konnektor), gibt es lediglich eine funktionale Einschränkung.

³⁰ Siehe die Abbildung der Standardansicht des KoCoBox MED+ Displays im folgenden Abschnitt.

6 Display

Im Betrieb zeigt das Display folgende Ansichten:

- die Standardansicht im Normalbetrieb
- Meldungen zu Fehlerzuständen mit Schweregrad³¹ **Error** und/oder **Fatal**; letzterer indiziert einen kritischen Betriebszustand³²

6.1 Standardansicht

Nach dem Systemstart der KoCoBox MED+ erscheint – bei einer parallelen Anbindung – die folgende Standard-Displayansicht:



Abbildung 26: Display der KoCoBox MED+ (G3)



Abbildung 27: Display der KoCoBox MED+ (G4)

Aufbau und Inhalt des Displays:

- obere Statusleiste (einzeilig, helle Schrift auf dunklem Hintergrund): *KoCoBox MED+* und aktuelle Uhrzeit
- Mittelfeld (fünfzeilig, dunkle Schrift auf hellem Hintergrund): *KoCo Connector*
- untere Statusleiste (zweizeilig, helle Schrift auf dunklem Hintergrund): Statusinformationen zu den einzelnen Verbindungen (TI, SIS, WAN, LAN)



Stellen Sie den Kontrast des Displays so ein, dass die Hinweise auf dem Display gut zu lesen sind.³³

³¹ Es gibt die Schweregrade Info, Warning, Error, Fatal; siehe [gemSpec_Kon], S. 34 ff.

³² Siehe [gemSpec_Kon], S. 33 ff.

³³ Zum Vorgehen siehe weiter unten.

Symbolik des Displays (von links nach rechts):

- VPN Status TI und SIS:
 - leeres Quadrat = keine Verbindung konfiguriert
 - ausgefülltes Quadrat = Verbindung konfiguriert
 - leere Raute = keine sichere Verbindung zur TI / zum SIS
 - ausgefüllte Raute = sichere Verbindung zur TI / zum SIS
- Link-Status für das WAN / die LAN-Schnittstelle:
 - ausgefülltes Quadrat = verbunden
 - leeres Quadrat = getrennt



Scheitert der Systemstart, erscheint auf dem Display eine Meldung. Zudem wird die Diagnose mit Fehlercode angezeigt.³⁴

6.1.1 Menüstruktur

Über den Button OK gelangen Sie von der Standard-Displayansicht aus in das Hauptmenü der KoCoBox MED+.

Diese enthält vier Menüpunkte:

- 1. Status
- 2. Betriebszustand
- 3. Informationen
- 4. Versionen

Die folgende Übersicht zeigt die Menüstruktur mit Hauptmenü, Untermenü, Unterpunkten (bzw. Infos) sowie Infos (bzw. Befehlen).

³⁴ Mehr dazu finden Sie im Kapitel Sicherheitsrelevante Szenarien.

Allgemeine Menüstruktur

Beachten Sie die Darstellungshinweise:

- Text erscheint auf dem Display,
- ausführbare(r) Funktion/Befehl,
- jeweils aktuell gültige Information wird angezeigt

| Hauptmenü | Untermenü | Unterpunkt / Info | Info / Befehl |
|-----------|----------------------------|---|--|
| Hauptmenü | | | |
| 1. Status | | | |
| | 1. VPN | TI: Aktiviert/Deaktiviert SIS: Aktiviert/Deaktiviert | |
| | 2. Netzwerk | LAN 1: Aktiv/Inaktiv WAN: Aktiv/Inaktiv | |
| | 3. Konfiguration | 1.WAN-Konfig. 2.LAN-Konfig. | Status: Aktiviert/Deaktiviert Typ: Dynamisch/Statisch |
| | | | IP-Adresse: XXX.XXX.X.XXX Netzmaske: XX.XXX.X.X Gateway: XXX.XXX.X.X |
| | | 3.Displaykontrast. ³⁵ | Gering Mittel Hoch |
| | | 4.Werksreset | Nein Ja |
| | 4. Neustart. ³⁶ | Neustart? | Nein Ja |

³⁵ Die aktuelle Einstellung ist hier mit einem dunklen Balken unterlegt.

³⁶ Die Voreinstellung Nein ist hier mit einem dunklen Balken unterlegt.

| Hauptmenü | Untermenü | Unterpunkt / Info | Info / Befehl |
|----------------------------------|--------------------------------|----------------------|---------------|
| 2. Betriebszustand ³⁷ | | | |
| | 1. Fehlerzustandsmeldung Nr. 1 | | |
| | Status: ok / krit. | | |
| | 2. Fehlerzustandsmeldung Nr. 2 | | |
| | Status: ok / krit. | | |
| | 3. Fehlerzustandsmeldung Nr. 3 | | |
| | Status: ok / krit. | | |
| | (...) | | |
| 3. Informationen | | | |
| | 1. Produkt | Produktinfo: | |
| | | Produktname: | |
| | | Name des Produkts | |
| | | Hersteller: | |
| | | Name des Herstellers | |
| | | Produkttyp: | |
| | | Name des Produkttyps | |
| | 2. Datum und Uhrzeit | Datum & Uhrzeit: | |
| | | XX.XX.XX YY:YY | |
| 4. Versionen | | | |
| | Version: | | |
| | Firmwareversion: | | |
| | X.Y.Z | | |
| | Hardwareversion: | | |
| | X.Y.Z | | |
| | Produkttypversion: | | |
| | X.Y.Z | | |

³⁷ Auf dem Display werden alle Fehlerzustandsmeldungen aus der Fehlerzustandsliste mit jeweiligem Status aufgelistet: ‚ok‘ bedeutet, dass der Fehlerzustand nicht eingetreten ist, ‚krit.‘ bedeutet, der Fehlerzustand ist eingetreten. Siehe dazu in den gematik-Spezifikationen: TAB_KON_503 Betriebszustand_Fehlerzustandsliste

6.1.2 Navigationslogik des Steuermenüs

Man bedient das textbasierte Steuermenü der KoCoBox MED+ über die Steuer-Buttons an der Frontseite.

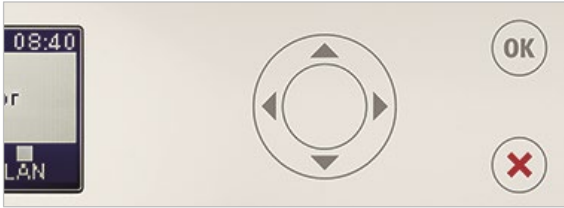


Abbildung 28: Front der KoCoBox MED+ (G3) mit Display und Steuer-Buttons - Ausschnitt

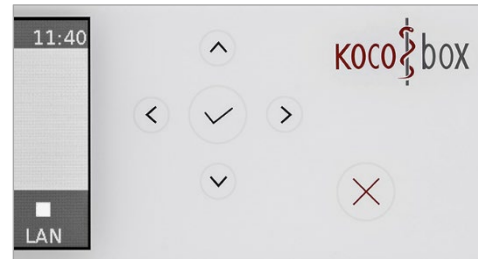


Abbildung 29: Front der KoCoBox MED+ (G4) mit Display und Steuer-Buttons - Ausschnitt

- Mit OK (G3) / Häkchen (G4) gelangen Sie von der Standardansicht in das Hauptmenü der KoCoBox MED+. Über die Steuer-Buttons oben/unten navigieren Sie in den Zeilen des Hauptmenüs entsprechend.
- Der jeweils ausgewählte Menüpunkt ist mit einem dunklen (G3) / roten (G4) Balken hinterlegt. Ist das untere Ende erreicht, springt der Balken wieder auf die erste Zeile nach oben.
- Für den Aufruf eines Menüpunkts betätigen Sie den Button OK (G3) / Häkchen (G4).
- Im mittleren hellen Anzeigenfeld werden in maximal fünf Zeilen Informationen ausgegeben: Unter der Titelzeile, die dem Menüpunkt entspricht, folgen maximal vier Zeilen mit (nummerierten) Einträgen bzw. (abgekürztem) Text.
- Die aktuell ausgewählte Zeile ist jeweils dunkel (G3) / rot (G4) unterlegt, wenn sich darunter eine weitere Ebene mit Informationen/Befehlen befindet (= auswählbarer Eintrag). Fehlt die Unterlegung, gibt es keine weitere Informationsebene mehr.
- Die Folgeansicht trägt den Titel dieses ausgewählten Untermenüs. Darunter folgt die Darstellung der entsprechenden Informationen.
- Sofern ein Eintrag über mehr als vier Zeilen geht bzw. eine Liste mehr als vier Zeilen hat, erscheint rechts oben in der Titelzeile ein kleiner schwarzer Pfeil nach unten. Sofern die Einträge auswählbar sind, wird der Display-Inhalt erst beim Erreichen des unteren/oberen Endes der Liste verschoben; die verborgenen Einträge werden erst angezeigt, wenn das untere/obere Listenende erreicht ist.
- Haben ein Eintrag bzw. eine Liste mehr als acht Zeilen, so erscheinen nach einmaligem Betätigen des Steuer-Buttons unten rechts oben in der Titelzeile zwei kleine schwarze Pfeile nach oben und nach unten. Der Steuer-Button kann so oft gedrückt werden, bis das Ende der Liste erreicht wird. Auf dem Display erscheint dann rechts oben in der Titelzeile ein kleiner schwarzer Pfeil nach oben. Dies zeigt, es gibt keine weiteren Informationen mehr.
- Gibt es keine weiterführenden Einträge, verschiebt sich die Darstellung auf dem Display sofort pro Druck des Buttons unten/oben um eine Displayansicht unten/oben.

6.2 Fehlerzustandsanzeige

Treten ein oder mehrere Fehlerzustände auf, die den Schweregrad **Error** bzw. **Fatal** haben, so werden diese direkt auf dem Display der KoCoBox MED+ angezeigt.

Die Fehlerzustandsanzeige am Display ist wie folgt aufgebaut:

- Die Titelzeile zeigt in Spitzklammern <Error (1)>; bei mehreren Fehlerzuständen sind die Fehler aufsteigend nummeriert.
- Die folgenden drei Zeilen geben eine abgekürzte Fehlerbeschreibung, die letzte Zeile eine Handlungsanweisung.

Man navigiert darin wie folgt:

- Über den Steuer-Button *rechts*/*links* wechselt man jeweils zur jeweils nächsten Fehlerzustandsmeldung. Diese ist jeweils nummeriert. Ist keine Fehlerzustandsmeldung mehr vorhanden, erscheint die Standardansicht des Displays.
- Wird bei einer angezeigten Fehlerzustandsmeldung auf den Button **OK** gedrückt, so kommt man zum Hauptmenü. Dort ist der Hauptmenüpunkt *Status* dunkel unterlegt.
- Sofern keine weitere Aktivität im Hauptmenü erfolgt, springt die Anzeige nach kurzer Zeit automatisch zurück zur ursprünglich angezeigten (ersten) Fehlerzustandsmeldung.
- Dies gilt auch, wenn man die Standardansicht der KoCoBox MED+ aufgerufen hatte.



Folgen Sie bei angezeigten Fehlerzuständen auf dem Display bitte unverzüglich den Handlungsanweisungen.

7 Inbetriebnahme des Konnektors

Die Inbetriebnahme des Konnektors umfasst einerseits vorbereitende Schritte für den administrativen Zugang zur KoCoBox MED+ und andererseits die Herstellung der Grundkonfiguration für den sicheren Zugang zur Telematikinfrastruktur in Abschnitt 7.4, gefolgt von der Konfiguration des Anwendungskonnektors in Abschnitt 7.5 und der Fachmodule in Abschnitt 7.7. Für funktionsübergreifende Konfigurationsaufgaben steht weiterhin ein Konnektormanagement zur Verfügung, wie in Abschnitt 7.6 beschrieben.

Die KoCoBox MED+ unterstützt Maßnahmen zur Gewährleistung einer Mandantenfähigkeit. Diese wirken sich auf die Zusammenarbeit mit Kartenterminals und Karten sowie auf den Systeminformationsdienst aus. Bestimmte Funktionen und deren Konfiguration sind folglich an eine Mandantenzuordnung gebunden, während globale Konfigurationsparameter mandantenübergreifend wirksam werden³⁸. Die Definition von Mandanten ist Teil der Konfiguration des Infomodells, wie in Abschnitt 7.6.2 dargestellt.



Vor Konfigurationsänderung einer globalen Funktion (beispielsweise für die Aktivierung/ Deaktivierung der automatischen Aktualisierung), von der alle Mandanten betroffen sind, hat der Administrator die Zustimmung aller Mandanten einzuholen.

Um den Konnektor sicher in Betrieb nehmen zu können, ist eine initiale Konfiguration erforderlich. Diese erfolgt über die browserbasierte Managementschnittstelle der KoCoBox MED+.

Dafür loggen Sie sich über einen sicheren Zugang als Super-Administrator³⁹ ein, vergeben ein persönliches Passwort, spielen eine aktuelle, gültige Trust-service Status List (TSL) des aktuellen Vertrauensraums der TI sowie eine CRL ein, führen bei Bedarf ein Softwareupdate durch und geben systematisch die (Grund-) Einstellungen ein bzw. übernehmen die per Werkskonfiguration vorhandenen Voreinstellungen. Nach dem Pairing eines Kartenterminals⁴⁰, dem Bearbeiten des Informationsmodells sowie der Registrierung beim Zugangsdienstprovider ist die initiale Konfiguration des Konnektors abgeschlossen.



Für den Zugang zur Managementschnittstelle – der Administrationsoberfläche für den Konnektor – benötigen Sie einen **aktuellen** Browser. Details dazu finden Sie unten im Abschnitt Bereitstellung des Web-Browsers.



Stellen Sie im Vorfeld der Inbetriebnahme des Konnektors sicher, dass auf dem für den Zugang zur Managementschnittstelle genutzten Netzwerkrechner einer der oben genannten Web-Browser installiert ist.



Bei der Auslieferung oder nach einem Werksreset wird die LAN-Konfiguration komplett auf DHCP gesetzt, so dass die IP-Einstellungen automatisch von einem DHCP-Server in Ihrem Netzwerk bezogen werden. Die WAN-Einstellungen sind ebenfalls auf DHCP eingestellt.



Stellen Sie sicher, dass in Ihrem LAN ein DHCP-Server zur Verfügung steht. Andernfalls bekommt der Konnektor keine IP-Adresse zugewiesen und ist nicht im Praxisnetzwerk erreichbar.⁴¹

³⁸ Es ist davon auszugehen, dass alle Änderungen von Konfigurationsparametern außerhalb des Kartendienstes globale Auswirkungen besitzen. Änderungen im Infomodell betreffen potenziell ebenfalls andere Mandanten. Daher ist eine Abstimmung mit allen Mandanten für die meisten Konfigurationsänderungen der KoCoBox MED+ angebracht.

³⁹ Siehe im Detail zu den verschiedenen Benutzerrollen der KoCoBox MED+ und ihren Bezeichnungen im System den Abschnitt Benutzerverwaltung. Zur besseren Lesbarkeit des Fließtextes werden die Rollenbezeichnungen ausgeschrieben.

⁴⁰ Hinweis: Momentan können Cherry-Tastaturen (Modell G87-1505), Cherry ST-1506-Kartenterminals und Ingenico Orga-6141-Kartenterminals als Hardware-Komponenten verwendet werden.

⁴¹ Im Fall der Nichtvergabe der IP siehe Kapitel 7.1.

Bereitstellung des Web-Browsers

Die browserbasierte Managementschnittstelle der KoCoBox MED+ kann unter verschiedenen Betriebssystemen angesprochen werden. Der Hersteller empfiehlt als Webbrowser Mozilla Firefox. Dieser wird für die Betriebssysteme Windows (ab Microsoft Windows 10), Linux und macOS (ab Version 10.9) bereitgestellt. Firefox ist in seinem Zusammenspiel mit der KoCoBox MED+ qualitätsgesichert. Eine Übersicht der Betriebssysteme mit Browser-Downloadpunkten zeigt Tabelle 2.

Weitere Browsertypen sind unter Umständen ebenfalls geeignet. Für eine sichere und vollständige Funktion derartiger Browser zur Administration der KoCoBox MED+ kann jedoch keine Gewährleistung übernommen werden.

| Betriebssystem | Browser | Verfügbarkeit, Versionseinschränkungen |
|----------------|-----------------|--|
| Windows | Mozilla Firefox | <p><i>installierbare Version:</i> https://www.mozilla.org/firefox/</p> <p><i>portable Version:</i> https://portableapps.com/de/apps/internet/firefox_portable/</p> |
| macOS, iOS | Mozilla Firefox | <p><i>installierbare Version:</i> https://www.mozilla.org/firefox/ dort das Produkt „Firefox für Desktop“ auswählen, unter „Download-Optionen und weitere Sprachen“ mit der Auswahl Installationsprogramm „macOS“ bzw. mit der Auswahl Browser „iOS“ (für iPad)</p> <p><i>Die Verwendung portabler Versionen empfehlen wir aktuell nicht, da diese überwiegend in älteren Versionsständen angeboten werden.</i></p> |
| Linux | Mozilla Firefox | <p><i>installierbare Version:</i> https://www.mozilla.org/firefox/ dort das Produkt „Firefox für Desktop“ auswählen, unter „Download-Optionen und weitere Sprachen“ mit der Auswahl „Installationsprogramm Linux 64-bit oder Linux 32-bit“</p> <p><i>Die portable Version ist abhängig von der jeweiligen Linux-Distribution – beispielhaft ist dies für Ubuntu bzw. dessen Derivate:</i> https://wiki.ubuntuusers.de/Portable_Firefox/</p> |

Tabelle 2: Übersicht der Browser-Downloadpunkte

7.1 Vorbereitungen

Stellen Sie sicher, dass das Gerät entsprechend den vorherigen Beschreibungen korrekt angebunden und die Stromversorgung gewährleistet ist.

Die initiale Konfiguration des Konnektors erfolgt über eine browserbasierte Managementschnittstelle der KoCoBox MED+. Die zugehörige Verbindung wird mittels TLS geschützt. Diese TLS-Verbindung nutzt die serverseitige Authentisierung mittels eines durch den Konnektor an den Browser bereitgestellten Zertifikats.



Der Administrator ist für die Gewährleistung der netzwerktechnischen Verbindungssicherheit verantwortlich.

Für die Inbetriebnahme betrifft dies besonders die Vertrauenswürdigkeit der Verbindung zum Konnektor. Hierzu muss die Authentizität der Verbindung zur Managementschnittstelle des Konnektors geprüft werden. Das ist durch die Prüfung der Gültigkeit des durch den Konnektor an den Browser gesendeten TLS-Zertifikats gegen die Zertifikatskette der ausstellenden Instanzen (CAs) möglich.



Diese Prüfung ist nach einer Laufzeitverlängerung der Konnektorzertifikate zu wiederholen, siehe Abschnitt **Laufzeitverlängerung**. Im Fall einer erfolgreichen Prüfung stellt dies sicher, dass eine zuvor bestehende Authentizität der Verbindung auch weiterhin gegeben ist.



Der Administrator hat hier zu kontrollieren, ob die TLS-Verbindung zwischen seinem Netzwerkrechner und dem Konnektor korrekt aufgebaut wurde. Dies umfasst die Prüfung des vom Konnektor übermittelten Zertifikats anhand der Darstellung im Web-Browser. Lassen Sie sich dafür das Zertifikat anzeigen und vergleichen Sie die angezeigte Zahl in der Zeile *Allgemeiner Name (CN)* mit der in den Lieferdokumenten angegebenen Seriennummer des Konnektors. **Nur wenn diese übereinstimmen, dürfen Sie die Credentials (Benutzername und Passwort) für die Anmeldung am Konnektor im Browser eingeben!**

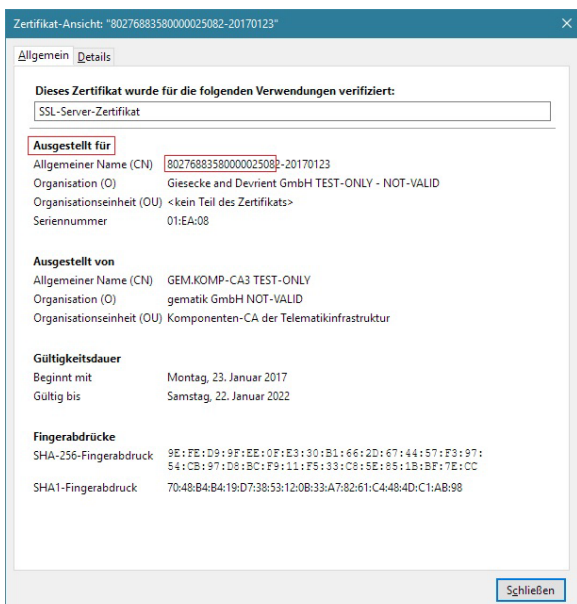


Abbildung 30: Beispiel für TLS-Zertifikatsanzeige im Browser mit Seriennummer



Bitte beachten Sie, dass die angezeigte Zahl im Browser um ein Zeichen länger ist als die Seriennummer des Konnektors. Diese ist **genau 19 Zeichen** lang.

Die entsprechenden Zertifikate sind auf der von der gematik bereitgestellten Seite <https://download.tsl.ti-dienste.de/> (PU) in ihrer jeweils gültigen Version veröffentlicht und können von dort über eine reguläre TLS-Verbindung authentisiert heruntergeladen werden. Diese Verbindung ist vertrauenswürdig durch das gültige, von D-Trust ausgestellte Zertifikat (siehe die folgende Abbildung).

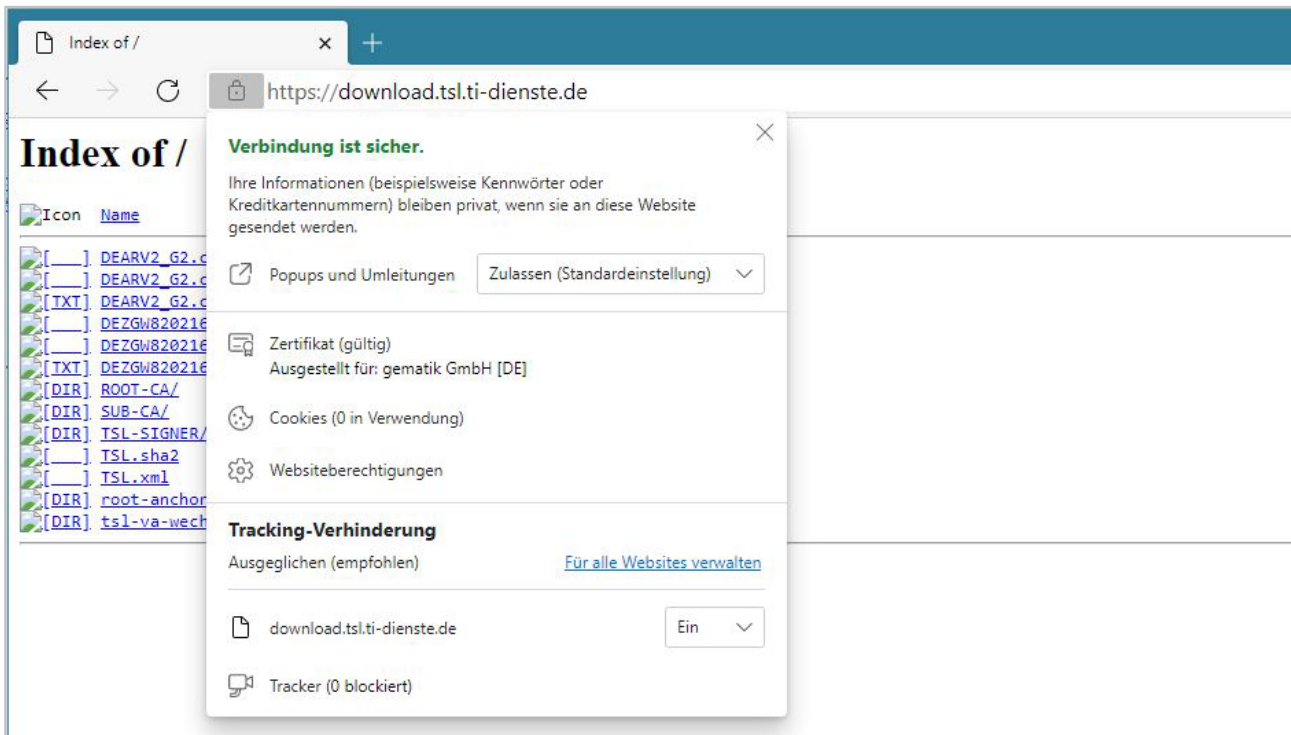


Abbildung 31: Downloadpunkte für vertrauenswürdige PKI-Elemente der PU

Aktuell stellen die Zertifikate GEM.RCA1 bis GEM.RCA8 (Root-CA-Zertifikate für RSA und ECC) sowie GEM.KOMP-CA1 bis GEM.KOMP-CA8 (Komponenten-CA-Zertifikate für RSA und ECC) die zur Prüfung notwendigen vertrauenswürdigen Zertifikate dar.⁴²

Nach dem Herunterladen sind die Zertifikate in den durch den Browser/das System genutzten Zertifikatsstore zu importieren. Anschließend kann mit Hilfe der Browsermechanismen oder durch das System bereitgestellten Mechanismen die Vertrauenswürdigkeit des TLS-Konnektorzertifikats geprüft werden, wie beispielhaft in der folgenden Abbildung dargestellt.

⁴² Stand: März 2024

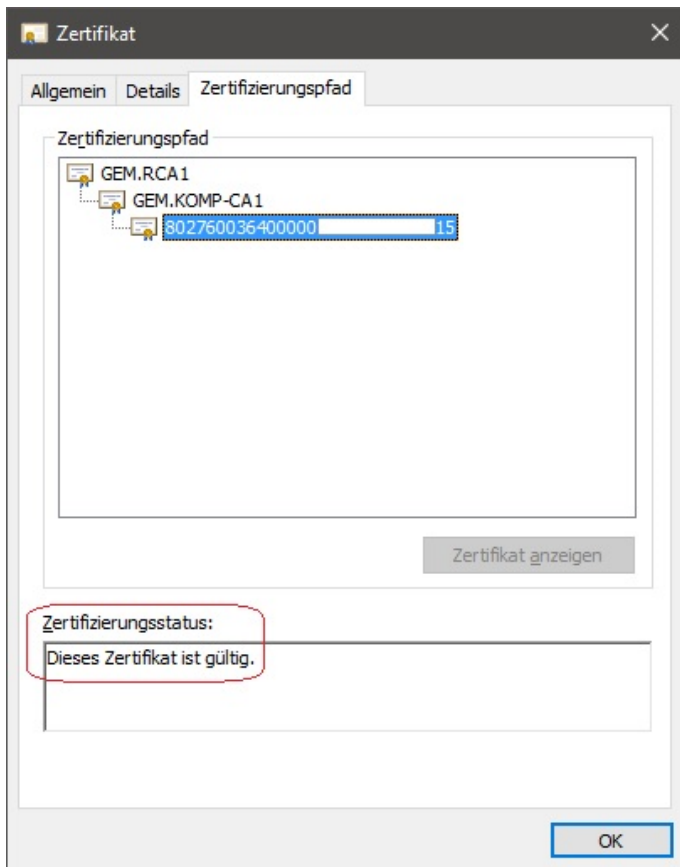


Abbildung 32: Gültige Zertifikatskette

Eventuell akzeptiert der Browser das Zertifikat nicht direkt, da die in das TLS-Konnektorzertifikat eingebettete Information für den Antragsteller (Subject) auf dem Zielsystem nicht zur Domänenbezeichnung bzw. IP-Adresse der TLS-Verbindungspartner passt:



SSL_ERROR_BAD_CERT_DOMAIN Sichere Kommunikation mit der Gegenstelle ist nicht möglich:
Angeforderter Domainname stimmt nicht mit dem Zertifikat des Servers überein.



Dann kann der Administrator auf Grund der geprüften Vertrauenskette für dieses Konnektorzertifikat eine Ausnahme im Browser einrichten.

Halten Sie die folgenden Informationen zur Konfiguration sowie zur Registrierung des Konnektors beim Registrierungsservice bereit:

- ICCSN⁴³ der SM-B⁴⁴ (auf der Karte aufgedruckt oder über den Kartendienst der Managementschnittstelle einsehbar)
- Nummer des Vertrags (ContractID) mit dem Zugangsdienstprovider (ZGDP)⁴⁵
- Informationen zur lokalen Netzinfrastruktur (z.B. die IP-Adresse des Gateways)
- eine gültige TSL oder die URL eines öffentlich zugänglichen Download-Punkts für die TSL⁴⁶ (u.a. für den VPN-Tunnel-Aufbau und die Inbetriebnahme von Kartenterminals)
- eine gültige CRL oder die URL eines öffentlich zugänglichen Download-Punkts für die CRL⁴⁶



Der Import einer gültigen TSL und CRL ist zu Beginn der initialen Konfiguration des Konnektors erforderlich. Der Ablauf wird detailliert im Abschnitt *Zertifikatsdienst* erläutert.

Binden Sie die KoCoBox MED+ wie folgt in das lokale Netz ein:

1

Starten Sie den Netzwerk-Rechner, über dessen Browser Sie die Managementschnittstelle der KoCoBox MED+ aufrufen und der per LAN mit dem Konnektor verbunden ist.



Bitte beachten Sie dabei: Der Netzwerk-Rechner muss für dasselbe Netz konfiguriert sein wie die KoCoBox MED+.

2

Rufen Sie über das Display die LAN-IP des Konnektors auf.⁴⁷ Da der DHCP-Client per Voreinstellung aktiviert ist, holt sich der Konnektor vom DHCP-Server seine LAN-IP. Sie wird auf dem Display der KoCoBox MED+ angezeigt.

3

Tragen Sie diese IP-Adresse der KoCoBox MED+ (<https://<IP-KON>:9443/administration/start.htm>) in die Browserzeile ein.



Für den Fall, dass der Konnektor nach 30 Sekunden noch keine IP-Adresse bezogen hat (kein DHCP-Server im internen Netz verfügbar), wird ihm die Fallback-Adresse des DHCP-Clients gemäß RFC⁴⁸ zugewiesen. Diese IP-Adresse wird **nicht** aus dem Praxisnetz sein. Sie ist auch über das Display ablesbar und kann ebenfalls wie oben beschrieben für den Zugang zur Managementschnittstelle genutzt werden.



Die Managementschnittstelle kann **ausschließlich** über <https://> erreicht werden. Über dieses Interface erfolgt **immer** die Zugangskontrolle mit der Authentifizierung des Benutzers.

⁴³ die weltweit eindeutige Identifikationsnummer eines Chipmoduls einer Smartcard

⁴⁴ Die SM-B adressiert sowohl eine echte SMC-B als auch eine in einem HSM-B enthaltene virtuelle SMC-B. Siehe [gemSpec_Kon], S. 28

⁴⁵ Diese Nummer bekommt der Betriebsstättenverantwortliche von seinem ZGDP, mit dem er einen Vertrag für den Zugang zur TI abgeschlossen hat.

⁴⁶ Diese kann getrennt für RSA- und ECC-Algorithmennutzung heruntergeladen werden. Bei RSA sind dies für TSL bzw. CRL folgende Adressen: <https://download.tsl.ti-dienste.de/> (Dateiname: TSL.xml) bzw. <http://download.crl.ti-dienste.de/crl/> (Dateiname: vpnk-ca1.crl). Bei ECC sind dies folgende Adressen: <https://download.tsl.ti-dienste.de/ECC/> (Dateiname: ECC-RSA_TSL.xml) bzw. <http://download.crl.ti-dienste.de/crl/> (Dateiname: vpnk2-ca.crl).

⁴⁷ Im Hauptmenü unter Status / Konfiguration / LAN-Konfig.

⁴⁸ Siehe [RFC3927]; Default-Adresse aus: 169.254.0.0/16

7.2 Administrator-Passwort

Bei der Auslieferung der KoCoBox MED+ sind die initialen Zugangsdaten zur Managementschnittstelle (Name und Passwort) voreingestellt:

- Name: koko-root
- Passwort: InItal4StartUp!⁴⁹

Geben Sie diese im Login-Fenster ein und bestätigen Sie dies über den Button Anmelden.



Dieser Administrator ist mit der Rolle *Super-Administrator (SuperAdmin)* angelegt. Er kann weder angepasst noch gelöscht werden. Solange nur ein Benutzer in der Rolle *SuperAdmin* existiert, kann dieser weder angepasst noch gelöscht werden.

KoCoBox-Managementsschnittstelle

Name:

Passwort:

Anmelden

Abbildung 33: Login-Fenster der KoCoBox MED+ Managementschnittstelle



Beachten Sie für die weiteren Schritte die folgenden Sicherheitshinweise für die sichere Administration der KoCoBox MED+:

- Das Auslieferungspasswort (= Einmalpasswort⁵⁰) **muss** beim ersten Login sofort geändert werden. Deswegen ist es **zwingend notwendig**, dass Sie **zuerst ein persönliches Passwort vergeben**.
- Dieses persönliche Passwort darf **nur Ihnen allein** bekannt sein. Behandeln Sie es deshalb bitte **streng vertraulich**.
- Administratoren der KoCoBox MED+ können ihr persönliches Passwort im Bereich *mein Profil* jederzeit ändern. Passwörter werden generell **nie im Klartext** angezeigt.
- Ändern Sie Ihr persönliches Passwort **sofort**, wenn es einer zweiten Person bekannt geworden ist oder Sie einen Verdacht dahingehend haben. Prüfen Sie in dieser Situation zusätzlich die Protokolle der KoCoBox MED+ darauf, ob Einstellungen am Konnektor unberechtigt geändert wurden. Kontaktieren Sie gegebenenfalls einen Servicetechniker für weitere Maßnahmen.
- Allgemein ist der Zugang zur Managementschnittstelle nur **autorisierten Personen** gestattet, die sich dort mittels persönlichen Passworts authentisieren.

⁴⁹ Bitte beachten Sie: Hier sind der erste und dritte Buchstabe ein großes „i“.

⁵⁰ Dies wird einmalig nur für die Erstanmeldung an der Managementschnittstelle vergeben.

Auf der Managementschnittstelle können zeitgleich mehrere Benutzer eingeloggt sein.



Generell ist es jedoch ratsam, nur **einen** Administrator einzuloggen. Andernfalls könnten Konfigurationsänderungen nicht korrekt abgespeichert werden.



Beachten Sie, dass Anmeldungen mit identischen Benutzerparametern zu einer Übernahme der Administrationssitzung im Browser führen. Bei Verwendung eines tab-gestützten Browsers kann es jedoch sein, dass Sie sich weiterhin innerhalb einer Sitzung bewegen.

Änderung des Auslieferungspassworts

KoCoBox-Managementschnittstelle

Sie müssen ein neues Passwort wählen. Beachten Sie dabei die Passwort-Policy!

Das Passwort muss zwischen 8 und 20 Stellen lang sein und muss mindestens 3 Zeichenklassen (Kleinbuchstaben, Großbuchstaben, Ziffern, Sonderzeichen (!@#\$%^&* _ =+ - /)) aufweisen. Der Benutzername darf darin nicht vorkommen, auch nicht rückwärts geschrieben. Außerdem darf es nicht identisch sein mit einem der letzten 3 Passwörter.

altes Passwort:

neues Passwort:

neues Passwort bestätigen:

Abbildung 34: Persönliches Passwort vergeben

Nach der Eingabe der initialen Zugangsdaten gelangen Sie zum Fenster *Passwort ändern für Administrator*. Führen Sie die initiale Passwortänderung wie folgt durch:

1

Geben Sie im oberen Eingabefeld *altes Passwort* das Auslieferungspasswort ein.

2

Geben Sie anschließend Ihr **persönliches neues Passwort** ein und wiederholen Sie es korrekt.



Achten Sie darauf, dass Sie dabei **unbeobachtet** sind, notieren Sie es **nicht** an leicht zugänglichen Stellen und speichern Sie es **keinesfalls** auf Funktionstasten ab.



Beim Erstellen Ihres persönlichen Passworts beachten Sie bitte folgende Sicherheitshinweise:

- Die Länge muss mindestens 8 und kann maximal 24 Zeichen betragen.
- Verwenden Sie mindestens ein Zeichen aus den Zeichenklassen Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen. Diese sind wie folgt definiert:
 - Großbuchstaben: ABCDEFGHIJKLMNOPQRSTUVWXYZ
 - Kleinbuchstaben: abcdefghijklmnopqrstuvwxyz
 - Zahlen: 0123456789

- Sonderzeichen sind: !@#%&^™*_+=-/
■ Im Passwort **müssen** drei der vier Zeichenklassen enthalten sein.
■ Der Benutzername darf nicht enthalten sein (weder vor- noch rückwärts, unter Ignorierung der Groß-/Kleinschreibung).
■ Beim Vergeben eines neuen Passworts dürfen die letzten drei Passwörter nicht noch einmal verwendet werden.
■ Verwenden Sie keine trivialen Passwörter, einfache Namen oder Begriffe aus dem Wörterbuch – egal in welcher Sprache.
■ Verwenden Sie keine Passwörter, die eine persönliche Information (Vornamen, Familiennamen, Kosenamen, Geburtsdaten, Telefonnummern etc.) enthalten.
■ Verwenden Sie keine Anagramme, Zahlenfolgen wie 12345 oder Buchstabenfolgen wie abcde etc.
■ Einmalpasswörter haben die Länge von 20 Zeichen.



Der Konnektor initiiert in einem Zeitraum zwischen 30 und 360 Tagen einen Passwortwechsel beim nächsten Login.⁵¹



Verwenden Sie für mehr Sicherheit aus jeder Zeichenklasse mindestens ein Zeichen: Kombinieren Sie Zahlen und Sonderzeichen unter Einbeziehung von Groß- und Kleinbuchstaben. Erstellen Sie insgesamt ein möglichst langes Passwort.

3

Über **Passwort ändern** schicken Sie Ihr neues persönliches Passwort an die KoCoBox MED+. Sobald die Änderung erfolgreich war, erscheint eine entsprechende Meldung.

4

Melden Sie sich per **Abmelden-Funktion** (rechts oben) aus der Managementschnittstelle ab.

5

Loggen Sie sich mit dem Namen **koco-root** sowie Ihrem neuen persönlichen Passwort erneut in die Managementschnittstelle der KoCoBox MED+ ein.

6

Nach der korrekten Eingabe Ihres persönlichen Passworts gelangen Sie auf die Status-Seite der Managementschnittstelle.

Fehler beim Login



Für den Fall, dass Sie den Button **Passwort ändern** betätigen und eine ungültige oder falsche Kombination aus Namen und Passwort eingetragen ist, erscheint eine Fehlermeldung⁵².



Geben Sie in der Zeile *Namen* die korrekte Benutzerkennung (bei der Initialkonfiguration bzw. nach einem Werksreset: *koco-root*) und in der Zeile *Passwort* das korrekte Passwort (bei der Initialkonfiguration bzw. nach einem Werksreset: *InitialStartup!*) ein. Beachten Sie dabei Groß- und Kleinschreibung. Bestätigen Sie dies mit dem Button **Anmelden**.



Nach einem erfolglosen Anmeldeversuch gibt es eine **Verzögerung** von drei Sekunden, bis das Passwort für Ihre Benutzerkennung erneut eingegeben werden kann. Nach vier erfolglosen Anmeldeversuchen wird eine **einminütige Verzögerung** für erneute Passworteingaben aktiviert.

⁵¹ Die Voreinstellung umfasst 120 Tage.

⁵² Siehe Abbildung unten

Passwortänderung

Im Betrieb wird das Passwort wie folgt geändert:

- 1** Melden Sie sich im Login-Fenster mit Namen und altem Passwort an.
- 2** Über mein Profil gelangen Sie in das Eingabefeld für Ihr persönliches Benutzerprofil. Hier steht unter dem Button Passwort ändern die entsprechende Funktion zur Verfügung. Gehen Sie wie oben beschrieben vor.
- 3** Nach der erfolgreichen Passwortänderung gelangen Sie zurück zum Login-Fenster. Melden Sie sich dort mit Ihrem Namen und dem neuen Passwort an.



Aus Sicherheitsgründen prüft die KoCoBox MED+ bei einer Passwortänderung immer, ob das neu definierte Passwort bereits mit einem der letzten drei Passwörter übereinstimmt. Ist dies der Fall, erscheint in einem Dialogfenster die Aufforderung, ein **völlig neues Passwort** zu erstellen.



Setzt ein Administrator, der die entsprechenden Berechtigungen besitzt, das Passwort eines anderen Administrators um, so wird letzterer beim nächsten Einloggen in die Managementschnittstelle **gezwungen**, sein Passwort zu ändern, damit dieses **nur ihm persönlich** bekannt ist.

Fehler bei der Passwortänderung



Für die Fälle, dass Sie Passwort ändern klicken und Einträge fehlen, bei der Eingabe des neuen Passworts ein Schreibfehler unterlaufen ist oder das vermeintlich neue Passwort schon einmal verwendet wurde oder zu kurz ist, erscheint eine kurze Fehlermeldung ohne Angabe näherer Einzelheiten.⁵³

KoCoBox-Managementschnittstelle

Sie müssen ein neues Passwort wählen. Beachten Sie dabei die Passwort-Policy!

Das Passwort muss zwischen 8 und 20 Stellen lang sein und muss mindestens 3 Zeichenklassen (Kleinbuchstaben, Großbuchstaben, Ziffern, Sonderzeichen (!@#\$%^&* _+~/)) aufweisen. Der Benutzername darf darin nicht vorkommen, auch nicht rückwärts geschrieben. Außerdem darf es nicht identisch sein mit einem der letzten 3 Passwörter.

altes Passwort:

neues Passwort:

neues Passwort bestätigen:

Es ist ein Fehler bei der Passwortänderung aufgetreten!

Abbildung 35: Fehlermeldung bei falscher Passwordeingabe

⁵³ Die gilt sowohl für Fehler bei der initialen Konfiguration als auch für Fehler bei der Passwortänderung im Betrieb.



Löschen Sie ggf. die Fehleingabe(n) und tragen Sie sowohl das alte Passwort⁵⁴ als auch das neue persönliche Passwort korrekt neu ein. Beachten Sie dabei die Vorgaben zu Länge und Aufbau des Passworts. Bestätigen Sie das neue Passwort mit *Passwort ändern*.



Für den Fall, dass Sie ohne Einträge in die Felder *Neues Passwort* und *Wiederholen* getätigt zu haben auf *Anmelden* klicken, erscheint eine Fehlermeldung ohne Angabe näherer Einzelheiten.



Tragen Sie in beide Felder das neue, persönliche Passwort ein und bestätigen Sie es mit *Passwort ändern*.



Bitte beachten Sie: Sofern keine korrekten Eingaben gemacht werden können, müssen Sie, um auf das Login-Fenster der Managementschnittstelle zurückzukommen, den **Browser schließen** und wieder **neu öffnen**. Andernfalls werden Sie immer wieder zu diesem Passwortänderungsfenster zurückgeführt.

⁵⁴ Im Fall der Vergabe eines neuen persönlichen Passworts nach einem Werksreset ist dies das Initialpasswort (Auslieferungspasswort).

7.3 Aufbau und Semantik der Managementschnittstelle

Nach dem erfolgreichen Login mittels persönlichen Passworts erscheint die Status-Seite⁵⁵ der Managementschnittstelle. Das Navigieren innerhalb der Managementschnittstelle folgt der Logik eines Browsers: Die – thematisch untergliederten – Konfigurationsbereiche sind per Klick auf einen verlinkten Begriff aufrufbar.



Die Browser-Buttons sind für die Navigation innerhalb der Managementschnittstelle **nicht verwendbar!** Dafür muss das Navigationsmenü genutzt werden. Eine Aktualisierung per F5-Taste ruft die Status-Seite der Managementschnittstelle auf.



Konfigurationshinweis: In sämtlichen Konfigurationsbereichen erhalten Sie beim Mouseover (z.B. bei Überschriften, Feld- oder Zeilenbeschriftungen) einen **Tooltip** mit detaillierten Erklärungen und Sicherheitshinweisen.

| Zeit | Zustand | Typ | Schwere | Parameter |
|---------------------|--|-----------|---------|--|
| 20.11.2023 11:34:11 | OPERATIONAL_STATE/EC_OTHER_ERROR_STATE(2) | OPERATION | WARNING | Bedeutung = Protokollspeicher zu mehr als 80% gefüllt.; Protokoll = system:OP, system:SEC |
| 20.11.2023 11:34:14 | OPERATIONAL_STATE/EC_LOG_OVERFLOW | OPERATION | WARNING | Bedeutung = Wenn im Rahmen der Regeln für die rollierende Speicherung von Logging-Einträger älter als LOG_DAYS bzw. FM_cfmName>_LOG_DAYS sind, tritt der Fehlerzustand ein.; Protokoll |
| 20.11.2023 11:34:38 | OPERATIONAL_STATE/EC_TLS_Client_Certificate_Security | SECURITY | INFO | Bedeutung = Das für die Authentifizierung gegenüber dem Clientsystem konfigurierte Zertifikat h |

Abbildung 36: Aufbau der Managementschnittstelle am Beispiel der Status-Seite

Aufteilung der Bedienoberfläche

Die Managementschnittstelle besteht aus der Titelleiste, der Informationsleiste, der Navigationsspalte (links) und einem Anzeigebereich (rechts).

Die weiß unterlegte Titelleiste enthält links den Herstellernamen *KoCo Connector*, den Titel *KoCoBox- Managementschnittstelle*, die konfigurierten Verbindungen TI, SIS, WAN, LAN (analog zum Display) sowie rechts das Produkt-Logo als grafisches Element.

⁵⁵ Die auf der Status-Seite hinterlegten Informationen werden im Abschnitt Status beschrieben.



Abbildung 37: Titelleiste der KoCoBox MED+ Managementschnittstelle

Die dunkelgraue Informationsleiste enthält:

- links Informationen zum Benutzer, dem eingeloggten Administrator: neben seiner Benutzerkennung wird in eckigen Klammern seine Rolle angezeigt
- rechts die Anzeige des Session-Timeouts in Minuten:Sekunden; die letzten 30 Sekunden vor dem Ende der Session werden invertiert angezeigt
- rechts daneben die Funktion mein Profil, worüber man in das Profil des eingeloggten Administrators (u.a. mit Kontaktdaten sowie Passwortänderungs-Funktion) gelangt
- am rechten Rand die Funktion Abmelden, über die sich der aktive Administrator von der Managementschnittstelle ausloggen kann



Bitte achten Sie stets darauf, sich ordnungsgemäß von der Managementschnittstelle abzumelden.



Nach mehr als einstündiger Inaktivität (Session-Timeout) auf der Managementschnittstelle wird man vom System automatisch ausgeloggt. Es erscheint das Login-Fenster, über das Sie sich erneut anmelden können.⁵⁶

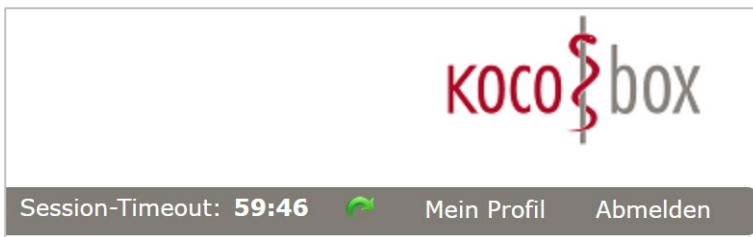


Abbildung 38: Anzeige des Session-Timeout

Über das  Reload-Symbol – oder über Interaktionen – kann der Session-Timeout zurückgesetzt werden.

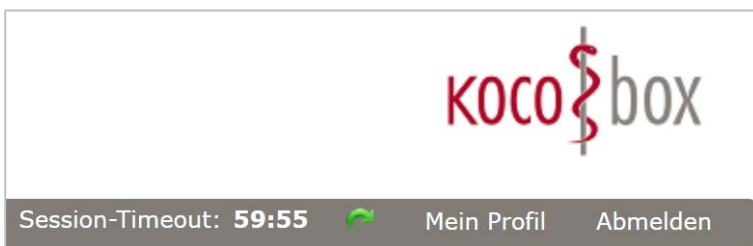


Abbildung 39: Session-Timeout zurücksetzen

Der Timer wird in den letzten 30 Sekunden vor Ablauf der Session invertiert angezeigt, um zu verdeutlichen, dass die Session demnächst endet.

⁵⁶ Beim erneuten Login werden Sie per Dialogfenster ggf. darauf hingewiesen, dass seit dem Ausloggen neue Einträge im Sicherheitsprotokoll aufgelaufen sind.



Abbildung 40: Invertierte Sekundenanzeige vor dem Ablauf der Session

Über die hellgrau unterlegte Navigationsspalte links erfolgt der Aufruf der einzelnen Konfigurationsbereiche für die (Sicherheits-)Einstellungen der KoCoBox MED+. Sie bestehen aus 20 Haupt-Kategorien, von denen 9 weitere Unterbereiche enthalten. Diese ruft man mittels Klick auf das Plus-Symbol vor dem jeweiligen Haupt-Kategorietitel auf. Ein Klick auf den verlinkten Begriff öffnet die Ansicht für die Einstellungsoptionen zum gewählten Unterbereich bzw. das Anzeigefenster für Informationen.

Haupt-Kategorien der Navigationsspalte mit Unterbereichen

- *Status*
- *Kartendienst*
- *Kartenterminaldienst*
- *Systeminformationsdienst*
- *Zertifikatsdienst* mit dem Unterbereich *CA-Import, Status verwendeter Zertifikate* und *Laufzeitverlängerung*
- *Protokollierungsdienst* mit den Unterbereichen *Sicherheitsprotokoll, Systemprotokoll* und *Performanceprotokoll*
- *LAN / WAN* mit dem Unterbereich *Firewall SIS*
- *DHCP*
- *VPN* mit dem Unterbereich *Registrierung*
- *Zeitdienst*
- *DNS*
- *Verwaltung* mit den Unterbereichen *Clientsysteme, Ex-/Import* und *Telematikdienste*
- *Fachmodul VSDM* mit den Unterbereichen *Systemprotokoll, Performanceprotokoll* und *Fehlerprotokoll*
- *Fachmodul AMTS* mit den Unterbereichen *Ablaufprotokoll, Performanceprotokoll* und *Fehlerprotokoll*
- *Fachmodul NFDM* mit den Unterbereichen *Ablaufprotokoll, Performanceprotokoll* und *Fehlerprotokoll*
- *Fachmodul ePA* mit den Unterbereichen *Ablaufprotokoll, Performanceprotokoll, Fehlerprotokoll* und *Telematikdienste*
- *Benutzerverwaltung*
- *Infomodell*
- *Aktualisierung* mit dem Unterbereich *Übersicht*
- *Signaturdienst*

Semantik

Im weiß unterlegten Anzeigefenster werden die Inhalte (Konfigurationsparameter) angezeigt. Unterschiedliche Inhaltsfelder sind mit dunkelgrauen Überschriftsbalken, die ggf. noch hellgraue Überschriftsbalken haben, voneinander abgegrenzt.








Die Eingabefelder sind für die manuelle Dateneingabe in der Regel einzeilig. Sie können an verschiedenen Stellen auch per Pull-Down-Menü gefüllt werden. Zudem werden Radiobuttons für das Ein-/Ausschalten, Aktivieren/Deaktivieren sowie für das Auswählen unter mehreren Optionen verwendet. Daneben stehen Konfigurationsfenster für weitere Einstellungen zur Verfügung. Diese werden per Button aufgerufen.







Anweisungen bzw. Informationen erscheinen weitestgehend in Tooltip-Texten, auch Meldungen bei erfolgreichen oder fehlerhaften Eingaben sind 'sprechend'.

Allgemein gilt für die Konfiguration:

- Die Eingabefelder sind weiß oder rosa hinterlegt. Letztere **müssen** ausgefüllt werden! Es erfolgt eine direkte logische Prüfung der Eingaben in jedem Eingabefeld. Nach erfolgreicher Eingabe erscheinen die Inhalte in schwarz/weiß.
- Die Eingabefelder sind ausfüllbar bzw. zeigen Voreinstellungen an, die man bei Bedarf ändern kann.
- In Dialogfenstern werden Meldungen, Hinweise oder Fragen angezeigt, die z.B. bestätigt oder verworfen werden.
- Über Windowsfenster werden lokale Verzeichnisse, z.B. für den Down-/Upload von Dateien, geöffnet.
- Der Tooltip-Text erscheint in weißer Schrift auf dunkelgrauem Hintergrund.
- Dunkelgraue Buttons, Beschriftungen oder Symbole bedeuten Aktivität, aktive Funktion.
- Hellgraue Buttons, Beschriftungen, Symbole oder Hintergründe bedeuten Inaktivität, deaktivierte Funktion.

Symbole

-  In den auf der Managementschnittstelle verwendeten Tabellen symbolisiert der grüne Stift die Bearbeiten-Funktion.
-  Der rote Kreis mit weißem Kreuz symbolisiert die Löschen-bzw. Verboten-Funktion.
-  Die beiden im Kreis angeordneten blauen Pfeile symbolisieren die Ändern-Funktion (z.B. PIN ändern).
-  Der Schlüssel mit Plus-Zeichen im grünen Kreis symbolisiert die Schlüsselerzeugen-Funktion für das Erzeugen eines Schlüssels.
-  Das 'i' im gelben Kreis symbolisiert den PIN-Status.
-  Das rote Warndreieck mit weißem Ausrufezeichen symbolisiert die Funktion PIN entsperren.
-  Der weiße Haken im grünen Kreis symbolisiert die Funktion PIN verifizieren.
Der schwarze Haken im umrandeten Quadrat symbolisiert die Default-Einstellung/Voreinstellung.

-  Der gebogene Pfeil nach rechts symbolisiert die Zurücksetzen-Funktion.
-  Die beiden gebogenen grünen rechts-links-Pfeile symbolisieren die Aktualisieren-Funktion.
-  Der kreisrunde hellblaue Pfeil symbolisiert die Aktualisierungsfunktion für Übersichtslisten.
-  Das ‚i‘ im blauen Kreis kennzeichnet eine Information im Dialogfenster.
-  Das weiße Fragezeichen im orangenen Kreis symbolisiert eine Frage im Dialogfenster.
-  Das schwarze Ausrufezeichen im gelben Kreis symbolisiert eine Warnung im Dialogfenster.

7.4 Grundkonfiguration des Konnektors

Im Folgenden wird die Grundkonfiguration des Netzkonnektors für die sichere Einbindung in die die TI erklärt. Die per Werkskonfiguration eingetragenen Werte sind vorgegeben.⁵⁷



Der Konnektor ist bei Auslieferung per Voreinstellung für die serielle Anbindung (,in Reihe') mit Nutzung des SIS konfiguriert.



Um die Übersichtlichkeit zu wahren, wird im vorliegenden Handbuch eine **parallele Anbindung des Konnektors mit Internetzugang** dargestellt. Der Sichere Internet Service (SIS) ist dabei nicht aktiviert.



Bei Anschluss des Netzwerks an das Internet über den Konnektor entstehen weitere Risiken, die der Betreiber des Konnektors beachten muss. Ausführliche Informationen zu den Gefahren und Sicherheit im Netz stehen auf den Seiten des BSI unter www.bsi-fuer-buerger.de zur Verfügung.⁵⁸



Weitere Möglichkeiten für die Konfiguration finden Sie im Anhang im Abschnitt Weitere Konfigurationsoptionen.



Bei (zukünftigen) Änderungen an den Konfigurationen der KoCoBox MED+ **muss** der dafür verantwortliche Administrator dies im Betriebsführungsbuch vermerken und unterschreiben.⁵⁹

7.4.1 Status

Zur generellen Basisinformation finden Sie unter Status die *Betriebszustandsmeldungen*⁶⁰ in einer tabellarischen Übersicht, den *Status des Vertrauensraums* (TSL), den *Status der Vertrauensliste der Bundesnetzagentur* (BNetzA-VL) sowie *Produktinformationen*.



Einstellungen werden hier nicht vorgenommen.

⁵⁷ Diese Werte stammen aus der jeweils aktuellen Konnektor-Spezifikation der gematik (zu finden im Fachportal <https://fachportal.gematik.de>).

⁵⁸ Diese Informationen werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) aktuell gehalten. Wir empfehlen, diese Seiten (www.bsi.bund.de) regelmäßig zu besuchen und das Verhalten im Internet den aktuellen Erkenntnissen anzupassen.

⁵⁹ Aus Sicherheitsgründen **müssen** Änderungen an der Konfiguration auf eine **natürliche Person** zurückgeführt werden können.

⁶⁰ mit den Spalten Zeit, Type, Schwere, Beschreibung sowie Parameter

| Betriebszustandsmeldungen | | | |
|---------------------------|--|-----------|---|
| Zeit | Zustand | Typ | Schwere Parameter |
| 20.11.2023 11:34:11 | OPERATIONAL_STATE/EC_OTHER_ERROR_STATE(2) | OPERATION | WARNING Bedeutung = Protokollspeicher zu mehr als 80% gefüllt.; Protokoll = system:OP, system:SEC |
| 20.11.2023 11:34:14 | OPERATIONAL_STATE/EC_LOG_OVERFLOW | OPERATION | WARNING Bedeutung = Wenn im Rahmen der Regeln für die rollierende Speicherung von Logging-Einträgen Einträge gelöscht werden, die nicht älter als LOG_DAYS bzw. FM_<fmName>_LOG_DAYS sind, tritt der Fehlerzustand ein.; Protokoll = system:OP, system:SEC |
| 20.11.2023 11:34:38 | OPERATIONAL_STATE/EC_TLS_Client_Certificate_Security | SECURITY | INFO Bedeutung = Das für die Authentifizierung gegenüber dem Clientsystem konfigurierte Zertifikat hat ein Sicherheitsniveau von weniger als 120bit. Zu verwenden ist ein RSA Zertifikat mit mindestens 3000 bit Schlüssellänge oder ein ECC Zertifikat. |

| Status des Vertrauensraums (TSL) | | Produktinformation | |
|----------------------------------|---|--------------------------------------|--|
| Sequenznummer: | 10482 | Produkttyp /-version: | Konnektor-test-ptv5p.r91.g2bcd4bb / 5.54.1 |
| Startzeit: | Wed Jun 10 16:57:21 CEST 2020 | Hersteller Name / Kennung: | KoCo Connector / KOCO |
| Nächste Aktualisierung: | Thu Dec 21 12:30:18 CET 2023 | Produkt Name / Kennung: | KoCoBox MED+ / kocobox |
| Validität: | gültig | Produktversion: | 5.5.3:4.0.0 |
| Typ: | ECC-RSA | Firmware-Gruppenversion: | 102 |
| Fingerprint: | 77:49:69:ce:a7:48:c6:7d: 2b:70:39:92:58:d0:be:fb: 14:d5:a2:41:3a:d0:77:e6: 95:7c:51:2c:f1:06:6f:87 | Name des Konnektors im lokalen Netz: | KoCoBox |
| | | Informationszeitpunkt: | Thu Nov 23 15:48:35 CET 2023 |

| Status der Vertrauensliste der Bundesnetzagentur (BNetzA-VL) | |
|--|-------------------------------|
| Sequenznummer: | 34 |
| Nächste Aktualisierung: | Sat Jul 25 06:22:43 CEST 2026 |
| Validität: | gültig |
| Letzte Aktualitätsprüfung: | Thu Nov 23 03:01:00 CET 2023 |

Abbildung 41: Übersicht zu den Statusinformationen

Der *Status des Vertrauensraums (TSL)* stellt dar, in welcher Art von Vertrauensraum sich die KoCoBox MED+ befindet:

- Ist die Sequenznummer der TSL kleiner als 10000, so handelt es sich um einen RSA-Vertrauensraum. Dies bedeutet, dass der Konnektor mit Diensten auf Basis des RSA-Kryptoalgorithmus geschützt kommuniziert. Dies wird weiterhin durch den Eintrag Typ: RSA unterstrichen.
- Bei einer Sequenznummer der TSL von größer/gleich 10000 arbeitet der Konnektor in einem ECC-basierten Vertrauensraum. Hierin unterstützt der Konnektor zusätzlich die Kommunikation mit Diensten auf Basis von Kryptoalgorithmen mit elliptischen Kurven. Zusätzlich werden aus Kompatibilitätsgründen weiterhin RSA-Kryptoalgorithmen unterstützt. Dies wird durch den Eintrag *Typ: ECC-RSA* dargestellt.

ECC-Migration

Der Wechsel des Vertrauensraums erfolgt weitgehend automatisch und mittelfristig vom RSA- in den ECC-RSA-Vertrauensraum (im Bereich *Typ* erkennbar). Dieser Vorgang ist irreversibel. Er dient zur Aufrechterhaltung der langfristigen Sicherheit des Gesamtsystems Telematikinfrastruktur.

| Status des Vertrauensraums (TSL) | |
|----------------------------------|---|
| Sequenznummer: | 10482 |
| Startzeit: | Wed Jun 10 16:57:21 CEST 2020 |
| Nächste Aktualisierung: | Thu Dec 21 12:30:18 CET 2023 |
| Validität: | gültig |
| Typ: | ECC-RSA |
| Fingerprint: | 77:49:69:ce:a7:48:c6:7d: 2b:70:39:92:58:d0:be:fb: 14:d5:a2:41:3a:d0:77:e6: 95:7c:51:2c:f1:06:6f:87 |

Abbildung 42: Ausschnitt des Vertrauensraumstatus (TSL) im ECC-RSA-Vertrauensraum

7.4.2 Zusammenfassende Übersicht zur Initialkonfiguration

Im Folgenden wird überblicksartig das chronologische Vorgehen für die initiale Konfiguration des Konnektors im parallelen Anbindungsmodus (ohne SIS) dargestellt.



Achten Sie bitte sorgfältig darauf, die jeweiligen Einstellungen abzuspeichern – in der Regel per Button Übernehmen oder OK.

1

Vorbereitungen für die Initialkonfiguration treffen (siehe Kapitel 5 sowie 7.2)

- Verbinden Sie das Gerät LAN-seitig mit dem entsprechenden Kabel mit der bestehenden IT-Infrastruktur (eingeschalteter Router/Switch für den Internetzugang, Netzwerkrechner).
- Stecken Sie das Stromkabel des Konnektors in eine Steckdose.
- Warten Sie den Systemstart des Konnektors (ca. 10-15 Min.) ab, bis das Display der unteren Abbildung (die LAN-Port-Belegung kann abweichen) entspricht.
- Die für den Aufruf der Managementschnittstelle notwendige IP-Adresse der KoCoBox MED+ (<IP-KON>) kann am Display abgelesen werden. Gehen Sie dazu über den Steuer-Button in den Menü-Bereich *Status/Konfiguration/LAN-Konfig*.
- Öffnen Sie am Netzwerkrechner den Browser und geben Sie diese IP-Adresse der KoCoBox MED+ (<https://<IP-KON>:9443/administration/start.htm>) in die Browserzeile ein.
- Es erscheint das Login-Fenster. Melden Sie sich hier mit dem Benutzernamen *koco-root* und dem initialen Passwort/ Auslieferungspasswort (*Initial4StartUp!*) als Super-Administrator an.
- Geben Sie anschließend zwei Mal das neue persönliche Passwort ein. Erstellen Sie bitte ein sicheres Passwort mit mindestens 8 Zeichen aus drei verschiedenen Zeichenklassen.
- Nach erfolgreicher Anmeldung erscheint die Status-Seite der KoCoBox MED+ Managementschnittstelle.

2

Im Bereich *Zertifikatsdienst* per Button TSL importieren eine gültige TSL manuell importieren (siehe Kapitel 7.4.4.2 bzw. 7.5.5)

3

Im Bereich *Zertifikatsdienst* per Button CRL importieren eine gültige CRL manuell importieren (siehe Kapitel 7.4.4.2 bzw. 7.5.5)

4

Bei Bedarf im Zeitdienst die Konnektor-Systemuhr einstellen (siehe Kapitel 7.4.3.4)

5

LAN/WAN Dienst konfigurieren (siehe Kapitel 7.4.3.1)


- Vergeben Sie einen Hostnamen und setzen Sie beim *Anbindungsmodus Internet* per Radiobutton die Option *IAG*. Der Anbindungsmodus parallel erscheint automatisch bei ausgeschaltetem *WAN-Adapter*.
- Belassen Sie die Voreinstellung (Aktivierung) des *DHCP-Client* an der LAN-Schnittstelle. Die Adresse des *lokalen Netzwerks*, an das der LAN-Adapter des Konnektors angeschlossen ist, ergibt sich automatisch aus den eingetragenen Werten.
- Falls der DHCP-Client an der LAN-Schnittstelle deaktiviert ist (*aus*), geben Sie die *IP-Adresse des LAN-Adapters*, die dazugehörige *Subnetzmaske* sowie die *IP-Adresse des IAG* ein. Diese muss in Byte-Schreibweise konfiguriert sein.
- Behalten Sie die voreingestellte Zeit für den *Service Timeout* bei.
- Behalten Sie die Voreinstellung für die *Länge der IP-Pakete* (Maximum Transmission Unit, MTU) bei.
- Speichern Sie dies per Button *Übernehmen* ab.

6

Im Bereich *Verwaltung* prüfen, ob der *Leistungsumfang ONLINE* aktiviert ist (siehe Kapitel 7.5.1)

7

Im Bereich *Kartenterminaldienst* Kartenterminal(s) pairen (siehe Kapitel 7.4.4.1 sowie 7.5.3)

- Wählen Sie ein Kartenterminal aus der Liste der bekannten Kartenterminals aus und rufen Sie per  Bearbeitungsfunktion das Konfigurationsfenster auf.
- Klicken Sie auf den Button *Status manuell ändern* und wählen Sie die Option *zugewiesen* aus.
- Rufen Sie den Button *manuell pairen* auf. Bestätigen Sie die Frage im Dialogfenster mit OK. Der Bitte-Warten-Balken zeigt die Dauer des Pairingvorgangs an.
- Bestätigen Sie dann im Fingerprint-Fenster das Kartenterminal-Zertifikat mittels *Pairing abschließen*.
- Wechseln Sie zum Kartenterminal und quittieren Sie die *Pairing-Meldung* auf dem Display per Tastatur (grüner Knopf) – oder herstellerspezifisch per Eingabe der Admin-PIN des Kartenterminals.
- Notieren Sie nach Abschluss des Pairings die Kartenterminal-ID (CT-ID). Bestätigen Sie abschließend die Erfolgsmeldung auf der Managementschnittstelle mittels OK.

8


Im Bereich *Infomodell* die Relationen definieren (siehe Kapitel 7.6.2)

- Legen Sie (einen) Mandant(en) an.
- Tragen Sie – sofern vorhanden – das Clientsystem ein und weisen sie (den) Mandant(en) zu.
- Richten Sie den Arbeitsplatz *Konnektor* ein und weisen Sie (den) Mandant(en) zu.
- Richten Sie die (Praxis-)Arbeitsplätze ein und weisen Sie (den) Mandant(en) zu.
- Tragen Sie die SMB im Infomodell ein (SMB ID vergeben, ICCSN der SMB eintragen) und weisen Sie (den) Mandant(en) zu.
- Fügen Sie (das) Kartenterminal(s) zu und weisen Sie (den) Mandant(en) sowie den Arbeitsplatz zu. Wichtig: Dem Arbeitsplatz *Konnektor* muss mindestens ein Kartenterminal zugewiesen werden.

- Fügen Sie CS-AP Objekt hinzu und definieren Sie (die) zugehörige(n) Mandant(en), Clientsystem und Arbeitsplatz.
- Speichern Sie per Button Übernehmen ab.

9

Im Bereich *Fachmodul VSDM* für jeden im Infomodell angelegten Mandanten ein Schlüssel-Paar anlegen (siehe Kapitel 7.7)

- Öffnen Sie in der Liste *Schlüssel für Prüfungsnachweise ...* für jeden aufgeführten Mandanten (der im Infomodell definiert wurde) per  Klick auf das Konfigurationsfenster zum Anlegen eines Mandanten-Schlüssel-Paares zur Verschlüsselung des Prüfungsnachweises auf der eGK.
- Wählen Sie aus, ob Sie die Zeichenfolge für die Ableitung des Schlüssels durch den Konnektor erzeugen lassen oder selbst eingeben möchten.
Beachten Sie bitte, dass die Zeichenfolge exakt 16 Zeichen lang sein muss.
- Sofern Sie mehrere Konnektorpaaire (Offline- und Online-Konnektor) administrieren, verwenden Sie bitte unterschiedliche Zeichen für das Generieren des Schlüssels.
- Bestätigen Sie die eingegebene Zeichenfolge mit OK.
- Per Button Übernehmen speichern Sie dies ab.


10

Im Bereich *DNS* die DNS-Einstellungen vornehmen (siehe Kapitel 7.4.3.5)

- Im Feld *DNS Domain VPN-Zugangsnetz* ist per Default der DNS-Domainname für die Service Discovery der VPN-Konzentratoren des VPN-Zugangsdienstes eingetragen. Dieser Wert muss nicht angepasst werden.⁶¹
- Geben Sie im Feld *DNS Domain lokales Netz* den Domainnamen für das Praxisnetz vor Ort ein.
- Fügen Sie im Bereich *DNS Server (einstellbar)* in der Tabelle *Internet* über den Button DNS Server hinzufügen folgende IP ein: 8.8.8.8.⁶²

11

Freischaltung der SMC-B im Bereich *Kartendienst* (siehe Kapitel 7.5.2)

- Stecken Sie die SMC-B in das Kartenterminal, das dem Arbeitsplatz *Konnektor* zugewiesen ist.
- Öffnen Sie in der Tabelle Karten in der Spalte PIN in der Zeile der entsprechenden SMC-B durch Klick auf das PIN verifizieren-Symbol  das entsprechende Eingabefenster.
- Tragen Sie in das Eingabefeld den Mandanten aus dem Infomodell ein, dem die SMC-B zugewiesen ist und bestätigen Sie dies mit OK.
- Geben Sie nach Aufforderung auf dem Kartenterminal die PIN der SMC-B ein und quittieren Sie die Eingabe. Per Anzeigefenster wird die Freischaltung anerkannt.

⁶¹ Der Default-Wert im Konnektor für das Feld *DNS Domain VPN-Zugangsnetz* lautet *vpnzugd.telemed-ti.net*.

⁶² Hier muss ein beliebiger öffentlich zugänglicher Domain Name Server eingetragen werden, die 8.8.8.8 ist hier beispielhaft.

12 Registrierung des Konnektors mit gesteckter SMC-B im Unterbereich *VPN / Registrierung* durchführen (Kapitel 7.4.3.3., Abschnitt Registrierung)

- Tragen Sie im Feld *Vertragsnummer* die ContractID Ihres Vertrags mit dem Zugangsdienstprovider ein.
- Wählen Sie im Feld *zur Registrierung zu nutzende SMC-B (ICCSN)* im Drop-down Menü die entsprechende SMC-B aus.
- Bestätigen Sie die Eingabe über den Button *Registrieren*.

In der Standard-Displayansicht wird die erfolgreiche initiale Konfiguration mit Verbindung in die TI (paralleler Anbindungsmodus ohne SIS) wie folgt dargestellt:



Abbildung 43: Display der KoCoBox MED+ nach der Initialkonfiguration (G3)



Abbildung 44: Display der KoCoBox MED+ nach der Initialkonfiguration (G4)

Das KoCoBox MED+ Display zeigt in der unteren Statuszeile an:

- die Verbindung zur TI ist konfiguriert, es besteht eine sichere Verbindung (= volles Quadrat, volle Raute)
- es ist keine Verbindung zum SIS konfiguriert (= leeres Quadrat, leere Raute)
- die WAN-Verbindung ist inaktiv (= leeres Quadrat)
- die LAN-Verbindung ist aktiv (= volles Quadrat)



Die erfolgreiche Verbindung zum VPN-Konzentrator der zentralen TI beweist die Authentizität des Konnektors. Damit erfüllt er die notwendigen Sicherheitsanforderungen.



Zusammenfassend ist die KoCoBox MED+ dann integer und authentisch, wenn die folgenden Bedingungen erfüllt sind:

- Der Konnektor wurde von einem autorisierten Lieferanten bezogen.
- Die Verpackung der KoCoBox MED+ ist intakt.
- Das Gerät wurde nicht manipuliert, die beiden Sicherheitssiegel am Gehäuse sind unversehrt.
- Es sind genau diejenigen Sicherheitssiegel, die es sein sollen.
- Das Gerät hat nach Abschluss der Konfiguration eine sichere Verbindung zur TI.

7.4.3 Konfiguration des Netzkonnektors

In diesem Abschnitt werden die Mechanismen beschrieben, mit denen der Konnektor auf der einen Seite in das lokale Netz (LAN) des Endkunden, auf der anderen Seite in die TI bzw. die Bestandsnetze angebunden wird. Diese wesentlichen Aspekte betreffen Routing und Firewall.⁶³

Die grundlegenden Einstellungen für den Netzkonnektor werden in den folgenden Konfigurationsbereichen der Managementschnittstelle vorgenommen:

- *LAN / WAN*
- *DHCP*
- *VPN*
- *Zeitdienst*
- *DNS*
- *Verwaltung*



Folgen Sie den Beschreibungen in den folgenden Abschnitten, um eine sichere Konfiguration des Netzkonnektors zur Anbindung an die TI durchzuführen.

⁶³ Vgl. [gemSpec_Kon], S. 380 f.

7.4.3.1 LAN / WAN

Netzwerkkonfigurationen

Basiskonfiguration

Hostname:

Anbindungsmodus Internet: SIS IAG KEINER
 Routingmodus Intranet: Redirect Block

Anbindungsmodus: **PARALLEL**
WAN Adapter Modus: ein aus

Adresse IAG:
Übermittelte Bestandsnetze aktivieren: an aus

LAN

Lokales Netzwerk: **192.168.2.0/24**

IP-Adresse des LAN-Adapters:

Subnetzmaske des LAN-Adapters:

DHCP Client LAN Status: ein aus

Länge IP-Pakete (MTU):

WAN

WAN Netzwerk:

IP-Adresse des WAN-Adapters:

Subnetzmaske des WAN-Adapters:

DHCP Client WAN Status: ein aus

Länge IP-Pakete (MTU):

Bandbreitenbegrenzung:

Umgebungsparameter

TI zentral:
Offene Fachdienste:

TI dezentral:
Gesicherte Fachdienste:

SIS:
DNS Toplevel Domain:

DNS TI-WA Toplevel Domain:

Aktive Bestandsnetze

| | Aktiv | ID | Name | Netz |
|-------------------------------------|-------|----------|---------------------------------|-------------------|
| <input checked="" type="checkbox"/> | X | BNGEM | Bestandsnetz gematik | 188.144.128.0/24 |
| <input checked="" type="checkbox"/> | X | KZVWL | ZOD-Portal KZV WL | 212.3.66.8/29 |
| <input checked="" type="checkbox"/> | X | IBM | Impfnachweis | 161.156.128.32/28 |
| <input checked="" type="checkbox"/> | X | Demis | Demis Meldeportal | 84.17.163.80/30 |
| <input checked="" type="checkbox"/> | X | SplitDNS | TI-SplitDNS | 84.17.163.84/30 |
| <input checked="" type="checkbox"/> | X | RKIRU | Robert Koch-Institut RZ - RU | 193.175.81.72/29 |
| <input checked="" type="checkbox"/> | X | ORGTI | OGR-Telematikinfrastruktur - RU | 193.28.70.0/30 |

Intranetrouten

Intranetroute hinzufügen ...

| | Segment | Next-Hop |
|--|-----------------|-------------|
| | 192.168.33.0/24 | 192.168.2.5 |

Routingtabelle

| Forwarding Status | Zieladresse | Next-Hop | Routing Typ | Routing Protokoll | Routing Präferenz |
|-------------------|------------------|--------------|-------------|-------------------|-------------------|
| eingeschaltet | 192.168.2.0/24 | 192.168.2.62 | statisch | kernel | 5 |
| eingeschaltet | 192.168.33.0/24 | 192.168.2.5 | statisch | kernel | 5 |
| eingeschaltet | | 192.168.2.5 | statisch | kernel | 5 |
| eingeschaltet | 185.188.3.4/32 | 192.168.2.5 | statisch | kernel | 5 |
| eingeschaltet | 10.30.0.0/16 | 10.22.67.126 | statisch | kernel | 5 |
| eingeschaltet | 84.17.163.84/30 | 10.22.67.126 | statisch | kernel | 5 |
| eingeschaltet | 193.175.81.72/29 | 10.22.67.126 | statisch | kernel | 5 |
| eingeschaltet | 193.28.70.0/30 | 10.22.67.126 | statisch | kernel | 5 |

Adresse testen

IP-Adresse:

FQDN-Adresse:

Abbildung 45: Beispielhafte Netzwerkkonfigurationen.⁶⁴

⁶⁴ Anmerkung der Redaktion: Die abgebildete Konfiguration ist exemplarisch für eine Testumgebung.

Rufen Sie in der Navigationsspalte *LAN/WAN* auf. Es erscheint das Einstellungsfenster für die *Netzwerkkonfigurationen*.

Hier gibt es mehrere Bereiche für Konfigurationen (*Basiskonfiguration, LAN, WAN*) sowie unten einen Bereich zum Testen von *IP-Adressen* und *FQDN-Adressen* (Domainnamen).

Im Bereich *Umgebungsparameter* werden die Netzwerksegmente der zentralen Dienste, der *DNS-Toplevel-Domain* sowie der *DNS TI-WA Toplevel Domain*⁶⁵ automatisch eingetragen, diese sind nicht editierbar.



Falls durch eine Anwendung im Praxisnetz DNS-Anfragen an die KoCoBox MED+ geschickt werden, ist auf Folgendes zu achten: An den Request des angefragten FQDN darf keine lokale Suchdomäne (DNS-Suffix) angehängt sein. Ansonsten werden Anfragen, die nicht direkt beantwortet werden können, an dritte DNS-Server gerichtet werden. Der in der KoCoBox MED+ enthaltene DNS-Resolver arbeitet rekursiv und sendet solche Anfragen zwingend weiter. Eventuell sind hierzu zusätzliche Maßnahmen bei der Konfiguration von Active Directory-Domänen bzw. einzelner Arbeitsstationen nötig, wenn auf andere Anwendungen des Gesundheitswesens (aAdG / Bestandsnetze) zugegriffen werden soll.

In der Tabelle *aktive Bestandsnetze* werden die verfügbaren Bestandsnetze⁶⁶ mit ID und Namen aufgelistet. Hier können Sie *Bestandsnetze freischalten*, indem Sie es in der ersten Spalte durch das Setzen des Häkchens aktivieren, sowie *im lokalen Netz routen*.

Die Tabelle *Intranetrouten* zeigt eine Liste von Routen zum Erreichen der Clientsysteme und Kartenterminals des Konnektors, jeweils mit IP-Netzwerk und dazugehörigem Next Hop.

Über den Button *Intranet Route hinzufügen...* kann man im Konfigurationsfenster jeweils die IP-Adresse sowie den Next Hop eintragen. Mit OK wird der Eintrag bestätigt.



Der Wert *Redirect* beim *Routingmodus Intranet* im Bereich *Basiskonfiguration* kann nur gesetzt werden, wenn zuvor ein oder mehrere *Intranetrouten* definiert wurden.

Zur Information werden in der *Routingtabelle* automatisch konfigurierte Routen angezeigt.

Im unteren Bereich *Adresse testen* haben Sie die Möglichkeit, die Erreichbarkeit von *IP-Adressen* oder *FQDN-Adressen* / Domainnamen (z.B. von Kartenterminals im Praxisnetz) zu testen, indem Sie diese in das Feld eintragen und den Button *IP testen* bzw. *FQDN testen* betätigen.

⁶⁵ Dieses Feld beinhaltet eine Toplevel-Domain für weitere Anwendungen der TI.

⁶⁶ wie zum Beispiel das Sichere Netz der KVen (SNK)

Während der Test durchgeführt wird, erscheint ein *Bitte-Warten*-Balken. Ist der Test beendet, erscheint eine Erfolgsmeldung bzw. eine Fehlermeldung.



Die Änderung der *LAN-IP Adresse* der KoCoBox MED+ führt zur Neu-Initialisierung des Kartenterminaldienstes. So wird dort die modifizierte LAN-Konfiguration berücksichtigt und die Kartenterminals bleiben verbunden. Dazu werden aktive Verbindungen zu den Kartenterminals abgebaut und anschließend wiederhergestellt. Dieser Vorgang kann bis zu 5 Minuten dauern. Abschließend sind die Kartenterminals wieder zu nutzen.



Bitte beachten sie, dass der dauerhafte VPN-Datendurchsatz des Konnektors für alle Verbindungen in Summe maximal 25 Mbit/s beträgt.

Netzwerkkonfigurationen (parallel) für den Online-Anschluss – Modus *Internet Access Gateway (IAG)*

Zur Basiskonfiguration bei paralleler Anbindung der KoCoBox MED+ ans Praxisnetz gehen Sie wie folgt vor:

- 1** Vergeben Sie einen Hostnamen und setzen Sie beim *Anbindungsmodus Internet* per Radiobutton die Option *IAG*.
- 2** Der Anbindungsmodus *parallel* erscheint automatisch bei ausgeschaltetem *WAN-Adapter*. Dies entspricht der Voreinstellung.
- 3** Die *IP-Adresse des IAG* (Standardgateway) erscheint automatisch, sofern der *DHCP Client* aktiviert ist (Radiobutton ein). Andernfalls tragen Sie die IP-Adresse des IAG manuell ein. Dies muss das Standardgateway in Ihrem Praxisnetz sein.
- 4** Beim *Routingmodus Intranet* wird festgelegt, ob andere Subnetze den Konnektor nutzen dürfen (Redirect) oder nicht (Block).⁶⁷
- 5** Die Funktion *übermittelte Bestandsnetze aktivieren* ist per Voreinstellung eingeschaltet (Radiobutton ein).



Über das Internet Access Gateway (z.B. Router mit DSL-/Kabelmodem) können Angriffe aus dem Internet erfolgen. Deswegen muss die Firewall entsprechend sicher konfiguriert werden. Generell wird die Verwendung des Secure Internet Service (SIS) empfohlen.

⁶⁷ Dies wird hier nur der Vollständigkeit halber aufgelistet. Es ist für die Konfiguration der Internetanbindung nicht relevant und nur dann einzustellen, sofern das Endkunden-Netz aus mehreren Netzen besteht. Der *Routingmodus Intranet* bezieht sich auf Routen, die in andere Netze im Intranet angelegt werden, z.B. ein weiteres Subnetz auf der LAN-Seite des Konnektors.

LAN

Der Radiobutton beim *DHCP-Client* an der LAN-Schnittstelle ist per Voreinstellung aktiviert. Somit werden die *IP-Adresse des LAN-Adapters* sowie die dazugehörige *Subnetzmaske* vom DHCP-Server geliefert und automatisch eingetragen. Die Adresse des *lokalen Netzwerks*, an das der LAN-Adapter des Konnektors angeschlossen ist, ergibt sich automatisch aus den eingetragenen Werten.

1

Falls der *DHCP-Client* an der LAN-Schnittstelle deaktiviert ist (aus), geben Sie die *IP-Adresse des LAN-Adapters* sowie die dazugehörige *Subnetzmaske* ein. Diese muss in Byte-Schreibweise konfiguriert sein.⁶⁸

2

Tragen Sie die *Länge der IP-Pakete* (Maximum Transmission Unit, MTU) ein; die Voreinstellung ist 1.500. Wir empfehlen, diese beizubehalten.⁶⁹

3



Bei der Adressvergabe für den LAN-Adapter sind ausschließlich private IP-Adressen erlaubt. Öffentliche IP-Adressen werden **nicht** unterstützt.

WAN

Da der *WAN-Adapter* ausgeschaltet ist (paralleler Anbindungsmodus), sind die WAN-Parameter nicht zu konfigurieren.



Für den Fall der Nutzung einer langsamen Internetverbindung (z.B. ISDN) sollte im Feld *Bandbreitenbegrenzung* ein Wert eingetragen werden. Er schränkt das Volumen des ausgehenden Datenverkehrs in kbits/s ein. Sofern Sie einen Wert eintragen möchten, muss dieser größer/gleich 20 sein.

Mit dem Button **Übernehmen** speichern Sie die Konfigurationen ab.

Firewall zum Secure Internet Service (SIS)

Dieser Bereich kann konfiguriert werden, sofern der Anbindungsmodus *SIS* bei der Basiskonfiguration im Bereich *LAN/WAN* beibehalten wurde. Damit ist eine sichere Verbindung ins Internet möglich.



Bedingung für die Nutzung des SIS ist ein Vertrag des Endkunden mit einem entsprechenden Service Provider / Zugangsdienstprovider (ZGDP).

⁶⁸ Eine Darstellung von 255.255.255.0 wäre /24.

⁶⁹ Der Wert kann jedoch bei komplexeren Netzwerk-Infrastrukturen der jeweiligen Umgebung angepasst werden.



Abbildung 46: Konfigurationsbereich für die Firewall zum Secure Internet Service (SIS)

In der Tabelle *SIS Firewall-Regeln* finden Sie die Liste der Firewall-Regeln an der WAN-Schnittstelle zum SIS. Sie zeigt für den Sender die *IP-Adresse* sowie den *Port* an, für den Empfänger die *IP-Adresse*, den *Port* sowie die *Richtung* und die *Aktion*.

Über den Button *Regeln hinzufügen...* können Sie die notwendigen Regeln definieren: Die *IP-Adresse des Senders* sowie die *IP-Adresse des Empfängers* müssen eingetragen werden, optional sind der *TCP-Port des Senders* sowie der *TCP-Port des Empfängers*. Zudem können Sie *Richtung* und *Aktion* per Drop-down Menü festlegen. Per *Übernehmen* speichern Sie die Firewall-Regel ab.

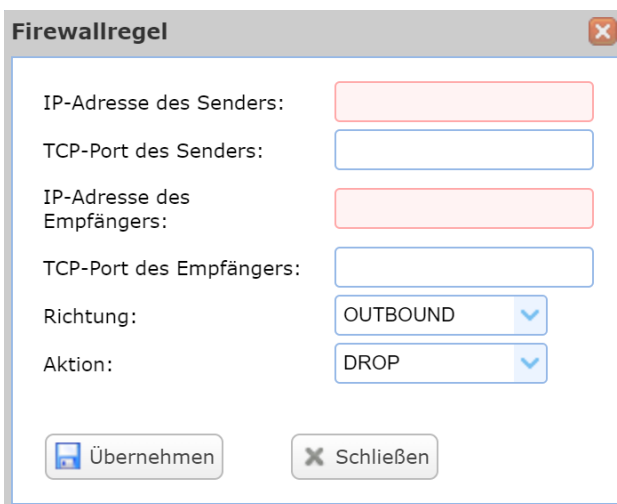


Abbildung 47: Konfiguration der Firewall-Regeln

Einen Tabelleneintrag können Sie per Klick auf die jeweilige Listenzeile editieren oder löschen. Mittels *Übernehmen* bestätigen Sie die Einstellungen.



Die Firewallregeln, die der Administrator selbst definieren kann, dienen der Einschränkung des Zugriffs von internen Systemen auf Systeme im Internet hinter dem SIS-Tunnel.

Im Modus *IAG* kann der Konnektor die Kommunikation der Systeme im LAN mit dem Internet nicht einschränken, da die Pakete nicht im Konnektor weitergeleitet werden.

Im Modus *SIS* filtert der Konnektor die weitergeleiteten Pakete anhand der Quell-IP-Adresse, Ziel-IP-Adresse, Quell-Port und Ziel-Port. Das Weglassen von Port oder IP betrifft jeweils alle Ports bzw. alle IPs.



Durch die Regeln kann der Zugriff gegenüber dem Standard nur weiter eingeschränkt und nicht erweitert werden. Man kann beispielsweise konfigurieren, dass bestimmte Rechner im LAN keinen Internetzugriff haben (leere Zieladresse) oder dass für alle Rechner im LAN bestimmte Ziel-Adressen gesperrt werden (leere Quell-Adresse).



Bitte beachten Sie, dass bei fehlender Verbindung zum SIS alle Firewallregeln, die der Administrator definiert, unwirksam sind.

7.4.3.2 DHCP

In diesem Bereich konfigurieren Sie die DHCP-Einstellungen. Diese umfassen Parameter des DHCP-Clients und die Konfiguration des konnektor-eigenen DHCP-Servers.

Abbildung 48: Konfiguration der DHCP-Einstellungen

Im oberen Bereich *DHCP Client* finden Sie zwei Buttons: Erneuere DHCP LAN Lease und Erneuere DHCP WAN Lease. Durch Klick des jeweiligen Buttons erscheint ein Dialogfenster mit der Frage, ob man das LAN bzw. WAN Lease wirklich erneuern möchte. Nach Bestätigung durch OK wird der Befehl jeweils ausgeführt.



Diese Funktion ist nur bei aktivierter DHCP-Konfiguration im Bereich LAN/WAN verfügbar.

Im Bereich *DHCP Server* haben Sie in der Zeile *DHCP Server Status* mittels Radiobutton ein die Möglichkeit, den DHCP-Server an der LAN-Schnittstelle zu aktivieren. Per Voreinstellung ist der DHCP-Server deaktiviert.

Beim Adressbereich *Dynamic Lease* können Sie angeben, aus welchem Bereich von IP-Adressen der DHCP-Server IP-Adressen dynamisch vergeben darf.



Kontrollieren Sie gegebenenfalls voreingestellte IP-Adressen und bestätigen Sie diese mittels Übernehmen. Andernfalls tragen Sie die IP-Adressen manuell ein und speichern diese ebenfalls mit dem Button Übernehmen ab.



Speichern Sie mittels Übernehmen die Einstellungen ab, auch wenn Sie bereits in den Konfigurationsfenstern Eingaben gemacht und gespeichert haben. Dies gilt auch dann, wenn Sie

keine Client-Gruppen anlegen möchten.

Im Folgenden wird das Anlegen der Client-Gruppe(n) beschrieben.

Client-Gruppe bearbeiten ✕

Bezeichnung:

Konnektor-NTP an Clients: ja nein

Konnektor als Default-Gateway: ja nein Default-Gateway:

Netzmaske des Clients:

Konnektor-DNS an Clients: ja nein

Domainname des Clients:

Leasedauer dynamischer Adressen:

Routen:

Bestandsnetz-Routen:

Intranet-Routen:

externe DNS
 DNS-Server hinzufügen ...

Hostnamen
 Hostnamen hinzufügen ...

Static Leases
 Static Lease hinzufügen ...

Routen
 Route hinzufügen ...

| IP | Subnetz | Next-Hop |
|----|---------|----------|
| | | |

Bestandsnetz-Routen

| Aktiv | IP | Subnet: | Next-Hop |
|-------------------------------------|----------------|---------|--------------|
| <input checked="" type="checkbox"/> | 188.144.128.0 | 24 | 192.168.2.62 |
| <input checked="" type="checkbox"/> | 212.3.66.8 | 29 | 192.168.2.62 |
| <input checked="" type="checkbox"/> | 161.156.128.32 | 28 | 192.168.2.62 |
| <input checked="" type="checkbox"/> | 84.17.163.80 | 30 | 192.168.2.62 |
| <input checked="" type="checkbox"/> | 84.17.163.84 | 30 | 192.168.2.62 |
| <input checked="" type="checkbox"/> | 193.175.81.72 | 29 | 192.168.2.62 |
| <input checked="" type="checkbox"/> | 193.28.70.0 | 30 | 192.168.2.62 |

Intranet-Routen

| Aktiv | IP | Subnet: | Next-Hop |
|-------------------------------------|--------------|---------|-------------|
| <input checked="" type="checkbox"/> | 192.168.33.0 | 24 | 192.168.2.5 |

DHCP Options

Übernehmen

✕ Schließen

Abbildung 49: Konfigurationsmaske zur Bearbeitung der Client-Gruppen

Im Bereich *Client-Gruppen* haben Sie die Möglichkeit, mindestens zwei Client-Gruppen zu verwalten. Dabei ist die gesamte Parameter-Liste für jede Client-Gruppe getrennt konfigurierbar.

Dabei gehen Sie wie folgt vor:

- 1** Über den Button *Client-Gruppe hinzufügen...* öffnen Sie das Konfigurationsfenster *Client-Gruppe bearbeiten*.
- 2** Tragen Sie den Namen der Client-Gruppe ein.
- 3** Definieren Sie bei *Konnektor-NTP an Clients* per Radiobutton ja/nein, ob der Konnektor die Adresse des konnektor-internen NTP-Servers per DHCP an die Clients senden soll oder nicht. Per Voreinstellung ist dies aktiviert.
- 4** Legen Sie per Radiobutton ja/nein fest, ob beim Client der *Konnektor als Default-Gateway* fungieren soll. Per Voreinstellung ist dies deaktiviert. Soll der Konnektor nicht das Default Gateway sein, so tragen Sie in das Feld die Adresse des zu verwendenden Default Gateways als Parameter ein.
- 5** Tragen Sie die *Netzmaske des Clients* ein.
- 6** Für den Fall, dass unter *Konnektor-DNS an Clients* der konnektor-eigene DNS-Server nicht übergeben werden soll (entsprechend der Voreinstellung nein), fügen Sie die Adressen externer – aus dem Netz des Endkunden erreichbarer – DNS-Server über den Button *DNS Server hinzufügen...* ein. Dazu tragen Sie im Konfigurationsfenster die IP-Adresse ein und bestätigen dies mit OK.
- 7** Geben Sie im Feld *Domainname des Clients* einen gültigen Domainnamen ein. Über den Button *Hostnamen hinzufügen...* können Sie eine Liste von MAC-Adressen konfigurieren und sie den Hostnamen der Clients zuweisen.
- 8** Tragen Sie im Konfigurationsfenster dafür jeweils Hostnamen und MAC-Adresse ein. Die entstandene Liste können Sie jederzeit bearbeiten, indem Sie Einträge einfügen, ändern oder löschen.
- 9** Legen Sie die *Leasedauer dynamischer Adressen* in Minuten fest. Über den Button *Static Lease hinzufügen...* öffnen Sie das Konfigurationsfenster, in dem Sie die IP-Adresse und die MAC-Adresse eintragen und per OK bestätigen.
- 10** Durch Klick des Buttons *Route hinzufügen...* können Sie Routen zur Verteilung an die Clients frei konfigurieren. Tragen Sie dazu im Konfigurationsfenster die IP-Adresse, die Subnetzmaske sowie dazugehörigen Next Hop ein.
- 11** Wiederholen Sie dies für *Bestandsnetz-Routen* und *Intranetrouten*.

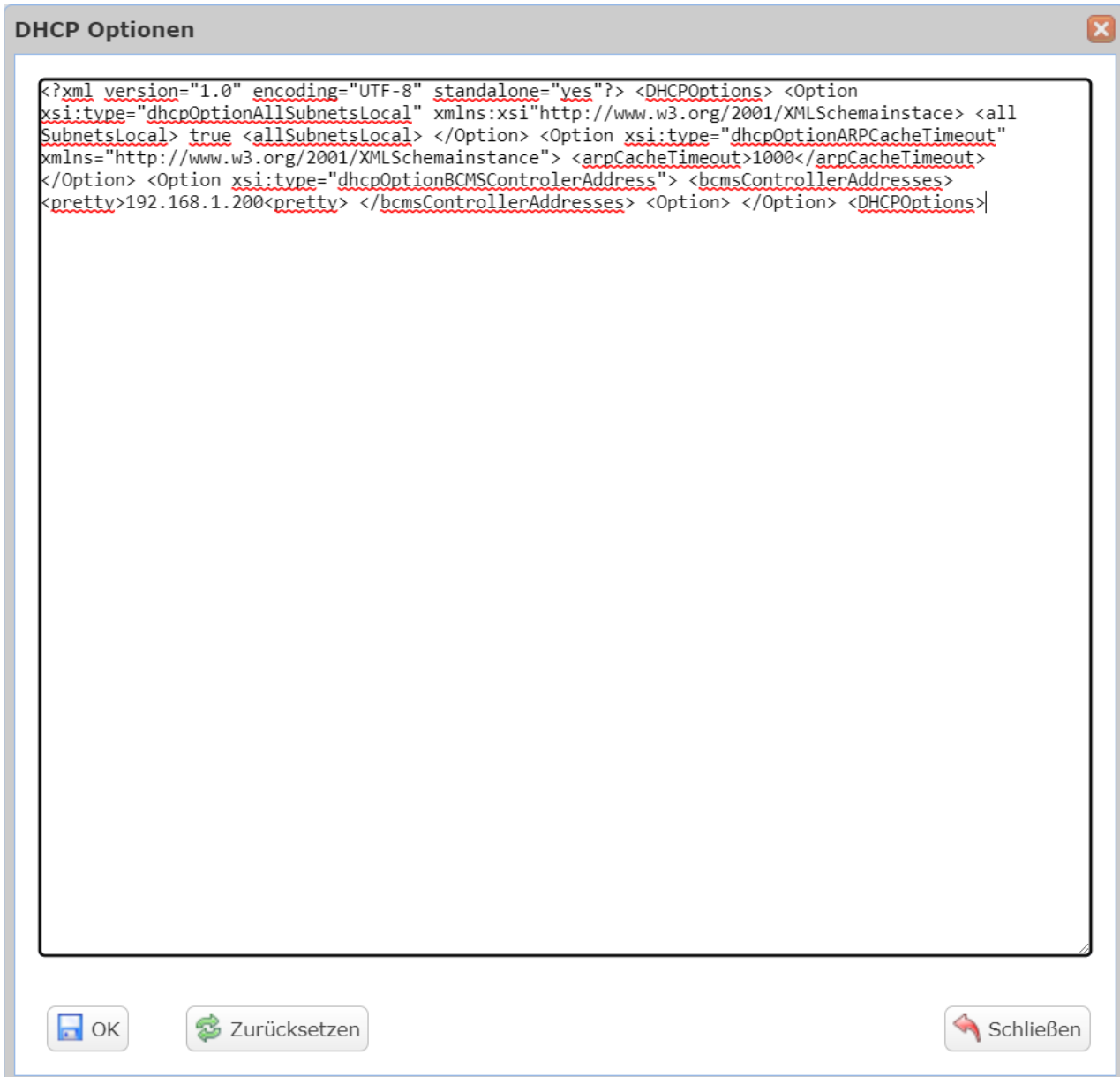


Abbildung 50: Eintrag von DHCP-Optionen für eine Client-Gruppe



Bei Bedarf können über den Button DHCP-Options erweiterte DHCP-Optionen eingestellt werden. Diese müssen XML-Schema konform eingegeben werden. Dabei können mehrere Optionen hintereinander eingefügt werden. Zu beachten ist dabei, dass die nachfolgenden Optionen innerhalb der Option-Tags erscheinen. Per OK werden diese gespeichert, mittels Zurücksetzen gelöscht.

12

Nach dem Bestätigen müssen die Konfigurationen im Konfigurationsfenster *Client-Gruppe bearbeiten* mittels Übernehmen nochmals gespeichert werden.

7.4.3.3 VPN (Virtual Private Network)

In diesem Bereich werden die Einstellungen für die Absicherung der Anbindung des Konnektors an die TI⁷⁰ sowie für den SIS vorgenommen.



Hier finden Sie auch den Unterbereich *Registrierung* für die Freischaltung des Zugangs zur TI über den ZGDP.

VPN

| | |
|--|--|
| TI-VPN-Konzentrator Adresse: 185.188.3.5 | Länge IP-Pakete TI: <input style="width: 100%;" type="text" value="1318"/> |
| SIS-VPN-Konzentrator Adresse: Kein VPN zu SIS aufgebaut. | Länge IP-Pakete SIS: <input style="width: 100%;" type="text" value="1318"/> |
| VPN Timeout Modus: <input type="radio"/> ein <input checked="" type="radio"/> aus | VPN Idle Timeout: <input style="width: 100%;" type="text" value="600 Sekunden"/> |
| Nutzung Hash & URL: <input type="radio"/> ein <input checked="" type="radio"/> aus | Replay Window: <input style="width: 100%;" type="text" value="32"/> |
| IKE Keep-Alive-Modus: <input checked="" type="radio"/> ein <input type="radio"/> aus | NAT Keep-Alive-Modus: <input checked="" type="radio"/> ein <input type="radio"/> aus |
| IKE Keep-Alive-Interval: <input style="width: 100%;" type="text" value="30 Sekunden"/> | NAT Keep-Alive-Interval: <input style="width: 100%;" type="text" value="20 Sekunden"/> |
| IKE Keep-Alive-Versuche: <input style="width: 100%;" type="text" value="3"/> | |

Übernehmen
 Verwerfen

VPN-Verbindungen

VPN zu TI aufbauen
VPN zu TI abbauen

VPN zu SIS aufbauen
VPN zu SIS abbauen

Abbildung 51: Konfigurationsbereich für das Virtual Private Network (VPN)

Für die Konfiguration rufen Sie in der Navigationsspalte *VPN* auf.

Hier erscheinen in der Zeile *TI-VPN-Konzentrator-Adresse* bzw. *SIS-VPN-Konzentrator-Adresse* die entsprechenden IP-Adressen der verfügbaren Konzentratoren, sofern Verbindungen bestehen. Ist dies nicht der Fall, so wird der Text *Keine Verbindung zur TI* angezeigt.

Die *Länge der IP-Pakete TI* bzw. die *Länge der IP-Pakete SIS* ist jeweils voreingestellt (1318) und kann bei Bedarf geändert werden.

Beim *VPN Timeout Modus* entscheiden Sie mittels Radiobutton *ein*, ob nach Inaktivität die VPN-Verbindung automatisch abgebaut werden soll. Per Voreinstellung ist dies deaktiviert.



Nur bei der Nutzung von DSL-Verbindungen ohne Flatrate sollten Sie diese Einstellung aktivieren. Generell raten wir vom Betrieb ohne Flatrate jedoch ab, da unkontrolliert Kosten entstehen können.



Bitte beachten Sie: Falls Sie den *VPN Timeout Modus* aktivieren, müssen Sie den *IKE Keep-Alive Modus* (siehe unten) deaktivieren.

⁷⁰ für die Verwendung der Telematikanwendungen nach § 291a SGB V

In der Zeile *VPN Idle Timeout* können Sie die Zeit eintragen (voreingestellt sind 600 Sekunden), nach der eine inaktive VPN-Verbindung zum Abbau der Verbindung führt.

Hier ist die Größe des *Replay Window* eintragbar. Für diesen Standard-VPN-Parameter ist der Wert 32 voreingestellt.



Das *Replay Window* darf ausschließlich für Fehlersuche oder Testzwecke auf den Wert 0 gesetzt werden, da diese Einstellung die Replay Detection für Datenpakete deaktiviert und damit die Sicherheit der Verbindung beeinträchtigt.

Unter *Nutzung Hash & URL* entscheiden Sie per Radiobutton ein/aus, ob das Hash & URL-Verfahren zum Zertifikatsaustausch genutzt werden soll. Per Voreinstellung ist dies deaktiviert.

Anschließend erfolgt die Konfiguration der Einstellungen für den *IKE Keep-Alive Modus* sowie für den *NAT Keep-Alive Modus*: Per Radiobutton ein/aus entscheiden Sie jeweils, ob das entsprechende Paket gesendet werden soll oder nicht. Per Voreinstellung ist sind beide Funktionen aktiviert.



Wir empfehlen hier, die Voreinstellungen beizubehalten.

Im Feld *IKE Keep Alive Interval* definieren Sie die Zeit in Sekunden, nach welcher ein neues IKE Keep-Alive-Paket gesendet werden soll (voreingestellt sind 30 Sekunden). Analog füllen Sie im Feld *NAT Keep Alive Interval* die Zeit in Sekunden aus, nach der ein neues *NAT Keep-Alive-Paket* gesendet werden soll (voreingestellt sind 20 Sekunden).

Schließlich können Sie in der Zeile *IKE Keep Alive Versuche* definieren, nach wie vielen IKE Keep-Alive-Paketen ohne Acknowledge Message die Verbindung beendet wird. Es sind drei Versuche voreingestellt.



Bitte beachten Sie dazu generell die folgenden Sicherheitshinweise:

- Die IKE-Lifetime beträgt maximal 161 Stunden.
- Die IPsec-SA-Lifetime beträgt maximal 23 Stunden.
- Der Konnektor wird 20 Minuten vor Ablauf der jeweiligen Lifetime jeweils ein Rekeying beginnen.

Die genannten Werte sind **nicht** durch den Administrator konfigurierbar.

Über die Buttons *VPN zu TI aufbauen*⁷¹, *VPN zu TI abbauen* und *VPN zu SIS aufbauen*⁷², *VPN zu SIS abbauen* in unteren Bereich *VPN-Verbindungen* werden die entsprechenden Tunnel auf- bzw. abgebaut.

⁷¹ Voraussetzung dafür ist, dass der Leistungsumfang ONLINE (im Navigationsbereich *Verwaltung*) aktiviert ist.

⁷² Dies setzt einen bestehenden VPN-Tunnel in die TI voraus.

VPN

| | |
|--|--|
| TI-VPN-Konzentrator Adresse: 185.188.3.5 | Länge IP-Pakete TI: <input type="text" value="1318"/> |
| SIS-VPN-Konzentrator Adresse: 185.188.3.558 | Länge IP-Pakete SIS: <input type="text" value="1318"/> |
| VPN Timeout Modus: <input type="radio"/> ein <input checked="" type="radio"/> aus | VPN Idle Timeout: <input type="text" value="600 Sekunden"/> |
| Nutzung Hash & URL: <input type="radio"/> ein <input checked="" type="radio"/> aus | Replay Window: <input type="text" value="32"/> |
| IKE Keep-Alive-Modus: <input checked="" type="radio"/> ein <input type="radio"/> aus | NAT Keep-Alive-Modus: <input checked="" type="radio"/> ein <input type="radio"/> aus |
| IKE Keep-Alive-Interval: <input type="text" value="30 Sekunden"/> | NAT Keep-Alive-Interval: <input type="text" value="20 Sekunden"/> |
| IKE Keep-Alive-Versuche: <input type="text" value="3"/> | |

Übernehmen
 Verwerfen

VPN-Verbindungen

VPN zu TI aufbauen
VPN zu TI abbauen

VPN zu SIS aufbauen
VPN zu SIS abbauen

Abbildung 52: Konfigurationsbereich für das VPN mit Verbindung in die TI und zum SIS

Registrierung

In diesem Bereich erfolgt die Registrierung am Zugangsdienst.



Bevor Sie eine Verbindung in die TI aufbauen können, müssen Sie den Konnektor beim Zugangsdienstprovider (ZGDP) freischalten.



Voraussetzung für die erfolgreiche Registrierung beim ZGDP ist die Freischaltung der SMC-B.⁷³ Dies ist nur mit einem gepaarten Kartenterminal und einer durch den entsprechenden Mandanten verwalteten SMC-B möglich.



Pairen Sie das Kartenterminal entsprechend der Beschreibung im Abschnitt *Kartenterminaldienst*, bevor Sie mit der Registrierung beim Zugangsdienstprovider beginnen.⁷⁴

⁷³ Details zum Ablauf der Freischaltung der SMC-B werden weiter unten im Abschnitt Kartendienst beschrieben.

⁷⁴ Details zum Ablauf des Pairings werden weiter unten im Abschnitt Kartenterminaldienst beschrieben.

Registrierung am Zugangsdienst

Vertragsnummer:

Registrationsdienst: <https://register.d-vpnzugd-ref.telemed-ti.net:8443/RegistrationServer/services/provisioningPort/>

zur Registrierung zu nutzende SMC-B (ICCSN):

zu registrierendes VPN-Zertifikat: ECC RSA

letzte Freischaltung

aktuell freigeschaltet: **nein**

Abbildung 53: Zugangsdienst-Registrierung

Zur Registrierung der KoCoBox MED+ am Zugangsdienst ist die Eingabe folgender Daten erforderlich:

- Vertragsnummer / ContractID
- SMC-B (ICCSN)

Zudem muss per Radiobutton das zu registrierende VPN-Zertifikat ausgewählt werden (ECC oder RSA)⁷⁵. Über den Button Registrieren schicken Sie die Daten ab.



War die Freischaltung erfolgreich, werden die Art der Freischaltung (RSA/ECC), Datums- und Uhrzeitangabe des Freischaltzeitpunktes sowie die verwendete SMC-B angezeigt.

Registrierung am Zugangsdienst

Vertragsnummer:

Registrationsdienst: <https://register.f-vpnzugd-ref.telemed-ti.net:8443/registration-server/services/provisioningPort/>

zur Registrierung zu nutzende SMC-B (ICCSN):

zu registrierendes VPN-Zertifikat: ECC RSA

letzte Freischaltung

aktuell freigeschaltet: **RSA**


RSA


Zeitpunkt: **19.12.2022 13:09:05**


mit SMC-B: **80276883110000096304**


Abbildung 54: Anzeige nach erfolgreicher Registrierung am Zugangsdienst

⁷⁵ Bei Konnektoren mit einfach personalisierten gSMC-Ks ist ausschließlich die RSA-Option sichtbar.

 Ist die Freischaltung nicht erfolgt (wenn z.B. das Netzkonnetorzertifikat oder die SMC-B abgelaufen ist) oder tritt ein anderer Fehler auf, erscheint eine entsprechende Fehlermeldung.

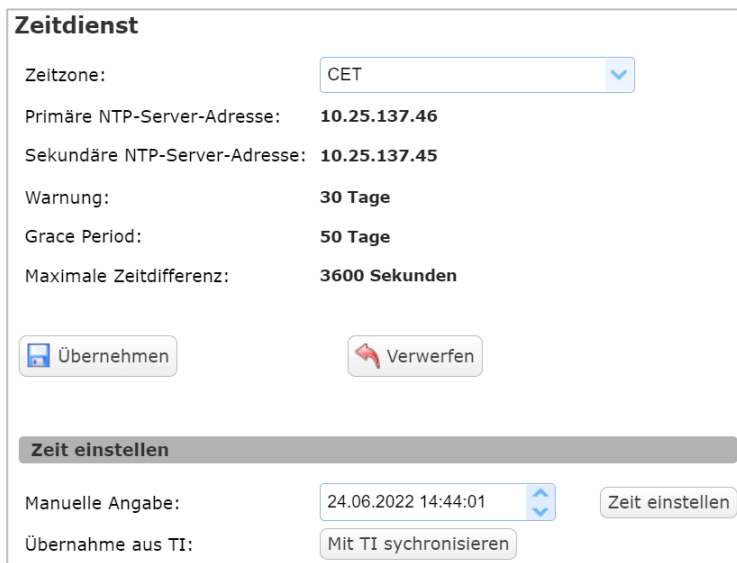
 Prüfen Sie in diesem Fall die Einträge. Sofern dies nicht erfolgreich ist, kontaktieren Sie den Support.

 Stellen Sie durch die Konfiguration des Clientsystems sicher, dass Ereignisse mit dem Topic SMC_K/REGISTER/ERROR abonniert sind.
Um Fehlermeldungen hinsichtlich der SMC-B während wiederholter Registrierung (Re-Registrierung) zu vermeiden, stellen Sie bitte sicher, dass eine freigeschaltete SMC-B dafür verfügbar ist.

 Stellen Sie durch die Konfiguration des Clientsystems sicher, dass Ereignisse mit den Topics SMC_K/UPDATE/ERROR und SMC_K/DOWNLOAD/ERROR abonniert sind.
Bei Auftreten dieser Meldungen⁷⁶ soll sich der Benutzer oder Administrator **unverzüglich** mit dem Hersteller der KoCoBox MED+ in Verbindung setzen.

7.4.3.4 Zeitdienst

Der Zeitdienst ist Basis einer gleichen Systemzeit für sämtliche in der TI einzusetzenden Produkttypen und damit zentral für die sichere Anbindung des Konnektors.



Zeitdienst

Zeitzone: CET

Primäre NTP-Server-Adresse: 10.25.137.46

Sekundäre NTP-Server-Adresse: 10.25.137.45

Warnung: 30 Tage

Grace Period: 50 Tage

Maximale Zeitdifferenz: 3600 Sekunden

Übernehmen Verwerfen

Zeit einstellen


Manuelle Angabe: 24.06.2022 14:44:01 Zeit einstellen

Übernahme aus TI: Mit TI synchronisieren

Abbildung 55: Konfigurationsbereich für den Zeitdienst

⁷⁶ Eine entsprechende Fehlermeldung bedeutet, dass die automatische Laufzeitverlängerung der Zertifikate der gSMC-Ks in der KoCoBox MED+ nicht erfolgreich ausgeführt werden konnte. Dieser Umstand erfordert die Unterstützung des Herstellers, da der reibungslose Weiterbetrieb der KoCoBox MED+ über das Ablaufdatum der bestehenden Zertifikate hinaus nicht möglich ist.

Rufen Sie in der Navigationsspalte den Bereich Zeitdienst auf und gehen Sie dann wie folgt vor:

- 1** Zunächst ist per Drop-down Menü die *Zeitzone* auszuwählen, in der der Konnektor eingesetzt wird. Voreingestellt ist die *Central European Time (CET) / Mitteleuropäische Zeit (MEZ)*.
- 2** Anschließend erfolgt die Konfiguration des primären und sekundären Stratum 2 Zeitservers der zentralen TI-Plattform für die Synchronisation mit dem NTP-Server des Konnektors. Hier sind die *primäre NTP Server Adresse* sowie die *sekundäre NTP Server Adresse* voreingestellt. Mittels Übernehmen werden beide Einstellungen gespeichert.
-  Im Standardonlinebetrieb sollte der Stratum 2 Zeitserver der TI aktiviert werden. Mit der erfolgreichen Verbindung in die TI ist dieser automatisch aktiv.
- 3** In der Zeile *Warnung* erscheint die Anzahl an Tagen nach der ersten erfolglosen Zeitsynchronisierung, nach der eine Warnung an den Betreiber erfolgen soll. Die Voreinstellung ist 30 Tage.
- 4** In der Zeile *Grace Period* erscheint die Anzahl an Tagen nach der ersten erfolglosen Zeitsynchronisierung, nach welcher der Konnektor in einen kritischen Betriebszustand übergehen muss. Hier sind 50 Tage voreingestellt.
- 5** Im Feld *maximale Zeitdifferenz* erscheint die maximale Zeitabweichung in Sekunden zwischen Systemzeit und Zeit des Stratum 2 Zeitservers zum Zeitpunkt der Zeitsynchronisierung. Die Voreinstellung beträgt 3600 Sekunden. Im unteren Bereich *Zeit einstellen* haben Sie zwei weitere Möglichkeiten, die Systemzeit des Konnektors einzutragen:
 - 1** Auf manuellem Weg⁷⁷ erfolgt dies in einer Zeile für Datum und Uhrzeit und kann per Tastatur oder mittels Pfeilen nach oben/unten konfiguriert werden. Über den Button *Zeit einstellen* bestätigen Sie den Eintrag.
 - 2** Die Systemzeit aus der TI stellen Sie über den Button *mit TI synchronisieren* ein.

⁷⁷ falls keine Verbindung in die TI besteht

Zeitdienst

Zeitzone: CET ▼

Primäre NTP-Server-Adresse: **10.25.137.46**

Sekundäre NTP-Server-Adresse: **10.25.137.45**

Warnung: **30 Tage**

Grace Period: **50 Tage**

Maximale Zeitdifferenz: **3600 Sekunden**

Übernehmen
Verwerfen

Zeit einstellen

Manuelle Angabe: 24.06.2022 14:44:01 ▲▼ Zeit einstellen

Übernahme aus TI: Mit TI synchronisieren

Abbildung 56: Anzeige des Zeitdienstes bei Verbindung zur TI



Bitte beachten Sie, dass die Systemzeit nur im Offline-Modus des Konnektors manuell modifiziert werden kann.



Bitte sorgen Sie dafür, dass die Systemzeit richtig eingestellt ist, um eine korrekte Protokollierung zu gewährleisten. Besonders im **Offline-Modus** hat der Administrator darauf zu achten, dass die genaue Uhrzeit eingestellt ist, um einen vorzeitigen Verlust von Einträgen im Sicherheitsprotokoll auszuschließen.



Wird der Konnektor **dauerhaft im Offline-Modus** betrieben, so ist nach der initialen Einstellung der korrekten Zeit mit einer durchschnittlichen Abweichung von 1,6 Minuten pro Jahr zu rechnen. Der Administrator soll alle zwei Jahre kontrollieren, ob die aktuelle Systemzeit noch vorliegt und diese gegebenenfalls korrigieren.

7.4.3.5 DNS (Domain Name Server)

Im Navigationsbereich *DNS* wird der Namensdienst konfiguriert. Hier sind zum einen DNS Server einstellbar, zum anderen werden im unteren Bereich nicht editierbare IP-Adressen von DNS Servern (TI, SIS und Bestandsnetze) dargestellt.

DNS

DNS Top Level Domain TI: **telematik-test.**

DNS Top Level Domain TI-WA: **ti-wa-test.**

DNS Domain VPN-Zugangsnetz:

DNS Domain lokales Netz:

DNS-Server (einstellbar)

Internet

DNS-Server hinzufügen ...

| IP | | | | | | | |
|----|---|---------|--|--|--|--|--|
| ✎ | ✖ | 8.8.8.8 | | | | | |
| ✎ | ✖ | 8.8.4.4 | | | | | |

Intranet

DNS-Server hinzufügen ...

| IP | | | | | | | |
|----|--|--|--|--|--|--|--|
| | | | | | | | |

DNS-Server (nicht einstellbar)

Telematikinfrastruktur

| IP | | | | | | | |
|----|--|--|--|--|--|--|--|
| | | | | | | | |
| | | | | | | | |

SIS

| IP | | | | | | | |
|----|--|--|--|--|--|--|--|
| | | | | | | | |

Bestandsnetze

| Domäne | | | | IP | | | |
|--------|--|--|--|----|--|--|--|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Abbildung 57: Konfigurationsbereich für den Domain Name Server (DNS)

Wählen Sie in der Navigationsspalte den Bereich *DNS* aus. Zunächst werden die *Top Level Domain* des Namensraumes TI sowie die *Top Level Domain* des Namensraumes *TI-WA* dargestellt. Beide sind nicht konfigurierbar.⁷⁸

Bei der *DNS Domain VPN-Zugangsnetz* tragen Sie den DNS-Domainnamen für die Service Discovery der VPN-Konzentratoren des VPN-Zugangsdienstes ein.

Geben Sie in der Zeile *DNS Domain lokales Netz* den DNS-Domainnamen ein, der von einem DNS-Server beim Arzt / Apotheker bzw. Kostenträger aufgelöst wird.

Dieser Name darf weder mit einem Punkt beginnen noch mit einem Punkt enden.

⁷⁸ Der Wert wird im unter LAN/WAN im Bereich *Umgebungsparameter* im Feld *DNS-Toplevel-Domain* eingestellt und hier nur angezeigt.

© KoCo Connector GmbH 2024

Seite 78 von 289


Im Bereich *DNS Server (einstellbar)* können Sie nun die notwendigen DNS Server für das Internet sowie das Intranet hinzufügen. Dies erfolgt jeweils über den Button DNS Server hinzufügen: Es erscheint das Konfigurationsfenster *DNS-Eintrag*, in das Sie die öffentliche/lokale IP-Adresse hineinschreiben. Mit Klick auf OK bestätigen Sie dies, mittels Schließen verlassen Sie das Fenster, ohne dass die IP-Adresse gespeichert wurde.

Die konfigurierten IP-Adressen erscheinen als Liste in den Feldern *Internet* bzw. *Intranet*. Darin können sie jeweils bearbeitet werden:

Über  öffnen Sie das Konfigurationsfenster *DNS-Eintrag*, in dem Sie die IP-Adresse editieren können. Mittels OK speichern Sie die Änderung ab, mittels Schließen verlassen Sie das Konfigurationsfenster, ohne dass die IP-Adresse gespeichert wurde.



Abbildung 58: Eintragen der IP-Adresse

Mittels  entfernen Sie den Eintrag. Es erscheint ein Dialogfenster, worin Sie die Löschaktion per OK bestätigen oder verwerfen.

Im unteren Bereich *DNS Server (nicht einstellbar)* finden Sie in den drei Tabellenfeldern *Telematikinfrastruktur*, *SIS* und *Bestandsnetze* eine Übersicht der jeweils fest eingetragenen IP-Adressen (in der Tabelle *Bestandsnetze* zusätzlich mit dem Namen der Domäne). Hier handelt es sich jeweils um Listen von DNS-Servern, die zur Namensauflösung des Namensraums der TI, des Namensraums Internet bei Nutzung des SIS sowie der Namensräume von Bestandsnetzen verwendet werden.



Die Listeneinträge in diesen Tabellen können nicht editiert werden. Sie werden direkt von den VPN-Konzentratoren der TI an den Konnektor übermittelt.

7.4.4 Verbindung in die Telematikinfrastruktur

Um TI- bzw. SIS-Verbindungen aufbauen zu können, ist eine erfolgreiche Registrierung am VPN-Zugangsdienst notwendig. Nur wenn diese Registrierung in der Konnektor-Konfiguration persistiert ist, kann eine VPN-Verbindung aufgebaut werden. Dies ist oben im Bereich VPN und dort im Abschnitt Registrierung beschrieben.

Dafür kann eine im Infomodell bekannte SMC-B genutzt werden.⁷⁹ Diese SMC-B sollte bereits eine Echt-PIN besitzen und in einem Kartenterminal, das für die Verwendung mit der Managementschnittstelle vorgesehen

⁷⁹ Siehe unten den Abschnitt Informationsmodell

ist, stecken..⁸⁰

Der Registrierungsprozess⁸¹ muss nur einmalig durchgeführt werden. Dabei speichert die KoCoBox MED+ die erfolgreiche Registrierung in der Konfiguration und fragt sie beim Verbindungsaufbau von dort ab. Zudem kann auch eine Deregistrierung durchgeführt werden. VPN-Verbindungen sind danach nicht mehr möglich.



Eine Anfrage zum Freischalten oder Aufheben eines bereits freigeschalteten Konnektors muss spezifikationskonform mittels einer XAdES-Signatur signiert und an den Registrierungsserver per SOAP-Protokoll gesendet werden.



Gibt es beim De-/Registrieren eine Fehlermeldung bezüglich der Firewall, ist der Leistungsumfang ONLINE (LU_ONLINE) deaktiviert und muss aktiviert werden..⁸²



Abbildung 59: Fehlermeldung beim Registrierungsdienst - Aktivierung Leistungsumfang ONLINE notwendig

⁸⁰ Siehe dazu den Abschnitt Kartenterminaldienst sowie unten die Zusammenfassung

⁸¹ Siehe dazu in Abschnitt VPN / Registrierung

⁸² Siehe unten den Abschnitt Verwaltung

Folgende Informationen ermöglichen eine erfolgreiche Registrierung: Da es eine Kundendaten-Datenbank auf Seiten des Registrierungservers gibt, ist die Überprüfung der ContractID erforderlich. Insofern muss jeder Konnektor – sofern er nicht zu Testzwecken abgewiesen werden will – eine gültige, für seine ICCSN ausgestellte ContractID verwenden.⁸³



Als SMC-B muss eine Karte verwendet werden, deren CA-Zertifikat in der aktuellen TSL der gewählten Umgebung enthalten ist.



Bitte stellen Sie sicher, dass der Konnektor eine **aktuelle** Zeiteinstellung hat⁸⁴, da der Registrierungsserver nur 30 Sekunden für den Registrierungsprozess vorsieht. Sollte die Uhrzeit des Konnektors von der des Registrierungservers stark abweichen, ist eine erfolgreiche Registrierung nicht möglich.

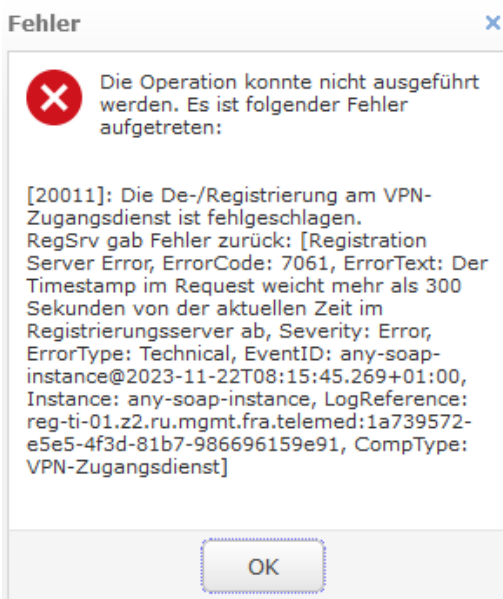


Abbildung 60: Fehlermeldung beim Registrierungsdienst wegen Zeitabweichung

Falls der Konnektor für den Online-Modus konfiguriert ist, baut er automatisch eine VPN-Verbindung zur TI auf, sobald er hochgefahren ist und alle Umgebungsparameter sowie TSL/CRL passend gesetzt sind.



Hier ist zu beachten, dass die korrekten Netze für die gewünschte Umgebung eingetragen werden.

⁸³ Weitere Informationen über das Beziehen einer ContractID können in der Dokumentation des VPN-Zugangsdienstes nachgelesen werden. Die ContractID ist gegebenenfalls separat zu beantragen.

⁸⁴ Siehe oben im Abschnitt Zeitdienst

7.4.4.1 Anschluss von Kartenterminals

Im unteren Abschnitt Kartenterminaldienst finden Sie ausführliche Erläuterungen zum Anschließen von Kartenterminals bzw. dem Pairing mit dem Konnektor. Führen Sie für die initiale Inbetriebnahme der KoCoBox MED+ für ein angeschlossenes Kartenterminal das Pairing durch (dies ist Voraussetzung für das Anmelden beim VPN-Zugangsdienst).

Bisher konfigurierte Kartenterminals bleiben durch einen Update-Prozess erhalten, die Konfigurationen werden jeweils übernommen. Zudem berücksichtigt die KoCoBox MED+ die bereits konfigurierten Status der Kartenterminals, sie werden beim Hochfahren des Geräts einbezogen und wiederhergestellt.



Kartenterminals, die angeschlossen werden sollen, müssen eine entsprechende Adresse aus dem konfigurierten IP-Adressraum der KoCoBox MED+ haben.

Die *Service Discovery* für Kartenterminals erfolgt bei der KoCoBox MED+ während des Gerätestarts sowie über den Button Kartenterminals finden im Kartenterminaldienst. Dadurch werden für erkannte Kartenterminals im lokalen Netzwerk Einträge in der Kartenterminal-Liste auf der Managementschnittstelle im Bereich *Kartenterminaldienst* erzeugt und angezeigt.



Man kann Kartenterminals auch manuell hinzufügen. Dafür muss die IP-Adresse des Geräts bekannt sein, sie darf nicht in der Liste der gefundenen Kartenterminals vermerkt sein.



Im Infomodell muss ein Arbeitsplatz namens *Konnektor* hinzugefügt werden, der mit den Kartenterminals verknüpft wird, mit denen PIN-Operationen über die Managementschnittstelle vorgenommen werden sollen. Auch neu hinzugefügte Kartenterminals sollten für eine zukünftige Nutzung an der Managementschnittstelle mit diesem Arbeitsplatz verknüpft werden.⁸⁵

⁸⁵ Siehe unten den Abschnitt Infomodell

7.4.4.2 Import von TSL/CRL

Voraussetzung für eine Verbindung zur Telematikinfrastruktur ist, initial eine TSL und CRL manuell in die KoCoBox MED+ zu importieren.⁸⁶

Ein TSL-Import ersetzt die aktuell verwendete Liste, wenn die zu importierende TSL entsprechend signiert und eine höhere Sequenznummer bzw. Seriennummer beinhaltet. Eine CRL muss über die Managementschnittstelle zusätzlich importiert werden. Der TSL-Import benötigt eine gewisse Zeit, währenddessen wird der *Bitte-Warten*-Balken angezeigt. Das Ende des Imports erfolgt durch die Bestätigungsmeldung.



Bitte verlassen Sie während des Imports die Seite des Zertifikatsdienstes **nicht**.

Zusätzlich können TSLs auch von definierten Downloadpunkten bezogen werden. Dies sowie die Aktualisierung erfolgt periodisch (innerhalb von 24 Stunden).⁸⁷



Erfolgreiche VPN-Verbindungen in die jeweilige Umgebung können nur dann aufgebaut werden, wenn sowohl eine gültige TSL als auch CRL aus dem gleichen Vertrauensraum im Konnektor gespeichert sind und die Registrierung am VPN-Zugangsdienst erfolgreich war.

OCSP-Prüfungen werden gegen den jeweiligen http-Forwarder in der Zielumgebung durchgeführt, der entsprechende Request an den im Zertifikat beschriebenen OCSP-Responder weiterleitet. Eine Erreichbarkeit des Forwarders kann über die Managementschnittstelle der KoCoBox MED+ im Bereich Zertifikatsdienst geprüft werden.

Wenn für das Gerät der Leistungsumfang ONLINE konfiguriert ist, wird beim Import der TSL immer versucht, das TSL-Signer-Zertifikat gegen den zugehörigen OCSP zu prüfen.



Wenn keine Verbindung zur TI besteht, kann dieser Schritt nicht erfolgreich durchgeführt werden. Dies bedeutet: Wenn – aus welchem Grund auch immer – **keine** Verbindung zu TI besteht, muss beim Konnektor der Leistungsumfang ONLINE auf *nicht aktiviert* gesetzt werden, damit eine TSL erfolgreich manuell importiert werden kann.

⁸⁶ Siehe dazu die detaillierten Ausführungen unten im Abschnitt Zertifikatsdienst

⁸⁷ TSL und CRL sind umgebungsabhängig und müssen für die Einwahl in die gewünschte Produktivumgebung (PU) entsprechend importiert und verfügbar gemacht werden.

7.5 Konfiguration des Anwendungskonnektors

Die KoCoBox MED+ unterstützt mittels TLS (Transport Layer Security)-Schnittstelle in Richtung der Clientsysteme für alle Außenschnittstellen die in den folgenden Abschnitten näher beschriebenen Basisdienste.⁸⁸ Deren jeweilige Konfigurationsmöglichkeiten werden im Folgenden erläutert.

7.5.1 Verwaltung

Unter *Verwaltung* können Sie – auch wenn der Konnektor im Auslieferungszustand alle Leistungsmerkmale aufweist – grundsätzliche Leistungsumfänge gezielt deaktivieren. Dies ermöglicht Ihnen, das Gerät besser in die technische/organisatorische Struktur der Betriebsstätte zu integrieren.⁸⁹ Zudem kann man hier den Neustart des Konnektors und den Werksreset durchführen.

In den Unterbereichen Clientsysteme und Ex-/Import erfolgt die Anbindung der Clientsysteme sowie das Ex-/Importieren der Konfigurationsdaten-Datei (einschließlich Kartenterminal-Konfigurationen).



Vor dem Import muss der Konnektor offline gesetzt werden (Radiobutton beim Leistungsumfang ONLINE auf nicht aktiviert einstellen), wenn zum Zeitpunkt des Imports keine aktive TI-Verbindung besteht oder aufgebaut werden kann.

Beim Import einer Konfiguration muss die durch den Konnektor generierte Passphrase zuerst eingegeben werden, erst danach wird die zu importierende Datei über den Dialog ausgewählt. Der Prozess beginnt unmittelbar.

⁸⁸ Vgl. [gemSpec_Kon], Kap. 3.4 „Fachliche Anbindung der Clientsysteme“

⁸⁹ Vgl. [gemSpec_Kon], S. 419 f.

Verwaltung der Leistungsumfänge

Leistungsumfang ONLINE: aktiviert nicht aktiviert

Leistungsumfang Signaturanwendungskomponente: aktiviert nicht aktiviert

Betrieb als Standalone Konnektor: aktiviert nicht aktiviert

Selbsttest

Reset

Werksreset

Betriebsdatenmeldedienst

Betriebsdaten automatisch senden: aktiviert nicht aktiviert

Lizenzbestimmungen

Abbildung 61: Konfigurationsbereich zur Verwaltung der Leistungsumfänge

Generell können Sie folgende Konfigurationen vornehmen und über die Buttons Übernehmen bzw. Verwerfen annehmen bzw. abbrechen:

- Deaktivieren des *Leistungsumfangs ONLINE*: Er muss für eine erfolgreiche Verbindung zur TI aktiviert sein. Dies ist per Voreinstellung gegeben.⁹⁰
- Der *Leistungsumfang Signaturanwendungskomponente* muss aktiviert sein, um zum einen Dokumente signieren oder verifizieren zu können – und zum anderen die automatische Aktualisierung der Vertrauensliste der Bundesnetzagentur (BNetzA-VL) zu erlauben. Dies ist per Voreinstellung aktiviert.
- Aktivieren für den *Betrieb als Standalone Konnektor*⁹¹: Dies ist per Voreinstellung deaktiviert.

⁹⁰ Wird diese Einstellung deaktiviert, so baut die KoCoBox MED+ grundsätzlich keine Online-Verbindungen auf – weder zur TI, noch zum SIS. Dies hat Auswirkungen auf die folgenden Funktionsmerkmale: Zertifikatsdienst, Anbindung der Clientsysteme (TLS-Dienst), Anbindung LAN/WAN, VPN-Client, Zeitdienst, Software-Aktualisierung (Update).

⁹¹ Bei Aktivierung führt der Konnektor mit Zugang zur TI ohne ein steuerndes Clientsystem ereignisgetrieben Fachanwendungen aus. Er steht aus Fachsicht somit ‚alleine‘, ohne Clientsysteme. [gemSpec_Kon], S. 27

Mittels Übernehmen speichern Sie die Einstellungen.



Bitte beachten Sie, dass eine gespeicherte Konfiguration abweichende IP-Adressen und Passworte enthalten kann. Nach dem Import dieser Konfiguration ist der Konnektor ausschließlich mit diesen Daten erreichbar.



Bitte beachten Sie, dass in einer Konfiguration mit aktivierten Anbindungsmodus SIS (siehe das Kapitel LAN / WAN) nach einem Deaktivieren des Leistungsumfangs ONLINE zwingend ein Neustart der KoCoBox MED+ zu erfolgen hat. Dies gewährleistet vollständige Konsistenz der Betriebsparameter.

Selbsttest

Über den Button Selbsttest führt der Konnektor eine Prüfung der Integrität der Daten im Dateisystem des Konnektors durch.

Der Vorgang wird nach Bestätigung der Rückfrage im Dialogfenster gestartet und nimmt einige Zeit in Anspruch. Ist das Prüfergebnis positiv, erscheint eine entsprechende Meldung. Somit liegen keinerlei Probleme mit Signaturen gespeicherter Daten vor.

Mittels OK wird die Prüfung beendet.

Ist das Prüfergebnis negativ, erscheint eine entsprechende Meldung, die Sie per OK schließen.

Ein negatives Testergebnis, d.h. ein Fehlschlag des Selbsttests, kann durch eine beeinträchtigte Integrität der konnektoreigenen Software bedingt sein. In diesem Fall erscheint auf der Status-Seite der Management-schnittstelle in der Tabelle Betriebszustandsmeldungen die Meldung *Software Integrity Check failed*, ebenso auf dem Display der KoCoBox MED+.



Sofern durch einen Neustart des Geräts die Meldung nicht behoben werden konnte, verwenden Sie den Konnektor nicht weiter. Kontaktieren Sie umgehend Ihren Support.

Reset

Durch Betätigung des Buttons Neustart des Konnektors erfolgt ein Neustart der KoCoBox MED+. Im Verlauf des Neustarts führt das Gerät automatisch einen Selbsttest aus.

Mit dem Button `EC_OTHER_ERROR_STATE` zurücksetzen kann ein Benutzer (mit der Rolle *Super-Administrator* oder *Administrator*) den Fehlerzustand `EC_OTHER_ERROR_STATE` des Konnektors manuell aufheben.⁹²



Solange dieser sicherheitskritische Fehlerzustand anhält, kann die KoCoBox MED+ folgende Aufgaben nicht ausführen:

⁹² Der Fehlerzustand `EC_OTHER_ERROR_STATE(1)` entsteht, wenn der Konnektor als Folge einer Out-of-Memory-Exception in einen sog. Heap-Overflow gerät: Dabei kommt das Gerät aufgrund der Verarbeitung großer Dateien an die Grenzen seines internen Speichers, die weitere Datenverarbeitung ist dadurch nicht mehr möglich. Der Konnektor erkennt selbst diese Fehlersituation und meldet sie dem System als Fehler `EC_OTHER_ERROR_STATE(1)`. In Folge des Heap-Overflows wird der Konnektor heruntergefahren und neu gestartet. Der Fehlerzustand `EC_OTHER_ERROR_STATE(2)` besitzt den Charakter einer Warnung und entsteht, wenn der Protokollspeicher des Konnektors zu mehr als 80 Prozent gefüllt ist.

- automatisches Update der TSL und CRL vom Downloadpunkt
- Beziehen von KSR-Updateinformationen und -paketen.

Nach dem manuellen Zurücksetzen des Fehlerzustands über den Button EC_OTHER_ERROR_STATE zurücksetzen nimmt der Konnektor automatisch einen Neustart vor. Alle Systemdienste der KoCoBox MED+ werden neu initialisiert.



Durch Eingabe der IP-Adresse des Konnektors (<https://<IP-KON>:9443/administration/start.htm>) ist dieser wieder erreichbar. Eventuell wird Ihnen durch Ihren Browser eine andere, ähnliche URL angeboten. Diese ist manuell auf die anfangs im Display angezeigte Startadresse zu korrigieren.

Werksreset

Eine ausführliche Beschreibung der Möglichkeiten des Werksresets finden Sie unten im Kapitel Konnektormanagement / Werksreset.

Betriebsdatenmeldedienst

Die KoCoBox MED+ kann im Rahmen des Betriebsdatenmeldedienstes (BDMD) regelmäßig Zustandsdaten an eine definierte zusätzliche Schnittstelle des VPN-Zugangsdienstes senden. Voraussetzung für die erfolgreiche Operation ist eine freigeschaltete SMC-B.

Die übermittelten Informationen umfassen:

- Produktinformation (Statusinformation) des Konnektors
- Anbindungsmodus TI/SIS
- Einstellungen der Clientsystemanbindung
- Einstellungen des SW-Updates
- Informationen zu den Zertifikaten der gSMC-Ks im Konnektor, insbesondere Ablaufzeitpunkte
- Informationen zu den verbundenen KTs
- Informationen zur aktuellen TSL, BnetzA-VL und CRL im Konnektor

Über den Button Betriebsdaten senden können diese Informationen unmittelbar verschickt werden.

Das Senden der Betriebsdaten kann automatisch erfolgen. Diese Funktion ist per Voreinstellung aktiviert. Die Betriebsdaten werden somit ein Mal täglich an den VPN-Zugangsdienst übermittelt. Durch Auswahl der Einstellung nicht aktiviert wird der automatische Versand der Betriebsdaten unterbunden.

Per Übernehmen werden Änderungen in dieser Konfiguration (Radiobutton nicht aktiviert) gespeichert.



Hierbei werden keinerlei personenbezogene, personenbeziehbare oder medizinische Daten.⁹³ versandt.

⁹³ Die Vertragsnummer (ContractId) wird konform zu den gematik-Vorgaben der Telematik-API (OperatingData.xsd) verpflichtend an den VPN-Zugangsdienst übermittelt und dort vor jeglicher Weitergabe der Daten an die gematik entfernt.

Lizenzbestimmungen

Am Fue des Anzeigefensters im Bereich *Verwaltung der Leistungsumfnge* knnen Sie sich ber den Button Lizenzbestimmungen anzeigen das entsprechende Dokument fr die KoCoBox MED+ als Text anzeigen lassen. Sie finden hier Informationen zur Lizenzierung der Software, einen Haftungshinweis sowie die Datenschutzerklrung des Herstellers der KoCoBox MED+.

Die KoCoBox MED+ enthlt Open Source Software. Bitte beachten Sie hierzu das Kapitel *Lizenzinformationen* im Anhang.

7.5.1.1 Clientsysteme

In diesem Unterbereich werden die Konfigurationen zur Anbindung der Clientsysteme durchgefhrt.

Anbindung Clientsysteme

Zugriff auf Dienstverzeichnisdienst auch via HTTP ermglichen: ein aus
 Verbindung nur via TLS: ein aus

Authentisierung Clientsystem

Authentisierung verpflichtend: ein aus
 Authentisierungsmodus-LDAP: ein aus
 Authentisierungsmodus-SOAP: Zertifikat Benutzername / Passwort

Zugangsdaten fr Clientsysteme:

| Clientensystem | Benutzer |
|----------------|----------|
| WP2 | user123 |

Zertifikat fr Authentisierung Clientsystem hinzufgen ...

| Clientensystem | Distinguished Name | Aussteller | Kryptographisches Verfahren | Gltigkeitsdauer | SHA256-Fingerabdruck |
|----------------|--------------------|------------|-----------------------------|---|---|
| WP2 | CN=WP2 | CN=KoCoBox | ECC-256 | notBefore = Tue Nov 21 12:20:52 CET 2023, notAfter = Sun Jan 10 12:56:46 CET 2027 | 83 5E 39 FE 8F 5B F9 77 DD BE A6 47 48 F4 F2 92 65 96 19 A5 6A 43 58 CE 91 BB 55 DA 37 73 DD FF |
| WP1 | CN=WP1 | CN=KoCoBox | ECC-256 | notBefore = Tue Nov 21 12:21:27 CET 2023, notAfter = Sun Jan 10 12:56:46 CET 2027 | 26 F1 83 AD 8C 04 F4 9F 42 75 D6 91 1C 8B AE A7 48 4A E0 DC 40 69 8F F0 11 EF 78 90 1C A6 74 5D |

Authentisierung Konnektor

Zertifikat fr Authentisierung Konnektor hinzufgen ...

| Aktiv | Alias | Distinguished Name | Aussteller | Kryptographisches Verfahren | Gltigkeitsdauer | SHA256-Fingerabdruck |
|----------------------------------|-----------|---|---|-----------------------------|---|---|
| <input checked="" type="radio"/> | C.AK-AUT | C=DE,ST=Berlin,L=Berlin,PostalCode=10963,STREET=Dessauer Str. 28/29,O=KoCo Connector GmbH TEST-ONLY - NOT-VALID,CN=8027688358000048312-20220111 | C=DE,O=gematik GmbH NOT-VALID,OU=Komponenten-CA der Telematikinfrastruktur,CN=GEM.KOMP-CA54 TEST-ONLY | RSA-2048 | notBefore = Tue Jan 11 12:56:47 CET 2022, notAfter = Sun Jan 10 12:56:46 CET 2027 | 9D 17 91 AB 9B 03 D5 00 15 51 C2 F2 4A BE 14 E7 D2 66 4D B1 36 73 91 24 F0 8F 03 18 F0 40 79 E9 |
| <input type="radio"/> | C.AK-AUT2 | C=DE,ST=Berlin,L=Berlin,PostalCode=10963,STREET=Dessauer Str. 28/29,O=KoCo Connector GmbH TEST-ONLY - NOT-VALID,CN=8027688358000048312-20220111 | C=DE,O=gematik GmbH NOT-VALID,OU=Komponenten-CA der Telematikinfrastruktur,CN=GEM.KOMP-CA50 TEST-ONLY | ECC-256 | notBefore = Tue Jan 11 12:56:44 CET 2022, notAfter = Sun Jan 10 12:56:43 CET 2027 | 16 14 CB 9B F0 A6 83 6E A4 43 5A 22 50 E7 44 4F 60 78 01 D3 D6 A4 3D 5D AD EB 81 E9 F0 85 8F 86 |

Abbildung 62: Konfigurationsbereich fr die Anbindung der Clientsysteme

Die Anbindung der Clientsysteme sollte grundstzlich TLS-geschtzt (und damit ber https) erfolgen. Da dies nicht von allen Clientsystemen untersttzt wird, ermglicht die KoCoBox MED+ per Konfiguration zustzlich den Zugriff ber http.

Der Aufbau von TLS-Verbindungen zwischen Clientsystem und Konnektor erfolgt entweder einseitig oder beidseitig authentisiert. Hierzu sind verschiedene Konfigurationen sowohl fr die Clientsystemseite als auch fr die Konnektorseite mglich.

Die KoCoBox MED+ authentisiert sich grundstzlich mit Hilfe eines Zertifikats gegenber dem Clientsystem. Standardmig wird hierzu das Zertifikat C.AK.AUT der im Konnektor befindlichen gSMC-K verwendet. Es ist mglich, an dieser Stelle ein anderes Zertifikat durch den Konnektor zu erzeugen und exportieren (z.B. auf Basis elliptischer Kurven gem NIST-Spezifikation). Dieses kann dann dem Clientsystem zur Verfgung gestellt werden.



Alternativ erlaubt der Konnektor den Import eines Schlsselpaars mit X.509-Zertifikat in Form einer passwortgeschtzten PKCS#12-Datei. Aus der Menge dieser Zertifikate ist in der Clientsystem-Verwaltung genau eines fr die TLS-Authentisierung des Konnektors gegenber dem Clientsystem auszuwhlen.

Für das Clientsystem kann konfiguriert werden, ob generell eine Authentisierung erfolgen soll oder nicht. Falls ja, kann diese entweder mittels einer Kombination aus Benutzername und Passwort oder auf Basis eines Zertifikats stattfinden. Soll ein Zertifikat zum Einsatz kommen, so kann dieses durch den Konnektor erzeugt und als passwordgeschützte PKCS#12-Datei exportiert werden. Diese Daten können dann dem Clientsystem zur Verfügung gestellt werden.



Alternativ gestattet die KoCoBox MED+ den Import eines Zertifikats, das in der Clientsystem-Verwaltung des Konnektors einem Clientsystem zugeordnet wird.



Bitte beachten Sie:

- Ohne Authentisierung des Konnektors durch das Clientsystem (TLS-Client-Authentication) können CETP-Nachrichten (Benachrichtigungen, die durch den Konnektor an das Clientsystem gesendet werden) nicht authentisch, integer und vertraulich empfangen werden.
- Ohne Authentisierung durch das Clientsystem könnte ein Angreifer dem Clientsystem beliebige, irreführende Nachrichten senden und damit die Abläufe in der Praxis stören.
- Eine ungesicherte Verbindung zwischen Clientsystem und Konnektor bietet gar keinen Schutz gegen Man-in-the-Middle Attacken und ist daher zu vermeiden.
- Eine einseitige TLS-Authentisierung des Konnektors kann dazu führen, dass unbemerkt qualifizierte elektronische Signaturen (QES) über von Angreifern aus dem LAN bereitgestellte Dokumente erzeugt werden.

Zunächst wird mittels Radiobutton ja/nein der Zugriff auf den *Dienstverzeichnisdienst* (immer) *auch via http* ermöglicht bzw. unterbunden. Per Voreinstellung ist dies möglich.

In der nächsten Zeile *Verbindung nur via TLS* kann die verpflichtende Verwendung eines TLS gesicherten Kanals mittels Radiobutton ein/aus an- oder abgeschaltet werden. Per Voreinstellung ist dies eingeschaltet.



Beim Abschalten erscheint ein Warnhinweis. In diesem müssen Sie als Administrator bestätigen, dass Sie über die mit der Abschaltung verbunden Risiken informiert sind. In diesem Fall übernimmt der Endkunde die Verantwortung für die Sicherstellung der vertraulichen Übertragung.

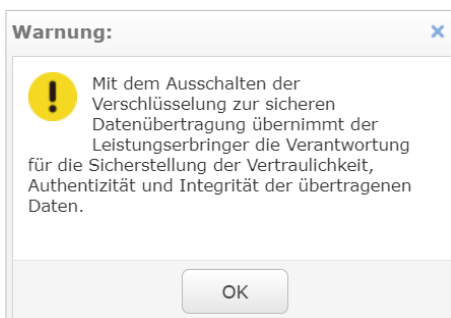


Abbildung 63: Warnhinweis beim Ausschalten der TLS-Option

Eine TLS-Verbindung ist auch möglich, wenn die verpflichtende Verwendung von TLS ausgeschaltet ist. In diesem Fall werden die dazu angezeigten, inaktiv dargestellten, Optionen aus dem Bereich *Authentisierung Clientsystem* verwendet.

Im Bereich *Authentisierung Clientsystem* können Sie über den Radiobutton *aktiviert/nicht aktiviert* die verpflichtende Authentisierung der Clientsysteme gegenüber dem Konnektor konfigurieren. Diese ist per Voreinstellung aktiviert.

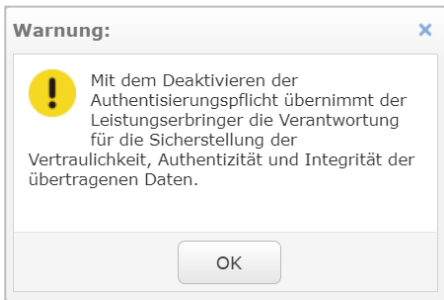


Abbildung 64: Warnhinweis beim Ausschalten der verpflichtenden Authentisierung



Beim Abschalten erscheint ein Warnhinweis. In diesem müssen Sie als Administrator bestätigen, dass Sie über die mit der Abschaltung verbundenen Risiken informiert sind. In diesem Fall übernimmt der Endkunde die Verantwortung für die Sicherstellung der Vertraulichkeit, Authentizität und Integrität der übertragenen Daten.



Falls TLS aktiviert wird, müssen entsprechende Konfigurationen am Clientsystem vorgenommen werden.⁹⁴



Die Funktion Komfortsignatur kann nur bei aktivierter Option *Authentisierung verpflichtend* eingeschaltet werden.

Der Authentisierungsmodus kann separat für den LDAP-Dienst über den Radiobutton *Authentisierungsmodus-LDAP* konfiguriert werden. Voreingestellt ist: ein. Hier ist zu beachten, dass die clientseitige Authentisierung immer per Zertifikat erfolgt – nicht per Benutzername/Passwort.

Anschließend wird der *Authentisierungsmodus-SOAP* für das Clientsystem gegenüber dem Konnektor per Radiobutton definiert: per *Zertifikat* oder *Benutzername/Passwort*. Voreingestellt ist Zertifikat.

In den beiden Tabellen werden je nach definiertem Authentisierungsmodus entweder die *Zugangsdaten* oder die *Zugangszertifikate* für die Clientsysteme angezeigt.

Im Bereich *Zugangsdaten für Clientsysteme* ordnen Sie per Zugangsdaten hinzufügen der jeweiligen *Clientsystem-ID* eine *Benutzer/Passwort*-Kombination zu und bestätigen dies über den Button OK.

⁹⁴ Diese sind dem jeweiligen Handbuch zu entnehmen.

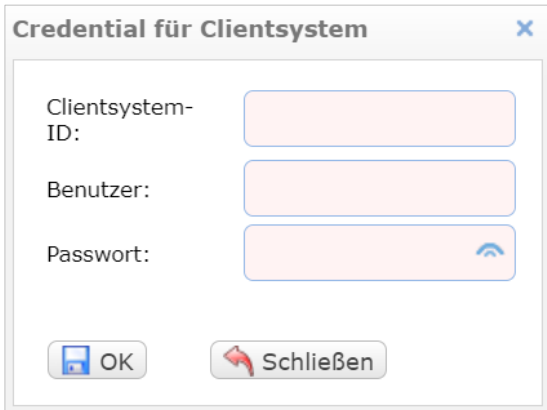


Abbildung 65: Konfiguration der Zugangsdaten für das Clientsystem



Bitte beachten Sie bei der Wahl des Passworts⁹⁵, dass dies technisch zwar ab sechs Zeichen möglich ist, aber mindestens 17 Zeichen⁹⁶ empfohlen werden, um ausreichend Sicherheit zu gewährleisten. Falls Sie ein zu kurzes - und damit unsicheres - Passwort eintragen, erscheint ein entsprechender Warnhinweis.



Über das Augen-Symbol in der Passwort-Zeile können Sie sich Ihr eigenes Passwort im Klartext anzeigen lassen.

Alternativ können Sie über den Button Zufallspasswort generieren ein Passwort erzeugen lassen.

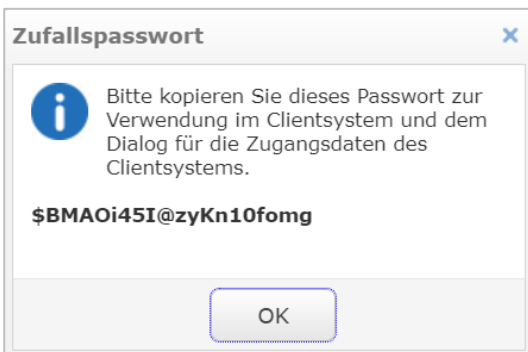



Abbildung 66: Zufallspasswort zur Anbindung des Clientsystems


Folgen Sie den Anweisungen im Dialogfeld und tragen Sie das erzeugte Zufallspasswort per Copy & Paste ein. Dazu öffnen Sie über den Button Zugangsdaten hinzufügen den Konfigurationsbereich für die Clientsystem-Anbindung.

Hier können Sie im *Passwort*-Feld per Klick auf das Augen-Symbol  entscheiden, ob Sie sich das Zufallspasswort im Klartext anzeigen lassen oder nicht. Bestätigen Sie die Ihre Einträge (*Clientsystem-ID*, *Benutzer* sowie *Passwort* abschließend mit OK.

⁹⁵ Siehe dazu die Sicherheitshinweise zum Passwort in Kapitel Administratorpasswort.

⁹⁶ Bei dem für Passwörter verfügbaren Zeichenvorrat entspricht dies einem Sicherheitsniveau von 100 Bits.

Abbildung 67: Passwordeintrag für Clientsystem mit aktiverter Ansicht des Passworts

Nachdem Sie die Clientsystemanbindung abgeschlossen haben und bei einem Tabelleneintrag mittels  dessen Konfigurationsfenster erneut öffnen, sehen Sie aus Sicherheitsgründen im Passwortfeld **keinen** Eintrag, obwohl das Passwort für diese Clientsystemanbindung zugeordnet und hinterlegt ist.

Anbindung Clientsysteme

Zugriff auf Dienstverzeichnisdienst auch via HTTP ermöglichen: ein aus
 Verbindung nur via TLS: ein aus

Authentisierung Clientsystem

Authentisierung verpflichtend: ein aus
 Authentisierungsmodus-LDAP: ein aus
 Authentisierungsmodus-SOAP: Zertifikat Benutzername / Passwort

Zugangsdaten für Clientsysteme:

| Clientsystem | Distinguished Name | Aussteller | Kryptographisches Verfahren | Gültigkeitsdauer | SHA256-Fingerabdruck |
|--------------|--------------------|------------|-----------------------------|---|---|
| WP2 | CN=WP2 | CN=KoCoBox | ECC-256 | notBefore = Tue Nov 21 12:20:52 CET 2023, notAfter = Sun Jan 10 12:56:46 CET 2027 | 83 5E 39 FE 5B F9 77 DD BE A6 47 48 F4 F2 92 65 96 19 A5 6A 43 98 CE 91 BB 55 DA 37 73 D0 FF |
| WP1 | CN=WP1 | CN=KoCoBox | ECC-256 | notBefore = Tue Nov 21 12:21:27 CET 2023, notAfter = Sun Jan 10 12:56:46 CET 2027 | 26 F1 83 A0 8C 04 F4 9F 42 75 D6 91 1C 8B AE A7 A8 4A E0 DC 40 69 8F F0 11 EF 7B 90 1C A6 74 5D |

Authentisierung Konnektor

Zertifikat für Authentisierung Konnektor hinzufügen ...

| Aktiv | Alias | Distinguished Name | Aussteller | Kryptographisches Verfahren | Gültigkeitsdauer | SHA256-Fingerabdruck |
|----------------------------------|-----------|---|---|-----------------------------|---|---|
| <input checked="" type="radio"/> | C.AK.AUT | C=DE,ST=Berlin,L=Berlin,PostalCode=10963,STREET=Desauyer Str. 28/29,O=KoCo Connector GmbH,TEST-ONLY - NOT-VALID,CN=8027688359000048312-20220111 | C=DE,O=gematik GmbH NOT-VALID,OU=Komponenten-CA der Telematikinfrastruktur,CN=GEM.KOMP-CA54-TEST-ONLY | RSA-2048 | notBefore = Tue Jan 11 12:56:47 CET 2023, notAfter = Sun Jan 10 12:56:46 CET 2027 | 90 17 91 A8 9B D3 D5 D0 15 51 C2 F2 4A BE 14 E7 D2 66 4D B1 36 73 51 2A F0 8F D3 1B F0 40 79 E5 |
| <input type="radio"/> | C.AK.AUT2 | C=DE,ST=Berlin,L=Berlin,PostalCode=10963,STREET=Desauyer Str. 28/29,O=KoCo Connector GmbH,TEST-ONLY - NOT-VALID,CN=8027688359000048312-20220111 | C=DE,O=gematik GmbH NOT-VALID,OU=Komponenten-CA der Telematikinfrastruktur,CN=GEM.KOMP-CA50-TEST-ONLY | ECC-256 | notBefore = Tue Jan 11 12:56:44 CET 2023, notAfter = Sun Jan 10 12:56:43 CET 2027 | 16 14 CB 9B F0 A6 83 6E A4 43 5A 22 50 E7 44 4F 60 7B 01 D3 D6 A4 3D 50 AD EB B1 E8 F0 85 8F 86 |

Abbildung 68: Übersicht zu angebotenen Clientsystemen

Im Bereich *Authentisierung Clientsystem* findet man eine tabellarische Übersicht darüber. Hier werden *Clientsystem*, *Distinguished Name*, *Aussteller*, *Kryptographisches Verfahren*, *Gültigkeitsdauer* und *SHA 256-Fingerabdruck* der Zugangszertifikate aufgelistet.

Über *Zertifikat für Authentisierung Clientsystem hinzufügen...* ordnen Sie der jeweiligen Clientsystem-ID ein Zertifikat zu.

Dazu öffnet sich nach Klick auf diesen Button ein Pop-up-Fenster.



Abbildung 69: Konfiguration zum Anlegen eines Clientsystem-Zertifikats mit ECC

Darin tragen Sie die Clientsystem-ID ein und wählen per Radiobutton das gewünschte Zertifikat aus.

1 Zum einen können Sie vom Konnektor konnektor-eigene Zertifikate (RSA-2048, RSA-3072 oder ECC mit den Kurvenparametern brainpoolP256r1 oder secp256r1) erzeugen lassen. Diese werden als Container per Download zur Verfügung gestellt und stehen dann für die Konfiguration der sicheren Verbindung mit dem Clientsystem bereit.⁹⁷



Beim Erzeugen entstehen in der Tabelle ein neuer Eintrag für das Endgeräte-Zertifikat (z.B. *WP 2*) sowie für den Download der Zertifikatscontainer.⁹⁸ im Format PKCS#12 mit diesem Endgeräte-Zertifikat und dem zugehörigen CA-Zertifikat (z.B. *Konnektor-72*⁹⁹). Dieser Zertifikatscontainer ist auch zur geschützten Anbindung an die LDAP-Funktionalität (z.B. KIM-Client) der KoCoBox MED+ geeignet.

2 Alternativ können Sie ein durch das Clientsystem bereitgestelltes Zertifikat in den sicheren Zertifikatspeicher des Konnektors importieren. Wählen Sie dafür die Option selbst erstelltes Zertifikat importieren. Nach Klick auf OK werden Sie aufgefordert, das Zertifikat im Dateisystem auszuwählen und hochzuladen.



Bitte beachten Sie:

- Die Clientsystem-ID und Clientsystem-Bezeichnung im Infomodell müssen identisch sind.
- In den Konnektor wird nur der öffentliche Schlüssel importiert.
- Der Konnektor unterstützt DER-encoded oder PEM-Zertifikate der Schlüsseltypen RSA-2048 und RSA-3072 sowie ECC mit den Kurvenparametern brainpoolP256r1 oder secp256r1 (NIST).



Bitte beachten Sie, dass nach einer Änderung der Methoden zur Zertifikatsnutzung ein **Neustart** des Konnektors notwendig ist. Damit werden die Änderungen konnektorweit übernommen und das Clientsystem kann eine gesicherte Verbindung mit dem Konnektor aufbauen.



Bitte achten Sie beim Import selbst erstellter Zertifikate darauf, dass diese hinsichtlich Kryptoalgorithmen und Schlüssellängen den Empfehlungen in der BSI-Richtlinie [TR-03116-1] entsprechen. Werden hingegen Zertifikate mit **nicht konformen** Algorithmen und/oder Schlüssellängen importiert, dann gilt das Clientsystem in einer entsprechenden TLS-basierten Verbindung als **nicht authentifiziert**. Das bedeutet, dass der sichere Einsatz des Konnektors im LAN **nicht** gegeben ist.

⁹⁷ Das Importieren dieses Zertifikatscontainers wird in der Dokumentation des Clientsystems beschrieben.

⁹⁸ Der Zertifikatscontainer wird in einem zip-Archiv verpackt für den Download bereitgestellt.

⁹⁹ Dieser Bezeichner wird von dem unter LAN/WAN eingestellten Hostnamen abgeleitet. Es handelt sich um ein selbstsigniertes Zertifikat mit einer zum Endgeräte-Zertifikat identischen Laufzeit.



Die Verwendung von RSA-Schlüsseln mit einer Mindestlänge von 3072 Bits oder von ECC-Zertifikaten sollte bevorzugt werden, da entsprechend BSI-Richtlinie [TR-03116-1] die Nutzung von RSA-Schlüsseln mit der Länge von 2048 Bits nur bis Ende 2023 empfohlen wurde.



Bei Verwendung der Kombination Benutzername/Passwort soll der Benutzer im Clientsystem sein Passwort **erst dann** eingeben, wenn die Verbindung offensichtlich TLS-geschützt ist.¹⁰⁰

Standardmäßig authentisiert sich der Konnektor gegenüber einem Clientsystem mit seinem Zertifikat C.AK.AUT als RSA-2048 Schlüssel. Mit der Einführung von ECC-Schlüsseln und auch größerer RSA-Schlüssel ist eine genaue Auswahl, welche Schlüssel den Konnektor authentisieren, erforderlich. Diese wird nachfolgend beschrieben.

Im Bereich *Authentisierung Konnektor* können Zertifikate für die Konnektorauthentisierung gegenüber mit ihm verbundenen Clients in der Tabelle eingesehen werden.



Bitte beachten Sie, dass hier ein Zertifikat ausgewählt sein **muss**.

Über den Button Zertifikat für Authentisierung Konnektor hinzufügen... können Sie entsprechende Zertifikate einbringen.

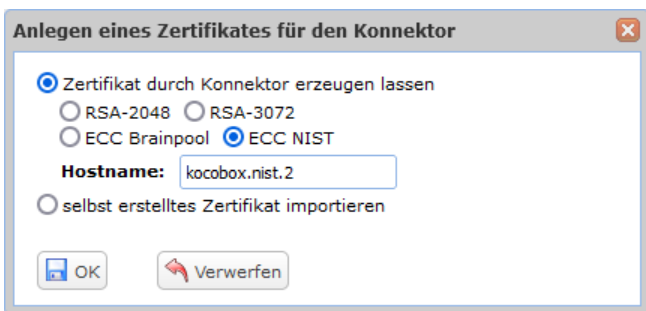


Abbildung 70: Anlegen eines Konnektor-Authentisierungszertifikats ECC-NIST

Im Dialogfeld zum Anlegen eines Zertifikats für den Konnektor können Sie auswählen, ob Sie ein Zertifikat vom Konnektor erzeugen lassen – hier stehen die Optionen RSA-2048, RSA-3072, ECC Brainpool oder ECC NIST.¹⁰¹ zur Verfügung – oder alternativ ein selbst erstelltes Zertifikat importieren.¹⁰²

Der Konnektor unterstützt das Generieren sowie den Import von Authentisierungszertifikaten der Schlüsseltypen RSA-2048, RSA-3072 sowie ECC mit den Kurvenparametern brainpoolP256r1 oder secp256r1 (NIST).

¹⁰⁰ Dies ist implementierungsabhängig im Clientsystem vorhanden. Bitte wenden Sie sich bei Unklarheiten an dessen Hersteller.

¹⁰¹ In der Hersteller-Dokumentation des entsprechenden Primärsystems ist die Information zu finden, welcher Schlüsseltyp verwendet werden muss (ECC Brainpool oder ECC NIST). In beiden Fällen wird mit 256 Bit-Schlüsseln operiert.

¹⁰² Es lassen sich ausschließlich PKCS#12-Container importieren - also inklusive des zugehörigen privaten Schlüssels. Dies ist notwendig, da die KoCoBox MED+ im Zuge der Konnektorauthentisierung selbst Signieroperationen ausführt.



Die Verwendung von RSA-Schlüsseln mit einer Mindestlänge von 3072 Bits oder von ECC-Zertifikaten sollte bevorzugt werden, da entsprechend der BSI-Richtlinie [TR-03116-1] die Nutzung von RSA-Schlüsseln mit der Länge von 2048 Bits nur bis Ende 2023 empfohlen wurde.



Sofern hier Zertifikate mit RSA-2048 konfiguriert sind, meldet der Konnektor den Betriebszustand `EC_TLS_Client_Certificate Security`¹⁰³. Bis Ende 2025 ist der Einsatz dieser Schlüssel zulässig. Dieser Betriebszustand wird durch einen Wechsel auf längere RSA-Schlüssel oder generell ECC-Schlüssel aufgehoben. Aus Sicherheitsgründen wird, spätestens bei Auftreten des genannten Betriebszustands, ein Wechsel auf RSA-3072-Schlüssel bzw. ECC-Schlüssel empfohlen.

Im Feld *Hostname* können Sie einen spezifischen Hostnamen eintragen, der zum Generieren des Zertifikats benutzt wird. Der eingegebene Hostname wird hierbei zum CN bzw. SubjectAltName im Zertifikat.

Mittels OK speichern Sie die Konfiguration ab.

Sofern Sie die Option Zertifikat durch Konnektor erzeugen lassen gewählt haben, wird im Zuge der Erzeugung einmalig eine zip-Datei mit dem Konnektor-Authentisierungszertifikat und dem ausstellenden CA-Zertifikat durch den Browser zum Download angeboten.

Das CA-Zertifikat sollte für das Clientsystem in dessen genutztem Zertifikatsspeicher hinterlegt werden, damit die Authentizität des Konnektors bei Verbindungen zwischen Clientsystem und Konnektor korrekt geprüft werden kann.



Bitte achten Sie unbedingt darauf, für den Hostnamen ausschließlich die Zeichen **A-Z**, **a-z**, **0-9**, **.**, **—** zu verwenden. Als erstes Zeichen des Hostnamens sind unzulässig: **.** (Punkt) sowie **—** (Bindestrich).

Sofern Sie die Option selbst erstelltes Zertifikat importieren gewählt haben, werden Sie nach Klick auf OK aufgefordert, das Zertifikat im Dateisystem auszuwählen und hochzuladen.



Der Konnektor authentisiert sich bei aktivierter TLS-Verbindung im Bereich *Verwaltung* gegenüber dem Clientsystem.

Für den Administratorzugang (TCP-Port 9443) können keine Zertifikate für die Konnektorauthentisierung konfiguriert werden. Standardmäßig wird hier das Zertifikat C.AK.AUT verwendet.

Sofern der Client ECDSA mit Brainpoolkurven unterstützt, kann er das während der TLS-Schlüsselaushandlung über das Feld `supported_groups` im ClientHello anzeigen. Dann verwendet die KoCoBox MED+ das passende Zertifikat C.AK.AUT2 (ECDSA mit einem Schlüssel auf einer brainpoolP256r1-Kurve). Diese Funktion wird von üblichen Webbrowsern nicht unterstützt.

7.5.1.2 Ex-/Import

In diesem Unterbereich können Sie den *Import / Export der Konfigurationsdaten* der KoCoBox MED+ (z.B. nach einem Werksreset oder auf ein neues Gerät) durchführen.

¹⁰³ Dies gilt auch für lauffzeitverlängerte Schlüssel, da diese ebenfalls vom Typ RSA-2048 sind.

Die vollständige Konnektor-Konfiguration (Netzkonnektor, Anwendungskonnektor inkl. Fachmodule) wird verschlüsselt und signiert exportiert. Alle Konfigurationsparameter werden in einer gezippten Datei zum Download angeboten. Die exportierte Konfiguration wird mittels der anzugebenden Passphrase symmetrisch verschlüsselt und mit der verwendeten SMC-B signiert.



Bitte beachten Sie hierzu besonders die Sicherheitshinweise am Ende des Kapitels.

Export / Import der Konfigurationsdaten

Export

SM-B ICCSN:

Import

Passphrase:

Abbildung 71: Konfigurationsdaten exportieren und importieren



Bitte beachten Sie folgende Hinweise:

- Der Export der gesamten Konnektor-Konfiguration beinhaltet auch sämtliche **Kartenterminal-Konfigurationen**. Diese können anschließend beim Import der Konnektor-Konfiguration bei Bedarf selektiv in die KoCoBox MED+ importiert werden. Dabei werden die Kartenterminal-IDs (CT-IDs) aus der Ursprungskonfiguration übernommen.
- Sofern die Konfigurationen in eine andere KoCoBox MED+ importiert werden, wird automatisch ein **Wartungspairing** durchgeführt, wenn der zuvor eingestellte Status des Kartenterminals größer als zugewiesen war.
- Prüfen Sie **vor dem Export**, ob sich in den Entitätsbezeichnern des Infomodells (siehe Kapitel Infomodell) ungültige Zeichen befinden. Korrigieren Sie dies gegebenenfalls. Ansonsten besteht die Gefahr, dass die exportierten Daten bei einem erneuten Import abgelehnt werden.
- Für den **Export** muss eine **SMC-B verfügbar** sein. Diese wird über das Dropdown-Menü ausgewählt und muss dann mittels PIN an einem aktiven Kartenterminal freigeschaltet werden
- Für den **Import einer Konfiguration** muss eine **aktuell gültige TSL** im Konnektor vorhanden sein.

Gehen Sie für den Export wie folgt vor:

- 1 Wählen Sie zunächst über das Drop-down Menü eine SM-B aus. Diese muss im Infomodell hinterlegt worden sein.¹⁰⁴

Abbildung 72: Auswahl der SM-B für Export der Konfigurationsdaten

- 2 Klicken Sie den Button Export Konfiguration. Am Kartenterminal werden Sie aufgefordert, die zur ausgewählten SM-B gehörende PIN einzugeben.¹⁰⁵

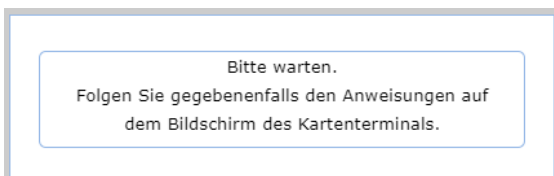


Abbildung 73: Anzeige für den Exportprozess

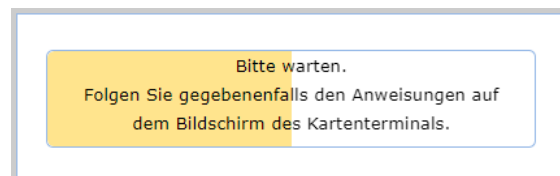


Abbildung 74: Anzeige für den Fortschritt im Exportprozess

Beim Import von Konfigurationen kann es trotz ansonsten korrekter Daten vorkommen, dass die zum Zeitpunkt des Exports verwendete SMC-B nun abgelaufen ist. Ist dies eingetreten, dann erscheint ein Dialog mit einer Rückfrage. Prüfen Sie hierbei, ob die im Feld *Ausgestellt für/Subject* dargestellte Organisation zur Praxis bzw. Klinikabteilung passt. Überlegen Sie, ob Sie diesem Zertifikat noch vertrauen können. Nur wenn dies gegeben ist, sollten Sie mit ja fortfahren. Ansonsten empfiehlt sich ein Abbruch des Imports.

¹⁰⁴ Siehe den Abschnitt Infomodell

¹⁰⁵ Die Konfigurationsdaten werden an dieser Stelle mit einer CMS Signatur versehen. Dazu wird der Schlüssel PrK.HCI.OSIG.R2048 der zuvor freigeschalteten SMC-B verwendet.

- 3** Per Anzeigefenster erscheint die Rückfrage zum Export sowie das Importpasswort (= *Passphrase*) mit dem Hinweis, dass diese für den Import benötigt wird. Notieren sie dieses und bewahren Sie sie sicher auf. Sie wurde einmalig erzeugt und ist nur für diese Exportdatei gültig.

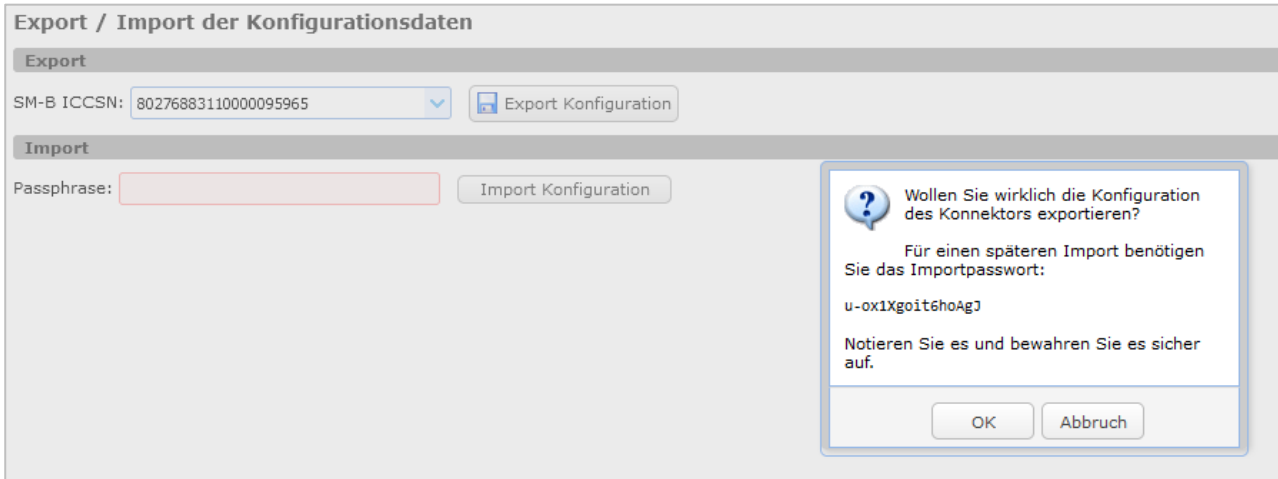


Abbildung 75: Importpasswort für späteren Import der Konfigurationsdaten

- 4** Im daraufhin erscheinenden Download-Fenster wählen Sie einen Speicherort für die Konfigurationsdaten-Datei aus und bestätigen Sie diesen mit OK.

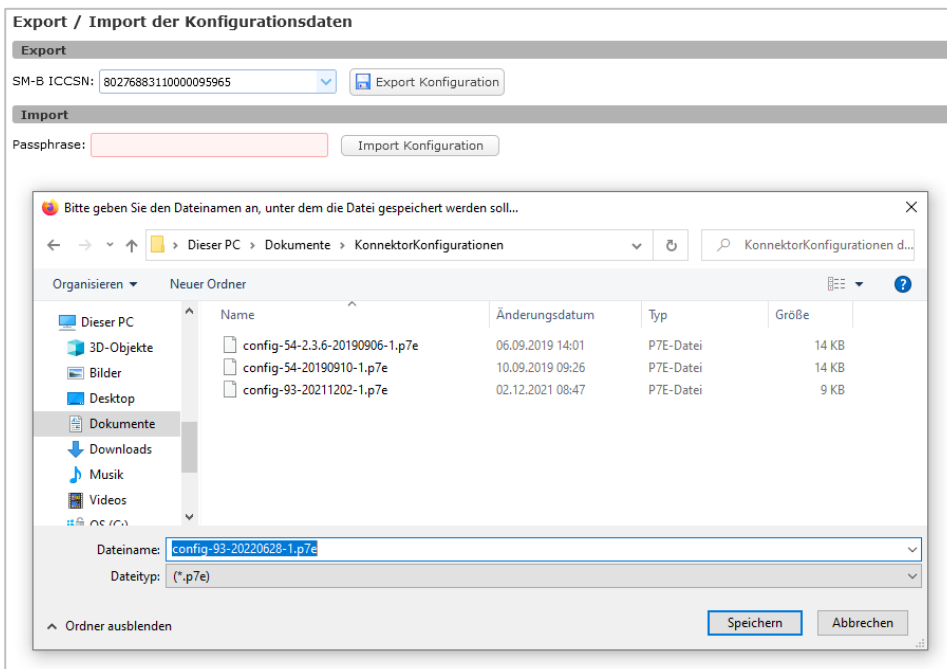


Abbildung 76: Speichern der Konfigurationsdaten-Datei



Beachten Sie bitte vorweg: Vor dem Import muss der Leistungsumfang ONLINE **deaktiviert** werden, sofern beim Import keine aktive VPN-TI-Verbindung besteht oder aufgebaut werden kann.¹⁰⁶ Dafür setzen Sie im Bereich *Verwaltung* den *Leistungsumfang ONLINE* per Radiobutton auf nicht aktiviert und speichern dies mittels Übernehmen ab.

Für den Import der Konfigurationsdaten gehen Sie wie folgt vor:

1

Geben Sie **zunächst** das der Konfigurationsdaten-Datei zugewiesene Importpasswort (= Passphrase) ein, damit die Datei entschlüsselt werden kann und klicken Sie dann auf den Button Import Konfiguration. Wählen Sie über das erscheinende Upload-Fenster die Konfigurationsdaten-Datei aus und bestätigen Sie dies mittels Öffnen.

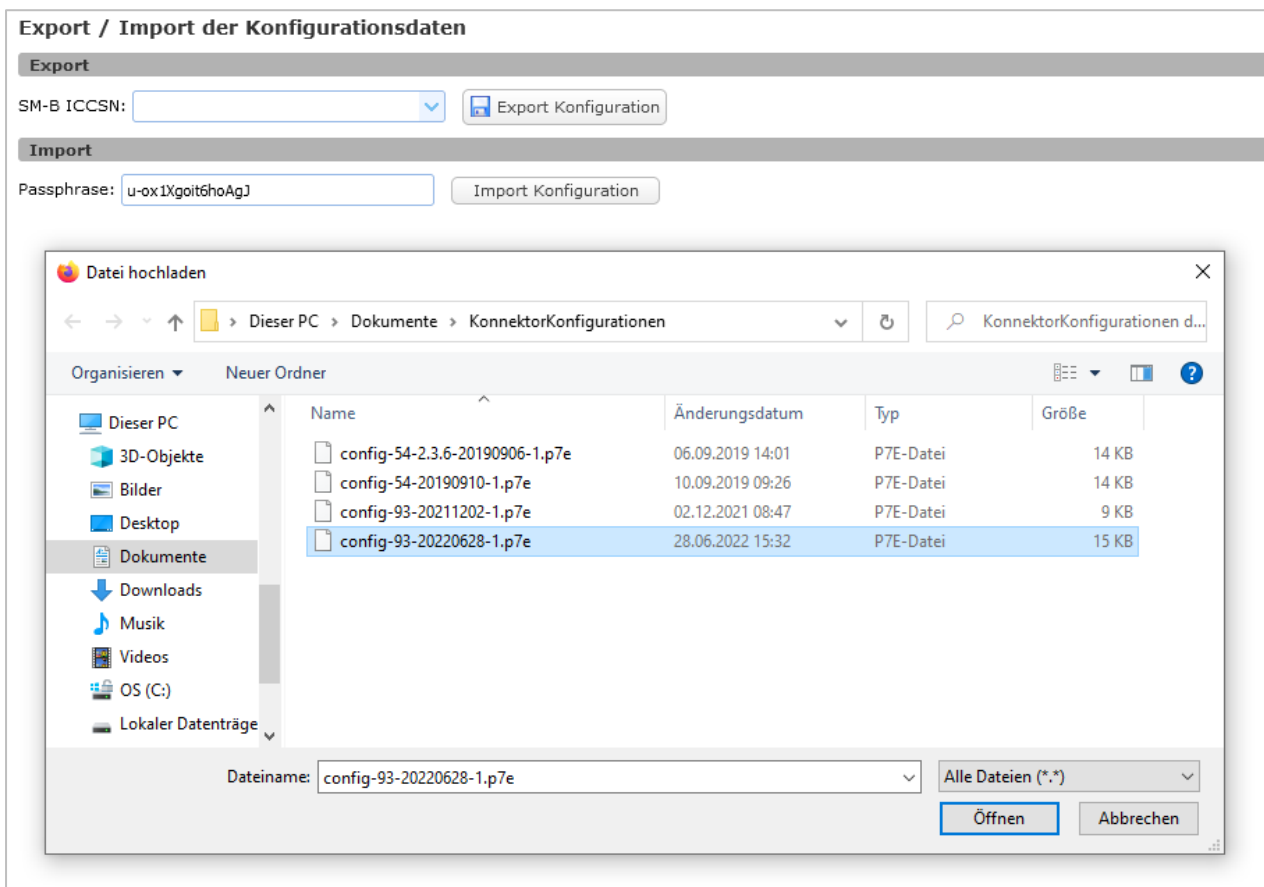


Abbildung 77: Importieren der Konfigurationsdaten-Datei

¹⁰⁶ z.B. wenn es sich um ein neues Gerät handelt, das noch nicht für die Verbindung in die TI konfiguriert ist

Zu Beginn des Importprozesses erscheint ein Anzeigefenster, in dem Sie anhand des Signaturzeitpunkts und des Signaturzertifikats kontrollieren können, ob die korrekte Konfigurationsdatei geladen wird. Bestätigen Sie – sofern die Angaben stimmen und Sie diesen vertrauen – diese Prüfung mittels OK.

2

Beim Import von Konfigurationen kann es trotz ansonsten korrekter Daten vorkommen, dass die zum Zeitpunkt des Exports verwendete SMC-B nun abgelaufen ist. Ist dies eingetreten, dann erscheint ein Dialog mit einer Rückfrage. Prüfen Sie hierbei, ob die im Feld *Ausgestellt für/Subject* dargestellte Organisation zur Praxis bzw. Klinikabteilung passt. Überlegen Sie, ob Sie diesem Zertifikat noch vertrauen können. Nur wenn dies gegeben ist, sollten Sie mit Ja fortfahren. Andernfalls empfiehlt sich ein Abbruch des Imports.

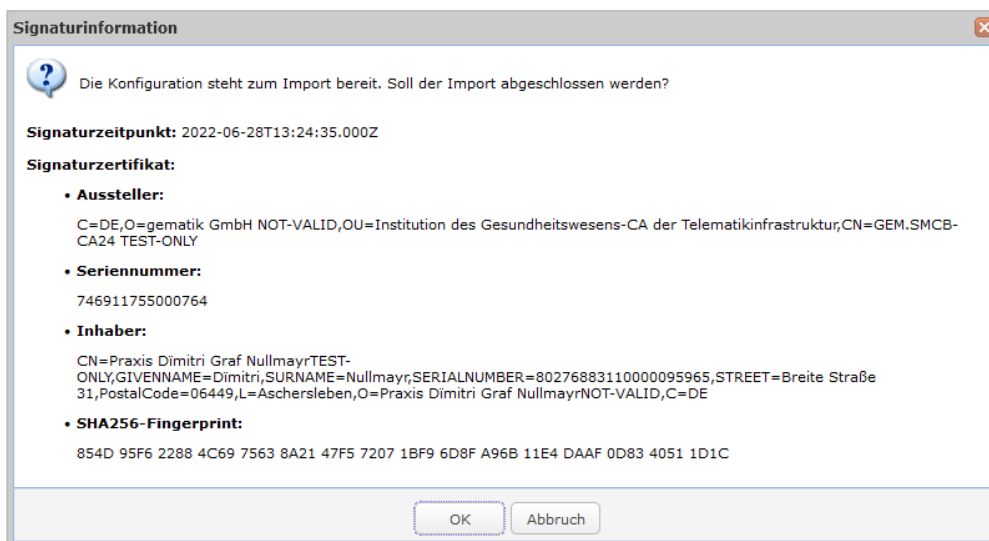


Abbildung 78: Anzeigefenster zur Kontrolle der Signaturinformationen

3

Anschließend erscheint ein Konfigurationsfenster für den Import von Kartenterminals.¹⁰⁷ Darin wählen Sie aus, welche dieser Kartenterminals Sie wieder importieren möchten, indem Sie ggf. Häkchen entfernen. Bestätigen Sie dies mittels OK.¹⁰⁸ Damit werden die Konfigurationsparameter übernommen.

¹⁰⁷ Wird die Konfigurationsdaten-Datei in eine andere KoCoBox MED+ importiert, so führt diese im Hintergrund ein Wartungspairing durch, sofern ein Netzwerkzugriff vom Konnektor auf das Kartenterminal möglich ist. Dies erfordert keine Interaktion eines Benutzers/Administrators. Sofern keine Verbindung möglich ist, wird kein Wartungspairing durchgeführt.

¹⁰⁸ Falls vor dem Import schon Kartenterminal-Konfigurationen auf dem Konnektor vorhanden waren, werden diese gelöscht; es stehen nur noch diejenigen aus der Export-Datei zur Verfügung.

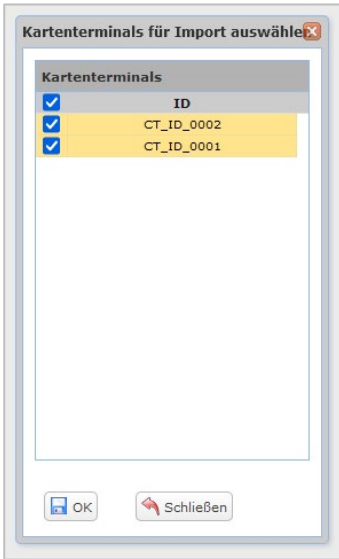


Abbildung 79: Auswahl für den Kartenterminal-Import

- 4** Nach der erfolgreichen Übernahme der Konfigurationsdaten (dies dauert einige Zeit) erscheint ein Dialogfenster zum Neustart des Konnektors. Nach Klick auf OK wird dieser durchgeführt. Somit ist der Import der Konfigurationsdaten abgeschlossen, alle Konfigurationsparameter sind aktiviert.

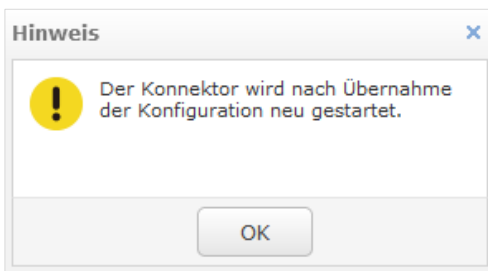


Abbildung 80: Dialogfenster mit Hinweis auf Neustart nach Konfigurationsübernahme



Bitte beachten Sie:

- Eine exportierte Konfiguration enthält **keine** Informationen zur Registrierung, diese können beim Import nicht übernommen werden. Nach dem erfolgreichen Import der Konfiguration ist eine **erneute Registrierung** am VPN-Zugangsdienst erforderlich.
- Kartenterminals, die vor dem Import einer Konfiguration auf dem Konnektor im Kartenterminaldienst vorhanden waren, sind nach erfolgreichem Import gelöscht. Es werden **nur die importierten Kartenterminals** in den Kartenterminaldienst übernommen und in den entsprechenden exportierten Zustand gebracht.
- Falls die Konfigurationsdaten von einem Konnektor exportiert wurden, der sich in einer statischen IP-Adresskonfiguration befindet, führt dies beim Import in einen Konnektor mit einer dynamischen IP-Adresskonfiguration (DHCP) zu einer herstellereigenen Fehlermeldung (20500): *Fehler in der Modulkonfiguration!* Sie vermeiden dies, indem Sie schon **vor** dem Export der Konfigurationsdaten die Liste der DNS-Server leeren. **Alternativ** können Sie **vor** dem Import der Daten den betreffenden Konnektor temporär auf eine statische IP-Adresskonfiguration einstellen.


- Beim Import von Konfigurationen aus Vorgängerversionen der KoCoBox MED+ wird das Laden einer Konfiguration möglicherweise mit einer Fehlermeldung abgeschlossen. Hierbei ist fallweise eine partielle Konfiguration erfolgt. Zur Vermeidung von Sicherheitslücken prüfen Sie als Administrator in solchen Fällen alle konfigurierbaren Felder. **Beachten Sie hierzu bitte:** Sicherheitsrelevante Parameter müssen so konfiguriert werden, dass eine **Gefährdung des Praxisnetzes** und der TI durch den Betrieb der KoCoBox MED+ ausgeschlossen werden kann.



Bitte beachten Sie folgende Sicherheitshinweise:

- Aus Sicherheitsgründen kann der Exportvorgang nur von einem am Konnektor angemeldeten Benutzer mit mindestens der Rolle Administrator ausgelöst werden.
- Aus Sicherheitsgründen kann der Importvorgang nur von einem am Konnektor angemeldeten Benutzer mit der Rolle Super-Administrator ausgelöst werden.
- Der für den Export bzw. Import von Konfigurationsdaten der KoCoBox MED+ jeweils verantwortliche Administrator muss dies im Betriebsführungsbuch dokumentieren und unterschreiben.
- Bewahren Sie das Passwort für die Entschlüsselung von exportierten Konfigurationsdaten **vertraulich** auf. Nur zum Zugriff berechnigte Personen dürfen in den Besitz dieser Information gelangen. Schützen Sie exportierte Konfigurationsdaten ebenfalls vor unbefugtem Zugriff.

7.5.1.3 Telematikdienste

In diesen Unterbereich werden in einer Übersichtsliste die Verfügbarkeiten der zentralen Telematikdienste aufgezeigt. Die Liste der Dienste wird mit dem Auslösen der Abfrage mittels Klick auf den Button **Alle aktualisieren** gefüllt. Eine Aktualisierung bestehender Daten kann durch Betätigung des Knopfes  erfolgen.








| Telematikdienste | | | |
|--|--------|---------------------|---|
| Verfügbarkeit der Telematikdienste | | | |
| 30 ▾ | ⏪ ⏩ | Seite 1 von 1 | 1 bis 7 von 7 Datensätzen |
| Alle aktualisieren | | | |
| Dienst | Status | letzter Prüfzeitpun | FQDN |
|  KSR-Server | | | download-ref.ksr.telematik-test |
|  OCSP-Forwarder | | | httpfwd-ti.d-ref.tm.vpn-zugd.telematik-test |
|  TSL-Downloadpunkt | | | download-ref.tsl.telematik-test |
|  CRL-Downloadpunkt | | | download-testref.crl.ti-dienste.de |
|  VZD-Server | | | directory-ref.vzd.telematik-test |
|  BNetzA-VL-Downloadpunkt | | | download-testref.bnetzavl.telematik-test |
|  Intermediaer-VSDM-Server | | | im-fd-01.d-ref.tm.intermediaer.telematik-test |

Abbildung 81: Übersicht verfügbarer Telematikdienste

In der Übersicht finden sich folgende Informationen:

- Dienst: Name des Telematikdienstes
- Status: zeigt an, ob der Dienst aktuell erreichbar ist. Folgende Anzeigen sind erwartbar:
 - wird geprüft OK, Verbindungsprüfung läuft gerade
 - erreichbar OK, Telematikdienst ist ordnungsgemäß erreichbar
 - DNS_ERROR Fehler, DNS-Abfrage wird nicht aufgelöst
 - NETWORK_ERROR Fehler, ein Netzwerkproblem ist aufgetreten
 - REJECTED Fehler, Telematikdienst lehnt die Verbindung ab
- letzter Prüfzeitpunkt: Zeitpunkt der letzten Statusabfrage in diesem Dialog
- FQDN: eindeutiger Domänenbezeichner des Dienstes

7.5.2 Kartendienst

Der Konnektor führt eine Liste aller Karten, die in die vom Konnektor verwalteten Kartenterminals gesteckt sind. Im Navigationsbereich *Kartendienst* finden sich die dazugehörigen Übersichten und Einstellungsoptionen.¹⁰⁹

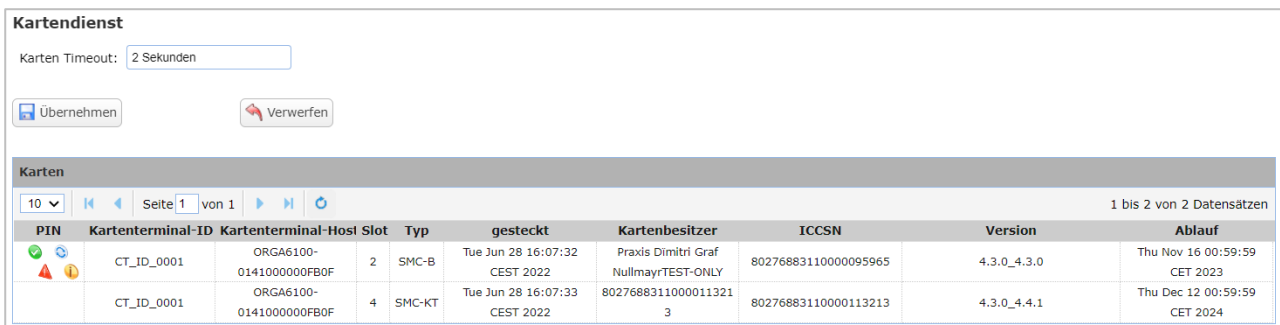


Abbildung 82: Konfigurationsbereich für den Kartendienst

In diesem Bereich kann zunächst beim *Karten Timeout* die erlaubte Kartenlesezeit festgelegt werden. Der Wertebereich reicht von 1 bis 30 Sekunden (voreingestellt sind 2 Sekunden). Dieser Eintrag wird mittels Übernehmen bestätigt.


¹⁰⁹ Vgl. [gemSpec_Kon], Kap. 4.1.5 „Kartendienst“

Gleichzeitig bietet dieser Bereich einen Überblick über die jeweiligen aktuell gesteckten Karten mit Detailinformationen.¹¹⁰:

- PIN¹¹¹
- Kartenterminal-ID
- Kartenterminal-Hostnamen
- Slot, in dem die Karte steckt
- Kartentyp: Heilberufsausweis (HBA), elektronische Gesundheitskarte (eGK), gSMC-KT oder SMC-B,
- Zeitpunkt, an dem die Karte gesteckt wurde
- Kartenbesitzer: Name des Karteninhabers bzw. der Institution
- ICCSN
- Version der Karte; diese ist wie folgt in 3 Oktetten kodiert:
 - das 1. Oktett enthält I2OS (Hauptversionsnummer, 1)
 - das 2. Oktett enthält I2OS (Nebenversionsnummer, 1)
 - das 3. Oktett enthält I2OS (Revisionsnummer, 1).¹¹²
- Ablaufdatum der Karte

Um eine SMC-B verwenden zu können, muss sie **vorher** freigeschaltet werden. Stecken Sie diese dafür in das aktive und verbundene Kartenterminal.

Zum Freischalten der SMC-B gehen Sie wie folgt vor:

- 1** Klicken Sie in der Tabelle *Karten* in der Spalte PIN in der Zeile der entsprechenden SMC-B auf PIN verifizieren . Es öffnet sich das Eingabefenster *PIN verifizieren*.
- 2** Tragen Sie in das Eingabefeld den Mandanten aus dem Infomodell ein, dem die SMC-B zugewiesen ist. Bestätigen Sie dies mit OK.
- 3** Auf dem Kartenterminal-Display erscheint die Aufforderung zur Eingabe der SMC-B-PIN. Geben Sie diese über die Kartenterminal-Tastatur ein und bestätigen Sie diese.
- 4** Schließlich erscheint ein Anzeigefenster mit der Bestätigung der Freischaltung.



Bitte beachten Sie, dass nach dem Ziehen der Karte aus dem Kartenterminal diese erneut freigeschaltet werden muss.

¹¹⁰ Die detaillierten Versionsangaben zu den gesteckten Karten im CETP-Event sind im Anhang zu finden.

¹¹¹ Die Symbole in dieser Spalte (PIN verifizieren, PIN ändern, PIN entsperren, PIN Status) erscheinen nur für SMC-Bs. Per Mouseover erscheinen die Funktionen der Symbole als Tooltip auf der Managementschnittstelle.

¹¹² Vgl. [gemSpec_Karten_Fach_TIP]

7.5.3 Kartenterminaldienst

Der Kartenterminaldienst managt alle vom Konnektor adressierbaren Kartenterminals. Dabei versetzt das Pairing zwischen dem Konnektor und dem eHealth-Kartenterminal den Konnektor in die Lage, die Kartenterminals zu erkennen, die vom Administrator für den Betrieb mit dem Konnektor vorgesehen sind. Es ermöglicht damit eine gesicherte Verbindung zwischen beiden Geräten.¹¹³

Kartenterminaldienst

Service Discovery Zyklus:

Service Discovery Timeout:

Service Discovery Port:

Service Announcement Port:

Keep Alive Interval:

Keep Alive Versuche:

TLS-Handshake Timeout:

Unterstützte EHEALTH-Interface-Versionen: **[1.0.0]**

Kartenterminals

30 Seite 1 von 1 1 bis 1 von 1 Datensätzen

Kartenterminal hinzufügen ... Kartenterminals finden

| | Kartentermin: | physisc | MAC-Adresse | Name | IP-Adresse | Port | Status |
|--|---------------|---------|-------------------|-------------------------|--------------|------|--------|
| | CT_ID_0001 | ja | 00:0D:F8:04:AD:AF | ORGA6100-0141000000FB0F | 192.168.2.67 | 4742 | aktiv |

Abbildung 83: Konfigurationsbereich für den Kartenterminaldienst

Über die Parameter des Kartenterminaldienstes kann das Handling und die Kommunikation mit Kartenterminals konfiguriert werden.



Broadcasts zur *Service Discovery* wirken sich nur auf das aktuelle Netzwerksegment aus, sie werden nicht netzwerkübergreifend verteilt.

Zudem sind folgende Daten für den Kartenterminaldienst in diesem Bereich einzutragen:

- *Service Discovery Zyklus* (= das selbstständige Auffinden von Kartenterminals durch den Konnektor im Netzwerk) mit einer Werteskala von 0 bis 60 Minuten; Voreinstellung: 10 Minuten
Die Service Discovery des Konnektors kann man durch das Eintragen von 0 Minuten für den *Service Discovery Zyklus* deaktivieren.
- *Service Discovery Timeout* (= Zeitintervall, in dem auf einen Service Discovery Request eine Antwort vom Kartenterminal erwartet wird) mit einer Werteskala von 1 bis 3 Sekunden; Voreinstellung: 3 Sekunden
- *Service Discovery Port* (= Port des Kartenterminals, an den der Konnektor seine Anfrage sendet). Hier kann jeder Wert von 0 bis 65.535 eingetragen werden.¹¹⁴

¹¹³ Vgl. [gemSpec_KT], S. 37 ff.

¹¹⁴ Hier ist sicherzustellen, dass andere Netzwerkgeräte nicht über den gewählten Port kommunizieren.

- *Service Announcement Port* (=Kartenterminals melden über diesen Port des Konnektors ihre Service Announcements). Hier kann jeder Wert von 0 bis 65.535 eingetragen werden.¹¹⁵
- *Keep Alive Interval* (=Keep-Alive Methode unter Verwendung von GET STATUS Anfragen an das KT): Sekunden-Intervall, in dem Keep-Alive-Nachrichten an das Kartenterminal gesendet werden, mit einer Werteskala von 1 bis 10 Sekunden; Voreinstellung: 10 Sekunden
- *Keep Alive Versuche*: Anzahl von aufeinander folgenden, nicht beantworteten Keep-Alive Nachrichten, nachdem ein Timeout der TLS-Verbindung festgestellt wird, mit einer Werteskala von 3 bis 10; Voreinstellung: 3
Für ein zuverlässiges Verhalten mit allen zugelassenen Kartenterminal-Typen wird empfohlen, diesen Wert auf 5 zu setzen.¹¹⁶
- *TLS-Handshake Timeout* mit einer Werteskala von 1 bis 60 Sekunden; Voreinstellung: 10 Sekunden
- Versionsanzeige für *unterstützte EHEALTH-Interface-Versionen*



Sollten Sie bei Verwendung der Kartenterminals feststellen, dass diese die aktive Verbindung zum Konnektor verlieren und manuelle Verbindungsversuche erfolglos bleiben, dann setzen Sie die Parameter für *KeepAlive* und *Keep Alive Interval* auf ihre Maximalwerte (jeweils den Wert 10). So ist ein Timeout innerhalb der Kommunikation von Konnektor zu Kartenterminal von 100 Sekunden möglich, ohne dass die Verbindung verloren geht.



Verbindungsverluste können z.B. beim Ziehen von gesteckten Karten aus dem Kartenterminal heraus als auch beim Bestätigen des Pairings am Gerät auftreten. In diesen Fällen sollten Sie die oben genannten Parameter entsprechend anpassen, um dies zu vermeiden.



Beachten Sie folgende Hinweise:

- Bitte tragen Sie nur ganzzahlige Werte ein.
- Die voreingestellten Werte sollten nach Möglichkeit übernommen werden.

Mittels Übernehmen speichern Sie die Konfigurationsparameter des Kartenterminaldienstes ab. Die Konfigurationen werden sofort, d.h. ohne Neustart des Konnektors, wirksam.

Im unteren Bereich finden Sie eine tabellarische Auflistung aller dem Konnektor bekannten Kartenterminals mit jeweiligem Status.¹¹⁷

Mit dem Button Kartenterminals finden kann man auf manuellem Weg das Auffinden von Kartenterminals durch den Konnektor im Netzwerk anstoßen.¹¹⁸

¹¹⁵ Hier ist sicherzustellen, dass andere Netzwerkgeräte nicht über den gewählten Port kommunizieren.

¹¹⁶ Die gesamte Wartezeit (Timeout) der KoCoBox MED+ auf Keep-Alive-Reaktion des Kartenterminals setzt sich aus Intervall x Versuche zusammen. Der Standard-Timeout seitens Kartenterminal beträgt, je nach Kartenterminal-Hersteller, bis zu 41 Sekunden. Davon beinhalten ca. 30 Sekunden die direkte Wartezeit auf eine PIN-Eingabe. Je nach Hersteller kommt noch eine Karenzzeit von ca. 10 Sekunden hinzu. Für eine sichere Funktion wird ein Wert von 50 Sekunden empfohlen.

¹¹⁷ Das Update der Kartenterminals wird unten im Abschnitt Aktualisierung beschrieben.

¹¹⁸ Dies entspricht der oben beschriebenen Service Discovery Funktion, die nicht automatisch, sondern manuell durchgeführt wird.



Abbildung 84: Erfolgsmeldung zum Auffinden von Kartenterminals

Bestätigen Sie die Erfolgsmeldung mit OK.

Findet der Konnektor ein neues Kartenterminal, erscheint dieses in der Übersichtsliste mit dem Status *bekannt*.

Über den Button Kartenterminal hinzufügen... öffnet sich das entsprechende Konfigurationsfenster. Darin tragen Sie die *IP-Adresse* (obligatorisch) sowie ggf. den (SICCT-) *Port*, die *MAC-Adresse* und den (SICCT-Terminal-) *Namen*.¹¹⁹ des Kartenterminals ein.



Der sicherste und schnellste Weg zum Hinzufügen eines Kartenterminals ist dessen Übernahme mittels **sämtlicher** ausgefüllter Konfigurationsparameter.

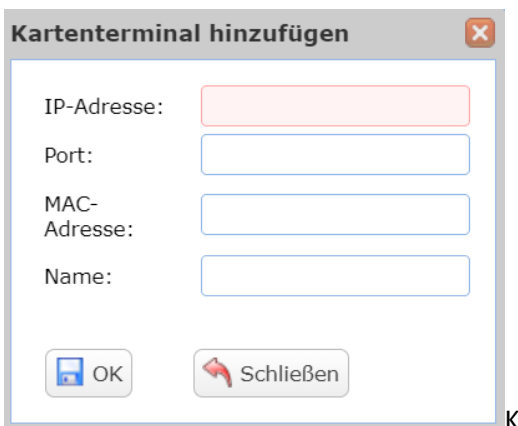


Abbildung 85: Kartenterminal hinzufügen

Mit OK speichern Sie die Einträge ab, über Schließen verlassen Sie das Konfigurationsfenster.

¹¹⁹ Alternative Bezeichnung: FriendlyName



Beim Hinzufügen eines Kartenterminals im Kartenterminaldienst des Konnektors darf dieses noch nicht mit gleichem SICCT-Terminal-Namen in der Liste vorhanden sein. Der Konnektor meldet sonst einen Fehler.




Möchte man dieses Kartenterminal dennoch hinzufügen, muss man zuvor den gleichlautenden Eintrag in der Liste löschen. Anschließend kann das Kartenterminal manuell durch Eingabe von IP-Adresse, SICCT-Port, MAC-Adresse und SICCT-Terminal-Name hinzugefügt werden.



Bitte achten Sie beim Einrichten des Kartenterminals (direkt am Kartenterminal!) darauf, für den Gerätenamen ausschließlich die Zeichen **A-Z, Ä, Ö, Ü, a-z, ä, ö, ü, 0-9, ., -, _ und Leerzeichen** zu verwenden. Als letztes Zeichen des Gerätenamens sind unzulässig: **., -, _ und Leerzeichen**. Nur bei Verwendung des beschriebenen Zeichensatzes kann der Gerätename korrekt in der Übersicht der KoCoBox MED+ dargestellt werden. Dies gilt auch für die Eingabe des Namens im Feld *Name* des Dialogs Kartenterminal hinzufügen.



Generell empfehlen wir die Zuweisung eines Kartenterminals über den Button Kartenterminal hinzufügen.¹²⁰

Die schon vorhandenen Tabelleneinträge können Sie entweder durch Doppel-Klick auf die entsprechende Zeilen oder per  bearbeiten:

Es öffnet sich das Konfigurationsfenster *Kartenterminal bearbeiten*, das detaillierte Informationen zum Kartenterminal sowie weitere Bearbeitungsfelder bereitstellt.

¹²⁰ Zwar kann man den Hostnamen – wie oben beschrieben – grundsätzlich manuell ändern. Es kann allerdings passieren, dass durch ein Service Announcement der Kartenterminals die Werte wieder überschrieben werden. Dann entspricht der Hostname wieder dem Wert, welchen das Kartenterminal ursprünglich geschickt hatte. Insofern ist die Zuweisung per Button ratsam.

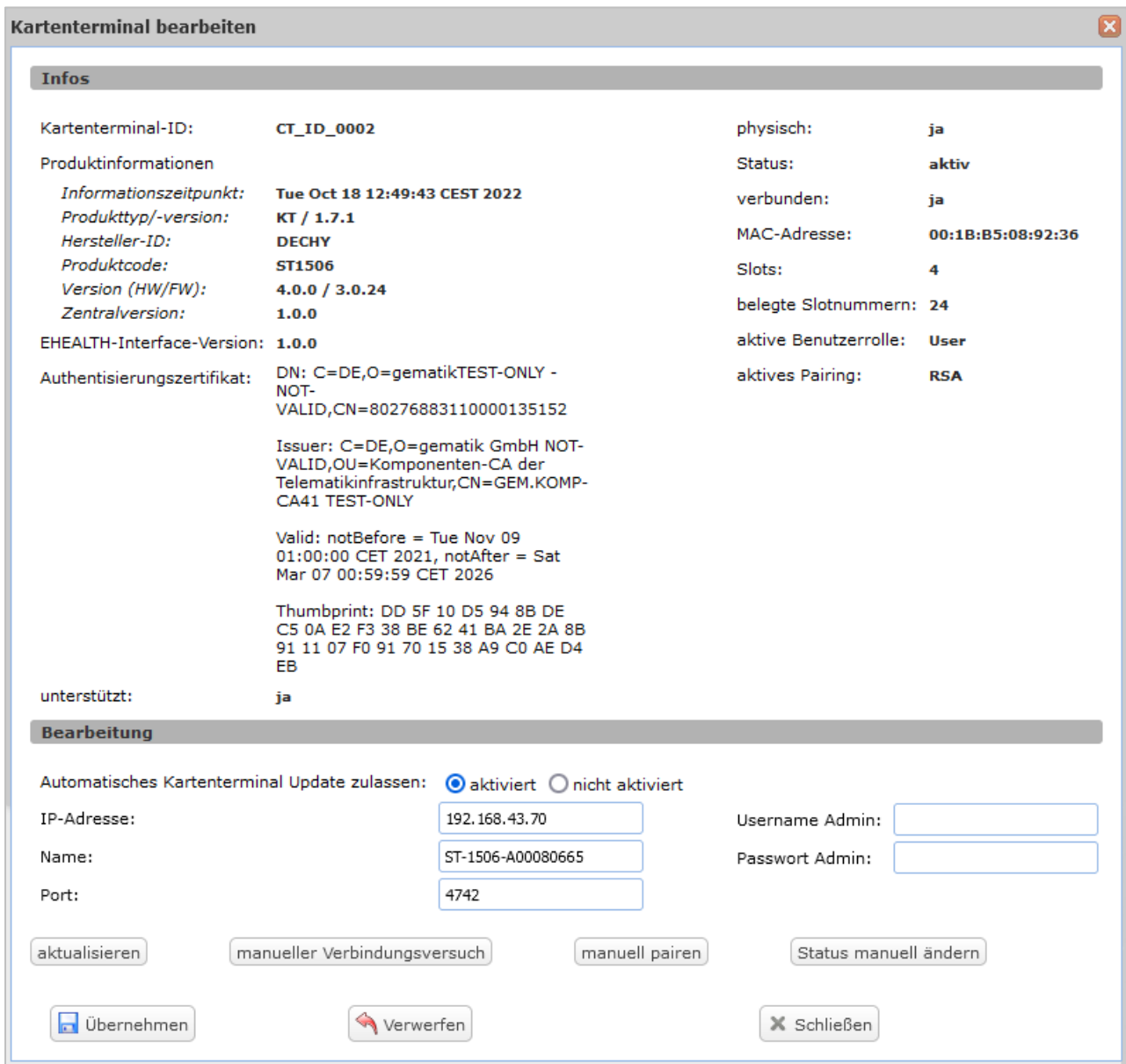


Abbildung 86: Vorhandenes Kartenterminal bearbeiten

Im oberen Info-Bereich findet man folgende Detailinformationen zum Kartenterminal:

- *Kartenterminal-ID*: zur eindeutigen, statischen Identifikation des Kartenterminals
- *Produktinformationen*¹²¹: Informationszeitpunkt, Produkttyp/-version, Hersteller-ID, Produktcode, Version (HW/FW), Zentralversion sowie EHEALTH-Interface-Version
- Ausführliche Informationen zum *Authentisierungszertifikat* des Kartenterminals:
 - Distinguished Name des Inhabers (*DN*)
 - Angaben zum Aussteller (*Issuer*)

¹²¹ vgl. [gemSpec_Kon], S. 85 ff.

- Gültigkeitszeitraum (*Valid*)
- Fingerabdruck (*Thumbprint*)
- *unterstützt*: Version des Kartenterminals wird durch den Konnektor unterstützt (*ja/nein*)
- *physisch*: physisches (oder logisches) Kartenterminal (*ja/nein*); zur Unterscheidung von eHealth-Kartenterminals und HSM-Bs
- *Status* des Kartenterminals mit den Ausprägungen
 - *bekannt*: über Service Announcement/Service Discovery erkannt
 - *zugewiesen*: durch den Administrator konfiguriert
 - *gepairt*: Pairing erfolgreich.¹²²
 - *aktiv*: kann genutzt werden
 - *aktualisierend*: es läuft ein Updatevorgang
- *verbunden*: Verfügbarkeitsstatus des Kartenterminals (*ja/nein*)
- *MAC-Adresse* des Kartenterminals
- *Anzahl der Slots* des Kartenterminals
- *belegte Slotnummern*: Liste der aktuell mit Karten belegten Slots
- *Aktive* Benutzerrolle: Benutzerrolle, die für die aktuelle Session verwendet wird
- *Aktives* Pairing: Anzeige des für das Pairing genutzten kryptografischen Schlüsseltyps, dies kann RSA oder ECC sein

Im unteren Bearbeitungsbereich sind *IP-Adresse*, *Name* und *Port* des Kartenterminals einzutragen.

Hier erfolgt auch die Auswahl, ob für das betreffende Kartenterminal das automatische Softwareupdate zugelassen werden soll. Diese Einstellung ist standardmäßig aktiviert. Weitere Informationen zum automatischen Softwareupdate finden sich im Kapitel Aktualisierung.

Die Konfigurationen werden per Übernahme-Button abgespeichert.



Sofern das Kartenterminal über den Konnektor aktualisiert werden soll (KSR-Update), müssen Sie bei physischen Kartenterminals den (Benutzer-)Namen und das Passwort des Kartenterminal-Administrators eintragen.

Die folgende Abbildung gibt einen Überblick über die verschiedenen Status eines Kartenterminals in Verbindung mit dem Konnektor.

¹²² Der Übergang vom Status *gepairt* zu *aktiv* erfolgt automatisch. Der Administrator kann jedoch jederzeit manuell ein Kartenterminal von *aktiv* auf *gepairt* und umgekehrt setzen.



Abbildung 87: Übersicht der Verbindungsstatus eines Kartenterminals zum Konnektor

Sie haben nun die folgenden Optionen:

- **Button manueller Verbindungsversuch:** Falls das Kartenterminal zwar nicht verbunden, aber aktiv ist, kann hierüber ein Verbindungsaufbau initiiert werden.
- **Button manuell pairen:** Falls das Kartenterminal zugewiesen ist und die Version unterstützt wird, kann hierüber ein Pairing ausgelöst werden. Dies bestätigen Sie im Dialogfenster mit OK.
- **Button Status manuell ändern:** Hierüber kann der Status des Kartenterminals geändert werden. Wählen Sie dazu im erscheinenden Konfigurationsfenster den gewünschten neuen Status aus und bestätigen Sie dies mit OK.
- **Button aktualisieren:** Über diesen Button können die angezeigten Detailinformationen für das Kartenterminal manuell aktualisiert werden.¹²³



Diese Aktualisierungsfunktion greift für Kartenterminals mit dem Status *aktiv*, *gepairt* und *zugewiesen*. Bei Geräten mit dem Status *bekannt* erscheint bei sämtlichen Detailinformationen die Angabe *noch nicht bekannt*.




Prüfen Sie vor dem erstmaligen Pairing, ob das Gehäuse des zu verbindenden Kartenterminals und dessen Versiegelung unversehrt sind. Sollte ein bereits gepairtes Kartenterminal unvermittelt den Zustand *zugewiesen* einnehmen, so kann ein Ausfall der Identitätskarte gSMC-KT des Kartenterminals oder gar eine Manipulation vorliegen. Überprüfen Sie in solchen Fällen, ob im Kartenterminal die korrekte gSMC-KT gesteckt ist. Prüfen Sie ebenfalls, ob das Gehäuse und die Versiegelung des Kartenterminals unversehrt sind. Sollte hierbei ein Schaden entdeckt werden, **führen Sie das Pairing nicht aus**, sondern wenden Sie sich an Ihren Servicepartner.

¹²³ Diese Funktion kann auch in der tabellarischen Auflistung der Kartenterminals über das Aktualisieren-Icon angestoßen werden.



Abbildung 88: Konfigurationsfenster zur Statusänderung eines Kartenterminals

Mit Übernehmen speichern Sie die Einstellungen ab, über Schließen verlassen Sie das Konfigurationsfenster. Mittels  löschen Sie den entsprechenden Tabelleneintrag.




Das Hinzufügen und Löschen, sowie das Ändern des Status eines Kartenterminals wird im Systemprotokoll dokumentiert.

Durchführung Kartenterminal-Pairing im Kartenterminaldienst

Um ein dem Konnektor schon bekanntes¹²⁴ Kartenterminal zu pairen, gehen Sie wie folgt vor:

1

Wählen Sie ein Kartenterminal aus der Liste der bekannten Kartenterminals aus und rufen Sie per Bearbeitungsfunktion  das Konfigurationsfenster auf.

2

Klicken Sie auf den Button Status manuell ändern und wählen Sie die Option *zugewiesen* aus.¹²⁵ Warten Sie auf das Dialogfenster mit der Erfolgsmeldung und bestätigen Sie diese mit OK.

3

Rufen Sie den Button manuell pairen auf und bestätigen Sie die Frage im Dialogfenster mit OK. Der *Bitte-Warten*-Balken symbolisiert den Pairingvorgang.





4

Prüfen Sie im dann geöffneten Fingerprint-Fenster den angezeigten Fingerprint anhand der Ihnen zum Kartenterminal vorliegenden Dokumentation. Wenn dieser gültig ist, können Sie von einer authentischen Verbindung ausgehen und das Pairing abschließen.¹²⁶ Anderenfalls sollten Sie den Pairingvorgang abbrechen.





¹²⁴ Ein dem Konnektor bekanntes Gerät ist ein Kartenterminal, das in der Kartenterminal-Liste erscheint und in der Status-Spalte als *bekannt* angezeigt wird.

¹²⁵ Es wird die TLS-Verbindung zum Kartenterminal aufgebaut, die weiteren Parameter werden vom Gerät abgefragt und im KT-Objekt gespeichert.

¹²⁶ In der Regel liegt der passende Fingerprint zum Zertifikat des Kartenterminals diesem Gerät in Papierform bei. Alternativ kann dieser auch als Aufkleber am Kartenterminal vorhanden sein.

-  Quittieren Sie die Pairing-Meldung auf dem Kartenterminal-Display, entweder per (grünem) Bestätigen-Knopf der Tastatur oder (herstellerspezifisch) mittels Eingabe der Admin-PIN des Kartenterminals.
 -  Notieren Sie nach Abschluss des Pairings die Kartenterminal-ID (CT-ID).¹²⁷ Warten Sie schließlich das Dialogfenster mit der Erfolgsmeldung (Managementschnittstelle) ab und bestätigen Sie dies mit OK.
-  Vergewissern Sie sich anhand der IP-Adresse oder der MAC-Adresse, welches Kartenterminal Sie verwenden. Sie finden die MAC-Adresse auf dem Geräteschild des Kartenterminals.
-  Wichtig ist, dass es im Infomodell (siehe Abschnitt Infomodell) einen Arbeitsplatz namens *Konnektor* (bitte auf die genaue Schreibweise achten) gibt. Dieser muss mit dem genutzten (gepairten) Kartenterminal verbunden sein, andernfalls können keine Zugriffe vom Konnektor auf dieses Kartenterminal erfolgen. Zusätzlich muss dieser Arbeitsplatz mit dem zu verwendenden Mandanten verknüpft werden, so dass der Super-Administrator über die Managementschnittstelle Kartenoperationen durchführen kann.

Um die Informationen im Kartenterminaldienst zu aktualisieren, gehen Sie wie folgt vor:

-  Öffnen Sie das Konfigurationsfenster *Kartenterminal bearbeiten* durch Auswahl in der Liste der bekannten Kartenterminals.
 -  Ändern Sie über den Button Status manuell ändern vorübergehend den Status des Kartenterminals. Hierbei werden die Informationen des Kartenterminals aktualisiert.
 -  Schließen Sie das Konfigurationsfenster *Kartenterminal bearbeiten* über den Button Schließen.
-  Bitte beachten Sie, dass in Abhängigkeit vom Statuswechsel eventuell nicht alle Informationen über das Kartenterminal erneuert werden. Wenn Sie den gesamten Datensatz zu diesem Kartenterminal aktualisieren möchten, ist gegebenenfalls die Aufhebung des Pairings notwendig.

7.5.4 Systeminformationsdienst

Der Systeminformationsdienst stellt für die Basisdienste, Fachmodule und Clientsysteme sowohl aktiv (Push-Mechanismus) als auch passiv (Pull-Mechanismus) Informationen zur Verfügung. Er dient als zentraler Mechanismus. So kann er von anderen Basisdiensten und Fachmodulen zum Verteilen und Bereitstellen von Informationen, die von ihnen stammen, verwendet werden.¹²⁸

¹²⁷ Die CT-ID ist für den Eintrag im Infomodell erforderlich.

¹²⁸ Vgl. [gemSpec_Kon], Kap. 4.1.6 „Systeminformationsdienst“

Systeminformationsdienst

Maximale Anzahl Zustellversuche:

Monitoring von Operationen

| Operationsname | OK_Val | NOK_Val | Alarmwert |
|-------------------------|--------|---------|---|
| VerifyCertificate | 1 | 5 | <input style="width: 50px;" type="text" value="401"/> |
| EncryptDocument | 1 | 5 | <input style="width: 50px;" type="text" value="101"/> |
| DecryptDocument | 1 | 5 | <input style="width: 50px;" type="text" value="101"/> |
| SignDocument (nonQES) | 1 | 5 | <input style="width: 50px;" type="text" value="41"/> |
| VerifyDocument (nonQES) | 1 | 5 | <input style="width: 50px;" type="text" value="61"/> |

EC_CRYPTOPERATION_ALARM zurücksetzen

Übernehmen
 Verwerfen

Abbildung 89: Konfigurationsbereich für den Systeminformationsdienst

Im Bereich *Systeminformationsdienst* definieren Sie zunächst die *maximale Anzahl der Zustellversuche* (im Wertebereich von 1 bis 10) für CETP-Events, bevor die abonnierten Topics des Clientsystems aus dem Systeminformationsdienst gelöscht werden.

Wenn ein CETP-Event nach der maximalen Anzahl an Zustellversuchen nicht erfolgreich versendet werden kann, löscht der Konnektor alle Abonnements zu diesem Clientsystem in der internen Verwaltung des Konnektors. In der Folge erhält das Clientsystem keine Ereignisse mehr von diesem Konnektor.

In der Übersicht *Monitoring von Operationen* werden der Operationsname OK_Val, NOK_Val¹²⁹ sowie der Alarmwert (im Wertebereich 0 bis 9999; 0 bedeutet deaktiviert) angezeigt. In dieser Liste sind die Operationen des Konnektors aufgeführt, die kryptografische Verfahren verwenden und die durch eine Missbrauchserkennung überwacht werden können:

- *Zertifikatsprüfung*: Prüfung von Zertifikaten
- *EncryptDocument*: ein Dokument wird (hybrid) verschlüsselt
- *DecryptDocument*: ein Dokument wird (hybrid) entschlüsselt
- *SignDocument (nonQES)*: ein Dokument wird mittels fortgeschrittener Signatur signiert
- *VerifyDocument (nonQES)*: ein mit fortgeschrittener Signatur signiertes Dokument wird verifiziert

¹²⁹ OK_Val bedeutet einen erfolgreichen Abschluss der Operation, NOK_Val bedeutet ein fehlerhaftes Beenden der Operation



Stellen Sie sicher, dass für den Regelbetrieb keine Deaktivierung der Missbrauchserkennung erfolgt. Achten Sie darauf, dass in sämtlichen Feldern keine 0 eingetragen ist. Eine Deaktivierung bedeutet, dass der Missbrauch der kryptografischen Funktionen nicht erkannt werden kann und damit kein sicherer Betrieb des Konnektors möglich ist.



Ausführliche Erklärungen finden Sie in den Tooltips zur Überschrift *Monitoring von Operationen* sowie zur *Zertifikatsprüfung*¹³⁰ und weiter unten im Abschnitt Signaturdienst.

Zunächst ist die Operation *Zertifikatsprüfung* zu konfigurieren. Hier ist der Alarmwert *401* per Voreinstellung eingetragen. Anschließend können bei Bedarf die Alarmwerte für die Operationen Verschlüsselung (Voreinstellung: *101*), Entschlüsselung (Voreinstellung: *101*), Signieren (Voreinstellung: *41*) und Verifizieren (Voreinstellung: *61*) konfiguriert werden.

Die Einträge sind über den Button Übernehmen zu speichern.



Die KoCoBox MED+ unterstützt Missbrauchserkennungen: Sobald eine auffällige Häufung von Operationsaufrufen in den letzten 10 Minuten erkannt wurde, gibt der Konnektor eine Alarmmeldung aus. Diese ist auf dem Display sowie in der Liste der Betriebszustandsmeldungen ersichtlich. Ausschließlich der Administrator kann über den Button `EC_CRYPTOPERATION_ALARM` die Alarmmeldung zurücksetzen.



Wird die Missbrauchserkennung signalisiert, muss sich der Benutzer / Administrator vergewissern, dass das Netz weiterhin sicher betrieben wird. Dies schließt z.B. Maßnahmen zur Viruserkennung, Einbruchserkennung u.ä. ein. Wenn aus fachlicher Sicht der sichere Betrieb des Konnektors **nicht** mehr garantiert werden kann, darf der Konnektor **nicht mehr benutzt werden**, bis dieser unsichere Netzzustand behoben ist.

Die Höchstzahl an Subscriptions (Abonnements von Clientsystemen, die sich für den Erhalt von CETP-Events, d.h. Konnektor-Ereignisse, anmelden) für einen Konnektor beträgt 999. Sollte dieser Wert überschritten werden, teilt der Konnektor dies (u.a. per Display) als herstellereigenspezifische Fehlermeldung¹³¹ mit.



Bei dieser Fehlermeldung sollten Sie als Administrator den Konnektor neu starten, um wieder Subscriptions verarbeiten zu können.

7.5.5 Zertifikatsdienst

Der Zertifikatsdienst bietet eine Schnittstelle für das Überprüfen der Gültigkeit von Zertifikaten an.¹³² Er stellt unter anderem die vertrauenswürdige Kommunikation sicher.

¹³⁰ Ausführlicher zur Signaturzertifikatsprüfung siehe [gemSpec_Kon], S. 289 ff.

¹³¹ Fehler 20032, siehe auch im unteren Abschnitt Herstellerspezifische Fehlermeldungen

¹³² Vgl. [gemSpec_Kon], Kap. 4.1.9 „Zertifikatsdienst“

Zertifikatsdienst

Certificate Revocation List (CRL)

Primäre Downloadadresse: <http://download-testref.crl.ti-dienste.de/crl/vpnk-ca1.crl>
 Sekundäre Downloadadresse: <http://download-testref.crl.ti-dienste.de/crl/vpnk-ca1.crl>
 Import:
 Aktualisierung:

Trust-service Status List (TSL)

TSL-Signer-CA Downloadadresse: <http://download-ref.tsl.telematik-test/ECC/GEM.TSL-CA28.der>
 TSL-Signer-CA-CROSS-Downloadadresse: <http://download-ref.tsl.telematik-test/ECC/GEM.TSL-CA28-CROSS54.der>
 Primäre TSL-Downloadadresse: http://download-ref.tsl.telematik-test/ECC/ECC-RSA_TSL-ref.xml
 Sekundäre TSL-Downloadadresse: http://download-bak-ref.tsl.telematik-test/ECC/ECC-RSA_TSL-ref.xml
 Primäre TSL-Downloadadresse Internet: http://download-testref.crl.ti-dienste.de/TSL-ECC-test/ECC-RSA_TSL-test.xml
 Primäre TSL-Downloadadresse IP Internet: 84.17.168.222
 Sekundäre TSL-Downloadadresse Internet:
 Sekundäre TSL-Downloadadresse IP Internet:
 Grace Period:
 Import:
 Aktualisierung:

Online Certificate Status Protocol (OCSP)

Primäre Adresse des Forwarders: <httpfwd-ti.d-ref.tm.vpn-zugd.telematik-test>
 Sekundäre Adresse des Forwarders:
 TCP-Port des OCSP-Forwarders: 3128

 Grace Period nonQES:
 Timeout nonQES:
 Timeout QES:

BNetzA-VL

Import:
 Aktualisierung:
 Zeitraum des periodischen Updates:

Prüfungen

Intervall Überprüfung Kartenzertifikate:
 Warnung vor Ablauf von Zertifikaten:
 Ablauf innerhalb Frist:

Abbildung 90: Konfigurationsbereich für den Zertifikatsdienst

Der Zertifikatsdienst unterstützt sowohl RSA-Zertifikate als auch ECC-Zertifikate und -Schlüssel. Die sukzessive Umstellung auf ECC-Schlüssel erfolgt weitgehend automatisch. Gewöhnlich wird von dieser Umstellung lediglich die veränderte Darstellung der Adressen für Downloadpunkte sichtbar sein.



In Ausnahmefällen kann diese Umstellung nicht automatisch erfolgen. Dann ist eine manuelle ECC-Migration auszuführen. Dies ist auf der Statusseite beispielsweise durch eine über mehrere Tage anhaltende Darstellung des Vertrauensraumtyps RSA erkennbar.

ECC Migration

Trust-service Status List (TSL)

Primäre TSL-Downloadadresse: <http://download-ref.tsl.telematik-test/TSL-ref.xml>
 Sekundäre TSL-Downloadadresse: <http://download-bak-ref.tsl.telematik-test/TSL-ref.xml>
 TSL-Signer-CA Downloadadresse: **Die Information steht erst ab der ECC-Migration zur Verfügung.**

Abbildung 91: Manuelle ECC-Migration



Für eine manuelle ECC-Migration sind nacheinander drei Dateien zu laden. Diese werden separat über einen öffentlichen Downloadpunkt bereitgestellt. Ein TSL-CA-Cross-Zertifikat repräsentiert die Vertrauensstellung zwischen der CA der RSA-basierten TSL und der CA der ECC-basierten TSL. Beim TSL-CA-Zertifikat handelt es sich um ein ECC-Zertifikat für die ECC-TSL. Die ECC-RSA-TSL stellt die neue ECC-TSL dar, die sowohl ECC-basierte als auch RSA-basierte Dienste beschreibt. Wurden alle Daten erfolgreich geladen, ist die ECC-Migration erfolgreich ausgeführt.



Bei einer fehlgeschlagenen ECC-Migration kann der Vorgang bis zum Erfolg wiederholt werden. Eine erfolgreich abgeschlossene ECC-Migration ist **nicht umkehrbar**.

Der Bereich *Certificate Revocation List (CRL)* zeigt die primäre und sekundäre Adresse des Download-Servers für die der CRL als URI an. Über den Button CRL importieren kann man diese manuell einbringen.

Für das unmittelbare Auslösen einer automatischen CRL-Aktualisierung steht der Button CRL aktualisieren zur Verfügung.

Im Bereich *Online Certificate Status Protocol (OCSP)* werden die primäre und sekundäre Adresse der OCSP-Forwarder sowie der TCP-Port des OCSP-Forwarders beim Zugangsdienstprovider dargestellt.

Über den Button OCSP-Forwarder prüfen können Sie kontrollieren, ob einer der beiden Server per ICMP-Echo (ping) erreichbar ist. Mit Hilfe des Buttons OCSP-Request testen kann man prüfen, ob ein (beliebiger) OCSP-Request zu einer erhaltenen OCSP-Antwort führt. Das Ergebnis wird jeweils per Dialogfenster angezeigt.

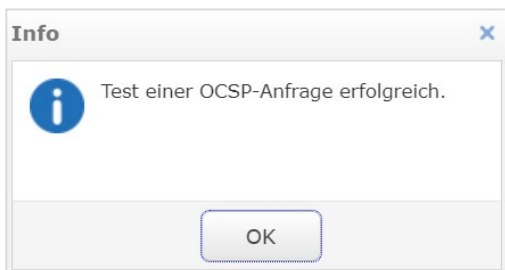


Abbildung 92: Meldung nach erfolgreichem Test einer OCSP-Anfrage

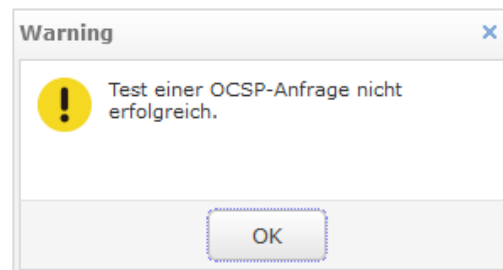


Abbildung 93: Meldung nach erfolglosem Test einer OCSP-Anfrage

Unter *Grace Period nonQES* legen Sie fest, wie lange erhaltene OCSP-Antworten für nonQES-Zertifikate zwischengespeichert werden. Der Wertebereich ist 0 bis 20 Minuten, voreingestellt sind 10 Minuten.

In der Zeile *Timeout nonQES* definieren Sie den Timeout für OCSP-Abfragen bei der Prüfung von nonQES-Zertifikaten. Der Wertebereich beträgt 1 bis 120 Sekunden, voreingestellt sind 20 Sekunden.

Beim *Timeout QES* tragen Sie den Timeout für OCSP-Abfragen bei der Prüfung von QES-Zertifikaten ein. Der Wertebereich beträgt 1 bis 120 Sekunden, voreingestellt sind 20 Sekunden.

Im Bereich *Trust-service Status List (TSL)* werden die *primäre* und *sekundäre TSL-Downloadadresse* sowie die *TSL-Signer-CA Downloadadresse* und die *TSL-Signer-CA-Downloadadresse* angezeigt. Diese sind nicht konfigurierbar.

Darunter kann man manuell im Feld *TSL-Backup-Downloadadresse* die entsprechende Adresse der TSL im

Internet¹³³ sowie im Feld *TSL-Backup-IP-Adresse* die entsprechende Backup-IP-Adresse der TSL im Internet¹³⁴ eintragen.



Im Fall, dass eine TSL-Aktualisierung innerhalb der TI fehlschlägt, versucht der Konnektor automatisch eine TSL-Aktualisierung aus dem Internet von der TSL-Backup-Downloadadresse bzw. der TSL-Backup-IP-Adresse.

In Feld *Grace Period* kann man einstellen, wie viele Tage der Konnektor mit einer nicht aktualisierten TSL weiter betrieben werden kann (Wertebereich: 1 bis 30 Tage). Die Voreinstellung lautet 30 Tage.

Über den Button TSL importieren können Sie diese manuell auswählen und einbringen.

Zum unmittelbaren Auslösen eines automatischen TSL-Imports steht der Button TSL aktualisieren zur Verfügung.

Im Bereich *BNetzA-VL* werden die für die QES-Zertifikatsprüfung notwendigen QES-Signer-Zertifikate durch die Vertrauensliste der Bundesnetzagentur (BNetzA-VL) bereitgestellt. Dabei ist das Signer-Zertifikat der BNetzA-VL in der TSL enthalten.

Analog zum Import der TSL laden Sie über den Button BNetzA-VL importieren eine BNetzA-VL manuell.¹³⁵

Über den Button BNetzA-VL aktualisieren kann man unmittelbar eine automatische Aktualisierung der BNetzA-VL auslösen.

Beim *Zeitraum des periodischen Updates* legen Sie fest, nach wie vielen Stunden ein regelmäßiges Update der BNetzA-VL erfolgen soll. Der Wertebereich ist 1 bis 168 Stunden; voreingestellt sind 24 Stunden.

Im Bereich *Prüfungen* kann man beim *Intervall Überprüfung der Kartenzertifikate* einstellen, in welchem Zeitabstand die Ablauffrist der Zertifikate aller gesteckten Karten überprüft wird. Der Wertebereich ist 0 bis 365 Tage, 0 bedeutet keine Überprüfung. Per Voreinstellung ist ein Tag definiert.

Unter *Warnung vor Ablauf von Zertifikaten* wird festgelegt, wie viele Tage vor dem Ablauf von Zertifikaten eine Warnung über die Managementschnittstelle bzw. per Betriebszustandsmeldung abgegeben wird. Der Wertebereich liegt zwischen 0 und 180 Tagen, 0 bedeutet keine Warnung. Über den Button Ablauf prüfen können Sie die im System bekannten Karten diesbezüglich kontrollieren.

Für die initiale Konfiguration gehen Sie wie folgt vor:

- 1** Importieren Sie zunächst die *Trust-service Status List (TSL)* über den Button TSL importieren.¹³⁶
- 2** Importieren Sie anschließend die CRL über den Button CRL importieren.¹³⁷

¹³³ Dies ist die Backup-Adresse außerhalb der TI, falls der Downloadpunkt der primären und sekundären TSL-Downloadadresse keine TSL liefern kann.


¹³⁴ Hier kann man die dazugehörige IP-Adresse als Rückfallwert eingeben, falls die DNS-Auflösung nicht funktioniert.


¹³⁵ Der Downloadpunkt ist: <https://tl.bundesnetzagentur.de/TL-DE.xml> [Stand: März 2024]


¹³⁶ Die gültige TSL kann über einen öffentlich zugänglichen Download-Punkt heruntergeladen und in einem lokalen Dateiverzeichnis abgelegt werden. Falls der Konnektor keine aktuelle TI-Verbindung hat, muss zum erfolgreichen Import der TSL der Leistungsumfang ONLINE deaktiviert werden.

¹³⁷ Die gültige CRL kann über einen öffentlich zugänglichen Download-Punkt heruntergeladen und in einem lokalen Dateiverzeichnis abgelegt werden. Alternativ ist auch ein Neustart des Konnektors möglich; darüber wird die CRL dann automatisch geladen. Nach diesem ersten (manuellen) Import prüft der Konnektor für TSL/CRL einmal täglich, ob eine aktuelle TSL/CRL verfügbar ist und lädt diese ggf. vom Downloadpunkt herunter.

- 3 Sobald der Konnektor mit der TI verbunden ist, werden im Bereich *Online Certificate Status Protocol* die primäre und sekundäre Adresse des Forwarders¹³⁸ sowie der TCP-Port des OCSP-Forwarders beim Zugangsdienstprovider angezeigt.
- 4 Für die *Grace Period nonQES*, den *Timeout nonQES* sowie den *Timeout QES* sind die Voreinstellungen eingetragen. Dies gilt auch im rechten Feld für die *Grace Period* zur *Trust-service Status List*.
- 5 Schließlich können Sie unter *Prüfungen* die Zeitabstände definieren, in denen das Ablaufen der Zertifikate aller gesteckten Karten überprüft werden soll und wie viele Tage vor deren Ablaufen auf der Managementschnittstelle eine Warnung erscheinen soll. Passen Sie bei Bedarf die jeweiligen Zeitabstände an.
- 6 Nachdem Sie sämtliche Einstellungen und Importe vorgenommen haben, speichern Sie diese mit dem Button Übernehmen ab.

 Im Online-Konnektor wird einmal täglich die Gültigkeit der TSL überprüft. Bei Bedarf wird sie automatisch heruntergeladen.

 Die für die Signaturfunktion des Konnektors erforderliche Vertrauensliste der Bundesnetzagentur (BNetzA-VL) wird bei aktiviertem *Leistungsumfang Signaturanwendungskomponente* (im Bereich *Verwaltung*) im definierten Zeitraum automatisch heruntergeladen. Sie kann alternativ im Bereich *Aktualisierung* manuell importiert werden.

 Im Zusammenhang mit der Konfiguration im Bereich *Verwaltung der Leistungsumfänge* ergeben sich Änderungen im Bereich *Zertifikatsdienst*. Sobald die Einstellung *Leistungsumfang ONLINE* deaktiviert ist, werden die folgenden Buttons inaktiv und damit **ausgegraut**: CRL aktualisieren, OCSP-Forwarder prüfen, OCSP-Request testen, TSL aktualisieren, BNetzA-VL aktualisieren. Eine Reaktivierung der Einstellung *Leistungsumfang ONLINE* aktiviert ebenfalls wieder diese Buttons.

7.5.5.1 CA-Import

Im Unterbereich CA¹³⁹-Import werden neue CA-Zertifikate manuell durch den Administrator importiert. Diese sind nur für die hybride Verschlüsselung von TI-fremden Zertifikaten vorgesehen. Den Import führen Sie über den Button neues CA-Zertifikat importieren durch.

| Import CA-Zertifikate | | | |
|---|------------|------------------|---------------------|
| Importierte CA-Zertifikate | | | |
| Distinguished Name | Aussteller | Gültigkeitsdauer | SHA-256 Fingerprint |
| <input type="button" value="CA-Zertifikat hinzufügen"/> | | | |

Abbildung 94: Importieren von CA-Zertifikaten

In der Tabelle wird für das eingebundene Zertifikat jeweils der *Distinguished Name*, der *Aussteller*, die *Gültigkeitsdauer* sowie der *SHA-256 Fingerprint* angezeigt.

¹³⁸ Hier handelt es sich jeweils um die Adresse des primären bzw. sekundären OCSP-Forwarders (HTTPS-Proxy) beim Zugangsdienstprovider als FQDN.

¹³⁹ Certificate / Certification Authority (Zertifizierungsstelle)



Beachten Sie für manuell importierte X.509-CA-Zertifikate folgende Sicherheitshinweise¹⁴⁰:

- Sie übernehmen als Administrator die Verantwortung für die Verlässlichkeit der importierten CA-Zertifikate.
- Sie können sich bei Ihrer Entscheidung für einen Import von CA-Zertifikaten auf die Informationen der gematik stützen.
- In diesem Zusammenhang veröffentlicht die gematik Informationen über CA-Betreiber, die das Erfüllen der Sicherheitsanforderungen der gematik nachgewiesen haben.

7.5.5.2 Status verwendeter Zertifikate

In diesem Bereich finden Sie eine tabellarische Übersicht über die verwendeten Zertifikate der gSMCKs. In den Spalten werden das jeweilige *Zertifikat*, das *kryptografische Verfahren*, der *Gültigkeitszeitraum*, der *Zertifikatsinhaber* und *-aussteller* sowie die *Seriennummer* angezeigt.

| Zertifikat | Kryptographisches Verfahren | gültig von | gültig bis | Inhaber | Aussteller | Seriennummer |
|------------------------------|-----------------------------|-------------------------------|-------------------------------|---|---|--------------|
| VPN-Tunnel (C.NK.VPN) | RSA-2048 | Mon Dec 13 15:14:31 CET 2021 | Sat Dec 12 15:14:30 CET 2026 | C=DE,ST=Berlin,L=Berlin,PostalCode=10963,STREET=Dessauer Str. 28/29,O=KoCo Connector GmbH TEST-ONLY - NOT-VALID,OI=8027688358000046472-20211213 | C=DE,O=gematik GmbH NOT-VALID,OU=Komponenten-CA der Telematikinfrastruktur,CN=GEM.KOMP-CAS4-TEST-ONLY | 1065 |
| VPN-Tunnel (C.NK.VPN2) | ECC-256 | Mon Dec 13 15:14:31 CET 2021 | Sat Dec 12 15:14:30 CET 2026 | C=DE,ST=Berlin,L=Berlin,PostalCode=10963,STREET=Dessauer Str. 28/29,O=KoCo Connector GmbH TEST-ONLY - NOT-VALID,OI=8027688358000046472-20211213 | C=DE,O=gematik GmbH NOT-VALID,OU=Komponenten-CA der Telematikinfrastruktur,CN=GEM.KOMP-CAS0-TEST-ONLY | 14546 |
| TLS zum PS (C.AK.AUT) | RSA-2048 | Mon Dec 13 15:14:33 CET 2021 | Sat Dec 12 15:14:32 CET 2026 | C=DE,ST=Berlin,L=Berlin,PostalCode=10963,STREET=Dessauer Str. 28/29,O=KoCo Connector GmbH TEST-ONLY - NOT-VALID,OI=8027688358000046472-20211213 | C=DE,O=gematik GmbH NOT-VALID,OU=Komponenten-CA der Telematikinfrastruktur,CN=GEM.KOMP-CAS4-TEST-ONLY | 1070 |
| TLS zum PS (C.AK.AUT2) | ECC-256 | Mon Dec 13 15:14:33 CET 2021 | Sat Dec 12 15:14:32 CET 2026 | C=DE,ST=Berlin,L=Berlin,PostalCode=10963,STREET=Dessauer Str. 28/29,O=KoCo Connector GmbH TEST-ONLY - NOT-VALID,OI=8027688358000046472-20211213 | C=DE,O=gematik GmbH NOT-VALID,OU=Komponenten-CA der Telematikinfrastruktur,CN=GEM.KOMP-CAS0-TEST-ONLY | 14551 |
| TLS zum KT (C.SAK.AUT) | RSA-2048 | Mon Dec 13 15:14:31 CET 2021 | Sat Dec 12 15:14:30 CET 2026 | C=DE,ST=Berlin,L=Berlin,PostalCode=10963,STREET=Dessauer Str. 28/29,O=KoCo Connector GmbH TEST-ONLY - NOT-VALID,OI=8027688358000046472-20211213 | C=DE,O=gematik GmbH NOT-VALID,OU=Komponenten-CA der Telematikinfrastruktur,CN=GEM.KOMP-CAS4-TEST-ONLY | 1067 |
| TLS zum KT (C.SAK.AUT2) | ECC-256 | Mon Dec 13 15:14:31 CET 2021 | Sat Dec 12 15:14:30 CET 2026 | C=DE,ST=Berlin,L=Berlin,PostalCode=10963,STREET=Dessauer Str. 28/29,O=KoCo Connector GmbH TEST-ONLY - NOT-VALID,OI=8027688358000046472-20211213 | C=DE,O=gematik GmbH NOT-VALID,OU=Komponenten-CA der Telematikinfrastruktur,CN=GEM.KOMP-CAS0-TEST-ONLY | 14548 |
| C2C für SUK (C.SAK.AUTO_CVC) | ECC | Mon Dec 13 00:00:00 CET 2021 | Thu Dec 10 00:00:00 CET 2026 | 8027688358000046472 | CAS0-TEST-ONLY DEARX | |
| C2C für SUK (C.CA_SAK_CS) | ECC | Thu Apr 09 00:00:00 CEST 2020 | Sat Apr 08 00:00:00 CEST 2028 | DEARX | DE0XX | |

Abbildung 95: Übersicht zum Status der verwendeten Zertifikate

¹⁴⁰ Vgl. [gemSpec_Kon], Kap. 3.6 „Verwendung manuell importierter CA-Zertifikate“

7.5.5.3 Laufzeitverlängerung

Die Funktion Laufzeitverlängerung ermöglicht es dem Administrator, die Laufzeit der in den gSMC-Ks der KoCoBox MED+ hinterlegten Zertifikate zu verlängern. Ohne diese Funktion laufen die bestehenden Zertifikate ab, und die weitere Nutzung der Telematik-Infrastruktur ist dann mit dieser KoCoBox MED+ (ohne eine Laufzeitverlängerung) nicht mehr möglich.

Hierzu werden pro gSMC-K eigene Containerdateien mit erneuerten Zertifikatsdaten bereitgestellt. Der Vorgang erfolgt gewöhnlich automatisch, kann jedoch durch den Administrator forciert werden.



Es ist alternativ eine manuelle Aktualisierung möglich, für die dann die Containerdateien separat per Upload zur KoCoBox MED+ eingespielt werden.

Laufzeitverlängerung

Manuelle Laufzeitverlängerung

↑

↑

↑

Automatische Laufzeitverlängerung

automatische Laufzeitverlängerung: EIN

AK.AUT für Authentisierung des Konnektors gegenüber Clientsystem

Auf alte Zertifikate zurücksetzen

Abbildung 96: Laufzeitverlängerung

Manuelle Laufzeitverlängerung

Im Abschnitt *manuelle Laufzeitverlängerung* werden die erwarteten Dateinamen der einzelnen Containerdateien auf den Buttons dargestellt. Die Dateinamen entsprechen den ICCSNs der eingebauten gSMC-Ks der KoCoBox MED+. Beim Klick auf den jeweiligen Button kann der passende Container mit den entsprechenden Zertifikaten zum Upload aus dem lokalen Dateisystem ausgewählt werden.



Achten Sie auf die korrekte Zuordnung der Containerdatei zur gSMC-K. Diese ist gegeben, wenn der Name der jeweils ausgewählten Datei mit dem dargestellten erwarteten Dateinamen übereinstimmt¹⁴¹. Anderenfalls kann ein reibungsloser Weiterbetrieb der KoCoBox MED+ nicht gewährleistet werden.

¹⁴¹ Es handelt sich um zip-Archive, die die passenden Zertifikate enthalten. Im Zweifelsfall kann solch ein Archiv extrahiert werden. Die ICCSN der betreffenden gSMC-K stellt dabei einen Namensbestandteil der meisten Zertifikatsdateien dar. Diese müssen mit den Vorgaben aus dem Dialog übereinstimmen, z.B. passen die Daten, wenn die Vorgabe 80276883580000048312.zip sich bei den extrahierten Zertifikatsdateien als C.AK.AUT_RSA_80276883580000048312.pem wiederfindet, analog für die anderen Zertifikate.

Nachdem alle Containerdateien ausgewählt sind, wird durch Klick auf den Button **Manuelle Verlängerung** starten der Vorgang gestartet.

Sollten hierbei Probleme auftreten, können mittels Klick auf den Button **Zertifikate löschen** die in der KoCoBox MED+ befindlichen, zuvor geladenen Zertifikate gelöscht werden. Anschließend kann über ein erneutes Hochladen der Zertifikatscontainer der gesamte Vorgang wiederholt werden.

Automatische Laufzeitverlängerung

Die *automatische Laufzeitverlängerung* erfolgt gewöhnlich, indem der Konnektor täglich die Bereitstellung auf dem zentralen Portal prüft und - sofern verfügbar - dann nutzt. Um die Laufzeitverlängerung z.B. im Zuge von Wartungsarbeiten unmittelbar vorzunehmen, kann dies durch Klick auf den Button **Verlängerung starten** ausgelöst werden.

Sollten hierbei Probleme bemerkt werden, kann über den Schalter **automatische Laufzeitverlängerung ein/aus** die Automatik angehalten werden.

AK.AUT für Authentisierung des Konnektors gegenüber Clientsystem

Eine erfolgte Laufzeitverlängerung beeinflusst auch die Authentisierung des Konnektors gegenüber dem Clientsystem. Das alte Zertifikat C.AK.AUT gilt nicht mehr, und das neue C.AK.AUT muss aktiviert werden. Dies ist im Abschnitt *AK.AUT für Authentisierung des Konnektors gegenüber Clientsystem* möglich. Hier wird diese Aktion durch Klick auf den Button **AK.AUT aktivieren** ausgeführt.

Auf alte Zertifikate zurücksetzen

Sollten Probleme während des Vorgangs auftreten, dann kann (temporär) auf den Ausgangszustand zurückgesetzt werden, indem im Abschnitt *Auf alte Zertifikate zurücksetzen* der Button **Reset** betätigt wird. Anschließend sollte die Laufzeitverlängerung erneut stattfinden, um die Funktion der KoCoBox MED+ aufrecht zu erhalten.



Nach der Laufzeitverlängerung kann es zu Problemen mit verbundenen Geräten (insbesondere Kartenterminals) kommen. Zeitlich verlängerte Zertifikate können seitens gematik von einer anderen Zertifiziererautorität (CA) ausgestellt worden sein, welche in der TSL des verbundenen Kartenterminals noch nicht hinterlegt ist. Damit geht das Pairing verloren, und es kann ohne eine aktualisierte TSL des Kartenterminals auch nicht wiederhergestellt werden. In solchen Fällen kann hier auf die alten Zertifikate zurückgesetzt werden, um kurzfristig und vorübergehend die Verbindung zum Kartenterminal wiederherzustellen. Danach ist eine Aktualisierung der TSL des Kartenterminals erforderlich. Für die Art der Bereitstellung dieser TSL wenden Sie sich an Ihren Servicepartner bzw. an den Hersteller des betreffenden Kartenterminals. Anschließend kann erneut manuell oder automatisch auf die laufzeitverlängerten Zertifikate umgestellt werden.

7.5.6 Protokollierungsdienst

Der *Protokollierungsdienst* zeichnet system- und sicherheitsrelevante Ereignisse, sowie Ereignisse im Kontext der Performancemessung innerhalb des Konnektors auf.¹⁴²

Er enthält die Unterbereiche *Sicherheitsprotokoll*, *Systemprotokoll* und *Performanceprotokoll*.¹⁴³

¹⁴² Vgl. [gemSpec_Kon], Kap. 4.1.10 „Protokollierungsdienst“

¹⁴³ Details zum Aufbau der Logfiles siehe weiter unten

Protokollierung

Log-Level für das Systemlog Debug


Speicherdauer der Einträge im Sicherheitsprotokoll: 180 Tage

Speicherdauer der Einträge im System- und Performanceprotokoll: 180 Tage

Protokolliere erfolgreiche Kryptooperationen: einschalten ausschalten

Abbildung 97: Konfigurationsbereich für den Protokollierungsdienst

- 1** Rufen Sie den Navigationsbereich Protokollierungsdienst auf und definieren Sie zunächst allgemeine Werte für diesen Dienst.
- 2** Die Einstellung des *Log-Levels für das Systemlog* erfolgt per Drop-down Menü (voreingestellt ist *Warning*).
- 3** Anschließend legen Sie die *Speicherdauer für die Einträge im Sicherheitsprotokoll* sowie im *System- und Performanceprotokoll* fest (voreingestellt sind jeweils 180 Tage).
- 4** Ob auch erfolgreich ausgeführte *Kryptooperationen* im Sicherheitsprotokoll gespeichert werden sollen, legen Sie über die Radiobuttons *einschalten / ausschalten* fest. Letzteres ist voreingestellt.

 Wir empfehlen die Übernahme der vorgegebenen Werte.

Mit Übernehmen speichern Sie die Einträge ab.

Unterbereiche Sicherheitsprotokoll, Systemprotokoll und Performanceprotokoll

In den drei Unterbereichen findet man die tabellarische Übersicht aller Logeinträge mit den folgenden Informationen:

- Zeitpunkt,
- Schwere,
- Beschreibung,
- Parameter.





Mittels Protokoll-Download kann man die Tabellen-Einträge der drei Unterbereiche jeweils herunterladen.

| Systemprotokoll | | | |
|----------------------------|---------|--------------------------------|---|
| 20 | | Seite 1 von 41 | 1 bis 20 von 808 Datensätzen |
| Zeitpunkt | Schwere | Beschreibung | Parameter |
| 27.06.2022 10:53:38.601 | ERR | ADMINISTRATIONSSERVICE/ERROR | Bedeutung=Interner Fehler; ErrorType=Technical; Error=4001; ErrorSeverity=Error |
| 27.06.2022 10:53:38.530 | WARN | CARD/ERROR | Bedeutung=Timeout bei der PIN-Eingabe; ErrorType=Technical; Error=4043; ErrorSeverity=Warning |
| 27.06.2022 10:52:41.293 | ERR | ADMINISTRATIONSSERVICE/ERROR | Bedeutung=Interner Fehler; ErrorType=Technical; Error=4001; ErrorSeverity=Error |
| 27.06.2022 10:52:41.221 | WARN | CARD/ERROR | Bedeutung=Timeout bei der PIN-Eingabe; ErrorType=Technical; Error=4043; ErrorSeverity=Warning |
| 27.06.2022 10:50:51.465 | INFO | OPERATIONAL_STATE/SYSTEM_STATE | log=0%; VmSize_ak=8393184kB; fd_ak=325; update=10%; uptime=1203371s; fd_sys=960; VmSize_nk=4859340kB; fd_nk=113; oom_kill=0; sec2=7%; sec1=7%; MemAvailable=46%; root=31%; loadavg=0.00 0.00 0.00 |
| 27.06.2022 09:50:51.468 | INFO | OPERATIONAL_STATE/SYSTEM_STATE | log=0%; VmSize_ak=8392784kB; fd_ak=324; update=10%; uptime=1199771s; fd_sys=960; VmSize_nk=4859340kB; fd_nk=113; oom_kill=0; sec2=7%; sec1=7%; MemAvailable=46%; root=31%; loadavg=0.00 0.00 0.00 |
| 27.06.2022 | | | log=0%; VmSize_ak=8392784kB; fd_ak=324; update=10%; uptime=1196171s; fd_sys=928; |

Protokoll löschen

Abbildung 98: Übersicht zum Systemprotokoll

In den Unterbereichen *Systemprotokoll* und *Performanceprotokoll* können Sie über den Button Protokoll löschen die jeweiligen Einträge entfernen.

-  Das Löschen des Sicherheitslogs ist nicht möglich, die Größe des Sicherheitslogs ist festgelegt.
-  Auf neue Einträge ins Sicherheitslog wird beim Login auf der Managementschnittstelle per Meldung im Anzeigefenster hingewiesen.
-  Werten Sie in diesem Fall unverzüglich das Sicherheitslog aus. Auch auf dem Display der KoCoBox MED+ erscheinen die entsprechenden Betriebszustandsmeldungen sowie ein Verweis auf das Handbuch (siehe auch das Kapitel Sicherheitsrelevante Szenarien).
-  Der Konnektor überwacht sich selbst in festgelegten Zeitabständen hinsichtlich Änderungen seines Betriebszustandes.¹⁴⁴ Im Protokoll werden die Ergebnisse dieser Überwachung dokumentiert.¹⁴⁵

Details zum Aufbau der Logfiles

Im Folgenden werden die Logdateien des Konnektors konkret beschrieben. Dabei sind die Parameter über alle Logdateien hinweg gleich.

¹⁴⁴ Vgl. [gemSpec_Kon], Kap. 3.3 „Betriebszustand“

¹⁴⁵ Der Aufbau eines solchen Eintrags im Log entspricht der Notation Wert = true oder Wert = false. False bedeutet hierbei, dass kein Fehlerzustand besteht. True bedeutet, dass ein Fehlerzustand eingetreten ist. Letzteres wird zusätzlich auf der Statusseite sowie am Display des Konnektors signalisiert, vgl. hierzu auch den Abschnitt Status und den Abschnitt Sicherheitskritische Fehlerzustände.

- Sicherheitsprotokoll: Hier werden Logeinträge hinterlegt, die nicht löscher sind. Dies verhindert, die Spuren von Manipulation, Manipulationsversuchen und Angriffen zu verwischen.
- Systemprotokoll: Hier werden Logeinträge hinterlegt, die dem Administrator zur Information dienen und die nicht dem Sicherheitsprotokoll zugehören.
- Performanceprotokoll: Hierin werden Performanceangaben zu Konnektor-Operationen dokumentiert.

| Kennung in der Logdatei | Beschreibung |
|-------------------------|--|
| Logrefid | eindeutige Referenz des Logeintrages im Konnektor |
| Timestamp | Zeitstempel des Logeintrages |
| Module | Bezeichnung des betroffenen Konnektormoduls |
| Amount | Anzahl, wie oft die Meldung in diesem Logeintrag zusammengefasst ist ¹⁴⁶ |
| Topic | Topic des protokollierten Ereignisses |
| protocolType | Schweregrad des Protokollierungseintrages |
| protocolSeverity | Protokollierungsart |
| Parameter | ereignisabhängige Parameter mit weiteren Details zum protokollierten Ereignis und Fehler |

Tabelle 3: Aufbau der Logdateien im Protokollierungsdienst

7.5.7 Signaturdienst

Der Signaturdienst bietet Clientsystemen und Fachmodulen eine Schnittstelle zum Signieren von Dokumenten und Prüfen von Dokumentensignaturen.¹⁴⁷

Er steht standardmäßig zur Verfügung und bietet zweierlei Funktionalitäten:

- die nicht-qualifizierte elektronische Signatur (nonQES): diese erfolgt mit der Institutionenkarte (Praxisausweis, SMC-B) sowie
- die qualifizierte elektronische Signatur (QES): Diese erfolgt mittels Heilberufsausweis (HBA).¹⁴⁸

Generell erfüllt die KoCoBox MED+ im Rahmen ihres Signaturdienstes folgende Funktionen:

- Signieren: Mittels einer elektronischen Signatur lassen sich die Integrität (Unverändertheit) und Authentizität (verbindliche Zuordnung zu einer bestimmten Person) beispielsweise eines Dokuments feststellen.
Allgemein versteht man unter einer elektronischen Signatur mit elektronischen Informationen verknüpfte Daten, mit denen der Unterzeichner bzw. Signaturersteller identifiziert und die Integrität der signierten elektronischen Informationen geprüft werden kann. Sie erfüllt somit aus technischer Sicht

¹⁴⁶ Ähnliche Logeinträge werden nach bestimmten, komplexen Regeln zusammengefasst.

¹⁴⁷ Vgl. [gemSpec_Kon], Kap. 4.1.8 „Signaturdienst“

¹⁴⁸ sowie den HBA-Vorläuferkarten HBA-qSig und ZOD_2.0 (=HBAX)

den gleichen Zweck wie eine eigenhändige Unterschrift auf Papierdokumenten.¹⁴⁹

- Verifizieren: Beim Verifizieren werden Authentizität und Integrität des signierten Dokuments geprüft, d.h.: Es wird geprüft, ob das Dokument im Zuge seiner Übertragung manipuliert wurde. Zudem kann auch ermittelt werden, ob der, der vorgibt, es signiert zu haben, dies auch wirklich getan hat.



Wenn bei der Prüfung von Signaturen (QES, nonQES) das Ergebnis VALID ist, wird ein identischer Erstellungs- und Prüfzeitpunkt angenommen. Der Grund dafür ist, dass es zum Zeitpunkt der Einführung von elektronischen Signaturen im Rahmen der Telematik-Infrastruktur keine historischen Algorithmen gibt.

Um fachliche Abläufe korrekt abzubilden, ist es gegebenenfalls erforderlich, ein Dokument mehrfach parallel zu signieren oder existierende Signaturen gegenzusignieren. Dies wird von der KoCoBox MED+ für beide Arten von Signaturen (QES, nonQES) unterstützt – ebenso wie Gegensignaturen, die jeweils alle existierenden Signaturen gegensignieren.

Der Signaturprozess selbst kann – sofern die Funktionalität angeboten wird – im Praxis-/Arztinformationssystem (PVS, AIS) direkt angestoßen werden. Der Signaturvorgang wird mittels PIN-Eingabe über das E-Health Kartenterminal bestätigt.¹⁵⁰

Beachten Sie bitte in diesem Fall folgenden Sicherheitshinweis:



Geben Sie Ihre PIN nur dann per Tastatur am E-Health-Kartenterminal ein, wenn das AIS/PVS die **gleiche** Jobnummer anzeigt wie auf dem Display des Kartenterminals. Stimmen diese Jobnummern nicht überein, geben Sie bitte Ihre PIN nicht ein.¹⁵¹



Beachten Sie hierzu bitte die Sicherheitshinweise im oberen Kapitel Verwaltung im Abschnitt Clientsysteme.

Signaturdienst

Einfachsignaturmodus: ein aus

Komfortsignaturmodus: aktiviert nicht aktiviert



 

Abbildung 99: Konfigurationsbereich des Signaturdienstes bei deaktiviertem Komfortsignaturmodus

Sie können hier den *Einfachsignaturmodus* per Radiobutton ein- bzw. ausschalten. Per Voreinstellung ist dieser eingeschaltet.

Die Konfiguration des Einfachsignaturmodus wechselt das sogenannte „Security Environment“ und hat

¹⁴⁹ Vgl. https://de.wikipedia.org/wiki/Elektronische_Signatur [Stand: März 2024]

¹⁵⁰ Siehe ausführlicher dazu die Dokumentation / Anleitung des jeweils eingesetzten Clientsystems.

¹⁵¹ Sofern dieser Fehler wiederholt auftritt, kontaktieren Sie bitte Ihren Support.

Einfluss auf die Behandlung von Dokumenten bei einer QES-Stapelsignatur:

- Bei aktivierter Funktion (Radiobutton ein) wird ein einzelnes Dokument nur als solches behandelt.
- Bei deaktivierter Funktion (Radiobutton aus) wird ein einzelnes Dokument wie ein Dokumentenstapel behandelt. Dieser erfordert die Anwendung von Secure Messaging¹⁵² für das Signieren.

Darüber hinaus kann hier der Komfortsignaturmodus aktiviert bzw. nicht aktiviert werden. Dieser ermöglicht nach einmaliger PIN-Eingabe das Signieren mehrerer Dokumente über einen längeren Zeitraum.¹⁵³

Mittels Übernehmen speichern Sie die jeweilige Konfiguration ab.



Nur Dokumente mit einer qualifizierten elektronischen Signatur (QES) gemäß eIDAS-Verordnung [eIDAS-VO] Kap. 1, Art. 3/12¹⁵⁴ können als elektronische Form eine per Gesetz geforderte Schriftform auf Papier ersetzen, vgl. § 126a BGB. Damit ersetzt die QES in der digitalen Welt rechtssicher die Unterschrift per Hand. Dafür ist eine Signaturkarte, wie z.B. der elektronische Heilberufsausweis (HBA), sowie die persönliche PIN des Signierenden (z.B. Arzt) erforderlich.



Fortgeschrittene (sowie auch einfache) elektronische Signaturen können gemäß § 127 BGB für formfreie Vereinbarungen eingesetzt werden. Die fortgeschrittene (nicht-qualifizierte) elektronische Signatur wird mittels PIN für die Institutionskarte (SMC-B, Praxisausweis) erstellt.



Bitte beachten Sie: Das Signaturformat PKCS#1 darf nur zu Authentisierungszwecken mit dem Authentisierungsschlüssel des HBAX und des SM-B verwendet werden.

¹⁵² Siehe dazu unten im Glossar den Eintrag zur Card-to-Card Authentisierung

¹⁵³ Siehe ausführlich zur Konfiguration weiter unten im Abschnitt Komfortsignatur

¹⁵⁴ <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910> [Stand: März 2024]



Bitte beachten Sie folgende Ausführungen zu Sicherheitsaspekten bei Signaturformaten:

- Für die Nutzung verschiedener Signaturformate existieren heute eine Vielzahl von Angriffen gegen die zu signierenden oder signierten Daten. Einerseits wird hierbei versucht, die Signatur als solche zu umgehen oder andererseits einen anderen Inhalt als gültig signiert erklären zu lassen. Besonders betroffen sind hiervon signierte XML-Dokumente (XAdES - sowohl für QES als auch für nonQES.155) und signierte PDF-Dokumente (PADES).
- Der Konnektor verringert das Risiko solcher Angriffe durch interne Schutzmaßnahmen und die Eingrenzung auf bestimmte Signaturschemata. Werden also Dokumente, die **nicht** den nachfolgend genannten Kriterien entsprechen, der KoCoBox MED+ zur Verifikation vorgelegt, erhält der Nutzer eine Ungültigkeitsaussage für die betreffende Signatur. Gleichfalls unterstützt die KoCoBox MED+ nur das Signieren von Dokumenten, die diesen Kriterien entsprechen.

Der Signaturdienst der KoCoBox MED+ unterstützt bei der Verifikation von Signaturen verschiedene Verfahren:

- PKCS#1 RSASSA-PSS
- PKCS#1 RSASSA-PKCS1-v1_5
- Elliptic Curve Digital Signature Algorithm (ECDSA)

CADES

Der Konnektor unterstützt sowohl nonQES- als auch QES-Signaturverfahren gemäß [CADES-BL] und [CADES]. Hierbei kommen die Signaturvarianten „detached signature“ und „enveloping signature“ zum Einsatz. Signiert wird ein gesamtes Binär-Dokument. Die Signatur wird außerhalb des Dokuments übergeben. Es werden die Dateitypen Text und TIFF sowie - ausschließlich für nonQES - Binärdateien unterstützt.

XAdES / QES

Der Konnektor unterstützt qualifizierte Signaturen auf XML-Dokumenten gemäß [XAdES-BL] und [XAdES] ausschließlich in Verbindung mit einer benannten Signaturrechtlinie. In der vorliegenden Version ist dies ausschließlich die in der Firmware der KoCoBox MED+ verankerte Signaturrechtlinie des Fachmoduls NFDM. Die letztgenannte Funktionalität ist dem Fachmodul NFDM vorbehalten und kann nicht durch Nutzer aufgerufen werden.

Eigenschaften der unterstützten Signaturrechtlinie SR_DF_NFDM_NOTFALLDATEN:

- konform zu [gemRL_QES_NFDM]
- qualifizierte elektronische Signatur
- erlaubt eine detached XAdES-Signatur, die innerhalb des Dokuments eingebettet ist
- unterstützt Daten, bei denen das Dokument XML-Schema-valide zum gematik-Schema „/fa/nfds/NFD_Document_v1_4.xsd“ mit dem targetNamespace „http://ws.gematik.de/fa/nfds/NFD_Document/v1.4“ ist.

¹⁵⁵ nonQES wird aktuell nicht unterstützt.

Hierbei kommt die die Signaturvariante „detached signature“ zum Einsatz. Signiert wird ein ausgewähltes Nicht-Root-Element mit Sub-Elementen im Eingangs-XML-Dokument. Die Signatur wird innerhalb des Dokuments, jedoch außerhalb des signierten Sub-Baums abgelegt.

Die verwendeten Schemata sind gegenüber den durch die gematik spezifizierten Schemata zusätzlich für den Einsatz mit NFD-Dokumenten gehärtet (siehe hierzu im Anhang das Kapitel **Gehärtete Schemata für XAdES-NFD**). Die einzige unterstützte Transformation findet zur Kanonisierung der XML-Daten gemäß <https://www.w3.org/2006/12/xml-c14n11> (ohne Kommentare) statt.

XAdES / nonQES

Der Konnektor unterstützt aktuell keine nicht-qualifizierten Signaturen auf XML-Dokumenten.



Der Hersteller empfiehlt generell die Verwendung von CAdES-Signaturen zur Vermeidung von Risiken, die bei Nutzung von XML-Signaturen ansonsten unumgänglich sind.

PAdES

Der Konnektor unterstützt sowohl nonQES- als auch QES-Signaturverfahren gemäß [PAdES-BL], und [PAdES] von PDF/A-Dokumenten, schränkt jedoch die Verwendung von PAdES-Signaturen wie folgt ein:

PAdES-Signaturen, die nicht das gesamte PDF-Dokument umfassen, werden als ungültig gewertet. Weiterhin werden keine Updates auf einem bereits signierten Dokument unterstützt:

- Es können keine OCSP-Responses in den Document Security Store eingebettet werden.
- Dokumentinkludierende Gegensignaturen in Form von PDF Serial Signatures werden nicht unterstützt.

Die KoCoBox MED+ führt eine robuste Analyse von PDF-Dokumenten aus. Das Ziel der Funktionalität ist, eine möglichst große Spanne von PDF-Dokumenten verarbeiten zu können.



Die KoCoBox MED+ ist nicht geeignet, Aussagen über die Standardkonformität von PDF-Dokumenten zu treffen; sie ist kein PDF-Validierer.



Der Benutzer ist dafür verantwortlich, die übergebenen PDF-Dokumente auf ihre Konformität zum PDF-Standard zu prüfen. Insbesondere **muss** der Benutzer sicherstellen, dass die PDF-Start- und PDF-Endemarkierungen an den korrekten Positionen gemäß [PAdES, dort siehe [1]] im Dokument stehen. Wenn der Benutzer Dokumente in den Signaturprozess einbringt, die diesen Vorgaben nicht entsprechen, so sind diese Dokumente nach dem Signaturvorgang unter Umständen nicht mehr lesbar.

Komfortsignatur

Die Funktion Komfortsignatur gestattet es, mehrere Dokumente mit einem Heilberufsausweis (HBA) qualifiziert zu signieren (QES), ohne für jedes Dokument erneut die PIN eingeben zu müssen. Sie wird in den Einstellungen des Signaturdienstes aktiviert und über das Arzt- bzw. Praxisinformationssystem (AIS/PVS) angesprochen.

Der Komfortsignaturmodus wird mittels Radiobutton konfiguriert und ist per Voreinstellung nicht aktiviert.



Der Komfortsignaturmodus kann nur dann aktiviert werden, wenn die Verbindung zwischen Clientsystem und KoCoBox MED+ gesichert ist.¹⁵⁶ Anderenfalls ist die Auswahl deaktiviert. Die Einstellung hierzu erfolgt über die Verwaltung für Clientsysteme. Hier sind **zwingend** die Verbindung via TLS und die verpflichtende Authentisierung zu aktivieren.

Abbildung 100: Konfigurationsbereich für den Signaturdienst mit aktiviertem Komfortsignaturmodus

Sobald der Komfortsignaturmodus aktiviert ist, können zusätzliche Einstellungen vorgenommen werden.

Der größtmögliche Wert, den Sie im Feld *Maximale Anzahl Komfortsignaturen* eintragen können, liegt bei 250. Der Wertebereich reicht von 1 bis 250 (voreingestellt sind 100).

Die maximale Anzahl für Komfortsignaturen begrenzt die Menge an Signaturen, die mit einer PIN-Verifikation am HBA ausgeführt werden können.



Nach Überschreitung der in diesem Feld vorgegebenen Anzahl ist eine **erneute PIN-Verifikation** erforderlich.



Diese maximale Anzahl von Komfortsignaturen ist, neben der Einstellung in der KoCoBox MED+, im HBA abgelegt. Der Wert kann **nicht** überschritten werden.

Der Wert im Feld *Maximale Dauer Komfortsignaturen* definiert den Zeitraum, in welchem ab dem ersten Aufruf die Menge an Dokumenten mit einmaliger PIN-Verifikation ausgeführt werden kann.

Der längstmögliche Zeitraum umfasst 24 Stunden (Wertebereich von 1 bis 24 Stunden, voreingestellt sind 6 Stunden).

¹⁵⁶ Dies setzt voraus, dass im Bereich *Verwaltung / Clientsystem* die *Verbindung nur via TLS* sowie die *verpflichtende Authentisierung* aktiviert sind.



Nach dem Ablauf dieser Zeitspanne ist eine **erneute PIN-Verifikation** erforderlich.



Das Entfernen des HBA terminiert die Komfortsignatur-Sitzung. Nach dem erneuten Stecken des HBA kann über die PIN-Verifikation eine neue Komfortsignatur-Sitzung mit den konfigurierten Werten der KoCoBox MED+ ausgeführt werden.



Die Authentifizierung des HBA-Inhabers erfolgt für die Komfortsignaturfunktion durch das angeschlossene Clientsystem. Diese Authentifizierung ist erforderlich, denn sie leistet einen unverzichtbaren Beitrag zur Sicherheit des Komfortsignaturverfahrens.



Nach Aktivierung der Komfortsignatur und Eingabe der HBA-PIN ist es jedem Nutzer des verbundenen Clientsystems für die unter "maximale Dauer Komfortsignaturen" konfigurierte Zeit bzw. für die unter "maximale Anzahl Komfortsignaturen" konfigurierte Anzahl an Signaturen möglich, Dokumente im Namen des HBA-Inhabers elektronisch zu unterschreiben.



Für die sichere Verwendung der Komfortsignaturfunktionalität muss das angeschlossene Clientsystem pro Aktivierung der Komfortsignaturfunktion (Komfortsignatur-Sitzung) eine eindeutige UserID im Format UUID gemäß RFC4122 generieren. Hierfür muss das Clientsystem garantiert ausreichenden Zufall, d.h. in einer Menge von mindestens 128 bits, bereitstellen und verwenden. Der Anbieter des Clientsystems stellt Ihnen hierzu nötige Informationen zur Verfügung.

7.5.8 LDAP-Proxy

Der Konnektor bietet den Dienst LDAP-Proxy an. Dieser kann beispielsweise durch einen KIM-Client genutzt werden, um Zugriff auf die in der TI hinterlegten Austauschinformationen des Verzeichnisdienstes (VZD) zu erhalten.

Der LDAP-Proxy selbst muss nicht separat konfiguriert werden; er ist jedoch nur nutzbar, wenn eine Online-Verbindung zur TI besteht. In diesem Fall ist er unter der IP-Adresse der KoCoBox MED+ auf den Ports 389 (LDAP) oder 636 (LDAPS) zu erreichen.



Aus Sicherheitsgründen wird empfohlen, ausschließlich mit LDAPS zu arbeiten. Für die Auswahl, ob LDAP oder LDAPS nutzbar ist, gelten die Anbindungseinstellungen für die Clientsysteme weitgehend, d.h. der Schutz der Verbindung zum LDAP-Proxy folgt den Einstellungen, die für die Anbindung der Clientsysteme für die Nutzung der allgemeinen Konnektordienste konfiguriert sind. Basic-Authentication wird hierbei jedoch **nicht** unterstützt. Stattdessen ist zertifikatsbasierte Authentisierung zu verwenden.



Wir empfehlen allgemein, die **clientseitige TLS-Authentisierung** zu konfigurieren. Nur so kann eine ausreichende Sicherheit für den Zugriff auf die Dienste des Verzeichnisdienstes gewährleistet werden. Das nötige Clientzertifikat bzw. Schlüsselpaar kann im Bereich *Verwaltung/Clientsysteme/Zugangszertifikate für Clientsysteme* konfiguriert werden.

7.5.9 Verschlüsselungsdienst

Der Verschlüsselungsdienst bietet Clientsystemen und Fachmodulen eine Schnittstelle zum Ver- und Entschlüsseln von Dokumenten. Dazu werden

- hybride und symmetrische Ver-/Entschlüsselung von CMS-Dokumenten gemäß [RFC5652] sowie
- hybride Ver-/Entschlüsselung von XML-Dokumenten entsprechend [W3C] Recommendation „XML Encryption Syntax and Processing“

unterstützt. Das hierfür genutzte Verfahren entspricht PKCS#1 gemäß [RFC8017].



Der Verschlüsselungsdienst selbst muss nicht separat konfiguriert werden.

Für die Dokumentenverschlüsselung verwendet die KoCoBox MED+ als symmetrischen Schlüssel ausschließlich eine Schlüssellänge von 256 bits. Für die Entschlüsselung von Dokumenten werden die symmetrischen Schlüssellängen 256, 192 und 128 bits unterstützt.

Die möglichen Empfänger der mit Hilfe des Verschlüsselungsdienstes gesicherten Daten orientieren sich an den für die KoCoBox MED+ verfügbaren Empfängerzertifikaten. Diese müssen für Verschlüsselung geeignet¹⁵⁷, zum Zeitpunkt der Verschlüsselung (Referenzzeitpunkt) gültig sowie mittels eines gemäß [gemSpec_PKI] zulässigen Kryptoalgorithmus unterschrieben worden sein.

Empfängerzertifikate können genutzt werden, wenn:

- deren CA sich in der Liste der importierten CAs befindet (siehe im Kapitel Zertifikatsdienst / CA-Import) oder
- deren CA in der TSL der KoCoBox MED+ aktiv ist und die mindestens eine der folgenden Policies enthält:
 - a) OID_EGK_ENC (1.2.276.0.76.4.68)
 - b) OID_EGK_ENCV (1.2.276.0.76.4.69)
 - c) OID_HBA_ENC (1.2.276.0.76.4.74)
 - d) OID_SMCB_ENC (1.2.276.0.76.4.76)



Das Empfängerzertifikat darf zum Referenzzeitpunkt **nicht widerrufen** sein.

XML-Formate werden für die Ver-/Entschlüsselung von Dokumenten mit folgenden Eckwerten unterstützt:

- max. Textgröße pro Einzelknoten = 30 MB im äußeren Dokument (Base64)
- max. Tiefe des Dokumentenbaums = 256 Ebenen
- max. erlaubte Größe für die Vorschau (Lookup) innerhalb des Dokuments = 4 MB
- max. Größe eines einzelnen Bezeichners (Markup Identifier) = 1.000 Bytes
- max. Größe einer generischen Entität = 10.000 Bytes
- max. Wert Verzeichnisgröße (Dictionary Size) = 10 MB



Damit wird ein Schutz gegen böartige (malformed) Dokumente angestrebt.

¹⁵⁷ Dies wird durch das Zertifikatselement KeyUsage = keyEncipherment ermöglicht.

7.6 Konnektormanagement

In den folgenden Abschnitten werden die übergreifenden Konfigurationen der KoCoBox MED+ dargestellt.

7.6.1 Benutzerverwaltung

Die KoCoBox MED+ bietet eine Verwaltung der Nutzer, die das Gerät in der Rolle eines Administrators konfigurieren sowie die Protokolle einsehen dürfen. In der Benutzerverwaltung werden die anmeldeberechtigten Administratoren-Benutzer definiert.



Abbildung 101: Benutzerverwaltung der KoCoBox MED+

Hierbei werden zwei Administrator-Rollen mit verschiedenen Rechten unterschieden:



- *Admin*¹⁵⁸: Hat ausschließlich Zugriff über den lokalen Endpunkt der Managementschnittstelle (Webinterface) und verwaltet alle Konfigurationsdaten des Konnektors, außer die Benutzerverwaltung. Zudem hat er, sofern sie ihm vom *SuperAdmin* zugewiesen wurden, erweiterte Berechtigungen (Werksreset durchführen).
- *SuperAdmin*¹⁵⁹: Hat ausschließlich Zugriff über den lokalen Endpunkt der Managementschnittstelle (Webinterface), verwaltet Benutzerkonten sowie alle Konfigurationsdaten des Konnektors. Zudem kann er die Kontaktdaten anderer Administrator-Benutzer – auch die eines weiteren Super-Administrators – bearbeiten.

Zudem gibt es zwei herstellerspezifische Benutzer-Rollen:

- *Supporter*: Besitzt überwiegend lesende Berechtigungen auf Konfigurationen der KoCoBox MED+. Er darf für das Einsatzszenario *Standalone mit physischer Trennung* aktuelle TSLS/CRLs einbringen und manuell die Zeit des Konnektors einstellen. Zudem sind ihm das Herunterladen von Logs und das Auslösen des Konnektorneustarts gestattet; darüber hinaus gehende Änderungen dieser Konfigurationen sind nicht möglich, die Benutzerverwaltung ist ihm nicht zugänglich.
- *LogDownloader*: Hat nur die Berechtigung, Logdateien einzusehen und diese herunterzuladen, weitere Konfigurationen der KoCoBox MED+ kann er weder einsehen noch modifizieren.

¹⁵⁸ Zur besseren Lesbarkeit im Fließtext wird diese Rolle auch als *Lokaler Administrator* bezeichnet.

¹⁵⁹ Zur besseren Lesbarkeit im Fließtext wird diese Rolle auch als *Super-Administrator* bezeichnet.

Die Tabelle *Benutzer* listet die Administrator-Benutzer der KoCoBox MED+ mit *Name*, *Rolle* sowie den zugewiesenen Rechten (*Werksreset durchführen*) auf. Sie können mittels  editiert werden. Per Löschen-Symbol  wird der Benutzer entfernt.

Administrator-Benutzer hinzufügen



Abbildung 102: Anlegen eines neuen Administrators in der Benutzerverwaltung

Ein neuer Administrator-Benutzer der KoCoBox MED+ wird mit der gewünschten Rolle wie folgt angelegt:

- 1 Über den Button *Benutzer hinzufügen ...* öffnen Sie das Konfigurationsfenster *Benutzer hinzufügen*. Tragen Sie in der Zeile *Name* eine Bezeichnung ein und weisen Sie dann per Drop-down Liste die vorgesehene Rolle (*SuperAdmin*, *Admin*¹⁶⁰, *LogDownloader*, *Supporter*¹⁶¹) sowie ggf. bestimmte Rechte (*Werksreset durchführen*) zu. Mittels *OK* wird der Eintrag bestätigt.
- 2 Es erscheint ein Anzeigefenster, das das Einmalpasswort beinhaltet. Notieren Sie dieses für den neu angelegten Administrator-Benutzer.

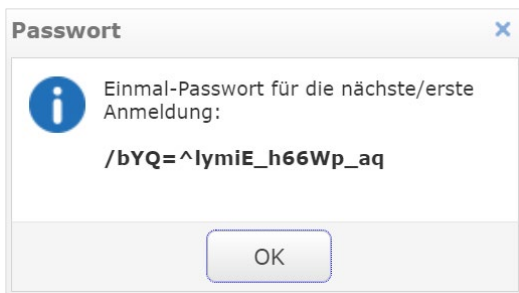


Abbildung 103: Anzeige des Einmalpassworts

- 3 Verlassen Sie abschließend dieses Anzeigefenster mit *OK*.
Der neu angelegte Administrator erscheint nun in der Tabelle *Benutzer*.

¹⁶⁰ Das ist der lokale Administrator.

¹⁶¹ Die Rollen *LogDownloader* und *Supporter* sind herstellerspezifische Rollen, die Rolle *RemoteAdmin* ist unwirksam.



Dieser neue Administrator-Benutzer **muss** das Einmalpasswort bei seinem ersten Login auf der Managementschnittstelle in sein **persönliches Passwort ändern**.¹⁶²




Dem lokalen Administrator kann die erweiterte Berechtigung zum Durchführen eines Werksreset von einem Super-Administrator erteilt bzw. entzogen werden. Dies wird im Eigenschaften-Fenster des lokalen Administrators konfiguriert, indem die entsprechenden Häkchen gesetzt bzw. entfernt werden.



Benutzer mit der Rolle *Super-Administrator* erhalten grundsätzlich diese erweiterten Berechtigungen. Diese können ihnen auch nicht entzogen werden. Aus Sicherheitsgründen ist die Berechtigung zum Werksreset hier standardmäßig deaktiviert. Bitte aktivieren Sie diese, um in der Rolle *Super-Administrator* über die Administrationsoberfläche einen Werksreset auszuführen.

Administrator-Benutzer löschen

In der Rolle *Super-Administrator* löschen Sie mittels  einen Administrator-Benutzer. Bestätigen Sie die Frage im Dialogfenster mit OK.

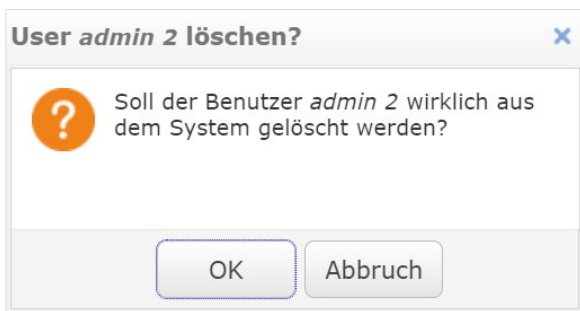



Abbildung 104: Löschen eines Administrator-Benutzers



Ein Administrator kann nicht gelöscht werden, solange er im System eingeloggt ist.

Passwort eines Administrators ändern

Um das Passwort eines Administrator-Benutzers zu löschen, rufen Sie  über das entsprechende Konfigurationsfenster auf.

¹⁶² Das Vorgehen entspricht dem der zweistufigen Vergabe des neuen Passworts bei der Erstanmeldung des Administrators an der Managementschnittstelle der KoCoBox MED+.

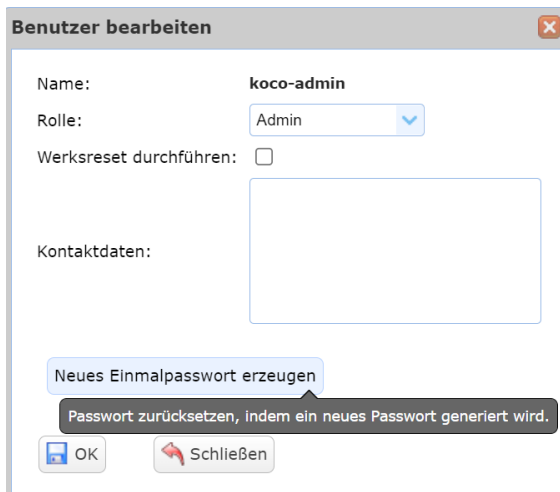


Abbildung 105: Passwort eines bestehenden Administrators ändern

Über den Button Neues Einmalpasswort erzeugen wird für diesen Administrator ein neues Einmalpasswort angelegt. Notieren Sie dieses Passwort für den betreffenden Administrator und hinterlegen Sie diese Info geschützt.

Per OK schließt man das Konfigurationsfenster wieder.



Mit diesem Einmalpasswort muss sich der entsprechende Administrator auf der Management-schnittstelle einloggen und anschließend sofort ein **eigenes persönliches Passwort** vergeben.

7.6.2 Infomodell

Im Bereich *Infomodell* werden einzelnen Personen (Mandanten) einzelne Arbeitsplätze und Clientsysteme zugewiesen.¹⁶³

Infomodell

Infomodell importieren

Die einzelnen Entitäten des Infomodells können über die folgenden Tabellen bearbeitet werden. Die Relationen zwischen ihnen werden in den Dialogen zur Bearbeitung verwaltet. So kann beispielsweise die Zuordnung eines Kartenterminals zu einem Arbeitsplatz sowohl im Bearbeiten-Dialog des entsprechenden Arbeitsplatzes vorgenommen werden als auch im Bearbeiten-Dialog des Kartenterminals.

Mandanten

Mandant hinzufügen ...

| | | |
|--|--|---------------------|
| | | M1 |
| | | Mandant_ePA_Default |

Clientsysteme

Clientsystem hinzufügen ...

| | | |
|--|--|--------------------------|
| | | CS1 |
| | | Clientsystem_ePA_Default |

Arbeitsplätze

Arbeitsplatz hinzufügen ...

| | | |
|--|--|-----------------------|
| | | Konnektor |
| | | WP1 |
| | | Workplace_ePA_Default |

SMBen

SMB hinzufügen ...

| Bezeichnung | ICCSN | | |
|-------------|-------|--------|---------------------|
| | | SMC_M1 | 8027688311000095965 |

Kartenterminals

Kartenterminal hinzufügen ...

| Kartenterminal | Slots | | |
|----------------|-------|------------|---------|
| | | CT_ID_0001 | 1,2,3,4 |

CS-AP Objekte

CS-AP Objekt hinzufügen ...

| | Mandant | Clientsystem | Arbeitsplatz |
|--|---------------------|--------------------------|-----------------------|
| | M1 | CS1 | Konnektor |
| | M1 | CS1 | WP1 |
| | Mandant_ePA_Default | Clientsystem_ePA_Default | Workplace_ePA_Default |

Remote-PIN-KT Objekte

Remote-PIN-KT Objekt hinzufügen ...

| Mandant | Arbeitsplatz | Kartenterminal |
|---------|--------------|----------------|
|---------|--------------|----------------|

Übernehmen

Verwerfen





Abbildung 106: Beispiel-Informationsmodell für die erlaubten Zugriffsmöglichkeiten

¹⁶³ zur Umsetzung des Informationsmodells siehe [PP-0098], S. 89; im Anhang findet sich im Abschnitt Ergänzende technische Informationen ein exemplarisches Infomodell mit dem dazugehörigen XML-Schema.


Die Konfigurationen im Bereich *Infomodell* können auf zwei Wegen vonstatten gehen:

- 1** Zum einen kann man das komplette Infomodell (in Form einer XML-Datei) importieren.



Mit dem Button *Infomodell importieren* lesen Sie aus einem Verzeichnis eine entsprechende XML-Datei ein, die das komplette Infomodell abbildet. Mittels *Übernehmen*-Button werden sämtliche Tabellen des Infomodells direkt gefüllt.

-  Beachten Sie bei der Namensvergabe für die einzelnen Entitäten, dass die Symbole `&` `<` `>` `"` `'` `/` nicht unterstützt werden.¹⁶⁴ Infomodelle und Konfigurationen, die solche Symbole enthalten, führen zu einem Fehler beim Import.
-  Es ist nicht möglich, einzelne Teile eines Infomodells einzulesen!
-  Bitte achten Sie bei Erstellung und Import eines individualisierten, statischen Infomodells darauf, dass dieses konsistent und ohne unreferenzierte Einträge definiert wird. Andernfalls funktioniert der Konnektor nicht, auch SOAP Requests werden nicht ausgeführt.
-  Es ist möglich, das initial leere Infomodell zu speichern und den Konnektor damit zu starten. Voraussetzung für die Durchführung fachlicher Anwendungen ist jedoch ein korrekt ausgefülltes Infomodell.

- 2** Zum anderen können die einzelnen Elemente des Modells durch einen Administrator angelegt und gespeichert werden.

-  Bitte beachten Sie, dass der Administrator jederzeit für die korrekte Zuordnung von Kartenterminals und Clientsystemen verantwortlich ist.

Im Rahmen der **mandantenbezogenen Administration** (Einstiegspunkt ist der Mandant) werden die einzelnen Entitäten des Modells über die jeweiligen Tabellen (Mandanten, Clientsysteme, Arbeitsplätze, SMBen, Kartenterminals, CS-AP Objekte, Remote-PIN-KT Objekte) bearbeitet. Die Beziehungen zwischen ihnen werden in den Konfigurationsfenstern zur Bearbeitung verwaltet.¹⁶⁵

-  Für die Nutzung des Fachmoduls ePA ist eine Beziehung zum Infomodell erforderlich. Die hierzu nötigen Daten werden mit jedem Aufruf an der Dienstschnittstelle durch das Clientsystem übergeben. Ist dies nicht gegeben, dann ist eine **feste** Standardbeziehung einzurichten.
-  Die Verwendung der Standardbeziehung ist **nur** für die Nutzung des Dienstes PHRService möglich.

¹⁶⁴ Ältere Softwareversionen des Konnektors unterstützten diese Symbole. Bereits bestehende Infomodelle mit solchen unzulässigen Entitäts-IDs werden bei einer Softwareaktualisierung beibehalten. Möchte man aber Änderungen daran vornehmen, muss man das Infomodell vollständig korrigieren.

¹⁶⁵ So kann beispielsweise die Zuordnung eines Kartenterminals zu einem Arbeitsplatz sowohl im Bearbeiten-Dialog des entsprechenden Arbeitsplatzes vorgenommen werden als auch im Bearbeiten-Dialog des Kartenterminals.

Die zugehörigen Entitäten müssen dazu in den Tabellen Mandanten, Clientsysteme und Arbeitsplätze mit ihren Beziehungen angelegt werden:

- Mandanten: *Mandant_ePA_Default*
- Clientsysteme: *Clientsystem_ePA_Default*, muss *Mandant_ePA_Default* zugewiesen sein
- Arbeitsplätze: *Workplace_ePA_Default*, muss *Mandant_ePA_Default* zugewiesen sein

Gehen Sie dafür wie folgt vor:

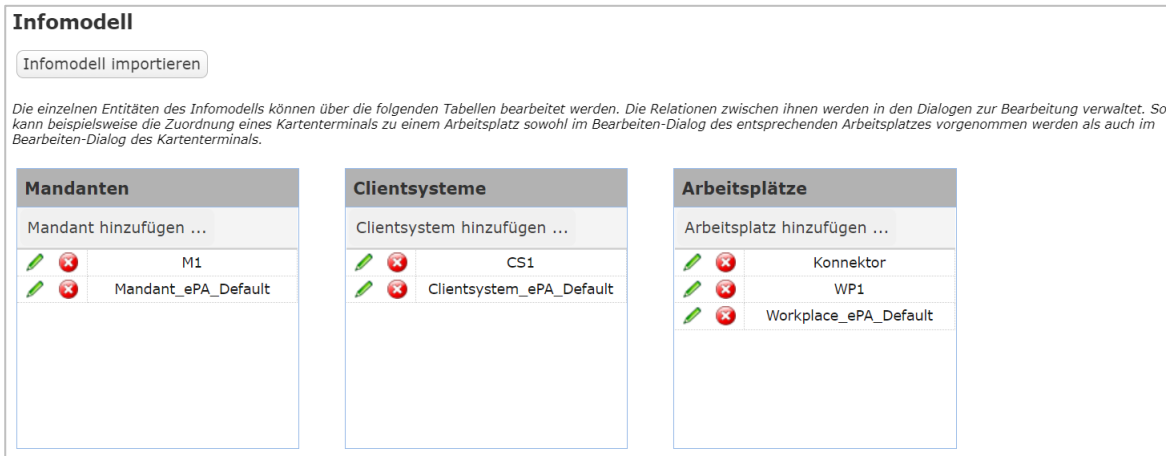


Abbildung 107: Infomodell-Konfigurationsbereiche für Mandanten, Clientsysteme und Arbeitsplätze

- 1** Definieren Sie einen Mandanten bzw. wählen Sie in der Tabelle *Mandanten* einen Mandanten aus: Über den Button Mandant hinzufügen... öffnet sich das Konfigurationsfenster *Eintrag*. Geben Sie hier die *Mandant-ID* ein.
- 2** Ordnen Sie pro Mandant aus den bereits eingepflegten Entitäten (SMB, Clientsystem, Arbeitsplatz, Kartenterminal) die für den Mandanten im Zugriff erlaubten zu, indem Sie in der jeweiligen Tabelle entsprechende Häkchen setzen. Bestätigen Sie dies mittels OK.
- 3** Ordnen Sie pro Mandant die jeweiligen Arbeitsplätze dem Clientsystem zu: Über den Button Clientsystem hinzufügen... öffnet sich das Konfigurationsfenster *Eintrag*. Tragen Sie hier die *Clientsystem-ID* ein und stellen Sie die Relation zum Mandanten her, indem Sie das Häkchen in der Tabelle entsprechend setzen. Mittels OK bestätigen Sie dies.

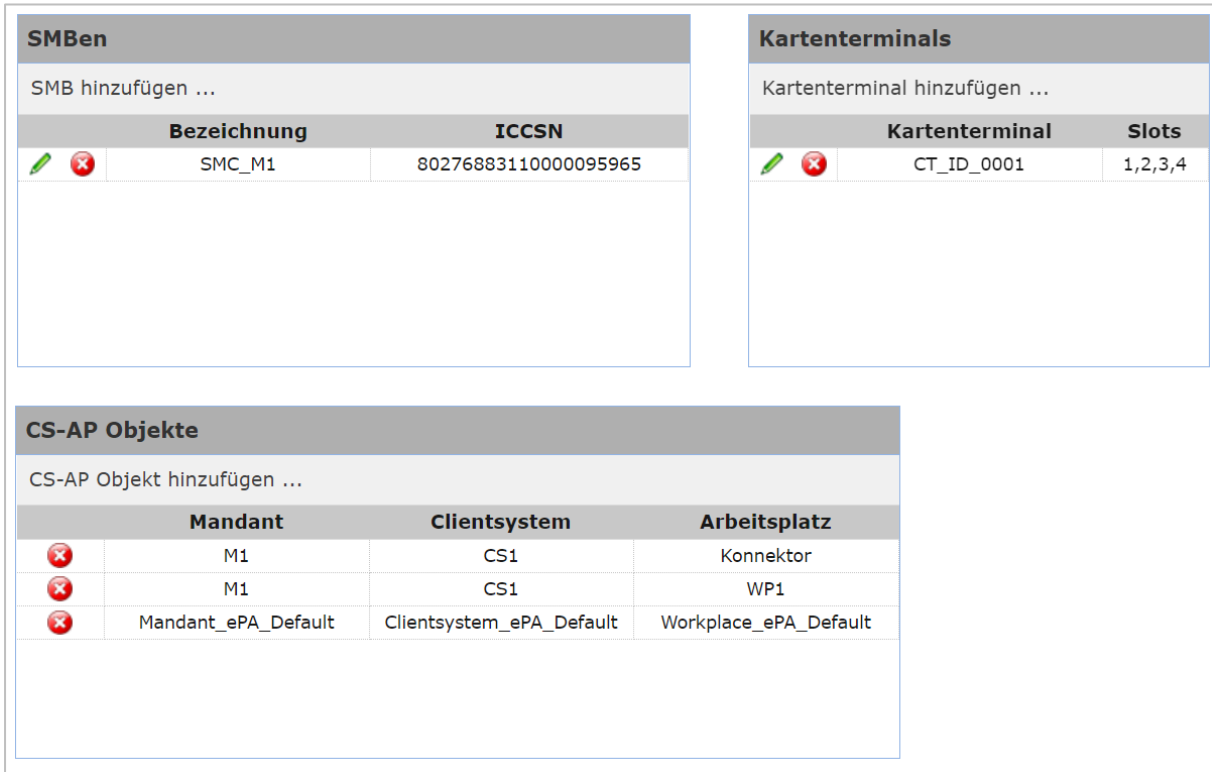


Abbildung 108: Infomodell-Konfigurationsbereiche für SMBen, Kartenterminals und CS-AP Objekte




- 4** Ordnen Sie pro Mandant die lokalen Kartenterminals zu, über die man jeweils pro Arbeitsplatz die Remote-PIN eingeben darf: Über Arbeitsplatz hinzufügen... öffnet sich das Konfigurationsfenster *Eintrag*. Geben Sie hier die Arbeitsplatz-ID ein und stellen Sie durch entsprechende Häkchen die Beziehung zum Mandanten/Kartenterminal her. Bestätigen Sie dies mit OK.
- 5** Über den Button SMB hinzufügen... öffnet sich das Konfigurationsfenster *Eintrag*. Sie tragen hier die *SMB-ID* sowie die *ICCSN* ein und ordnen diese dem entsprechenden Mandanten zu, indem Sie das Häkchen setzen. Mittels OK bestätigen Sie die Einträge.
- 6** Über den Button Kartenterminal hinzufügen... öffnet sich das Konfigurationsfenster *Eintrag*. Sie fügen hier die *Kartenterminal-ID* ein und setzen bei der entsprechenden Slotnummer das Häkchen. Ordnen Sie entsprechend Mandanten/Arbeitsplatz zu, indem Sie die passenden Häkchen setzen. Mittels OK bestätigen Sie die Konfiguration.
- 7** Über den Button CS-AP Objekt hinzufügen... öffnet sich das Konfigurationsfenster *Eintrag*. Sie setzen hier die entsprechenden Häkchen in den Tabellen Mandant/Clientsystem/Arbeitsplatz. Mittels OK bestätigen Sie die Konfiguration.



Abbildung 109: Infomodell-Konfigurationsbereich für Remote-PIN-KT Objekte

8 Über den Button Remote-PIN-KT Objekte hinzufügen... öffnet sich das Konfigurationsfenster *Eintrag*. Sie setzen hier die entsprechenden Häkchen in den Tabellen Mandant/Arbeitsplatz/Kartenterminal. Mittels OK bestätigen Sie die Einträge.

Nach Beenden sämtlicher Konfigurationen bestätigen Sie diese mittels Übernehmen.


 Die Einträge in den Tabellen können Sie mittels  bearbeiten oder mittels  löschen. In der Tabelle *CS-AP Objekte* können Einträge nur gelöscht werden.


7.6.3 Aktualisierung

Im Bereich *Aktualisierung* können Sie die KoCoBox MED+ selbst als auch die von ihr verwalteten Kartenterminals softwareseitig aktualisieren. Zudem ist die Prüfung auf neue Konfigurationen der Infrastruktur (Bestandsnetze) möglich.

Im Unterbereich *Übersicht* kann man den aktuellen Status von Updates für den Konnektor und die Kartenterminals einsehen.

Updates werden gewöhnlich durch die Server des Konfigurations- und Software Repository-Dienstes (KSR-Dienst) bereitgestellt. Sie erscheinen entsprechend ihrer Verfügbarkeit für den Konnektor und die verwalteten Geräte in den Listen der Softwareaktualisierung. Einzelne Updates werden hier ausgewählt und aktiviert.

 Die KoCoBox MED+ erlaubt zusätzlich eine **automatische Ausführung der Aktualisierung** nach Freigabe. In diesem Fall ermittelt der Konnektor zur Verfügung stehende Aktualisierungen und startet selbsttätig den Aktualisierungsvorgang für die Konnektor- und Kartenterminalsoftware.

 Die automatische Aktualisierung (Auto-Update) ist standardmäßig aktiviert. Sie erfolgt standardmäßig mittwochs 1:00 Uhr.

Alternativ sind Updates für das lokale Hochladen in die KoCoBox MED+ bei Ihrem Servicepartner oder dem jeweiligen Hersteller der Software verfügbar, wie z.B. für die KoCoBox MED+ unter der Internet-URL (siehe weiter unten in diesem Kapitel). Sie werden dann als einzelne Dateien über den Bereich Aktualisierung direkt von einem lokalen Verzeichnis eingespielt und für die Aktualisierung des betreffenden Geräts aktiviert.



Die Verbindung zum KSR-Dienst erfolgt über eine TLS-Verbindung. Die Onlinekommunikation zum KSR-Dienst ist möglich, sofern die entsprechende technische Infrastruktur zur Verfügung steht und zugehörige Updatepakete dort abgelegt sind.¹⁶⁶

Softwareaktualisierung

Internet-URL für Firmware-Download: https://www.kococonnector.com/kococonnector_downloads/downloads.de.jsp

Endpunkt für Firmware-Download: <https://download-ref.ksr.telematik-test:443/>

Endpunkt für Konfigurationsdaten-Download:

Verfügbare Aktualisierungen automatisch herunterladen: aktiviert nicht aktiviert

Automatische Updates ausführen: aktiviert nicht aktiviert

Konnektor-Aktualisierungen

| | Herstellerkennung | Produkt | installierte Firm | Firmware-Version | Hardware-Version | nach KT-Updates ausf | Ausführung geplant für | Zugehörigkeit |
|-------------------------------------|-------------------|---------|-------------------|------------------|------------------|----------------------|------------------------|---------------|
| <input checked="" type="checkbox"/> | KOCOC | kocobox | 5.5.3 | 5.1.10 | 4.0.0 | Nein | | OPB |

Kartenterminal-Aktualisierungen

10 | Seite 1 von 1

1 bis 1 von 1 Datensätzen

| <input type="checkbox"/> | Kartente | Herstellerkennung | Produktken | installierte Firmware-Versi | Firmware-Versi | Hardware-Version | Ausführung geplant für | Zugehörigkeit |
|-------------------------------------|-----------|-------------------|------------|-----------------------------|----------------|------------------|------------------------|---------------|
| <input checked="" type="checkbox"/> | CT_ID_000 | INGHC | ORGA6100 | 3.8.2 | 3.8.2 | 1.2.0 | | OPB |

Aktualisierungen planen

Abbildung 110: Durchführung von Softwareaktualisierungen



Bitte beachten Sie folgende Sicherheitshinweise:

- Bitte aktivieren Sie nur dann ein Software-Update, wenn Sie **ausreichend Informationen** über dessen Inhalt erhalten haben. Dies soll Ihnen eine bewusste Entscheidung bei der Freischaltung ermöglichen. Bitte nutzen Sie hierzu auch die im weiteren Verlauf des Kapitels beschriebenen Updateinformationen.

¹⁶⁶ Auch wenn dort keine Updatepakete bereitstehen, ist eine Verbindung möglich. Voraussetzung ist eine VPN-Verbindung in die TI. Das Ergebnis der Prüfung ist dann negativ.

- Es darf nur eine **freigegebene, offiziell verfügbare, signierte** Software installiert werden.¹⁶⁷ Der Konnektor prüft, ob die Software aufgespielt werden darf.
- Bereitgestellte Software-Updates für die KoCoBox MED+ sind **zeitnah einzuspielen**, um stets die aktuellsten Versionen der Sicherheitstechnologien zu verwenden.
- Software-Updates können eine Behebung von zwischenzeitlich entdeckten Sicherheitsproblemen beinhalten. Diese sind durch eine FWPriority = KRITISCH gekennzeichnet. Bei derartigen Updates wird **dringend** zur Installation geraten. Bei verzögertem oder ausgelassenem Update setzt der Betreiber sein Praxisnetz einem erhöhtem Sicherheitsrisiko aus.



Über die *Internet-URL*

https://www.kococonnector.com/kococonnector_downloads/downloads.de.jsp
(statische Angabe) steht der Firmware-Download zur Verfügung.

In den Zeilen *Endpunkt für Firmware-Download* bzw. *Endpunkt für Konfigurationsdaten-Download* stehen die Endpunkte des Konfigurationsdienstes zum Download der Firmware bzw. der Konfigurationsdaten. Diese werden automatisch im Rahmen des VPN-Verbindungsaufbaus zur TI ermittelt.

Bei der Option *Verfügbare Aktualisierungen automatisch herunterladen* ruft der Konnektor auf dem KSR bereitgestellte Update-Pakete ab. Bei Firmware-Updates, die den Konnektor selbst betreffen, lädt er dasjenige mit der höchsten Firmware-Version herunter. Per Voreinstellung ist diese Option aktiviert.

Über die Option *Automatische Updates ausführen* wird die automatische Softwareaktualisierung für den Konnektor und alle angeschlossenen Kartenterminals generell mittels Radiobutton aktiviert bzw. nicht aktiviert.

Durch die Option *Automatische Konnektor Updates ausführen* wird mittels Radiobutton die automatische Firmwareaktualisierung des Konnektors aktiviert. Hier ist zu entscheiden, ob das Update auch automatisch durchgeführt werden soll. Sofern dies nicht der Fall ist, kann dies per Radiobutton nicht aktiviert konfiguriert werden.

Mit der Option *Auswahl von Erprobungsaktualisierungen* wird festgelegt, ob Erprobungs-Update-Pakete angezeigt werden oder nicht. Per Voreinstellung ist dies nicht aktiviert. Sobald der Button aktiviert wird, erscheint ein Warnhinweis, dass die Installation von Erprobungs-Update-Paketen nur für Teilnehmer der Erprobung vorgesehen ist.

Mittels Übernehmen speichern Sie die Einstellungen ab.

¹⁶⁷ Die Firmware-Versionen werden von der gematik GmbH (www.gematik.de) zugelassen, zertifiziert und bestätigt. Die zugehörigen Bestätigungen zur qualifizierten elektronischen Signatur (QES) sowie die Sicherheitszertifizierung nach Common Criteria sind unter www.bundesnetzagentur.de und unter www.bsi.bund.de hinterlegt.



Sofern innerhalb eines kürzeren Zeitraums geprüft werden soll, ob Update-Pakete auf dem KSR zur Verfügung stehen, kann diese Information über den Button Update-Informationen ermitteln abgefragt werden.



Für die Abfrage aktueller Konfigurationsdaten der Bestandsnetze steht der Button Infrastrukturkonfiguration aktualisieren zur Verfügung.¹⁶⁸

Die automatische Aktualisierung wird über den Button Automatisches Update konfigurieren geplant. In einem neuen Konfigurationsfenster können Sie die konkrete Ausführung einstellen.

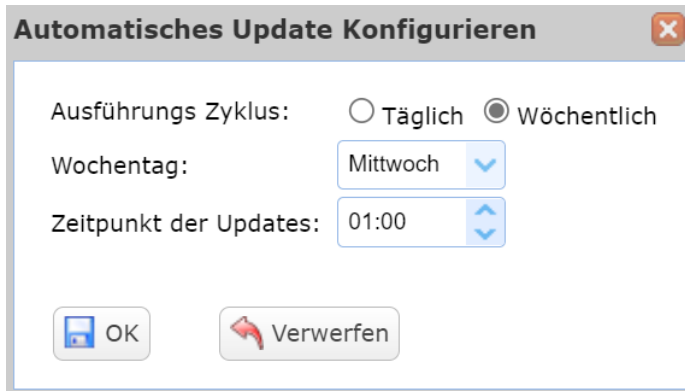


Abbildung 111: Konfiguration des automatischen Updates

Über die beide Radiobuttons täglich bzw. wöchentlich legen Sie den *Ausführungszyklus* für das automatische Update fest. Der *Wochentag* sowie der genaue *Zeitpunkt des Updates* können mittels einer Auswahlliste definiert werden.

Über den Button OK bestätigen Sie die Eingaben.

Aktualisierung Konnektor


Die Tabelle *Konnektor-Aktualisierungen* zeigt die vorhandenen Firmware-Updates für die KoCoBox MED+ an und informiert über *Herstellerkennung*, *Produktkennung*, *installierte Firmware-Version*, *Firmware-Version*, *Hardware-Version*, ob die Aktualisierung *nach KT-Updates* ausgeführt werden soll, zu welchem *Ausführungszeitpunkt* man die Konnektor-Aktualisierung plant und welcher Phase das Update zuzuordnen ist (*Zugehörigkeit*).

Der Anwender des Konnektors kann über eine vorgenommene Softwareaktualisierung durch das verwendete Clientsystem automatisch informiert werden. Hierfür sind vor der Aktualisierung der KoCoBox MED+ durch das Clientsystem die Ereignisse KSR/UPDATE/START, KSR/UPDATE/SUCCESS, KSR/UPDATE/END und KSR/UPDATE/ERROR des Systeminformationsdienstes zu abonnieren. Das Clientsystem erhält dann im Zuge der Softwareaktualisierung die entsprechende Benachrichtigung mit der Version der Konnektor-Software. Nach einer erfolgreichen Softwareaktualisierung ist die neue Version auch durch einen berechtigten Benutzer auf der Statusseite (siehe Kapitel Status) sowie direkt im Display der KoCoBox MED+ über Versionen ablesbar.



¹⁶⁸ Anzeige der Liste im Bereich LAN/WAN; Informationen zu Bestandsnetzen werden automatisch in den Konnektor übernommen; Netze können in der Tabelle *Aktive Bestandsnetze* aktiviert werden; Beachten Sie, dass nach einer Aktualisierung der Liste der Bestandsnetze diese standardmäßig aktiviert werden.



Details zum ausgewählten Update können in der Tabelle per Klick  auf  in der jeweiligen Zeile eingesehen werden.

Dazu öffnet sich das Anzeigefenster *Elemente der Updateinformation*.

Elemente der Updateinformation

UpdateID: 40096dc9b114a5d86fc16639_OPB
 ProductVendorID: KOCOC
 ProductCode: kocobox
 HWVersion: 4.0.0
 ProductName: KoCoBox MED+
 CreationDate: 09.10.2023 00:00:00
 DeploymentInformation - StartDate:
 DeploymentInformation - Deadline: 15.11.2024 00:00:00
 FWVersion: 5.1.10
 FWPriority: KRITISCH
 Dateien sind bereits heruntergeladen. Dateien vom KSR laden

| Firmwaredateien | |
|--|---------------------------------|
| Dateiname | Notes |
| /KOCOC/kocobox/40096dc9b114a5d86fc16639_OPB/filesystemupdate_5.1.10_1.fu | Firmwarefile der Version 5.1.10 |

| Dokumentationsdateien | |
|--|---|
| Dateiname | Notes |
| /KOCOC/kocobox/40096dc9b114a5d86fc16639_OPB/KoCoBox-ReleaseNotes-5.1.10-2023-10-06.pdf | Dokumentationsdatei: KoCoBox-ReleaseNotes-5.1.10-2023-10-06.pdf |

Firmware Releasenotes
 Alternativer Downloadpunkt: https://www.kococonnector.com/kococonnector_downloads/downloads.de.jsp ; Zusätzlicher Hinweis: Mit dieser Version wird erstmalig die Funktion des automatischen Softwareupdates aktiv, sobald die Einstellungen "Automatische Updates ausführen" und "Automatische Konnektor Updates zulassen" im Bereich "Aktualisierung" auf "aktiviert" gestellt sind. ; Falls eine TSL-Aktualisierung innerhalb der TI fehlschlägt, versucht der Konnektor automatisch eine TSL-Aktualisierung aus dem Internet von der TSL-Backup-Downloadadresse bzw. der TSL-Backup-IP-Adresse.

Firmware Group Releasenotes
 Die Firmware Gruppe enthält die Firmwareversionen 5.1.10 und 5.1.11.

Abbildung 112: Detailanzeige zum Firmware-Update für den Konnektor

Über den Button Dateien vom KSR laden werden die Firmware-Updates für den Konnektor – nach Bestätigung mit OK – vom KSR-Server heruntergeladen.

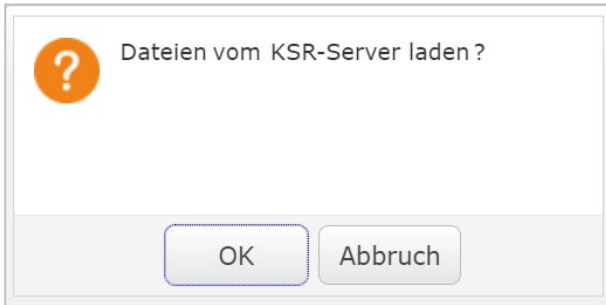


Abbildung 113: Dialogfenster zur Bestätigung des KSR-Downloads

Nach Abschluss dieses Downloads können die Firmware-Updates über den Button Aktualisierung planen (unten im Anzeigebereich) dann direkt installiert werden.

Bei einer wiederholten Anforderung zum Herunterladen von Updatedaten vom KSR erscheint ein Dialogfenster mit dem Hinweis, dass die Dateien schon heruntergeladen wurden.

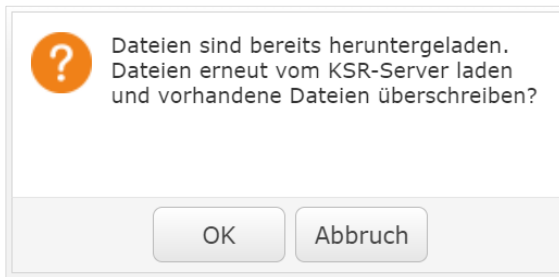


Abbildung 114: Dialogfenster mit Hinweis zum erneuten KSR-Download

Das **manuelle** Hochladen von Update-Paketen für den Konnektor verläuft wie folgt:

1 Über den Button Konnektor Dateien importieren laden Sie aus einem lokalen Verzeichnis zuerst die Update-Pakete in den Secure Storage (Datenspeicher) des Konnektors.¹⁶⁹ Diese müssen eine Zip-Datei enthalten, in der sich die UpdateInfo.xml¹⁷⁰ sowie die Firmware-Datei befinden. Der Bitte-Warten-Balken zeigt die Dauer des Importvorgangs an.



Währenddessen darf **kein** anderer Bereich der Managementschnittstelle aufgerufen werden, da der Uploadvorgang sonst abbricht.

2 Bestätigen Sie das Dialogfenster mit dem Hinweis zum Ende des Imports.

¹⁶⁹ Dies nimmt je nach Größe der Zip-Datei einige Zeit in Anspruch, was der *Bitte-Warten*-Balken visualisiert.

¹⁷⁰ Die UpdateInfo.xml muss ebenfalls durch den Hersteller signiert sein. Diese Signatur muss vor dem Beginn des Update-Prozesses vom Konnektor erfolgreich verifiziert worden sein.

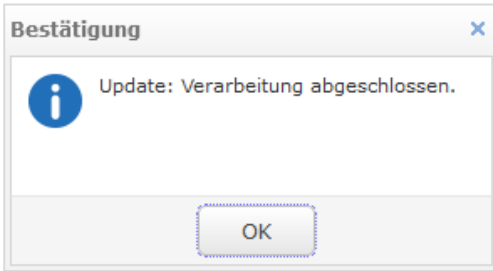



Abbildung 115: Dialogfenster mit Information zum Ende des Update-Imports

- 3** Anschließend laden Sie die Signaturdatei des Zip-Archivs (Sig-Datei) hoch.
 - 4** Nach diesem Import überprüft der Konnektor, ob die Signatur der Zip-Datei gültig ist. Erst dann entpackt er die Daten in seinen Datenspeicher.
 - 5** Sobald dies erfolgreich durchgeführt wurde, wird Ihnen die Aktualisierung in der Tabelle angezeigt und Sie können den Updateprozess starten.
-  Wir empfehlen, vor einer Aktualisierung der Konnektor-Firmware die aktuellen Protokolldateien herunterzuladen und im Konnektor zu löschen (das Sicherheitsprotokoll kann nicht gelöscht werden).

Um die Update-Installation auszulösen (unabhängig von der Art des Uploads) gehen Sie wie folgt vor:

- 1** Haken Sie in der Tabelle das gewünschte Update an.
- 2** Starten Sie mittels Button Aktualisierungen planen die Installation des Updates, ohne einen Ausführungszeitpunkt anzugeben.

Anschließend visualisiert ein *Bitte-Warten*-Balken die interne Übergabe an den Konnektor zur Ausführung der Aktualisierung. Diese findet dann im Hintergrund statt.



Abbildung 116: Bitte-Warten-Balken

- 3** Nach einem erfolgreichen Firmware-Update führt der Konnektor automatisch einen Neustart durch, der ein paar Minuten in Anspruch nimmt...¹⁷¹

¹⁷¹ Die Managementschnittstelle meldet den erfolgreichen Neustart des Konnektors nicht. Auf dem Display der KoCoBox MED+ wird der Neustart-Vorgang angezeigt. Sobald er abgeschlossen ist, erscheint die Standard-Anzeige. Über seine IP-Adresse (<https://<IP-KON>:9443/administration/start.htm>) ist der Konnektor wieder erreichbar. Hinweis: Eventuell wird Ihnen durch Ihren Browser eine andere, ähnliche URL angeboten. Diese muss dann manuell auf die anfangs auf dem Display angezeigte Startadresse korrigiert werden.

4

Sobald die Standard-Displayansicht auf der KoCoBox MED+ erscheint, können Sie in die Browser-Zeile die IP-Adresse der Managementschnittstelle eintragen, um das Login-Fenster aufzurufen.¹⁷² Melden Sie sich mit Ihrer Benutzerkennung (Name) und Ihrem persönlichen Passwort wieder an.



Sobald auf der Status-Seite der Managementschnittstelle in der Tabelle Betriebszustandsmeldungen die Fehlerzustandsmeldung *EC_Connector_Software_Out_Of_Date* erscheint, sollten Sie eine Softwareaktualisierung durchführen.



Schlägt die Aktualisierung der Konnektor-Firmware fehl, so erscheint eine qualifizierte Fehlermeldung. Die Firmware-Version ändert sich nicht, die Konfigurationen bleiben erhalten.

Tritt während der Softwareaktualisierung ein Spannungsausfall an der KoCoBox MED+ ein, dann kann dieser Vorgang nicht erfolgreich zu Ende geführt werden, und es kann auch keine Fehlermeldung gegeben werden. In diesem Fall steht die KoCoBox MED+ für die Dauer des Ausfalls nicht zur Verfügung und startet bei wieder anstehender Versorgungsspannung mit der Vorgängerversion der Software.



Der Administrator sollte hierzu anhand der Statusseite (siehe Kapitel Status) überprüfen, ob dies korrekt nachvollziehbar ist und die Nichtverfügbarkeit der KoCoBox MED+ auf den Spannungsausfall und nicht auf einen anders bedingten Neustart zurückzuführen ist. Wenden Sie sich im Zweifelsfall an Ihren Servicepartner.



Nach einem Firmware-Update des Konnektors sollten Sie eine **zuvor exportierte Konnektorkonfiguration erneuern**, um potenzielle Versionsprobleme beim späteren Einlesen einer Konfiguration zu vermeiden. Beachten Sie hierzu die Vorgehensweise im Abschnitt Verwaltung / Ex-/ Import.

Aktualisierung Kartenterminal



Generell unterscheidet sich das Updateverfahren für das Kartenterminal von demjenigen für den Konnektor, da der Aktualisierungsprozess autark am Kartenterminal erfolgt.

Die Tabelle *Kartenterminal-Aktualisierungen* zeigt die vorhandenen Firmware-Updates für die von der KoCoBox MED+ gemanagten Kartenterminals an, die mindestens den Status *zugewiesen* besitzen.

Zu diesen werden Details zur *Kartenterminal-ID*, zur *Herstellerkennung*, zur *Produktkennung*, zur *installierten Firmware-Version*, zur *Firmware-Version*, zur *Hardware-Version*, zum *Ausführungszeitpunkt* (zu dem man die Kartenterminal-Aktualisierung plant), sowie zu welcher Phase das Update zuzuordnen ist (Zugehörigkeit) dargestellt.




Der Konnektor prüft im Zuge dieser Funktion **nicht** die Integrität von Update-Information und tatsächlichen Update-Daten. Der administrative Anwender ist für die Korrektheit des Updates verantwortlich. **Prüfen** Sie also, ob die Angaben in der Datei *KT-UpdateInfo.xml* den tatsächlichen Daten im Updatepaket für das Kartenterminal in Dateistruktur und -version entsprechen.



Über den Button Gruppieren kann man die Liste der Kartenterminals nach Kartenterminalmodellen anordnen.

¹⁷² Siehe auch den Abschnitt Vorbereitungen

Details zum ausgewählten Update können in der Tabelle per Klick auf  in der jeweiligen Zeile eingesehen werden. Dazu öffnet sich das entsprechende Anzeigefenster.

Elemente der Updateinformation

UpdateID: **V03080201020001322051703_OPB**

ProductVendorID: **INGHC**

ProductCode: **ORGA6100**

HWVersion: **1.2.0**

ProductName: **ORGA 6141 online**

CreationDate: **17.05.2022 00:00:00**

DeploymentInformation - StartDate: **17.05.2022 00:00:00**

DeploymentInformation - Deadline: **17.05.2024 00:00:00**

FWVersion: **3.8.2**

FWPriority: **NORMAL**

Dateien sind bereits heruntergeladen.

Firmwaredateien

| Dateiname | Notes |
|--|-------|
| /INGHC/ORGA6100/V03080201020001322051703_OPB/ORGA6141_V382220517.dfu | 3.8.2 |

Dokumentationsdateien

| Dateiname | Notes |
|--|-------|
| /INGHC/ORGA6100/V03080201020001322051703_OPB/ORGA6141_V382220517.txt | 3.8.2 |

Firmware Releasenotes

ReadMe for ORGA 6141 V3.8.2

Firmware Group Releasenotes

Release Notes ORGA6141 V3.8.2

Abbildung 117: Detailanzeige zum Software-Update für das Kartenterminal

Über den Button **Dateien vom KSR laden** werden die Update-Dateien für das Kartenterminal vom KSR-Server heruntergeladen.



Wichtig ist, dass das Administratorpasswort für die Admin-SICCT-Session zum Kartenterminal im Kartenterminaldienst hinterlegt sind. Anderenfalls schlägt das Update fehl.

Um die Installation anzustoßen, gehen Sie wie folgt vor:

1

Über den Button *KT-Updateinfo.xml importieren* laden Sie eine gültige *UpdateInfo.xml*-Datei aus einem lokalen Verzeichnis auf den Konnektor hoch.

2

Anschließend laden Sie aus einem lokalen Verzeichnis die vom Hersteller des Geräts vorgesehene Firmware-Datei hoch. Dies erfolgt über den Button *KT-Firmware importieren*. Nach Ende des Hochladens erscheint eine Bestätigungsmeldung, danach wird diese Kartenterminal-Aktualisierung in der Tabelle angezeigt.

3

Setzen Sie das Häkchen in der Tabelle für das zu aktualisierende Kartenterminal. Über die Schaltfläche *Aktualisierung planen* können Sie den Updateprozess unmittelbar (ohne einen Ausführungszeitpunkt konfiguriert zu haben) starten, indem Sie die Rückfrage im Dialogfenster bestätigen. Die Übergabe zur Ausführung wird mittels *Bitte-Warten*-Balken visualisiert. Die Installation selbst verläuft dann im Hintergrund.

4

Nach dem erfolgreichen Firmware-Update des Kartenterminals startet dieses neu.



Sobald auf dem Display oder in der Tabelle Betriebszustandsmeldungen der Status-Seite auf der Managementschnittstelle die Meldung *Operational State Error EC_CardTerminal_Software_Out_Of_Date (\$ctid)* erscheint, sollten Sie eine Softwareaktualisierung durchführen.

Aktualisierungen planen/ermitteln



Ein Klick auf die Spaltenbeschriftung *Ausführungszeitpunkt* ermöglicht es in beiden Tabellen, jeweilige Aktualisierungen zu planen, sofern man sie **nicht unmittelbar** ausführen möchte. Die gerade bearbeitete Tabellenzeile ist in beiden Tabellen leicht farbig unterlegt.

Softwareaktualisierung

Internet-URL für Firmware-Download: https://www.kococonnector.com/kococonnector_downloads/downloads.de.jsp

Endpunkt für Firmware-Download: <https://download-ref.ksr.telematik-test:443/>

Endpunkt für Konfigurationsdaten-Download:

Verfügbare Aktualisierungen automatisch herunterladen: aktiviert nicht aktiviert

Automatische Updates ausführen: aktiviert nicht aktiviert

Automatische Konnektor Updates zulassen: aktiviert nicht aktiviert

Konnektor-Aktualisierungen

| | Herstellereerkennung | Produktkennung | installierte Firmwa | Firmware-Versi | Hardware-Versi | nach KT-Upda | Ausführung geplant für | Zugehörigkeit |
|--------------------------|----------------------|----------------|---------------------|----------------|----------------|--------------|------------------------|---------------|
| <input type="checkbox"/> | KOCOC | kocobox | 5.5.3 | 5.1.10 | 4.0.0 | Nein | 22.11.2023 08:28 | OPB |

Kartenterminal-Aktualisierungen

10 | Seite 1 von 1

| <input type="checkbox"/> | Kartenterminal-ID | Herstellereerkennung | Produktkennung | installierte Firmware-Version | Firmware-Versi |
|--------------------------|-------------------|----------------------|----------------|-------------------------------|----------------|
| <input type="checkbox"/> | CT_ID_0000 | INGHC | ORGA6100 | 3.8.2 | 3.8.2 |

Aktualisierungen planen

Abbildung 118: Planung von Softwareaktualisierungen


Das Aktualisierungsdatum können Sie jeweils per Klick in das Feld *Aktualisierungszeitpunkt* mittels Monatskalender und Uhrzeitfeld auswählen und per OK bestätigen.



Sofern die Konnektor-Aktualisierung **nach** einer Kartenterminal-Aktualisierung erfolgen soll, können Sie dies per Klick auf das jeweilige Feld in der Spalte *nach KT-Updates ausführen* definieren: Setzen Sie dort das Warten-Häkchen.





Allgemein können Sie Aktualisierungen für den Konnektor und verbundene Kartenterminals gemeinsam ausführen lassen. Dies geschieht dann im Hintergrund.

 Beachten Sie dafür Folgendes:

Sind Kartenterminal-Updates für die Zukunft geplant und soll die Konnektor-Aktualisierung sofort ausgeführt werden und

- ist das Warten-Häkchen gesetzt, wird nichts unmittelbar ausgeführt: das Konnektor-Update wartet, bis die Kartenterminal-Updates durchgeführt wurden.
- ist das Warten-Häkchen nicht gesetzt, wird das Konnektor-Update unmittelbar ausgeführt und die Kartenterminal-Updates erst zum definierten Zeitpunkt.

 Für das erfolgreiche Durchführen des Firmware-Updates eines Kartenterminals muss das Administratorpasswort für jedes zu aktualisierende Kartenterminal für eine Admin-SICCT-Session zum Kartenterminal im Kartenterminaldienst hinterlegt sein.

 Es können zeitgleich maximal fünf Firmware-Updates für Kartenterminals ausgeführt werden.

Sie speichern Ihre Aktualisierungsplanung ab, indem Sie per Klick auf den unteren Button Aktualisierungen planen das Dialogfenster öffnen und diese darin per OK bestätigen.

Das Update wird dann automatisch zu diesem festgesetzten Zeitpunkt durchgeführt.

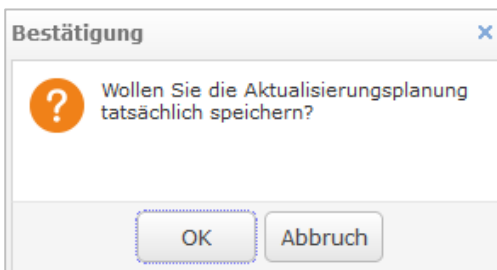



Abbildung 119: Planung für Software-Aktualisierungen bestätigen

 Für eine sofortigen Aktualisierung darf – wie oben schon erwähnt – kein Zeitpunkt definiert sein. Das Update kann dann direkt per Klick auf den Button Aktualisierung planen begonnen werden.

Übersicht

Der Unterbereich *Übersicht* gibt einen Überblick über den Status der Aktualisierungen für den Konnektor und die Kartenterminals.

Die Tabelle zeigt für Konnektor bzw. Kartenterminal(s) die interne *Update-ID*, die *Herstellerkennung*, die *Produktkennung*, die *Version*, den *Ausführungszeitpunkt* des Updates, den *Status* (als beschrifteter Verlaufs Balken), den *Bearbeitungsfehler* (als Code) sowie eine *Information*.

Die Übersicht erneuert sich – inklusive des Status der Aktualisierungen – automatisch alle 1.000 Millisekunden.

Übersicht und Status der Aktualisierungen

Aktualisierungen seit dem letzten Neustart des Konnektors

| Update-ID | Herstellerkennung | Produktkennung | Version | Ausführungszeitpunkt | Status | Bearbeitungsfehler | Information |
|-----------|-------------------|----------------|---------|-------------------------------|-----------------------|--------------------|-------------|
| 1 | KOCOC | kocobox | 5.0.6 | Tue Jun 28 09:02:15 CEST 2022 | Update ist geplant... | | |

Übersicht und Status der Aktualisierungen

Aktualisierungen seit dem letzten Neustart des Konnektors

| Update-ID | Herstellerkennung | Produktkennung | Version | Ausführungszeitpunkt | Status | Bearbeitungsfehler | Information |
|-----------|-------------------|----------------|---------|-------------------------------|------------------------------|--------------------|-------------|
| 1 | KOCOC | kocobox | 5.0.6 | Tue Jun 28 09:02:57 CEST 2022 | Prüfe Integrität Firmware... | | |

Abbildung 120: Beispielhafte Statusanzeigen zum Konnektor-Update im Zeitverlauf

Übersicht und Status der Aktualisierungen

Aktualisierungen seit dem letzten Neustart des Konnektors

| Update-ID | Herstellerkennung | Produktkennung | Version | Ausführungszeitpunkt | Status | Bearbeitungsfehler | Information |
|-----------|-------------------|----------------|---------|-------------------------------|--------|--------------------|-------------|
| 1 | KOCOC | kocobox | 4.2.22 | Tue Jul 05 15:46:58 CEST 2022 | Fehler | 4185 | |

Abbildung 121: Fehleranzeige für Konnektor-Update

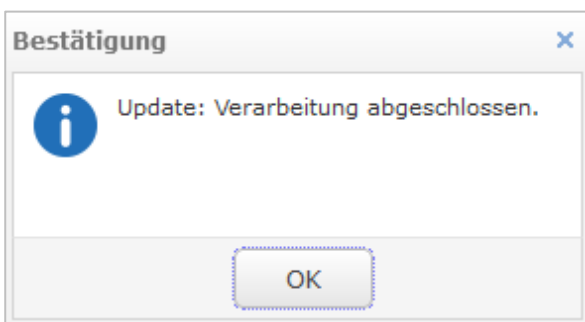


Abbildung 122: Meldung zum Abschluss der Update-Verarbeitung

Mein Profil

Durch Klick auf den Link [mein Profil](#) rechts in der Informationsleiste der Managementschnittstelle gelangt man zum Überblick über die Benutzerdaten des aktuell eingeloggten Administrators.



The screenshot shows a dialog box titled "Benutzer bearbeiten" with a close button (X) in the top right corner. The dialog contains the following information:

| | |
|---|---|
| Name: | koco-root |
| Zeitpunkt der letzten Anmeldung: | Nov 24, 2023, 11:12:23 AM |
| Zeitpunkt der letzten Passwortänderung: | May 25, 2023, 10:46:39 AM |
| Kontaktdaten: | KoCo Connector GmbH, Dessauer Str. 28-26, 10963 Berlin info@kococonnector.com Tel.: +49 (0) 30-24 64 90-0 |

At the bottom of the dialog, there are three buttons: "Passwort ändern", "OK", and "Schließen".

Abbildung 123: Mein Profil für Administrator-Benutzer mit Passwort ändern-Button

Es werden der *Name* des eingeloggten Administrators, der *Zeitpunkt des letzten Logins* sowie der *Zeitpunkt der letzten Passwortänderung* angezeigt.

Im Freitextfeld *Kontaktdaten* können die entsprechenden Informationen hinterlegt werden.



Über den Button [Passwort ändern](#) gelangt man in ein Konfigurationsfenster, in dem man das persönliche Passwort neu vergeben kann..¹⁷³



Beachten Sie bei der Neuvergabe des persönlichen Passworts die Sicherheitshinweise zur Passwortvergabe.

¹⁷³ Siehe dazu die Ausführungen im Abschnitt [Administrator-Passwort](#)

7.6.4 Werksreset

Generell können Sie über den Werksreset das Gerät in den Auslieferungszustand zurücksetzen. Dies kann zum einen über die Managementschnittstelle sowie – in besonderen Situationen (z.B. Passwort unbekannt) – per herstellerspezifischem Werksreset erfolgen. Letzterer wird in diesem Kapitel gesondert beschrieben.

Im Allgemeinen ist zum Werksreset Folgendes zu beachten:



Alle zwischenzeitlich vorgenommenen Konfigurationen (sowie System- und Performanceprotokoll) werden sicher gelöscht bzw. durch die Werte bei Auslieferung ersetzt. Der aktuelle Vertrauensraum, das Sicherheitsprotokoll sowie die aktuell installierte Firmware bleiben erhalten.



Um die komplette Neukonfiguration des Konnektors zu vermeiden, können Sie **vor** dem Werksreset einen Export der Konfigurationsdaten durchführen – und diese danach wieder importieren.¹⁷⁴



Ein Werksreset ist technisch ohne die vorherige Deregistrierung des Konnektors durchführbar. Eine nachträgliche Deregistrierung ist in einem solchen Fall nicht ohne weiteres möglich. Sofern Sie den Konnektor dann nach einem Werksreset erneut in Betrieb nehmen möchten, benötigen Sie Ihre Vertragsnummer (ContractID).

Werksreset per Managementschnittstelle

Gehen Sie zur Durchführung wie folgt vor:



Klicken Sie im Bereich *Verwaltung* auf den Button Werksreset. Es erscheint ein Dialogfenster mit der Sicherheitsabfrage, ob der Konnektor wirklich auf die Werkseinstellungen zurückgesetzt werden soll.



Bestätigen Sie diese Sicherheitsabfrage mit Ja. Die Ausführung nimmt nun einige Minuten in Anspruch. Dabei erscheinen nacheinander folgende Anzeigen:

- Führe Werksreset aus...
- Werksreset erfolgreich!

Mit dem Erscheinen der Anzeige `Werksreset erfolgreich!` fährt das Gerät herunter. Bei der KoCoBox MED+ (G4) erlischt das Display anstelle der Anzeige `Werksreset erfolgreich!`.



Trennen Sie den Konnektor nun für mindestens 10 Sekunden von der Stromversorgung.



Sollte die Anzeige `Werksreset fehlgeschlagen!` sichtbar werden, so war der Werksreset erfolglos. Führen Sie in einem solchen Fall den Werksreset erneut aus. Bei wiederholtem Fehlschlagen des Werksresets handelt es sich um einen Defekt. Der Konnektor ist dann an den Hersteller zurückzuführen.



Um bei einer **Außerbetriebnahme** des Konnektors (Entsorgung) sicherzustellen, dass keine neuen Protokolleinträge erzeugt bzw. gespeichert werden, darf der Konnektor nach dem Werksreset **nicht** erneut gestartet werden. Demzufolge muss die Stromversorgung unterbrochen bleiben (siehe oben Punkt 3).

¹⁷⁴ Siehe im Abschnitt Verwaltung / Ex-/Import

- 4** Schließen Sie die KoCoBox MED+ sodann (wieder) an die Stromversorgung an. Das Gerät startet neu, was einige Zeit in Anspruch nimmt.
- 5** Nach der Anmeldung an der Managementschnittstelle¹⁷⁵ ist die erneute initiale Konfiguration bzw. der Import der vorher exportierten Konfigurationsdaten erforderlich.
- 6** Registrieren Sie den Konnektor schließlich erneut beim Zugangsdienstprovider.¹⁷⁶

Herstellerspezifischer Werksreset

Für den Fall, dass Sie sich nicht mehr über die Managementschnittstelle auf der KoCoBox MED+ einloggen können, weil Sie beispielsweise Ihr Passwort vergessen haben, steht Ihnen der alternative **herstellerspezifische Werksreset** zur Verfügung.



Dafür benötigen Sie einen direkten physischen Zugang zum Konnektor.

Zur Durchführung eines herstellerspezifischen Werksresets gehen Sie wie folgt vor:

- 1** Über das Steuerungsmenü im Display des Konnektors gelangen Sie zum `Werksreset`. Dieser ist unter dem Menüpunkt `Status / Konfiguration` zu erreichen (siehe oben auch im Kapitel Menüstruktur). Bestätigen Sie den unterlegten Menüpunkt `Werksreset` mit dem Steuer-Button OK. Es erscheint eine Sicherheitsabfrage, ob der Werksreset ausgeführt werden soll.
- 2** Bestätigen Sie diese Sicherheitsabfrage mit Ja. Die Ausführung nimmt nun einige Minuten in Anspruch. Dabei erscheinen nacheinander folgende Anzeigen:

- `Führe Werksreset aus...`
- `Werksreset erfolgreich!`

Mit dem Erscheinen der Anzeige `Werksreset erfolgreich!` fährt das Gerät herunter.

Bei der KoCoBox MED+ (G4) erlischt das Display anstelle der Anzeige `Werksreset erfolgreich!`.

- 3** Trennen Sie den Konnektor nun für mindestens 10 Sekunden von der Stromversorgung.



Achten Sie darauf, dass die Anzeige `Werksreset erfolgreich!` ca. 60 Sekunden dauerhaft auf dem Display sichtbar bleibt. Nur in diesem Fall ist der Werksreset erfolgreich durchgeführt.



Sollte die Anzeige `Werksreset fehlgeschlagen!` sichtbar werden, so ist der Werksreset gescheitert. Führen Sie in einem solchen Fall den Werksreset erneut aus. Bei wiederholtem Fehlschlagen des Werksresets handelt es sich um einen Defekt. Der Konnektor ist dann an den Hersteller zurückzuführen.

¹⁷⁵ Siehe Abschnitt Administrator-Passwort: Der Konnektor ist durch Eingabe seiner IP-Adresse (`https://<IP-KON>:9443/administration/start.htm`) wieder erreichbar. Hinweis: Eventuell wird Ihnen durch Ihren Browser eine andere, ähnliche URL angeboten. Diese muss dann manuell auf die anfangs auf dem Display angezeigte Startadresse korrigiert werden.

¹⁷⁶ Siehe Abschnitt VPN / Registrierung



Um bei einer **Außerbetriebnahme** des Konnektors (Entsorgung) sicherzustellen, dass keine neuen Protokolleinträge erzeugt bzw. gespeichert werden, darf der Konnektor nach dem Werksreset **nicht** erneut gestartet werden. Demzufolge muss die Stromversorgung unterbrochen bleiben (siehe oben Punkt 3).

4

Schließen Sie die KoCoBox MED+ sodann (wieder) an die Stromversorgung an. Das Gerät startet neu, was einige Zeit in Anspruch nimmt.

5

Nach der Anmeldung an der Managementschnittstelle¹⁷⁷ ist die erneute initiale Konfiguration bzw. der Import der vorher exportierten Konfigurationsdaten erforderlich.

6

Registrieren Sie den Konnektor schließlich erneut beim Zugangsdienstprovider.¹⁷⁸

¹⁷⁷ Siehe Abschnitt Administrator-Passwort: Der Konnektor ist durch Eingabe seiner IP-Adresse (<https://<IP-KON>:9443/administration/start.htm>) wieder erreichbar. Hinweis: Eventuell wird Ihnen durch Ihren Browser eine andere, ähnliche URL angeboten. Diese muss dann manuell auf die anfangs auf dem Display angezeigte Startadresse korrigiert werden.

¹⁷⁸ Siehe Abschnitt VPN / Registrierung

7.7 Fachmodule

Im Folgenden werden die Fachmodule, die der Konnektor zur Verfügung stellt, dargestellt. Vorweg erfolgt eine Beschreibung der fachmodulspezifischen Sicherheitsmaßnahmen zu deren Betrieb..¹⁷⁹

7.7.1 Fachmodulspezifische Sicherheitsmaßnahmen

Zur Einführung der in den folgenden Abschnitten beschriebenen Fachmodule AMTS, ePA und NFDM wird beschrieben, wie diese sicher konfiguriert und genutzt werden.



Bitte lesen Sie diesen Abschnitt sorgfältig und beachten Sie die Sicherheitshinweise.



Generell gilt, dass für einen zertifizierten Betrieb des Fachmoduls AMTS, ePA bzw. NFDM ein Heilberufsausweis (HBA) mit **gültigem** Zertifikat genutzt werden muss. Für einen zertifizierten Betrieb des Fachmoduls ePA muss eine Praxiskarte (SMC-B) mit **gültigem** Zertifikat eingesetzt werden.



Ein HBA oder eine SMC-B mit abgelaufenem Zertifikat darf **nicht** eingesetzt werden. Es ist organisatorisch sicherzustellen, dass für einen zertifizierungsgerechten Betrieb jegliche Testkarten (HBA, SMC-B) **nicht** in der produktiven Umgebung zum Einsatz kommen.

Die KoCoBox MED+ stellt ein kompaktes und aufeinander abgestimmtes System aus Basiskonnektor und Fachmodulen zur Verfügung. Da alle Funktionsmodule innerhalb einer Software-Version zur Verfügung gestellt werden, ist die korrekte Nutzung der inneren Schnittstellen zwischen den Modulen optimal abgestimmt und sichergestellt..¹⁸⁰

Die Verwendung der äußeren Dienstschnittstellen der Fachmodule soll **ausschließlich** gemäß Definition in der gematik-Spezifikation (NFDM, ePA, AMTS) erfolgen. Die KoCoBox MED+ unterstützt die dort beschriebene schemakonforme Nutzung der Schnittstellen.



Eine nicht-konforme Nutzung der Dienstschnittstellen kann zu Fehlermeldungen und Einbußen in der Sicherheitsleistung der Fachmodule führen, ist daher unbedingt zu vermeiden.



Implementierungshinweis: Beachten Sie bei der Verwendung der Dienstschnittstellen, dass über alle Fachmodule der KoCoBox MED+ hinweg jegliche Identifikatoren (z.B. für die Registrierung beim Basiskonnektor) eindeutig, d.h. unique sein müssen. Nur so ist eine nachvollziehbare, sichere Zusammenarbeit zwischen Fachmodul und Basiskonnektor gegeben.

¹⁷⁹ Die folgenden Ausführungen betreffen nicht das Fachmodul VSDM, da es als Teil des Anwendungskonnektors implementiert ist und nicht denselben Restriktionen unterliegt wie die Fachmodule AMTS, ePA und NFDM.

¹⁸⁰ Die eingesetzten Software-Technologien gewährleisten, dass die Dienstschnittstellen korrekt angesprochen werden, kein Missbrauch an diesen Stellen unbemerkt erfolgen kann und die Trennung der Fachmodulfunktionen von den Basisdiensten des Konnektors konsequent verfügbar ist.



Implementierungshinweis: Beachten Sie, dass eine Signaturrechtlinie, die im Kontext des Fachmoduls verwendet wird (z.B. für das Fachmodul NFDm) vom Fachmodul als Objekt an den Basiskonnektor über die Dienstschnittstelle übergeben werden muss. Ansonsten können die Signaturfunktionen des Basiskonnektors **nicht sicher** verwendet werden.



Zur sicheren Konfiguration und Nutzung eines Fachmoduls sowie zur geschützten Betriebsumgebung gelten die Sicherheitsziele für den Einsatz des Konnektors, die oben in Kapitel 3 dieses Handbuchs beschrieben sind. Da die KoCoBox MED+ immer gemeinsam mit ihren Fachmodulen ausgeliefert wird, entsprechen die Sicherheitseigenschaften der Fachmodule denen des Konnektors.

Daher gelten für den gesicherten Betrieb der Fachmodule dieselben Maßnahmen, die der Konnektor zum Schutz der Daten und Umgebung grundsätzlich bereitstellt. Diese wurden im Rahmen der Zertifizierung nach Common Criteria geprüft. Hierzu nötige anwenderseitige Sicherheitsmaßnahmen sind in Kapitel 2 für den Konnektor insgesamt beschrieben.



Prüfen Sie bitte unmittelbar nach Inbetriebnahme des Konnektors und nach jedem Firmware-Update die Versionsnummer des Konnektors und die Version der jeweiligen Fachmodule. Nehmen Sie diese nur dann in Betrieb, wenn diese Angaben korrekt sind.¹⁸¹



Die Versionsnummer der KoCoBox MED+ Firmware finden Sie zum einen auf der Status-Seite der Managementschnittstelle rechts im Bereich *Produktinformationen*, zum anderen können Sie sie über das Display aufrufen (unter 4. Versionen).



Die Versionsnummer der Firmware **muss** mit der aus dem entsprechenden CC-Zertifikat übereinstimmen.

Die CC-Zertifikate stehen unter



https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/Zertifizierte-Produkte-nach-CC/zertifizierte-produkte-nach-cc_node.html

zur Verfügung oder können alternativ über die Hersteller-Webseite als Anfrage per Kontakt-E-Mail mit dem Betreff „Zertifizierung [KoCoBox MED+]“ angefordert werden.



Die Versionsnummer des jeweiligen Fachmoduls finden Sie auf der Managementschnittstelle im entsprechenden Konfigurationsbereich unter *Informationen/Versionen*.

Die Versionsnummer der Fachmodule **muss** mit der aus dem jeweiligen TR-Zertifikat übereinstimmen.

¹⁸¹ Die jeweils zugehörigen Versionsnummern können Sie unter <https://www.kococonnector.com> einsehen.

Die TR-Zertifikate stehen unter



https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-TR/Zertifizierte-Produkte-nach-TR/zertifizierte-produkte-nach-tr_node.html

zur Verfügung oder können alternativ über die Hersteller-Webseite als Anfrage per Kontakt-E-Mail mit dem Betreff „Zertifizierung [KoCoBox MED+]“ angefordert werden.

Die Bedienung des Fachmoduls erfolgt über das Clientsystem. Für diese Verbindung gelten dieselben Regeln und Einstellungen wie für die sonstige Kommunikation des Konnektors. Diese sind im Bereich *Verwaltung / Clientsysteme* konfigurierbar.



Wir empfehlen, dort die Voreinstellung für TLS-verschlüsselte Kommunikation beizubehalten.



Beim Abschalten dieses TLS-gesicherten Kanals erscheint ein Warnhinweis. In diesem müssen Sie als Administrator bestätigen, dass Sie über die mit der Abschaltung verbundenen Risiken informiert sind. In diesem Fall übernimmt der Endkunde die Verantwortung für die Sicherstellung der vertraulichen Übertragung.



Für jedes einzelne Fachmodul werden Ablauf- bzw. Performance- und Fehlerprotokolle erstellt. Diese können Sie bei Bedarf jeweils exportieren.



Treten sicherheitsrelevante Probleme auf, dann werden diese in das Sicherheitsprotokoll des Konnektors eingetragen.¹⁸² Entsprechende Einträge sind anhand der Tabelle im Kapitel Sicherheitsrelevante Fehlermeldungen der Fachmodule zu prüfen, da der weitere sichere Betrieb des Fachmoduls möglicherweise nicht mehr gewährleistet ist. Gegebenenfalls ist der Betrieb des Konnektors sofort einzustellen und der Support zu kontaktieren, um weitere Handlungsanweisungen zu erhalten.

7.7.2 Versichertenstammdatenmanagement (VSDM)

Das Fachmodul VSDM wird als integraler Bestandteil des Anwendungskonnektors als eine der dezentralen Komponenten der TI betrieben. Es unterstützt die Anwendungsfälle der Fachanwendung VSDM, indem es dem Clientsystem (i.d.R. PVS/KIS) anwendungsspezifische Schnittstellen zum Auslesen der Versichertenstammdaten der eGK anbietet.¹⁸³

Im Bereich *VSDM* (Versichertenstammdatenmanagement) wird dieses Fachmodul konfiguriert. In den Unterbereichen *Systemprotokoll*, *Performanceprotokoll* und *Fehlerprotokoll* stehen jeweils Listen aller Logeinträge für dieses Fachmodul zur Verfügung.

¹⁸² Dies ist im Kapitel Protokollierungsdienst beschrieben.

¹⁸³ Vgl. [gemSpec_FM_VSDM], S. 10

Fachmodul VSDM

Informationen

Version: 7.11.0

Fachmodul Konfiguration

Servicename Intermediär:
 Automatische Onlineprüfung: ein aus
 Timeout für Fachdienste:
 Maximale Bearbeitungszeit für ReadVSD:
 Maximale Offline-Dauer:

Zugriffsberechtigungsdaten für AutoUpdateVSD

Hier wird angegeben, mit welchen Kontext-Daten die Operation AutoUpdateVSD ausgeführt werden soll. Die eingetragenen IDs müssen im Infomodell hinterlegt sein.

Mandant-ID:
 Clientsystem-ID:
 Arbeitsplatz-ID:

Protokollierungskonfiguration

Log-Level: ▼
 Speicherdauer:
 Performancelogging: ein aus

Schlüssel für Prüfungsnachweise

| | Mandant | Zeichenfolge |
|--|---------------------|------------------|
| | 01 | A{4XJU.;Hy&\9,&! |
| | Mandant_ePA_Default | Py!)ha{MoSekXR?6 |

Abbildung 124: Konfigurationsbereich für das Fachmodul VSDM

Bei der Konfiguration des Fachmoduls VSDM gehen Sie wie folgt vor:

- 1** Tragen Sie in der ersten Zeile den *Servicenamen* des *Intermediär* ein.¹⁸⁴ Per Voreinstellung ist *_vsdmintermediaer._tcp* hinterlegt.
- 2** Schalten Sie per Radiobutton die *automatische Onlineprüfung* der VSD ein. Diese startet beim Stecken einer eGK. Per Voreinstellung ist die Onlineprüfung ausgeschaltet.¹⁸⁵
- 3** Definieren Sie bei Bedarf den *Timeout für Fachdienste* in Sekunden. Per Voreinstellung sind 10 Sekunden festgelegt.
- 4** Tragen Sie anschließend die maximale Bearbeitungszeit für die *Operation ReadVSD* ein. Die Voreinstellung beträgt hier 30 Sekunden.
- 5** Geben Sie in der Zeile *maximale Offline-Dauer* den mit dem Vertragspartner vereinbarten Zeitraum ein. 0 Sekunden bedeutet keine Prüfung auf den maximalen Offline-Zeitraum.

Im folgenden Abschnitt *Zugriffsberechtigungsdaten für AutoUpdateVSD* tragen Sie ein, mit welchen Kontext-Daten des Infomodells die Operation AutoUpdateVSD ausgeführt werden soll.



AutoUpdateVSD kann nur beim Standalone-Konnektor angewandt werden.



Die eingetragenen IDs müssen im Infomodell¹⁸⁶ hinterlegt sein.

Geben Sie in die Felder *Mandant-ID*, *Clientsystem-ID* und *Arbeitsplatz-ID* die für den automatischen Abgleich der VSD vorgesehenen jeweiligen IDs ein.



Diese müssen im Infomodell vorher entsprechend definiert worden sein.

Legen Sie anschließend die *Protokollierungskonfiguration* fest:

- 1** Dafür ist der *Log-Level* (Debug, Info, Warning, Error, Fatal) per Drop-down Menü zu definieren. Es gibt den Mindestschweregrad der zu speichernden Einträge im Fachmodulprotokoll an. Per Voreinstellung ist *Info* eingetragen.
- 2** Geben Sie die *Speicherdauer* in Tagen ein, bevor das VSDM-Fachmodul-Protokoll gelöscht wird. Die Voreinstellung ist 180 Tage.
- 3** Aktivieren Sie bei Bedarf das *Performancelogging* mittels Radiobutton ein. Per Voreinstellung ist es ausgeschaltet.

In der unteren Liste *Schlüssel für Prüfungsnachweise ...* sind die Mandanten aufgeführt, die im Infomodell definiert wurden.

Für jeden dieser Mandanten muss ein Schlüssel für Prüfungsnachweise erzeugt werden. Dieser dient der


¹⁸⁴ Der *Servicename Intermediär* setzt sich zusammen aus dem eigentlichen Servicenamen sowie dem zu verwendenden Protokolltyp. Dieser Punkt dient der Abfrage des Resource Records beim DNS-Service Discovery.

¹⁸⁵ Diese Funktion ist nur im Standalone-Szenario verfügbar.

¹⁸⁶ Siehe den Abschnitt Infomodell

Verschlüsselung des Prüfungsnachweises auf der eGK.

Gehen Sie dafür wie folgt vor:

- 1 Öffnen Sie per Klick auf das Schlüsselsymbol  das Konfigurationsfenster zum Anlegen eines Mandanten-Schlüssel-Paares zur Verschlüsselung des Prüfungsnachweises auf der eGK. Dies muss für Operationen *ReadVSD* und *AutoUpdateVSD* gesetzt sein, andernfalls können diese nicht erfolgreich abgeschlossen werden.

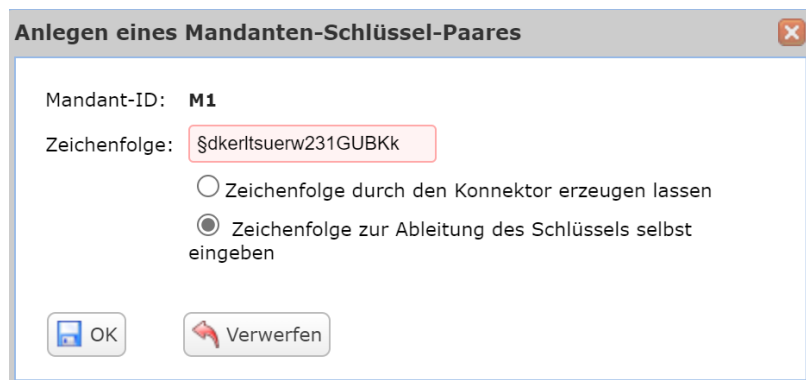


Abbildung 125: Konfigurationsfenster für das Anlegen eines Mandaten-Schlüssel-Paares

- 2 Wählen Sie aus, ob Sie die Zeichenfolge für die Ableitung des Schlüssels¹⁸⁷ durch den Konnektor erzeugen lassen oder selbst eingeben möchten. Beachten Sie bitte, dass die Zeichenfolge **exakt 16 Zeichen lang** sein muss. Für eine sichere Unterscheidung von erzeugten Prüfnachweisen wird empfohlen, die Zeichenfolge durch den Konnektor erzeugen zu lassen.
- 3 Sofern Sie mehrere Konnektorpaare (Offline- und Online-Konnektor) administrieren, stellen Sie sicher, dass **unterschiedliche Zeichen** für das Generieren des Schlüssels verwendet werden.
- 4 Bestätigen Sie die eingegebene Zeichenfolge mit OK.
- 5 Mit dem Button Übernehmen speichern Sie die Konfigurationen ab.

¹⁸⁷ 16 ASCII-Zeichen

Unterbereiche Systemprotokoll, Performanceprotokoll und Fehlerprotokoll

In den drei Unterbereichen findet man jeweils eine tabellarische Übersicht aller Logeinträge mit den folgenden Informationen

- Zeitpunkt,
- Schwere,
- Beschreibung,
- Parameter.

The screenshot shows the 'Systemprotokoll VSDM' interface. At the top, there is a navigation bar with 'Seite 1 von 3' and '1 bis 20 von 49 Datensätzen'. Below this is a table with four columns: 'Zeitpunkt', 'Schwere', 'Beschreibung', and 'Parameter'. The table contains 20 rows of log entries. Below the table, there is a 'Protokoll löschen' button. At the bottom, there is a 'Download' section with two input fields for 'Protokolleinträge von' (08.05.2017 10:00) and 'Protokolleinträge bis' (09.05.2017 17:30), and a 'Protokoll-Download' button.

| Zeitpunkt | Schwere | Beschreibung | Parameter |
|---------------------|---------|---------------------------------------|--|
| 27.04.2017 17:27:26 | INFO | FM_VSDM.ReadVSD.OfflineCheck.Update | Beschreibung=Ende |
| 27.04.2017 17:27:25 | INFO | FM_VSDM.ReadVSD.OfflineCheck.Update | Beschreibung=GVD lesen |
| 27.04.2017 17:27:25 | INFO | FM_VSDM.ReadVSD.OfflineCheck.Update | Beschreibung=PD lesen |
| 27.04.2017 17:27:25 | INFO | FM_VSDM.ReadVSD.OfflineCheck.Update | Beschreibung=VD lesen |
| 27.04.2017 17:27:25 | INFO | FM_VSDM.ReadVSD.OfflineCheck.Update | Beschreibung=VSDStatus lesen |
| 27.04.2017 17:27:24 | INFO | FM_VSDM.ReadVSD.OfflineCheck.Update | Beschreibung=AuditLog auf Karte schreiben |
| 27.04.2017 17:27:23 | INFO | FM_VSDM.ReadVSD.OfflineCheck.Update | Beschreibung=Prüfungsnachweis erzeugen |
| 27.04.2017 17:27:23 | INFO | FM_VSDM.ReadVSD.OfflineCheck.Update | Beschreibung=PINStatus SMB |
| 27.04.2017 17:27:23 | INFO | FM_VSDM.ReadVSD.OfflineCheck.Update | Beschreibung=C2C |
| 27.04.2017 17:27:23 | INFO | FM_VSDM.ReadVSD.OfflineCheck.Update | Beschreibung=Ende VSD Aktualisierung |
| 27.04.2017 17:27:20 | INFO | FM_VSDM.ReadVSD.OfflineCheck.Update | Beschreibung=VSD: GetNextCommandPackage |
| 27.04.2017 17:27:20 | INFO | FM_VSDM.ReadVSD.OfflineCheck.Update | Beschreibung=ResponseAPDU von Karte |
| 27.04.2017 17:27:20 | INFO | FM_VSDM.ReadVSD.OfflineCheck.Update | Beschreibung=CommandAPDU an Karte |
| 27.04.2017 17:27:20 | INFO | FM_VSDM.ReadVSD.OfflineCheck.Update | Beschreibung=Führe VSDDUpdate mit Endpunkt: 'https://intvsdm1-fd-lab.fra-lab-telemat.medintermediaer.telematik-lab:8443/vsdm/services/102171012/VSD/2.0/' aus. |
| 27.04.2017 17:27:20 | INFO | FM_VSDM.ReadVSD.OfflineCheck.Update | Beschreibung=Starte Update |
| 27.04.2017 17:27:19 | INFO | FM_VSDM.ReadVSD.OfflineCheck.NoUpdate | Beschreibung=Beginne VSD Aktualisierung |
| 27.04.2017 17:27:19 | INFO | FM_VSDM.ReadVSD | Beschreibung=UpdateFlag erhalten fuer: VSD [MANDATORY] |
| | | | Beschreibung=Suche nach CA Zertifikat mit Subject 'CN=C.CGM.KOMP-CA1' |

Abbildung 126: Exemplarische Ansicht zum Systemprotokoll VSDM mit Downloadfunktion

In allen drei Unterbereichen können Sie:

- über den Button Protokoll löschen die jeweiligen Einträge entfernen.
- im Bereich *Download* über *Protokolleinträge von* und *Protokolleinträge bis* per Kalenderfunktion definieren, für welchen Zeitraum Sie ein Protokoll herunterladen möchten.
- über den Button Protokoll-Download die Tabelleneinträge jeweils für den benannten Zeitraum herunterladen. Sofern Sie keinen Zeitraum definieren, wird das jeweilige Protokoll vollständig heruntergeladen.

Details zum Aufbau der Logfiles im Fachmodul VSDM

Im Folgenden werden die Logdateien für das Fachmodul VSDM konkret beschrieben. Dabei sind die Parameter über alle drei Logdateien hinweg gleich.

- Systemprotokoll: Hier befindet sich das Ablaufprotokoll der verarbeitenden Funktionen.
- Performanceprotokoll: In diesem Protokoll werden Performanceangaben zu Konnektor-Operationen dokumentiert.
- Fehlerprotokoll: In diesem Protokoll werden eventuelle, bei der Verwendung des Konnektors aufgetretene Fehler dokumentiert.

| Kennung in der Logdatei | Beschreibung |
|-------------------------|--|
| Logrefid | eindeutige Referenz des Logeintrages im Konnektor |
| Timestamp | Zeitstempel des Logeintrages |
| Module | Bezeichnung des betroffenen Konnektormoduls |
| Amount | Anzahl, wie oft die Meldung in diesem Logeintrag zusammengefasst ist. ¹⁸⁸ |
| Topic | Topic des protokollierten Ereignisses |
| protocolType | Protokollierungsart |
| protocolSeverity | Schweregrad des Protokollierungseintrages |
| Parameter | ereignisabhängige Parameter mit weiteren Details zum protokollierten Ereignis und Fehler |

Tabelle 4: Aufbau der Logfiles im Fachmodul VSDM

7.7.3 Arzneimitteltherapiesicherheit (AMTS)

Das Fachmodul Arzneimitteltherapiesicherheit (FM AMTS) ist eine Softwarekomponente. Sie setzt den E-Medikationsplan (eMP) als integralen Bestandteil des Konnektors um. Dabei nutzt es dessen Basisdienste zur Umsetzung aller Anwendungsfälle. Es stellt dem Konnektor Grundfunktionalitäten zur Verwaltung des E-Medikationsplans zur Verfügung, die durch das Primärsystem (Clientsystem in der Arztpraxis) genutzt werden.¹⁸⁹

Anwender rufen mittels ihres Clientsystems (AIS, PVS o.a.) das Fachmodul AMTS auf, um auf die eGK des Patienten zuzugreifen. Über ihre Rolle, die technisch durch das Zugriffsprofil ihrer Smartcard (HBA, SMC-B) repräsentiert wird, erhalten sie die benötigte Berechtigung zum Zugriff.¹⁹⁰

Im Bereich *Fachmodul AMTS* wird dieses konfiguriert. Im Unterbereich *Informationen* finden sich die Nummer der *Version* der Software sowie der konkrete *Build-Zeitpunkt* mit Datum und sekundengenaue

¹⁸⁸ Gleiche Logeinträge werden nach bestimmten, komplexen Regeln zusammengefasst.

¹⁸⁹ Vgl. [TR-03155], S. 6

¹⁹⁰ Vgl. [gemSpec_FM_AMTS], S.10

Uhrzeit.


Im Unterbereich *Protokollierungskonfiguration* werden der *Log-Level*, die *Speicherdauer* sowie das *Performancelogging* konfiguriert.

Fachmodul AMTS

Informationen



Version: 7.11.0
Build-Zeitpunkt: 15.11.2023, 10:18:19 UTC

Protokollierungskonfiguration

Log-Level: 

Speicherdauer:

Performancelogging: ein aus

 Übernehmen  Verwerfen

Download herstellerspezifischer Logs


 Protokoll-Download

Abbildung 127: Konfigurationsbereich für das Fachmodul AMTS

Legen Sie die *Protokollierungskonfiguration* wie folgt fest:

- 1 Zunächst ist der *Log-Level* (Debug, Info, Warning, Error, Fatal) per Drop-down Menü zu definieren. Es gibt den Mindestschweregrad der zu speichernden Einträge im Fachmodulprotokoll an. Per Voreinstellung erscheint *Warning*.
- 2 Geben Sie die *Speicherdauer* in Tagen ein, bevor das AMTS-Fachmodul-Protokoll gelöscht wird. Die Voreinstellung ist 180 Tage.
- 3 Aktivieren Sie bei Bedarf das *Performance logging* mittels Radiobutton ein. Per Voreinstellung ist es ausgeschaltet.

Unterbereiche Ablaufprotokoll, Performanceprotokoll und Fehlerprotokoll

In den drei Unterbereichen findet man jeweils eine tabellarische Übersicht aller Logeinträge mit den folgenden Informationen

- Zeitpunkt,
- Schwere,
- Beschreibung,
- Parameter.

| Zeitpunkt | Schwere | Beschreibung | Parameter |
|----------------------------|---------|------------------|---|
| 13.06.2022 10:32:05.927 | INFO | MGM/ADMINCHANGES | NewVal=true; User=koco-root; RefID=FM_AMTS_LOG_PERF |
| 13.06.2022 10:32:05.897 | INFO | MGM/ADMINCHANGES | NewVal=DEBUG; User=koco-root; RefID=FM_AMTS_LOG_LEVEL |

Protokoll löschen

Download

Protokolleinträge von:

Protokolleinträge bis:

Protokoll-Download

Abbildung 128: Exemplarische Ansicht zum Ablaufprotokoll AMTS mit Downloadfunktion

In allen drei Unterbereichen können Sie:

- über den Button *Protokoll löschen* die jeweiligen Einträge entfernen.
- im Bereich *Download* über *Protokolleinträge von* und *Protokolleinträge bis* per Kalenderfunktion definieren, für welchen Zeitraum Sie ein Protokoll herunterladen möchten.
- über den Button *Protokoll-Download* die Tabelleneinträge jeweils für den benannten Zeitraum herunterladen. Sofern Sie keinen Zeitraum definieren, wird das jeweilige Protokoll vollständig heruntergeladen.

Details zum Aufbau der Logfiles im Fachmodul AMTS

Im Folgenden werden die Logdateien für das Fachmodul AMTS konkret beschrieben. Dabei sind die Parameter über alle drei Logdateien hinweg gleich.

- Ablaufprotokoll: Hier befindet sich die Protokollierung der verarbeitenden Funktionen sowie Konfigurationsänderungen des Fachmoduls.
- Performanceprotokoll: In diesem Protokoll werden Performanceangaben zu Konnektor-Operationen dokumentiert.
- Fehlerprotokoll: In diesem Protokoll werden eventuelle, bei der Verwendung des Konnektors aufgetretene Fehler dokumentiert.

| Kennung in der Logdatei | Beschreibung |
|-------------------------|--|
| Logrefid | eindeutige Referenz des Logeintrages im Konnektor |
| Timestamp | Zeitstempel des Logeintrages |
| Module | Bezeichnung des betroffenen Konnektormoduls |
| Amount | Anzahl, wie oft die Meldung in diesem Logeintrag zusammengefasst ist. ¹⁹¹ |
| Topic | Name der Operation |
| protocolType | Protokollierungsart |
| protocolSeverity | Schweregrad des Protokollierungseintrages |
| Parameter | Parameter mit weiteren Details zum protokollierten Ereignis und Fehler |

Tabelle 5: Aufbau der Logfiles im Fachmodul AMTS

7.7.4 Elektronische Patientenakte (ePA)

Das Fachmodul elektronische Patientenakte (FM ePA) ist ein integraler Bestandteil der KoCoBox MED+ und nutzt deren Basisdienste zur Umsetzung aller Anwendungsfälle der Fachanwendung ePA. Es stellt der KoCoBox MED+ Grundfunktionalitäten für den Zugang zur patientengeführten elektronischen Patientenakte sowie für deren Verwaltung zur Verfügung. Die Nutzung dieser Funktionalitäten erfolgt durch das Clientsystem.

Anwender rufen über ihr Clientsystem (AIS, PVS o.a.) das Fachmodul ePA auf, um in der Praxisumgebung Aktenkonten von Patienten zu aktivieren und auf die Daten des ePA-Aktensystems zuzugreifen. Hierzu werden die eGK des Patienten sowie – in der aktuellen Ausprägung des Systems ePA – die SMC-B der Praxis benötigt.¹⁹²

Die Verbindungen zum ePA-Aktensystem sind gesondert durch TLS sowie weiterhin durch spezielle Protokolle für den Datenaustausch mit den Schlüsselgenerierungsdiensten (SGD-Protokoll) und der

¹⁹¹ Gleiche Logeinträge werden nach bestimmten, komplexen Regeln zusammengefasst.

¹⁹² vgl. [TR-03157] Kap. 1.1-1.2

Dokumentenverwaltung (VAU¹⁹³-Protokoll) geschützt.

Im Bereich *Fachmodul ePA* wird dieses konfiguriert. Im Unterbereich *Informationen* finden sich die Nummer der Version der Software sowie der konkrete Build-Zeitpunkt mit Datum und sekundengenauer Uhrzeit.

Im Unterbereich *Protokollierungskonfiguration* werden der Log-Level, die Speicherdauer sowie das Performancelogging konfiguriert.

Im Unterbereich *Default-Aufrufkontext* werden die kontextbezogenen IDs aus dem Infomodell (siehe Abschnitt 7.6.2) dargestellt.

Im Unterbereich *TLS-Verbindungsparameter* werden die TCP- und TLS-Verbindungsparameter für die Verbindungen der KoCoBox MED+ zum ePA-Aktensystem konfiguriert.

Im Unterbereich *Häufigkeitsbeschränkung für Aufrufe der Operation GetAuthorization List* kann die Beschränkung per Radiobutton ein auf einmal am Tag konfiguriert werden. Dies beschleunigt die Bearbeitungszeit von Patientenakten. Alternativ kann man diese Beschränkung ausschalten.

Abbildung 129: Konfigurationsbereich für das Fachmodul ePA

¹⁹³ Abkürzung für **Vertrauenswürdige Ausführungsumgebung**

Unterbereich Protokollierungskonfiguration

- 1** Zunächst ist der *Log-Level* (Debug, Info, Warning, Error, Fatal) per Drop-down Menü zu definieren. Es gibt den Mindestschweregrad der zu speichernden Einträge im Fachmodulprotokoll an. Per Voreinstellung erscheint *Warning*.
- 2** Geben Sie die *Speicherdauer* in Tagen ein, bevor das ePA-Fachmodul-Protokoll gelöscht wird. Die Voreinstellung ist 180 Tage.
- 3** Aktivieren Sie bei Bedarf das *Performancelogging* mittels Radiobutton ein. Per Voreinstellung ist es ausgeschaltet.

Unterbereiche Ablaufprotokoll, Performanceprotokoll und Fehlerprotokoll

In den drei Unterbereichen findet man jeweils eine tabellarische Übersicht aller Logeinträge mit den folgenden Informationen

- Zeitpunkt,
- Schwere,
- Beschreibung,
- Parameter.

The screenshot shows a web interface titled 'Ablaufprotokoll ePA'. At the top, there is a navigation bar with a dropdown menu set to '20', navigation arrows, and 'Seite 1 von 1'. On the right, it says '1 bis 2 von 2 Datensätzen'. Below this is a table with the following data:

| Zeitpunkt | Schwere | Beschreibung | Parameter |
|----------------------------|---------|------------------|--|
| 13.06.2022 10:32:15.242 | INFO | MGM/ADMINCHANGES | NewVal=true; User=koco-root; RefID=FM_EPA_LOG_PERF |
| 13.06.2022 10:32:15.213 | INFO | MGM/ADMINCHANGES | NewVal=DEBUG; User=koco-root; RefID=FM_EPA_LOG_LEVEL |

Below the table, there is a button labeled 'Protokoll löschen'. Underneath is a section titled 'Download' containing two input fields: 'Protokolleinträge von:' and 'Protokolleinträge bis:'. At the bottom of this section is a button labeled 'Protokoll-Download'.

Abbildung 130: Exemplarische Ansicht zum Ablaufprotokoll ePA mit Downloadfunktion

In allen drei Unterbereichen können Sie:

- 1** über den Button Protokoll löschen die jeweiligen Einträge entfernen;
- 2** im Bereich *Download* über *Protokolleinträge von* und *Protokolleinträge bis* per Kalenderfunktion definieren, für welchen Zeitraum Sie ein Protokoll herunterladen möchten;
- 3** über den Button Protokoll-Download die Tabelleneinträge jeweils für den benannten Zeitraum herunterladen. Sofern Sie keinen Zeitraum definieren, wird das jeweilige Protokoll vollständig heruntergeladen.

Details zum Aufbau der Logfiles im Fachmodul ePA

Im Folgenden werden die Logdateien für das Fachmodul ePA konkret beschrieben. Dabei sind die Parameter über alle drei Logdateien hinweg gleich.

- Ablaufprotokoll: Hier befindet sich die Protokollierung der verarbeitenden Funktionen sowie Konfigurationsänderungen des Fachmoduls.
- Performanceprotokoll: In diesem Protokoll werden Performanceangaben zu Konnektor-Operationen dokumentiert.
- Fehlerprotokoll: In diesem Protokoll werden eventuelle, bei der Verwendung des Konnektors aufgetretene Fehler dokumentiert.

| Kennung in der Logdatei | Beschreibung |
|-------------------------|--|
| Logrefid | eindeutige Referenz des Logeintrages im Konnektor |
| Timestamp | Zeitstempel des Logeintrages |
| Module | Bezeichnung des betroffenen Konnektormoduls |
| Amount | Anzahl, wie oft die Meldung in diesem Logeintrag zusammengefasst ist. ¹⁹⁴ |
| Topic | Name der Operation |
| protocolType | Protokollierungsart |
| protocolSeverity | Schweregrad des Protokollierungseintrages |
| Parameter | Parameter mit weiteren Details zum protokollierten Ereignis und Fehler |

Tabelle 6: Aufbau der Logfiles im Fachmodul ePA

Unterbereich Default-Aufrufkontext

Diese Werte sind über die Parameter des Infomodells einzustellen:

- Mandant_ePA_Default
- Clientsystem_ePA_Default
- Workplace_ePA_Default



Ohne gültigen Default-Aufrufkontext können **keine** ePA-Funktionalitäten genutzt werden. Dies wird durch den Hinweistext „Es fehlt der Default-Aufrufkontext im Infomodell ('Mandant_ePA_Default', 'Clientsystem_ePA_Default', 'Workplace_ePA_Default', sowie zusammenführendes CS-AP-Objekt)“ angezeigt.

¹⁹⁴ Gleiche Logeinträge werden nach bestimmten, komplexen Regeln zusammengefasst.

Unterbereich TLS-Verbindungsparameter

- Der Parameter *TLS-Handshake Timeout* bestimmt die Zeit, innerhalb der ein TLS-Verbindungsaufbau abgeschlossen sein muss. Die Voreinstellung ist 10 Sekunden.
- Die Anzahl der *Keep Alive* Versuche legt fest, wie viele Versuche in einer bestehenden TLS-Verbindung zu deren Aufrechterhaltung erlaubt sind. Die Voreinstellung liegt bei drei *Versuchen*.
- Der Parameter *TCP-Verbindungsaufbau Timeout* legt die maximal zulässige Zeit für den TCP-*Verbindungsaufbau* fest. Die Voreinstellung ist 10 Sekunden.
- Der Parameter *Request Timeout* legt die Zeitspanne fest, in der das Fachmodul ePA die Antwort auf jegliche *Anfrage* an eine Komponente des ePA-Aktensystems erwartet. Die Voreinstellung liegt bei 30 Sekunden.¹⁹⁵




Werden die hier konfigurierten Werte in den Verbindungen überschritten, führt dies zu Fehlschlag beim Zugriff auf die Komponenten des Aktensystems. Das Fachmodul beantwortet dann die Anfragen des Clientsystems an das ePA-Aktensystem mit einem Fehler.



Diese Parameter besitzen, neben ihrer technischen Auswirkung, auch eine Relevanz für die Sicherheit der Verbindung. Wenden Sie sich bei Verbindungsproblemen an Ihren Servicepartner, um eine sichere Konfiguration zu gewährleisten.

Telematikdienste

In diesen Unterbereich werden in einer Übersichtsliste die Verfügbarkeiten der zentralen Telematikdienste für die ePA aufgezeigt.

Die Liste der Dienste wird mit dem Auslösen der Abfrage mittels Klick auf den Button **Alle aktualisieren** gefüllt. Eine Aktualisierung bestehender Daten kann durch Betätigung des Knopfes  erfolgen.

¹⁹⁵ Vgl. [gemSpec_FM_ePA] Kap. 6.1 „Allgemein“

| Telematikdienste ePA | | | | |
|------------------------------------|---|----------------|-----------------------|--|
| Verfügbarkeit der Telematikdienste | | | | |
| 30 | ⏪ ⏩ | Seite 1 von 10 | ▶ ⏪ ⏩ | 1 bis 30 von 293 Datensätzen |
| Alle aktualisieren | | | | |
| Dienst | HomeCommunityID | Status | letzter Prüfzeitpunkt | FQDN |
| AUTHN | urn:oid:1.2.276.0.76.3.1.466.2.1.3.90.1 | erreichbar | 21.11.2023 14:38:48 | authn-epa-ru.bitmarck.epa.telematik-test |
| AUTHN | urn:oid:1.2.276.0.76.3.1.419 | erreichbar | 21.11.2023 14:38:50 | authn-epa-qu.bitmarck.epa.telematik-test |
| AUTHN | urn:oid:1.2.276.0.76.3.1.466.2.1.8.66.1 | erreichbar | 21.11.2023 14:38:50 | authn-epa-qt.bitmarck.epa.telematik-test |
| AUTHN | urn:oid:1.2.276.0.76.3.1.466.2.1.3.10.1 | erreichbar | 21.11.2023 14:38:48 | authn-epa-ru.bitmarck.epa.telematik-test |
| AUTHN | urn:oid:1.2.276.0.76.3.1.466.2.1.8.85.1 | erreichbar | 21.11.2023 14:38:50 | authn-epa-qt.bitmarck.epa.telematik-test |
| AUTHN | urn:oid:1.2.276.0.76.3.1.466.2.1.8.92.1 | erreichbar | 21.11.2023 14:38:50 | authn-epa-qt.bitmarck.epa.telematik-test |
| AUTHN | urn:oid:1.2.276.0.76.3.1.385 | erreichbar | 21.11.2023 14:38:50 | authn-epa-qu.bitmarck.epa.telematik-test |
| AUTHN | urn:oid:1.2.276.0.76.3.1.466.2.1.8.90.1 | erreichbar | 21.11.2023 14:38:50 | authn-epa-qt.bitmarck.epa.telematik-test |
| AUTHN | urn:oid:1.2.276.0.76.3.1.315.3.3.1.19 | erreichbar | 21.11.2023 14:38:49 | authn.ibm.epa.telematik-test |
| AUTHN | urn:oid:1.2.276.0.76.3.1.315.3.3.1.18 | erreichbar | 21.11.2023 14:38:49 | authn.ibm.epa.telematik-test |
| AUTHN | urn:oid:1.2.276.0.76.3.1.315.3.3.1.17 | erreichbar | 21.11.2023 14:38:49 | authn.ibm.epa.telematik-test |
| AUTHN | urn:oid:1.2.276.0.76.3.1.315.3.3.1.16 | erreichbar | 21.11.2023 14:38:49 | authn.ibm.epa.telematik-test |
| AUTHN | urn:oid:1.2.276.0.76.3.1.315.3.3.1.15 | erreichbar | 21.11.2023 14:38:49 | authn.ibm.epa.telematik-test |

Abbildung 131: Übersichtliste verfügbarer Telematikdienste für die ePA (Ausschnitt)

In der Übersicht finden sich folgende Informationen:

- **Dienst:** symbolischer Name des ePA-Diensttyps – hier sind folgende Typen möglich:
 - AMCRE Mandantenübergreifender Prüfdienst zur Ermittlung der Lokalisierung von Aktenkonten (mandantenübergreifendes CheckRecordExist)
 - AUTHN Authentisierungsdienst
 - AUTHZ Autorisierungsdienst
 - DOCV Dokumentenverwaltung
 - SGD1, SGD2 Schlüsselgenerierungsdienst 1 bzw. 2
- **HomeCommunityID:** Kennung des adressierten Aktensystems
- **Status:** zeigt an, ob der Dienst aktuell erreichbar ist. Folgende Anzeigen sind erwartbar:
 - wird geprüft OK, Verbindungsprüfung läuft gerade
 - erreichbar OK, TI-Dienst ist ordnungsgemäß erreichbar
 - DNS_ERROR Fehler, DNS-Abfrage wird nicht aufgelöst
 - NETWORK_ERROR Fehler, ein Netzwerkproblem ist aufgetreten
 - REJECTED Fehler, TI-Dienst lehnt die Verbindung ab
- **letzter Prüfzeitpunkt:** Zeitpunkt der letzten Statusabfrage in diesem Dialog
- **FQDN:** eindeutiger Domänenbezeichner des Dienstes

7.7.5 Notfalldaten-Management (NFDM)

Das Fachmodul Notfalldaten-Management (FM NFDM) ist ein integraler Bestandteil des Konnektors und nutzt dessen Basisdienste zur Umsetzung aller Anwendungsfälle der Fachanwendung NFDM. Es stellt dem Konnektor Grundfunktionalitäten zur Verwaltung von Notfalldatensätzen (NFD), und von Datensätzen für persönliche Erklärungen (DPE) auf der elektronischen Gesundheitskarte (eGK) zur Verfügung, die durch das Clientsystem genutzt werden.¹⁹⁶

Anwender rufen über ihr Clientsystem (AIS, PVS o.a.) das Fachmodul NFDM auf, um auf die eGK des Patienten zuzugreifen. Über ihre Rolle, die technisch durch das Zugriffsprofil ihrer Smartcard (HBA, SMC-B) repräsentiert wird, erhalten die Anwender die benötigte Berechtigung zum Zugriff auf dessen Notfalldaten.¹⁹⁷

Im Bereich *Fachmodul NDFM* wird dieses konfiguriert. Im Unterbereich *Informationen* finden sich die Nummer der *Version* der Software sowie der konkrete *Build-Zeitpunkt* mit Datum und sekundengenaue Uhrzeit.

Im Unterbereich *Protokollierungskonfiguration* werden der *Log-Level*, die *Speicherdauer* sowie das *Performancelogging* konfiguriert.

Fachmodul NFDM

Informationen

Version: 7.11.0



Build-Zeitpunkt: 15.11.2023, 10:18:19 UTC

Protokollierungskonfiguration

Log-Level:

Speicherdauer:

Performancelogging: ein aus

Download herstellerspezifischer Logs




Abbildung 132: Konfigurationsbereich für das Fachmodul NFDM

¹⁹⁶ Vgl. [TR-03154], S.7

¹⁹⁷ Vgl. [gemSpec_FM_NFDM], S. 12

Legen Sie die *Protokollierungskonfiguration* wie folgt fest:

- 1 Zunächst ist der *Log-Level* (Debug, Info, Warning, Error, Fatal) per Drop-down Menü zu definieren. Es gibt den Mindestschweregrad der zu speichernden Einträge im Fachmodulprotokoll an. Per Voreinstellung erscheint *Warning*.
- 2 Geben Sie die *Speicherdauer* in Tagen ein, bevor das NFDM-Fachmodul-Protokoll gelöscht wird. Die Voreinstellung ist 180 Tage.
- 3 Aktivieren Sie bei Bedarf das *Performancelogging* mittels Radiobutton ein. Per Voreinstellung ist es ausgeschaltet.

Unterbereiche Ablaufprotokoll, Performanceprotokoll und Fehlerprotokoll

In den drei Unterbereichen findet man jeweils eine tabellarische Übersicht aller Logeinträge mit den folgenden Informationen

- Zeitpunkt,
- Schwere,
- Beschreibung,
- Parameter.

| Zeitpunkt | Schwere | Beschreibung | Parameter |
|-------------------------|---------|--------------|---|
| 14.09.2018 17:30:00.456 | FATAL | writeDPE | Vorgangsnnummer=65fb270-399c-4e6d-84b1-c348f64700ef; Fehlercode=101; Zeitpunkt=1536939000219; CardHandle=19c1fa01-3620-4702-97b8-ee09de97b66; Fehlerdetails=Kartenfehler |
| 14.09.2018 14:30:33.655 | FATAL | readNFD | Vorgangsnnummer=f1662ca7-97cf-4311-b976-b2c41c2ae0fb; Fehlercode=111; Zeitpunkt=1536928233416; CardHandle=a68a53e9-8591-4e4d-b550-c2db125658d3; Detail=Notfalldaten konnten nicht gelesen werden. Grund: Fehler bei der Dekomprimierung.; Fehlerdetails=Fehler beim Lesen von Daten der eGK |
| 12.09.2018 18:45:09.430 | FATAL | writeDPE | Vorgangsnnummer=2f83d8ad-abac-47a2-aa49-e8da919b2fba; Fehlercode=101; Zeitpunkt=1536770709303; CardHandle=54f69d88-1536-4e8b-be24-8cf621e45f1e; Fehlerdetails=Kartenfehler |
| 12.09.2018 18:44:19.662 | ERR | writeDPE | Vorgangsnnummer=50e5d4f4-51f6-4456-9e60-c24011b3af33; Fehlercode=20035; Zeitpunkt=1536770699562; CardHandle=12384090-e223-4c1d-a085-e1893a590b77; Fehlerdetails=Kein Kartenobjekt zu cardHandle ermittelt. |
| 12.09.2018 18:27:42.828 | FATAL | writeDPE | Vorgangsnnummer=98528a7-bbf9-4352-b551-55d0d0750a94; Fehlercode=101; Zeitpunkt=1536769662569; CardHandle=12384090-e223-4c1d-a085-e1893a590b77; Fehlerdetails=Kartenfehler |
| 12.09.2018 18:26:24.374 | ERR | writeDPE | Vorgangsnnummer=f985577c-e12f-43af-a6d3-5d1f9fb3d91a; Fehlercode=20035; Zeitpunkt=1536769584334; CardHandle=1e45d24a-b309-4995-9d4f-1380eafb01e; Fehlerdetails=Kein Kartenobjekt zu cardHandle ermittelt. |
| 12.09.2018 18:25:55.425 | FATAL | writeDPE | Vorgangsnnummer=b8120b07-4833-4946-a645-49e8a91b87d0; Fehlercode=101; Zeitpunkt=1536769555192; CardHandle=1e45d24a-b309-4995-9d4f-1380eafb01e; Fehlerdetails=Kartenfehler |
| 12.09.2018 18:22:41.581 | ERR | writeDPE | Vorgangsnnummer=f985577c-e12f-43af-a6d3-5d1f9fb3d91a; Fehlercode=4093; Zeitpunkt=1536769361459; CardHandle=bbcb522-c30b-48c1-88b5-d295e43fd693; Fehlerdetails=Karte wird in einer anderen Kartensitzung exklusiv verwendet |
| 12.09.2018 18:21:39.012 | ERR | writeDPE | Vorgangsnnummer=3ceee190-ce68-48fb-9d7d-53810643c5a; Fehlercode=4093; Zeitpunkt=1536769298886; CardHandle=bbcb522-c30b-48c1-88b5-d295e43fd693; Fehlerdetails=Karte wird in einer anderen Kartensitzung exklusiv verwendet |
| 12.09.2018 18:21:00.750 | ERR | writeDPE | Vorgangsnnummer=b8120b07-4833-4946-a645-49e8a91b87d0; Fehlercode=5001; Zeitpunkt=1536769260625; CardHandle=bbcb522-c30b-48c1-88b5-d295e43fd693; Fehlerdetails=HBA/SMC-B nicht freigeschaltet |
| 12.09.2018 18:19:57.020 | ERR | writeDPE | Vorgangsnnummer=f0fd3c3b-879b-4fc2-baf5-e10294d7e75d; Fehlercode=3015; Zeitpunkt=1536769196919; CardHandle=bbcb522-c30b-48c1-88b5-d295e43fd693; Fehlerdetails=Das Primärsystem hat keine Zugriffsberechtigung auf den HBA/die SMC-B. |
| 12.09.2018 16:25:14.659 | ERR | writeDPE | Vorgangsnnummer=4d2833fc-1c1d-4492-b02b-302b44401f98; Fehlercode=5015; Zeitpunkt=1536762314613; CardHandle=4a882161-003a-4f4c-b4fc-f2599cbecae; Fehlerdetails=Das Primärsystem hat keine Zugriffsberechtigung auf den HBA/die SMC-B. |

Abbildung 133: Exemplarische Ansicht zum Ablaufprotokoll NFDM mit Downloadfunktion

In allen drei Unterbereichen können Sie:

- über den Button *Protokoll löschen* die jeweiligen Einträge entfernen.
- im Bereich *Download* über *Protokolleinträge von* und *Protokolleinträge bis* per Kalenderfunktion definieren, für welchen Zeitraum Sie ein Protokoll herunterladen möchten.
- über den Button *Protokoll-Download* die Tabelleneinträge jeweils für den benannten Zeitraum herunterladen. Sofern Sie keinen Zeitraum definieren, wird das jeweilige Protokoll vollständig heruntergeladen.

Details zum Aufbau der Logfiles im Fachmodul NFDM

Im Folgenden werden die Logdateien für das Fachmodul NFDM konkret beschrieben. Dabei sind die Parameter über alle drei Logdateien hinweg gleich.

- Ablaufprotokoll: Hier befindet sich die Protokollierung der verarbeitenden Funktionen sowie Konfigurationsänderungen des Fachmoduls.
- Performanceprotokoll: In diesem Protokoll werden Performanceangaben zu Konnektor-Operationen dokumentiert.
- Fehlerprotokoll: In diesem Protokoll werden eventuelle, bei der Verwendung des Konnektors aufgetretene Fehler dokumentiert.

| Kennung in der Logdatei | Beschreibung |
|-------------------------|--|
| Logrefid | eindeutige Referenz des Logeintrages im Konnektor |
| Timestamp | Zeitstempel des Logeintrages |
| Module | Bezeichnung des betroffenen Konnektormoduls |
| Amount | Anzahl, wie oft die Meldung in diesem Logeintrag zusammengefasst ist. ¹⁹⁸ |
| Topic | Name der Operation |
| protocolType | Protokollierungsart |
| protocolSeverity | Schweregrad des Protokollierungseintrages |
| Parameter | Parameter mit weiteren Details zum protokollierten Ereignis und Fehler |

Tabelle 7: Aufbau der Logfiles im Fachmodul NFDM



¹⁹⁸ Gleiche Logeinträge werden nach bestimmten, komplexen Regeln zusammengefasst.



8 Sicherheitsrelevante Szenarien

8.1 Einsatzumgebung

Beim Betrieb der KoCoBox MED+ in einem zugriffsgeschützten Raum sind verschiedene Situationen denkbar, die die Sicherheit und Vertrauenswürdigkeit des Geräts gefährden.

Informieren Sie das Fachpersonal und sämtliche weiteren Mitarbeiter hierüber.

|  Sicherheitsrelevantes Szenario |  Handlungsanweisungen |
|--|--|
| Diebstahl der KoCoBox MED+ | <p>Kontaktieren Sie sofort den Support / Ihren Zugangsdienstprovider, um das Sicherheitsmodul gSMC-K sperren zu lassen. Halten Sie Ihre ContractID, die ICCSN der gSMC-K sowie die Seriennummer (Ser) des Geräts bereit und folgen Sie den Anweisungen.</p> <p>Untersuchen Sie unbedingt die Umgebung auf eventuelle andere Manipulationen: Dies betrifft sowohl den medizinischen und verwaltungstechnischen Bereich als auch die IT-Ausstattung wie Server, Rechner oder Kartenterminals. Geben Sie ggf. Ihrem Support auch diesbezügliche Befunde durch.</p> |
| Bei Einbruch / Volldurchbruch: Auf den ersten Blick ist die KoCoBox MED+ unversehrt. | <p>Prüfen Sie bei einem Verdacht auf Manipulation des Geräts das Gehäuse, die Siegel sowie die Verkabelung hinsichtlich Veränderungen oder Beschädigungen.</p> <p>Führen Sie einen Neustart der KoCoBox MED+, indem Sie das Gerät vom Strom nehmen und es nach einer Minute wieder anschließen. Es wird beim Neustart ein Selbsttest auf Integrität durchgeführt. Ist dieser erfolgreich, kann das Gerät weiter genutzt werden.</p> <p>Schlägt der Selbsttest fehl, erscheint auf dem Display eine Fehlermeldung. Kontaktieren Sie umgehend den Support. Halten Sie die Seriennummer des Geräts bereit und folgen Sie den Anweisungen.</p> <p>Nutzen Sie das Gerät bis zur Klärung des Sachverhalts nicht.</p> |

|  Sicherheitsrelevantes Szenario |  Handlungsanweisungen |
|--|---|
| <p>Sicherheitssiegel an der KoCoBox MED+ entsprechen nicht mehr denjenigen, die ursprünglich angebracht waren.</p> <p>Sicherheitssiegel sind gebrochen oder wurden entfernt, Gehäuse ist scheinbar unversehrt.</p> <p>Sicherheitssiegel sind gebrochen oder wurden entfernt, Gehäuse ist geöffnet, Inneres ist dem Anschein nach intakt.</p> | <p>Kontaktieren Sie unverzüglich Ihren Support. Halten Sie die Seriennummer des Geräts bereit und folgen Sie den Anweisungen.</p> <p>Nutzen Sie das Gerät bis zur Klärung des Sachverhalts nicht.</p> |
| <p>Sicherheitssiegel sind gebrochen oder wurden entfernt, Gehäuse ist geöffnet, Sicherheitsmodul gSMC-K wurde entfernt.</p> | <p>Kontaktieren Sie unverzüglich Ihren Support. Halten Sie die Seriennummer des Geräts bereit und folgen Sie den Anweisungen.</p> <p>Nutzen Sie das Gerät bis zur Klärung des Sachverhalts nicht.</p> |

8.2 Sicherheitskritische Fehlerzustände




Das Display bzw. die Tabelle *Betriebszustandsmeldungen* auf der Status-Seite der Managementschnittstelle melden Fehlerzustände.

Die Prüfung auf derartige Fehlerzustände erfolgt automatisch durch den Konnektor. Sie wird mit ihrem Ergebnis in den Protokolldaten vermerkt.¹⁹⁹

Die in der folgenden Tabelle aufgelisteten fatalen Fehlerzustände führen zu einem sicherheitskritischen Betriebszustand, der durch den Administrator aufzulösen ist.




Sobald Sie einen oder mehrere sicherheitskritische Fehlerzustände der KoCoBox MED+ identifizieren, folgen Sie umgehend den Handlungsanweisungen.




|  Display-Anzeige |  Beschreibung |  Handlungsanweisung |
|---|---|---|
| EC_CRL_Out_Of_Date | Die im TOE hinterlegte CRL ist zu alt (Systemzeit $t >$ Next Update der CRL). Ist der Wert des Ablaufdatums der 01.01.1970, dann enthält der Konnektor keine aktuelle CRL. Dies tritt z.B. nach einem Werksreset auf. | Spielen Sie über die Managementschnittstelle im Bereich <i>Zertifikatsdienst</i> die CRL manuell über den Button CRL importieren ein. Ist dies nicht erfolgreich, kontaktieren Sie den Support. |
| EC_Firewall_Not_Reliable | Firewall-Regeln konnten nicht fehlerfrei generiert werden oder beim Laden der Firewall-Regeln ist ein Fehler aufgetreten. | Sie haben drei Möglichkeiten: Speichern Sie in der Managementschnittstelle im Bereich <i>LAN/WAN</i> die Netzwerkkonfiguration neu. Ist dies nicht erfolgreich, starten Sie die KoCoBox MED+ neu, indem Sie sie für etwa eine Minute vom Stromnetz trennen und erneut anschließen. Ist dies nicht erfolgreich, führen Sie auf der Managementschnittstelle im Navigationsbereich <i>Verwaltung</i> ein Werksreset ²⁰⁰ durch. |




¹⁹⁹ Siehe dazu im Kapitel Inbetriebnahme / Konfiguration des Anwendungskonnektors den Abschnitt Protokollierungsdienst

²⁰⁰ Dringende Empfehlung: Um eine Neu-Konfiguration zu vermeiden, führen Sie bitte **vor** dem Werksreset einen Export der Konfigurationsdaten des Konnektors durch. Diese können nach dem Werksreset wieder importiert werden. Siehe dazu im Kapitel Verwaltung den Abschnitt Ex-/Import.

|  Display-Anzeige |  Beschreibung |  Handlungsanweisung |
|---|---|--|
| EC_NK_Certificate_Expired | Die Sicherheitszertifikate für den Zugang zur Telematikinfrastruktur sind zeitlich abgelaufen. | Die Laufzeitverlängerung für die KoCoBox MED+ muss aktiviert bzw. manuell ausgeführt werden. Kontaktieren Sie ggf. den Support bzw. Ihren Dienstleister. |
| EC_NK_Certificate_Expiring | Die Sicherheitszertifikate für den Zugang zur Telematikinfrastruktur laufen in Kürze ab. Die Meldung erscheint erstmalig 180 Tage vor Ablauf und wird täglich erneuert. | Die Laufzeitverlängerung für die KoCoBox MED+ sollte aktiviert werden. Falls dies nicht innerhalb der nächsten Tage zum Erfolg führt, kontaktieren Sie den Support bzw. Ihren Dienstleister für eine Unterstützung zur manuellen Laufzeitverlängerung. |
| EC_Random_Generator_Not_Reliable ²⁰¹ | Der Zufallszahlengenerator kann die Anforderungen an die zu erzeugende Entropie nicht erfüllen. | Kontaktieren Sie umgehend den Support. |
| EC_Secure_KeyStore_Not_Available | Der sichere Zertifikats- und Schlüsselspeicher des Konnektors (gSMC-K oder Truststore) ist nicht verfügbar. | Starten Sie die KoCoBox MED+ neu, indem Sie sie für etwa eine Minute vom Stromnetz trennen. Ist dies nicht erfolgreich, kontaktieren Sie den Support. |
| EC_Security_Log_Not_Writable | Das Sicherheitslog kann nicht geschrieben werden. | Starten Sie die KoCoBox MED+ neu, indem Sie sie für etwa eine Minute vom Stromnetz trennen und erneut anschließen. Ist dies nicht erfolgreich, kontaktieren Sie den Support. |
| EC_Software_Integrity_Check_Failed | Eine oder mehrere konnektor-interne Integritätsprüfungen der aktiven Konnektorbestandteile sind fehlgeschlagen. | Starten Sie die KoCoBox MED+ neu, indem Sie sie für etwa eine Minute vom Stromnetz trennen und erneut anschließen. Ist dies nicht erfolgreich, kontaktieren Sie den Support. |

²⁰¹ Diese Fehlerzustandsmeldung wird durch den Netzkonnektor nie ausgelöst.

|  Display-Anzeige |  Beschreibung |  Handlungsanweisung |
|---|---|--|
| EC_Time_Difference_Intolerable | Die Abweichung zwischen der lokalen Zeit und der per NTP empfangenen Zeit bei der Zeitsynchronisation ist größer als NTP_MAX_TIMEDIFFERENCE. Nach einer Korrektur oder Bestätigung der Systemzeit durch einen Administrator muss der Konnektor den Fehlerzustand zurücksetzen. | Stellen Sie auf der Managementschnittstelle im Navigationsbereich <i>Zeitdienst</i> die Zeit manuell ein. Nutzen Sie alternativ den Button mit TI synchronisieren. Beachten Sie, dass – besonders bei längeren VPN-Offline-Zeiten des Konnektors – die Fehlermeldung erst nach einer zusätzlichen manuellen Korrektur auf die schon aktualisierte Zeitangabe verschwindet. |
| 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. | Starten Sie das Gerät neu, indem Sie es für etwa eine Minute vom Stromnetz trennen und erneut anschließen. Ist dies nicht erfolgreich, stellen Sie auf der Managementschnittstelle im Navigationsbereich <i>Zeitdienst</i> die Zeit manuell ein. Nutzen Sie alternativ den Button mit TI synchronisieren. Ist dies nicht erfolgreich, kontaktieren Sie den Support. |
| EC_TSL_Trust_Anchor_Out_Of_Date | Die Gültigkeit des Vertrauensankers ist abgelaufen. | Kontaktieren Sie den Support. |
| EC_TSL_Out_Of_Date_Beyond_Grace_Period | Systemzeit t mit $t > \text{NextUpdate-Element der TSL} + CERT_TSL_DEFAULT_GRACE_PERIOD_DAYS$ und eine neue TSL ist nicht verfügbar | Spielen Sie über die Managementschnittstelle im Bereich <i>Zertifikatsdienst</i> die TSL manuell über den Button TSL importieren ein. Ist dies nicht erfolgreich, kontaktieren Sie den Support. |

|  Display-Anzeige |  Beschreibung |  Handlungsanweisung |
|---|--|---|
| EC_OTHER_ERROR_STATE(1) | Konnektor gerät als Folge einer Out-of-Memory-Exception in einen sog. Heap-Overflow. | Prüfen Sie die Ursache für den Fehler. ²⁰² Beenden Sie den Fehlerzustand manuell über den Button EC_OTHER_ERROR_STATE zurücksetzen im Navigationsbereich <i>Verwaltung</i> . Der Konnektor nimmt automatisch einen Neustart vor. Alle Systemdienste der KoCoBox MED+ werden neu initialisiert. |

²⁰² Siehe im Detail die ausführliche Fußnote oben im Abschnitt Verwaltung / Reset.

| | | |
|--|--|--|
| Operational State Error EC_OTHER_ERROR_STATE(2) | Herstellerspezifische Fehlermeldung | Der Protokollspeicher des Konnektors ist zu mehr als 80 Prozent belegt. Überprüfen Sie die Protokolle und informieren Sie bitte Ihren Support. |
|--|--|--|



Folgen Sie den Anweisungen des Supports, um die erforderlichen Sicherheitsanforderungen zu erfüllen.

8.3 Selbsttest




Beim Hochfahren des Systems (Booten) führt die KoCoBox MED+ einen Selbsttest durch.²⁰³ Hier können verschiedene Fehler auftreten, die in der folgenden Tabelle aufgelistet sind.



Der Selbsttest wird von der KoCoBox MED+ **bei jedem Neustart automatisch** durchgeführt, um sicherheitstechnische Veränderungen zu prüfen. Dieser Mechanismus erschwert Manipulationen und Angriffe auf den Konnektor und schützt somit seine Integrität.



Folgen Sie den Handlungsanweisungen, sobald nach dem Start des Geräts entsprechende Fehlermeldungen auf dem Display erscheinen.

|  Display-Anzeige |  Beschreibung |  Handlungsanweisung |
|---|---|--|
| <i>Unbekanntes USB-Gerät. Boot fehlgeschlagen!</i> | Fehler beim Zugriff auf die Leseinheit der Smartcards. | Starten Sie die KoCoBox MED+ neu, indem Sie sie für etwa eine Minute vom Stromnetz trennen und erneut anschließen. Ist dies nicht erfolgreich, kontaktieren Sie bitte Ihren Support. |
| <i>Dateisystem fehlerhaft!</i> | Die Signatur kann nicht validiert werden. | Kontaktieren Sie Ihren Support. |
| <i>Dateisystem fehlerhaft!</i> | Hashwert stimmt nicht mit Referenzwert überein. | Kontaktieren Sie Ihren Support. |
| <i>Kryptographische Algorithmen ungültig!</i> | Die kryptographischen Algorithmen sind abgelaufen. | Kontaktieren Sie Ihren Support. |
| <i>Fehler beim Zugriff auf die gSMC-K!</i> | Die Smartcard wurde nicht erkannt. | Starten Sie die KoCoBox MED+ neu, indem Sie sie für etwa eine Minute vom Stromnetz trennen und erneut anschließen. Ist dies nicht erfolgreich, kontaktieren Sie bitte den Support. |
| <i>Dateisystem fehlerhaft!</i> | Entschlüsselung des Keyfiles für die verschlüsselten Partitionen auf dem Flash konnte nicht entschlüsselt werden. | Starten Sie die KoCoBox MED+ neu, indem Sie sie für etwa eine Minute vom Stromnetz trennen und erneut anschließen. Ist dies nicht erfolgreich, kontaktieren Sie den Support. |

²⁰³ Alternativ kann der Selbsttest manuell im Navigationsbereich *Verwaltung* über den Button Selbsttest durchführen angestoßen werden. Siehe dazu ausführlicher den Abschnitt *Verwaltung / Selbsttest*.

| | | |
|--------------------------------|---|--|
| <i>Dateisystem fehlerhaft!</i> | Die verschlüsselte Partition für das Log konnte nicht geöffnet werden. | Starten Sie die KoCoBox MED+ neu, indem Sie sie für etwa eine Minute vom Stromnetz trennen und erneut anschließen. Ist dies nicht erfolgreich, kontaktieren Sie den Support. |
| <i>Dateisystem fehlerhaft!</i> | Die verschlüsselten Partitionen für den sicheren Speicher konnte nicht geöffnet werden. | Starten Sie die KoCoBox MED+ neu, indem Sie sie für etwa eine Minute vom Stromnetz trennen und erneut anschließen. Ist dies nicht erfolgreich, kontaktieren Sie den Support. |

8.4 Sperrprozess und Außerbetriebnahme

Sperrprozess

Für den Fall, dass die KoCoBox MED+ gesperrt werden muss (z. B. weil sie gestohlen oder abhandengekommen ist), ist Folgendes zu beachten:

1 Der Zugangsdienstprovider muss umgehend informiert werden, damit er das Zertifikat für den TI-Zugang sperrt. Dafür sind Vertragsnummer (ContractID), Seriennummer der KoCoBox MED+ sowie die Daten der zur Registrierung genutzten SMC-B (ICCSN) bereitzuhalten.

2 Anschließend ist der Second-Level-Support zu kontaktieren.



Der Arzt / Apotheker und das Fachpersonal vor Ort sind unbedingt darauf hinzuweisen, dass das Deregistrieren der KoCoBox MED+ beim ZGDP **unverzüglich** nach Bemerken des Geräteverlusts erfolgen muss. Dazu ist umgehend der Servicepartner zu kontaktieren.

Außerbetriebnahme

Für den Fall, dass die KoCoBox MED+ dauerhaft außer Betrieb genommen werden soll (etwa wegen Entsorgung), muss das Gerät umgehend beim Zugangsdienstprovider deregistriert werden und einen Werksreset erfahren. Dies stellt den Datenschutz für die Rück- oder Weitergabe des Konnektors sicher.

Gehen Sie dazu wie folgt vor:

1 Rufen Sie in der Navigationsspalte unter *VPN* den Unterbereich *Registrierung* auf.

2 Tragen Sie die entsprechenden Daten in die Zeilen *Vertragsnummer (ContractID)* und *zur Registrierung zu nutzende SMC-B (ICCSN)* ein. Prüfen Sie diese Einträge auf ihre Korrektheit.

3 Klicken Sie auf den Button *deregistrieren*.

4 Führen Sie anschließend – gegebenenfalls nach Absprache mit Ihrem Support – noch einen Werksreset²⁰⁴ (siehe Kapitel Konnektormanagement / Werksreset) durch, wobei Sie das Gerät nach dem Herunterfahren **nicht** wieder an die Stromversorgung anschließen.

Melden Sie anschließend Ihrem Support, dass die KoCoBox MED+ außer Betrieb genommen wurde. Halten Sie dafür bei Bedarf die Seriennummer der KoCoBox MED+ bereit und folgen Sie den weiteren Anweisungen.

²⁰⁴ Siehe oben im Abschnitt Konfiguration des Anwendungskonnektors / Verwaltung / Werksreset

9 Anhang

9.1 Weitere Konfigurationsoptionen

9.1.1 Alternative Netzwerkkonfigurationen

Im Folgenden werden die weiteren möglichen Optionen für eine initiale Konfiguration des Konnektors beschrieben.

9.1.1.1 Anbindungsmodus Internet

Neben der oben beschriebenen Option (IAG) für den *Anbindungsmodus Internet* gibt es die Möglichkeiten *SIS* und *KEINER*:

- *SIS* stellt einen sicheren Internetzugang zur Verfügung. Voraussetzung ist ein entsprechender Vertrag mit einem Service Provider.
- *KEINER* verhindert, dass Anfragen aus dem internen Netzwerk in das Internet weitergeleitet werden.

9.1.1.2 Routingmodus Intranet

Neben der oben beschriebenen Option (Block) für den Routingmodus Intranet kann auch die Option Redirect ausgewählt werden. Dies ist nur möglich, wenn mindestens eine Intranet-Route definiert ist.

Mit dieser Option werden aus den konfigurierten internen Netzen Anfragen weitergeleitet.

9.1.1.3 WAN Adapter Modus

Neben der oben beschriebenen Option aus für den *WAN Adapter Modus*²⁰⁵ kann auch die Option ein gewählt werden. Diese wirkt sich direkt auf den *Anbindungsmodus* aus: Er schaltet sich automatisch auf seriell (,in Reihe') (*SERIAL*).



Beim *Anbindungsmodus* seriell (,in Reihe') steht die Option *IAG* für den *Anbindungsmodus Internet* nicht zur Verfügung.



Der *Anbindungsmodus* seriell (,in Reihe') erfordert eine Nutzung des SIS.

²⁰⁵ Die Illustration für die einfache Installation des Konnektors lehnt sich an das Szenario 1 in den Konnektor-Spezifikationen der gematik an. Siehe generell: [gemSpec_Kon], Anhang K

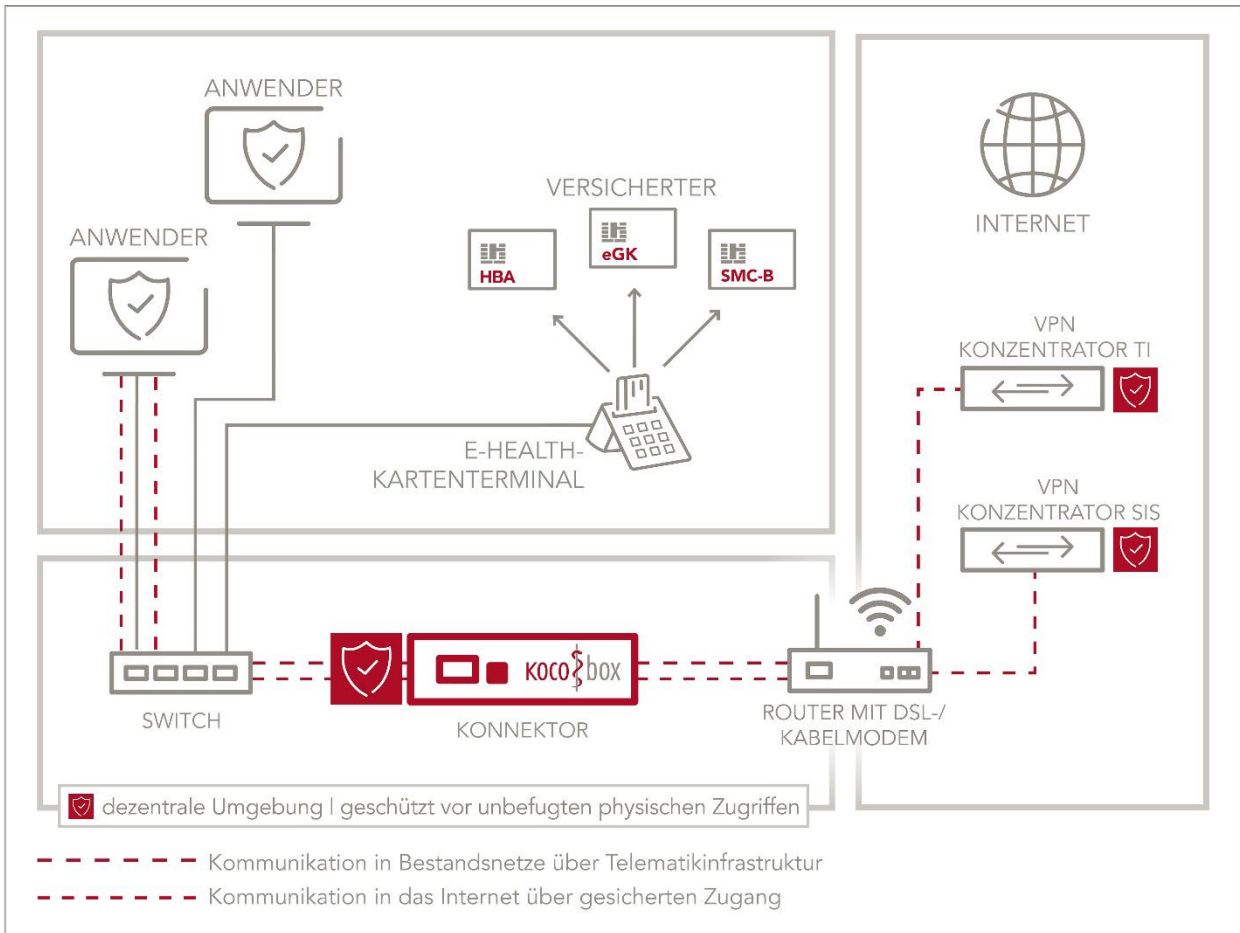


Abbildung 134: Szenario für die einfache Installation der KoCoBox MED+

Netzwerkkonfigurationen

Basiskonfiguration

Hostname:

Anbindungsmodus Internet: SIS IAG KEINER

Anbindungsmodus: **PARALLEL**

Adresse IAG:

Routingmodus Intranet: Redirect Block

WAN Adapter Modus: ein aus

Übermittelte Bestandsnetze aktivieren: an aus

Abbildung 135: WAN Adapter Modus eingeschaltet

Für den Fall, dass der *WAN Adapter Modus* aktiviert ist, müssen die folgenden Konfigurationen im Bereich WAN durchgeführt werden:

- 1 Der Radiobutton beim *DHCP-Client* an der WAN-Schnittstelle ist per Voreinstellung aktiviert. Somit werden die *IP-Adresse des WAN-Adapters* sowie die dazugehörige *Subnetzmaske* vom DHCP-Server geliefert und automatisch eingetragen. Die Adresse des *lokalen Netzwerks*, an das der WAN-Adapter des Konnektors angeschlossen ist, ergibt sich automatisch aus den eingetragenen Werten.

- 2 Falls der *DHCP-Client* an der WAN-Schnittstelle deaktiviert ist, geben Sie die *IP-Adresse des WAN-Adapters* sowie die dazugehörige *Subnetzmaske* ein. Die Adresse des *lokalen Netzwerks*, an das der WAN-Adapter des Konnektors angeschlossen ist, ergibt sich automatisch aus den eingetragenen Werten.
- 3 Tragen Sie bei Bedarf die Länge der *IP-Pakete (MTU)* ein; die Voreinstellung ist 1.500. Wir empfehlen, diese beizubehalten. Beachten Sie, dass bei deaktiviertem DHCP-Client am WAN-Adapter die eingestellten Parameter nicht wirksam werden.

9.1.2 Konfiguration ohne Internetanbindung

Diese Konfiguration ist für eine Praxis ohne Internetanschluss durchzuführen.



Beachten Sie bitte, dass hierbei folgende Funktionsmerkmale nicht zur Verfügung stehen: Zertifikatsdienst²⁰⁶, Anbindung der Clientsysteme (TLS-Dienst), Anbindung LAN/WAN, VPN-Client, Zeitdienst, Software-Aktualisierung.

Verwaltung der Leistungsumfänge

Leistungsumfang ONLINE: aktiviert nicht aktiviert

Leistungsumfang Signaturanwendungskomponente: aktiviert nicht aktiviert

Betrieb als Standalone Konnektor: aktiviert nicht aktiviert

Abbildung 136: Leistungsumfang ONLINE nicht aktiviert

Rufen Sie in der Navigationsspalte *Verwaltung* auf und setzen Sie den Radiobutton beim *Leistungsumfang ONLINE* auf nicht aktiviert.

Bestätigen Sie dies mittels Übernehmen.



Beachten Sie zusammenfassend für die Konfiguration der KoCoBox MED+ im Offline-Modus bitte folgende Sicherheitshinweise:

- Es wird weder eine Verbindung zur TI noch zum SIS hergestellt.
- Es findet keine Zeitsynchronisation mit dem Zeitserver der TI statt. In diesem Fall ist der Administrator für die korrekte Systemzeit verantwortlich.
- Ebenso findet keine automatische Aktualisierung von TSL/CRL statt. Diese sind vom Administrator manuell zu aktualisieren.

²⁰⁶ Im Bereich *Zertifikatsdienst* werden bei dieser Konfiguration die folgenden Buttons deaktiviert (ausgegraut): CRL aktualisieren, OCSP-Forwarder prüfen, OCSP-Request testen, TSL aktualisieren, BNetzA-VL aktualisieren.

9.1.3 Standalone-Szenario mit physischer Trennung

Für eine Praxis, deren internes Netz nicht an das Internet angeschlossen ist, besteht die Möglichkeit, den gesetzlich vorgeschriebenen Abgleich der Versichertenstammdaten (VSD) mit dem folgenden Einsatzszenario durchzuführen.²⁰⁷ Dafür sind zwei Konnektoren erforderlich.

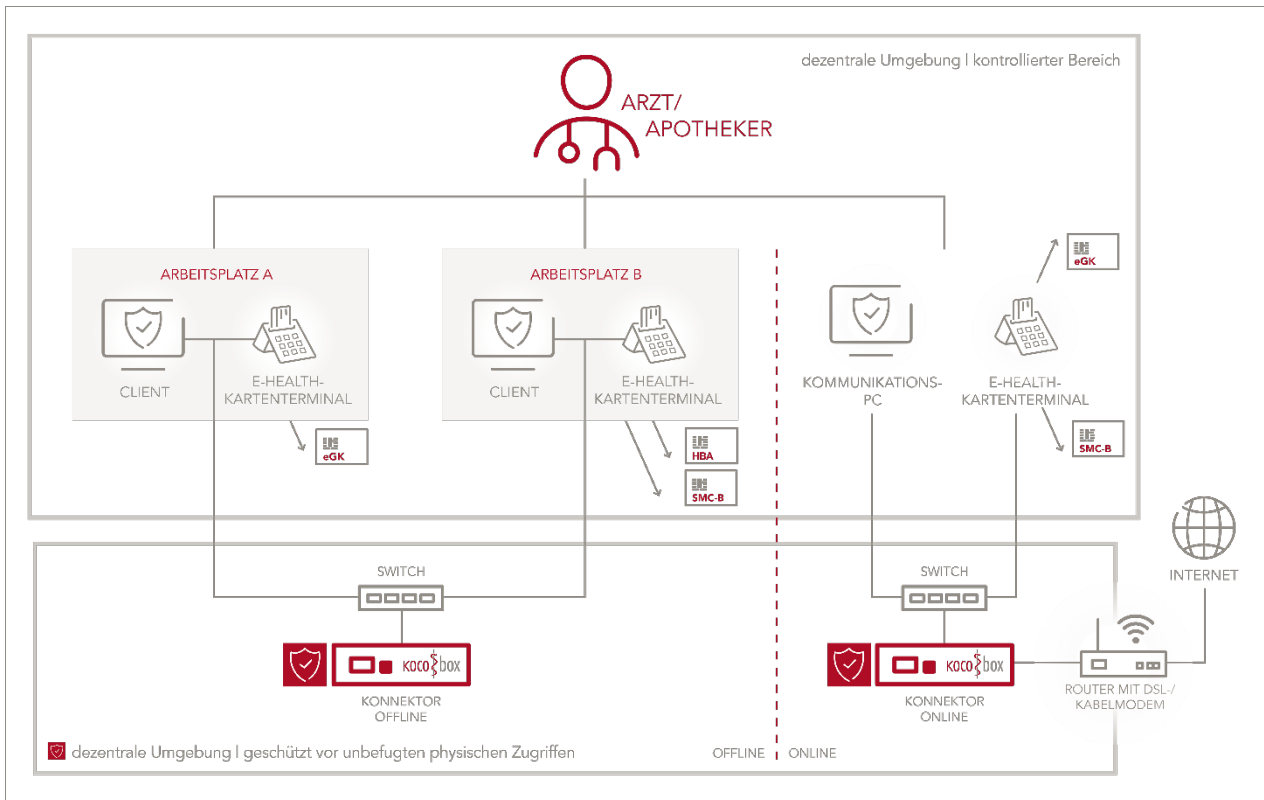


Abbildung 137: Einsatz der KoCoBox MED+ Standalone mit physischer Trennung der Konnektoren

Für dieses Szenario sind zwei Konnektoren vorgesehen, ein Offline-Konnektor und ein Online-Konnektor (siehe Abbildung).

Der Offline-Konnektor wird – wie bereits beschrieben – konfiguriert:

- Im Bereich *Verwaltung* wird der *Leistungsumfang ONLINE* deaktiviert (nicht aktiviert).
- Bei der Netzwerkkonfiguration ist der Anbindungsmodus parallel, der *WAN Adapter Modus* ist also ausgeschaltet.

²⁰⁷ Die Illustration für den Einsatz des Konnektors Standalone mit physischer Trennung lehnt sich an die Szenarien in den Konnektor-Spezifikationen an. Siehe [gemSpec_Kon], Anhang K.

Verwaltung der Leistungsumfänge

Leistungsumfang ONLINE: aktiviert nicht aktiviert

Leistungsumfang Signaturanwendungskomponente: aktiviert nicht aktiviert

Betrieb als Standalone Konnektor: aktiviert nicht aktiviert

Abbildung 138: Einstellungen bei physischer Trennung im Konnektor

Den Online-Konnektor im Standalone-Szenario konfigurieren Sie wie folgt:

- Im Bereich *Verwaltung* wird der *Betrieb als Standalone Konnektor* aktiviert.²⁰⁸
- Bei der *Netzwerkkonfiguration* ist der Anbindungsmodus seriell (‘in Reihe’), der *WAN Adapter Modus* ist also eingeschaltet.



Bei einem längerfristigen Betrieb in diesem Szenario werden die CRL und TSL des Konnektors ungültig. Dies wird über die Betriebszustandsmeldungen EC_CRL_Expiring, EC_TSL_Expiring, EC_TSL_Trust_Anchor_Expiring angezeigt. Um die Funktionalität des Konnektors aufrechtzuerhalten, kann ein Benutzer in der Rolle *Supporter*, *Admin* oder *SuperAdmin* rechtzeitig eine aktuelle CRL oder TSL in den Konnektor importieren (siehe oben im Abschnitt Import von TSL/CRL). Die entsprechende CRL oder TSL kann alternativ über <https://download.tsl.ti-dienste.de/> bzw. <http://download.crl.ti-dienste.de/crl/> bezogen werden.


²⁰⁸ In diesem Fall startet der Konnektor automatisch einen Abgleich der Versichertenstammdaten, wenn eine eGK in ein angeschlossenes Kartenterminal gesteckt wird.

9.2 Fehlermeldungen

9.2.1 Herstellerspezifische Fehlermeldungen

Die folgende Tabelle gibt eine Übersicht sämtlicher herstellerspezifischer Fehlermeldungen.


| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|---|------------|--|
| 20002 | Error | Security | Erforderliche Rollen sind nicht im Zertifikat vorhanden | Konnektor | Eine notwendige Rolle zur Durchführung einer Operation ist nicht im Zertifikat vorhanden. |
| 20003 | Error | Security | Das Zertifikat befindet sich nicht im Vertrauensraum. | Konnektor | Das zu prüfende CA-Zertifikat ist nicht in der im Konnektor geladenen TSL. |
| 20004 | Error | Technical | Der manuelle Import der CRL-Datei schlägt fehl. | Konnektor | Das Dateiformat der CRL ist ungeeignet. Die übergebene Datei ist zu prüfen. |
| 20005 | Error | Security | Karte entspricht nicht der Spezifikation | Konnektor | Die Informationen zur gesteckten Karte entsprechen nicht der aktuell gültigen Spezifikation. |
| 20007 | Error | Security | Die Extraktion der Daten aus der heruntergeladenen TSL-Datei schlägt fehl. | Konnektor | Informationen für den Zertifikatsdienst, die der aktuell zu ladenden TSL entnommen werden sollen, stehen nicht bereit. |
| 20009 | Error | Technical | Das VersichertenDatenTemplate der KVK enthält ungültige Daten. | Konnektor | Die gesteckte KVK enthält nicht valide Versichertendaten. |
| 20010 | Warning | Security | Das Gültigkeitsdatum der KVK ist überschritten. | Konnektor | Das Gültigkeitsdatum der KVK ist überschritten. |
| 20011 | Error | Technical | Die De-/Registrierung am VPN-Zugangsdienst ist fehlgeschlagen. | Konnektor | Die De-/Registrierung am VPN-Zugangsdienst ist fehlgeschlagen. |
| 20012 | Error | Technical | Der Anzeigetext ist zu lang. | Konnektor | Der übergebene DisplayText ist für das angesprochene Kartenterminal zu lang und muss kürzer sein. Hier ist eine Abstimmung mit |


| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|---|------------|---|
| | | | | | dem Hersteller des Clientsystems erforderlich. |
| 20014 | Error | Technical | Der Kartentyp entspricht nicht der Vorbedingung der Operation ReadVSD. | Konnektor | Der Kartentyp entspricht nicht der Vorbedingung der Operation ReadVSD. |
| 20015 | Error | Technical | Keine Response-APDU erhalten | Konnektor | Das durch den Konnektor gesendete Kommando an die Karte bzw. das Kartenterminal enthält keine Antwort. |
| 20016 | Error | Technical | Der Name der Gegenstelle kann nicht aufgelöst werden. | Konnektor | Die DNS-Adresse der Gegenstelle kann nicht aufgelöst werden. |
| 20017 | Info | Technical | Card2Card Authentisierung wurde durch 'resetCard' abgebrochen. | Konnektor | Ein Zurücksetzen der Karte während der C2C-Authentifizierung verhindert die erfolgreiche Ausführung. |
| 20018 | Error | Technical | Für den Mandanten ist keine SM-B hinterlegt. | Konnektor | Dem im Kontext verwendeten Mandanten ist im Infomodell keine SM-B zugeordnet. |
| 20019 | Error | Security | Ungültiger SignaturePolicyIdentifier | Konnektor | Bei der Operation wurde ein nicht gültiger SignaturePolicyIdentifier angegeben. |
| 20020 | Error | Technical | Angegebene IP-Adresse gehört zu einem anderen Port als der, der übergeben wurde. Angaben zum Port prüfen. | Konnektor | Eine Konfiguration auf der AdminGUI enthält ungültige Parameterwerte und kann nicht gespeichert werden. |
| 20023 | Error | Technical | Karte antwortet mit einer spezifischen Fehlermeldung (COS): {0} | Konnektor | Karte antwortet mit einer spezifischen Fehlermeldung, Fehlercode <Kartenfehlercode gemäß [gemSpec_COS]> |
| 20024 | Error | Technical | Die Echtheitsprüfung der eGK ist fehlgeschlagen. | Konnektor | Ein Fehler während der Echtheitsprüfung ist aufgetreten. |
| 20025 | Warning | Technical | Die maximale Bearbeitungszeit für die | Konnektor | Die Operation |

| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|---|------------|---|
| | | | Operation ist überschritten. | | ReadVSD/AutoUpdateVSD dauert länger als der konfigurierte Wert von MAXTIME_VSDM. |
| 20026 | Warning | Technical | Der Timeout für VSDM Dienste ist erreicht. | Konnektor | Der Konnektor erhält innerhalb der konfigurierten Zeit (TIMEOUT_VSDM) keine Antwort von den entfernten Systemen. |
| 20027 | Error | Security | Eine kritische Zertifikatserweiterung ist unbekannt oder enthält eine unbekannt Information. | Konnektor | Die Zertifikatsprüfung schlägt bei der Prüfung von kritischen Zertifikatserweiterungen fehl. |
| 20029 | Warning | Technical | MimeType des eingebetteten Dokuments kann nicht ermittelt werden. | Konnektor | Falls bei einer CMS-Parallelsignatur der Dokumenttyp des signierten Contents nicht ermittelt werden kann, erscheint dieser Fehler bei der Dokumentenvalidierung. Er macht die Erstellung einer Parallelsignatur nicht unmöglich, daher nur die Serverity <i>Warning</i> . |
| 20030 | Error | Security | QES-CA-Zertifikat des QES-EE-Zertifikats ist in TSL als expired gekennzeichnet. | Konnektor | Das Ablaufdatum des QES-CA-Zertifikats wurden anhand der Prüfung gegen die TSL überschritten. |
| 20031 | Error | Technical | Kartenterminal antwortet mit einer spezifischen Fehlermeldung (SICCT): {0} | Konnektor | Die angeforderte Operation kann nicht erfolgreich abgeschlossen werden, weil ein Fehler in der SICCT-Kommunikation aufgetreten ist. Der zugehörige Fehlercode kann in der SICCT Spezifikation ermittelt werden. |
| 20032 | Error | Technical | Anzahl der maximal möglichen Subscriptions (1000) ist bereits erreicht. | Konnektor | Es wurden mehr als 999 Subscriptions für Konnektor-Events |


| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|---|------------|---|
| | | | | | festgestellt, die zulässige Höchstzahl ist damit überschritten, und es können keine neuen Abonnements erteilt werden. |
| 20033 | Error | Security | Es ist keine TSL im Konnektor vorhanden. | Konnektor | Es ist keine TSL im Konnektor vorhanden. |
| 20034 | Error | Security | Für den Mandanten liegt kein VSDM_PNW_Key vor. | Konnektor | Für den Mandanten liegt kein Prüfungsnachweis-Schlüssel (PNW-Key) vor. |
| 20035 | Error | Technical | Kein Kartenobjekt zu cardHandle ermittelt. | Konnektor | Es konnte kein Kartenobjekt ermittelt werden. Die gesteckte Karte steht nicht zur Verfügung. |
| 20036 | Error | Technical | Zugriff auf gSMC-K des AK fehlgeschlagen. | Konnektor | Der Zugriff auf die gSMC-K des Anwendungskonnektors ist fehlgeschlagen. |
| 20039 | Error | Technical | Das Dokument enthält keine strukturell gültige CMS-Signatur. | Konnektor | Die im übergebenen Dokument enthaltene CMS-Signatur ist strukturell ungeeignet oder ungültig. |
| 20040 | Error | Technical | Der Admin-Client hat für den Parameter {0} einen unzulässigen Wert gesendet. | Konnektor | Der Admin-Client hat für den Parameter {0} einen unzulässigen Wert gesendet. |
| 20041 | Error | Technical | Zertifikat {0} ist auf der Karte fehlerhaft codiert. | Konnektor | Das Zertifikat ist auf der Karte fehlerhaft codiert. Es kann keine ICCSN aus der Inhaberinformation ermittelt werden. |
| 20042 | Error | Technical | Der Admin-Client hat einen unzulässigen Parameter {0} gesendet. | Konnektor | Der Admin-Client hat einen unzulässigen Parameter {0} gesendet. |
| 20043 | Error | Technical | Keine der angegebenen SubscriptionIds kann verarbeitet werden. | Konnektor | Beim Aufruf der OP RenewSubscriptions wird keine valide SubscriptionId angegeben. |
| 20045 | Warning | Technical | Einbettung von Sperrinformationen fehlgeschlagen | Konnektor | OCSF-Informationen stehen nicht für die |

| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|--|------------|--|
| | | | | | Einbettung in das zu signierende Dokument zur Verfügung. |
| 20046 | Error | Technical | Inkonsistente Bestandteile der VL im Speicher (VL, Hash, Validierungsdatum). Speicher wurde bereinigt und VL-Informationen gelöscht. | Konnektor | Es sind inkonsistente Bestandteile der Vertrauensliste im Speicher. Dieser wurde bereinigt, die VL-Informationen gelöscht. |
| 20047 | Error | Technical | Inkonsistente digitale Identität in VL. SubjectName: {0} | Konnektor | Die betreffende digitale Identität in der Vertrauensliste ist inkonsistent und kann nicht genutzt werden. |
| 20048 | Error | Technical | Die XSD-Schemavalidierung einer Antwort des {0} ist fehlgeschlagen. | Konnektor | Die XSD-Schemavalidierung einer Antwort des {0} ist fehlgeschlagen. |
| 20049 | Warning | Security | Algorithmen seit {0} als unsicher eingestuft | Konnektor | Algorithmen seit {0} werden als unsicher eingestuft. |
| 20050 | Error | Security | Algorithmus {0} ist unbekannt! | Konnektor | Der Algorithmus {0} ist unbekannt. |
| 20053 | Error | Technical | Fehler bei der PIN EGK Verifikation. VerifyPin für {0} lieferte Status {1} | Konnektor | Fehler bei der PIN-EGK-Verifikation, VerifyPin für {0} lieferte Status {1}. |
| 20055 | Warning | Technical | Endpunkt {0} zum Download der KSR-Konfigurationsdateien nicht erreichbar | Konnektor | Der TI-Dienst {0} zum Download der KSR-Konfigurationsdateien ist nicht erreichbar. |
| 20056 | Error | Security | Zertifikat enthält eine fehlerhafte Extension ({0}) | Konnektor | Das Zertifikat enthält eine fehlerhafte Erweiterung ({0}). |
| 20058 | Error | Technical | Kein Schema für Signaturrechtlinie {0} im Konnektor hinterlegt | Konnektor | Es ist kein Schema für Signaturrechtlinie {0} im Konnektor hinterlegt. |
| 20059 | Warning | Security | Signerzertifikat konnte nicht eindeutig ermittelt werden. | Konnektor | Bei der Signaturprüfung konnte unter den vorliegenden Zertifikaten kein eindeutiges Signerzertifikat |

| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|--|------------|---|
| | | | | | bestimmt werden. |
| 20060 | Error | Technical | Kombination von Signaturtyp und Signaturvariante wird nicht unterstützt. | Konnektor | Die Kombination von Signaturtyp und Signaturvariante wird nicht unterstützt. |
| 20061 | Error | Security | Signing Certificate Reference in den signedAttributes passt nicht mit der in der SignerInfo abgelegten Referenz überein. | Konnektor | Die Signing Certificate Reference in den signedAttributes passt nicht mit der in der SignerInfo abgelegten Referenz überein. |
| 20062 | Error | Technical | Import der Konfigurationsdaten erfordert statische Adresskonfiguration an allen aktiven Netzwerkadaptern. | Konnektor | Der Import der Konfigurationsdaten erfordert statische IP-Adresskonfiguration an allen aktiven Netzwerkadaptern. |
| 20063 | Error | Security | Signaturrichtlinie {0} nicht eingehalten. | Konnektor | Die im Dokument oder Request übergebene Signaturrichtlinie wurde nicht vollständig eingehalten. |
| 20064 | Error | Technical | Keine Signaturrichtlinie zu URI {0} gefunden. | Konnektor | Die im Dokument oder Request übergebene Signaturrichtlinie ist dem Konnektor unbekannt. |
| 20065 | Error | Technical | Änderung der PIN nicht möglich: PIN-Schutz ist deaktiviert. | Konnektor | ChangePin wurde auf einer PIN-Referenz aufgerufen, deren PIN-Schutz deaktiviert (Status DISABLED) ist. Zum Ändern der PIN ist diese vorher zu aktivieren (EnablePin). |
| 20066 | Error | Technical | Struktur der XML-Signatur ist fehlerhaft. | Konnektor | Die Struktur einer XML-Signatur im Dokument ist nicht schema-valide, die mathematische Prüfung der Signatur |

| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|---|------------|--|
| | | | | | kann deswegen nicht durchgeführt werden. |
| 20067 | Error | Security | OCSP-Archive-Cutoff für geprüftes Zertifikat überschritten. | Konnektor | Ein OCSP-Responder hat für ein QES-Zertifikat angezeigt, dass er keine verlässlichen Statusinformationen für dieses Zertifikat vorhält. |
| 20069 | Error | Technical | Kartenterminal mit gleichem Hostname bereits in der Liste der Kartenterminals vorhanden. Bitte Hostname des Kartenterminals ändern. | Konnektor | Konnektor TIP1-A_4557 Eindeutigkeit HOSTNAME verletzt. |
| 20070 | Warning | Security | Der Verification Report kann auf Grund fehlender Daten durch einen vorzeitigen Abbruch der Prüfung nicht (vollständig) erstellt werden. | Konnektor | Durch einen schwerwiegenden Fehler bei der Signaturverifikation, i.d.R. bei unstimmmigen Statusinformationen zum Signaturzertifikat, wird die weitere Prüfung gemäß Common-PKI abgebrochen. Die erforderlichen Daten für einen korrekten Report liegen dann nicht vor. |
| 20071 | Error | Security | BNetzA-VL ist nicht vorhanden. | Konnektor | Entsteht, wenn keine BNetzA-VL im Konnektor vorhanden ist und eine Zertifikatsprüfung auf Zertifikate in der BNetzA-VL zugreifen muss. |
| 20072 | Error | Security | Das QES-EE-Zertifikat ist ungültig. Es wurde außerhalb des Gültigkeitszeitraums der QES-CA ausgestellt. | Konnektor | Wird ausgelöst, wenn bei der Prüfung eines QES-Signer-Zertifikats festgestellt wird, dass es vor oder nach dem Gültigkeitszeitraum der ausstellenden QCA ausgestellt wurde. |
| 20073 | Warning | Security | Der im Request übergebene MimeType {0} stimmt nicht mit dem in der | Konnektor | Der im Request übergebene MimeType |

| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|---|----------------|---|
| | | | Signatur hinterlegten mimeType {1} überein. | | {0} stimmt nicht mit dem in der Signatur hinterlegten MimeType {1} überein. |
| 20075 | Error | Technical | Das Signaturschema RSASSA-PSS wird nicht von HBA-Vorläuferkarten unterstützt. | Konnektor | Das Signaturschema RSASSA-PSS wird nicht von HBA-Vorläuferkarten unterstützt. |
| 20076 | Error | Technical | Die CMS-SignerInformation ist nicht wohlgeformt. | Konnektor | Prüfen Sie das signierte Dokument auf korrekte Formattierung, wenden Sie sich ggf. sich an den Herausgeber. |
| 20077 | Error | Security | Algorithmenparameter können nicht ermittelt werden. | Konnektor | Das signierte Dokument wurde mit einem ungeeigneten Algorithmus erstellt. Wenden Sie sich an den Herausgeber. |
| 20078 | Error | Technical | Es wurden nicht valide Update-Informationen erkannt und entfernt. | Konnektor | Führen Sie die Datenaktualisierung erneut aus und kontaktieren Sie ggf. Ihren Support. |
| 20079 | Error | Security | Die Anzahl der zulässigen Kartenterminals wurde überschritten, es wird eine Service Discovery DOS Attacke vermutet. | Konnektor | Die Anzahl der zulässigen Kartenterminals wurde überschritten, es wird eine Service Discovery DOS Attacke vermutet. |
| 20080 | Error | Security | Kartenterminal <x> mit MAC-Adresse <y> wurde entfernt, da der Name nicht spezifikationskonform ist. | Kartenterminal | Das Kartenterminal hat sich mit einem ungültigen Namen beim Konnektor gemeldet. Prüfen Sie, ob die Namensvergabe für das Kartenterminal den Bedingungen im Kapitel Kartenterminaldienst entspricht. |
| 20081 | Warning | Technical | Es können keine Konfigurationsparameter der Komfortsignatur geändert werden, wenn die TLS Client-Authentisierung | Konnektor | Es wurde versucht, die Komfortsignatur im Signaturdienst ohne eine aktive |

| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|--|------------|---|
| | | | ausgeschaltet ist. | | TLS-Client-Authentisierung einzuschalten. |
| 20082 | Warning | Technical | Die TLS Client-Authentisierung kann nicht ausgeschaltet werden, solange der Leistungsumfang Komfortsignatur eingeschaltet ist. | Konnektor | Es wurde versucht die TLS-Client-Authentisierung auszuschalten, während die Komfortsignatur im Signatordienst aktiviert ist. |
| 20083 | Error | Technical | Das ECC Zertifikat kann nicht erzeugt werden, da kein ECC fähiges Schlüsselmaterial auf der GSMCK vorhanden ist. | Konnektor | Für die Ausstellung von ECDSA-Zertifikaten ist eine gSMC-K mit ECC-Unterstützung erforderlich. |
| 20084 | Warning | Technical | Empfängerzertifikat <x> liegt nicht vor. | Konnektor | Bei der Entschlüsselung von Daten konnte kein Empfängerzertifikat ermittelt werden. |
| 20085 | Warning | Technical | Keine verschlüsselten Daten für <x>. | Konnektor | Für den angegebenen Empfänger wurden die Daten nicht verschlüsselt. |
| 20086 | Warning | Security | Entschlüsselung für einen Empfänger schlägt fehl. Weitere Empfänger werden geprüft. | Konnektor | Die Entschlüsselung ist für einen der ermittelten Empfänger fehlgeschlagen. Die Entschlüsselung wird für weitere Empfänger fortgesetzt. |
| 20087 | Error | Security | Das End-Entity-Zertifikat wurde in der CertHash-Erweiterung mit einem falschen Algorithmus gehasht. | Konnektor | Das End-Entity-Zertifikat wurde in der CertHash-Erweiterung mit einem falschen Algorithmus gehasht. |
| 20093 | Error | Technical | kein PKCS#12 File | Konnektor | Der interne PKCS#12-KeyStore kann nicht geladen werden. |
| 20094 | Error | Technical | nicht unterstützter Algorithmus/Schlüssellänge | Konnektor | Der Algorithmus/die Schlüssellänge wird nicht unterstützt. |
| 20095 | Error | Technical | Zertifikatslaufzeit größer 5 Jahre | Konnektor | Es wurde versucht, |

| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|---|------------|---|
| | | | | | ein Zertifikat mit einer zu großen Laufzeit in den Konnektor zu importieren. |
| 20096 | Error | Technical | Fehler bei der Prüfung der Detached-Signatur/mathematische Prüfung | Konnektor | Die Prüfung der Detached-Signatur / die mathematische Prüfung ergab einen Fehler. |
| 20097 | Error | Technical | Fehler bei der Prüfung der Detached-Signatur/Zertifikatskettenprüfung | Konnektor | Die Prüfung der Detached-Signatur / die Zertifikatskettenprüfung ergab einen Fehler. |
| 20098 | Error | Technical | Fehler bei der Prüfung der Detached-Signatur/Struktur | Konnektor | Die Prüfung der Detached-Signatur / der Struktur ergab einen Fehler. |
| 20099 | Error | Technical | Fehler beim Senden der Betriebsdaten, BDM/ERROR | Konnektor | Der Serverdienst für den Empfang der Betriebsdaten kann nicht ermittelt werden. |
| 20100 | Error | Technical | Keine Signaturrichtlinie vorhanden | Konnektor | Für die Prüfung des angegebenen Dokuments ist keine Signaturrichtlinie vorhanden. |
| 20101 | Error | Technical | Information konnte nicht aus Zertifikat gelesen werden. | Konnektor | Beim Einlesen von Kartenzertifikaten trat ein Fehler auf. Die verwendeten Smartcards sind zu prüfen. |
| 20102 | Error | Technical | Fehler beim Download der gSMC-K-Zertifikate/MGM_LU_ONLINE=Disabled | Konnektor | Der Konnektor befindet sich nicht im Onlinebetrieb. Die automatische Laufzeitverängerung kann nicht erfolgen. |
| 20103 | Error | Technical | Fehler beim Download der gSMC-K-Zertifikate/keine_TI-VPN-Verbindung | Konnektor | Der Konnektor ist nicht per VPN mit der TI verbunden. Die automatische Laufzeitverängerung kann nicht erfolgen. |
| 20104 | Error | Technical | Fehler beim Download der gSMC-K-Zertifikate/Zertifikatsdownload | Konnektor | Der Download der Daten für die |


| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|---|------------|--|
| | | | | | automatische Laufzeitverlängerung schlug fehl. |
| 20105 | Error | Technical | Fehler beim Update der gSMC-K-Zertifikate/Incomplete | Konnektor | Die Daten für die automatisch Laufzeitverlängerung wurden unvollständig heruntergeladen. |
| 20106 | Error | Technical | Fehler beim Update der gSMC-K-Zertifikate/Profile | Konnektor | Die Zertifikatsdaten für die Laufzeitverlängerung sind fehlerhaft. Sie weisen ein defektes Zertifikatsprofil auf. |
| 20107 | Error | Technical | Fehler beim Update der gSMC-K-Zertifikate/ICCSN | Konnektor | Die Zertifikatsdaten für die Laufzeitverlängerung sind fehlerhaft. Sie sind einem anderen Konnektor per ICCSN zugeordnet. |
| 20108 | Error | Technical | Fehler beim Update der gSMC-K-Zertifikate/Date | Konnektor | Die Zertifikatsdaten für die Laufzeitverlängerung sind fehlerhaft. Sie besitzen ungeeignete Datumswerte für die Gültigkeit. |
| 20109 | Error | Technical | Fehler beim Update der gSMC-K-Zertifikate/Crypt | Konnektor | Die Zertifikatsdaten für die Laufzeitverlängerung sind fehlerhaft. Sie weisen kryptografische Fehler auf, z.B. unpassende Schlüssel. |
| 20110 | Error | Technical | Fehler beim Update der gSMC-K-Zertifikate/Signature | Konnektor | Die Zertifikatsdaten für die Laufzeitverlängerung sind fehlerhaft. Die Signatur der Daten ist ungültig. |
| 20111 | Error | Technical | Fehler beim Update der gSMC-K-Zertifikate/OCSP | Konnektor | Die Zertifikatsdaten für die Laufzeitverlängerung sind fehlerhaft. Die |

| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|---|------------|--|
| | | | | | Gültigkeit konnte nicht per OCSP bestätigt werden. |
| 20500 | Info | Technical | Fehler in der Modulkonfiguration! | Konnektor | Eine Konfiguration ist fehlerhaft und wurde nicht übernommen. |
| 20501 | Info | Technical | Lokales UDP Socket zum Auslesen von Log-Nachrichten konnte nicht geöffnet werden. | Konnektor | Ein lokales UDP Socket für das interne Empfangen von Log-Nachrichten konnte nicht geöffnet werden. |
| 20502 | Error | Technical | Fehler in der Kommunikation zwischen AK und NK | Konnektor | In der Kommunikation zwischen der NK und AK JVM liegt ein Fehler vor. |
| 20503 | Error | Technical | Fehler beim Starten des RMI-Proxybundles | Konnektor | Das RMI-Proxybundle konnte wegen eines Fehlers nicht gestartet werden. |
| 20504 | Error | Technical | Ein Shell-Skript gab einen Fehlercode zurück. | Konnektor | Ein Shell-Skript zeigt einen Fehlerfall an. |
| 20505 | Error | Security | Fehler beim Prüfen des Admin-Flags | Konnektor | Das Admin-Flag konnte nicht erfolgreich geprüft werden. |
| 20601 | Info | Technical | Skript zum Starten des DNS-Servers konnte nicht ausgeführt werden. | Konnektor | Das Skript zum Starten des DNS-Servers konnte nicht ausgeführt werden. |
| 20603 | Info | Technical | Skript zum Starten des DNS-Servers gab Fehler zurück. | Konnektor | Das Skript zum Starten des DNS-Servers gab Fehler zurück. |
| 20606 | Info | Technical | Die Konfigurationsdatei des DNS-Services konnte nicht geschrieben werden. | Konnektor | Die Konfigurationsdatei des DNS-Services konnte nicht geschrieben werden. |
| 20615 | Error | Technical | Skript zum Neuladen der DNS-Server-Konfiguration konnte nicht ausgeführt werden. | Konnektor | Das Skript zum Neuladen der DNS-Server-Konfiguration konnte nicht ausgeführt werden. |
| 20616 | Error | Technical | Skript zum Neuladen der DNS-Server-Konfiguration gab Fehler zurück. | Konnektor | Das Skript zum Neuladen der DNS-Server-Konfiguration gab Fehler zurück. |

| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|---|------------|--|
| 20650 | Error | Technical | Fehler beim Schreiben des Objekts in den sicheren Speicher! | Konnektor | Das Schreiben eines Objekts in den sicheren Speicher ist mit einem Fehler gescheitert. |
| 20651 | Error | Technical | Fehler beim Lesen des Objekts aus dem sicheren Speicher! | Konnektor | Das Lesen eines Objekts aus dem sicheren Speicher ist mit einem Fehler gescheitert. |
| 20652 | Error | Technical | Fehler beim Löschen des Objekts aus dem sicheren Speicher! | Konnektor | Das Löschen eines Objekts aus dem sicheren Speicher ist mit einem Fehler gescheitert. |
| 20700 | Fatal | Technical | Fehler beim Lesen des Protokolls | Konnektor | Das Lesen des Protokolls ist mit einem Fehler gescheitert. |
| 20701 | Fatal | Technical | Fehler beim Löschen von Einträgen aus dem Protokoll | Konnektor | Das Löschen eines Protokolleintrags ist mit einem Fehler gescheitert. |
| 20704 | Error | Technical | Es fehlen benötigte Parameter. | Konnektor | Bei der Nutzung des Protokolldienst wurden zu nicht alle benötigten Parameter angegeben. |
| 20705 | Error | Technical | Sicherheitseinträge dürfen nicht gelöscht werden. | Konnektor | Ein zu löschender Eintrag ist Teil des Sicherheitsprotokolls und darf nicht gelöscht werden. |
| 20706 | Error | Technical | Das Protokoll kann aktuell nicht gelesen werden. Versuchen Sie es später noch einmal. | Konnektor | Das Protokoll kann aktuell nicht gelesen werden. |
| 20750 | Error | Technical | Zeitzone des NTP-Services konnte nicht gesetzt werden! | Konnektor | Die Zeitzone des NTP-Dienstes konnte nicht gesetzt werden. |
| 20752 | Error | Technical | NTPD-Alive-Checkskript konnte nicht gestartet werden. | Konnektor | Das Skript zur Überprüfung des NTP-Prozesses konnte nicht gestartet werden. |
| 20754 | Error | Technical | Die Synchronisation mit der Hardware-Uhr konnte nicht durchgeführt werden. | Konnektor | Die Synchronisation mit der Hardware-Uhr konnte nicht durchgeführt werden. |




| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|---|------------|--|
| 20755 | Error | Technical | Der Zeitserver konnte nicht gestoppt werden. | Konnektor | Der NTP Prozess konnte nicht gestoppt werden. |
| 20756 | Error | Technical | NTPD-Konfiguration konnte nicht geschrieben werden. | Konnektor | Die Konfiguration des NTP Programms konnte nicht geschrieben werden. |
| 20757 | Error | Technical | Skript zum Holen der Systemzeit konnte nicht ausgeführt werden. | Konnektor | Das Skript für das Auslesen der Systemzeit konnte nicht ausgeführt werden. |
| 20758 | Error | Technical | Fehler beim Konvertieren der Ausgabe des Skripts zum Holen der Systemzeit. | Konnektor | Es gibt einen Konvertierungsfehler beim Verarbeiten der Ausgabe des Skripts für das Auslesen der Systemzeit. |
| 20759 | Error | Technical | Der Zeitserver konnte nicht gestartet werden. | Konnektor | Der NTP Prozess konnte nicht gestartet werden. |
| 20760 | Error | Technical | Einmal-Synchronisierung mit den Zeitservern der TI ist fehlgeschlagen. | Konnektor | Eine angeforderte direkte Synchronisierung mit den Zeitservern der TI ist fehlgeschlagen. |
| 20761 | Warning | Technical | Manuelles Setzen der Systemzeit im Online-Modus nicht möglich. | Konnektor | Das manuelle Einstellen der Systemzeit im Online-Modus ist nicht möglich. |
| 20800 | Error | Technical | Fehler beim Ausführen des Reboots | Konnektor | Ein Fehler beim Ausführen des Reboots ist aufgetreten. |
| 20802 | Error | Technical | Fehler beim Ausführen des Cleanup Scripts | Konnektor | Während des Updates ist ein Fehler beim Skript aufgetreten, das temporäre Dateien aufräumt. |
| 20803 | Error | Technical | Fehler beim Ausführen des Ping-Skriptes | Konnektor | Das Ausführen des Skripts, das die Netzwerkverbindung zu einem System prüft, wurde mit einem Fehler abgebrochen. |
| 20804 | Error | Technical | Der zu setzende Hostname ist ungültig. | Konnektor | Der zu setzende Hostname ist ungültig. |




| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|---|------------|--|
| 20805 | Error | Technical | Fehler beim Ausführen des Skripts zum Setzen des Hostnames | Konnektor | Das Skript zum Setzen des Hostnames konnte nicht ausgeführt werden. |
| 20806 | Error | Technical | Das Skript zum Setzen des Hostnames gab einen Fehler zurück. | Konnektor | Das Skript zum Setzen des Hostnames gab einen Fehler zurück. |
| 20807 | Error | Technical | Fehler beim Validieren der FQDN | Konnektor | Die für den Erreichbarkeitstest angegebene FQDN konnte nicht als gültig validiert werden. |
| 20809 | Error | Technical | Die Hardware-ID ist nicht abrufbar. | Konnektor | Die Hardware-ID ist nicht abrufbar. |
| 20811 | Error | Technical | Fehler beim Parsen des VPN-Zertifikats. | Konnektor | Es tritt ein Fehler beim Parsen des VPN-Zertifikats auf. |
| 20812 | Error | Technical | Fehler beim Löschen der Update Dateien | Konnektor | Während des Updates tritt ein Fehler beim Skript auf, der nicht mehr benötigte Updatedateien löscht. |
| 20814 | Error | Technical | Skript zum Testen der Algorithmen konnte nicht ausgeführt werden. | Konnektor | Das Skript zum Testen der Algorithmen konnte nicht ausgeführt werden. |
| 20815 | Error | Technical | Skript zum Testen der Systemintegrität konnte nicht ausgeführt werden. | Konnektor | Das Skript zum Testen der Systemintegrität konnte nicht ausgeführt werden. |
| 20816 | Error | Technical | Skript zum Testen der Systemintegrität gab Fehler zurück. | Konnektor | Das Skript zum Testen der Systemintegrität meldet Fehler zurück. |
| 20850 | Error | Technical | Fehler beim Ausführen eines VPN-Skripts | Konnektor | Es gibt einen Fehler beim Ausführen eines VPN-Skripts. |
| 20851 | Error | Technical | Fehler beim Erstellen der VPN-Konfigurationsdateien | Konnektor | Es gibt einen Fehler beim Erstellen der VPN-Konfigurationsdateien. |
| 20852 | Error | Technical | Fehler beim Öffnen eines lokalen Sockets für die Zertifikat-Validierung | Konnektor | Beim Öffnen eines lokalen Sockets zur Zertifikatsvalidierung tritt ein Fehler auf. |
| 20855 | Error | Technical | Keine Liste verfügbarer VPN- | Konnektor | Es konnte keine Liste |

| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|---|------------|---|
| | | | Konzentratoren erhalten | | der verfügbaren VPN-Konzentratoren ermittelt werden. |
| 20857 | Error | Technical | Die VPN Verbindung konnte nicht aufgebaut werden. Bitte das Protokoll prüfen. | Konnektor | Die VPN Verbindung konnte nicht aufgebaut werden. Die genaue auslösende Bedingung wurde protokolliert. |
| 20858 | Error | Technical | Ungültiger VPN-Zustandswechsel | Konnektor | Bei Auf- oder Abbau der VPN-Verbindung trat ein Problem auf. Wenn es sich um einen Verbindungsaufbau handelt: Warten Sie ca. 5 Minuten und kontaktieren bei weiteren Fehlermeldungen den Support. |
| 20860 | Error | Technical | Fehler beim Aktualisieren der CA-Zertifikate | Konnektor | Es gibt einen Fehler beim Aktualisieren der CA-Zertifikate. |
| 20861 | Error | Technical | Der IKE-Daemon konnte nicht gestartet werden. | Konnektor | Der IKE-Prozess des VPN Programms konnte nicht gestartet werden. |
| 20900 | Error | Technical | Fehler beim Setzen der Datenrateneinschränkung | Konnektor | Es gibt einen Fehler beim Setzen der Datenratenbeschränkung. |
| 20901 | Error | Technical | Beim Auflösen eines für die Firewall-Regeln benötigten Service ist ein Fehler aufgetreten. | Konnektor | Beim Auflösen eines für die Firewall-Regeln benötigten Service ist ein Fehler aufgetreten. |
| 20902 | Info | Technical | Der DHCP Client auf diesem Adapter ist deaktiviert. | Konnektor | Es wurden DHCP-Leases angefordert, obwohl kein DHCP-Client aktiv ist. |




9.2.2 Betriebszustandsmeldungen

Im Folgenden werden die Betriebszustandsmeldungen der KoCoBox MED+ sowie die Handlungsanweisungen zu deren Behebung in einer Übersicht dargestellt.




|  Displayanzeige |  Beschreibung | Schwe- regrad |  Handlungsanweisung |
|--|---|------------------|--|
| Operational State Error EC_CardTerminal_Software_Out_Of_Date (\$ctId) | Software auf Kartenterminal (\$ctId) ist nicht aktuell. | Info | Die Firmware des Kartenterminals ist nicht mehr aktuell. Es liegt eine aktuellere Version vor, bitte nehmen Sie umgehend eine Aktualisierung auf die aktuelle Firmware vor. |
| Operational State Error EC_Connector_Software_Out_Of_Date | I_KSRS_Download::list_Updates liefert mindestens eine UpdateInformation mit einer UpdateInformation / Firmware / FWVersion > aktuelle Version der Konnektorsoftware, deren UpdateInformation/Firmware/FWPriority = „Kritisch“ | Info | Die Firmware des Konnektors ist nicht mehr aktuell. Es liegt eine aktuellere Version vor, bitte nehmen Sie umgehend eine Aktualisierung auf die aktuelle Firmware vor. |
| EC_FW_Not_Valid_Status_Blocked | Konnektor Firmware muss aktualisiert werden. Zugang zur TI momentan nicht erlaubt. | Fatal | Die Firmware des Konnektors ist nicht mehr aktuell. Es liegt eine aktuellere Version vor, bitte nehmen Sie umgehend eine Aktualisierung auf die aktuelle Firmware vor, um wieder einen Zugang zur TI zu erhalten. |
| EC_NK_Certificate_Expired | Die Zertifikate der gSMC-Ks der KoCoBox MED+ sind abgelaufen. | Fatal | Bitte nehmen Sie umgehend eine Laufzeitverlängerung vor, um wieder Zugang zur TI zu erhalten. Kontaktieren Sie ggf. Ihren Support. |
| EC_NK_Certificate_Expiring | Die Zertifikate der gSMC-Ks der KoCoBox MED+ laufen in <= 180 Tagen ab. | Warning | Die Laufzeitverlängerung steht bevor. Diese wird normal automatisch 1x pro Tag geprüft/ausgeführt, wobei dann dieser Zustand aufgehoben wird. Sollte dieser Zustand über mehrere Tage/Wochen bestehen, kontaktieren Sie bitte Ihren Support. |
| Operational State Error EC_Time_Sync_Not_Successful | Der letzte Synchronisationsversuch der Systemzeit war nicht erfolgreich. | Info | Der letzte Synchronisationsversuch der Systemzeit war nicht erfolgreich. Sollte sich der Konnektor über einen längeren Zeitraum in diesem Zustand befinden, informieren Sie bitte Ihren Support. |




|  Displayanzeige |  Beschreibung | Schwe- regrad |  Handlungsanweisung |
|--|---|------------------|--|
| EC_TLS_Client_Certificate Security | Das für die Authentisierung gegenüber dem Clientsystem konfigurierte Zertifikat hat ein Sicherheitsniveau von weniger als 120bit. | Info | Für die Konnektorauthentisierung gegenüber dem Clientsystem ist ein RSA-Zertifikat mit mindestens 3000 bit Schlüssellänge oder alternativ ein ECC-Zertifikat zu verwenden. |
| Operational State Error EC_TSL_Update_Not_Successful | Das letzte Update der TSL war nicht erfolgreich. | Info | Die letzte Aktualisierung der TSL war nicht erfolgreich. Kontaktieren Sie Ihren Support für weitere Informationen. |
| EC_TSL_Expiring | Systemzeit t mit $t > \text{NextUpdate-Element der TSL} - 7 \text{ Tage}$ und $t \leq \text{NextUpdate-Element der TSL}$ | Info | Die Gültigkeit der TSL läuft innerhalb von sieben Tagen aus. Warten Sie ab, bis die TSL online aktualisiert wird. Alternativ kann die TSL manuell von geschultem Fachpersonal (Administrator, Supporter ²⁰⁹) installiert werden. |
| EC_BNetzA_VL_not_valid | Systemzeit t mit $t > \text{NextUpdate-Element der BNetzA-VL}$ | Warning | Prüfen Sie den Aktualisierungszeitraum für die BNetzA-VL und importieren Sie ggf. manuell eine aktuelle BNetzA-VL (Downloadpunkt: https://tl.bundesnetzagentur.de/TL-DE.XML) |
| EC_TSL_Trust_Anchor_Expiring | Gültigkeit des Vertrauensankers ist noch nicht abgelaufen, läuft aber innerhalb von 30 Tagen ab. | Info | Die Gültigkeit des TI- Vertrauensankers läuft innerhalb von 30 Tagen ab. Warten Sie ab, bis der neue Vertrauensanker über die aktualisierte TSL importiert wird. Alternativ kann die aktualisierte TSL mit dem Vertrauensanker manuell von geschultem Fachpersonal (Administrator) installiert werden. |
| Operational State Error EC_LOG_OVERFLOW | Wenn im Rahmen der Regeln für die rollierende Speicherung von Logging-Einträgen Einträge gelöscht werden, die nicht älter als LOG_DAYS bzw. FM_<fmName>_LOG_DAYS sind, tritt der Fehlerzustand ein. | Warnung | Es wurden Logeinträge gelöscht, die jünger als die konfigurierte Speicherzeit waren. Als Administrator können Sie diesen Fehlerzustand zurücksetzen, indem die konfigurierte Speicherzeit angepasst wird, oder die System- |

²⁰⁹ Siehe dazu den Abschnitt Benutzerverwaltung

|  Displayanzeige |  Beschreibung | Schwe- regrad |  Handlungsanweisung |
|--|--|------------------|--|
| | | | protokolle gelöscht werden. |
| EC_CRL_Expiring | Systemzeit $t > \text{NextUpdate}$ der CRL - 3 Tage | Warnung | Die Gültigkeit der CRL läuft innerhalb von drei Tagen aus. Warten Sie ab, bis die CRL online aktualisiert wird. Alternativ kann die TSL von geschultem Fachpersonal (Administrator, Supporter ²¹⁰) installiert werden. |
| EC_Time_Sync_Pending_Warning | MGM_LU_ONLINE=Enabled und keine erfolgreiche Synchronisation der Systemzeit seit d Tagen und $d > \text{NTP_WARN_PERIOD}$ und $d \leq \text{NTP_GRACE_PERIOD}$. 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. | Warnung | Sofern sich der Konnektor im Offline-Modus befindet, stellen Sie als Administrator bitte die genaue Zeit im Bereich <i>Zeitdienst</i> manuell neu ein. Befindet sich der Konnektor im Online-Modus, stellen Sie bitte im Bereich <i>VPN</i> über den Button VPN zur TI aufbauen die VPN-Verbindung her. Die Synchronisation mit der TI geschieht dann automatisch. |
| EC_TSL_Out_Of_Date_Within_Grace_Period | Systemzeit t mit $t > \text{NextUpdate}$ -Element der TSL und $t \leq \text{NextUpdate}$ -Element der TSL + $\text{CERT_TSL_DEFAULT_GRACE_PERIOD_DAYS}$ und eine neue TSL ist nicht verfügbar | Warnung | Die Gültigkeit der TSL läuft aus. Warten Sie ab, bis die TSL online aktualisiert wird. Alternativ kann die TSL manuell von geschultem Fachpersonal (Administrator, Supporter) installiert werden. |
| Operational State Error EC_CardTerminal_Not_Available (\$ctId) | Bekanntes Kartenterminal(\$ctId) ist nicht verfügbar. | Fehler | Überprüfen Sie das Kartenterminal. |
| Operational State Error EC_No_VPN_TI_Connection | Es ist kein sicherer Kanal (VPN) in die Telematikinfrastruktur aufgebaut. Der Wert 300 sec ist abgeleitet aus der maximalen Verbindungsaufbauzeit bei einem Standortausfall des VPN-Zugangsdienstes. | Fehler | Es wurde kein sicherer VPN Kanal in die Telematikinfrastruktur aufgebaut. Sollte sich der Konnektor einen längeren Zeitraum in diesem Zustand befinden, informieren Sie bitte Ihren Support. |
| Operational State Error EC_No_VPN_SIS_Connection | Es ist kein sicherer Kanal (VPN) zu den Sicheren Internet Services (SIS) aufgebaut. Der Wert 300 sec ist abgeleitet aus der maximalen Verbindungs- | Fehler | Es wurde keine sicherer VPN Kanal zu den Sicheren Internet Services (SIS) aufgebaut. Sollte sich der Konnektor einen längeren Zeitraum in diesem |


²¹⁰ Siehe dazu den Abschnitt Benutzerverwaltung


|  Displayanzeige |  Beschreibung | Schwe- regrad |  Handlungsanweisung |
|--|--|------------------|---|
| | aufbauzeit bei einem Standortausfall des VPN-Zugangsdienstes. | | Zustand befinden, informieren Sie bitte Ihren Support. |
| Operational State Error EC_No_Online_Connection | Konnektor kann Dienste im Transportnetz nicht erreichen. | Fehler | Der Konnektor kann Dienste im Transportnetz nicht erreichen. Sollte sich der Konnektor einen längeren Zeitraum in diesem Zustand befinden, informieren Sie bitte Ihren Support. |
| Operational State Error EC_FeatureOrTUC_Not_Available (\$Dienst/\$Operation) | Dienst \$Dienst oder Operation \$Operation nicht verfügbar. | Fehler | Ein Dienst oder eine Operation ist nicht verfügbar. Informieren Sie bitte Ihren Support. |
| EC_IP_Adresses_Not_Available | Die IP-Adressen des Netzkonnektors sind nicht oder falsch gesetzt. | Fehler | Die Meldung tritt auf, solange der DHCP-Client noch keine IP-Adresse erhalten hat. Warten Sie bitte mindestens eine Minute ab, ob die Meldung verschwindet. Bleibt die Meldung länger als zwei Minuten stehen, starten Sie die KoCoBox MED+ neu, indem Sie sie für etwa eine Minute vom Stromnetz trennen und erneut anschließen. |
| Operational State Error EC_OTHER_ERROR_STATE(2) | Herstellerspezifischer Fehlerzustand | Warnung | Der Protokollspeicher des Konnektors ist zu mehr als 80 Prozent belegt. Überprüfen Sie die Protokolle und informieren Sie bitte Ihren Support. |
| Operational State Error EC_OTHER_ERROR_STATE(3) | Herstellerspezifischer Fehlerzustand | Warnung | Dieser Fehlerzustand wird aktuell nicht ausgelöst. Es ist keine Aktion nötig. |
| Operational State Error EC_OTHER_ERROR_STATE(4) | Die Anzahl der zulässigen Kartenterminals wurde überschritten, Service Discovery DOS Attacke vermutet. | Fehler | Prüfen Sie im Netzwerk, ob ein Eindringling versucht, das System zu beeinflussen. Wenden Sie sich an Ihren Support. |
| Operational State Error EC_OTHER_ERROR_STATE(5) | Es liegt ein Manipulationsverdacht der gSMC-Ks vor. | Fehler | Der Fehler erscheint auf dem Display. Die Sicherheitsmechanismen der im Konnektor eingebauten Sicherheitsmodule melden einen Angriffsversuch. Informieren Sie bitte Ihren Support. |
| EC_CRYPTOPERATION_ALARM | Gemäß TIP1-A_4597 wurde ein | Warnung | Es gibt eine auffällige Häufung |


|  Displayanzeige |  Beschreibung | Schwe- regrad |  Handlungsanweisung |
|--|---|------------------|--|
| | <p>potenzieller Missbrauch einer Kryptooperation erkannt. Nur der Administrator kann die Alarmmeldung zurücksetzen.</p> | | <p>von Aufrufen (der Alarmwert ist überschritten). Informieren Sie bitte Ihren Support.</p> |

9.2.3 Sicherheitsrelevante Fehlermeldungen der Fachmodule

Die folgende Tabelle gibt eine Übersicht fachmodulspezifischer sicherheitsrelevanter Fehlermeldungen.

| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|--|---------------------|---|
| 101 | Fatal | Security | Kartenfehler | Fachmodule NFD, ePA | Karte defekt, Austausch nötig |
| 106 | Fatal | Security | Zertifikat auf eGK ungültig | Fachmodul NFD, ePA | Karte ungültig, Austausch nötig |
| 107 | Fatal | Security | Zertifikat auf eGK ungültig | Fachmodul NFD | Karte ungültig, Austausch nötig |
| 5002 | Error | Security | Fachliche Rolle nicht berechtigt zur Ausführung | Fachmodul NFD | Anmeldung mit korrekter fachlicher Rolle z.B. per HBA, ist erforderlich |
| 5008 | Error | Security | Die Versicherten-ID des Notfalldatensatzes stimmt nicht mit der Versicherten-ID der eGK überein. | Fachmodul NFD | Die eGK passt nicht zu den Daten, sie muss gegen die korrekte eGK des Inhabers gewechselt werden. Evtl. ist das Infomodell zu prüfen. |
| 5011 | Error | Security | Es konnte keine Berechtigungsregel ermittelt werden. | Fachmodul NFD | Wahrscheinlich ein Lesefehler der eGK, Austausch nötig |
| 5014 | Error | Security | Das Primärsystem hat keine Zugriffsberechtigung auf die eGK. | Fachmodul NFD | Das Infomodell ist zu prüfen. Ggf. ist der Support zu kontaktieren. |
| 5015 | Error | Security | Das Primärsystem hat keine Zugriffsberechtigung auf den HBA/die SMC-B. | Fachmodul NFD | Das Infomodell ist zu prüfen. Ggf. ist der Support zu kontaktieren. |
| 5016 | Error | Security | Die gegenseitige Authentisierung von eGK und HBA/SMC-B (Card-to-Card-Authentisierung) ist gescheitert. | Fachmodul NFD | Eine der beteiligten Karten ist nicht für die Verwendung geeignet. Ggf. liegt ein Defekt vor. Dann ist ein Tausch nötig. |
| 5017 | Error | Security | Der Notfalldatensatz ist nicht valide. | Fachmodul NFD | Der Datensatz auf der eGK ist defekt, er ist neu anzulegen, ggf. ist ein Austausch der eGK nötig. |

| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|---|----------------|--|
| 5018 | Error | Security | Die Signaturprüfung konnte nicht durchgeführt werden. | Fachmodul NFDM | Der Datensatz auf der eGK ist defekt, er ist neu anzulegen, ggf. ist ein Austausch der eGK nötig. |
| 5019 | Error | Security | PIN-Verifikation gescheitert | Fachmodul NFDM | Die PIN-Eingabe ist mit der korrekten PIN zu wiederholen. |
| 5108 | Error | Security | Die Versicherten-ID des Datensatz „Persönliche Erklärungen“ stimmt nicht mit der Versicherten-ID der eGK überein. | Fachmodul NFDM | Die eGK passt nicht zu den Daten, sie muss gegen die korrekte eGK des Inhabers gewechselt werden. Evtl. ist das Infomodell zu prüfen. |
| 5114 | Error | Security | Der Datensatz „Persönliche Erklärungen“ ist nicht valide. | Fachmodul NFDM | Der Datensatz auf der eGK ist defekt, dieser ist neu anzulegen, ggf. ist ein Austausch der eGK nötig. |
| 5501 | Warning | Security | Prüfung der qualifizierten elektronischen Signatur unvollständig oder nicht durchführbar bzw. Signatur ungültig | Fachmodul NFDM | Die gelesenen Daten der eGK sind nicht qualifiziert prüfbar. Eine Wiederholung des Vorgangs ist ratsam. Bei wiederholtem Scheitern bitte den Support kontaktieren. |
| 5504 | Error | Security | Signatur des Notfalldatensatzes ungültig; Prüfung der Hashwertkette bzw. kryptographische Prüfung der Signatur fehlgeschlagen | Fachmodul NFDM | Der Datensatz auf der eGK ist defekt, dieser ist neu anzulegen, ggf. ist ein Austausch der eGK nötig. |
| 5505 | Error | Security | Die Prüfung des Signaturzertifikats des Notfalldatensatzes auf Konformität zu einer qualifizierten elektronischen Signatur ist gescheitert. | Fachmodul NFDM | Die eGK passt nicht zu den Daten des Systems, sie muss gegen die korrekte eGK des Inhabers gewechselt werden. Evtl. ist das Infomodell zu prüfen. |

| Fehlercode | Schweregrad | Fehlertyp |  Fehlermeldung | Komponente | Auslösende Bedingung |
|------------|-------------|-----------|--|----------------|--|
| 6049 | Error | Security | Smartcard nicht freigeschaltet, Kartentyp = HBA/SMC-B bzw. eGK | Fachmodul AMTS | Prüfen, ob die PIN der betreffenden Karte gesperrt ist, Entsperren ist erforderlich. |
| 6052 | Error | Security | Verbindungsfehler zwischen Karten | Fachmodul AMTS | Die Card-to-Card-Authentisierung zwischen den Karten ist fehlgeschlagen. Prüfen Sie die Konfiguration des Infomodells. |
| 6063 | Error | Security | eGK gesperrt | Fachmodul AMTS | Karte gesperrt, Austausch gegen gültige Karte nötig, Lesen der alten Karte ist möglich. |
| 7202 | Error | Security | Verbindung zum Aktensystem fehlgeschlagen | Fachmodul ePA | Die Verbindung zum SGD bzw. der Dokumentenverwaltung schlug fehl. Kontaktieren Sie den Support. |
| 7203 | Error | Security | Die gegenseitige Authentisierung von eGK und SMC-B (Card-to-Card-Authentisierung) ist gescheitert. | Fachmodul ePA | Es konnte keine geschützte Verbindung zwischen der eGK und der SM-B aufgebaut werden. Prüfen Sie die Gültigkeit und/oder Funktion der Karten. |
| 7214 | Error | Security | Das Schlüsselmaterial der Akte entspricht nicht den Sicherheitsanforderungen. | Fachmodul ePA | Beim Generieren des Akten- oder Kontextschlüssels trat ein Fehler auf. Wiederholen Sie die Operation. Tritt der Fehler erneut auf, kontaktieren Sie den Support. |
| 7221 | Error | Security | Zertifikat auf SMC-B ungültig | Fachmodul ePA | Die Verbindung mit dem SGD wurde abgelehnt, weil die SM-B ein ungültiges Zertifikat aufweist. Prüfen Sie die Gültigkeit der SM-B. |

9.3 Ergänzende technische Informationen

In diesem Abschnitt finden Sie weitere Informationen zu technischen Details.

9.3.1 Startverhalten

Die KoCoBox MED+ prüft während ihres Starts verschiedene Systemparameter. Mit dem Abschluss dieser Prüfungen und der Aufnahme der internen Dienste wird der Zugang zur Managementschnittstelle aktiviert.

Unter bestimmten Umständen kann es vorkommen, dass dieser Vorgang länger andauernde interne Operationen der KoCoBox MED+ beinhaltet, z.B. wenn die Protokollspeicher gefüllt sind und die ältesten Protokolleinträge rollierend gelöscht werden. Während dieser Zeit ist die Managementschnittstelle inaktiv. Zudem reagiert der Konnektor nicht auf manuelle Eingaben.



Warten Sie das Ende des Vorgangs ab.



Wir raten vom Neustarten des Geräts durch Trennung von der Stromversorgung ab, da dies den Vorgang insgesamt verzögert.

9.3.2 Versionsangaben zu gesteckten Karten im CETP-Event

Im CETP-Event zu einer gesteckten Karte wird der Parameter CardVersion mit ausgegeben.

Dieser setzt sich aus maximal drei Versionsnummern zusammen:

- Die erste Versionsnummer (z.B. 3.0.4) beschreibt die COSVersion der Karte.
- Die zweite Versionsnummer (z.B. 4.0.0) beschreibt die ObjectSystemVersion.
- Die dritte Versionsnummer (z.B. 3.5.0) beschreibt die DataStructureVersion.²¹¹

²¹¹ Diese Versionsangabe muss nicht immer vorhanden sein.

9.3.3 Infomodell und XML-Schema

Im Folgenden werden ergänzend zum oberen Abschnitt Infomodell ein exemplarisches Infomodell und das dazugehörige XML-Schema dargestellt.

Infomodell

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

    <xs:element name="infomodell-statisch-aus-konfiguration">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="mandant" type="mandant" minOccurs="0"
maxOccurs="unbounded"/>
                <xs:element name="clientsystem" type="clientsystem" minOccurs="0"
maxOccurs="unbounded"/>
                <xs:element name="arbeitsplatz" type="arbeitsplatz" minOccurs="0"
maxOccurs="unbounded"/>
                <xs:element name="kartenterminal" type="kartenterminal" minOccurs="0"
maxOccurs="unbounded"/>
                <xs:element name="smb" type="smb" minOccurs="0"
maxOccurs="unbounded"/>
                <xs:element name="clientsystem-zu-mandant" type="clientsystem-zu-mandant"
minOccurs="0" maxOccurs="unbounded"/>
                <xs:element name="arbeitsplatz-zu-mandant" type="arbeitsplatz-zu-mandant"
minOccurs="0" maxOccurs="unbounded"/>
                <xs:element name="kartenterminal-zu-mandant" type="kartenterminal-zu-
mandant" minOccurs="0" maxOccurs="unbounded"/>
                <xs:element name="smb-zu-mandant" type="smb-zu-mandant" minOccurs="0"
maxOccurs="unbounded"/>
                <xs:element name="kartenterminal-lokal-zu-arbeitsplatz" type="kartenterminal-
lokal-zu-arbeitsplatz" minOccurs="0" maxOccurs="unbounded"/>
                <xs:element name="kartenterminal-remote-zu-arbeitsplatz"
type="kartenterminal-remote-zu-arbeitsplatz" minOccurs="0" maxOccurs="unbounded"/>
                <xs:element name="remote-pin-kt" type="remote-pin-kt" minOccurs="0"
maxOccurs="unbounded"/>
                <xs:element name="cs-ap" type="cs-ap" minOccurs="0"
maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
        <xs:key name="mandantKey">
            <xs:selector xpath="mandant"/>
            <xs:field xpath="@id"/>
        </xs:key>
        <xs:keyref name="mandant-clientsystem-Keyref" refer="mandantKey">
            <xs:selector xpath="clientsystem-zu-mandant"/>
            <xs:field xpath="@mandant-id"/>
        </xs:keyref>
        <xs:keyref name="mandant-arbeitsplatz-Keyref" refer="mandantKey">
            <xs:selector xpath="arbeitsplatz-zu-mandant"/>
            <xs:field xpath="@mandant-id"/>
        </xs:keyref>
    </xs:element>
</xs:schema>
```

```

<xs:keyref name="mandant-kartenterminal-Keyref" refer="mandantKey">
  <xs:selector xpath="kartenterminal-zu-mandant"/>
  <xs:field xpath="@mandant-id"/>
</xs:keyref>
<xs:keyref name="mandant-smb-Keyref" refer="mandantKey">
  <xs:selector xpath="smb-zu-mandant"/>
  <xs:field xpath="@mandant-id"/>
</xs:keyref>
<xs:keyref name="mandant-cs-ap-Keyref" refer="mandantKey">
  <xs:selector xpath="cs-ap"/>
  <xs:field xpath="@mandant-id"/>
</xs:keyref>
<xs:keyref name="mandant-remote-pin-kt-Keyref" refer="mandantKey">
  <xs:selector xpath="remote-pin-kt"/>
  <xs:field xpath="@mandant-id"/>
</xs:keyref>
<xs:key name="clientsystemKey">
  <xs:selector xpath="clientsystem"/>
  <xs:field xpath="@id"/>
</xs:key>
<xs:keyref name="clientsystem-mandant-Keyref" refer="clientsystemKey">
  <xs:selector xpath="clientsystem-zu-mandant"/>
  <xs:field xpath="@clientsystem-id"/>
</xs:keyref>
<xs:keyref name="clientsystem-cs-ap-Keyref" refer="clientsystemKey">
  <xs:selector xpath="cs-ap"/>
  <xs:field xpath="@clientsystem-id"/>
</xs:keyref>
<xs:keyref name="clientsystem-remote-pin-kt-Keyref" refer="clientsystemKey">
  <xs:selector xpath="remote-pin-kt"/>
  <xs:field xpath="@clientsystem-id"/>
</xs:keyref>
<xs:key name="arbeitsplatzKey">
  <xs:selector xpath="arbeitsplatz"/>
  <xs:field xpath="@id"/>
</xs:key>
<xs:keyref name="arbeitsplatz-mandant-Keyref" refer="arbeitsplatzKey">
  <xs:selector xpath="arbeitsplatz-zu-mandant"/>
  <xs:field xpath="@arbeitsplatz-id"/>
</xs:keyref>
<xs:keyref name="arbeitsplatz-kartenterminal-lokal-Keyref" refer="arbeitsplatzKey">
  <xs:selector xpath="kartenterminal-lokal-zu-arbeitsplatz"/>
  <xs:field xpath="@arbeitsplatz-id"/>
</xs:keyref>
<xs:keyref name="arbeitsplatz-kartenterminal-remote-Keyref" refer="arbeitsplatzKey">
  <xs:selector xpath="kartenterminal-remote-zu-arbeitsplatz"/>
  <xs:field xpath="@arbeitsplatz-id"/>
</xs:keyref>
<xs:keyref name="arbeitsplatz-cs-ap-Keyref" refer="arbeitsplatzKey">
  <xs:selector xpath="cs-ap"/>
  <xs:field xpath="@arbeitsplatz-id"/>
</xs:keyref>
<xs:key name="kartenterminalKey">

```

```

        <xs:selector xpath="kartenterminal"/>
        <xs:field xpath="@id"/>
    </xs:key>
    <xs:keyref name="kartenterminal-mandant-Keyref" refer="kartenterminalKey">
        <xs:selector xpath="kartenterminal-zu-mandant"/>
        <xs:field xpath="@kartenterminal-id"/>
    </xs:keyref>
    <xs:keyref name="kartenterminal-lokal-arbeitsplatz-Keyref" refer="kartenterminalKey">
        <xs:selector xpath="kartenterminal-lokal-zu-arbeitsplatz"/>
        <xs:field xpath="@kartenterminal-id"/>
    </xs:keyref>
    <xs:keyref name="kartenterminal-remote-arbeitsplatz-Keyref" refer="kartenterminalKey">
        <xs:selector xpath="kartenterminal-remote-zu-arbeitsplatz"/>
        <xs:field xpath="@kartenterminal-id"/>
    </xs:keyref>
    <xs:keyref name="kartenterminal-remote-pin-kt-Keyref" refer="kartenterminalKey">
        <xs:selector xpath="remote-pin-kt"/>
        <xs:field xpath="@kartenterminal-id"/>
    </xs:keyref>
    <xs:key name="smbKey">
        <xs:selector xpath="smb"/>
        <xs:field xpath="@id"/>
    </xs:key>
</xs:element>
<xs:complexType name="mandant">
    <xs:attribute name="id" type="IDType" use="required"/>
</xs:complexType>
<xs:complexType name="clientsystem-zu-mandant">
    <xs:attribute name="mandant-id" type="IDType" use="required"/>
    <xs:attribute name="clientsystem-id" type="IDType" use="required"/>
</xs:complexType>
<xs:complexType name="arbeitsplatz-zu-mandant">
    <xs:attribute name="mandant-id" type="IDType" use="required"/>
    <xs:attribute name="arbeitsplatz-id" type="IDType" use="required"/>
</xs:complexType>
<xs:complexType name="kartenterminal-zu-mandant">
    <xs:attribute name="mandant-id" type="IDType" use="required"/>
    <xs:attribute name="kartenterminal-id" type="IDType" use="required"/>
</xs:complexType>
<xs:complexType name="smb-zu-mandant">
    <xs:attribute name="mandant-id" type="IDType" use="required"/>
    <xs:attribute name="smb-id" type="IDType" use="required"/>
</xs:complexType>
<xs:complexType name="clientsystem">
    <xs:sequence minOccurs="0" maxOccurs="unbounded">
        <xs:element name="cs-auth-merkmal" type="xs:string"/>
    </xs:sequence>
    <xs:attribute name="id" type="IDType" use="required"/>
</xs:complexType>
<xs:complexType name="arbeitsplatz">
    <xs:attribute name="id" type="IDType" use="required"/>
    <xs:attribute name="xtv-id" type="IDType" use="optional"/>
</xs:complexType>

```

```

<xs:complexType name="kartenterminal-lokal-zu-arbeitsplatz">
  <xs:attribute name="arbeitsplatz-id" type="IDType" use="required"/>
  <xs:attribute name="kartenterminal-id" type="IDType" use="required"/>
</xs:complexType>
<xs:complexType name="kartenterminal-remote-zu-arbeitsplatz">
  <xs:attribute name="arbeitsplatz-id" type="IDType" use="required"/>
  <xs:attribute name="kartenterminal-id" type="IDType" use="required"/>
</xs:complexType>
<xs:complexType name="kartenterminal">
  <xs:sequence>
    <xs:element name="slot" type="kt-slot" minOccurs="1" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="id" type="IDType" use="required"/>
  <xs:attribute name="isPhysical" type="xs:boolean" default="true" use="optional"/>
</xs:complexType>
<xs:complexType name="kt-slot">
  <xs:attribute name="slotNo" type="xs:int" use="required"/>
</xs:complexType>
<xs:complexType name="smb">
  <xs:attribute name="id" type="IDType" use="required"/>
  <xs:attribute name="iccsn" use="required">
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:length value="20"/>
        <xs:pattern value="([0-9])*"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
  <xs:attribute name="isHSM" type="xs:boolean" default="false" use="optional"/>
</xs:complexType>
<xs:complexType name="cs-ap">
  <xs:attribute name="mandant-id" type="IDType" use="required"/>
  <xs:attribute name="clientsystem-id" type="IDType" use="required"/>
  <xs:attribute name="arbeitsplatz-id" type="IDType" use="required"/>
</xs:complexType>
<xs:complexType name="remote-pin-kt">
  <xs:attribute name="kartenterminal-id" type="IDType" use="required"/>
  <xs:attribute name="mandant-id" type="IDType" use="required"/>
  <xs:attribute name="arbeitsplatz-id" type="IDType" use="required"/>
</xs:complexType>
<xs:simpleType name="IDType">
  <xs:restriction base="xs:token">
    <xs:pattern value="[\d\w]{1}[\d\w\-\_]{0,63}/>
  </xs:restriction>
</xs:simpleType>
</xs:schema>

```

9.3.4 Gehärtete Schemata für XAdES-NFD

XAdES_NFDM_hardened.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- gematik revision="\main\rel_online\1" -->
<xsd:schema targetNamespace="http://uri.etsi.org/01903/v1.3.2#"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns=http://uri.etsi.org/01903/v1.3.2#
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#" elementFormDefault="qualified">
  <xsd:import namespace="http://www.w3.org/2000/09/xmldsig#"
    schemaLocation="xmldsig_NFDM_hardened.xsd"/>
  <!-- Start auxiliary types definitions: AnyType, ObjectIdentifierType,
    EncapsulatedPKIDataType and containers for time-stamp tokens -->
  <!-- Start AnyType -->
  <!-- Schemahärtung -->
  <!-- <xsd:element name="Any" type="AnyType"/>
  <xsd:complexType name="AnyType" mixed="true">
    <xsd:sequence minOccurs="0" maxOccurs="unbounded">
      <xsd:any namespace="##any" processContents="lax"/>
    </xsd:sequence>
    <xsd:anyAttribute namespace="##any"/>
  </xsd:complexType> -->
  <!-- End AnyType -->
  <!-- Start ObjectIdentifierType-->
  <!--<xsd:element name="ObjectIdentifier" type="ObjectIdentifierType"/>-->
  <xsd:complexType name="ObjectIdentifierType">
    <xsd:sequence>
      <xsd:element name="Identifier" type="IdentifierType"/>
      <!-- Schemahärtung -->
      <!--<xsd:element name="Description" type="xsd:string" minOccurs="0"/>
      <xsd:element name="DocumentationReferences" type="DocumentationReferencesType"
        minOccurs="0"/>-->
    </xsd:sequence>
  </xsd:complexType>
  <xsd:complexType name="IdentifierType">
    <xsd:simpleContent>
      <xsd:extension base="xsd:anyURI">
        <!-- Schemahärtung -->
        <!--<xsd:attribute name="Qualifier" type="QualifierType" use="optional"/>-->
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>
  <!-- Schemahärtung -->
  <!--<xsd:simpleType name="QualifierType">
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="OIDAsURI"/>
      <xsd:enumeration value="OIDAsURN"/>
    </xsd:restriction>
  </xsd:simpleType-->
  <!-- Schemahärtung -->
  <!--<xsd:complexType name="DocumentationReferencesType">
    <xsd:sequence maxOccurs="unbounded">
      <xsd:element name="DocumentationReference" type="xsd:anyURI"/>
    </xsd:sequence>
  </xsd:complexType-->
```

```

        </xsd:sequence>
    </xsd:complexType>-->
    <!-- End ObjectIdentifierType -->
    <!-- Start EncapsulatedPKIDataType -->
    <xsd:element name="EncapsulatedPKIData" type="EncapsulatedPKIDataType"/>
    <xsd:complexType name="EncapsulatedPKIDataType">
        <xsd:simpleContent>
            <xsd:extension base="xsd:base64Binary">
                <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
                <xsd:attribute name="Encoding" type="xsd:anyURI" use="optional"/>
            </xsd:extension>
        </xsd:simpleContent>
    </xsd:complexType>
    <!-- End EncapsulatedPKIDataType -->
    <!-- Start time-stamp containers types -->
    <!-- Start GenericTimeStampType -->
    <!-- Schemahärtung -->
    <!--<xsd:element name="Include" type="IncludeType"/>
    <xsd:complexType name="IncludeType">
        <xsd:attribute name="URI" type="xsd:anyURI" use="required"/>
        <xsd:attribute name="referencedData" type="xsd:boolean" use="optional"/>
    </xsd:complexType>
    <xsd:element name="ReferenceInfo" type="ReferenceInfoType"/>
    <xsd:complexType name="ReferenceInfoType">
        <xsd:sequence>
            <xsd:element ref="ds:DigestMethod"/>
            <xsd:element ref="ds:DigestValue"/>
        </xsd:sequence>
        <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
        <xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
    </xsd:complexType>-->
    <!-- Schemahärtung -->
    <!--<xsd:complexType name="GenericTimeStampType" abstract="true">
        <xsd:sequence>
            <xsd:choice minOccurs="0">
                <xsd:element ref="Include" minOccurs="0" maxOccurs="unbounded"/>
                <xsd:element ref="ReferenceInfo" maxOccurs="unbounded"/>
            </xsd:choice>
            <xsd:element ref="ds:CanonicalizationMethod" minOccurs="0"/>
            <xsd:choice maxOccurs="unbounded">
                <xsd:element name="EncapsulatedTimeStamp"
                    type="EncapsulatedPKIDataType"/>
                <xsd:element name="XMLTimeStamp" type="AnyType"/>
            </xsd:choice>
        </xsd:sequence>
        <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
    </xsd:complexType>-->
    <!-- End GenericTimeStampType -->
    <!-- Start XAdESTimeStampType -->
    <!-- Schemahärtung -->
    <!--<xsd:element name="XAdESTimeStamp" type="XAdESTimeStampType"/>
    <xsd:complexType name="XAdESTimeStampType">
        <xsd:complexContent>

```

```

        <xsd:restriction base="GenericTimeStampType">
            <xsd:sequence>
                <xsd:element ref="Include" minOccurs="0" maxOccurs="unbounded"/>
                <xsd:element ref="ds:CanonicalizationMethod" minOccurs="0"/>
                <xsd:choice maxOccurs="unbounded">
                    <xsd:element name="EncapsulatedTimeStamp"
                        type="EncapsulatedPKIDataType"/>
                    <xsd:element name="XMLTimeStamp" type="AnyType"/>
                </xsd:choice>
            </xsd:sequence>
            <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
        </xsd:restriction>
    </xsd:complexContent>
</xsd:complexType>-->
<!-- End XAdESTimeStampType -->
<!-- Start OtherTimeStampType -->
<!-- Schemahärtung -->
<!--<xsd:element name="OtherTimeStamp" type="OtherTimeStampType"/>
<xsd:complexType name="OtherTimeStampType">
    <xsd:complexContent>
        <xsd:restriction base="GenericTimeStampType">
            <xsd:sequence>
                <xsd:element ref="ReferenceInfo" maxOccurs="unbounded"/>
                <xsd:element ref="ds:CanonicalizationMethod" minOccurs="0"/>
                <xsd:choice>
                    <xsd:element name="EncapsulatedTimeStamp"
                        type="EncapsulatedPKIDataType"/>
                    <xsd:element name="XMLTimeStamp" type="AnyType"/>
                </xsd:choice>
            </xsd:sequence>
            <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
        </xsd:restriction>
    </xsd:complexContent>
</xsd:complexType>-->
<!-- End OtherTimeStampType -->
<!-- End time-stamp containers types -->
<!-- End auxiliary types definitions-->
<!-- Start container types -->
<!-- Start QualifyingProperties -->
<xsd:element name="QualifyingProperties" type="QualifyingPropertiesType"/>
<xsd:complexType name="QualifyingPropertiesType">
    <xsd:sequence>
        <xsd:element name="SignedProperties" type="SignedPropertiesType"/>
        <xsd:element name="UnsignedProperties" type="UnsignedPropertiesType"
            minOccurs="0"/>
    </xsd:sequence>
    <xsd:attribute name="Target" type="xsd:anyURI" use="required"/>
    <!-- Schemahärtung -->
    <!--<xsd:attribute name="Id" type="xsd:ID" use="optional"/>-->
</xsd:complexType>
<!-- End QualifyingProperties -->
<!-- Start SignedProperties-->
<xsd:element name="SignedProperties" type="SignedPropertiesType"/>

```



```

<xsd:complexType name="SignedPropertiesType">
  <xsd:sequence>
    <xsd:element name="SignedSignatureProperties"
      type="SignedSignaturePropertiesType"/>
    <xsd:element name="SignedDataObjectProperties"
      type="SignedDataObjectPropertiesType"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="required"/>
</xsd:complexType>
<!-- End SignedProperties-->
<!-- Start UnsignedProperties-->
<xsd:element name="UnsignedProperties" type="UnsignedPropertiesType"/>
<xsd:complexType name="UnsignedPropertiesType">
  <xsd:sequence>
    <xsd:element name="UnsignedSignatureProperties"
      type="UnsignedSignaturePropertiesType"/>
    <!-- Schemahärtung -->
    <!-- <xsd:element name="UnsignedDataObjectProperties"
      type="UnsignedDataObjectPropertiesType" minOccurs="0"/> -->
  </xsd:sequence>
  <!-- Schemahärtung -->
  <!--<xsd:attribute name="Id" type="xsd:ID" use="optional"/>-->
</xsd:complexType>
<!-- End UnsignedProperties-->
<!-- Start SignedSignatureProperties-->
<xsd:element name="SignedSignatureProperties" type="SignedSignaturePropertiesType"/>
<xsd:complexType name="SignedSignaturePropertiesType">
  <xsd:sequence>
    <xsd:element name="SigningTime" type="xsd:dateTime"/>
    <xsd:element name="SigningCertificate" type="CertIDListType"/>
    <xsd:element name="SignaturePolicyIdentifier" type="SignaturePolicyIdentifierType"/>
    <!-- Schemahärtung -->
    <!--<xsd:element name="SignatureProductionPlace"
      type="SignatureProductionPlaceType" minOccurs="0"/>
    <xsd:element name="SignerRole" type="SignerRoleType" minOccurs="0"/>-->
  </xsd:sequence>
  <!-- Schemahärtung -->
  <!--<xsd:attribute name="Id" type="xsd:ID" use="optional"/>-->
</xsd:complexType>
<!-- End SignedSignatureProperties-->
<!-- Start SignedDataObjectProperties-->
<xsd:element name="SignedDataObjectProperties" type="SignedDataObjectPropertiesType"/>
<xsd:complexType name="SignedDataObjectPropertiesType">
  <xsd:sequence>
    <xsd:element name="DataObjectFormat" type="DataObjectFormatType"/>
    <!-- Schemahärtung -->
    <!--<xsd:element name="CommitmentTypeIndication"
      type="CommitmentTypeIndicationType" minOccurs="0"
      maxOccurs="unbounded"/>
    <xsd:element name="AllDataObjectsTimeStamp" type="XAdESTimeStampType"
      minOccurs="0" maxOccurs="unbounded"/>
    <xsd:element name="IndividualDataObjectsTimeStamp" type="XAdESTimeStampType"
      minOccurs="0" maxOccurs="unbounded"/>-->
  </xsd:sequence>
  <!-- Schemahärtung -->
  <!--<xsd:attribute name="Id" type="xsd:ID" use="optional"/>-->
</xsd:complexType>

```

```

        </xsd:sequence>
        <!-- Schemahärtung -->
        <!--<xsd:attribute name="Id" type="xsd:ID" use="optional"/>-->
    </xsd:complexType>
    <!-- End SignedDataObjectProperties-->
    <!-- Start UnsignedSignatureProperties-->
    <xsd:element name="UnsignedSignatureProperties" type="UnsignedSignaturePropertiesType"/>
    <xsd:complexType name="UnsignedSignaturePropertiesType">
        <!-- Schemahärtung -->
        <!--<xsd:choice maxOccurs="unbounded">-->
        <xsd:sequence>
            <!--<xsd:element name="CounterSignature" type="CounterSignatureType"/>
            <xsd:element name="SignatureTimeStamp" type="XAdESTimeStampType"/>
            <xsd:element name="CompleteCertificateRefs" type="CompleteCertificateRefsType"/>
            <xsd:element name="CompleteRevocationRefs" type="CompleteRevocationRefsType"/>
            <xsd:element name="AttributeCertificateRefs" type="CompleteCertificateRefsType"/>
            <xsd:element name="AttributeRevocationRefs" type="CompleteRevocationRefsType"/>
            <xsd:element name="SigAndRefsTimeStamp" type="XAdESTimeStampType"/>
            <xsd:element name="RefsOnlyTimeStamp" type="XAdESTimeStampType"/>
            <xsd:element name="CertificateValues" type="CertificateValuesType"/>-->
            <xsd:element name="RevocationValues" type="RevocationValuesType" minOccurs="0"
                maxOccurs="unbounded"/>
            <!-- Schemahärtung -->
            <!--<xsd:element name="AttrAuthoritiesCertValues" type="CertificateValuesType"/>
            <xsd:element name="AttributeRevocationValues" type="RevocationValuesType"/>
            <xsd:element name="ArchiveTimeStamp" type="XAdESTimeStampType"/>-->
            <!-- Schemahärtung -->
            <!-- <xsd:any namespace="##other"/> -->
        </xsd:sequence>
        <!--</xsd:choice>-->
        <!-- Schemahärtung -->
        <!--<xsd:attribute name="Id" type="xsd:ID" use="optional"/>-->
    </xsd:complexType>
    <!-- End UnsignedSignatureProperties-->
    <!-- Start UnsignedDataObjectProperties-->
    <!-- Schemahärtung -->
    <!-- <xsd:element name="UnsignedDataObjectProperties" type="UnsignedDataObjectPropertiesType"/>
    <xsd:complexType name="UnsignedDataObjectPropertiesType">
        <xsd:sequence>
            <xsd:element name="UnsignedDataObjectProperty" type="AnyType"
                maxOccurs="unbounded"/>
        </xsd:sequence>
        <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
    </xsd:complexType> -->
    <!-- End UnsignedDataObjectProperties-->
    <!-- Start QualifyingPropertiesReference-->
    <!-- Schemahärtung -->
    <!--<xsd:element name="QualifyingPropertiesReference" type="QualifyingPropertiesReferenceType"/>
    <xsd:complexType name="QualifyingPropertiesReferenceType">
        <xsd:attribute name="URI" type="xsd:anyURI" use="required"/>
        <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
    </xsd:complexType>-->

```

```

<!-- End QualifyingPropertiesReference-->
<!-- End container types -->
<!-- Start SigningTime element -->
<xsd:element name="SigningTime" type="xsd:dateTime"/>
<!-- End SigningTime element -->
<!-- Start SigningCertificate -->
<xsd:element name="SigningCertificate" type="CertIDListType"/>
<xsd:complexType name="CertIDListType">
  <xsd:sequence>
    <xsd:element name="Cert" type="CertIDType" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="CertIDType">
  <xsd:sequence>
    <xsd:element name="CertDigest" type="DigestAlgAndValueType"/>
    <xsd:element name="IssuerSerial" type="ds:X509IssuerSerialType"/>
  </xsd:sequence>
  <!-- Schemahärtung -->
  <!--<xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>-->
</xsd:complexType>
<xsd:complexType name="DigestAlgAndValueType">
  <xsd:sequence>
    <xsd:element ref="ds:DigestMethod"/>
    <xsd:element ref="ds:DigestValue"/>
  </xsd:sequence>
</xsd:complexType>
<!-- End SigningCertificate -->
<!-- Start SignaturePolicyIdentifier -->
<xsd:element name="SignaturePolicyIdentifier" type="SignaturePolicyIdentifierType"/>
<xsd:complexType name="SignaturePolicyIdentifierType">
  <!-- Schemahärtung -->
  <!--<xsd:choice>-->
  <xsd:sequence>
    <xsd:element name="SignaturePolicyId" type="SignaturePolicyIdType"/>
  </xsd:sequence>
  <!--<xsd:element name="SignaturePolicyImplied"/>-->
  <!--</xsd:choice>-->
</xsd:complexType>
<xsd:complexType name="SignaturePolicyIdType">
  <xsd:sequence>
    <xsd:element name="SigPolicyId" type="ObjectIdentifierType"/>
    <!-- Schemahärtung -->
    <!--<xsd:element ref="ds:Transforms" minOccurs="0"/>-->
    <xsd:element name="SigPolicyHash" type="DigestAlgAndValueType"/>
    <!-- Schemahärtung -->
    <!-- <xsd:element name="SigPolicyQualifiers" type="SigPolicyQualifiersListType"
        minOccurs="0"/> -->
  </xsd:sequence>
</xsd:complexType>
<!-- Schemahärtung -->
<!-- <xsd:complexType name="SigPolicyQualifiersListType">
  <xsd:sequence>
    <xsd:element name="SigPolicyQualifier" type="AnyType" maxOccurs="unbounded"/>

```

```

        </xsd:sequence>
    </xsd:complexType>
    <xsd:element name="SPURI" type="xsd:anyURI"/>
    <xsd:element name="SPUserNotice" type="SPUserNoticeType"/>
    <xsd:complexType name="SPUserNoticeType">
        <xsd:sequence>
            <xsd:element name="NoticeRef" type="NoticeReferenceType" minOccurs="0"/>
            <xsd:element name="ExplicitText" type="xsd:string" minOccurs="0"/>
        </xsd:sequence>
    </xsd:complexType>
    <xsd:complexType name="NoticeReferenceType">
        <xsd:sequence>
            <xsd:element name="Organization" type="xsd:string"/>
            <xsd:element name="NoticeNumbers" type="IntegerListType"/>
        </xsd:sequence>
    </xsd:complexType>
    <xsd:complexType name="IntegerListType">
        <xsd:sequence>
            <xsd:element name="int" type="xsd:integer" minOccurs="0" maxOccurs="unbounded"/>
        </xsd:sequence>
    </xsd:complexType>-->
    <!-- End SignaturePolicyIdentifier -->
    <!-- Schemahärtung -->
    <!-- Start CounterSignature -->
    <!--<xsd:element name="CounterSignature" type="CounterSignatureType"/>
    <xsd:complexType name="CounterSignatureType">
        <xsd:sequence>
            <xsd:element ref="ds:Signature"/>
        </xsd:sequence>
    </xsd:complexType>-->
    <!-- End CounterSignature -->
    <!-- Start DataObjectFormat -->
    <xsd:element name="DataObjectFormat" type="DataObjectFormatType"/>
    <xsd:complexType name="DataObjectFormatType">
        <xsd:sequence>
            <xsd:element name="Description" type="xsd:string"/>
            <!-- Schemahärtung -->
            <!--<xsd:element name="ObjectIdentifier" type="ObjectIdentifierType"/>-->
            <xsd:element name="MimeType" type="xsd:string" minOccurs="0"/>
            <!-- Schemahärtung -->
            <!--<xsd:element name="Encoding" type="xsd:anyURI" minOccurs="0"/>-->
        </xsd:sequence>
        <xsd:attribute name="ObjectReference" type="xsd:anyURI" use="required"/>
    </xsd:complexType>
    <!-- End DataObjectFormat -->
    <!-- Start CommitmentTypeIndication -->
    <!-- Schemahärtung -->
    <!--<xsd:element name="CommitmentTypeIndication" type="CommitmentTypeIndicationType"/>
    <xsd:complexType name="CommitmentTypeIndicationType">
        <xsd:sequence>
            <xsd:element name="CommitmentTypeId" type="ObjectIdentifierType"/>
            <xsd:choice>
                <xsd:element name="ObjectReference" type="xsd:anyURI"

```

```

                maxOccurs="unbounded"/>
            <xsd:element name="AllSignedDataObjects"/>
        </xsd:choice>
        <xsd:element name="CommitmentTypeQualifiers"
            type="CommitmentTypeQualifiersListType" minOccurs="0"/>
    </xsd:sequence>
</xsd:complexType>-->
<!-- Schemahärtung -->
<!-- <xsd:complexType name="CommitmentTypeQualifiersListType">
    <xsd:sequence>
        <xsd:element name="CommitmentTypeQualifier" type="AnyType" minOccurs="0"
            maxOccurs="unbounded"/>
    </xsd:sequence>
</xsd:complexType> -->
<!-- End CommitmentTypeIndication -->
<!-- Start SignatureProductionPlace -->
<!-- Schemahärtung -->
<!--<xsd:element name="SignatureProductionPlace" type="SignatureProductionPlaceType"/>
<xsd:complexType name="SignatureProductionPlaceType">
    <xsd:sequence>
        <xsd:element name="City" type="xsd:string" minOccurs="0"/>
        <xsd:element name="StateOrProvince" type="xsd:string" minOccurs="0"/>
        <xsd:element name="PostalCode" type="xsd:string" minOccurs="0"/>
        <xsd:element name="CountryName" type="xsd:string" minOccurs="0"/>
    </xsd:sequence>
</xsd:complexType>-->
<!-- End SignatureProductionPlace -->
<!-- Start SignerRole -->
<!-- Schemahärtung -->
<!--<xsd:element name="SignerRole" type="SignerRoleType"/>
<xsd:complexType name="SignerRoleType">
    <xsd:sequence>
        <xsd:element name="ClaimedRoles" type="ClaimedRolesListType" minOccurs="0"/>
        <xsd:element name="CertifiedRoles" type="CertifiedRolesListType" minOccurs="0"/>
    </xsd:sequence>
</xsd:complexType>-->
<!-- Schemahärtung -->
<!-- <xsd:complexType name="ClaimedRolesListType">
    <xsd:sequence>
        <xsd:element name="ClaimedRole" type="AnyType" maxOccurs="unbounded"/>
    </xsd:sequence>
</xsd:complexType> -->
<!-- Schemahärtung -->
<!--<xsd:complexType name="CertifiedRolesListType">
    <xsd:sequence>
        <xsd:element name="CertifiedRole" type="EncapsulatedPKIDataType"
            maxOccurs="unbounded"/>
    </xsd:sequence>
</xsd:complexType>-->
<!-- End SignerRole -->
<!-- Schemahärtung -->
<!--<xsd:element name="AllDataObjectsTimeStamp" type="XAdESTimeStampType"/>
<xsd:element name="IndividualDataObjectsTimeStamp" type="XAdESTimeStampType"/>

```

```

<xsd:element name="SignatureTimeStamp" type="XAdESTimeStampType"/>-->
<!-- Start CompleteCertificateRefs -->
<!-- Schemahärtung -->
<!-- <xsd:element name="CompleteCertificateRefs" type="CompleteCertificateRefsType"/>
<xsd:complexType name="CompleteCertificateRefsType">
  <xsd:sequence>
    <xsd:element name="CertRefs" type="CertIDListType"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>-->
<!-- End CompleteCertificateRefs -->
<!-- Start CompleteRevocationRefs-->
<!-- Schemahärtung -->
<!--<xsd:element name="CompleteRevocationRefs" type="CompleteRevocationRefsType"/>
<xsd:complexType name="CompleteRevocationRefsType">
  <xsd:sequence>
    <xsd:element name="CRLRefs" type="CRLRefsType" minOccurs="0"/>
    <xsd:element name="OCSPRefs" type="OCSPRefsType" minOccurs="0"/>
    <xsd:element name="OtherRefs" type="OtherCertStatusRefsType" minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>-->
<!-- Schemahärtung -->
<!--<xsd:complexType name="CRLRefsType">
  <xsd:sequence>
    <xsd:element name="CRLRef" type="CRLRefType" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="CRLRefType">
  <xsd:sequence>
    <xsd:element name="DigestAlgAndValue" type="DigestAlgAndValueType"/>
    <xsd:element name="CRLIdentifier" type="CRLIdentifierType" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="CRLIdentifierType">
  <xsd:sequence>
    <xsd:element name="Issuer" type="xsd:string"/>
    <xsd:element name="IssueTime" type="xsd:dateTime"/>
    <xsd:element name="Number" type="xsd:integer" minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
</xsd:complexType>
<xsd:complexType name="OCSPRefsType">
  <xsd:sequence>
    <xsd:element name="OCSPRef" type="OCSPRefType" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="OCSPRefType">
  <xsd:sequence>
    <xsd:element name="OCSPIdentifier" type="OCSPIdentifierType"/>
    <xsd:element name="DigestAlgAndValue" type="DigestAlgAndValueType"
      minOccurs="0"/>
  </xsd:sequence>

```

```

</xsd:complexType>
<xsd:complexType name="ResponderIDType">
  <xsd:choice>
    <xsd:element name="ByName" type="xsd:string"/>
    <xsd:element name="ByKey" type="xsd:base64Binary"/>
  </xsd:choice>
</xsd:complexType>
<xsd:complexType name="OCSPIdentifierType">
  <xsd:sequence>
    <xsd:element name="ResponderID" type="ResponderIDType"/>
    <xsd:element name="ProducedAt" type="xsd:dateTime"/>
  </xsd:sequence>
  <xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
</xsd:complexType>-->
<!-- Schemahärtung -->
<!-- <xsd:complexType name="OtherCertStatusRefsType">
  <xsd:sequence>
    <xsd:element name="OtherRef" type="AnyType" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType> -->
<!-- End CompleteRevocationRefs-->
<!-- Schemahärtung -->
<!--<xsd:element name="AttributeCertificateRefs" type="CompleteCertificateRefsType"/>
<xsd:element name="AttributeRevocationRefs" type="CompleteRevocationRefsType"/>
<xsd:element name="SigAndRefsTimeStamp" type="XAdESTimeStampType"/>
<xsd:element name="RefsOnlyTimeStamp" type="XAdESTimeStampType"/>-->
<!-- Start CertificateValues -->
<!-- Schemahärtung -->
<!--<xsd:element name="CertificateValues" type="CertificateValuesType"/>
<xsd:complexType name="CertificateValuesType">
  <xsd:choice minOccurs="0" maxOccurs="unbounded">
    <xsd:element name="EncapsulatedX509Certificate" type="EncapsulatedPKIDataType"/>
    <xsd:element name="OtherCertificate" type="AnyType"/>
  </xsd:choice>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>-->
<!-- End CertificateValues -->
<!-- Start RevocationValues-->
<xsd:element name="RevocationValues" type="RevocationValuesType"/>
<xsd:complexType name="RevocationValuesType">
  <xsd:sequence>
    <!-- Schemahärtung -->
    <!--<xsd:element name="CRLValues" type="CRLValuesType" minOccurs="0"/>-->
    <xsd:element name="OCSPValues" type="OCSPValuesType" minOccurs="0"/>
    <!-- Schemahärtung -->
    <!-- <xsd:element name="OtherValues" type="OtherCertStatusValuesType"
      minOccurs="0"/> -->
  </xsd:sequence>
  <!-- Schemahärtung -->
  <!--<xsd:attribute name="Id" type="xsd:ID" use="optional"/>-->
</xsd:complexType>
<!-- Schemahärtung -->
<!--<xsd:complexType name="CRLValuesType">

```

```

        <xsd:sequence>
            <xsd:element name="EncapsulatedCRLValue" type="EncapsulatedPKIDataType"
                maxOccurs="unbounded"/>
        </xsd:sequence>
    </xsd:complexType>-->
    <xsd:complexType name="OCSPValuesType">
        <xsd:sequence>
            <xsd:element name="EncapsulatedOCSPValue" type="EncapsulatedPKIDataType"
                maxOccurs="unbounded"/>
        </xsd:sequence>
    </xsd:complexType>
    <!-- Schemahärtung -->
    <!-- <xsd:complexType name="OtherCertStatusValuesType">
        <xsd:sequence>
            <xsd:element name="OtherValue" type="AnyType" maxOccurs="unbounded"/>
        </xsd:sequence>
    </xsd:complexType> -->
    <!-- End RevocationValues-->
    <!-- Schemahärtung -->
    <!--<xsd:element name="AttrAuthoritiesCertValues" type="CertificateValuesType"/>
    <xsd:element name="AttributeRevocationValues" type="RevocationValuesType"/>
    <xsd:element name="ArchiveTimeStamp" type="XAdESTimeStampType"/>-->
</xsd:schema>

```

xmlsig_NFDM_hardened.xsd

```

<?xml version="1.0" encoding="utf-8"?>
<!-- gematik revision="\main\rel_online\rel_ors1\1" -->
<!-- edited with XMLSpy v2010 (http://www.altova.com) by n.n. (gematik) -->
<!DOCTYPE schema PUBLIC "-//W3C//DTD XMLSchema 200102//EN" "XMLSchema.dtd" [
    <!ATTLIST schema
        xmlns:ds CDATA #FIXED "http://www.w3.org/2000/09/xmlsig#"
    >
    <!ENTITY dsig 'http://www.w3.org/2000/09/xmlsig#'>
    <!ENTITY % p "">
    <!ENTITY % s "">
]

```

```

<!-- Schema for XML Signatures
http://www.w3.org/2000/09/xmlsig#
$Revision: 1.1 $ on $Date: 2002/02/08 20:32:26 $ by $Author: reagle $

```

Copyright 2001 The Internet Society and W3C (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved.
<http://www.w3.org/Consortium/Legal/>

This document is governed by the W3C Software License [1] as described in the FAQ [2].

[1] <http://www.w3.org/Consortium/Legal/copyright-software-19980720>

[2] <http://www.w3.org/Consortium/Legal/IPR-FAQ-20000620.html#DTD>

```

-->
<schema xmlns="http://www.w3.org/2001/XMLSchema" xmlns:ds="http://www.w3.org/2000/09/xmlsig#"
    xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"

```



```

        targetNamespace="http://www.w3.org/2000/09/xmldsig#" elementFormDefault="qualified"
        version="0.1">
<import namespace="http://uri.etsi.org/01903/v1.3.2#" schemaLocation="XAdES_NFDM_hardened.xsd"/>
<!-- Basic Types Defined for Signatures -->
<simpleType name="CryptoBinary">
  <restriction base="base64Binary"/>
</simpleType>
<!-- Start Signature -->
<element name="Signature" type="ds:SignatureType"/>
<complexType name="SignatureType">
  <sequence>
    <element ref="ds:SignedInfo"/>
    <element ref="ds:SignatureValue"/>
    <element ref="ds:KeyInfo"/>
    <element ref="ds:Object" minOccurs="1" maxOccurs="2"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
<element name="SignatureValue" type="ds:SignatureValueType"/>
<complexType name="SignatureValueType">
  <simpleContent>
    <extension base="base64Binary">
      <attribute name="Id" type="ID" use="optional"/>
    </extension>
  </simpleContent>
</complexType>
<!-- Start SignedInfo -->
<element name="SignedInfo" type="ds:SignedInfoType"/>
<complexType name="SignedInfoType">
  <sequence>
    <element ref="ds:CanonicalizationMethod"/>
    <element ref="ds:SignatureMethod"/>
    <element ref="ds:Reference" minOccurs="3" maxOccurs="3"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
<element name="CanonicalizationMethod" type="ds:CanonicalizationMethodType"/>
<complexType name="CanonicalizationMethodType" mixed="true">
  <!-- Schemahärtung -->
  <!--<sequence>
    <any namespace="##any" minOccurs="0" maxOccurs="unbounded"/>
    (0,unbounded) elements from (1,1) namespace
  </sequence>-->
  <attribute name="Algorithm" type="anyURI" use="required"/>
</complexType>
<element name="SignatureMethod" type="ds:SignatureMethodType"/>
<complexType name="SignatureMethodType" mixed="true">
  <!-- Schemahärtung -->
  <!--<sequence>
    <element name="HMACOutputLength" type="ds:HMACOutputLengthType" minOccurs="0"/>
    <any namespace="##other" minOccurs="0" maxOccurs="unbounded"/>
    (0,unbounded) elements from (1,1) external namespace
  </sequence>-->

```

```

    <attribute name="Algorithm" type="anyURI" use="required"/>
</complexType>
<!-- Start Reference -->
<element name="Reference" type="ds:ReferenceType"/>
<complexType name="ReferenceType">
  <sequence>
    <element ref="ds:Transforms"/>
    <element ref="ds:DigestMethod"/>
    <element ref="ds:DigestValue"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
  <attribute name="URI" type="anyURI" use="optional"/>
  <attribute name="Type" type="anyURI" use="optional"/>
</complexType>
<element name="Transforms" type="ds:TransformsType"/>
<complexType name="TransformsType">
  <sequence>
    <element ref="ds:Transform"/>
  </sequence>
</complexType>
<element name="Transform" type="ds:TransformType"/>
<complexType name="TransformType" mixed="true">
  <!-- Schemahärtung -->
  <!--<choice minOccurs="0" maxOccurs="unbounded">
    <any namespace="##other" processContents="lax"/>
    (1,1) elements from (0,unbounded) namespaces
    <element name="XPath" type="string"/>
  </choice>-->
  <attribute name="Algorithm" type="anyURI" use="required"/>
</complexType>
<!-- End Reference -->
<element name="DigestMethod" type="ds:DigestMethodType"/>
<complexType name="DigestMethodType" mixed="true">
  <!-- Schemahärtung -->
  <!--<sequence>
    <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
  </sequence>-->
  <attribute name="Algorithm" type="anyURI" use="required"/>
</complexType>
<element name="DigestValue" type="ds:DigestValueType"/>
<simpleType name="DigestValueType">
  <restriction base="base64Binary"/>
</simpleType>
<!-- End SignedInfo -->
<!-- Start KeyInfo -->
<element name="KeyInfo" type="ds:KeyInfoType"/>
<complexType name="KeyInfoType" mixed="true">
  <!--<choice>-->
  <sequence>
    <!-- Schemahärtung -->
    <!--<element ref="ds:KeyName"/>
    <element ref="ds:KeyValue"/>
    <element ref="ds:RetrievalMethod"/>-->

```

```

    <element ref="ds:X509Data"/>
    <!-- Schemahärtung -->
    <!--<element ref="ds:PGPData"/>
    <element ref="ds:SPKIDData"/>
    <element ref="ds:MgmtData"/>-->
    <!-- Schemahärtung -->
    <!-- ><any namespace="##other" processContents="lax"/> -->
    <!-- (1,1) elements from (0,unbounded) namespaces -->
<!--</choice>-->
</sequence>
<!-- Schemahärtung -->
<!--<attribute name="Id" type="ID" use="optional"/>-->
</complexType>
<!-- Schemahärtung -->
<!--<element name="KeyName" type="string"/>
<element name="MgmtData" type="string"/>
<element name="KeyValue" type="ds:KeyValue"/>
<complexType name="KeyValue" mixed="true">
    <choice>
        <element ref="ds:DSAKeyValue"/>
        <element ref="ds:RSAKeyValue"/>
        <any namespace="##other" processContents="lax"/>
    </choice>
</complexType>
<element name="RetrievalMethod" type="ds:RetrievalMethod"/>
<complexType name="RetrievalMethod">
    <sequence>
        <element ref="ds:Transforms" minOccurs="0"/>
    </sequence>
    <attribute name="URI" type="anyURI"/>
    <attribute name="Type" type="anyURI" use="optional"/>
</complexType> -->
<!-- Start X509Data -->
<element name="X509Data" type="ds:X509DataType"/>
<complexType name="X509DataType">
    <sequence maxOccurs="unbounded">
        <!-- <choice>-->
            <!-- Schemahärtung -->
            <!-- <element name="X509IssuerSerial" type="ds:X509IssuerSerialType"/>
            <element name="X509SKI" type="base64Binary"/>
            <element name="X509SubjectName" type="string"/>-->
            <element name="X509Certificate" type="base64Binary"/>
            <!-- Schemahärtung -->
            <!-- <element name="X509CRL" type="base64Binary"/>
            <any namespace="##other" processContents="lax"/> -->
        <!--</choice>-->
    </sequence>
</complexType>
<complexType name="X509IssuerSerialType">
    <sequence>
        <element name="X509IssuerName" type="string"/>
        <element name="X509SerialNumber" type="integer"/>
    </sequence>

```

```

</complexType>
<!-- End X509Data -->
<!-- Begin PGPDData -->
<!-- Schemahärtung -->
<!--<element name="PGPDData" type="ds:PGPDDataType"/>
<complexType name="PGPDDataType">
  <choice>
    <sequence>
      <element name="PGPKeyID" type="base64Binary"/>
      <element name="PGPKeyPacket" type="base64Binary" minOccurs="0"/>
      <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </sequence>
    <sequence>
      <element name="PGPKeyPacket" type="base64Binary"/>
      <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </sequence>
  </choice>
</complexType-->
<!-- End PGPDData -->
<!-- Begin SPKIDData -->
<!-- Schemahärtung -->
<!--<element name="SPKIDData" type="ds:SPKIDDataType"/>
<complexType name="SPKIDDataType">
  <sequence maxOccurs="unbounded">
    <element name="SPKISexp" type="base64Binary"/>
    <any namespace="##other" processContents="lax" minOccurs="0"/>
  </sequence>
</complexType-->
<!-- End SPKIDData -->
<!-- End KeyInfo -->
<!-- Start Object (Manifest, SignatureProperty) -->
<element name="Object" type="ds:ObjectType"/>
<complexType name="ObjectType" mixed="true">
  <sequence>
    <element ref="xades:QualifyingProperties" minOccurs="0"/>
    <element ref="ds:Manifest" minOccurs="0"/>
  </sequence>
  <!-- Schemahärtung -->
  <!--<attribute name="Id" type="ID" use="optional"/>
  <attribute name="MimeType" type="string" use="optional"/>
  <attribute name="Encoding" type="anyURI" use="optional"/>-->
  <!-- add a grep facet -->
</complexType>
<element name="Manifest" type="ds:ManifestType"/>
<complexType name="ManifestType">
  <sequence>
    <element ref="ds:Reference" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Id" type="ID" use="required"/>
</complexType>
<!-- Schemahärtung -->
<!--<element name="SignatureProperties" type="ds:SignaturePropertiesType"/>
<complexType name="SignaturePropertiesType">

```

```

    <sequence>
      <element ref="ds:SignatureProperty" maxOccurs="unbounded"/>
    </sequence>
    <attribute name="Id" type="ID" use="optional"/>
  </complexType-->

<!-- Schemahärtung -->
<!--<element name="SignatureProperty" type="ds:SignaturePropertyType"/>
<complexType name="SignaturePropertyType" mixed="true">
  <choice maxOccurs="unbounded">
    <any namespace="##other" processContents="lax"/>
    (1,1) elements from (1,unbounded) namespaces
  </choice>
  <attribute name="Target" type="anyURI" use="required"/>
  <attribute name="Id" type="ID" use="optional"/>
</complexType-->

<!-- End Object (Manifest, SignatureProperty) -->
<!-- Start Algorithm Parameters -->
<!-- Schemahärtung -->
<!--><simpleType name="HMACOutputLengthType">
  <restriction base="integer"/>
</simpleType-->
<!-- Start KeyValue Element-types -->
<!-- Schemahärtung -->
<!--<element name="DSAKeyValue" type="ds:DSAKeyValueType"/>
<complexType name="DSAKeyValueType">
  <sequence>
    <sequence minOccurs="0">
      <element name="P" type="ds:CryptoBinary"/>
      <element name="Q" type="ds:CryptoBinary"/>
    </sequence>
    <element name="G" type="ds:CryptoBinary" minOccurs="0"/>
    <element name="Y" type="ds:CryptoBinary"/>
    <element name="J" type="ds:CryptoBinary" minOccurs="0"/>
    <sequence minOccurs="0">
      <element name="Seed" type="ds:CryptoBinary"/>
      <element name="PgenCounter" type="ds:CryptoBinary"/>
    </sequence>
  </sequence>
</complexType>
<element name="RSAKeyValue" type="ds:RSAKeyValueType"/>
<complexType name="RSAKeyValueType">
  <sequence>
    <element name="Modulus" type="ds:CryptoBinary"/>
    <element name="Exponent" type="ds:CryptoBinary"/>
  </sequence>
</complexType-->
<!-- End KeyValue Element-types -->
<!-- End Signature -->
</schema>

```

9.4 Datenschutzerklärung

Datenschutzerklärung der CompuGroup Medical Deutschland AG –
Geschäftsbereich KoCo Connector GmbH

1. Datenschutzorganisation und Zuweisung von Verantwortlichkeiten im Datenschutz

Der Geschäftsbereich KoCo Connector GmbH betrachtet den verantwortungsvollen Umgang und die Einhaltung des Schutzes personenbezogener Daten als obersten Grundsatz. Die KoCoBox MED+ sichert stets die genaue Einhaltung aller relevanten Gesetze bei der Speicherung und Verarbeitung der personenbezogenen Daten.

CGM SE hat ein zentrales Datenschutzmanagement eingeführt, das innerhalb aller CGM-Unternehmen ein einheitliches und hohes Niveau für den Schutz personenbezogener Daten gewährleistet und die Einhaltung der entsprechenden Datenschutzgesetze sicherstellt.

Mit dieser Datenschutzerklärung erfüllen wir als KoCo Connector GmbH unsere Informationspflichten und stellen Ihnen Informationen über den Umgang mit Daten bei der CGM zur Verfügung. Diese Datenschutzerklärung bezieht sich auf die KoCoBox MED+.

Die aktuelle Version dieser Datenschutzerklärung finden Sie auf der Administrationsoberfläche der KoCoBox MED+ sowie im Downloadbereich unserer Homepage <https://www.kococonnector.com>.

Die Datenschutzerklärung für die Internetpräsenz finden Sie ebenfalls auf unserer Homepage, dort im unteren Seitenbereich.

2. Der Konnektor KoCoBox MED+

KoCoBox MED+ verfügt über ein eigenes Rollen- und Rechtekonzept. Der Zugriff auf die Software ist somit nur berechtigten Personen gestattet. Das Konzept regelt neben dem Zugriff auf das Produkt selbst auch den Zugriff auf bestimmte darin enthaltene Softwaremodule sowie die Ausführung von Schreib- und Lesevorgängen.

3. Verarbeitung von personenbezogenen Daten durch CGM

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person.

Wir verpflichten uns gemäß geltenden Datenschutzgesetzen (DS-GVO und BDSG neu), sämtliche Protokolldaten und sämtliche Daten zum technischen Betrieb nach Kündigung Ihres Vertrages zu löschen.

Hierbei sind wir jedoch gesetzlich verpflichtet, handels- und steuerrechtliche Aufbewahrungsfristen zu beachten, die über die Dauer des Vertragsverhältnisses hinausgehen können. Daten zum technischen Betrieb werden nur so lange vorgehalten, wie es technisch notwendig ist, spätestens jedoch nach Kündigung Ihres Vertrages gelöscht.

3.1 Daten zum technischen Betrieb

Daten zum technischen Betrieb werden nicht durch die KoCo Connector GmbH erhoben.

4. Verarbeitung von personenbezogenen Daten in der KoCoBox MED+

- Stammdaten der Administratoren
- Daten von eGK und HBA
 - Kartenummer (ICCSN)
 - Ablaufdatum der Karte

Diese Daten werden in der Datenbank im Konnektor gespeichert und verarbeitet.

4.1 Stammdaten der Praxis und der Praxismitarbeiter

Es erfolgt keine Speicherung von Stammdaten aus der Praxis.

4.2 Patientendaten

Zur Speicherung, Nutzung und Verarbeitung von Patientendaten bedarf es einer regelmäßigen Zustimmung des Betroffenen oder einer gesetzlichen Bestimmung, die dies gestattet. Die oben genannten Daten werden automatisch in der KoCoBox MED+ in Logfiles übertragen, wenn durch die in einer Arztpraxis tätigen Personen an den Kartenterminals entsprechende Chipkarten (eGK, HBA) gesteckt werden.

Stammdaten des Patienten: Es werden keine Stammdaten des Patienten erfasst.

Sensible Daten: Gesundheitsinformationen zählen zu den besonderen Arten personenbezogener Daten und sind als solche durch DS-GVO und BDSG besonders geschützt. Es werden keine Gesundheitsinformationen auf der KoCoBox MED+ gespeichert.

Löschungen können unter Berücksichtigung der gesetzlichen Aufbewahrungsfristen erfolgen. Ein Export der Daten, konkret der Logfiles, in ein gängiges maschinenlesbares Format ist möglich. Die zugehörigen Verfahren und Funktionen sind im Administrationshandbuch der KoCoBox MED+ beschrieben.

4.3 Verarbeitung von Praxisdaten und besonderen Arten personenbezogener Daten | Patientendaten in integrierten Modulen

Es werden keine integrierten Module zusammen mit der KoCoBox MED+ standardmäßig installiert.

5. Datenübermittlung

Die KoCoBox MED+ übermittelt keine personenbezogenen Daten.

6. Verpflichtung auf Vertraulichkeit, Datenschutzschulungen

Patientendaten, insbesondere die Gesundheitsdaten, unterliegen neben den Sicherheitsanforderungen der Datenschutzgesetze (DS-GVO und BDSG neu) zusätzlich strengen Auflagen aus dem Strafgesetzbuch (StGB) sowie den Sozialgesetzbüchern (SGB) und werden von der CGM besonders sensibel behandelt.

KoCo Connector GmbH beschränkt den Zugriff auf Vertragsdaten, Protokolldaten und Daten zum technischen Betrieb auf Mitarbeiter und Auftragnehmer der CGM, für die diese Informationen zwingend erforderlich sind, um die Leistungen vertragsgerecht zu erbringen. Diese Personen sind an die Einhaltung dieser Datenschutzerklärung und an Vertraulichkeitsverpflichtungen (DS-GVO, §203 StGB) verpflichtend gebunden. Die Verletzung dieser Vertraulichkeitsverpflichtungen kann mit Kündigung und Strafverfolgung geahndet werden.

Die Mitarbeiter werden regelmäßig hinsichtlich Einhaltung des Datenschutzes geschult.

7. Sicherheitsmaßnahmen / Vermeidung von Risiken

Die CGM trifft alle notwendigen technischen und organisatorischen Sicherheitsmaßnahmen, um Ihre personenbezogenen Daten sowie Ihrer Kundendaten (Patientendaten) vor unerlaubtem Zugriff, unerlaubten Änderungen, Offenlegung, Verlust, Vernichtung und sonstigem Missbrauch zu schützen. Hierzu gehören interne Prüfungen der Vorgehensweise bei der Datenerhebung, -speicherung und -verarbeitung, weiterhin Sicherheitsmaßnahmen zum Schutz vor unberechtigtem Zugriff auf Systeme, auf denen wir Vertragsdaten oder Daten zum technischen Betrieb speichern.

8. Technische und organisatorische Maßnahmen

Zur Gewährleistung der Datensicherheit überprüft die CGM regelmäßig den Stand der Technik. Hierzu werden unter anderem typische Schadenszenarien ermittelt sowie anschließend der Schutzbedarf für einzelne personenbezogene Daten abgeleitet und in Schadenskategorien eingeteilt. Zudem wird eine Risikobewertung durchgeführt.

Weiterhin dienen differenzierte Penetrationstest zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit dieser technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen werden folgende Grundsätze normiert:

- **Backup / Datensicherung (Praxis)**

Zur Vorbeugung der Datenverluste werden die Daten regelmäßig gesichert (Backup des AIS und der Zusatzprodukte).

- **Privacy by design**

Die CGM achtet darauf, dass Datenschutz und Datensicherheit bereits in der Planung und Entwicklung von IT-Systemen berücksichtigt werden. Somit wird dem Umstand vorgebeugt, dass die Vorgaben des Datenschutzes und der Datensicherheit erst nach dem Bereitstellen von IT-Systemen durch teure und zeitaufwendige Zusatzprogrammierungen umgesetzt werden müssen. Bereits bei der Herstellung werden Möglichkeiten wie Deaktivierung von Funktionalitäten, Authentifizierung oder Verschlüsselungen berücksichtigt.

- **Privacy by default**

Weiterhin sind die Produkte der CGM im Auslieferungszustand bereits datenschutzfreundlich voreingestellt, so dass nur die personenbezogenen Daten verarbeitet werden, die für den verfolgten Zweck erforderlich sind.

- **Kommunikation per E-Mail (Praxis/CGM)**

Sollten Sie mit der CGM per E-Mail in Kontakt treten wollen, weisen wir darauf hin, dass die Vertraulichkeit der übermittelten Informationen nicht gewährleistet ist. Der Inhalt von E-Mails kann von Dritten eingesehen werden. Wir empfehlen Ihnen daher, uns vertrauliche Informationen ausschließlich über den Postweg zukommen zu lassen.

- **Fernwartung**

In Ausnahmefällen kann es vorkommen, dass Mitarbeiter oder Auftragnehmer der CGM auf Patienten- und Kundendaten und somit evtl. auch auf ihre Praxisdaten zurückgreifen müssen. Hierzu gibt es zentrale Regelungen der CGM.

- Die Fernwartungs-Zugänge bleiben geschlossen und werden nur durch Kunden freigeschaltet.
- Passwörter zu Kundensystemen werden nur für die Fernwartung erteilt.
- Besondere Tätigkeiten werden durch das 4-Augenprinzip über qualifizierte Personen abgesichert.

- Wir verwenden Fernwartungsmedien, bei welchen der Kunde aktiv den Zugang freigeben muss und die Aktivitäten mitverfolgen kann.
- Die Dokumentation des Fernwartungszugriffes erfolgt im CRM System. Dokumentiert werden: ausführender Mitarbeiter, Zeitpunkt (Datum/Uhrzeit), Dauer, Zielsystem, das Fernwartungsmedium, kurze Beschreibung der Tätigkeit. Bei kritischen Tätigkeiten werden auch die nach dem 4-Augenprinzip herangezogenen Mitarbeiter erfasst.
- Die Aufzeichnung der Sitzungen ist verboten.

9. Rechte der Betroffenen

Personenbezogene Daten des Arztes und der Praxismitarbeiter

Sie haben das Recht auf Auskunft über zu Ihrer Person gespeicherte Daten sowie ggf. Rechte auf Berichtigung, Einschränkung der Verarbeitung, Widerspruch, Sperrung oder Löschung dieser Daten.

Bei der CGM erteilten Einwilligungen haben Sie das Recht, diese jederzeit mit der Wirkung für die Zukunft zu widerrufen.

Darüber hinaus haben Sie das Recht, sich einer Datenschutzaufsichtsbehörde zu beschweren, wenn Sie der Meinung sind, dass wir Ihre personenbezogenen Daten nicht richtig verarbeiten.

Wir verpflichten uns, sämtliche Vertragsdaten, sämtliche Protokolldaten und sämtliche Daten zum technischen Betrieb nach Kündigung Ihres Vertrages unaufgefordert zu löschen.

Hierbei sind wir jedoch gesetzlich verpflichtet, handels- und steuerrechtliche Aufbewahrungsfristen zu beachten, die über die Dauer des Vertragsverhältnisses hinausgehen können. Daten zum technischen Betrieb werden nur so lange vorgehalten, wie es technisch notwendig ist, spätestens jedoch nach Kündigung Ihres Vertrages gelöscht.

Personenbezogene Daten Ihrer Patienten

Ihre Patienten haben das Recht auf Auskunft über zu ihnen gespeicherten Daten, Mitnahme dieser Daten (Recht auf Datenportabilität) sowie ggf. Rechte auf Berichtigung, Einschränkung der Verarbeitung, Widerspruch, Sperrung oder Löschung dieser Daten.

Bei den Löschanfragen sind Sie jedoch gesetzlich verpflichtet, die geltenden Aufbewahrungsfristen zu beachten.

Bei den Ihnen erteilten Einwilligungen haben Ihre Patienten das Recht, diese jederzeit mit der Wirkung für die Zukunft zu widerrufen.

Darüber hinaus haben Ihre Patienten das Recht, sich bei der für Sie zuständigen Datenschutzaufsichtsbehörde zu beschweren, wenn Ihre Patienten der Meinung sind, dass Sie die personenbezogenen Daten der betreffenden Patienten nicht richtig verarbeiten.

10. Durchsetzung

Die CGM überprüft regelmäßig und durchgängig die Einhaltung dieser Datenschutzbestimmungen. Erhält die CGM formale Beschwerdeschriften, wird sie mit dem Verfasser bezüglich seiner Bedenken Kontakt aufnehmen, um eventuelle Beschwerden hinsichtlich der Verwendung von persönlichen Daten aufzulösen. Die CGM verpflichtet sich, dazu kooperativ mit den entsprechenden Behörden, einschließlich Datenschutzaufsichtsbehörden, zusammenzuarbeiten.

11. Änderungen an dieser Datenschutzerklärung

Beachten Sie, dass diese Datenschutzerklärung von Zeit zu Zeit ergänzt und geändert werden kann. Sollten die Änderungen wesentlich sein, werden wir eine ausführlichere Benachrichtigung ausgeben. Jede Version dieser Datenschutzerklärung ist anhand ihres Datums- und Versionsstandes in der Fußzeile dieses Dokuments (Stand) zu identifizieren. Außerdem archivieren wir alle früheren Versionen dieser Datenschutzerklärung zu Ihrer Einsicht auf Nachfrage beim Datenschutzbeauftragten der CompuGroup Medical Deutschland SE.

12. Verantwortlich für die KoCo Connector GmbH

Herr Mathias Nieting
KoCo Connector GmbH
Dessauer Str. 28/29
D-10963 Berlin
mathias.nieting@kococonnector.com

Datenschutzbeauftragter

Bei Fragen hinsichtlich der Verarbeitung Ihrer personenbezogenen Daten können Sie sich an den Datenschutzbeauftragten wenden, der im Falle von Auskunftersuchen oder Beschwerden Ihnen zur Verfügung steht.

Herr Hans Josef Gerlitz
CompuGroup Medical SE
Maria Trost 21
D-56070 Koblenz
HansJosef.Gerlitz@CGM.com

13. Zuständige Aufsichtsbehörde

Für die CGM - Geschäftsbereich
KoCo Connector GmbH ist die
Berliner Beauftragte für Datenschutz und die
Informationsfreiheit
Alt-Moabit 59-61
D-10555 Berlin
mailbox@datenschutz-berlin.de
als Aufsichtsbehörde zuständig.

9.5 Lizenzinformationen

Freie und Open Source Software

1. Das Produkt enthält Softwarebestandteile, die von den Rechteinhabern als Freie Software bzw. Open Source Software lizenziert werden (nachfolgend als „FOSS“ bezeichnet). Die entsprechenden Lizenzen sind in einer separaten Datei "licenses.htm" verfügbar und Sie können Nutzungsrechte in dem dort geregelten Umfang unmittelbar von den Rechteinhabern erwerben.
Die Open Source-Lizenzen haben Vorrang vor allen anderen Lizenzinformationen in Bezug auf die entsprechenden im Produkt enthaltenen FOSS-Softwarekomponenten.
2. Sie können den Quellcode dieser Softwarebestandteile von uns auf einem Datenträger erhalten, wenn Sie innerhalb von drei Jahren nach dem Vertrieb des Produkts durch uns bzw. zumindest solange, wie wir Support und Ersatzteile für das Produkt anbieten, eine Anfrage an unsere Kundenbetreuung an folgende Adresse stellen:
KoCo Connector GmbH
Dessauer Str. 28/29 10963 Berlin "
Quellcode [KoCoBox MED+]"
und EUR 10,- für die Kosten zur Erstellung und Übersendung des Datenträgers zahlen. Eine vollständige Dokumentation der FOSS, der Lizenzbedingungen und des Quellcodes finden Sie im Quellcode der FOSS.
3. Es ist Ihnen gestattet, Softwarebestandteile, die von uns stammen, für Ihren eigenen Gebrauch zu bearbeiten und zur Behebung von Fehlern solcher Bearbeitungen zu reengineeren, sofern diese Softwarebestandteile mit Programmbibliotheken unter der GNU Lesser General Public License (LGPL) verlinkt sind. Die Weitergabe der bei dem Reengineering gewonnenen Informationen und der bearbeiteten Software ist hingegen nicht gestattet.
4. Die Sicherheit ist ein wichtiges Thema im Bereich der Medizintechnik. Daher können modifizierte Versionen der verwendeten FOSS nur installiert werden, wenn die verwendeten Sicherheitsfeatures durch uns entfernt werden. Bitte beachten Sie, dass die Installation geänderter Software regelmäßig zum Verlust der Zertifizierung führt und die Betriebserlaubnis erlischt. Wenn Sie dennoch modifizierte Versionen der installieren möchten, die unter der GNU General Public License (GPL) und/oder der LGPL lizenziert sind, senden Sie bitte ein diesbezügliches unterzeichnetes Schreiben an folgende Adresse:
KoCo Connector GmbH
Dessauer Str. 28/29
10963 Berlin
"Freischaltung zur Installation [KoCoBox MED+]"
Wir informieren Sie anschließend über die nötigen Schritte, die für eine Einsendung des Produkts nötig sind. Wir werden nach Eintreffen des Produkts die Installation von GPL- und/oder LGPL-Software ermöglichen und unsere Marken auf dem Produkt entfernen. Die Weiterverteilung des Produkts mit modifizierter Software ist dann nicht gestattet. Auch die Verwendung des Produkts ist dann verboten, wenn sie gegen gesetzliche Bestimmungen verstößt.
Die Gewährleistung erlischt für alle Mängel, die auf der Verwendung modifizierter Software beruhen.
5. Auf Wunsch der Urheber und Rechteinhaber der eingesetzten FOSS weisen wir auf Folgendes hin:
„THE OPEN SOURCE SOFTWARE IN THIS PRODUCT IS DISTRIBUTED IN THE HOPE THAT IT WILL BE USEFUL, BUT WITHOUT ANY WARRANTY, WITHOUT EVEN THE IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. See the applicable licenses for more details.“
6. Die damit verbundenen Lizenzinformationen finden Sie in der Managementschnittstelle im Bereich *Verwaltung* unter dem Button Lizenzbestimmungen anzeigen.

9.6 Tabellenverzeichnis

| | |
|--|-----|
| Tabelle 1: Technische Daten der KoCoBox MED+ | 18 |
| Tabelle 2: Übersicht der Browser-Downloadpunkte | 39 |
| Tabelle 3: Aufbau der Logdateien im Protokollierungsdienst | 125 |
| Tabelle 4: Aufbau der Logfiles im Fachmodul VSDM | 165 |
| Tabelle 5: Aufbau der Logfiles im Fachmodul AMTS | 168 |
| Tabelle 6: Aufbau der Logfiles im Fachmodul ePA | 172 |
| Tabelle 7: Aufbau der Logfiles im Fachmodul NFDM | 177 |

9.7 Stichwortverzeichnis

A

| | |
|---|-------------------------|
| aAdG | 11, 62, 259 |
| aAdG-NetG..... | 11, 260 |
| Ablauf von Zertifikaten | 119 |
| Administration..... | 44 |
| Administrator | 43, 44, 45, 154 |
| Administrator-Benutzer löschen | 135 |
| Administrator-Passwort..... | 44 |
| Administrator-Rollen..... | 133 |
| Administratorzugang | 95 |
| Aktive Benutzerrolle | 110 |
| Aktivität | 52 |
| Aktualisierung | 141 |
| Aktualisierung nach KT-Updates | 144 |
| Aktualisierungsdatum..... | 151 |
| Aktualisierungsplanung | 150 |
| Aktualisierungszeitpunkt | 151 |
| Alarmmeldung | 115 |
| Alarmwert | 115 |
| Allgemeine Gebrauchsanleitung..... | 8 |
| Allgemeine Menüstruktur..... | 34 |
| Alternative Netzwerkkonfigurationen | 188 |
| Amount..... | 125, 165, 168, 172, 177 |
| Anagramme..... | 46 |
| Anbindungsmodus Internet..... | 57, 63 |
| Anbindungsmodus parallel..... | 191 |
| Anbindungsmodus seriell (,in Reihe') | 188, 192 |
| andere Anwendungen des Gesundheitswesens..... | 11, 62, 259, 260, 280 |
| Angreifer..... | 14 |
| Angriffe..... | 185 |
| Angriffspotenzial | 14 |
| Anschlüsse..... | 25 |
| Anschlusswerte | 12 |
| Anzahl der Slots des Kartenterminals..... | 110 |
| Anzeigefenster | 51 |
| Anzeigenbereich | 49 |
| Anzeigenfeld | 36 |
| Arbeitsplatz hinzufügen..... | 140 |
| Arbeitsplatz namens Konnektor..... | 82 |
| Arbeitsplatz-ID..... | 140, 162 |
| Aufbau der Logfiles im Fachmodul AMTS | 168 |
| Aufbau der Logfiles im Fachmodul NFDM | 177 |
| Ausführungszeitpunkt..... | 144, 148 |
| Auslieferung | 44 |
| Auslieferungspasswort | 44, 45, 48 |
| Auslieferungszustand | 155 |
| Außerbetriebnahme | 155, 157, 187 |
| Authentifizierung | 43 |

| | |
|---|-----|
| authentisch..... | 60 |
| authentisieren..... | 44 |
| Authentisierungsinformationen..... | 15 |
| Authentisierungsmodus..... | 90 |
| Authentisierungszertifikat des Kartenterminals..... | 109 |
| Authentisierungszertifikate..... | 94 |
| Authentizität..... | 125 |
| Authentizität des Netzkonnektors..... | 59 |
| automatische Aktualisierung..... | 141 |
| automatische Onlineprüfung der VSD..... | 162 |
| autorisierte Personen..... | 14 |
| Auto-Update..... | 141 |

B

| | |
|--|------------------|
| Bandbreitenbegrenzung..... | 64 |
| Basic-Authentication..... | 131 |
| Basisdienste..... | 84 |
| Bedienung..... | 6 |
| belegte Slotnummern..... | 110 |
| Benutzerdaten..... | 154 |
| Benutzerkennung..... | 44, 46, 47 |
| Benutzerverwaltung..... | 51, 133 |
| Beschreibung..... | 185 |
| Bestandsnetze freischalten..... | 62 |
| Bestandsnetz-Routen..... | 69 |
| Betriebsbedingungen..... | 18 |
| Betriebsdaten..... | 87 |
| Betriebsdatenmeldedienst..... | 87 |
| Betriebsführungsbuch..... | 11, 54, 102 |
| Betriebsstättenkarte..... | 10 |
| Betriebstemperatur..... | 18 |
| Betriebszustand..... | 32, 33 |
| Betriebszustandsmeldungen..... | 54, 209 |
| Bildschirmdiagonale..... | 18 |
| BNetA..... | 54, 85, 118, 271 |
| BNetA-VL..... | 119 |
| bösartige (malformed) Dokumente..... | 132 |
| brainpoolP256r1..... | 93, 94 |
| Breitband-Internet-Anschluss..... | 29 |
| Browser..... | 49 |
| browserbasierte Managementschnittstelle..... | 38 |
| Browser-Button..... | 49 |
| Browsertypen..... | 39 |
| BSI-TR-03116-1..... | 93, 95 |
| Buchstabenfolgen..... | 46 |
| Bundesnetzagentur..... | 54, 85, 118, 271 |

C

| | |
|----------------|----|
| CA-Import..... | 51 |
|----------------|----|

| | |
|-----------------------------------|---------------|
| CA-Zertifikat..... | 93, 95 |
| CA-Zertifikate..... | 119 |
| Certificate Status Protocol | 119 |
| CETP-Event..... | 104, 114, 217 |
| Clientensystem-ID | 162 |
| Client-Gruppen | 69 |
| Clientsystem hinzufügen | 139 |
| Clientsystem ID | 139 |
| Clientsystem_ePA_Default | 172 |
| Clientsysteme..... | 51, 84, 88 |
| Clientsystem-Hersteller | 10 |
| CMS-Signatur | 196 |
| COSVersion der Karte | 217 |
| CS-AP Objekt hinzufügen..... | 140, 141 |

D

| | |
|--|---------------|
| DataStructureVersion | 217 |
| Datenschutzerklärung..... | 238 |
| Datenschutzorganisation | 238 |
| Default-Aufrufkontext..... | 169 |
| Defekt | 155, 156, 214 |
| DER-encoded Zertifikate | 93 |
| Design..... | 19 |
| detached signature..... | 128, 129 |
| DHCP | 51 |
| DHCP-Server | 66 |
| Diagnose..... | 33 |
| Diebstahl..... | 178 |
| Diebstahlsicherung | 25 |
| Dienstverzeichnisdienst..... | 89 |
| Display | 32, 59 |
| Distinguished Name..... | 92 |
| DNS | 51 |
| DNS Server | 78 |
| DNS-Service Discovery..... | 162 |
| Downloadpunkt..... | 87, 118 |
| Downloadpunkte für vertrauenswürdige PKI-Elemente der PU | 41 |
| D-Trust | 41 |
| dunkelgraue Buttons | 52 |
| Durchführen eines Werksreset..... | 135 |

E

| | |
|---------------------------|--------------|
| EC_OTHER_ERROR_STATE..... | 86 |
| ECC Brainpool..... | 94 |
| ECC-Migration | 55, 116, 117 |
| ECC-RSA-TSL | 117 |
| ECC-Zertifikate | 95, 116 |
| Einbindung..... | 13 |
| Einbruch | 14, 178 |

| | |
|---|-------------|
| Einfachsignaturmodus | 126 |
| Eingabefelder | 52 |
| Einloggen..... | 44 |
| Einmalpasswort..... | 134 |
| Einrichtung der vollständigen Betriebsumgebung..... | 9 |
| Einsatz..... | 18 |
| Einsatzumgebung..... | 6, 13, 178 |
| Einstellungen..... | 51 |
| Einstellungsoptionen | 51 |
| Einträge | 36 |
| Elektronische Patientenakte (ePA) | 168 |
| E-Medikationsplan (eMP) | 165 |
| Endgeräte-Zertifikat | 93 |
| Endkunde..... | 15, 89, 266 |
| Endpunkt für Firmware-Download..... | 143 |
| Endpunkt für Konfigurationsdaten-Download..... | 143 |
| Entitätsbezeichner..... | 96 |
| Entschlüsselung..... | 102 |
| enveloping signature | 128 |
| ePA-Aktensystem | 169 |
| Erprobungsaktualisierungen..... | 143 |
| Erprobungs-Update-Pakete | 143 |
| Ersatzverfahren | 13 |
| Erstanmeldung | 135 |
| erweiterte DHCP-Optionen | 70 |
| Ex-/Import | 95 |
| Export Konfiguration | 97 |
| exportierte Konfiguration | 101 |
| exportierte Konfigurationsdaten..... | 102 |
| Exportprozess | 97 |

F

| | |
|---|---|
| Fachmodul Arzneimitteltherapiesicherheit (FM AMTS)..... | 165 |
| Fachmodul ePA | 169 |
| Fachmodul Notfalldaten-Management (FM NFDm) | 175 |
| Fachmodul VSDM | 51, 160 |
| Fachpersonal | 178 |
| Fehleingabe..... | 48 |
| Fehler bei der Passwortänderung..... | 47 |
| Fehler beim Login | 46 |
| Fehlercode..... | 33 |
| Fehlermeldung | 46, 47 |
| Fehlerprotokoll..... | 160, 164, 165, 167, 168, 171, 172, 176, 177 |
| Fehlerzustandsanzeige | 37 |
| Firewall SIS | 51 |
| Firewallregeln | 66 |
| Firmware-Update | 147 |
| Firmware-Updates | 144, 148 |
| Firmware-Version..... | 148 |
| First-Level-Support..... | 10 |

| | |
|-----------------------------|----------|
| Flüssigkeiten | 12 |
| Freischalten der SMC-B..... | 104 |
| Freischaltung | 71, 74 |
| FriedlyName | 107 |
| Führe Werksreset aus | 155, 156 |
| Funktionsstörungen | 12 |
| Funktionstasten..... | 45 |

G

| | |
|---|---------|
| ganzzahlige Werte | 106 |
| Garantie | 8 |
| Gehäuse..... | 60, 179 |
| Gehäusefüße | 8 |
| gematik-Implementierungsrichtlinien | 10 |
| Gerät | 178 |
| Grace Period nonQES | 119 |
| Groß- und Kleinschreibung..... | 46 |
| Grundkonfiguration | 54 |
| Gültigkeitszeitraum..... | 120 |
| Gummifüße | 26 |

H

| | |
|---|--------------|
| Handlungsanweisung | 37, 180, 185 |
| Hardware-Version | 148 |
| Haupt-Kategorien..... | 51 |
| Haupt-Kategorietitel | 51 |
| Hauptmenü..... | 33 |
| hellgraue Buttons..... | 52 |
| Hersteller-ID | 109 |
| Herstellernamen | 49 |
| Herstellerspezifische Fehlermeldungen | 193 |
| Herstellerspezifischer Werksreset..... | 156 |
| Hinzufügen eines Kartenterminals..... | 108 |
| Hologramm..... | 21, 28 |
| http-Forwarder | 83 |

I

| | |
|---|---------|
| ICMP-Echo | 117 |
| im lokalen Netz routen..... | 62 |
| Import / Export der Konfigurationsdaten | 95 |
| Import der Konfigurationsdaten..... | 101 |
| Importpasswort..... | 98 |
| Inaktivität | 50, 52 |
| Inbetriebnahme | 11, 15 |
| Infomodell | 51, 137 |
| Infomodell importieren | 138 |
| Information..... | 6 |
| Informationen | 33 |

| | |
|---------------------------------|--------------|
| Informationsebene | 36 |
| Informationsleiste | 49, 50 |
| Informationszeitpunkt | 109 |
| initiale Konfiguration | 38, 56 |
| initiale Passwortänderung | 45 |
| Initialkonfiguration | 46 |
| Initialpasswort | 48 |
| Installation | 6 |
| integer | 60 |
| Integrität | 28, 125, 185 |
| Interface | 43 |
| Intermediär | 162 |
| Internet Access Gateway | 14, 63 |
| Intranetrouten | 62, 69 |

K

| | |
|--|-------------------------|
| Kartendienst | 51, 103 |
| Kartenterminal bearbeiten | 108 |
| Kartenterminal hinzufügen | 140 |
| Kartenterminal zuweisen | 107 |
| Kartenterminaldienst | 51, 105 |
| Kartenterminal-ID | 109, 113, 140, 148 |
| Kartenterminal-Pairing | 112 |
| Kartenterminal-Updates | 152 |
| Keep Alive Interval | 106 |
| Keep Alive Versuche | 106, 173 |
| Kensington Lock | 25 |
| Kensington-Schloss | 15, 25 |
| KIM | 131, 269, 272, 274, 281 |
| Komfortsignatur | 90, 130 |
| Komfortsignaturmodus | 127 |
| KOM-LE-Client | 93 |
| Kommunikation im Medizinwesen | 269, 281 |
| Konfiguration | 9 |
| Konfiguration des Anwendungskonnektor | 84 |
| Konfiguration ohne Internetanbindung | 190 |
| Konfigurationen | 6 |
| Konfigurationsbereich | 51 |
| Konfigurationsbereich für das Fachmodul AMTS | 166 |
| Konfigurationsbereich für das Fachmodul NFDM | 175 |
| Konfigurationsbereich für das Fachmodul VSDM | 161 |
| Konfigurationsdaten der Bestandsnetze | 144 |
| Konfigurationsfenster | 52 |
| Konfigurationsparameter | 29 |
| Konnektor | 9, 185 |
| Konnektor-Aktualisierungen | 144 |
| Konnektorauthentisierung | 94, 95 |
| Konnektor-Authentisierungszertifikat | 95 |
| Konnektor-Authentisierungszertifikats ECC-NIST | 94 |
| Konnektormanagement | 133 |

| | |
|----------------------------------|-----|
| Kryptoalgorithmus | 132 |
| kryptografisches Verfahren | 120 |
| KSR-Updateinformationen | 87 |

L

| | |
|---------------------------------------|---|
| LAN | 25, 64 |
| LAN / WAN | 51 |
| Länge der IP-Pakete..... | 57, 64 |
| LAN-Verbindung | 59 |
| Laufzeitverlängerung | 40, 121 |
| LDAP-Funktionalität | 93 |
| LDAP-Proxy | 131 |
| Leasedauer dynamischer Adressen | 69 |
| Leistungsumfang ONLINE..... | 57, 72, 80, 83, 84, 85, 99, 118, 190, 191 |
| Leistungsumfänge..... | 84 |
| Lieferumfang..... | 8 |
| Lizenzbestimmungen..... | 88 |
| Login | 44, 135 |
| Login-Fenster..... | 44, 50 |
| Logrefid..... | 125, 165, 168, 172, 177 |
| Lokaler Administrator | 133 |
| Lüftungsschlitze | 12 |

M

| | |
|--|-----------------------------------|
| MAC-Adresse des Kartenterminals | 110 |
| Managementschnittstelle..... | 9, 50, 135 |
| Mandant hinzufügen..... | 139 |
| Mandant_ePA_Default..... | 172 |
| mandantenbezogene Administration | 138 |
| Mandanten-Schlüssel-Paar | 58 |
| Mandant-ID..... | 139, 162 |
| Mandant-Schlüssel-Paar | 163 |
| Manipulation | 15 |
| manipuliert..... | 21 |
| manuell importierte CA-Zertifikate | 120 |
| manuell pairen..... | 111 |
| Manuelle ECC-Migration..... | 116 |
| manueller Verbindungsversuch | 111 |
| maximale Anzahl Komfortsignaturen | 130 |
| maximale Dauer Komfortsignaturen | 130 |
| maximale Offline-Dauer | 162 |
| Mein Profil | 154 |
| Meldungen | 52 |
| Menüstruktur..... | 33 |
| Missbrauchserkennungen..... | 115 |
| Mitarbeiter..... | 178 |
| mobile Hardware | 25 |
| Module..... | 125, 165, 168, 172, 177, 267, 274 |
| Monitoring von Operationen | 114 |

Mouseover..... 49

N

Namensdienst 78
 NAT Keep-Alive-Pakete 72
 Navigationslogik 36
 Navigationsspalte 49
 Netzkonnektor 54
 netzseitige Einsatzszenarien 29
 Netzwerkfähigkeit 29
 Netzkabel 30, 31
 Netzwerkkonfigurationen..... 62
 Neustart 185
 Neustart des Konnektors 84, 86
 nicht-qualifizierte elektronische Signatur (nonQES) 125
 Normalbetrieb 32
 Nutzung Hash & URL 72

O

ObjectSystemVersion 217
 OCSP-Prüfungen 83
 OCSP-Responder..... 83
 Offline-Konnektor 191
 Offline-Modus..... 77, 190, 211, 271
 Online-Konnektor..... 191
 Operation ReadVSD 162

P

PAdES 129
 Pairing..... 82
 Pairingvorgang 112
 parallel..... 29
 paralleler Anbindungsmodus 64
 Parameter..... 54, 64, 69, 72, 112, 123, 124, 125, 164, 165, 167, 168, 171, 172, 176, 177, 205, 217
 Parameter CardVersion 217
 Parameter des Kartenterminaldienstes..... 105
 Passphrase 98
 Passwort 44, 46
 Passwort ändern 45
 Passwort eines Administrators ändern..... 135
 Passwort vergessen..... 156
 Passwortänderung 47
 Passwortwechsel 46
 PEM-Zertifikate 93
 Performanceprotokoll..... 51, 122, 123, 124, 125, 160, 164, 165, 166, 167, 168, 171, 172, 175, 176, 177
 persönliches Passwort 44, 135
 physischen Zugang 156
 PIN-Operationen 82

| | |
|--|------------------------|
| Platzierung der Sicherheitssiegel..... | 22 |
| Plus-Symbol..... | 51 |
| Port des Kartenterminals..... | 110 |
| primäre NTP Server Adresse | 76 |
| Produktcode | 109 |
| Produktinformationen..... | 54, 109 |
| Produkt-Logo..... | 49 |
| Produkttyp/-version..... | 109 |
| protocolType..... | 165, 168, 172, 177 |
| Protokollierungsdienst..... | 51, 122, 123, 125, 180 |
| Protokollierungskonfiguration..... | 169 |
| Prüfen von Dokumentensignaturen..... | 125 |
| Prüfungsnachweise..... | 162 |

Q

| | |
|--|----------|
| QES-Signaturverfahren..... | 128, 129 |
| qualifizierte elektronische Signatur (QES) | 125 |

R

| | |
|--------------------------------------|--------|
| Rechenzentrum | 14 |
| Registrierung..... | 51, 71 |
| Registrierung am Zugangsdienst | 73 |
| Registrierungsserver..... | 80 |
| Reload-Funktion..... | 53 |
| Reload-Symbol..... | 50 |
| Remote-PIN-KT Objekte..... | 138 |
| Request Timeout..... | 173 |
| Reset..... | 86 |
| Ressource Records | 162 |
| Router | 14 |
| Routingmodus Intranet..... | 63 |
| Routingtabelle..... | 62 |
| RSA-2048 | 94 |
| RSA-Schlüssel | 95 |
| RSA-Zertifikate | 116 |

S

| | |
|-------------------------------------|-------------------------|
| Schadsoftware..... | 16 |
| Schlüssel für Prüfungsnachweis..... | 58, 162 |
| Schlüsselgenerierungsdienst..... | 273, 282 |
| Schnittstellen..... | 158, 160, 266, 269, 276 |
| Schreibfehler | 47 |
| Schriftkonventionen..... | 7 |
| Schulung..... | 15 |
| Schutzmaßnahmen | 15 |
| Schweregrad | 37 |
| Second-Level-Support..... | 10 |
| secp256r1 (NIST)..... | 93, 94 |

| | |
|---|------------------------------|
| Secure Internet Service..... | 29, 63, 64 |
| sekundäre NTP Server Adresse | 76 |
| Selbsttest..... | 86, 185 |
| Semantik | 49, 52 |
| Sequenznummer..... | 83 |
| seriell („in Reihe“) | 29 |
| serielle Anbindung..... | 54 |
| Seriennummer | 27, 120 |
| Service Discovery | 105 |
| Service Discovery Port | 105 |
| Service Discovery Timeout | 105 |
| Service Discovery Zyklus..... | 105 |
| Service Timeout | 57 |
| Session-Timeout..... | 50 |
| SGD | 168, 216, 273, 282 |
| SHA 256-Fingerabdruck..... | 92 |
| Sichere Clientsystemanbindung..... | 16 |
| sichere Verbindung | 59 |
| sicheren Betrieb | 12 |
| Sicherheit..... | 178 |
| Sicherheitsabfrage | 155, 156 |
| Sicherheitsanforderungen | 6, 15, 28, 59, 184 |
| Sicherheitshinweise | 12, 15, 44, 45 |
| Sicherheitskonzept..... | 14 |
| Sicherheitsmaßnahmen..... | 15 |
| Sicherheitsprotokoll | 51, 122, 155 |
| Sicherheitsrelevante Fehlermeldungen der Fachmodule | 214 |
| Sicherheitsrelevante Szenarien..... | 178 |
| Sicherheitsschloss | 14 |
| Sicherheitsschrauben | 12, 15, 26, 28 |
| Sicherheitssiegel | 14, 15, 19, 21, 28, 60 |
| sicherheitstechnische Veränderungen..... | 185 |
| Sicherheitsvorgaben | 9 |
| Sicherung..... | 15 |
| Sicherungsmaßnahmen..... | 14 |
| Sicherungsrichtungen | 14 |
| Signaturdatei des Zip-Archivs..... | 147 |
| Signaturdienst | 125 |
| Signaturrechtlinie | 128, 159, 197, 198, 265, 287 |
| Signaturvarianten..... | 128 |
| Signaturzeitpunkt..... | 100 |
| Signaturzertifikat..... | 100 |
| Signer-Zertifikat | 118 |
| Signieren | 125 |
| Signieren von Dokumenten..... | 125 |
| SIS-VPN-Konzentrator-Adresse..... | 71 |
| SMB hinzufügen | 140 |
| SMC-K exp | 20 |
| SOAP-Protokoll | 80 |
| Spannungsausfall..... | 148 |
| Sperrprozess..... | 187 |

| | |
|---|--|
| Standalone Konnektor | 85 |
| Standalone mit logischer Trennung | 191 |
| Standalone-Szenarien | 191 |
| Standard-Displayansicht | 32 |
| Stapelsignatur | 127 |
| Startverhalten | 217 |
| Status | 33, 51 |
| Status des Kartenterminals | 110 |
| Status des Vertrauensraums | 54 |
| Status manuell ändern | 111 |
| Status verwendeter Zertifikate | 120 |
| Statusinformationen | 32 |
| Statusleiste | 32 |
| Status-Seite | 46, 49 |
| Statuszeile | 59 |
| Steckdose | 12 |
| Steckernetzteil | 8 |
| Steuer-Buttons | 12, 36 |
| Steuerelemente | 24 |
| Steuermenü | 24, 36 |
| Störungen | 18 |
| Stratum-2 Server der TI | 76 |
| Stromnetz | 30, 31 |
| Stromversorgung | 40 |
| Super-Administrator | 133 |
| Support | 28 |
| Supportfall | 27 |
| Support-Hotline | 10 |
| Support-Instanzen | 10 |
| Symbole | 52 |
| Symbolik des Displays | 33 |
| System | 30, 31, 50 |
| Systeminformationsdienst | 51, 113 |
| Systemprotokoll | 51, 122, 123, 124, 125, 160, 164, 165, 167, 168, 171, 172, 175, 176, 177 |
| Systemstart | 32, 33 |
| Systemzeit | 75, 76 |

T

| | |
|-------------------------------------|-------------------------|
| TCP-Verbindungsaufbau Timeout | 173 |
| Technische Daten | 18 |
| Telematikdienste | 173 |
| Telematikdienste für die ePA | 173 |
| Telematikinfrastruktur | 9, 71 |
| Temperaturschwankungen | 12 |
| Third-Level-Support | 10 |
| Timeout für Fachdienste | 162 |
| Timeout QES | 119 |
| Timestamp | 125, 165, 168, 172, 177 |
| Timeout nonQES | 119 |
| Titelleiste | 49 |

| | |
|----------------------------------|-------------------------|
| Titelzeile | 36 |
| TI-VPN-Konzentrator-Adresse..... | 71 |
| TLS-Handshake Timeout | 106, 173 |
| TLS-Schnittstelle | 84 |
| TLS-Verbindungsparameter | 169 |
| Tooltip..... | 49 |
| Topic | 125, 165, 168, 172, 177 |
| Trusted Service List | 119 |
| TSL-CA-Cross-Zertifikat | 117 |
| TSL-CA-Zertifikat | 117 |
| TSL-Signer-Zertifikat | 83 |
| Typenschild..... | 26 |

U

| | |
|---|-----|
| Übernahme der Konfigurationsdaten | 101 |
| Überwachung | 14 |
| Umgebungsparameter | 62 |
| Unbefugter | 15 |
| Unterbereiche..... | 51 |
| Unterlegung | 36 |
| Untermenü | 36 |
| unterstützte Produkttyp-Versionen..... | 106 |
| Update-Informationen ermitteln..... | 144 |
| Update-Pakete | 146 |
| Updates für das lokale Hochladen | 142 |

V

| | |
|---|---------------|
| VAU | 169, 278, 283 |
| Verankerung..... | 15 |
| Verantwortlicher | 14, 15 |
| Verbindung in die Telematikinfrastruktur..... | 79 |
| Verbindung via TLS..... | 89 |
| Verbindung zur TI..... | 59 |
| Verbindungsverluste | 106 |
| Verfügbare Aktualisierungen automatisch herunterladen | 143 |
| Verfügbarkeitsstatus des Kartenterminals | 110 |
| Verifizieren | 126 |
| Verpackung..... | 8, 19 |
| Verpackungssiegel | 8, 19 |
| Verschlüsselungsdienst..... | 132 |
| Versichertenstammdatenmanagement..... | 160, 165, 175 |
| Version (HW/FW)..... | 109 |
| Versionen..... | 33 |
| Versionsangaben zu gesteckten Karten im CETP-Event..... | 217 |
| Vertragsnummer | 74, 187 |
| Vertrauensliste der Bundesnetzagentur | 119 |
| Vertrauensraum | 55, 155 |
| Vertrauenswürdige Ausführungsumgebung..... | 278, 283 |
| Vertrauenswürdigkeit | 12, 178 |

| | |
|--|----------|
| Verwaltung | 51 |
| Verwaltung von Notfalldatensätzen (NFD)..... | 175 |
| Verzeichnisdienst | 131 |
| Volldurchbruch | 178 |
| VPN | 51, 71 |
| VPN Idle Timeout | 72 |
| VPN Status..... | 33 |
| VPN-Konzentrator | 59 |
| VSDM..... | 160, 165 |

W

| | |
|--|-------------|
| WAN | 25, 64 |
| WAN und LAN-Adresse | 20 |
| WAN-Verbindung | 59 |
| Warnung an den Betreiber | 76 |
| Wartungspairing..... | 96, 100 |
| Web-Browser..... | 39 |
| Werkseinstellungen | 155 |
| Werksreset | 84, 87, 155 |
| Werksreset durchführen | 133 |
| Werksreset erfolgreich | 155, 156 |
| Werksreset per Managementschnittstelle | 155 |
| widerrechtlicher Zugang..... | 15 |
| Workplace_ePA_Default | 172 |
| Wörterbuch..... | 46 |

X

| | |
|----------------------|-----|
| XAdES / nonQES | 129 |
| XAdES / QES..... | 128 |
| XAdES-Signatur..... | 80 |
| XML-Datei | 138 |
| XML-Schema..... | 137 |

Z

| | |
|--|------------|
| Zahlenfolgen | 46 |
| Zeichenklassen..... | 45 |
| Zeitdienst..... | 51, 75, 76 |
| Zeitpunkt der letzten Passwortänderung | 154 |
| Zeitsynchronisierung..... | 76 |
| Zeitzone | 76 |
| Zentralversion | 109 |
| Zertifikatsaussteller..... | 120 |
| Zertifikatscontainer | 93 |
| Zertifikatsdienst | 51, 115 |
| Zertifikatsinhaber | 120 |
| Zertifikatsprüfung..... | 115 |
| Zertifikatsstore | 41 |
| Zubehörteile | 8 |

| | |
|---|--------|
| Zugang zur Managementschnittstelle | 44 |
| Zugangsdaten..... | 44, 45 |
| Zugangskontrolle | 43 |
| Zugangszertifikate für Clientsysteme | 92 |
| Zugriff | 15 |
| Zugriffsberechtigungsdaten für AutoUpdateVSD..... | 162 |
| zugriffsbeschränkt..... | 15 |
| zugriffsgeschützt..... | 15 |
| Zugriffsschutz | 14 |

9.8 Glossar

Das folgende Glossar wurde in weiten Teilen in enger Anlehnung an das zentrale Projekt-Glossar der gematik²¹² sowie ergänzend aus Wikipedia-Quellen erstellt. Die im vorliegenden Handbuch verwendeten Begriffe und Fachtermini stehen damit im Einklang.

| Begriff | Synonym / Abkürzung | Erläuterung / Definition |
|--|------------------------|--|
| First-Level-Support | | Support des Servicepartners des Endkunden (Leistungserbringers, LE) |
| Second-Level-Support | | Support des Service Providers (z.B. Clientsystem-/Primärsystemhersteller oder Reseller) |
| Third-Level-Support | | Anbietersupport durch den Hersteller (KoCo Connector GmbH) |
| | | |
| Acrylnitril-Butadien-Styrol | ABS | Material, aus dem das Gehäuse der KoCoBox MED+ G3 besteht |
| Administrator | | Administrator der KoCoBox MED+ ist eine vom Besitzer des Geräts autorisierte, vertrauenswürdige und fachlich geschulte Person, die mittels Benutzerkennung (Name) und persönlichem Passwort einen autorisierten Zugang zur Managementschnittstelle hat. |
| Anbietersupport | | Supportfunktion im übergreifenden Incident (und Problem) Management, geleistet durch die produktverantwortlichen Anbieter. Diese Funktion stellt den 2nd und 3rd Level Support dar, wobei Incident- und Problemmeldungen ausschließlich von Service Providern, anderen Anbietern oder Herstellern aufgegeben werden, nicht von Anwendern, PEDs oder Versicherten. Die Koordination des Anbietersupports erfolgt durch die Service Provider. ²¹³ |
| andere Anwendungen des Gesundheitswesens | aAdG | Zur Anwendungskategorie „andere Anwendungen des Gesundheitswesens“ gehören Anwendungen, deren Dienste direkt an die TI-Plattform angebunden sind und die alle Leistungen der TI-Plattform analog zu den fachanwendungsspezifischen Diensten nutzen können. Jeder Dienst einer aAdG ist in der TI als Teilnehmer der TI identifizierbar. aAdG ist eine Anwendungskategorie weiterer Anwendungen. |

²¹² Vgl. [gemGlossar]

²¹³ Vgl. [gemGlossar], S. 7 sowie alle folgenden

| Begriff | Synonym / Abkürzung | Erläuterung / Definition |
|--|------------------------|--|
| andere Anwendungen des Gesundheitswesens ohne Zugriff auf Dienste der TI in angeschlossenen Netzen des Gesundheitswesens | aAdG-NetG | Die Anwendungskategorie „andere Anwendungen des Gesundheitswesens ohne Zugriff auf Dienste der TI in angeschlossenen Netzen des Gesundheitswesens“ umfasst an die TI angebundene Netze mit einer oder mehreren Anwendungen, deren Dienste netztechnisch über die TI durch Nutzer dieser Anwendung erreicht werden können. aAdG-NetG ist eine Anwendungskategorie weiterer Anwendungen. |
| Anwender | | Anwender sind natürliche Personen oder Organisationen, welche die TI-Services nutzen und dadurch i. d. R. einen Mehrwert für ihren Geschäftsprozess erwarten. Als Anwender werden dabei sowohl diejenigen Akteure bezeichnet, die tatsächlich mit dem IT-System arbeiten (es nutzen) als auch diejenigen, die eine Nutzung veranlassen und insofern für die bestimmungsgemäße Nutzung der Systeme verantwortlich sind. |
| Anwendungskonnektor | AK | Der Anwendungskonnektor ist ein Funktionsblock des Konnektors. Er bietet anwendungsnahe Basisdienste (inklusive SAK) und Fachmodule zur Nutzung durch ein Clientsystem an. |
| Apothekenverwaltungssystem | AVS | Primärsystem der Apotheker |
| Authentifizierung | | Die Authentifizierung bezeichnet den Vorgang, die Identität einer Person oder eines Rechnersystems anhand eines bestimmten Merkmals zu überprüfen. Die Authentifizierung stellt die Frage: Ist das die Person, die sie vorgibt zu sein? |
| Authentisierung | | Dies ist ein Verfahren zum Nachweis einer Identität. Als Beispiel kann die Passwortabfrage beim Starten eines Rechners genannt werden. Die Authentisierung beantwortet die Frage: Bin ich die Person, die ich vorgebe? |
| Authentizität | | Authentizität bezeichnet den Zustand, in dem die Identität eines Kommunikationspartners bzw. die Urheberschaft an einem Objekt sichergestellt ist. Unter dem Nachweis der Authentizität von elektronischen Daten versteht man den Nachweis über die Echtheit der Daten (Integrität) und die eindeutige Zuordnung zum Verfasser, Ersteller und/oder Absender. |
| Autorisierung | | Die Autorisierung beschreibt i. A. die Vergabe der Erlaubnis, etwas Bestimmtes zu tun |

| Begriff | Synonym / Abkürzung | Erläuterung / Definition |
|-----------------|------------------------|---|
| | | (Rechteverwaltung). Im Kontext Gesundheitskarte wird der Begriff insbesondere im Sinne von § 291a, Abs. 5 SGB V/GMG verwendet. So wird mittels der Autorisierung durch den Patienten bspw. definiert, dass ein im Vorfeld authentifizierter Arzt (Authentifizierung) auf ausgewählte Informationsobjekte (Zugriff auf freiwillige Anwendungen) ohne Anwesenheit der eGK des Versicherten zugreifen darf. |
| | | |
| Basisdienste | | Querschnittliche Leistungen der TI-Plattform auf logischer Ebene zur Unterstützung der Fachanwendungen mit allen nötigen technischen und organisatorischen Anteilen. Basisdienste werden in der anwendungs-unterstützenden Schicht der TI-Plattform angeboten. |
| Benutzer | | Wird einer Identität das Recht für den Zugriff auf ein oder mehrere Systeme beispielsweise durch die Vergabe einer Rolle erteilt, so spricht man von einem Benutzer. Einer Identität können mehrere Benutzer zugeordnet werden. Ein Benutzer kann mehrere Anmeldenamen besitzen, mit deren Hilfe er sich gegenüber verschiedenen IT-Systemen anmelden kann. |
| Benutzerkennung | | Anmeldename, mit dem sich der Administrator an der Managementschnittstelle der KoCoBox MED+ authentifiziert. |
| Berechtigter | | Natürliche Person, die vom Eigentümer eines Objektes (z.B. Daten, Fachanwendung) berechtigt wurde, das Objekt zu einem definierten Zweck zu nutzen. |
| Bestandsnetze | | Netze, die vor der Einführung der TI existierten und deren Anwendungen von den Leistungserbringern genutzt werden. Sie sind über die TI zugänglich. |
| Betreiber | | Betreiber sind Organisationen, welche Dienste der Telematikinfrastruktur bereitstellen. Die Betreiber der Telematikinfrastruktur sind im Dokument Betriebspolicy festgelegt. Betreiber können den Dienst selbst betreiben oder einen Provider mit dem Betrieb des Dienstes beauftragen. Sie verantworten die Einhaltung der zum Dienst gehörenden Betriebs- und Servicelevel gegenüber der gematik. Betreiber erhalten eine Anbieterzulassung gemäß §291a 1b, |

| Begriff | Synonym / Abkürzung | Erläuterung / Definition |
|------------------------------|------------------------|--|
| | | sofern sie nicht durch gesetzlichen Auftrag zur Bereitstellung eines Dienstes verpflichtet sind. |
| Betriebsführungsbuch | BfB | Im BfB der KoCoBox MED+ werden Abläufe und Vorgehensweisen für bestimmte Situationen bzw. Änderungen am Gerät vom dafür verantwortlichen Administrator / Benutzer mit Unterschrift dokumentiert. |
| Byte | B | Byte ist eine Standardeinheit, um Speicherkapazitäten oder Datenmengen zu bezeichnen und steht für ein Oktett von Bits. (1 Byte= 8 Bit) |
| Card-to-Card Authentisierung | | <p>Sie umfasst</p> <ul style="list-style-type: none"> a) einseitige asymmetrische Authentisierung ohne Aushandlung eines Sessionkey, b) einseitige symmetrische Authentisierung ohne Aushandlung eines Sessionkey, c) gegenseitige asymmetrische Authentisierung ohne Aushandlung eines Sessionkey, d) gegenseitige symmetrische Authentisierung ohne Aushandlung eines Sessionkey, e) gegenseitige asymmetrische Authentisierung mit Aushandlung eines Sessionkey, und Aufbau eines Secure Messaging Kanals f) gegenseitige symmetrische Authentisierung mit Aushandlung eines Sessionkey, und Aufbau eines Secure Messaging Kanals <p>Die externe Authentisierung mit Ausnahme von e verändert den Authentisierungsstatus der prüfenden Chipkarte.</p> |
| Certification Authority | CA | Siehe unten: Zertifizierungsstelle |
| Clientsystem | | Bezeichnung für dezentrale Systeme, die als Clients mit der TI interagieren, ohne Bestandteil der TI zu sein (z.B. PVS-, AVS-, KIS-Systeme, E-Mail-Clients). Sie bestehen aus Hard- und Software-Bestandteilen. |
| Clientsystem-Schnittstelle | | Über diese vom Konnektor angebotene Schnittstelle können Clientsysteme einerseits die Fachanwendungen der Telematikinfra-struktur, andererseits aber auch Funktionen der Basisdienste des Konnektors als so genannte Basisanwendungen |

| Begriff | Synonym / Abkürzung | Erläuterung / Definition |
|------------------------------------|------------------------|--|
| | | aufrufen. Die cetp-Schnittstelle ist ebenfalls Bestandteil der Clientsystem-Schnittstelle. |
| Certificate Revocation List | CRL | Zertifikatssperrliste; Liste, die die Ungültigkeit von Zertifikaten beschreibt; anhand der CRL ist feststellbar, ob ein Zertifikat gesperrt oder widerrufen wurde und warum. |
| Cryptographic Message Syntax | CMS | Cryptographic Message Syntax (CMS; deutsch Kryptographische Nachrichtensyntax) ist ein Standard vom IETF für gesicherte kryptographische Mitteilungen. CMS ist die Obermenge des PKCS #7 (Public-Key Cryptography Standards #7) welche auf S/MIME aufsetzt. Der Version 2 lag der gleiche Standard zugrunde. Ab Version 3 spricht man von Cryptographic Message Syntax. CMS wird beschrieben in Abstract Syntax Notation One (ASN.1). Die Architektur von CMS setzt auf X.509 Verschlüsselung bzw. Zertifikaten auf. |
| Connector Event Transport Protocol | cetp | Kommunikationsprotokoll für die Zustellung von Ereignissen des Konnektors an Clientsysteme. |
| ContractID | | Vertragsnummer des Vertrags, den der LE / Betriebsstättenverantwortliche mit dem Zugangsdienstprovider (ZGDP) hat. |
| Datenschutz | | Bezeichnet den Schutz vor Missbrauch bei der Verarbeitung und Speicherung personenbezogener oder personenbeziehbarer Daten. Das eigentliche Schutzobjekt sind hierbei nicht nur persönliche Daten, sondern vielmehr unmittelbar die Persönlichkeitsrechte jeder natürlichen Person als Individuum. |
| Dienst | Service | Der Begriff wird in der IT verwendet zur Bezeichnung von technischen, in sich geschlossenen Funktionskomponenten, die einen Prozess unterstützen. Der Dienst wird dabei über eines oder mehrere Netzwerkprotokolle der Anwendungsschicht realisiert. Im Sinne der Telematikinfrastruktur ist ein Dienst immer eine Entität, die normalerweise über Netzwerkprotokolle angesprochen wird und damit eine physische Ausprägung besitzt (siehe auch Service). |
| Domain Name System / Namensdienst | DNS | Bezeichnung für das im Internet verwendete System von hierarchisch gegliederten Bereichsnamen. Über die Domain-Datenbanken wird eine Zuordnung von |

| Begriff | Synonym / Abkürzung | Erläuterung / Definition |
|----------------|--------------------------------|---|
| | | sprechenden Server-Namen in IP-Adressen vorgenommen. Der Namensdienst ist ein Produkttyp. |

| | | |
|-------------------------------------|------|---|
| Dynamic Host Configuration Protocol | DHCP | Ermöglicht mit Hilfe eines entsprechenden Servers die automatische Zuweisung einer IP-Adresse und weiterer Konfigurationsparameter am Computer in einem Netzwerk. |
| eHealth-Kartenterminal | | LAN-fähiges Kartenterminal nach SICCT-Spezifikation, das die spezifischen Anforderungen zum Lesen und Schreiben von Daten auf die eGK und zur sicheren Kommunikation mit der Telematikinfrastruktur erfüllt. Das eHealth-Kartenterminal ist ein Produkttyp. |
| ECC Brainpool | | Der ECC-Brainpool, eine Arbeitsgruppe des staatlich-industriellen Vereins TeleTrust (Mitglieder u. a. BKA, BSI) zum Thema Elliptic Curve Cryptography, hat 2005 eine Anzahl von elliptischen Kurven spezifiziert, welche im März 2010 im RFC 5639 der IETF standardisiert wurde. Bei diesen Kurven ist besonders die Wahl der Bitlänge 512 zu erwähnen, abweichend zur von vielen anderen Institutionen (z. B. NIST, SECG) präferierten Bitlänge 521. |
| ECC NIST | | ECC-Verfahren sind ein relativ junger Teil der asymmetrischen Kryptografie und gehören seit 1999 zu den NIST-Standards. Das sind aber keine eigenständigen kryptografischen Algorithmen, sondern sie basieren im Prinzip auf dem diskreten Logarithmus bei reellen Zahlen, wie man es von Diffie-Hellman und DSA kennt. |
| eIDAS-Verordnung | | eIDAS (englisch: e lectronic I dentification, A uthentication and trust S ervices), in Deutschland auch IVT, bezeichnet die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (Signaturrichtlinie). |
| Einboxkonnektor | | Die Funktionsblöcke Anwendungskonnektor und Netzkonnektor sind hier in einer physischen Einheit gebündelt. Diese Ausprägung des Konnektors ist für den Betrieb kleiner und mittelgroßer Leistungserbringereinrichtungen ausgelegt und wird durch den Hersteller des Konnektors als Komplettsystem ausgeliefert. |
| Einmalpasswort | | Einmalig zu verwendendes Passwort bei der Erstanmeldung eines neuen Benutzers / Administrators, das nach erstmaligem Gebrauch gewechselt werden muss. |

| | | |
|---|-----|---|
| elektronische Gesundheitskarte | eGK | Die elektronische Gesundheitskarte ist gemäß § 291 a SGB V eine personenbezogene Identifikationskarte, die Versicherte der Gesetzlichen (GKV) und der Privaten (PKV) Krankenversicherung zur Inanspruchnahme ärztlicher und zahnärztlicher Behandlung gemäß § 15 SGB V berechtigt. Sie enthält gemäß § 291 a SGB V Angaben, die für die Übermittlung elektronisch veranlasster ärztlicher Verordnungen geeignet sind. |
| elektronische Patientenakte | ePA | Die ePA ist eine geplante Datenbank, in der die Anamnese, Behandlungsdaten, Medikamente, Allergien und weitere Gesundheitsdaten der Krankenversicherten sektor- und fallübergreifend, landesweit einheitlich gespeichert werden sollen. |
| Endkunde | | Damit ist der Leistungserbringer z.B. Arzt oder Apotheker gemeint. |
| Ethernet | | Derzeit gebräuchlichste LAN-Technologie. |
| Fachanwendung | | Die Fachanwendung ist eine Anwendung der TI mit allen nötigen technischen und organisatorischen Anteilen auf Anwendungsebene. Fachanwendungen nutzen die TI-Plattform unter Berücksichtigung der Schnittstellen- und Ablaufdefinitionen und richten sich nach der Nutzungspolicy. |
| Fachmodul | | Ein dezentraler Anwendungsanteil der Fachanwendung innerhalb der TI mit sicherer Anbindung an die TI-Plattform unter Nutzung der Schnittstellen- und Ablaufdefinitionen der TI-Plattform. |
| Firmware | FM | „Fest eingebrannte“ Betriebssoftware eines Gerätes. |
| Fortgeschrittene elektronische Signatur | | Sie erfüllt folgende Anforderungen: <ul style="list-style-type: none"> a) ist eindeutig dem Unterzeichner zugeordnet; b) ermöglicht die Identifizierung des Unterzeichners; c) wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen seiner alleinigen Kontrolle verwenden kann; d) ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann. |
| | | |

| | | |
|---------------------------------------|----------------------------|--|
| Fully-Qualified Domain Name | FQDN | Ein absoluter Domain Name innerhalb eines DNS Namensraumes, der ausgehend vom Knoten, den er kennzeichnet, die Labels aller darüber liegenden Hierarchiestufen bis zum Wurzelverzeichnis (root) enthält. |
| Gesundheitstelematik | | (...) Gesundheitstelematik beinhaltet die Telematikinfrastruktur sowie Infrastrukturen für eine Nachnutzung der TI in weiteren Anwendungen im Gesundheitswesen einschließlich der dafür benötigten Betriebsinfrastrukturen. Auch das Typ2-Netz, Mehrwertnetze und die darüber angeschlossenen Mehrwertdienste sind Teil der Gesundheitstelematik. |
| Hersteller | | Hersteller der TI stellen ein Produkt gemäß den Spezifikationen der gematik her und übernehmen die Produkthaftung gemäß den gesetzlichen Vorgaben und den Support gegenüber ihren Kunden. Hersteller von dezentralen Produkten der TI unterscheiden sich von Anbietern insbesondere dadurch, dass das verantwortete Produkt keinen IT-Service darstellt, sondern physische Geräte oder Software, welche in der Hoheit der Anwender betrieben werden. |
| Hypertext Transfer Protocol | http | HTTP ist ein Protokoll zur Übertragung von Daten, das insbesondere im Rahmen des World Wide Web zum Einsatz kommt und sich meist auf das verbindungsorientierte TCP stützt. |
| Institutionskarte | Security Module Card Typ B | Die Institutionskarte entspricht technisch weitgehend dem Heilberufsausweis (HBA), bezieht sich jedoch auf eine organisatorische Instanz des Gesundheitswesens (z.B. Praxis, Apotheke, Krankenhaus). Die Institutionskarte wird auch als Security Module Card Typ B (SMC-B) bezeichnet. |
| Integrated Circuit Card Serial Number | ICCSN | Die ICCSN ist die weltweit eindeutige Identifikationsnummer eines Chipmoduls einer Smartcard. Für die Karten der TI schlüsselt sich die ICCSN auf in (a) Ident-Nummer des Herausgebers (IIN) mit dem Branchen-hauptschlüssel, dem Länderkenn-zeichen und Kartenherausgeberschlüssel sowie (b) der kartenindividuellen Seriennummer. |

| | | |
|-----------------------------------|------|--|
| Integrität | | Integrität bezeichnet die Sicherstellung der Unverfälschtheit von Informationsobjekten und Systemen. Der Verlust der Integrität von Informationsobjekten kann bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden. Datenintegrität bezeichnet die Integrität von gespeicherten und übertragenen Daten. Systemintegrität bezeichnet die Unverfälschtheit von Programmen und Programmcode und damit die korrekte Funktion der Anwendungen, IT-Infrastruktur und Systemkomponenten. |
| Internet Access Gateway | IAG | Die Bezeichnung steht für die Geräte, die den Internetzugang ermöglichen und typischerweise vom Internet Service Provider (ISP) zur Verfügung gestellt werden (z.B. Router mit DSL Router und DSL Modem). |
| Internet Control Message Protocol | ICMP | Es dient in Rechnernetzwerken dem Austausch von Informations- und Fehlermeldungen über das Internet-Protokoll in der Version 4 (IPv4). Für IPv6 existiert ein ähnliches Protokoll mit dem Namen ICMPv6. |
| Installation | | Funktionsfähige Bereitstellung von Hardware und Software in einer definierten Umgebung. |
| Integrität | | Integrität bezeichnet die Sicherstellung der Unverfälschtheit von Informationsobjekten und Systemen. Der Verlust der Integrität von Informationsobjekten kann bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden. Datenintegrität bezeichnet die Integrität von gespeicherten und übertragenen Daten. Systemintegrität bezeichnet die Unverfälschtheit von Programmen und Programmcode und damit die korrekte Funktion der Anwendungen, IT-Infrastruktur und Systemkomponenten. |
| Interface | | Schnittstelle eines Systems, auf die durch andere Systeme zugegriffen werden kann. Bei der KoCoBox MED+ ist zum Beispiel die Managementschnittstelle das Interface zur Administration des Geräts. |
| Intermediär | | Vermittler zwischen zwei Systemen, wobei beide Systeme jeweils dem Intermediär vertrauen, nicht jedoch zwangsweise einander. Der Intermediär VSDM wird als fachanwendungsspezifischer Dienst in der TI betrieben. Er unterstützt die |

| | | |
|---|----------------------|---|
| | | Anwendungsfälle der Fachanwendung VSDM, indem er Nachrichten vom Fachmodul an die Fachdienste VSDM weiterreicht und die Antworten zustellt. Der Intermediär ist ein Produkttyp und gehört zur Anwendung VSDM. |
| Internet Service Provider | ISP | Anbieter von Internetdiensten |
| IT Service Management TI | ITSM-TI | Von der gematik auf die spezifischen Anforderungen der Telematikinfrastruktur (TI) im deutschen Gesundheitswesen aus-gerichtetes ITSM-Framework. Das ITSM-TI orientiert sich am Standard IT Service Management, basierend auf ITIL V3. Das lokal implementierte ITSM der Anbieter und Hersteller ist über durch die gematik definierte Schnittstellen (Reporting, übergreifende Service-Management-Prozesse) mit dem ITSM-TI verbunden. |
| | | |
| Kartenterminal, eHealth | eH-KT | LAN-fähiges Kartenterminal nach SICCT-Spezifikation, das die spezifischen Anforderungen zum Lesen und Schreiben von Daten auf die eGK und zur sicheren Kommunikation mit der Telematikinfrastruktur erfüllt. Das E-Health-Kartenterminal ist ein Produkttyp. |
| Kommunikation im Medizinwesen | KIM (früher: KOM-LE) | KIM sorgt für den sicheren Austausch von sensiblen Informationen wie Befunden, Bescheiden, Abrechnungen oder Röntgenbildern über die TI und verbindet damit Nutzer im Gesundheitswesen über Einrichtungs-, System- und Sektorengrenzen hinweg. |
| Komponente | | Innerhalb der TI werden Komponenten als dezentrale Produkttypen bezeichnet. |
| Konfigurations- und Software-Repository | KSR | Basisdienst der TI-Plattform mit zentralen und dezentralen Schnittstellen, verwaltet Konfigurationsdaten und Software Updates für dezentrale Produkte. |
| Konfigurationsdienst | | Der Konfigurationsdienst ist ein zentraler Dienst der TI für die Bereitstellung von Konfigurationsdaten und Softwareupdates dezentraler Komponenten (Konnektoren, Kartenterminals). Updates zugelassener Funktionalitäten und Konfigurationsdaten können von den Herstellern auf diesem Weg zum Download bereitgestellt werden. Der Konfigurationsdienst ist ein Produkttyp und ein betriebsunterstützendes System im Rahmen des ITSM-TI. |

| | | |
|----------------------------|-----|---|
| Konnektor | | Der Konnektor koordiniert und verschlüsselt die Kommunikation zwischen Clientsystem, eGK, HBA/SMC und zentraler Telematikinfrastruktur. Er stellt damit das Bindeglied zwischen diesen Komponenten auf Leistungserbringerseite bzw. eKiosk und Telematikinfrastruktur dar. Der Konnektor ist ein Produkttyp. |
| Konnektoridentität | | Die Geräteidentität des Konnektors teilt sich in drei Identitäten auf, eine für den Netzkonnektor, eine für den Anwendungskonnektor und eine für die Signaturanwendungskomponente. |
| Leistungserbringer | LE | Ein Leistungserbringer gehört zu einem zugriffsberechtigten Personenkreis nach § 291a Abs. 4 SGB V und erbringt Leistungen des Gesundheitswesens für Versicherte. |
| Lieferant | | Lieferant ist der Reseller, bei dem der Endkunde die Box bezieht und mit dem er einen Service-Vertrag abgeschlossen hat. |
| MAC Adresse | | eindeutige Hardware-Adresse einer Netzwerkkarte |
| Maximum Transmission Unit | MTU | Die MTU beschreibt die maximale Paketgröße eines Protokolls der Vermittlungsschicht (Schicht 3) des OSI-Modells, gemessen in Oktetten, welche ohne Fragmentierung in den Rahmen (engl. ‚Frames‘) eines Netzes der Sicherungsschicht (Schicht 2) übertragen werden kann. |
| Memory Management Unit | MMU | (...) benennt eine Hardwarekomponente eines Computers, welche den Zugriff auf den Arbeitsspeicher verwaltet. |
| Namensdienst | DNS | Siehe oben: Domain Name Server |
| Network Time Protocol, The | NTP | Ein Netzwerkprotokoll, das mit dem Hintergrund entwickelt wurde, eine Vielzahl von vernetzten Systemen mit einer einheitlichen Zeitinformation zu versorgen, so dass diese Systeme auch tatsächlich über eine einheitliche Systemzeit verfügen. Die Entwicklung lässt sich zurückverfolgen bis zu einer Vorführung während der US National Computer Conference im Jahr 1979, während derer erste Gedanken zu einer weltweiten Computerzeitsynchronisation geäußert wurden. (Quelle: [CNTS]) |

| | | |
|-------------------------|------------|---|
| Netzkonnektor | NK | Der Netzkonnektor als dezentrale Komponente der TI-Plattform stellt die sichere Verbindung auf Netzwerkebene zwischen den dezentralen Systemen auf der einen Seite und den zentralen Diensten der TI-Plattform sowie den fachanwendungsspezifischen Diensten auf der anderen Seite her. |
| NTP-Server | | Serversysteme, die mittels NTPd (NTP daemon) Zeitsynchronisationsdienste anbieten und sich selbst mit einer Zeitquelle synchronisieren können. In Deutschland bietet die Physikalisch-Technische Bundesanstalt beispielsweise öffentliche Stratum 1 Server an, die unter den Namen ptbtime1.ptb.de und ptbtime2.ptb.de erreichbar sind. |
| | | |
| OCSP-Responder Proxy | OCSP-Proxy | Der OCSP-Responder Proxy ermöglicht die Statusprüfungen von Zertifikaten, deren OCSP-Responder nicht direkt an die TI angeschlossen sind. Dies gilt für OCSP-Responder der Bundesnetzagentur (BNetzA) sowie für OCSP-Responder der HBA-Vorläuferkarten. Die OCSP-Responses der BNetzA werden durch den OCSP-Proxy gecacht, um die Performance zu erhöhen und die Belastung des OCSP-Responders der BNetzA gering zu halten. Der OCSP-Responder Proxy ist ein Produkttyp. |
| Offline-Modus Konnektor | | Im Offline-Modus des Konnektors kann keine Verbindung zum VPN-Zugangsdienst aufgebaut werden (z. B. weil die WAN-Schnittstelle nicht angeschlossen oder die Verbindung gestört ist). |
| Online-Modus Konnektor | | Im Online-Modus des Konnektors besteht eine VPN-Verbindung zur zentralen Telematikinfrastruktur oder es wird davon ausgegangen, dass diese Verbindung jederzeit aufgebaut. |
| Online-Prüfung der VSD | | Gemäß § 291 SGB V gesetzlich vorgegebene Prüfung auf Gültigkeit und Aktualität der Versichertenstammdaten (VSD), beinhaltet folgende Schritte: <ul style="list-style-type: none"> - Prüfung der Gültigkeit der eGK - Prüfung der Aktualität der VSD - Aktualisierung der Daten, wenn Änderungen vorliegen Die Initiierung der Anwendungsfälle erfolgt durch einen Funktionsaufruf aus dem Primärsystem oder über das Standalone-Szenario. |
| | | |

| | | |
|-----------------------------------|------|--|
| Online-Produktivbetrieb (Stufe 1) | OPB1 | Im Rahmen des OPB1 wurden die Fachanwendungen VSDM und KIM (früher: KOM-LE) und ein Basisdienst für die Nutzung der qualifizierten elektronischen Signatur eingeführt. |
| Online-Rollout (Stufe 1) | ORS1 | Definierte Phase zur Einführung der TI. Nach erfolgreichem Abschluss des Basis-Rollouts erfolgte im Online-Rollout (Stufe 1) der Aufbau und Erprobungsbetrieb der dezentralen und der zentralen Produkte der TI. (...) |
| Pairing | | Bezeichnet den Prozess der logischen Verknüpfung zweier Komponenten durch den Austausch eindeutiger und geheimer Informationen. Das Pairing zwischen Konnektor und E-Health-Kartenterminal versetzt den Konnektor in die Lage, Kartenterminals zu erkennen, die für den Betrieb mit diesem Konnektor vorgesehen sind. Das Pairing ermöglicht es einem Kartenterminal und einem Konnektor, sich nach dem TLS-Verbindungsaufbau gegenseitig zu authentifizieren. |
| Personal Identification Number | PIN | Eine PIN ist eine in der Regel vier- bis achtstellige persönliche Geheimzahl, welche zur Authentifizierung ihres Inhabers bei der Nutzung elektronischer Anwendungen genutzt wird. So kann z.B. über eine PIN eine Signaturerstellungseinheit vor unberechtigtem Zugriff geschützt werden. |
| Primärsystem | PS | Ein IT-System, das bei einem Leistungserbringer eingesetzt wird – z.B. eine Praxisverwaltungssoftware (PVS), ein Krankenhausinformationssystem (KIS) oder eine Apothekensoftware (AVS) – und sich unter dessen administrativer Hoheit befindet. Das Primärsystem ist kein Bestandteil der TI-Plattform. |
| Produkt | | Ein Produkt ist eine konkrete Realisierung eines Produkttyps. Es setzt die an den Produkttyp gestellten Anforderungen um und ist diesbezüglich testbar bzw. prüfbar. Produkte der TI werden durch die gematik zugelassen. |
| Protokollierung | | In der Telematikinfrastruktur versteht man unter „Protokollierung“ sowohl das fachliche (Audit), als auch das technische Protokollieren (Logging) von Daten. |
| Protection Profiles | PP | Schutzprofile |

| | | |
|--------------------------------------|-----------------------|---|
| Provider | | Ein Provider ist im Kontext der TI ein Anbieter oder Dienstleister. |
| Qualifizierte elektronische Signatur | QES | Qualifizierte elektronische Signatur ist eine fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht. |
| Rechteverwaltung | Permission Management | Die Rechteverwaltung ist die konzeptionelle und administrative Festlegung von Zugriffsrechten von Benutzern/Subjekten, also z.B. die Zuordnung von Benutzern zu Gruppen, basierend auf der Identität des Benutzers/Subjekts. |
| Rolle | | Eine Rolle beschreibt die Verhaltensweise eines Akteurs in einer definierten Aufgabenstellung. Bei der KoCoBox MED+ kann man in der Benutzerverwaltung verschiedene Rollen anlegen, die über unterschiedliche Rechte bei der Administration verfügen. Die Rechte sind jeweils pro Rolle definiert. Dies entspricht dem Konzept einer rollenbasierten Zugangskontrolle. |
| Router | | Aktive Netzwerkkomponente, die zwischen zwei Netzen gleichen Typs mit unterschiedlichen Adressräumen vermittelt. |
| Schlüsselgenerierungsdienst | SGD | Ein Schlüsselgenerierungsdienst generiert Schlüssel für eine Entität, die sich mittels einer eGK, einer alternativen Versichertenidentität, einer SMC-B oder einer SMC-KTR gegenüber dem SGD authentisiert hat. Für einen Versicherten müssen zwei SGD zur Verfügung stehen: ein SGD 1, der dem Akten-system beige-stellt ist, und ein SGD 2 außerhalb des Aktensystems. Der SGD 1 (SGD FAD) ist ein fachanwendungsspezifischer Dienst (FAD), der auf Nutzeranfrage verschiedene versichertenindividuelle AES-Schlüssel generiert. Der SGD 2 (SGD TIP) wird auf der TI-Plattform betrieben. |
| Schutzprofile | Protection profiles | Schutzprofile ermöglichen es, eine Sicherheitslage anhand von Gefährdungen, Annahmen über die Betriebsumgebung der IT, Sicherheitszielen usw. zu beschreiben. Schutzprofile bilden somit die Grundlage für die Standardisierung der |

| | | |
|--|---------------------|--|
| | | Sicherheitsanforderungen an bestimmte Produkte und deren Prüfung. |
| Secure Internet Service | SIS | Gesicherter Internetzugang |
| Security Module Card Typ B | SMC-B | Die SMC-B ist ein Schlüsselspeicher für die privaten Schlüssel, die eine Einheit oder Organisation des Gesundheitswesens (z.B. Praxis, Apotheke, Krankenhaus) ausweisen. Diese Schlüssel dienen als Ausweis gegenüber der eGK und gegenüber anderen Komponenten der TI. Die Security Module Card Typ B ist ein Produkttyp. |
| Service | | Ausschnitt aus der von der Telematikinfrastruktur angebotenen Funktionalität. Die Funktionalität (Operation(en)) wird über ein Interface aufgerufen. Im Gegensatz zum Dienst muss das Interface nicht unbedingt über Netzwerkprotokolle adressiert werden. Beispiel ist die Ticketservice-Komponente des Konnektors. Im Sinne der Gesundheitstelematik kann ein Service auch eine Prozessunterstützung sein. In diesem Handbuch wird Service seiner umgangssprachlichen Verwendung nach auch in Zusammenhang mit Dienstleistungen, die für die Installation bzw. Wartung und Betrieb erbracht werden, verwendet. |
| Servicepartner (Systempartner) | | Der Servicepartner ist die Firma, die u.a. vor Ort mittels Service-Techniker den Servicevertrag erfüllt. |
| Servicevertrag | SVT | Ein Servicevertrag (SVT) ist eine Vereinbarung mit einem externen Kunden und enthält Absprachen über die Erbringung von definierten Services. Da er eine externe Vereinbarung ist, entspricht ein Servicevertrag einem Vertrag im juristischen Sinne sowie Dienstleistungsvereinbarung. Die juristischen Regelungen sind im Rahmenvertrag enthalten. Dienstleistungen werden in den zum Rahmenvertrag gehörenden Leistungsscheinen definiert und die dazu gehörenden SLAs spezifizieren die Leistungsparameter. |
| Sichere Kommunikation zwischen Leistungserbringern | KOM-LE (heute: KIM) | Die Fachanwendung KOM-LE ermöglicht den vertraulichen und sicheren Austausch von Nachrichten und medizinischen Dokumenten zwischen den Teilnehmern der Telematikinfrastruktur – über alle Sektoren und Berufsgruppen hinweg. |
| Sicherheit | Safety, Security | Objektiv ist Sicherheit eine Sachlage, bei der das Risiko nicht größer als ein identifiziertes Grenzniveau ist. Subjektiv ist Sicherheit das sich immer wieder bestätigende Gefühl von bestimmten negativen |

| | | |
|------------------------------|-------------------------------|---|
| | | Ereignissen nicht getroffen zu werden. Im Deutschen werden darunter die beiden Teilbereiche „Safety“ und „Security“ gemeinsam beschrieben: Safety ist dem Schutz von Menschen und Sachwerten vor dem Versagen technischer Systeme gewidmet und Security als Schutz von Informationen und Informationsverarbeitung gegen intelligente Angreifer gedacht. Eine Vielzahl sicherheitskritischer Anwendungen zeigt das starke Zusammenwachsen dieser Themenbereiche, die aber trotz allgemeinen Bemühens immer noch weitgehend nebeneinanderher bearbeitet werden. |
| Sicherheitsanforderung | Security / Safety Requirement | Sicherheitsanforderungen legen fest, gegen welche kritischen Bedrohungen eines IT-Systems bzgl. Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität Maßnahmen ergriffen werden müssen. Sicherheitsanforderungen bauen entweder auf funktionalen oder nicht-funktionalen Anforderungen auf und detaillieren ausschließlich deren Sicherheitsrelevanz oder sie beschreiben eigenständige Anforderungen, die nur Sicherheitsaspekte erfüllen. Sie klassifizieren sich in Sicherheitsanforderungen mit und ohne Geheimhaltung. |
| Sicherheitskonzept | | Das Sicherheitskonzept ist die Dokumentation der Anwendung der einheitlichen Methoden der Informationssicherheit der TI. |
| sicherheitsrelevant | | (a) Eine Komponente/ein Dienst/ein Prozess ist sicherheitsrelevant, wenn diese/dieser korrekt arbeiten/funktionieren muss, um die Sicherheit (des Systems) zu gewährleisten. (b) Ein Informationsobjekt ist sicherheitsrelevant, wenn dessen Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit oder Nichtabstreitbarkeit geschützt werden muss, um die Sicherheit (des Systems) zu gewährleisten. |
| Signaturanwendungskomponente | SAK | Signaturanwendungskomponenten sind gemäß [eIDAS-VO] Kap. 1, Art. 3/23 zumindest Signaturerstellungseinheiten, d.h. Software- und Hardwareprodukte, die dazu bestimmt sind, Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen. |
| | | |

| | | |
|------------------------|-----|---|
| Standalone-Szenario | | Im Standalone-Szenario erfolgt die Online-Prüfung der VSD ohne Netzanbindung des PVS an die Telematikinfrastruktur. Dabei wird beim Stecken der eGK vom Fachmodul VSDM in der Online-Umgebung automatisch eine Online-Prüfung initiiert. Das Lesen der VSD kann dabei durch das Primärsystem mittels einer physikalischen Trennung (zwei Konnektoren mit Kartenterminal) oder einer logischen Trennung (Konnektor mit logischer Trennung) ohne direkte Netzanbindung an die TI durchgeführt werden. |
| Switch | | Verbindet mehrere Geräte in einem LAN |
| System | | Die Gesamtheit miteinander verknüpfter und sich gegenseitig beeinflussender Elemente, die entsprechend einem bestimmten Zweck organisiert ist. Das System hat eine gänzlich andere Qualität als die Summe seiner Elemente. |
| Target of Evaluation | TOE | Evaluationsgegenstand (EVG) |
| Telematik | | Telematik ist zusammengesetzt aus den Begriffen Telekommunikation und Informatik. Er beschreibt die Zusammenführung, Verarbeitung und Weitergabe verteilter, u.U. heterogener Datenbestände. |
| Telematikinfrastruktur | TI | Die Telematikinfrastruktur ist die bevorzugte Informations-, Kommunikations- und Sicherheitsinfrastruktur des deutschen Gesundheitswesens mit allen technischen und organisatorischen Anteilen. Die TI vernetzt alle Akteure und Institutionen des Gesundheitswesens miteinander und ermöglicht dadurch einen organisations-übergreifenden Datenaustausch innerhalb des Gesundheitswesens. Die TI unterstützt die Anwendungen der Versicherten gemäß §291a SGB V und bildet darüber hinaus die Plattform für weitere interoperable und kompatible IT-Anwendungen im deutschen Gesundheitswesen. Die TI enthält die Komponenten und Dienste der TI-Plattform, die Fachdienste, die Client- und die Fachmodule. |
| TI-Plattform | | Die TI-Plattform als anwendungsunabhängiger Teil der TI dient der Unterstützung der Fachanwendungen mit allen nötigen technischen und organisatorischen Anteilen. Enthalten sind alle nötigen Schnittstellen- und Ablaufdefinitionen für die Fachanwendungen auf den Schichten Netzwerk, Infrastruktur und Anwendungsunterstützung. Die TI- |

| | | |
|-----------------------------|--------------|--|
| | | Plattform besteht aus dezentralen Komponenten, den zentralen Diensten und dem Zugangsnetz. |
| Transport Layer Security | TLS | Transport Layer Security (TLS, deutsch Transportschichtssicherheit; Vorgängerbezeichnung: Secure Sockets Layer, SSL, letzte Version: 3.0), ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. SSL wurde abgelöst mit neuem Namen TLS und beginnend mit Version 1.0 weiterentwickelt und standardisiert. |
| Trustcenter | | Institution, die Zertifikate im Zusammenhang mit der digitalen Signatur ausgibt, welche die Identität einer Person oder eines Systems bestätigen (Zertifizierungsstelle). |
| Trust Service Provider | TSP | Organisation, welche einen oder mehrere (elektronische) Trust Services anbietet |
| Trust-service Status List | TSL | Eine Trust-service Status List bietet alle relevanten Informationen zur vertrauenswürdigen Verteilung und Prüfung der Wurzelzertifikate verschiedener „Certification Authorities“ in Form einer signierten XML-Datei (ETSI-Standard). Hierdurch können auch bereits existierende heterogene PKI's nach einem einheitlichen Schema eingebunden werden. |
| | | |
| Uniform Resource Identifier | URI | Ein Uniform Resource Identifier (Abk. URI, englisch für einheitlicher Bezeichner für Ressourcen) ist ein Identifikator und besteht aus einer Zeichenfolge, die zur Identifizierung einer abstrakten oder physischen Ressource dient. |
| Uniform Resource Locator | URL | Standard zur Adressierung beliebiger Objekte im Internet. Bsp.: Webseiten, PDF-Dokumente, Grafiken und Audiodateien. |
| User Datagram Protocol | UDP | Das UDP ist ein minimales, verbindungsloses Netzwerkprotokoll, das zur Transportschicht der Internetprotokollfamilie gehört. UDP ermöglicht Anwendungen den Versand von Datagrammen in IP-basierten Rechnernetzen. |
| | | |
| Vertrauenswürdig | trust worthy | In der IT-Sicherheit gilt ein System als vertrauenswürdig, wenn es die gesetzten Sicherheitsziele nach dem aktuellen Stand der Technik derart erfüllt, dass ein Nicht-Erreichen der Schutzziele unmöglich erscheint. Die Vertrauenswürdigkeit repräsentiert das subjektive Empfinden einer Person über den Zustand eines Systems. Die Vertrauenswürdigkeit |

| | | |
|---------------------------------------|-----------------|---|
| | | kann durch Maßnahmen wie z.B. eine Zertifizierung von Produkten erhöht werden. |
| Vertraulichkeit | Confidentiality | Vertraulichkeit ist Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten / Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein. |
| Versichertenstammdatenmanagement | VSDM | VSDM ist eine Fachanwendung der TI und rea-lisiert die Onlineprüfung und -aktualisierung der Versichertenstammdaten auf der eGK. Sie beinhaltet das dezentrale Fachmodul VSDM, den Intermediär VSDM sowie die Schnittstellen und Kommunikation zu den Fachdiensten VSDM (UFS, VSDD, CMS) und zu den Primärsystemen und beschreibt die Funktionalität des VSDM. |
| Vertrauensdienstegesetz | VDG | Das deutsche Vertrauensdienstegesetz ergänzt die eIDAS-Verordnung (EU) Nr. 910/2014. |
| Vertrauenswürdige Ausführungsumgebung | VAU | Die Vertrauenswürdige Ausführungsumgebung definiert die technischen Mechanismen zur Gewährleistung von Datenschutz- und Informationssicherheitseigenschaften. Dazu gehören z.B. <ul style="list-style-type: none"> - Erkennung und Schadensreduzierung und -verhinderung von Angriffen - Ausschluss der schadhaften Einwirkung der Verarbeitung von Daten eines Versicherten auf die Verarbeitung von Daten eines anderen Versicherten - Ausschluss des Betreibers vom Zugriff auf die personenbezogenen medizinischen Daten - Überprüfbarkeit des Sicherheitszustands des Systems aus Sicht des sich verbindenden Systems |
| Virtuelles Privates Netz | VPN | Bei einem VPN wird unter Verwendung kryptographischer Mechanismen und öffentlicher Transportnetze (z.B. Internet) ein virtuelles privates Netz geschaffen, in dem die Teilnehmer so sicher wie in einem lokalen Netz kommunizieren können. |
| VPN-Konzentrator | VPN-K | Sammelpunkt für mehrere VPN-Verbindungen. |
| | | |
| Wide Area Network | WAN | Globales Netzwerk, bei dem der private Entscheidungsbereich des Anwenders verlassen wird, d.h. zur Datenübertragung müssen i.d.R. öffentliche Leitungen (bspw. das Kabelnetz der Deutschen Telekom) eingesetzt werden. |
| | | |

| | | |
|-----------------------|---------------------------------------|---|
| Zeitdienst | | Der Zeitdienst stellt eine NTP-basierte Zeitsynchronisation zur Verfügung. Der Zeitdienst ist ein Produkttyp. |
| Zertifizierungsstelle | Certificate / Certification Authority | In der Informationssicherheit ist eine Zertifizierungsstelle (englisch certificate authority oder certification authority) eine Organisation, die digitale Zertifikate herausgibt. |
| Zugangsdienstprovider | ZGDP | Bietet einen Zugang in die TI an. |
| Zugangskontrolle | Admission Control | Die Zugangskontrolle soll den unbefugten Zugang zu einem IT-System verhindern und führt hierzu eine Identifikation und eine Überprüfung der angegebenen Identität (Authentifizierung) des Benutzers (Subjekt) durch, bevor der Zugang gewährt wird. Sie umfasst die Verwaltung der Benutzerkennungen (Benutzerverwaltung) und die Rechteprüfung beim Zugangsversuch, einschließlich der Beweissicherung. |
| Zugriffskontrolle | Access Control | Die Zugriffskontrolle eines IT-Systems soll den unbefugten Zugriff auf Objekte (z.B. Daten, Anwendungen) verhindern. Sie umfasst die Rechteverwaltung, die Rechtezuweisung und die Rechteprüfung beim Zugriffsversuch, einschließlich der Beweissicherung. |
| Zulassung | | Die Produkte der TI und deren Anbieter sind zur Teilnahme an der TI von der gematik zuzulassen. Die Zulassung wird Produkten der TI erteilt, wenn die gesetzlich geforderten Nachweise zur Funktionsfähigkeit, Interoperabilität und Sicherheit des Produkts (§291b Abs.1a SGB V) vorliegen. Anbieter werden zugelassen, wenn sie für den Betrieb der Produkte der TI die Anforderungen an Verfügbarkeit und Sicherheit ihrer Leistungen vorgelegt (§291b Abs.1a SGB V) erfüllen. |

9.9 Abkürzungsverzeichnis

| Abkürzung | Langform |
|------------------|---|
| aAdG | andere Anwendungen des Gesundheitswesens |
| AIS | Arztinformationssystem |
| AK | Anwendungskonnektor |
| AMTS | Arzneimitteltherapiesicherheit |
| API | Application Programming Interface |
| AUT | authentication, Authentifizierung |
| AVS | Apothekenverwaltungssystem |
| BÄK | Bundesärztekammer |
| BLZ | Betriebsleitzentrale |
| BNetzA | Bundesnetzagentur |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| CA | Certification Authority |
| CC | Common Criteria |
| CET | Central European Time |
| CMS | Cryptographic Message Syntax |
| CN | Common Name |
| CRL | Certificate Revocation List |
| CT-ID | Kartenterminal-ID |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System, Domain Name Service |
| DPE | Datensatz persönliche Erklärungen |
| ECC | Elliptic Curve Cryptography |
| eGK | elektronische Gesundheitskarte |
| eIDAS | electronic IDentification, Authentication and trust Services |
| ePA | elektronische Patientenakte |
| FM | Fachmodul |
| FQDN | Fully Qualified Domain Name |
| FTP | File Transfer Protocol |
| FW | Firmware |
| HBAX | Bezeichnung für Chipkarten des Typs HBA, HBA-qSig und ZOD 2.0 |

| Abkürzung | Langform |
|------------------|---|
| HSM-B | HSM-Variante einer Institutionskarte vom Typ B (Secure Module Card). Das SM-B wird als virtuelle Karte verstanden, die in einem virtuellen Kartenterminal steckt. |
| http | Hypertext Transfer Protocol |
| https | Hypertext Transfer Protocol Secure |
| IAG | Internet Access Gateway |
| IANA | Internet Assigned Numbers Authority |
| ICCSN | Integrated Circuit Card Serial Number |
| ICMP | Internet Control Message Protocol |
| IDP | Identitätsprovider |
| IP | Internet Protocol |
| ISP | Internet Service Provider |
| IT | Informationstechnik |
| JVM | Java Virtual Machine |
| KB | Kilo Byte (1024 Bytes) |
| KIM | Kommunikation im Medizinwesen |
| KIS | Krankenhausinformationssystem |
| KSR | Konfigurations- und Software Repository |
| LAN | Local Area Network |
| LDAP | Leightweight Directory Access Protocol |
| LE | Leistungserbringer |
| MAC | Message Authentication Code |
| MB | Mega Byte (1024x1024 Bytes) |
| MGF | Mask Generation Function |
| MMU | Memory Management Unit |
| MTU | Maximum Transmission Unit |
| NATT | Network Address Translation Traversal |
| NFDM | Notfalldaten-Management |
| NK | Netzkonnektor |
| NTP | Network Time Protocol |
| OTP | One-Time-Passwort |
| PAP | Password Authentication Protocol |

| Abkürzung | Langform |
|------------------|---|
| PAT | Port Adress Translation |
| PKI | Public Key Infrastructure |
| PP | Protection Profile |
| PPP | Point-to-Point Protocol |
| PPPoE | PPP over Ethernet |
| PS | Primärsystem |
| PVS | Praxisverwaltungssystem |
| QES | Qualifizierte elektronische Signatur |
| RFC | Request for Comments |
| RMI | Remote Method Invocation |
| SAK | Signaturanwendungskomponente |
| SCaVA | Signature Creation Application and Signature Validation Application |
| SER | Seriennummer der KoCoBox MED+ |
| SGB V | Sozialgesetzbuch Fünftes Buch |
| SGD | Schlüsselgenerierungsdienst |
| SICCT | Secure Interoperable Chip Card Terminal |
| SMC-B | Security Module Card Typ B |
| SM-K | Security Module Konnektor |
| SIM | Subscriber Identity Module |
| SIS | Secure Internet Service, Sicherer Internet Service |
| SMMU | Source-Measurement-Multiplex-Unit |
| SMTP | Simple Mail Transfer Protocol |
| SN | Serial Number, Seriennummer |
| SNK | Sicheres Netz der KVen |
| SOAP | Simple Object Access Protocol |
| SSL | Secure Socket Layer |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TI | Telematikinfrastuktur |
| TLS | Transport Layer Security |
| TOE | Target of Evaluation |
| TSL | Trust-service Status List |
| TSP | Trust Service Provider |
| UDP | User Datagram Protocol |

| Abkürzung | Langform |
|------------------|--|
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| VAU | Vertrauenswürdige Ausführungsumgebung |
| VZD | Verzeichnisdienst |
| VDG | Vertrauensdienstegesetz |
| VO | Verordnung |
| VPN | Virtual Private Network |
| VPN-K | VPN-Konzentrator |
| VSD | Versichertenstammdaten |
| VSDM | Versichertenstammdatenmanagement |
| WA | Weitere Anwendungen |
| WAN | Wide Area Network |
| XAdES | XML Advanced Electronic Signature: ETSI Standard zur Signatur von XML-Dokumenten |
| XML | Extensible Markup Language |
| ZGDP | Zugangsdienstprovider |
| ZIS | Zugangs- und Integrationsschicht |

9.10 Abbildungsverzeichnis

| | |
|--|----|
| Abbildung 1: Geräteverpackung mit Siegeln und Verpackungsaufklebern (G3) | 19 |
| Abbildung 2: Geräteverpackung mit Siegeln und Verpackungsaufklebern (G4) | 19 |
| Abbildung 3: Verpackungssiegel der KoCoBox MED+ | 19 |
| Abbildung 4: Verpackungsaufkleber mit Seriennummer (G3) | 20 |
| Abbildung 5: Verpackungsaufkleber mit Seriennummer (G4) | 20 |
| Abbildung 6: Verpackungsaufkleber mit Barcodes (G3) | 20 |
| Abbildung 7: Verpackungsaufkleber mit Barcodes (G4) | 20 |
| Abbildung 8: Optik des Sicherheitssiegels im Originalzustand (G3) | 21 |
| Abbildung 9: Ansicht nach Manipulation (G3) | 21 |
| Abbildung 10: Optik des Sicherheitssiegels im Originalzustand (G4) | 21 |
| Abbildung 11: Ansicht nach Manipulation (G4) | 21 |
| Abbildung 12: KoCoBox MED+ (G3) - Seitenansicht rechts mit Sicherheitssiegel | 22 |
| Abbildung 13: KoCoBox MED+ (G3) - Seitenansicht links mit Sicherheitssiegel | 22 |
| Abbildung 14: KoCoBox MED+ (G4) Ansicht rechts mit Sicherheitssiegel | 23 |
| Abbildung 15: KoCoBox MED+ (G4) Ansicht links mit Sicherheitssiegel | 23 |
| Abbildung 16: Front der KoCoBox MED+ (G3) mit Display und Steuer-Buttons | 24 |
| Abbildung 17: Front der KoCoBox MED+ (G4) mit Display und Steuer-Buttons | 24 |
| Abbildung 18: Rückseite der KoCoBox MED+ (G3) mit Anschlüssen | 25 |
| Abbildung 19: Rückseite der KoCoBox MED+ (G4) mit Anschlüssen | 25 |
| Abbildung 20: Bodenansicht der KoCoBox MED+ (G3) | 26 |
| Abbildung 21: Bodenansicht der KoCoBox MED+ (G4) | 26 |
| Abbildung 22: Typenschild am Boden der KoCoBox MED+ (G3) | 27 |
| Abbildung 23: Typenschild am Boden der KoCoBox MED+ (G4) | 27 |
| Abbildung 24: Serielle („in Reihe“) Anbindung der KoCoBox MED+ | 30 |
| Abbildung 25: Parallele Anbindung der KoCoBox MED+ | 31 |
| Abbildung 26: Display der KoCoBox MED+ (G3) | 32 |
| Abbildung 27: Display der KoCoBox MED+ (G4) | 32 |
| Abbildung 28: Front der KoCoBox MED+ (G3) mit Display und Steuer-Buttons - Ausschnitt | 36 |
| Abbildung 29: Front der KoCoBox MED+ (G4) mit Display und Steuer-Buttons - Ausschnitt | 36 |
| Abbildung 30: Beispiel für TLS-Zertifikatsanzeige im Browser mit Seriennummer | 40 |
| Abbildung 31: Downloadpunkte für vertrauenswürdige PKI-Elemente der PU | 41 |
| Abbildung 32: Gültige Zertifikatskette | 42 |
| Abbildung 33: Login-Fenster der KoCoBox MED+ Managementschnittstelle | 44 |
| Abbildung 34: Persönliches Passwort vergeben | 45 |
| Abbildung 35: Fehlermeldung bei falscher Passwordeingabe | 47 |
| Abbildung 36: Aufbau der Managementschnittstelle am Beispiel der Status-Seite | 49 |
| Abbildung 37: Titelleiste der KoCoBox MED+ Managementschnittstelle | 50 |
| Abbildung 38: Anzeige des Session-Timeout | 50 |
| Abbildung 39: Session-Timeout zurücksetzen | 50 |
| Abbildung 40: Invertierte Sekundenanzeige vor dem Ablauf der Session | 51 |
| Abbildung 41: Übersicht zu den Statusinformationen | 55 |
| Abbildung 42: Ausschnitt des Vertrauensraumstatus (TSL) im ECC-RSA-Vertrauensraum | 55 |
| Abbildung 43: Display der KoCoBox MED+ nach der Initialkonfiguration (G3) | 59 |
| Abbildung 44: Display der KoCoBox MED+ nach der Initialkonfiguration (G4) | 59 |
| Abbildung 45: Beispielhafte Netzwerkkonfigurationen | 61 |
| Abbildung 46: Konfigurationsbereich für die Firewall zum Secure Internet Service (SIS) | 65 |
| Abbildung 47: Konfiguration der Firewall-Regeln | 65 |

| | |
|---|-----|
| Abbildung 48: Konfiguration der DHCP-Einstellungen | 66 |
| Abbildung 49: Konfigurationsmaske zur Bearbeitung der Client-Gruppen | 68 |
| Abbildung 50: Eintrag von DHCP-Optionen für eine Client-Gruppe..... | 70 |
| Abbildung 51: Konfigurationsbereich für das Virtual Private Network (VPN)..... | 71 |
| Abbildung 52: Konfigurationsbereich für das VPN mit Verbindung in die TI und zum SIS | 73 |
| Abbildung 53: Zugangsdienst-Registrierung | 74 |
| Abbildung 54: Anzeige nach erfolgreicher Registrierung am Zugangsdienst | 74 |
| Abbildung 55: Konfigurationsbereich für den Zeitdienst | 75 |
| Abbildung 56: Anzeige des Zeitdienstes bei Verbindung zur TI..... | 77 |
| Abbildung 57: Konfigurationsbereich für den Domain Name Server (DNS)..... | 78 |
| Abbildung 58: Eintragen der IP-Adresse..... | 79 |
| Abbildung 59: Fehlermeldung beim Registrierungsdienst - Aktivierung Leistungsumfang ONLINE notwendig | 80 |
| Abbildung 60: Fehlermeldung beim Registrierungsdienst wegen Zeitabweichung..... | 81 |
| Abbildung 61: Konfigurationsbereich zur Verwaltung der Leistungsumfänge | 85 |
| Abbildung 62: Konfigurationsbereich für die Anbindung der Clientsysteme | 88 |
| Abbildung 63: Warnhinweis beim Ausschalten der TLS-Option | 89 |
| Abbildung 64: Warnhinweis beim Ausschalten der verpflichtenden Authentisierung..... | 90 |
| Abbildung 65: Konfiguration der Zugangsdaten für das Clientsystem | 91 |
| Abbildung 66: Zufallspasswort zur Anbindung des Clientsystems | 91 |
| Abbildung 67: Passworteintrag für Clientsystem mit aktiverter Ansicht des Passworts..... | 92 |
| Abbildung 68: Übersicht zu angebotenen Clientsystemen | 92 |
| Abbildung 69: Konfiguration zum Anlegen eines Clientsystem-Zertifikats mit ECC | 93 |
| Abbildung 70: Anlegen eines Konnektor-Authentisierungszertifikats ECC-NIST | 94 |
| Abbildung 71: Konfigurationsdaten exportieren und importieren | 96 |
| Abbildung 72: Auswahl der SM-B für Export der Konfigurationsdaten..... | 97 |
| Abbildung 73: Anzeige für den Exportprozess..... | 97 |
| Abbildung 74: Anzeige für den Fortschritt im Exportprozess | 97 |
| Abbildung 75: Importpasswort für späteren Import der Konfigurationsdaten..... | 98 |
| Abbildung 76: Speichern der Konfigurationsdaten-Datei | 98 |
| Abbildung 77: Importieren der Konfigurationsdaten-Datei | 99 |
| Abbildung 78: Anzeigefenster zur Kontrolle der Signaturinformationen | 100 |
| Abbildung 79: Auswahl für den Kartenterminal-Import | 101 |
| Abbildung 80: Dialogfenster mit Hinweis auf Neustart nach Konfigurationsübernahme | 101 |
| Abbildung 81: Übersicht verfügbarer Telematikdienste | 102 |
| Abbildung 82: Konfigurationsbereich für den Kartendienst | 103 |
| Abbildung 83: Konfigurationsbereich für den Kartenterminaldienst | 105 |
| Abbildung 84: Erfolgsmeldung zum Auffinden von Kartenterminals | 107 |
| Abbildung 85: Kartenterminal hinzufügen | 107 |
| Abbildung 86: Vorhandenes Kartenterminal bearbeiten..... | 109 |
| Abbildung 87: Übersicht der Verbindungsstatus eines Kartenterminals zum Konnektor..... | 111 |
| Abbildung 88: Konfigurationsfenster zur Statusänderung eines Kartenterminals..... | 112 |
| Abbildung 89: Konfigurationsbereich für den Systeminformationsdienst | 114 |
| Abbildung 90: Konfigurationsbereich für den Zertifikatsdienst | 116 |
| Abbildung 91: Manuelle ECC-Migration..... | 116 |
| Abbildung 92: Meldung nach erfolgreichem Test einer OCSP-Anfrage | 117 |
| Abbildung 93: Meldung nach erfolglosem Test einer OCSP-Anfrage..... | 117 |
| Abbildung 94: Importieren von CA-Zertifikaten | 119 |
| Abbildung 95: Übersicht zum Status der verwendeten Zertifikate | 120 |

| | |
|---|-----|
| Abbildung 96: Laufzeitverlängerung | 121 |
| Abbildung 97: Konfigurationsbereich für den Protokollierungsdienst..... | 123 |
| Abbildung 98: Übersicht zum Systemprotokoll..... | 124 |
| Abbildung 99: Konfigurationsbereich des Signaturdienstes bei deaktiviertem Komfortsignaturmodus . | 126 |
| Abbildung 100: Konfigurationsbereich für den Signaturdienst mit aktiviertem Komfortsignaturmodus. | 130 |
| Abbildung 101: Benutzerverwaltung der KoCoBox MED+ | 133 |
| Abbildung 102: Anlegen eines neuen Administrators in der Benutzerverwaltung..... | 134 |
| Abbildung 103: Anzeige des Einmalpassworts..... | 134 |
| Abbildung 104: Löschen eines Administrator-Benutzers | 135 |
| Abbildung 105: Passwort eines bestehenden Administrators ändern..... | 136 |
| Abbildung 106: Beispiel-Informationsmodell für die erlaubten Zugriffsmöglichkeiten..... | 137 |
| Abbildung 107: Infomodell-Konfigurationsbereiche für Mandanten, Clientsysteme und Arbeitsplätze... | 139 |
| Abbildung 108: Infomodell-Konfigurationsbereiche für SMBen, Kartenterminals und CS-AP Objekte | 140 |
| Abbildung 109: Infomodell-Konfigurationsbereich für Remote-PIN-KT Objekte | 141 |
| Abbildung 110: Durchführung von Softwareaktualisierungen..... | 142 |
| Abbildung 111: Konfiguration des automatischen Updates | 144 |
| Abbildung 112: Detailanzeige zum Firmware-Update für den Konnektor | 145 |
| Abbildung 113: Dialogfenster zur Bestätigung des KSR-Downloads | 146 |
| Abbildung 114: Dialogfenster mit Hinweis zum erneuten KSR-Download | 146 |
| Abbildung 115: Dialogfenster mit Information zum Ende des Update-Imports..... | 147 |
| Abbildung 116: Bitte-Warten-Balken..... | 147 |
| Abbildung 117: Detailanzeige zum Software-Update für das Kartenterminal | 149 |
| Abbildung 118: Planung von Softwareaktualisierungen | 151 |
| Abbildung 119: Planung für Software-Aktualisierungen bestätigen | 152 |
| Abbildung 120: Beispielhafte Statusanzeigen zum Konnektor-Update im Zeitverlauf..... | 153 |
| Abbildung 121: Fehleranzeige für Konnektor-Update | 153 |
| Abbildung 122: Meldung zum Abschluss der Update-Verarbeitung..... | 153 |
| Abbildung 123: Mein Profil für Administrator-Benutzer mit Passwort ändern-Button | 154 |
| Abbildung 124: Konfigurationsbereich für das Fachmodul VSDM | 161 |
| Abbildung 125: Konfigurationsfenster für das Anlegen eines Mandanten-Schlüssel-Paares | 163 |
| Abbildung 126: Exemplarische Ansicht zum Systemprotokoll VSDM mit Downloadfunktion..... | 164 |
| Abbildung 127: Konfigurationsbereich für das Fachmodul AMTS | 166 |
| Abbildung 128: Exemplarische Ansicht zum Ablaufprotokoll AMTS mit Downloadfunktion | 167 |
| Abbildung 129: Konfigurationsbereich für das Fachmodul ePA | 169 |
| Abbildung 130: Exemplarische Ansicht zum Ablaufprotokoll ePA mit Downloadfunktion | 171 |
| Abbildung 131: Übersichtliste verfügbarer Telematikdienste für die ePA (Ausschnitt) | 174 |
| Abbildung 132: Konfigurationsbereich für das Fachmodul NFDM | 175 |
| Abbildung 133: Exemplarische Ansicht zum Ablaufprotokoll NFDM mit Downloadfunktion | 176 |
| Abbildung 134: Szenario für die einfache Installation der KoCoBox MED+ | 189 |
| Abbildung 135: WAN Adapter Modus eingeschaltet | 189 |
| Abbildung 136: Leistungsumfang ONLINE nicht aktiviert..... | 190 |
| Abbildung 137: Einsatz der KoCoBox MED+ Standalone mit physischer Trennung der Konnektoren | 191 |
| Abbildung 138: Einstellungen bei physischer Trennung im Konnektor | 192 |

9.11 Referenzen

| ID | Bezeichnung |
|-------------------|--|
| [CADES] | European Telecommunications Standards Institute. Electronic Signatures and Infrastructures (ESI). CMS Advanced Electronic Signatures (CADES). ETSI Technical Specification. Version 2.2.1. ETSI, Apr. 2013, https://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf |
| [CADES-BL] | European Telecommunications Standards Institute. Electronic Signatures and Infrastructures (ESI). CADES Baseline Profile. ETSI Technical Specification. Version 2.1.1. ETSI, März 2012, https://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.01.01_60/ts_103173v020101p.pdf |
| [eIDAS-VO] | Amtsblatt der Europäischen Union, Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, CELEX_32014R0910_DE_TXT.pdf, 28.08.2014 |
| [gemGlossar] | gematik, Einführung der Gesundheitskarte, Glossar der Telematikinfrastruktur, gemGlossar_V5.2.0.pdf, 20.01.2022, https://fachportal.gematik.de/glossar |
| [gemILF_PS] | gematik, Implementierungsleitfaden Primärsysteme – Telematikinfrastruktur (TI) (einschließlich VSDM, QES-Basisdienste, KOM-LE), gemILF_PS_V2.20.0.pdf, 25.07.2023, https://fachportal.gematik.de/fileadmin/Fachportal/Downloadcenter/Implementierungsleitfaeden/gemILF_PS_V2.20.0.zip |
| [gemILF_PS_AMTS] | gematik, Implementierungsleitfaden Primärsysteme – elektronischer Medikationsplan/AMTS-Datenmanagement (Stufe A), gemILF_PS_AMTS_1.7.0.pdf, 12.11.2020, https://fachportal.gematik.de/fileadmin/Fachportal/Downloadcenter/Implementierungsleitfaeden/gemILF_PS_AMTS_V1.7.0.pdf |
| [gemILF_PS_ePA] | Implementierungsleitfaden Primärsysteme - Elektronische Patientenakte (ePA) (ePA-Stufe 2.5), gemILF_PS_ePA_V2.52.0.pdf, 31.03.2023, https://fachportal.gematik.de/fileadmin/Fachportal/Downloadcenter/Implementierungsleitfaeden/gemILF_PS_ePA_V_2.52.0.zip |
| [gemILF_PS_NFDM] | gematik, Implementierungsleitfaden Primärsysteme – Notfalldaten-Management (NFDM), gemILF_PS_NFDM_1.5.0.pdf, 26.08.2022, https://fachportal.gematik.de/fileadmin/Fachportal/Downloadcenter/Implementierungsleitfaeden/gemILF_PS_NFDM_V1.5.0.zip |
| [gemRL_QES_NFDM] | gematik, Signaturrechtlinie QES Notfalldaten-Management (NFDM), gemRL_QES_NFDM_V1.4.1.pdf, 02.03.2020 |
| [gemSpec_FM_AMTS] | gematik, Elektronische Gesundheitskarte und Telematikinfrastruktur, Spezifikation Fachmodul AMTS, gemSpec_FM_AMTS_V1.4.0.pdf, 15.05.2019 |

| | |
|---------------------------|---|
| [gemSpec_FM_ePA] | gematik, Elektronische Gesundheitskarte und Telematikinfrastruktur, Spezifikation Fachmodul ePA, gemSpec_FM_ePA_V1.52.0.pdf, 01.21.2022 |
| [gemSpec_FM_NFDM] | gematik, Elektronische Gesundheitskarte und Telematikinfrastruktur, Spezifikation Fachmodul NFDM, gemSpec_FM_NFDM_V1.6.2.pdf, 30.06.2021 |
| [gemSpec_FM_VSDM] | gematik, Einführung der Gesundheitskarte, Spezifikation Fachmodul VSDM, gemSpec_FM_VSDM_V2.7.0.pdf, 02.12.2022 |
| [gemSpec_Karten_Fach_TIP] | gematik, Einführung der Gesundheitskarte, Befüllvorschriften für die Plattformanteile der Karten der TI, gemSpec_Karten_Fach_TIP_G2.1_3.0.0.pdf, 18.12.2017 |
| [gemSpec_KT] | gematik, Elektronische Gesundheitskarte und Telematikinfrastruktur, Spezifikation eHealth-Kartenterminal, gemSpec_KT_V3.14.pdf, 31.01.2022 |
| [gemSpec_Kon] | gematik, Elektronische Gesundheitskarte und Telematikinfrastruktur, Spezifikation Konnektor, gemSpec_Kon_V5.18.0.pdf, 28.11.2022 |
| [gemSpec_PKI] | gematik, Elektronische Gesundheitskarte und Telematikinfrastruktur, Übergreifende Spezifikation Spezifikation PKI, gemSpec_PKI_V2.14.1.pdf, 16.12.2022 |
| [PADES] | European Telecommunications Standards Institute. Electronic Signatures and Infrastructures (ESI). PDF Advanced Electronic Signature Profiles. Part 3: PAdES Enhanced – PAdES-BES and PAdES-EPES Profiles. ETSI Technical Specification. Version 1.2.1. ETSI, Juli 2010, https://www.etsi.org/deliver/etsi_ts/102700_102799/10277803/01.02.01_60/ts_10277803v010201p.pdf |
| [PADES-BL] | European Telecommunications Standards Institute. Electronic Signatures and Infrastructures (ESI). PAdES Baseline Profile. ETSI Technical Specification. Version 2.2.2. ETSI, Apr. 2013, https://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf |
| [PP-0097] | Bundesamt für die Sicherheit in der Informationstechnik: Common Criteria Schutzprofil (Protection Profile) Schutzprofil 1: Anforderungen an den Netzkonnektor BSI-CC-PP-0097, Bonn, https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0097_0097V2.html |
| [PP-0098] | Bundesamt für die Sicherheit in der Informationstechnik: Common Criteria Schutzprofil (Protection Profile) Schutzprofil 2: Anforderungen an den Konnektor BSI-CC-PP-0098, Bonn, https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0098_0098V2_0098V3.html |
| [RFC3927] | Network Working Group, Dynamic Configuration of IPv4 Link-Local Addresses, May 2005, https://tools.ietf.org/html/rfc3927 |

| | |
|--------------|---|
| [RFC5652] | Network Working Group, Cryptographic Message Syntax (CMS), September 2009, https://tools.ietf.org/html/rfc5652 |
| [RFC8017] | Internet Engineering Task Force (IETF), PKCS #1: RSA Cryptography Specifications Version 2.2, November 2016, https://tools.ietf.org/html/rfc8017 |
| [TR-03116-1] | Bundesamt für die Sicherheit in der Informationstechnik: Kryptographische Vorgaben für Projekte der Bundesregierung. Teil 1: Telematikinfrastruktur, Bonn, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116.pdf |
| [TR-03154] | Bundesamt für die Sicherheit in der Informationstechnik: Konnektor – Prüfspezifikation für das Fachmodul NFDM, Bonn, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03154/TR-03154.pdf |
| [TR-03155] | Bundesamt für die Sicherheit in der Informationstechnik: Konnektor – Prüfspezifikation für das Fachmodul AMTS, Bonn, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03155/TR-03155.pdf |
| [TR-03157] | Bundesamt für die Sicherheit in der Informationstechnik: Konnektor – Prüfspezifikation für das Fachmodul ePA, Bonn, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03157/TR-03157.pdf |
| [W3C] | Frederick Hirsch u.a. XML Encryption Syntax and Processing Version 1.1. W3C Recommendation. http://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/ . W3C, Apr. 2013. |
| [XAdES] | European Telecommunications Standards Institute. Electronic Signatures and Infrastructures (ESI). XML Advanced Electronic Signatures (XAdES). ETSI Technical Specification. Version 1.4.2. ETSI, Dez. 2010, https://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.02_60/ts_101903v010402p.pdf |
| [XAdES-BL] | European Telecommunications Standards Institute. Electronic Signatures and Infrastructures (ESI). XAdES Baseline Profile. ETSI Technical Specification. Version 2.1.1. ETSI, März 2012, https://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf |