Administratorhandbuch

KoCoBox HSK

Version 1

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

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

Die Software-Versionsnummer rufen Sie über die Managementschnittstelle auf der Status-Seite ab.

Dokumentenversion:	1
Dokumentensprache:	deutsch (de)
zuletzt geändert:	17. September 2025

Inhaltsverzeichnis

Allgemeine Informationen

Dieses Administratorhandbuch beschreibt die KoCoBox HSK der KoCo Connector GmbH inklusive ihrer Fachmodule und Dienste.

Die Ausführungen zur KoCoBox[1] 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] Die KoCoBox setzt sich aus dem Anwendungskonnektor (AK) und den Fachmodulen (FM) zusammen. Ausführliche Informationen dazu: [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)
- 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.

1 Einleitung

Ein 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)[2] des Gesundheitswesens zu gewährleisten.

Die KoCoBox HSK der KoCo Connector GmbH stellt eine virtualisierte Instanz eines Konnektors auf einem rechenzentrumsbasierten Highspeed-Konnektor (HSK) dar. Sie kann damit die Funktionen des Konnektors für große Institutionen (wie beispielsweise Krankenhäuser, Pflegeheime, Arztpraxen, Apotheken u.a.) als hochverfügbare und skalierbare Komponente übernehmen. Der zugehörige HSK bindet als Teil eines TI-Gateways[3] die Institutionen mittels einer sicheren, verschlüsselten Verbindung an die Telematikinfrastruktur an und ersetzt hierdurch eine Vielzahl von Einbox-Konnektoren.

Dieses Administratorhandbuch beschreibt die initiale sowie weiterführende Konfiguration zur sicheren Einbindung des Konnektors in die TI.

Die KoCoBox muss sehr hohen Sicherheitsstandards Rechnung tragen, insofern sind die Sicherheitsvorgaben mit besonderer Sorgfalt einzuhalten.

Zielgruppe

Zielgruppe dieses Handbuchs sind die Administratoren des Konnektors der KoCo Connector GmbH. Administratoren sind autorisierte, vertrauenswürdige und fachlich kompetente Personen, die die KoCoBox HSK über die passwortgeschützte Managementschnittstelle konfigurieren und verwalten.

Eine nicht-autorisierte, nicht fachlich geschulte bzw. nicht vertrauenswürdige Person darf den Konnektor aus Sicherheitsgründen nicht administrieren!

Weiterhin finden sich im Abschnitt 8.5 Implementierungs- und Konfigurationsanforderungen für Clientsystemhersteller als Ergänzung zum Implementierungsleitfaden aus der Spezifikation der gematik.

Weitere Dokumente

Mit diesem Handbuch sind für eine Einrichtung der vollständigen Betriebsumgebung des Konnektors weitere ergänzende Dokumente wichtig:

- Für die Konfiguration und Verwendung des Clientsystems/der Clientsysteme[4] durch den Arzt/Apotheker/Pflegefachkraft o.ä. gilt die Dokumentation des Clientsystemherstellers.
- Für die Konfiguration und Verwendung der Kartenterminals gilt die Dokumentation des Kartenterminal-Herstellers.
- Für die Verwendung der 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

[2] Synonym auch: Produkte der TI

[3] Eine technische Lösung, mittels derer Konnektoren in einem Rechenzentrum für eine Vielzahl von Praxen und/oder weitere Nutzergruppen einen TI-Anschluss bereitstellen

[4] Die Primärsysteme werden im Kontext der Verwendung der KoCoBox auch als Clientsystem bezeichnet.

Verschlüsselungsrichtlinien gelten die umgesetzten Anforderungen aus den gematik-Implementierungsrichtlinien[5]. Entsprechende Hinweise sind der Benutzerdokumentation des Clientsystems/der Clientsysteme zu entnehmen.

Für die Entwicklung von Primärsystemen (Praxisverwaltungssysteme, Arztinformationssysteme etc.) gilt in erster Linie die Spezifikation der gematik, verbunden mit dem Implementierungsleitfaden, wie unter

https://fachportal.gematik.de/hersteller-anbieter/primaersysteme/

zur Verfügung gestellt.

Integrationstests können gegen den durch die gematik bereitgestellten Konnektorsimulator für Primärsysteme KoPS erfolgen, siehe hierzu

https://fachportal.gematik.de/toolkit/kops/

Support

Für den Konnektor gibt es drei Support-Instanzen[6]

- First-Level-Support: Support-Hotline des Servicepartners[7]
- Second-Level-Support: Support-Instanz des Resellers bzw. des Clientsystem-Herstellers
- Third-Level-Support: Support des Herstellers, der KoCo Connector GmbH

[5] betrifft [gemILF_PS], [gemILF_PS_NFDM, gemILF_PS_AMTS]

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

[7] Synonym auch: Systempartner

2 Allgemeine Sicherheitshinweise

- Lesen Sie vor Inbetriebnahme des Konnektors dieses Administratorhandbuch sorgfältig durch und bewahren Sie es gut auf.
- Nutzen Sie TLS-Cipher-Suites mit AES-GCM bei der Datennetz-Verbindung mit der KoCoBox. 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.[8]
- Achten Sie darauf, dass Sie generell vor Beginn der administrativen Tätigkeiten am Konnektor 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 Bestandsnetze[9] oder Fachdienste zugreifen, ebenfalls keine ECN Bits benutzen.
- Verwenden Sie den Konnektor nur für den vorgesehenen Zweck.
- 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 an einen anderen Betriebsstättenverantwortlichen einen Werksreset in der Instanz aus. Sollte dieser fehlschlagen, ist der Supportpartner zu benachrichtigen, so dass die Konnektorinstanz gelöscht und als neue Instanz bereitgestellt wird.
- Prüfen Sie die Unversehrtheit von Kartenterminals, bevor Sie sie im Netzwerk mit dem Konnektor 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 des Konnektors 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.

---

[8] 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.

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

3 Sicherheitsziele für den Einsatz der KoCoBox HSK

Das folgende Kapitel beschreibt ausführlich die Rahmenbedingungen, unter denen der Konnektor eingesetzt werden darf und dabei die vorgegebenen Sicherheitsziele erfüllt.

Es gliedert sich in die Beschreibung

- 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 wird entsprechend der Sicherheitsvorgaben nur in einem Rechenzentrum betrieben, das von einem von der gematik zugelassenen Dienstleister unterhalten wird.

Sicherheitshinweise

Zusammenfassend sind zur sicheren Inbetriebnahme und für den sicheren Betrieb des Konnektors folgende Sicherheitsanforderungen zu erfüllen:

- 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 im Umfeld des Endkunden ist durch organisatorische und technische Maßnahmen zu schützen.
- Sofern sich ein Unbefugter widerrechtlichen Zugang / Zugriff verschafft, wird dies unverzüglich erkannt.
- Es ist ein eindeutig identifizierbarer Verantwortlicher benannt, der das fehlerfreie Funktionieren aller Sicherheitsmaßnahmen zuverlässig überwacht.

3.2 Sichere Clientsystemanbindung

Bei der Einbindung des Konnektors in das lokale Netz muss sichergestellt sein, dass die KoCoBox 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.[10]

- 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.[11]
- Stellen Sie sicher, dass es in sicherer Art und Weise administriert wird (z.B. mittels geschützten Passworts bzw. 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 sicher, dass das Clientsystem / die Clientsysteme nur auf sichere Art und Weise mit dem Internet verbunden sind.
- 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.[12] 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* oder *genehmigt* aus. In der Ergebnisliste muss der Konnektor der KoCo Connector GmbH 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 Angriffe aus dem Internet grundsätzlich **nicht** ausgeschlossen werden können. Sorgen Sie daher im Praxisnetz für eine **stets aktuell gehaltene Absicherung** der genutzten Clientsysteme, z.B. mittels **Systemupdates und Virenscannern**, sowie die Verwendung **sicherer Grundeinstellungen und Zugangsdaten** der entsprechenden Arbeitsstationen.

Für die Einbindung des Konnektors in die LAN-Netzwerkinfrastruktur gilt in erster Linie die Spezifikation der gematik, hierbei insbesondere auch [gemSpec_Net] und [gemSpec_Krypt], wie unter

https://fachportal.gematik.de/ bzw. https://gemspec.gematik.de/

zur Verfügung gestellt.

---

[10] 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.

[11] 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-primaersysteme/liste-der-bestaetigten-primaersysteme/

[12] 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.[13]

- 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) 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.

[13] Siehe [PP-0097], S. 58

4 Technische Daten

Bei der KoCoBox HSK handelt es sich um eine virtualisierte Software-Instanz, die in einem Rechenzentrum betrieben wird. Für den Betrieb notwendige Parameter werden durch den Betreiber konfiguriert. Weitere relevante technischen Daten der ausführenden Hardware stehen nicht zur Verfügung.

5 Sicherer Anschluss des Konnektors

Bei der KoCoBox HSK handelt es sich um einen Softwaredienst, der aus einem Rechenzentrum ausschließlich über gesicherte Zugangsleitungen angeboten wird. Hieraus ergehen keinerlei zusätzliche Anforderungen an den sicheren Anschluss des Konnektors für den Nutzer des Konnektors.

Dennoch sind die nachfolgenden Hinweise zu beachten.

Das lokale Netz (LAN) in der Praxis ist mit geeigneten Maßnahmen außerhalb der KoCoBox HSK vor Angriffen aus dem Internet zu schützen (Firewall, aktuelle Antivirensoftware etc.). Der für das Praxisnetzwerk zuständige Administrator ist für dessen Schutz verantwortlich.

Beachten Sie weiterhin die Hinweise betreffs Clientsystemanbindung im Abschnitt 3.2 .

6 Inbetriebnahme des Konnektors

Die Inbetriebnahme des Konnektors umfasst vorbereitende Schritte für den administrativen Zugang zur Managementschnittstelle, gefolgt von der Konfiguration des Anwendungskonnektors in Abschnitt 6.5 und der Fachmodule in Abschnitt 6.7 . Für funktionsübergreifende Konfigurationsaufgaben steht weiterhin ein Konnektormanagement zur Verfügung, wie in Abschnitt 6.6 beschrieben.

Die KoCoBox 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 werden[14]. Die Definition von Mandanten ist Teil der Konfiguration des Infomodells, wie in Abschnitt 6.6.2 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 die KoCoBox sicher in Betrieb nehmen zu können, ist ihre initiale Konfiguration erforderlich. Diese erfolgt über eine browserbasierte Managementschnittstelle.

Dafür loggen Sie sich über einen sicheren Zugang als Super-Administrator[15] ein, vergeben ein persönliches Passwort, spielen eine aktuelle, gültige Trust-service Status List (TSL) des aktuellen Vertrauensraums der TI ein, führen bei Bedarf ein Softwareupdate für vorhandene Kartenterminals durch und geben systematisch die (Grund-) Einstellungen ein bzw. übernehmen die per Werkskonfiguration vorhandenen Voreinstellungen. Nach dem Pairing eines Kartenterminals[16] sowie dem Bearbeiten des Informationsmodells ist die initiale Konfiguration des Konnektors abgeschlossen.

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

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

Prüfen Sie im Vorfeld des Einsatzes der KoCoBox in einem TI-Gateway, ob dort außerdem für weitere Benutzer[17] Zugang zur KoCoBox konfiguriert ist. Nutzen Sie hierzu Ihre Anmeldung am Nutzerportal des TI-Gateways. Wenden Sie sich bei erkannten Problemen an Ihren Supportdienstleister zur Klärung.

---

[14] 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 des Konnektors angebracht.

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

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

[17] Initial darf keine Freischaltung für Remote-Zugänge zur KoCoBox aus DVO-Netzen konfiguriert sein.

Bereitstellung des Web-Browsers

Die browserbasierte Managementschnittstelle des Konnektors 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 qualitätsgesichert. Eine Übersicht der Betriebssysteme mit Browser-Downloadpunkten zeigt Tabelle 1.

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

Betriebssystem	Browser	Verfügbarkeit, Versionseinschränkungen
Windows	Mozilla Firefox	*installierbare Version:* https://www.mozilla.org/firefox/ aufrufen und dort die Option *„Für Desktop herunterladen“* auswählen. *portable Version:* https://portableapps.com/de/apps/internet/firefox_portable/
macOS, iOS	Mozilla Firefox	*installierbare Version:* https://www.mozilla.org/firefox/ aufrufen und dort die Option *„Desktop“* und darin *„Weitere Infos“* auswählen, auf der Folgeseite *„Download-Optionen und weitere Sprachen“* → *„Firefox“* mit der Auswahl für die Plattform *„macOS“* -> *„Sprache“*. Für iOS ist auf der Startseite *„Mobile“ und darin „Weitere Infos“* sowie auf der Folgeseite der Eintrag *„iOS“* auszuwählen. *Die Verwendung portabler Versionen empfehlen wir aktuell nicht, da diese überwiegend in älteren Versionsständen angeboten werden.*
Linux	Mozilla Firefox	*installierbare Version:* https://www.mozilla.org/firefox/ aufrufen und dort die Option *„Desktop“* und darin *„Weitere Infos“* auswählen, auf der Folgeseite *„Download-Optionen und weitere Sprachen“* → *„Firefox“* mit der Auswahl für die Plattform *„Linux 64-bit“/„Linux 32-bit“* -> *„Sprache“*. *Die portable Version ist abhängig von der jeweiligen Linux-Distribution – beispielhaft ist dies für Ubuntu bzw. dessen Derivate:* https://wiki.ubuntuusers.de/Portable_Firefox/

Tabelle 1: Übersicht der Browser-Downloadpunkte

6.1 Vorbereitungen

Der Administrator erhält vom Vertriebspartner die Zugangsdaten zu seiner KoCoBox HSK. Mit diesen Daten sind eine unmittelbare Anmeldung und Nutzung der Dienste möglich. Die initiale Konfiguration erfolgt über eine browserbasierte Managementschnittstelle. 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 das Gewährleisten der netzwerktechnischen Verbindungssicherheit verantwortlich.

Für die Inbetriebnahme betrifft dies besonders die Vertrauenswürdigkeit der Verbindung zum Konnektor. Hierzu muss die Authentizität der Verbindung zur Managementschnittstelle 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.

Der Administrator hat zu kontrollieren, ob die TLS-Verbindung zwischen seinem Netzwerkrechner und dem Konnektor korrekt aufgebaut wurde. Dies umfasst die Prüfung des vom Konnektor übermittelten Zertifikats.

Durch KoCo Connector wird die Anwendung **TLS-Validator** für Ihre PC-Zielplattform bereitgestellt. Für die erfolgreiche Ausführung der Prüfung benötigen Sie weiterhin Zugang zum Internet.

Starten Sie die Anwendung auf dem PC. Geben Sie die IP-Adresse Ihres Konnektors ein und drücken die Eingabetaste oder betätigen den Knopf **Prüfen**.

Die Anwendung lädt nun das Konnektorzertifikat von der angegebenen Adresse und prüft es automatisch gegen die im Internet verfügbaren Ausstellerzertifikate der gematik. Einzelne Schritte werden dabei in einer Liste angezeigt. War die Prüfung erfolgreich, dann wird dies durch einen grünen Punkt und die Ausschrift „Prüfung erfolgreich“ dargestellt.

Die Liste enthält bei erfolgreicher Prüfung zusätzlich den **SHA-256-Fingerabdruck** des Konnektorzertifikats.

Nur bei erfolgreicher Prüfung des TLS-Validators dürfen Sie die Credentials (Benutzername und Passwort) für die Anmeldung am Konnektor im Browser eingeben!

Erfolglose Prüfungen sind farblich und textuell durch einen gelben (Prüfung unvollständig) oder roten Punkt (Prüfung fehlgeschlagen) gekennzeichnet. In beiden Fällen wird das Konnektorzertifikat als **NICHT gültig** bewertet.

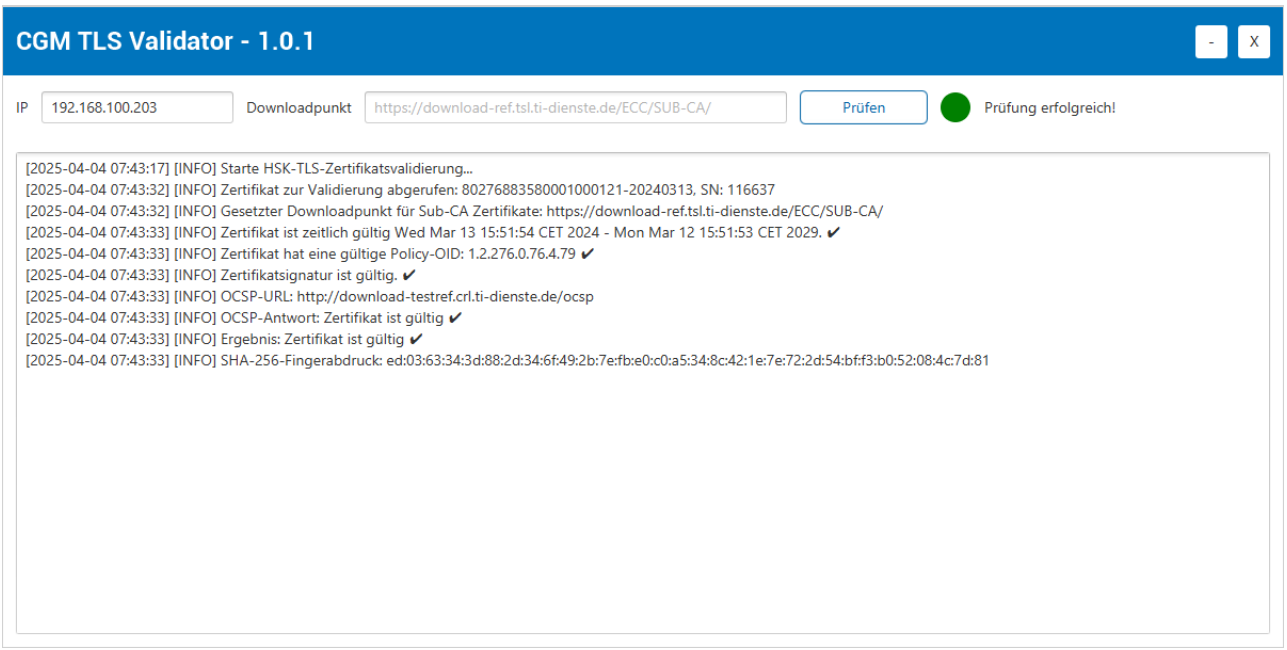


Abbildung 1: Beispiel für eine erfolgreiche Zertifikatsprüfung mittels TLS-Validator

Die Prüfung kann jederzeit wiederholt werden. Beachten Sie für spätere Zeitpunkte, dass diese nur dann erfolgreich sein wird, wenn im Konnektor das Standardzertifikat C.AK.AUT2 für die Authentisierung des Konnektors eingestellt ist, siehe Abschnitt Clientsysteme.

Prüfen Sie nach dem ersten Anmelden, ob in Ihrem Zugang weitere Konten mit Administratorberechtigungen existierten, siehe Abschnitt Benutzerverwaltung. Das darf nicht der Fall sein. Sollte dies dennoch vorliegen, wenden Sie sich unmittelbar an Ihren Supportdienstleister zur Klärung des Sachverhalts.

Prüfen Sie nach dem ersten Anmelden, dass kein Informationsmodell konfiguriert ist. Nutzen Sie hierfür die Beschreibung im Abschnitt Infomodell. Sollte ein vorkonfiguriertes Infomodell vorliegen, ist mit Unterstützung des Supportdienstleisters der Sachverhalt zu klären und die korrekte Anpassung auf Ihre Umgebung vorzunehmen.

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

Starten Sie den Netzwerk-Rechner, über dessen Browser Sie die Managementschnittstelle aufrufen und der per LAN + VPN mit dem Konnektor verbunden ist. Die Zieladresse des Konnektors ist Teil der bereitgestellten Zugangsdaten.

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

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 zuvor mittels TLS-Validator geprüften Vertrauenskette für dieses Konnektorzertifikat eine Ausnahme im Browser einrichten. Dies gilt gleichfalls für die Aufnahme in die sogenannte Allow-List angeschlossener Clientsysteme – auch hier kann das Konnektorzertifikat hinzugefügt werden. Wenden Sie sich ggf. an den Hersteller oder Lieferanten Ihres Clientsystems, um hierzu Unterstützung zu erfahren.

6.2 Administrator-Passwort

Die initialen Zugangsdaten zur Managementschnittstelle (Name und Passwort) sind voreingestellt:

- Name: koco-root
- Passwort: InItal4StartUp![18]

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.

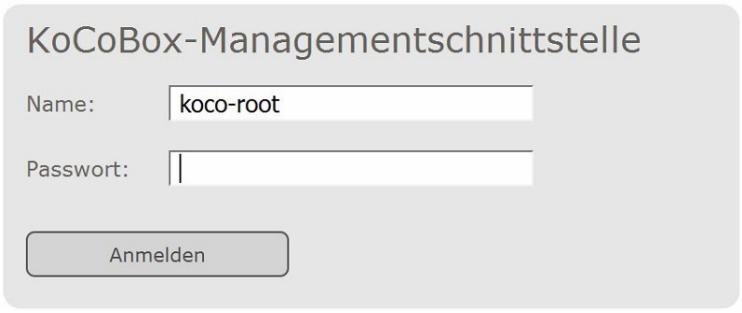


Abbildung 2: Login-Fenster der Managementschnittstelle

Beachten Sie für die weiteren Schritte die folgenden Sicherheitshinweise für die sichere Administration des Konnektors:

- Das Auslieferungspasswort (= Einmalpasswort[19]) **muss** beim ersten Login sofort geändert werden. Deswegen ist es **zwingend notwendig**, dass Sie **zuallererst ein persönliches Passwort vergeben**.
- Dieses persönliche Passwort darf **nur Ihnen allein** bekannt sein. Behandeln Sie es deshalb bitte **streng vertraulich**.
- Administratoren 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 des Konnektors darauf, ob Einstellungen 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.

[18] Dies ist das Auslieferungspasswort. Bitte beachten Sie: Hier sind der erste und dritte Buchstabe ein großes „i".

[19] Dies wird einmalig für die Erstanmeldung an der Managementschnittstelle vergeben. Auch nach einem Werksreset ist dieses Passwort für die Erstanmeldung zu verwenden.

Auf der Managementschnittstelle können zeitgleich mehrere Benutzer eingeloggt sein. Generell ist es jedoch ratsam, nur **einen** Administrator einzuloggen. Anderenfalls 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[20] kann es jedoch sein, dass Sie sich weiterhin innerhalb einer Sitzung bewegen.

Änderung des Auslieferungspassworts

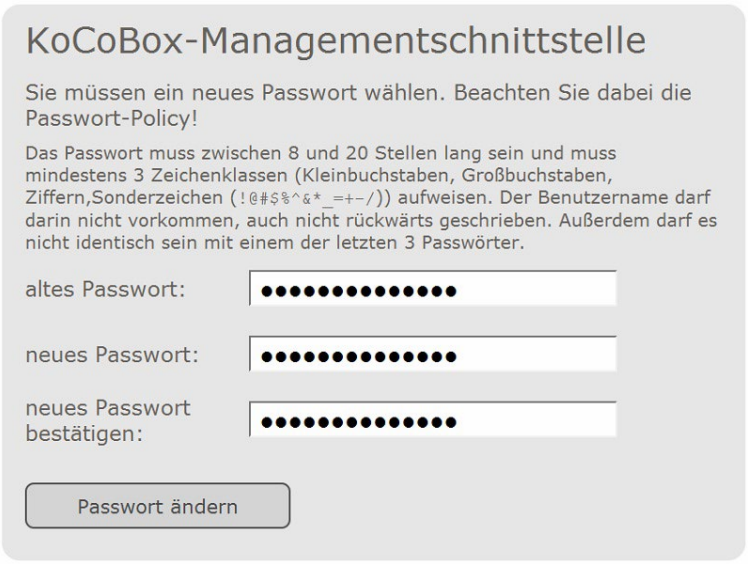


Abbildung 3: Persönliches Passwort vergeben

Nach der Eingabe der initialen Zugangsdaten gelangen Sie automatisch 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

[20] Dies ist bei nahezu allen marktüblichen Browsertypen gegeben.

- 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 365 Tagen einen Passwortwechsel beim nächsten Login.[21]

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 den Konnektor. 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 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 Fehlermeldung[22].

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: *InItal4StartUp!*) 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.

[21] Die Voreinstellung umfasst 120 Tage.

[22] 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 der Konnektor 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[23]

Abbildung 4: Fehlermeldung bei falscher Passworteingabe

[23] 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 Passwort[24] 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**. Anderenfalls werden Sie immer wieder zu diesem Passwortänderungsfenster zurückgeführt.

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

6.3 Aufbau und Semantik der Managementschnittstelle

Nach dem erfolgreichen Login mittels persönlichen Passworts erscheint die Status-Seite[25] 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.

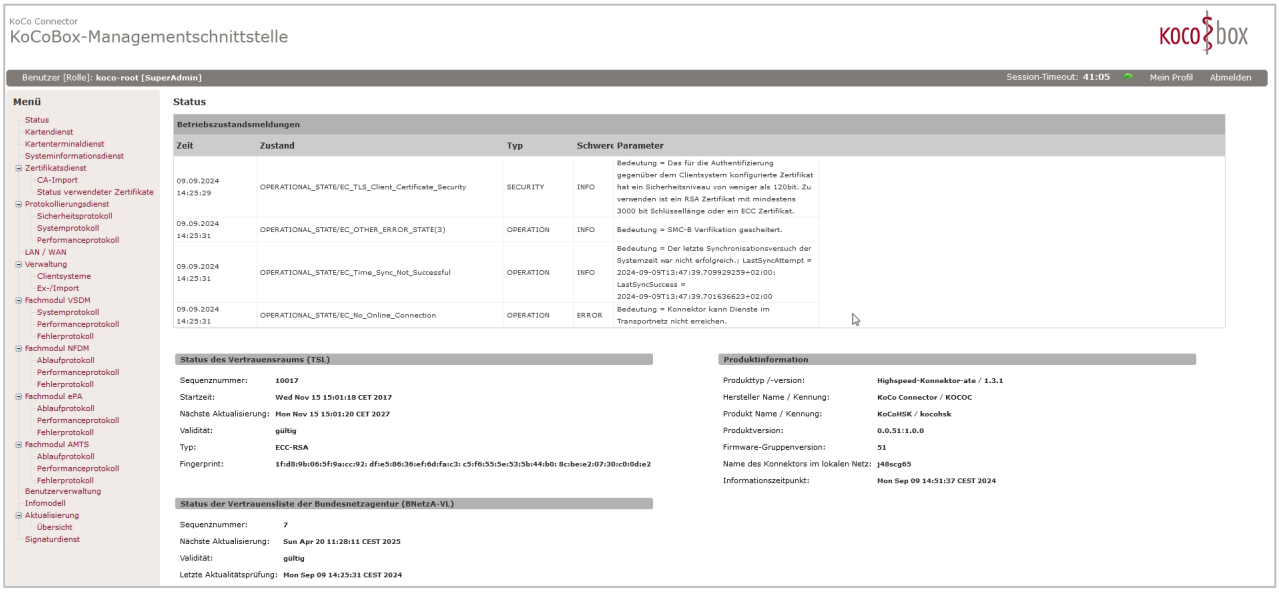


Abbildung 5: Aufbau der Managementschnittstelle am Beispiel der Status-Seite

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* sowie rechts das Produkt-Logo als grafisches Element.

[25] Die auf der Status-Seite hinterlegten Informationen werden im Abschnitt Status beschrieben.

Abbildung 6: Titelleiste der 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.[26]

Abbildung 7: Anzeige des Session-Timeout

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

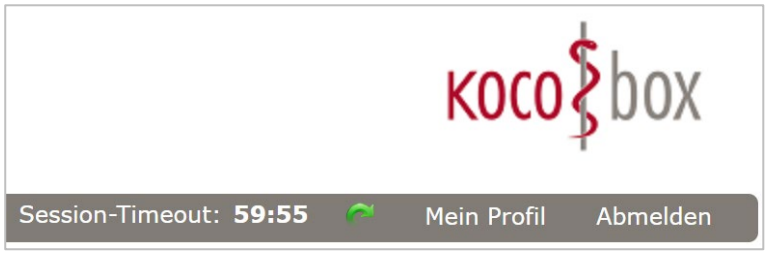


Abbildung 8: Session-Timeout zurücksetzen

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

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

Abbildung 9: Invertierte Sekundenanzeige vor dem Ablauf der Session

Über die hellgrau unterlegte Navigationsspalte links erfolgt der Aufruf der einzelnen Konfigurationsbereiche für die (Sicherheits-)Einstellungen. Sie bestehen aus 16 Haupt-Kategorien, von denen 8 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*
- *Protokollierungsdienst* mit den Unterbereichen *Sicherheitsprotokoll*, *Systemprotokoll* und *Performanceprotokoll*
- *LAN / WAN*
- *Verwaltung* mit den Unterbereichen *Clientsysteme, Ex-/Import*
- *Fachmodul VSDM* mit den Unterbereichen *Systemprotokoll, Performanceprotokoll* und *Fehlerprotokoll*
- *Fachmodul NFDM* mit den Unterbereichen *Ablaufprotokoll*, *Performanceprotokoll* und *Fehlerprotokoll*
- *Fachmodul ePA* mit den Unterbereichen *Ablaufprotokoll, Performanceprotokoll* und *Fehlerprotokoll*
- *Fachmodul AMTS* mit den Unterbereichen *Ablaufprotokoll*, *Performanceprotokoll* und *Fehlerprotokoll*
- *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 Unterschriftsbalken 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.

6.4 Grundkonfiguration des Konnektors

Im Folgenden wird die Grundkonfiguration des Konnektors für die sichere Einbindung in die Telematikinfrastruktur erklärt. Die per Werkskonfiguration eingetragenen Werte sind vorgegeben.[27]

Bei (zukünftigen) Änderungen an den Konfigurationen **muss** der dafür verantwortliche Administrator dies im Betriebsführungsbuch vermerken und unterschreiben.[28]

6.4.1 Status

Zur generellen Basisinformation finden Sie unter Status die *Betriebszustandsmeldungen*[29] in einer tabellarischen Übersicht, den *Status des Vertrauensraums* (TSL), den *Status der Vertrauensliste der Bundesnetzagentur (BNetzA-VL)* sowie *Produktinformation*.

Einstellungen werden hier nicht vorgenommen.

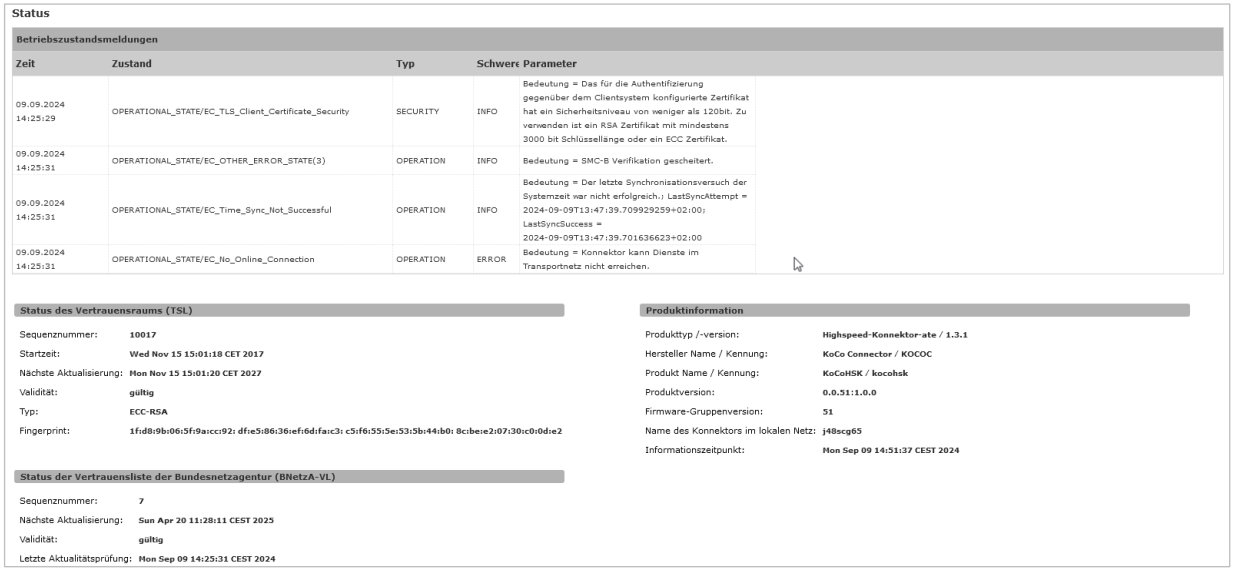


Abbildung 10: Übersicht zu den Statusinformationen

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

---

[27] Diese Werte stammen aus der jeweils aktuellen Konnektor-Spezifikation der gematik (zu finden im Fachportal https://fachportal.gematik.de bzw. auf https://gemspec.gematik.de).

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

[29] mit den Spalten Zeit, Type, Schwere, Beschreibung sowie Parameter

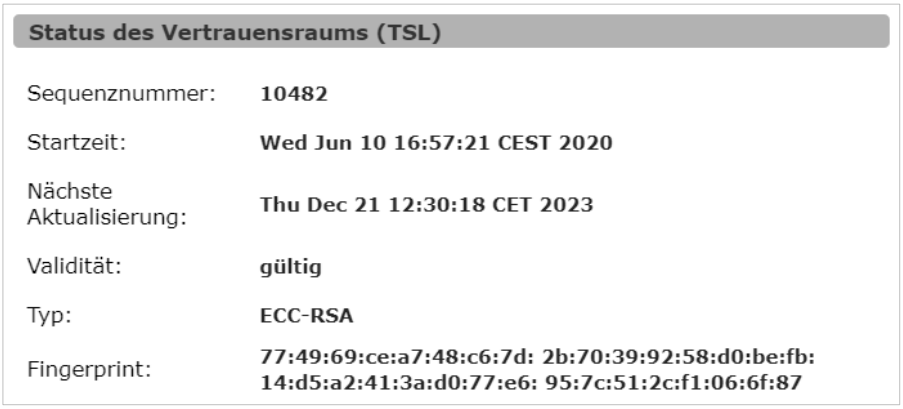


Abbildung 11: Ausschnitt des Vertrauensraumstatus (TSL) im ECC-RSA-Vertrauensraum

6.4.2 Zusammenfassende Übersicht zur Initialkonfiguration

Im Folgenden wird überblicksartig das chronologische Vorgehen für die initiale Konfiguration des Konnektors 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 , 6.1 sowie 7.2)

- Öffnen Sie am Netzwerkrechner den Browser und geben Sie die mit den Verbindungsinformationen erhaltene IP-Adresse der KoCoBox HSK

  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 (InItal4StartUp!) als Super-Administrator an.
- Sie werden anschließend zur unmittelbaren Änderung dieses Passworts aufgefordert.
- Geben Sie zwei Mal das neue persönliche Passwort ein. Erstellen Sie bitte ein sicheres Passwort mit 19 (empfohlene Anzahl, jedoch mindestens 8) Zeichen aus drei verschiedenen Zeichenklassen.
- Nach erfolgreicher Anmeldung erscheint die Status-Seite der Managementschnittstelle.

2 Bei einem Einsatz in einem TI-Gateway[30] folgende Punkte prüfen:

- Im Bereich *Benutzerverwaltung* dürfen keine weiteren Benutzer der Rolle Super-Administrator vorliegen (siehe Kapitel 6.6.1).
- Im Bereich *Infomodell* muss ein leeres Modell vorliegen (siehe Kapitel 6.6.2).

Sollte dies nicht gegeben sein, wenden Sie sich zur Klärung an Ihren Supportpartner.

[30] Der Zugang zu einer KoCoBox HSK ist ausschließlich über eine VPN-Verbindung aus dem Netz des Leistungserbringers (z.B. Arztpraxis, Apotheke) möglich. Daher ist keine Prüfung auf unerwünschte Freischaltungen für Zugänge zum Konnektor aus DVO-Netzbereichen im Zugangsportal des TI-Gateways erforderlich.

3 Im Bereich *Verwaltung – Clientsysteme* ist für die Konnektorauthentisierung an der Managementschnittstelle ein konnektorindividuelles Zertifikat auszuwählen (siehe Kapitel 6.5.1.1).

4 Im Bereich *Zertifikatsdienst* per Button TSL importieren eine gültige TSL manuell importieren (siehe Kapitel 6.4.4.2 bzw. 6.5.5)

5 *LAN/*WAN Dienst einsehen (siehe Kapitel 6.4.3)

- Prüfen Sie bei Bedarf in der Übersicht die aktiven Bestandsnetze. Wenden Sie sich bei fehlenden Einträgen an Ihren Supportpartner.
- Testen Sie bei Bedarf eine IP-Adresse und/oder FQDN-Adresse auf Erreichbarkeit.

Im Bereich *Verwaltung* den Leistungsumfang für die Signaturanwendungskomponente konfigurieren (siehe Kapitel 6.5.1)

6 Im Bereich *Kartenterminaldienst* Kartenterminal(s) pairen (siehe Kapitel 6.4.4.1 sowie 6.5.3)

- 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 OK-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.

7 Im Bereich *Infomodell* die Relationen definieren (siehe Kapitel 6.6.2)

- 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.

8 Im Bereich *Fachmodul VSDM* für jeden im Infomodell angelegten Mandanten ein Schlüssel-Paar anlegen (siehe Kapitel 6.7)

- 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.
- Bestätigen Sie die eingegebene Zeichenfolge mit OK.
- Per Button Übernehmen speichern Sie dies ab.

9 Freischaltung der SMC-B im Bereich *Kartendienst* (siehe Kapitel 6.5.2)

- 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.

6.4.3 Übersicht zu den Netzwerkkonfigurationen LAN/WAN

Der Bereich LAN/WAN gibt einen Überblick, Einstellungen werden hier nicht vorgenommen.

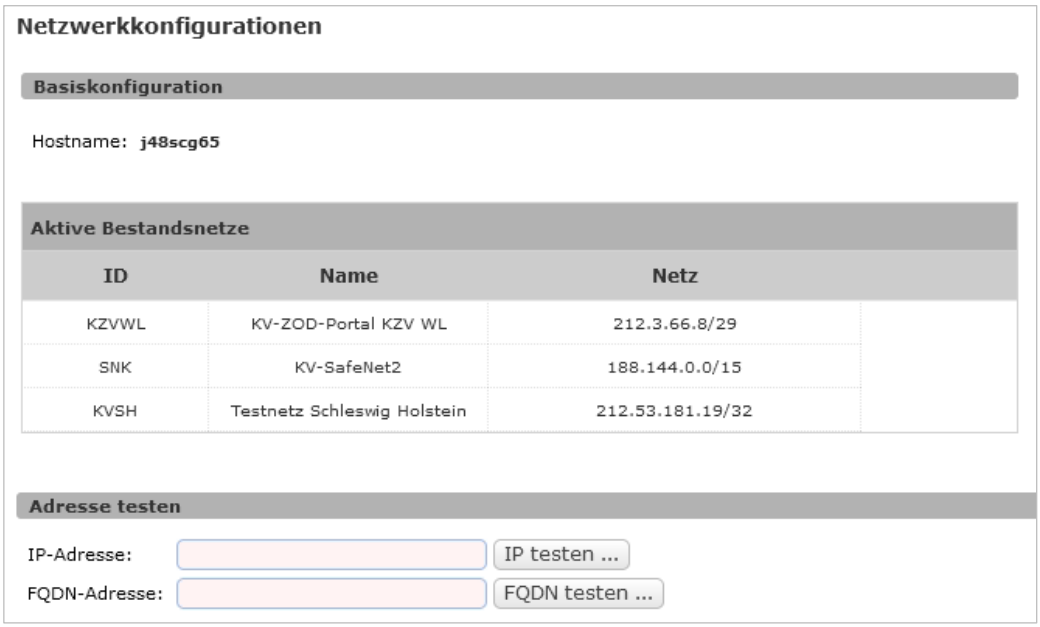


Abbildung 12: Exemplarischer Überblick zu den Netzwerkkonfigurationen der KoCoBox [31]

Im Bereich *Basiskonfiguration* wird der Hostname angezeigt. Dieser Wert ist statisch, er wurde durch den HSK bei der Erstellung der Instanz des Konnektors automatisch vergeben.

[31] Anmerkung der Redaktion: Der Überblick ist exemplarisch für eine Testumgebung.

Die darunterliegende Tabelle gibt einen Überblick zu den aktiven Bestandsnetzen (mit ID, Namen und Netz). Eine Aktivierung oder Deaktivierung von Bestandsnetzen erfolgt durch den Betreiber des HSK.

Im 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.

Während der Test durchgeführt wird, erscheint ein *Bitte-Warten*-Balken. Ist der Test beendet, erscheint eine Erfolgsmeldung bzw. eine Fehlermeldung. Prüfen Sie in diesem Fall Ihre Eingabe.

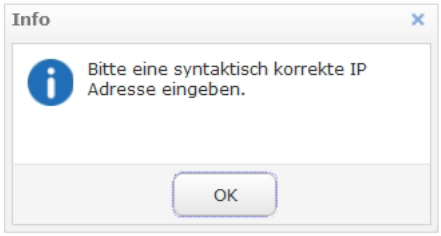


Abbildung 13: Fehlermeldung bei Falscheingabe

6.4.4 Aktivierung der Verbindung in die Telematikinfrastruktur

Um TI-Verbindungen aufbauen zu können, ist eine einmalige erfolgreiche Aktivierung der Verbindung notwendig.

Dafür kann eine im Infomodell bekannte SMC-B genutzt werden.[32] Diese SMC-B sollte bereits eine Echt-PIN besitzen und in einem Kartenterminal, das für die Verwendung mit der Managementschnittstelle vorgesehen ist, stecken.[33]

Der Aktivierungsprozess ist einmalig durchzuführen. Hierzu wird im Bereich *Kartendienst* die betreffende SMC-B ausgewählt und dort eine Freischaltung ausgeführt, wie in Abschnitt 6.5.2 beschrieben.

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

6.4.4.1 Anschluss von Kartenterminals

Im unteren Abschnitt Kartenterminaldienst finden Sie ausführliche Erläuterungen zum Anschließen von Kartenterminals bzw. dem Pairing mit dem Konnektor. Führen Sie zur initialen Inbetriebnahme für ein angeschlossenes Kartenterminal das Pairing durch.

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

Kartenterminals, die angeschlossen werden sollen, müssen eine entsprechende Adresse aus dem konfigurierten IP-Adressraum des Konnektors haben.

[32] Siehe unten den Abschnitt Informationsmodell

[33] Siehe dazu den Abschnitt Kartenterminaldienst sowie unten die Zusammenfassung

Die *Service Discovery* für Kartenterminals erfolgt während des Konnektorstarts 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.[34]

6.4.4.2 TSL-Import

Voraussetzung für eine Nutzung der Telematikinfrastruktur ist, initial eine TSL manuell in die KoCoBox zu importieren.[35]

Ein TSL-Import ersetzt die aktuell verwendete Liste, wenn die zu importierende TSL entsprechend signiert und eine höhere Sequenznummer bzw. Seriennummer beinhaltet. 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 wird die TSL von definierten Downloadpunkten bezogen und so aktuell gehalten. Dies erfolgt nach dem erstmaligen Import automatisch und periodisch (innerhalb von 24 Stunden).

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

[34] Siehe unten den Abschnitt Infomodell

[35] Siehe dazu die detaillierten Ausführungen unten im Abschnitt Zertifikatsdienst

6.5 Konfiguration des Anwendungskonnektors

Der Konnektor unterstützt mittels TLS-Schnittstelle in Richtung der Clientsysteme für alle Außenschnittstellen die in den folgenden Abschnitten näher beschriebenen Basisdienste[36]. Deren jeweilige Konfigurationsmöglichkeiten werden im Folgenden erläutert.

6.5.1 Verwaltung

Unter *Verwaltung* können Sie – auch wenn die KoCoBox im Auslieferungszustand alle Leistungsmerkmale aufweist – grundsätzliche Leistungsumfänge gezielt deaktivieren. Dies ermöglicht, die KoCoBox besser in die technische/organisatorische Struktur der Betriebsstätte zu integrieren[37]. 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).

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.

[36] Vgl. [gemSpec_Kon], Kap. 3.5 „Fachliche Anbindung der Clientsysteme“

[37] Vgl. [gemSpec_Kon], Kap. 4.3.6 „Leistungsumfänge und Standalone-Szenarios”

Abbildung 14: Konfigurationsbereich zur Verwaltung der Leistungsumfänge

Generell können Sie Konfigurationen über die Buttons Übernehmen bzw. Verwerfen annehmen bzw. abbrechen.

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.

Mittels Übernehmen speichern Sie die Einstellungen.

Bitte beachten Sie, dass eine gespeicherte Konfiguration abweichende Passworte enthalten kann. Nach dem Import dieser Konfiguration ist die KoCoBox ausschließlich mit diesen Daten erreichbar.

Selbsttest

Über den Button Selbsttest führt der Konnektor eine Prüfung der Integrität der Daten im Dateisystem 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 Managementschnittstelle in der Tabelle Betriebszustandsmeldungen die Meldung *Software Integrity Check failed*.

Sofern durch einen Neustart die Meldung nicht behoben werden konnte, verwenden Sie die KoCoBox nicht weiter. Kontaktieren Sie umgehend Ihren Support.

Reset

Durch Betätigung des Buttons Neustart des Konnektors erfolgt ein Neustart. In dessen Verlauf führt die KoCoBox 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* der KoCoBox manuell aufheben[38].

Solange dieser sicherheitskritische Fehlerzustand anhält, kann der Konnektor folgende Aufgaben nicht ausführen:

- automatisches Update der TSL vom Downloadpunkt
- Beziehen von KSR-Updateinformationen und –paketen für Kartenterminals.

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

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

[38] 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 die Instanz aufgrund der Verarbeitung großer Dateien an die Grenzen ihres zugeteilten 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 die Instanz 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.

Werksreset

Eine ausführliche Beschreibung der Möglichkeiten des Werksresets finden Sie unten im Abschnitt Konnnektormanagement / Werksreset.

Betriebsdatenmeldedienst

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

Die übermittelten Informationen umfassen:

- Produktinformation (Statusinformation)
- Verbindungsstatus TI
- Einstellungen der Clientsystemanbindung
- Operativer Zustand
- Informationen zu den Zertifikaten der Konnektor-Instanz, insbesondere Ablaufzeitpunkte
- Informationen zu den verbundenen Kartenterminals
- Informationen zur aktuellen TSL und BNetzA-VL im Konnektor
- Typ der Leistungserbringerumgebung (z.B. Arztpraxis)

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 einmal täglich an die Telematikinfrastruktur 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 versandt.

Lizenzbestimmungen

Am Fuße des Anzeigefensters im Bereich *Verwaltung der Leistungsumfänge* können Sie sich über den Button Lizenzbestimmungen anzeigen das entsprechende Dokument für die KoCoBox HSK als Text anzeigen lassen. Sie finden hier Informationen zur Lizensierung der Software, einen Haftungshinweis sowie die Datenschutzerklärung des Herstellers.

Der Konnektor enthält Open Source Software. Bitte beachten Sie hierzu das Kapitel *Lizenzinformationen* im Anhang.

6.5.1.1 Clientsysteme

In diesem Unterbereich werden die Konfigurationen zur Anbindung der Clientsysteme an die Dienstschnittstellen (SOAP und LDAP) sowie der Managementschnittstelle der KoCoBox HSK durchgeführt.

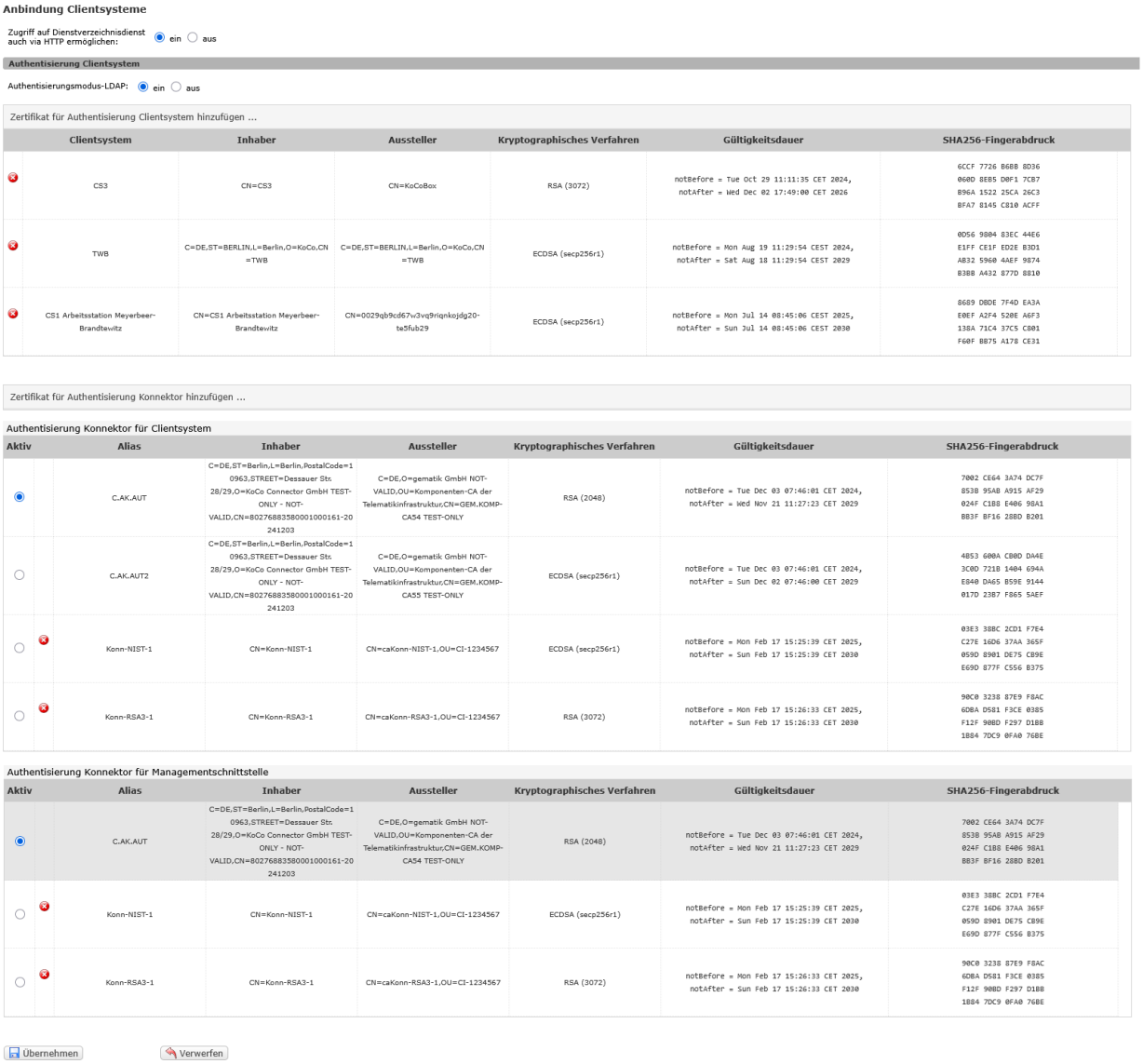


Abbildung 15: Konfigurationsbereich für die Anbindung der Clientsysteme

Der ausschließliche Zugriff auf den Dienstverzeichnisdienst (DVD) kann aus Kompatibilitätsgründen bei der KoCoBox auch via http erfolgen, dies ist entsprechend per Radiobutton ein/aus konfigurierbar.

Der Konnektor authentisiert sich grundsätzlich mit Hilfe eines Zertifikats gegenüber dem Clientsystem. Standardmäßig wird hierzu das Zertifikat C.AK.AUT der im Konnektor befindlichen gSMC-K verwendet. Es ist möglich, an dieser Stelle ein anderes Zertifikat durch den Konnektor zu erzeugen und exportieren (z.B. auf Basis elliptischer Kurven gemäß NIST-Spezifikation). Dieses kann dann dem Clientsystem zur Verfügung gestellt werden.

Alternativ erlaubt der Konnektor den Import eines Schlüsselpaars mit X.509-Zertifikat in Form einer passwortgeschützten PKCS#12-Datei. Aus der Menge dieser Zertifikate ist in der Clientsystem-Verwaltung genau eines für die TLS-Authentisierung der KoCoBox gegenüber dem Clientsystem

auszuwählen.

Für das Clientsystem kann ein Schlüsselpaar mit X.509-Zertifikat durch den Konnektor erzeugt und als passwortgeschützte PKCS#12-Datei exportiert werden. Diese Daten können dann dem Clientsystem zur Verfügung gestellt werden.

Alternativ gestattet der Konnektor den Import eines Zertifikats, das in der Clientsystem-Verwaltung 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 keinen Schutz gegen Man-in-the-Middle Attacken und ist daher zu vermeiden.

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 unter der IP-Adresse der KoCoBox auf dem Port 636 (LDAPS) zu erreichen. 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 hierfür erforderliche Clientzertifikat bzw. Schlüsselpaar ist unter *Authentisierung Clientsystem* zu registrieren.

Aus den Konfigurationsmöglichkeiten ergeben sich einige grundsätzliche Anforderungen an die Fähigkeiten und Konfiguration der Clientsysteme, siehe Abschnitt 8.5.1 :

- Zunächst wird mittels Radiobutton ja/nein der Zugriff auf den *Dienstverzeichnisdienst* (immer) *auch via http* ermöglicht bzw. unterbunden. Per Voreinstellung ist dies möglich.
- Der Authentisierungsmodus kann separat für den LDAP-Dienst über den Radiobutton *Authentisierungs-modus-LDAP* konfiguriert werden. Voreingestellt ist: ein. Es wird empfohlen diese Einstellung beizubehalten.

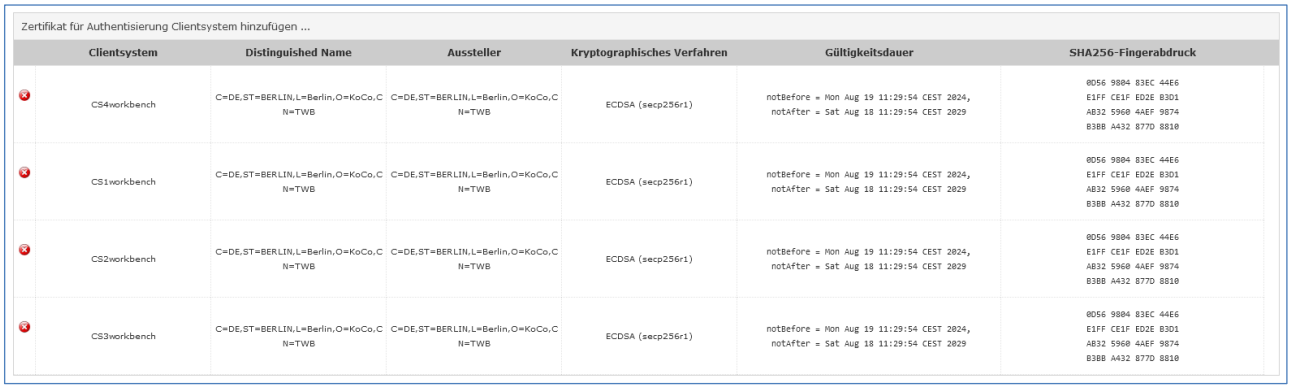


Abbildung 16: Übersicht zu angebundenen Clientsystemen

Im Bereich *Authentisierung Clientsystem* findet man eine tabellarische Übersicht über die einzelnen Konfigurationen. 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. Nach Klick auf diesen Button öffnet sich ein Pop-up-Fenster.

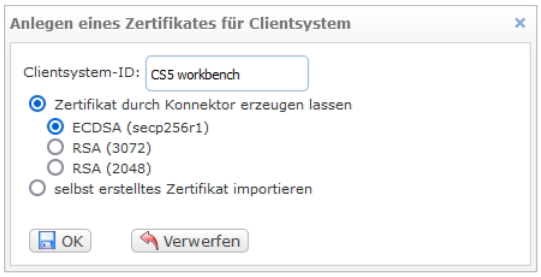


Abbildung 17: Konfiguration zum Anlegen eines Clientsystem-Zertifikats

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

1 Zum einen können Sie von der KoCoBox konnektoreigene Zertifikate – ECDSA (secp256r1), RSA (3072) oder RSA (2048) – erzeugen lassen. Diese werden als Container per Download zur Verfügung gestellt und stehen dann für die Konfiguration der sicheren Verbindung mit dem Clientsystem bereit.[39] Derartige Zertifikate sind ab Ausstellungsdatum für 5 Jahre gültig.

Beim Erzeugen entstehen in der Tabelle ein neuer Eintrag für das Endgeräte-Zertifikat (z.B. *CS5 workbench*) sowie für den Download der Zertifikatscontainer[40] im Format PCKS#12 mit diesem Endgeräte-Zertifikat und dem zugehörigen CA-Zertifikat (z.B. *j48scg65*[41]). Dieser Zertifikatscontainer ist auch zur geschützten Anbindung an die LDAP-Funktionalität (z.B. KIM-Client des Konnektors) geeignet.

2 Alternativ können Sie ein durch das Clientsystem bereitgestelltes Zertifikat in den sicheren Zertifikatsspeicher des Konnektors importieren. Wählen Sie dafür die Option selbst erstelltes

[39] Das Importieren dieses Zertifikatscontainers wird in der Dokumentation des Clientsystems beschrieben.

[40] Der Zertifikatscontainer wird in einem zip-Archiv verpackt für den Download bereitgestellt.

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

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 secp256r1 (NIST).
- Es wird der Import von Zertifikaten mit einer maximalen Gültigkeitsdauer von 5 Jahren zugelassen.

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 Krypto-algorithmen 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.

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 und der aktuelle Stand der gematik-Spezifikation die Verwendung solcher Schlüssel auf Ende 2025 limitiert.

Abgelaufene oder anderweitig ungültige bzw. nicht mehr benutzte Zertifikate sind aus der Liste umgehend zu löschen. Klicken Sie hierzu auf das Symbol der betreffenden Eintragszeile.

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 die KoCoBox HSK authentisieren, erforderlich. Diese wird nachfolgend beschrieben.

Im Bereich *Authentisierung Konnektor für Clientsystem* können in der Tabelle Zertifikate für die Konnektor-Authentisierung gegenüber mit ihm verbundenen Clients 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 18: Anlegen eines Konnektor-Authentisierungszertifikats

Im Dialogfeld zum *Anlegen eines Zertifikats für den Konnektor* können Sie auswählen, ob Sie ein Zertifikat vom Konnektor erzeugen lassen. Hier stehen die Optionen ECDSA (secp256r1), RSA (3072) oder RSA (2048) zur Verfügung. Alternativ können Sie ein selbst erstelltes Zertifikat importieren[42].

Die Verwendung von RSA-Schlüsseln mit einer Mindestlänge von 3072 Bits 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 und der aktuelle Stand der gematik-Spezifikation die Verwendung solcher Schlüssel auf Ende 2025 limitiert.

Sofern hier Zertifikate mit RSA-2048 konfiguriert sind, meldet der Konnektor den Betriebszustand EC_TLS_Client_Certificate_Security. Bis Ende 2025 ist der Einsatz dieser Schlüssel zulässig. Dieser Betriebszustand wird durch einen Wechsel auf längere RSA-Schlüssel bzw. auf 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.

[42] Es lassen sich ausschließlich PKCS#12-Container importieren - also inklusive des zugehörigen privaten Schlüssels. Dies ist notwendig, da die KoCoBox im Zuge der TLS-Authentisierung selbst Signieroperationen ausführt.

Sofern der Client ECDSA mit Brainpoolkurven unterstützt, kann er das während der TLS-Schlüsselaushandlung über das Feld supported_groups im ClientHello anzeigen. Bei entsprechender Systemkonfiguration durch den Hersteller verwendet die KoCoBox dann das passende Zertifikat C.AK.AUT2 (ECDSA mit einem Schlüssel auf einer brainpoolP256r1-Kurve). Diese Funktion wird von üblichen Webbrowsern **nicht** unterstützt.

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

Im Bereich Authentisierung Konnektor für Managementschnittstelle können Zertifikate für die Konnektor-Authentisierung für den Administratorzugang (TCP-Port 9443) gewählt werden. Hier kommt standardmäßig das Zertifikat C.AK.AUT zum Einsatz. Ein alternatives Zertifikat kann ausgewählt werden, wenn dieses zuvor im Bereich Authentisierung Konnektor für Clientsystem erstellt wurde.

Beim Einsatz im TI-Gateway ist zur eindeutigen Identifikation des Konnektors hier ein individuelles Zertifikat[43] auszuwählen. Dieses kann entweder durch den Konnektor erzeugt oder selbst erstellt sein. Das Zertifikat ist im Zertifikatsspeicher oder einer Freigabeliste (Allow List, White List …) des administrierenden Clients, also ggf. auch des verwendeten Webbrowsers, zu hinterlegen.

6.5.1.2 Ex-/Import

In diesem Unterbereich können Sie den *Import / Export der Konfigurationsdaten* der KoCoBox (z.B. nach einem Werksreset) durchführen.

Die vollständige Konfiguration (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.

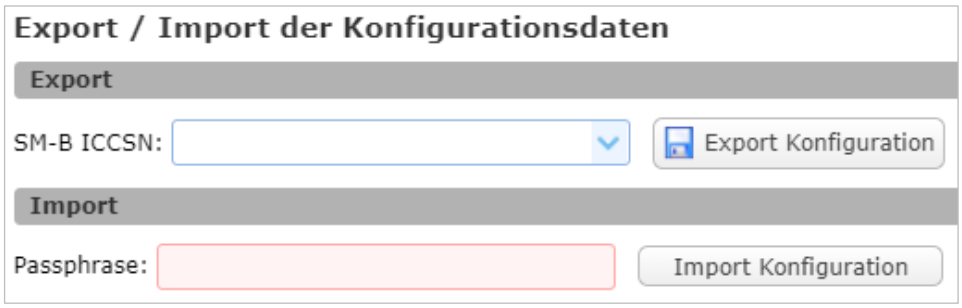


Abbildung 19: Konfigurationsdaten exportieren und importieren

[43] In einem TI-Gateway gelten die Identitäten der Zertifikate C.AK.AUT/C.AK.AUT2 jeweils für mehrere Konnektorinstanzen, weshalb sie für eine individuelle Identifizierung des Konnektors nicht genutzt werden können.

Bitte beachten Sie folgende Hinweise:

- Der Export der gesamten Konfiguration beinhaltet auch sämtliche **Kartenterminal-Konfigurationen**. Diese können anschließend beim Import der Konfiguration bei Bedarf selektiv in die KoCoBox importiert werden. Dabei werden die Kartenterminal-IDs (CT-IDs) aus der Ursprungskonfiguration übernommen.
- Sofern die Konfigurationen in eine andere KoCoBox 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.[44]

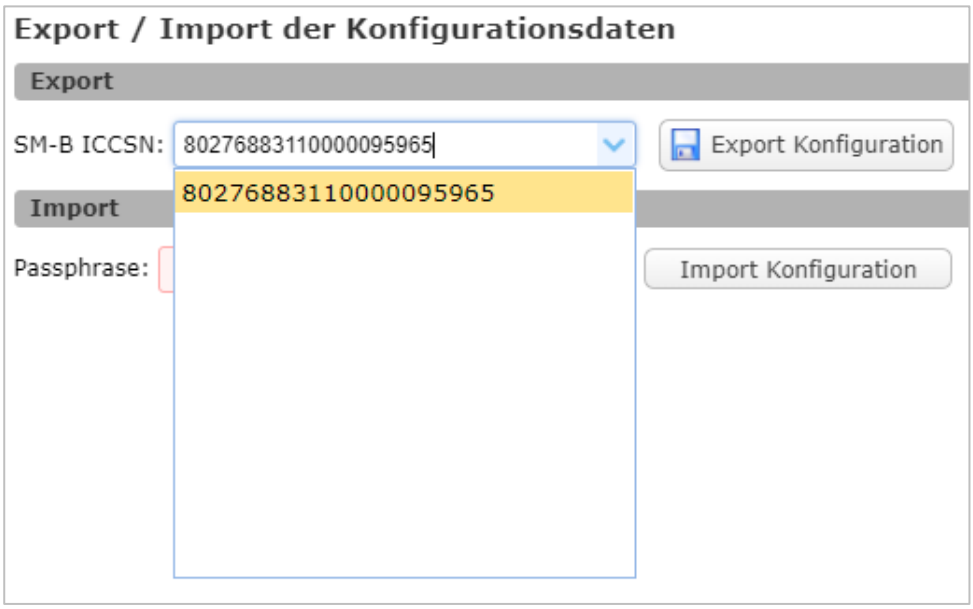


Abbildung 20: Auswahl der SM-B für Export der Konfigurationsdaten

2 Klicken Sie den Button Export Konfiguration. Am Kartenterminal werden Sie aufgefordert, die zur ausgewählten SM-B gehörende PIN einzugeben.[45]

[44] Siehe den Abschnitt Infomodell

[45] 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.

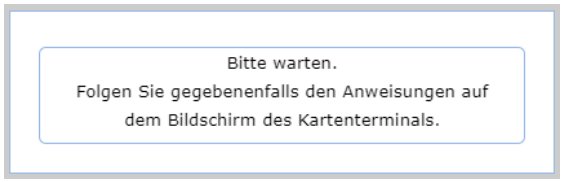


Abbildung 21: Anzeige für den Exportprozess

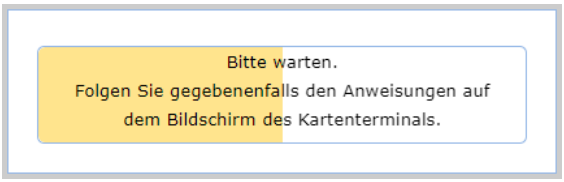


Abbildung 22: Anzeige für den Fortschritt im Exportprozess

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.

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.

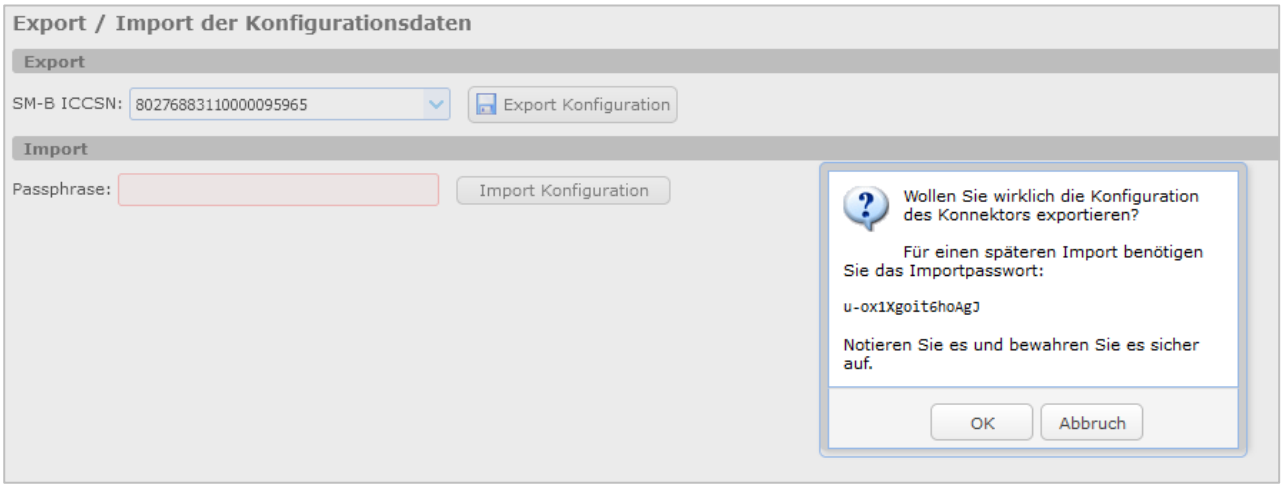


Abbildung 23: Importpasswort für späteren Import der Konfigurationsdaten

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

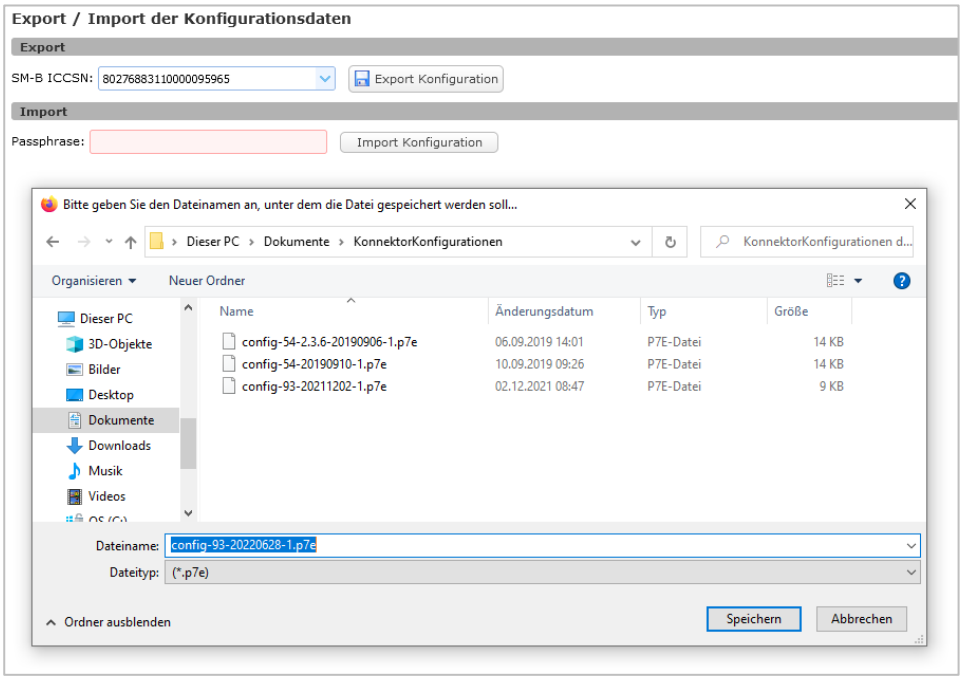


Abbildung 24: Speichern der Konfigurationsdaten-Datei

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.

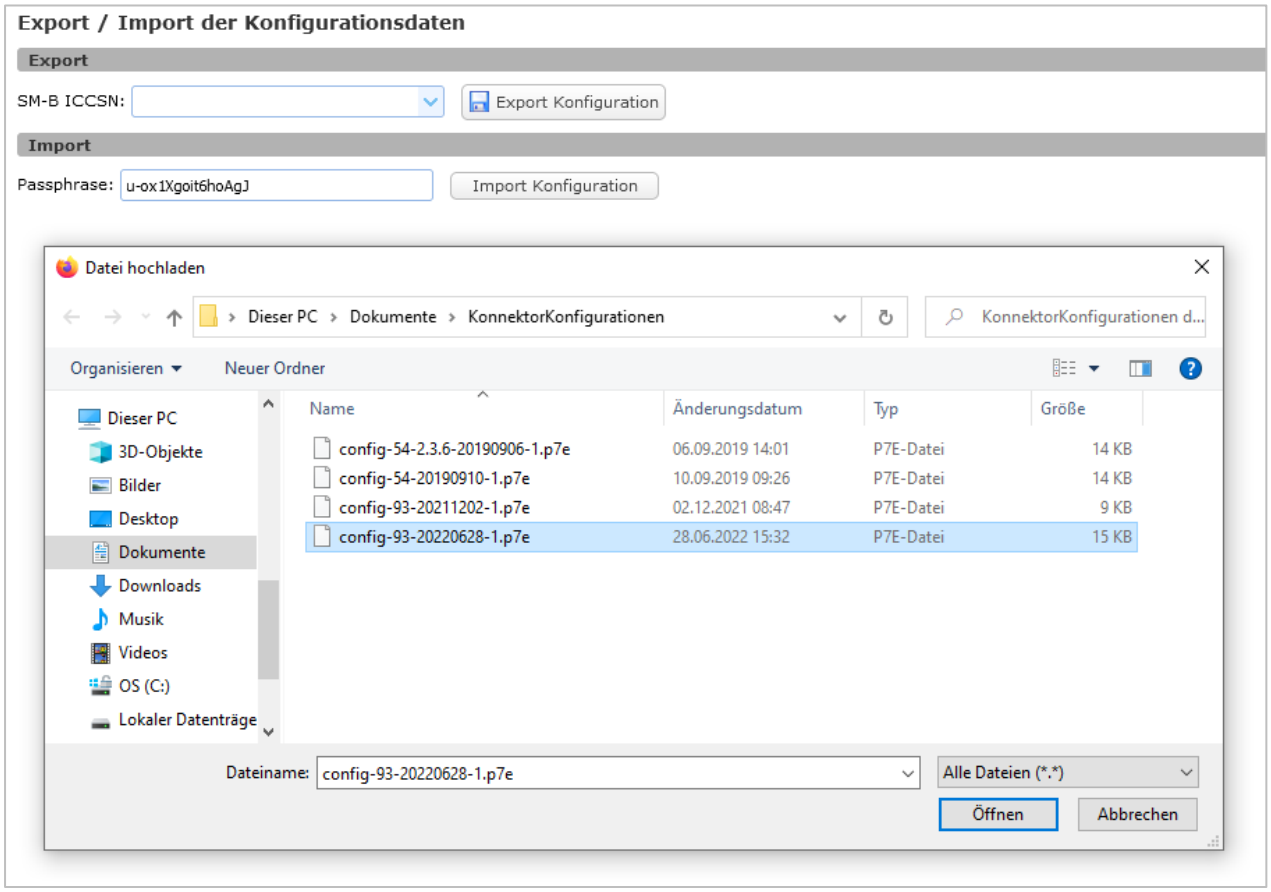


Abbildung 25: Importieren der Konfigurationsdaten-Datei

2 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.

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. zur entsprechenden Klinikabteilung passt. Überlegen Sie, ob Sie diesem Zertifikat noch vertrauen können. Nur wenn dies gegeben ist, sollten Sie mit Ja fortfahren. Anderenfalls empfiehlt sich ein Abbruch des Imports.

Abbildung 26: Anzeigefenster zur Kontrolle der Signaturinformationen

3 Anschließend erscheint ein Konfigurationsfenster für den Import von Kartenterminals.[46] Darin wählen Sie aus, welche dieser Kartenterminals Sie wieder importieren möchten, indem Sie ggf. Häkchen entfernen. Bestätigen Sie dies mittels OK.[47] Damit werden die Konfigurationsparameter übernommen.

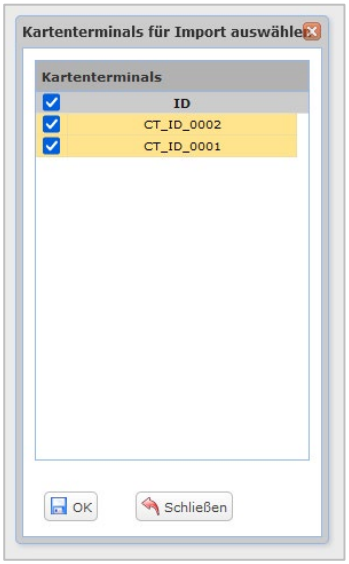


Abbildung 27: Auswahl für den Kartenterminal-Import

[46] Wird die Konfigurationsdaten-Datei in eine andere KoCoBox 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.

[47] 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.

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.

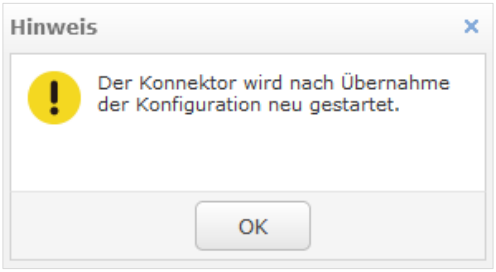


Abbildung 28: Dialogfenster mit Hinweis auf Neustart nach Konfigurationsübernahme

Bitte beachten Sie:

- 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.
- Beim Import von Konfigurationen aus Vorgängerversionen der KoCoBox 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 des Konnektors ausgeschlossen werden kann.

Bitte beachten Sie folgende Sicherheitshinweise:

- Aus Sicherheitsgründen kann der Exportvorgang nur von einem angemeldeten Benutzer mit mindestens der Rolle Administrator ausgelöst werden.
- Aus Sicherheitsgründen kann der Importvorgang nur von einem angemeldeten Benutzer mit der Rolle Super-Administrator ausgelöst werden.
- Der für den Export bzw. Import von Konfigurationsdaten des Konnektors 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 berechtigte Personen dürfen in den Besitz dieser Information gelangen. Schützen Sie exportierte Konfigurationsdaten ebenfalls vor unbefugtem Zugriff.

6.5.2 Kartendienst

Die KoCoBox führt eine Liste aller Karten, die in die von ihm verwalteten Kartenterminals gesteckt sind. Im Navigationsbereich *Kartendienst* finden sich die dazugehörigen Übersichten und Einstellungsoptionen.[48]

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

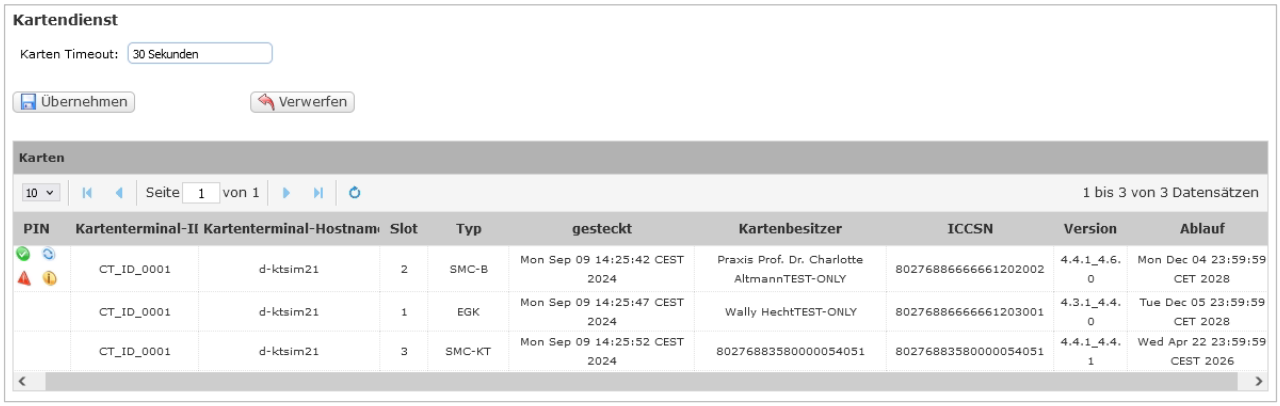


Abbildung 29: Konfigurationsbereich für den Kartendienst

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

Gleichzeitig bietet dieser Bereich einen Überblick über die jeweiligen aktuell gesteckten Karten mit Detailinformationen[49]:

- PIN[50]
- 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)[51]
- 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.

[49] Die detaillierten Versionsangaben zu den gesteckten Karten im CETP-Event sind im Anhang zu finden.

[50] 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.

[51] Vgl. [gemSpec_Karten_Fach_TIP]

6.5.3 Kartenterminaldienst

Der Kartenterminaldienst managt alle von der KoCoBox 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 ihm vorgesehen sind. Es ermöglicht damit eine gesicherte Verbindung zwischen Konnektor und Kartenterminal.[52]

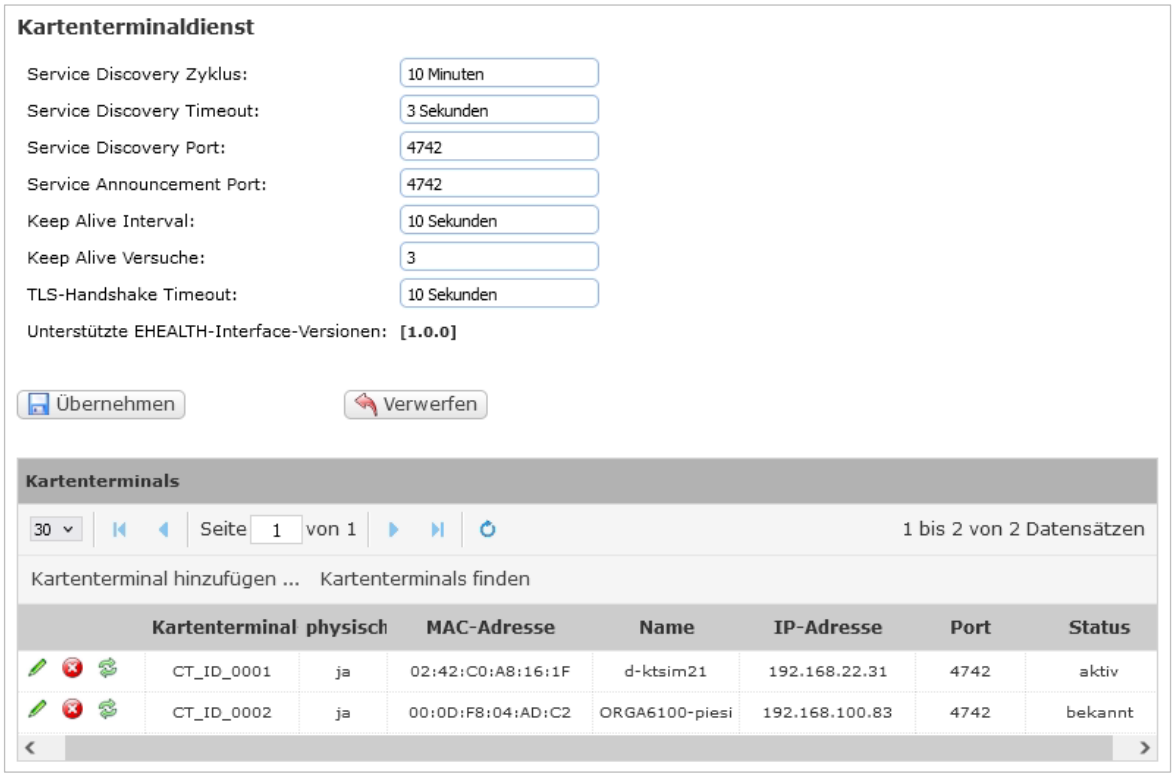


Abbildung 30: Konfigurationsbereich für den Kartenterminaldienst

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

[52] Vgl. [gemSpec_KT], S. 37 ff.

kann jeder Wert von 0 bis 65.535 eingetragen werden.[53]

- *Service Announcement Port* (=Kartenterminals melden über diesen Port des Konnektors ihre Service Announcements). Hier kann jeder Wert von 0 bis 65.535 eingetragen werden.[54]
- *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.[55]
- *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 zur KoCoBox 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 an diesem 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 der KoCoBox, wirksam.

Im unteren Bereich finden Sie eine tabellarische Auflistung aller dem Konnektor bekannten Kartenterminals mit jeweiligem Status.[56]

Mit dem Button Kartenterminals finden kann man auf manuellem Weg das Auffinden von Kartenterminals durch den Konnektor im Netzwerk anstoßen.[57]

---

[53] Hier ist sicherzustellen, dass andere Netzwerkgeräte nicht über den gewählten Port kommunizieren.

[54] Hier ist sicherzustellen, dass andere Netzwerkgeräte nicht über den gewählten Port kommunizieren.

[55] Die gesamte Wartezeit (Timeout) des Konnektors 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.

[56] Das Update der Kartenterminals wird unten im Abschnitt Aktualisierung beschrieben.

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

Abbildung 31: 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*[58] des Kartenterminals ein.

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

Abbildung 32: Kartenterminal hinzufügen

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

Beim Hinzufügen eines Kartenterminals im Kartenterminaldienst darf dieses noch nicht mit gleichem SICCT-Terminal-Namen in der Liste vorhanden sein. Die KoCoBox 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-

[58] Alternative Bezeichnung: FriendlyName

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 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.[59]

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

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

[59] 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.

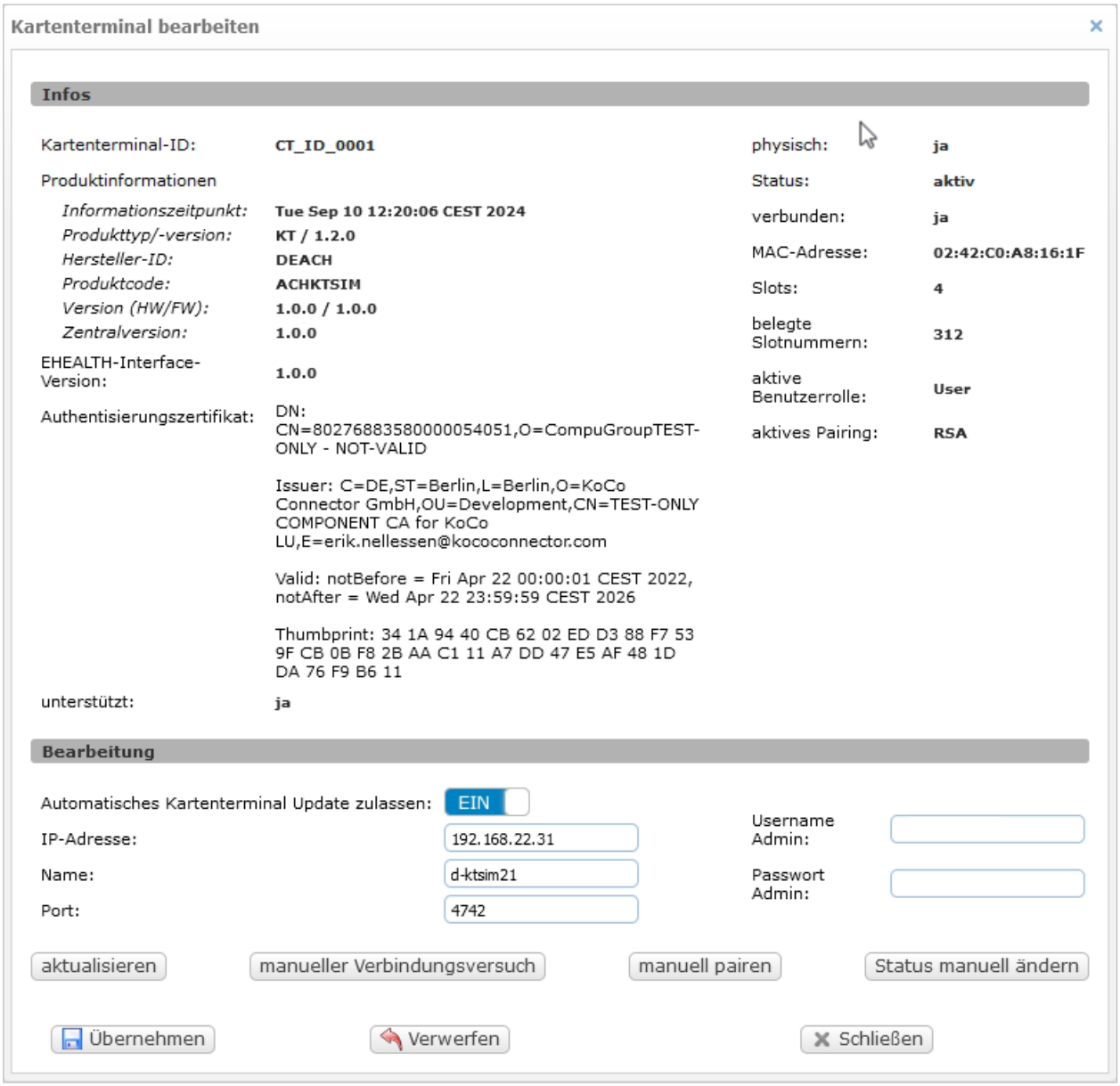


Abbildung 33: Vorhandenes Kartenterminal bearbeiten

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

- *Kartenterminal-ID*: zur eindeutigen, statischen Identifikation des Kartenterminals
- *Produktinformationen*[60]: 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)*

[60] vgl. [gemSpec_Kon], S. 85 ff.

  - Gültigkeitszeitraum *(Valid)*
  - Fingerabdruck *(Thumbprint)*
- *unterstützt*: Version des Kartenterminals wird durch die KoCoBox 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[61]
  - *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.

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

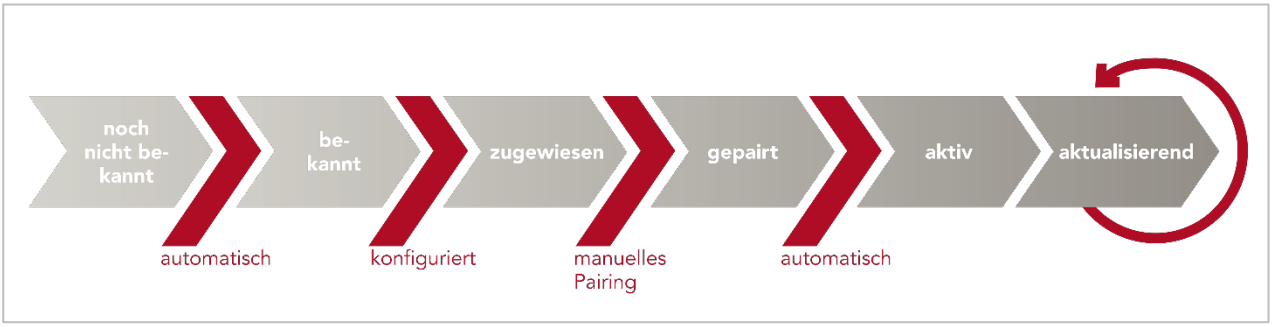


Abbildung 34: Übersicht der Verbindungsstatus eines Kartenterminals zum Konnektor

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.[62]

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.

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

Abbildung 35: 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 werden im Systemprotokoll dokumentiert.

Durchführung Kartenterminal-Pairing im Kartenterminaldienst

Um ein der KoCoBox schon bekanntes[63] 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.[64] 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.[65] Anderenfalls sollten Sie den Pairingvorgang abbrechen.
5. 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.

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

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

[65] 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.

Notieren Sie nach Abschluss des Pairings die Kartenterminal-ID (CT-ID).[66] 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, anderenfalls können keine Zugriffe vom Konnektorauf 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:

1. Öffnen Sie das Konfigurationsfenster *Kartenterminal bearbeiten* durch Auswahl in der Liste der bekannten Kartenterminals.
2. Ändern Sie über den Button Status manuell ändern vorübergehend den Status des Kartenterminals. Hierbei werden die Informationen des Kartenterminals aktualisiert.
3. 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.

6.5.4 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.[67]

[66] Die CT-ID ist für den Eintrag im Infomodell erforderlich.

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

Abbildung 36: 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 die KoCoBox alle Abonnements zu diesem Clientsystem in der internen Verwaltung. In der Folge erhält das Clientsystem keine Ereignisse mehr von ihm.

In der Übersicht *Monitoring von Operationen* werden der Operationsname OK_Val, NOK_Val[68] 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

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.

[68] OK_Val bedeutet einen erfolgreichen Abschluss der Operation, NOK_Val bedeutet ein fehlerhaftes Beenden der Operation

Ausführliche Erklärungen finden Sie in den Tooltips zur Überschrift *Monitoring von Operationen* sowie zur *Zertifikatsprüfung*[69] 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 unterstützt Missbrauchserkennungen: Sobald eine auffällige Häufung von Operationsaufrufen in den letzten 10 Minuten erkannt wurde, gibt er 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 **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 als herstellerspezifische Fehlermeldung[70] mit.

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

6.5.5 Zertifikatsdienst

Der Zertifikatsdienst bietet eine Schnittstelle für das Überprüfen der Gültigkeit von Zertifikaten an.[71] Er stellt unter anderem die vertrauenswürdige Kommunikation sicher.

[69] Ausführlicher zur Signaturzertifikatsprüfung siehe [gemSpec_Kon], S. 356ff.

[70] Fehler 20032, siehe auch im unteren Abschnitt Herstellerspezifische Fehlermeldungen

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

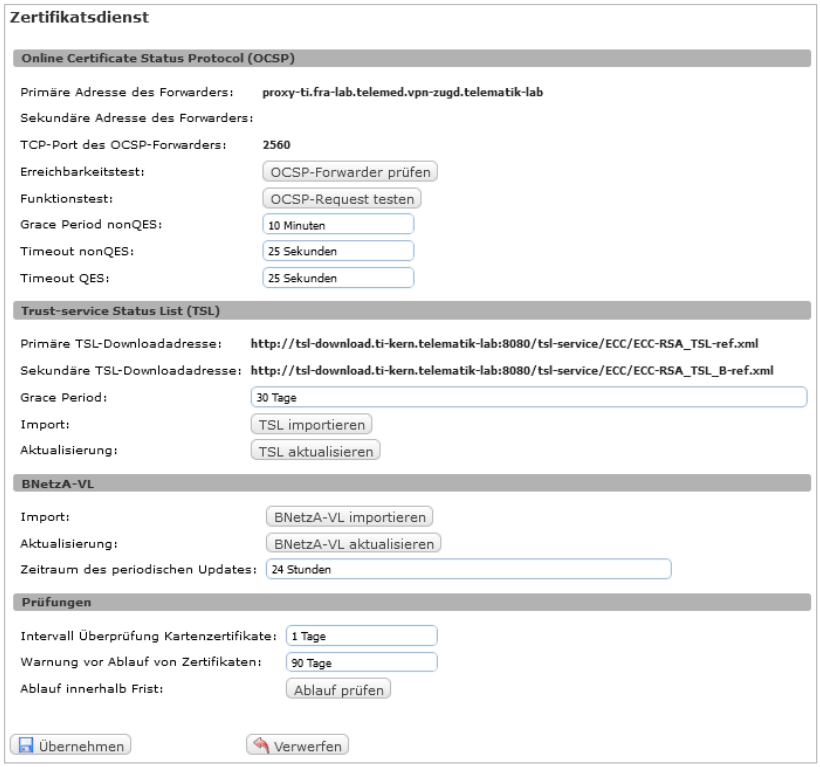


Abbildung 37: Konfigurationsbereich für den Zertifikatsdienst

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 38: Meldung nach erfolgreichem Test einer OCSP-Anfrage

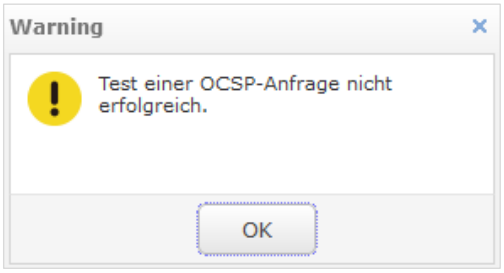


Abbildung 39: Meldung nach erfolglosem Test einer OCSP-Anfrage

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* angezeigt. Diese Adressen sind nicht konfigurierbar.

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.[72]

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 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. Den Ablauf von Zertifikaten innerhalb einer Frist (in der Zeile *Ablauf innerhalb Frist*) für die dem System bekannten Karten können Sie über den Button Ablauf prüfen kontrollieren. Nach Klick erscheint eine Übersicht der ablaufenden Karten inklusive Ablaufdatum.

[72] Der Downloadpunkt ist: https://tl.bundesnetzagentur.de/TL-DE.xml [Stand: September 2025]

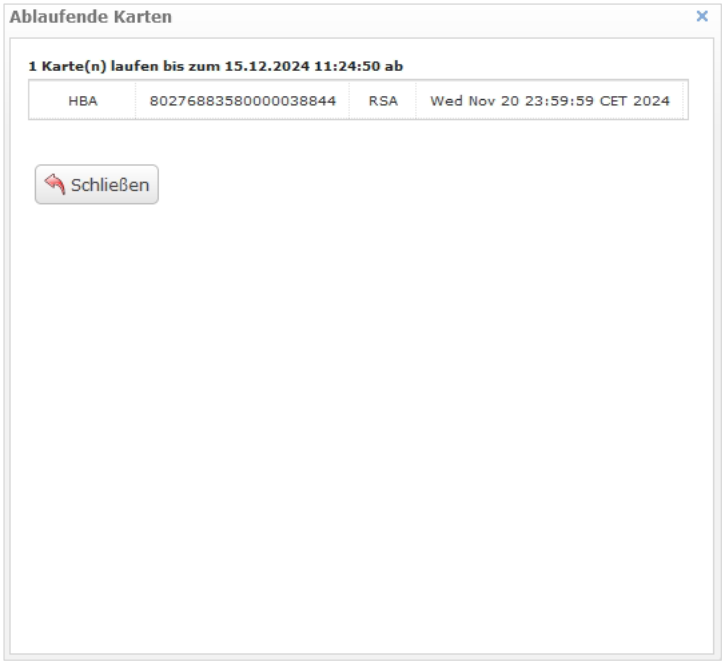


Abbildung 40: Übersicht für ablaufende Karten

Für die initiale Konfiguration gehen Sie wie folgt vor:

1 Importieren Sie zunächst die *Trust-service Status List (TSL)* über den Button TSL importieren.[73]

Im Bereich *Online Certificate Status Protocol* werden die primäre und sekundäre Adresse des Forwarders[74] sowie der TCP-Port des OCSP-Forwarders angezeigt.

3 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*.

4 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.

Nachdem Sie sämtliche Einstellungen und Importe vorgenommen haben, speichern Sie diese mit dem Button Übernehmen ab.

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

[73] 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.

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

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.

6.5.5.1 CA-Import

Im Unterbereich CA[75]-Import werden neue CA-Zertifikate manuell durch den Administrator importiert. Diese sind ausschließlich für die Hybridverschlüsselung für TI-fremde Empfänger vorgesehen. Solche importierten CA-Zertifikate stellen den dazu erforderlichen Vertrauensraum zur Verfügung. Die Hybridverschlüsselung kann dann das TI-fremde Zertifikat des Empfängers gegen die CA prüfen und den symmetrischen Schlüssel mit dem Empfängerzertifikat verschlüsseln.

Den Import führen Sie über den Button neues CA-Zertifikat importieren durch.

Abbildung 41: 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.

Beachten Sie für manuell importierte X.509-CA-Zertifikate folgende Sicherheitshinweise[76]:

- 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 nachgewiesen haben.

[75] Certificate / Certification Authority (Zertifizierungsstelle)

[76] Vgl. [gemSpec_Kon], Kap. 3.7 „Verwendung manuell importierter CA-Zertifikate“

6.5.5.2 Status verwendeter Zertifikate

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

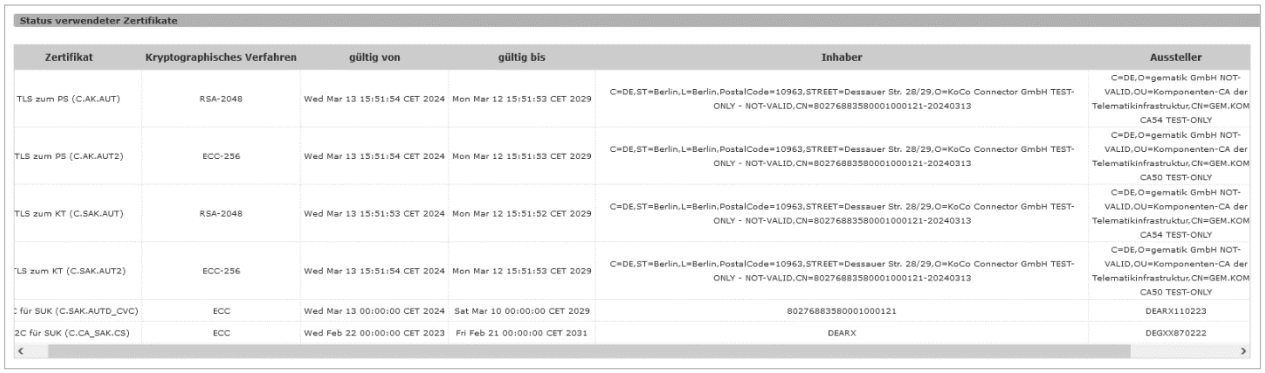


Abbildung 42: Übersicht zum Status der verwendeten Zertifikate

6.5.6 Protokollierungsdienst

Der *Protokollierungsdienst* zeichnet system- und sicherheitsrelevante Ereignisse, sowie Ereignisse im Kontext der Performancemessung innerhalb des Konnektors auf.[77]

Er enthält die Unterbereiche *Sicherheitsprotokoll*, *Systemprotokoll* und *Performanceprotokoll*.[78]

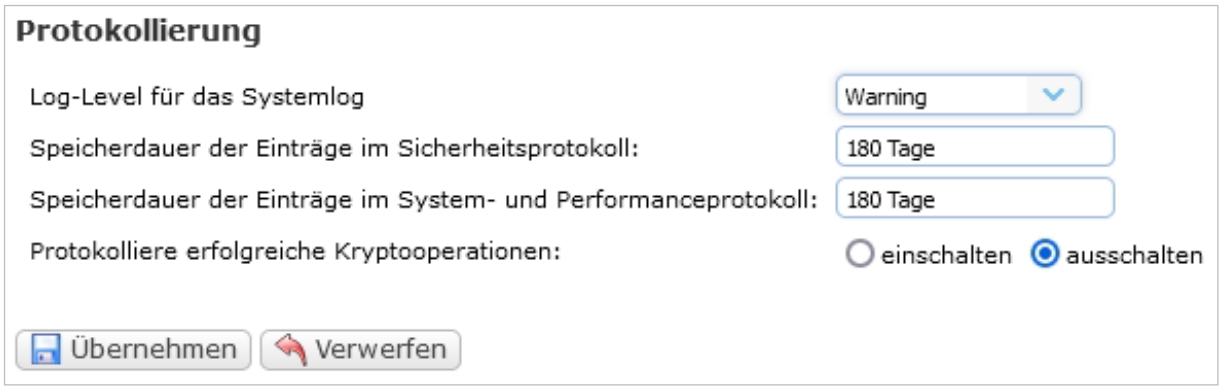


Abbildung 43: Konfigurationsbereich für den Protokollierungsdienst

1 Rufen Sie den Navigationsbereich Protokollierungsdienst auf und definieren Sie zunächst allgemeine Werte für diesen Dienst.

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).

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

[78] Details zum Aufbau der Logfiles siehe weiter unten

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,
- Spalte # (Kumulationszähler)
- Schwere,
- Beschreibung,
- Parameter.

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

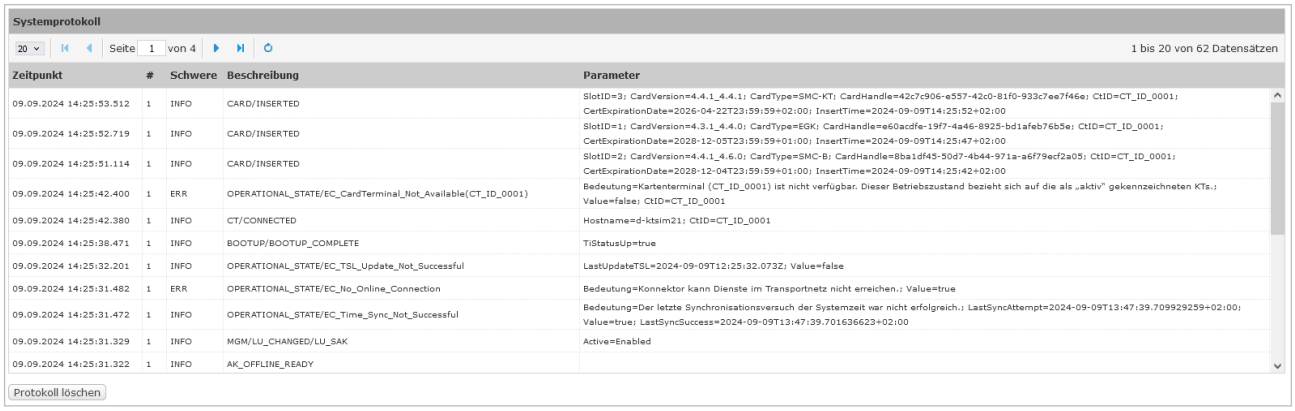


Abbildung 44: Übersicht zum Systemprotokoll

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.

Die KoCoBox überwacht sich selbst in festgelegten Zeitabständen hinsichtlich Änderungen seines Betriebszustandes.[79] Im Protokoll werden die Ergebnisse dieser Überwachung dokumentiert.[80]

Details zum Aufbau der Logfiles

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

- Sicherheitsprotokoll: Hier werden Logeinträge hinterlegt, die nicht löschbar 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 Moduls
Amount	Anzahl, wie oft die Meldung in diesem Logeintrag zusammengefasst ist[81]
Topic	Topic des protokollierten Ereignisses
protocolType	Schweregrad des Protokollierungseintrages
protocolSeverity	Protokollierungsart
Parameter	ereignisabhängige Parameter mit weiteren Details zum protokollierten Ereignis und Fehler

Tabelle 2: Aufbau der Logdateien im Protokollierungsdienst

6.5.7 Signaturdienst

Der Signaturdienst bietet Clientsystemen und Fachmodulen eine Schnittstelle zum Signieren von Dokumenten und Prüfen von Dokumentensignaturen.[82]

Er steht standardmäßig zur Verfügung und bietet zweierlei Funktionalitäten:

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

[80] 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 signalisiert, vgl. hierzu auch den Abschnitt Status und den Abschnitt Sicherheitskritische Fehlerzustände.

[81] Ähnliche Logeinträge werden nach bestimmten, komplexen Regeln zusammengefasst.

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

- 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).[83]

Generell erfüllt der Konnektor im Rahmen seines 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 den gleichen Zweck wie eine eigenhändige Unterschrift auf Papierdokumenten.[84]
- **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 der KoCoBox 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.[85]

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.[86]

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

[83] sowie den HBA-Vorläuferkarten HBA-qSig und ZOD_2.0 (=HBAx)

[84] Vgl. https://de.wikipedia.org/wiki/Elektronische_Signatur [Stand: September 2025]

[85] Siehe ausführlicher dazu die Dokumentation / Anleitung des jeweils eingesetzten Clientsystems.

[86] Sofern dieser Fehler wiederholt auftritt, kontaktieren Sie bitte Ihren Support.

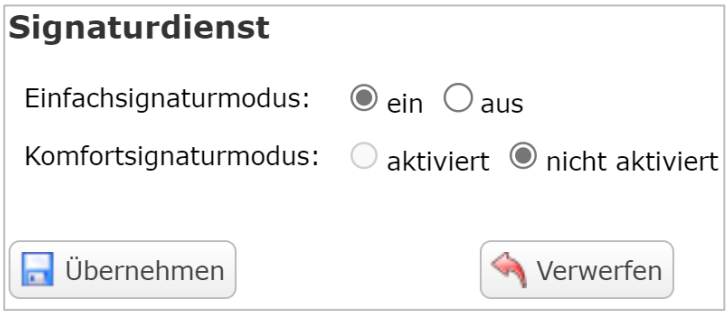


Abbildung 45: Konfigurationsbereich des Signaturdienstes bei deaktiviertem Komfortsignaturmodus

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 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 Messaging[87] 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.[88]

Mittels Übernehmen speichern Sie die jeweilige Konfiguration ab.

Nur Dokumente mit einer qualifizierten elektronischen Signatur (QES) gemäß eIDAS-Verordnung [eIDAS-VO] Kap. 1, Art. 3/12[89] 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.

Aus den Fähigkeiten des Signaturdienstes resultieren zusätzliche Anforderungen an die aufrufenden Clientsysteme, siehe hierzu Abschnitt 8.5.2 .

[87] Siehe dazu unten im Glossar den Eintrag zur Card-to-Card Authentisierung

[88] Siehe ausführlich zur Konfiguration weiter unten im Abschnitt Komfortsignatur

[89] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02014R0910-20241018 [Stand: September 2025]

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[90]) und signierte PDF-Dokumente (PAdES).
- Die KoCoBox verringert das Risiko solcher Angriffe durch interne Schutzmaßnahmen und die Eingrenzung auf bestimmte Signaturschemata. Werden also Dokumente, die **nicht** den nachfolgend genannten Kriterien entsprechen, dem Konnektor zur Verifikation vorgelegt, erhält der Nutzer eine Ungültigkeitsaussage für die betreffende Signatur. Gleichfalls unterstützt der Konnektor nur das Signieren von Dokumenten, die diesen Kriterien entsprechen.

Der Signaturdienst 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

Die KoCoBox unterstützt qualifizierte Signaturen auf XML-Dokumenten gemäß [XAdES-BL] und [XAdES] ausschließlich in Verbindung mit einer benannten Signaturrichtlinie. In der vorliegenden Version ist dies ausschließlich die in der Firmware der KoCoBox verankerte Signaturrichtlinie des Fachmoduls NFDM. Die letztgenannte Funktionalität ist dem Fachmodul NFDM vorbehalten und kann nicht durch Nutzer aufgerufen werden.

Eigenschaften der unterstützten Signaturrichtlinie 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.

[90] 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
Die KoCoBox 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 führt eine robuste Analyse von PDF-Dokumenten aus. Das Ziel der Funktionalität ist, eine möglichst große Spanne von PDF-Dokumenten verarbeiten zu können.

Der Konnektor ist nicht geeignet, Aussagen über die Standardkonformität von PDF-Dokumenten zu treffen; er 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.

Abbildung 46: 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 im Konnektor, 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).

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 des Konnektors 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.

6.5.8 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 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 verfügbaren Empfängerzertifikaten. Diese müssen für Verschlüsselung geeignet[91], 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 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.

[91] Dies wird durch das Zertifikatselement KeyUsage = keyEncipherment ermöglicht.

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 Vorausschau (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 bösartige (malformed) Dokumente angestrebt.

6.6 Konnektormanagement

In den folgenden Abschnitten werden die übergreifenden Konfigurationen der KoCoBox dargestellt.

6.6.1 Benutzerverwaltung

Der Konnektor bietet eine Verwaltung der Nutzer, die ihn in der Rolle eines Administrators konfigurieren sowie die Protokolle einsehen dürfen. In der Benutzerverwaltung werden die anmeldeberechtigte Administratoren-Benutzer definiert.

Abbildung 47: Benutzerverwaltung der KoCoBox

Hierbei werden zwei Administrator-Rollen mit verschiedenen Rechten unterschieden:

- *Admin*[92]: Besitzt 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*[93]: Besitzt 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. 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*: Besitzt lediglich die Berechtigung, Logdateien einzusehen und diese herunterzuladen, weitere Konfigurationen des Konnektors kann er weder einsehen noch modifizieren.

[92] Zur besseren Lesbarkeit im Fließtext wird diese Rolle auch als *Lokaler Administrator* bezeichnet.

[93] Zur besseren Lesbarkeit im Fließtext wird diese Rolle auch als *Super-Administrator* bezeichnet.

Die Tabelle *Benutzer* listet die Administrator-Benutzer der KoCoBox 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 48: Anlegen eines neuen Administrators in der Benutzerverwaltung

Ein neuer Administrator-Benutzer des Konnektors KoCoBox 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*[94], *LogDownloader*, *Supporter*[95]) sowie ggf. bestimmte Rechte (*Werksreset durchführen*) zu. Mittels OK wird der Eintrag bestätigt.

Es erscheint ein Anzeigefenster, das das Einmalpasswort beinhaltet. Notieren Sie dieses für den neu angelegten Administrator-Benutzer.

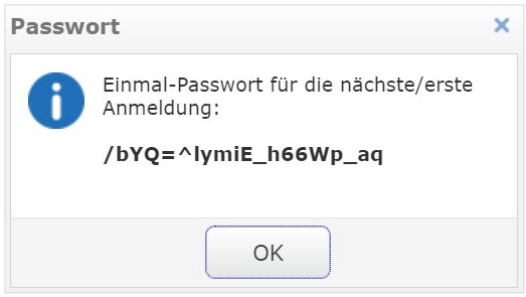


Abbildung 49: Anzeige des Einmalpassworts

3 Verlassen Sie abschließend dieses Anzeigefenster mit OK.

[94] Das ist der lokale Administrator.

[95] Die Rollen *LogDownloader* und *Supporter* sind herstellerspezifische Rollen, die Rolle *RemoteAdmin* ist unwirksam.

Der neu angelegte Administrator erscheint nun in der Tabelle *Benutzer*.

Dieser neue Administrator-Benutzer **muss** das Einmalpasswort bei seinem ersten Login auf der Managementschnittstelle in sein **persönliches Passwort ändern**.[96]

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.

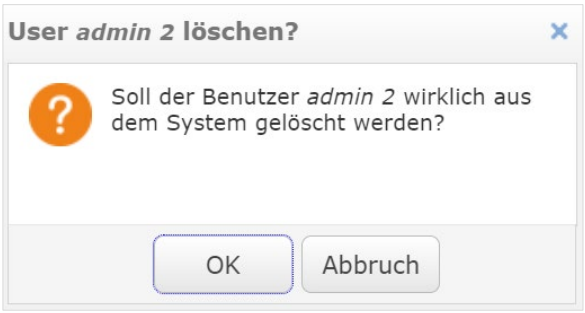


Abbildung 50: Löschen eines Administrator-Benutzers

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.

[96] Das Vorgehen entspricht dem der zweistufigen Vergabe des neuen Passworts bei der Erstanmeldung des Administrators an der Managementschnittstelle der KoCoBox.

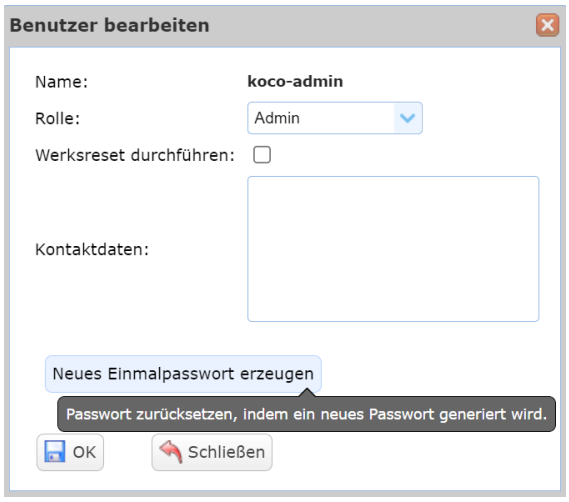


Abbildung 51: Passwort eines bestehenden Administrators ändern

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.

6.6.2 Infomodell

Im Bereich *Infomodell* werden einzelnen Personen (Mandanten) einzelne Arbeitsplätze und Clientsysteme zugewiesen.[97]

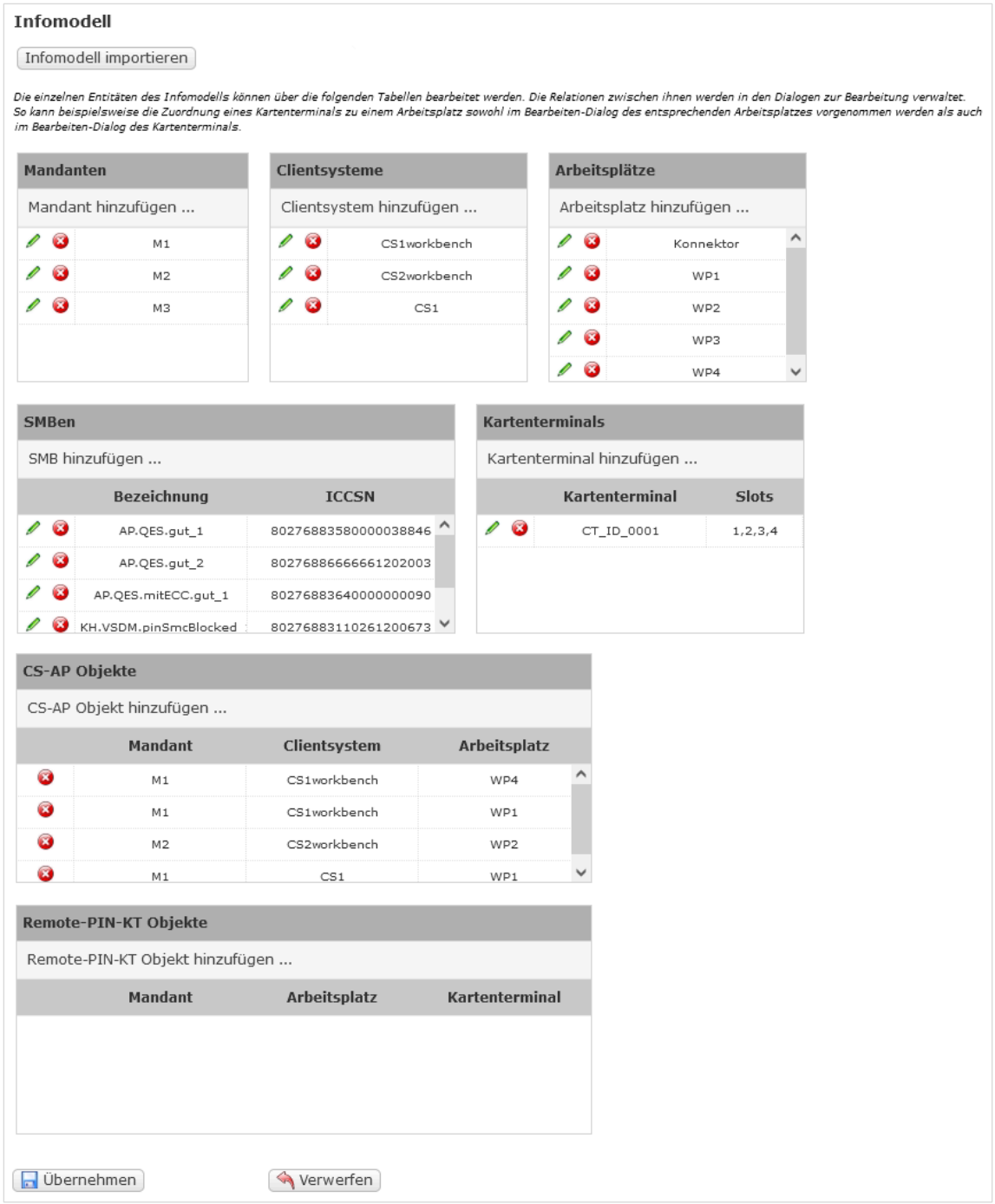


Abbildung 52: Beispiel-Informationsmodell für die erlaubten Zugriffsmöglichkeiten

[97] 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.[98] 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. Anderenfalls 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.

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.[99]

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.

[98] 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.

[99] 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:

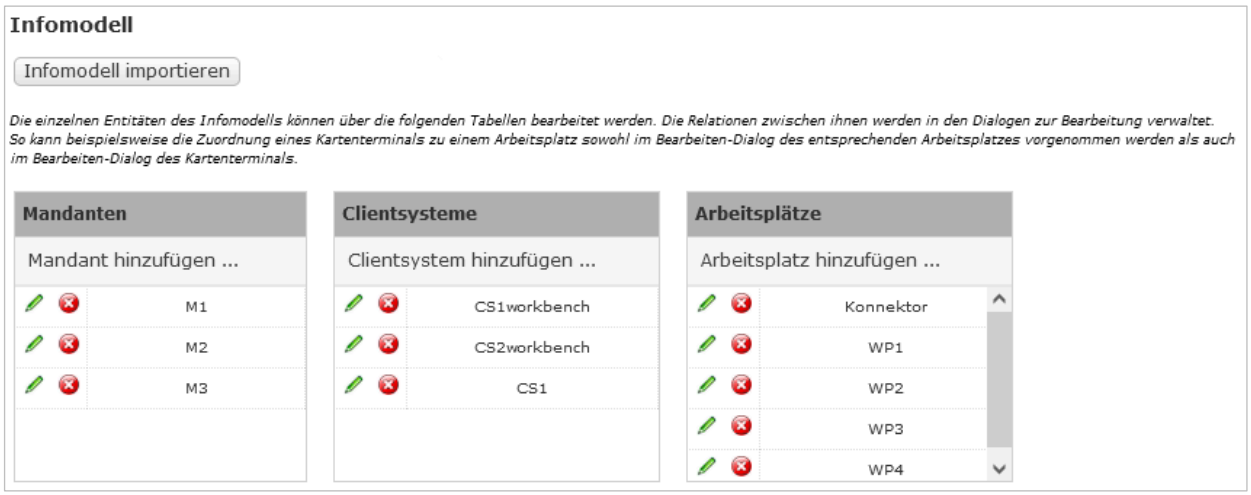


Abbildung 53: Infomodell-Konfigurationsbereiche für Mandanten, Clientsysteme und Arbeitsplätze

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.

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.

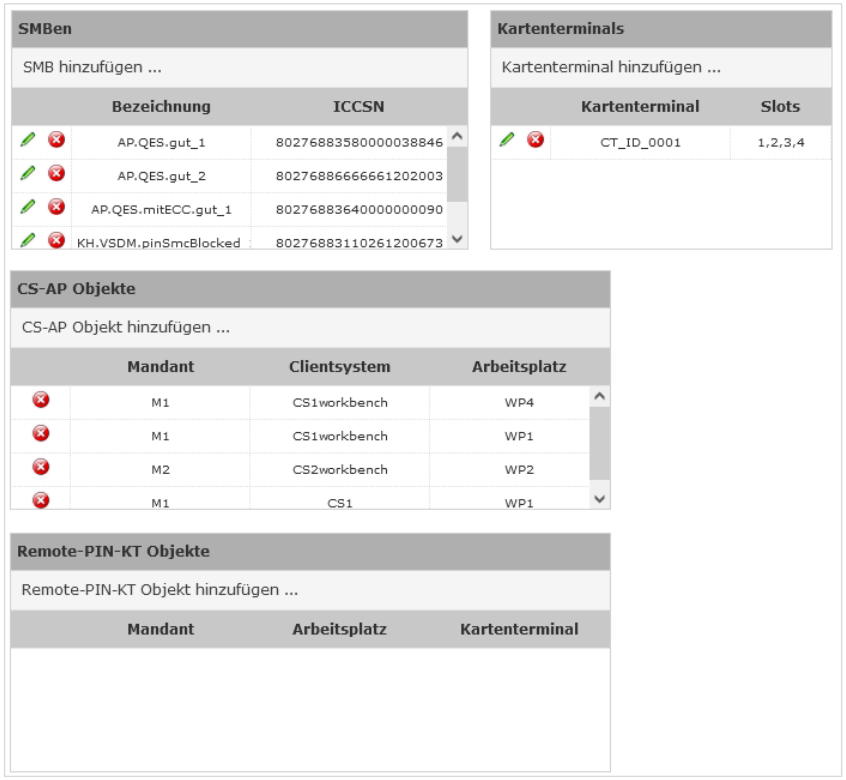


Abbildung 54: Infomodell-Konfigurationsbereiche für SMBen, Kartenterminals und CS-AP Objekte

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 55: 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.

Abbildung 56: Konfigurationsfenster zum Hinzufügen für Mandant, Arbeitsplatz, Kartenterminal

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.

6.6.3 Aktualisierung

Im Bereich *Aktualisierung* können Sie die von der KoCoBox verwalteten Kartenterminals softwareseitig aktualisieren.

Im Unterbereich *Übersicht* kann man den aktuellen Status von Updates für die Kartenterminals einsehen.

Updates werden gewöhnlich durch die Server des Konfigurations- und Software Repository-Dienstes (KSR-Dienst) bereitgestellt. Sie erscheinen entsprechend ihrer Verfügbarkeit für die verwalteten Geräte in der Liste *Kartenterminal-Aktualisierungen*. Einzelne Updates werden hier ausgewählt und aktiviert.

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 bei Ihrem Servicepartner oder dem jeweiligen Hersteller der Software verfügbar. Sie werden dann über den Bereich *Aktualisierung* direkt von einem lokalen Verzeichnis eingespielt und für die Aktualisierung des betreffenden Kartenterminals aktiviert.

Abbildung 57: Durchführung von Softwareaktualisierungen

Bitte beachten Sie folgende Sicherheitshinweise:

- Es darf nur eine **freigegebene, offiziell verfügbare, signierte** Software installiert werden.[100]
- Bereitgestellte Software-Updates für die Kartenterminals 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.

In der Zeile *Endpunkt für Firmware-Download* steht der Endpunkt des Konfigurationsdienstes zum Download

[100] Die Firmware-Versionen werden von der gematik GmbH (www.gematik.de) für den Betrieb in der Telematikinfrastruktur zugelassen bzw. genehmigt. Die zugehörigen Bestätigungen zur qualifizierten elektronischen Signatur (QES) sowie die Beschleunigten Sicherheitszertifizierung sind unter www.bundesnetzagentur.de und unter www.bsi.bund.de hinterlegt.

der Firmwaredaten.

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.

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.

Die automatische Aktualisierung wird über den Button Automatisches Update konfigurieren geplant. In einem neuen Konfigurationsfenster können Sie die konkrete Ausführung einstellen.

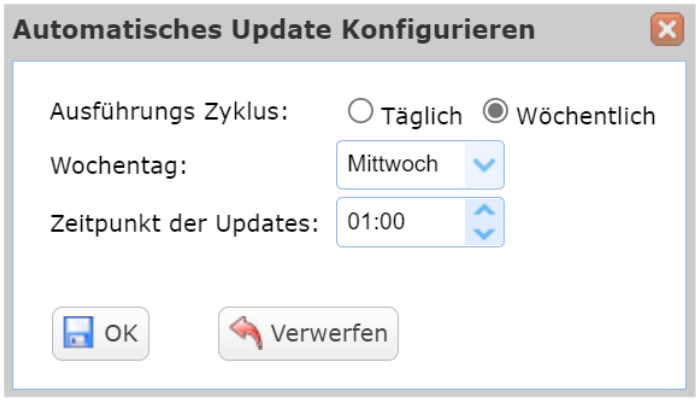


Abbildung 58: Konfiguration des automatischen Updates

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 Kartenterminal

Die Tabelle *Kartenterminal-Aktualisierungen* zeigt die vorhandenen Firmware-Updates für die von der KoCoBox 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 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.

Details zum ausgewählten Update können in der Tabelle per Klick auf in der jeweiligen Zeile eingesehen werden. Dazu öffnet sich das entsprechende Anzeigefenster.

Abbildung 59: 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.

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.

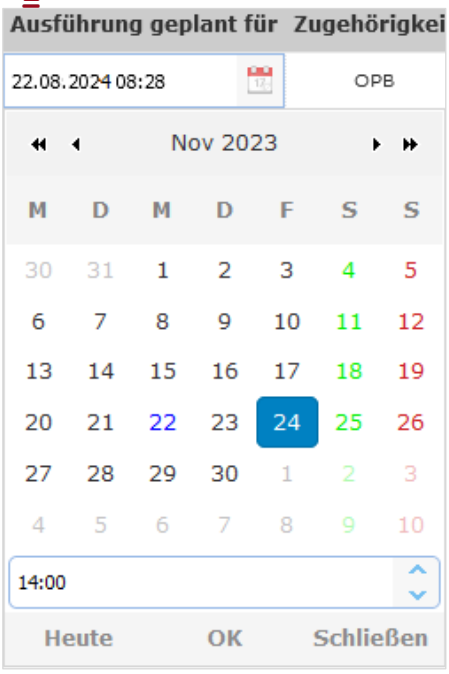
3 Setzen Sie das Häkchen in der Tabelle für das zu aktualisierende Kartenterminal. Über die Schaltfläche Aktualisierung planen können Sie den Updateprozess unmittelbar (ohne einen Ausführungszeitpunkt konfiguriert zu haben) starten, indem Sie die Rückfrage im Dialogfenster bestätigen. Die Übergabe zur 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 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 *Ausführung geplant für* ermöglicht die Planung der Aktualisierungen, sofern man sie **nicht unmittelbar** ausführen möchte. Die gerade bearbeitete



Tabellenzeile ist leicht farbig unterlegt.

Abbildung 60: Planung von Kartenterminal-Aktualisierungen

Das Aktualisierungsdatum können Sie jeweils per Klick in das Feld *Aktualisierungszeitpunkt* mittels Monatskalender und Uhrzeitfeld auswählen und per OK bestätigen.

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.

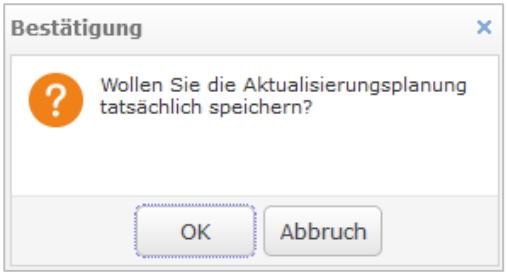


Abbildung 61: Planung für Software-Aktualisierungen bestätigen

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* zeigt den Status der Aktualisierungen für die Kartenterminals.

Die Tabelle zeigt für Kartenterminal(s) die interne *Update-ID*, die *Herstellerkennung*, die *Produktkennung*, die *Version*, den *Ausführungszeitpunkt* des Updates, den *Status* (als beschrifteter Verlaufsbalken), den *Bearbeitungsfehler* (als Code) sowie eine *Information*.

Die Übersicht erneuert sich – inklusive des Status der Aktualisierungen – automatisch alle 1.000 Millisekunden.

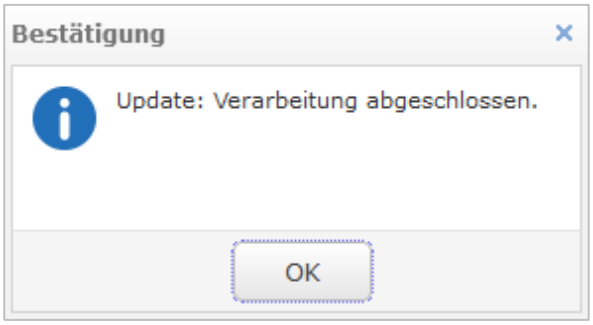


Abbildung 62: Meldung zum Abschluss der Update-Verarbeitung

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.

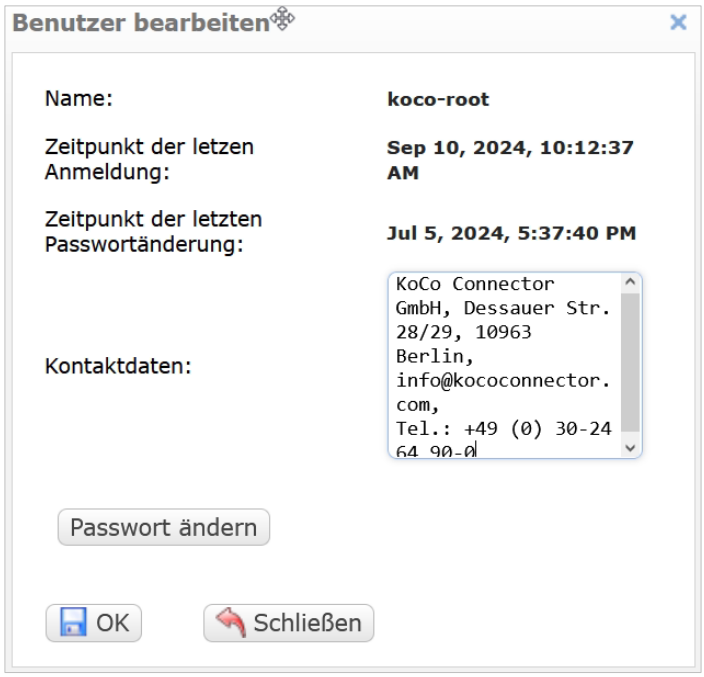


Abbildung 63: Mein Profil für Administrator-Benutzer mit Passwort ändern-Button

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.[101]

Beachten Sie bei der Neuvergabe des persönlichen Passworts die Sicherheitshinweise zur Passwortvergabe.

6.6.4 Werksreset

Generell können Sie über den Werksreset den Konnektor in den Auslieferungszustand zurücksetzen. Dies kann zum einen über die Managementschnittstelle sowie – in besonderen Situationen (z.B. Passwort unbekannt) – per Werksreset durch den Betreiber des Konnektors erfolgen.

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.[102]

[101] Siehe dazu die Ausführungen im Abschnitt Administrator-Passwort

[102] Siehe im Abschnitt Verwaltung / Ex-/Import

6.7 Fachmodule

Im Folgenden werden die Fachmodule, die die KoCoBox zur Verfügung stellt, dargestellt. Vorweg erfolgt eine Beschreibung der fachmodulspezifischen Sicherheitsmaßnahmen zu deren Betrieb.[103]

6.7.1 Fachmodulspezifische Sicherheitsmaßnahmen

Zur Einführung der in den folgenden Abschnitten beschriebenen Fachmodule 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 der Fachmodule NFDM, ePA bzw. AMTS 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.

Der Konnektor 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.[104]

Die Verwendung der äußeren Dienstschnittstellen der Fachmodule soll **ausschließlich** gemäß Definition in der gematik-Spezifikation (NFDM, ePA, AMTS) erfolgen. Der Konnektor 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. Dies ist daher unbedingt zu vermeiden.

Implementierungshinweis: Beachten Sie bei der Verwendung der Dienstschnittstellen, dass über alle Fachmodule des Konnektors 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.

[103] 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.

[104] 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 Signaturrichtlinie, 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 gelten die Sicherheitsziele für den Einsatz des Konnektors, die oben in Kapitel 3 dieses Handbuchs beschrieben sind.
Die Sicherheitseigenschaften der Fachmodule entsprechen 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 Beschleunigten Sicherheitszertifizierung des BSI geprüft. Hierzu nötige anwenderseitige Sicherheitsmaßnahmen sind in Kapitel 2 für die KoCoBox HSK insgesamt beschrieben.

Prüfen Sie bitte unmittelbar nach Inbetriebnahme der KoCoBox die Versionsnummer des Konnektors sowie die Versionsnummern der jeweiligen Fachmodule. Nehmen Sie diese nur dann in Betrieb, wenn diese Angaben korrekt sind.[105]

Die Versionsnummer der KoCoBox-Firmware finden Sie auf der Status-Seite der Managementschnittstelle rechts im Bereich *Produktinformationen.*

Die Versionsnummer der Firmware **muss** mit der aus dem entsprechenden BSZ-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/Beschleunigte-Sicherheitszertifizierung/Zertifizierte-Produkte-nach-BSZ/zertifizierte-produkte-nach-bsz_node.html

zur Verfügung oder können alternativ über die Hersteller-Webseite als Anfrage per Kontakt-E-Mail mit dem Betreff „*Zertifizierung [KoCoBox HSK]*" 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.

[105] 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 HSK]"* 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.

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.[106] 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 der KoCoBox sofort einzustellen und der Supportpartner zu kontaktieren, um weitere Handlungsanweisungen zu erhalten.

[106] Dies ist im Kapitel Protokollierungsdienst beschrieben.

6.7.2 Versichertenstammdatenmanagement (VSDM)

Das Fachmodul VSDM wird als integraler Bestandteil des KoCoBox-Anwendungskonnektors als eine der dezentralen Komponenten der Telematikinfrastruktur betrieben. Es unterstützt die Anwendungsfälle der Fachanwendung VSDM, indem es dem Clientsystem (i.d.R. PVS/KIS) anwendungsspezifische Schnittstellen zum Auslesen der Versichertenstammdaten der elektronischen Gesundheitskarte anbietet.[107]

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.

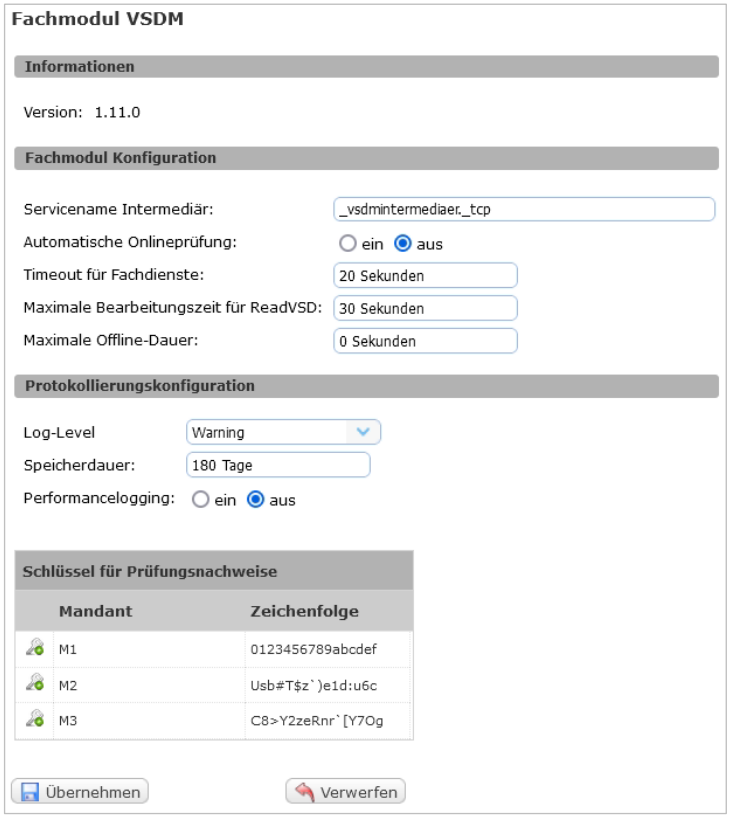


Abbildung 64: Konfigurationsbereich für das Fachmodul VSDM

Bei der Konfiguration des Fachmoduls VSDM gehen Sie wie folgt vor:

1 Tragen Sie in der ersten Zeile den *Servicenamen* des *Intermediär* ein.[108] Per Voreinstellung ist *_vsdmintermediaer._tcp* hinterlegt.

Schalten Sie per Radiobutton die *automatische Onlineprüfung* der VSD ein. Diese startet beim Stecken einer eGK. Per Voreinstellung ist die Onlineprüfung ausgeschaltet.[109]

[107] Vgl. [gemSpec_FM_VSDM], S. 10

[108] Der *Servicename Intermediär* setzt sich zusammen aus dem eigentlichen Servicenamen sowie dem zu verwendenden Protokolltyp. Dieser Punkt dient der Abfrage des Ressource Records beim DNS-Service Discovery.

[109] Diese Funktion ist nur im Standalone-Szenario verfügbar.

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.

Legen Sie anschließend die *Protokollierungskonfiguration* fest:

1 Dafür ist der *Log-Level* (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.

Geben Sie die *Speicherdauer* in Tagen ein, bevor das VSDM-Fachmodul-Protokoll gelöscht wird. Die Voreinstellung ist 180 Tage.

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 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 Operation *ReadVSD* gesetzt sein, anderenfalls kann diese nicht erfolgreich abgeschlossen werden.

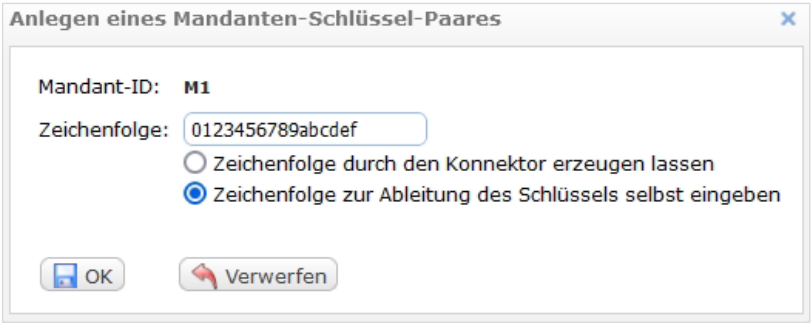


Abbildung 65: Konfigurationsfenster für das Anlegen eines Mandaten-Schlüssel-Paares

Wählen Sie aus, ob Sie die Zeichenfolge für die Ableitung des Schlüssels[110] 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 Bestätigen Sie die eingegebene Zeichenfolge mit OK.

4 Mit dem Button Übernehmen speichern Sie die Konfigurationen ab.

[110] 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.

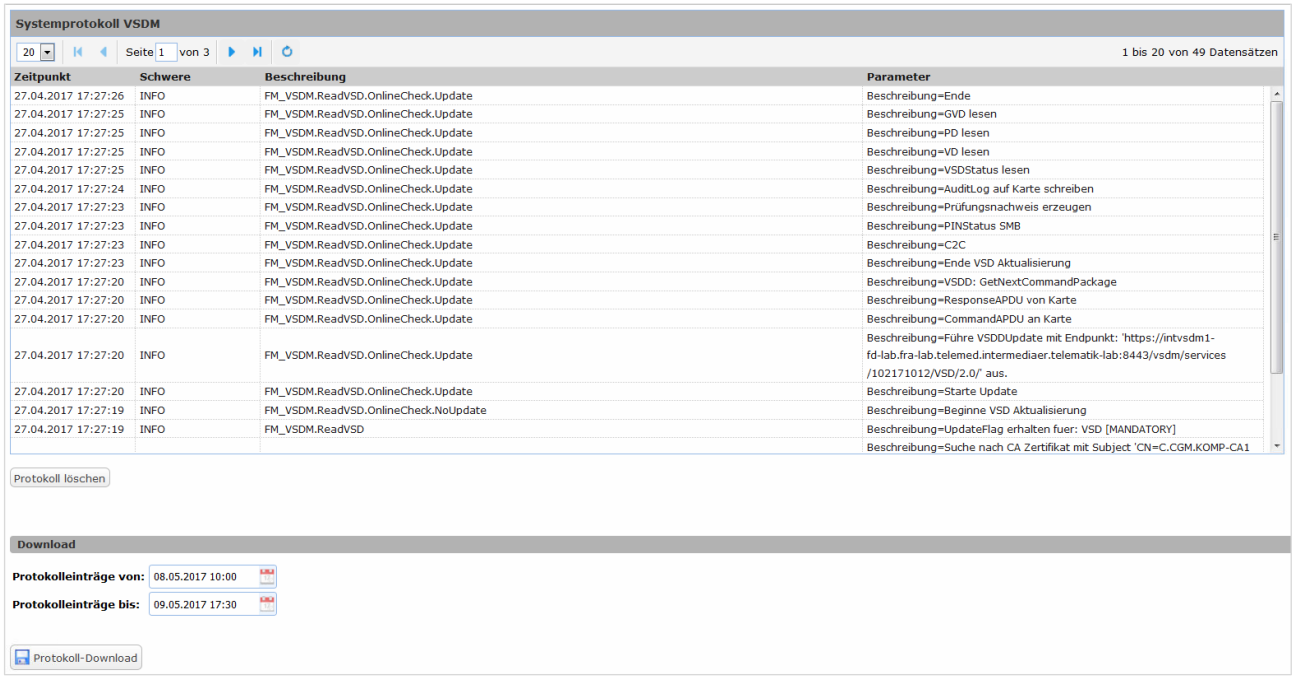


Abbildung 66: Exemplarische Ansicht zum Systemprotokoll VSDM mit Downloadfunktion

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 Moduls
Amount	Anzahl, wie oft die Meldung in diesem Logeintrag zusammengefasst ist[111]
Topic	Topic des protokollierten Ereignisses
protocolType	Protokollierungsart
protocolSeverity	Schweregrad des Protokollierungseintrages
Parameter	ereignisabhängige Parameter mit weiteren Details zum protokollierten Ereignis und Fehler

Tabelle 3: Aufbau der Logfiles im Fachmodul VSDM

[111] Gleiche Logeinträge werden nach bestimmten, komplexen Regeln zusammengefasst.

6.7.3 Notfalldaten-Management (NFDM)

Das Fachmodul Notfalldaten-Management (FM NFDM) ist ein integraler Bestandteil der KoCoBox 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.[112]

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.[113]

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 sekundengenauer Uhrzeit.

Im Unterbereich *Protokollierungskonfiguration* werden der *Log-Level*, die *Speicherdauer* sowie das *Performancelogging* konfiguriert.

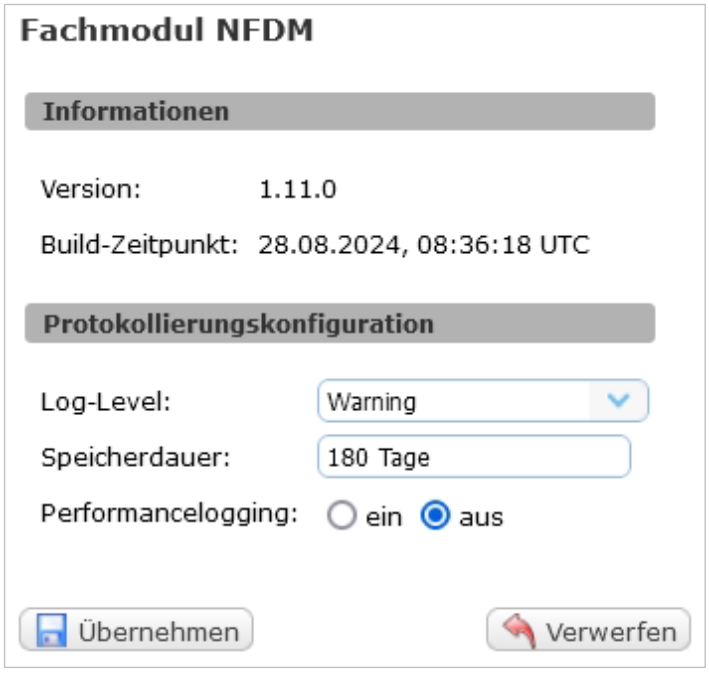


Abbildung 67: Konfigurationsbereich für das Fachmodul NFDM

[112] Vgl. [TR-03154], S.7

[113] Vgl. [gemSpec_FM_NFDM], S. 12

Legen Sie die *Protokollierungskonfiguration* wie folgt fest:

1 Zunächst ist der *Log-Level* (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*.

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.

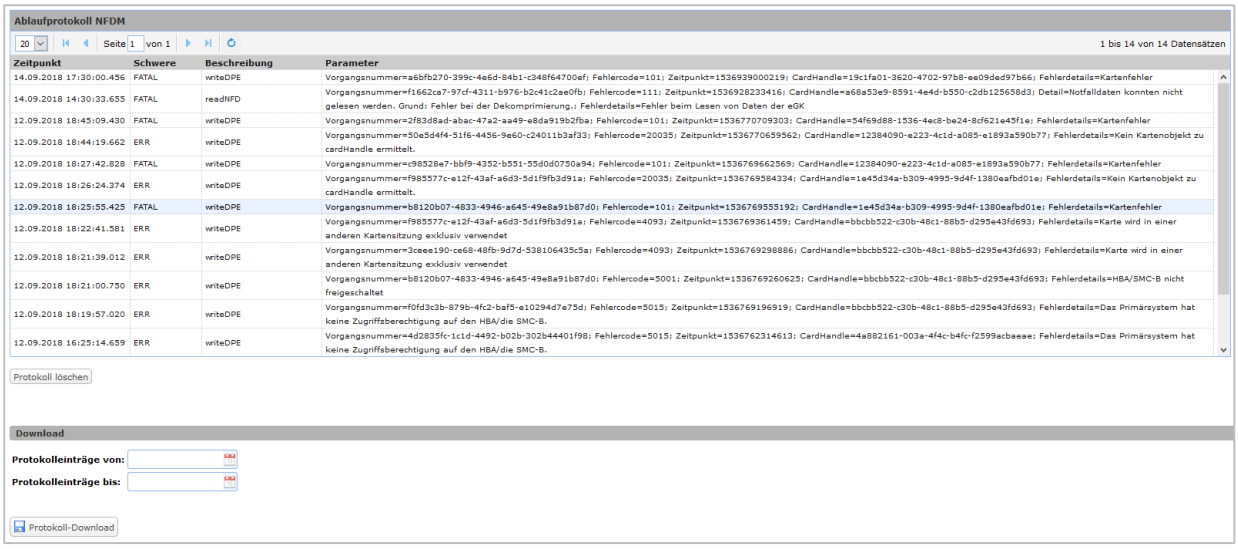


Abbildung 68: Exemplarische Ansicht zum Ablaufprotokoll NFDM mit Downloadfunktion

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 Moduls
Amount	Anzahl, wie oft die Meldung in diesem Logeintrag zusammengefasst ist[114]
Topic	Name der Operation
protocolType	Protokollierungsart
protocolSeverity	Schweregrad des Protokollierungseintrages
Parameter	Parameter mit weiteren Details zum protokollierten Ereignis und Fehler

Tabelle 4: Aufbau der Logfiles im Fachmodul NFDM

[114] Gleiche Logeinträge werden nach bestimmten, komplexen Regeln zusammengefasst.

6.7.4 Elektronische Patientenakte (ePA)

Das Fachmodul elektronische Patientenakte (FM ePA) ist ein integraler Bestandteil der KoCoBox. Es nutzt seine Basisdienste zur Umsetzung aller Anwendungsfälle der Fachanwendung ePA. Dem Konnektor stellt es 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 Praxis- bzw. Klinikumgebung 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.[115]

Die Verbindungen zum ePA-Aktensystem sind gesondert durch TLS sowie weiterhin durch spezielle Protokolle für den Datenaustausch mit den Schlüsselgenerierungsdiensten (SGD-Protokoll) und der Dokumentenverwaltung (VAU[116]-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 6.6.2) dargestellt.

Im Unterbereich *TLS-Verbindungsparameter* werden die TCP- und TLS-Verbindungsparameter für die Verbindungen der KoCoBox 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.

[115] vgl. [TR-03157] Kap. 1.1-1.2

[116] Abkürzung für **V**ertrauenswürdige **A**usführungs**u**mgebung

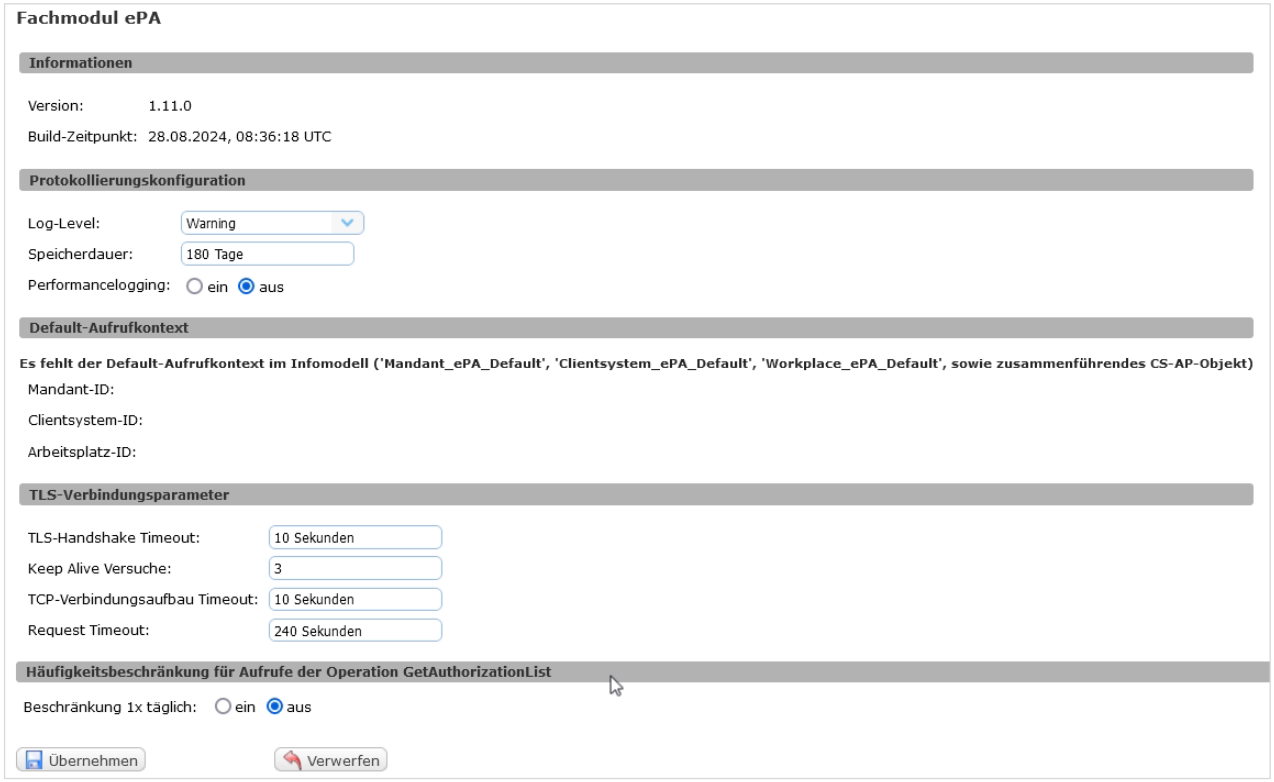


Abbildung 69: Konfigurationsbereich für das Fachmodul ePA

Unterbereich Protokollierungskonfiguration

1 Zunächst ist der *Log-Level* (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*.

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.

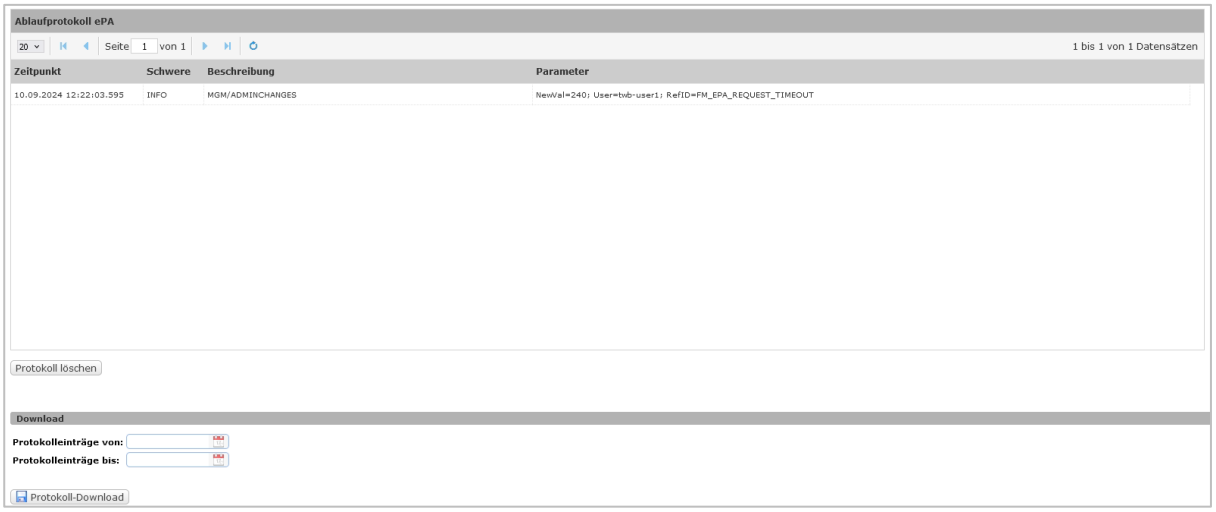


Abbildung 70: Exemplarische Ansicht zum Ablaufprotokoll ePA mit Downloadfunktion

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 Moduls
Amount	Anzahl, wie oft die Meldung in diesem Logeintrag zusammengefasst ist[117]
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 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.

[117] 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.[118]

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.

Unterbereich Häufigkeitsbeschränkung für Aufrufe der Operation GetAuthorizationList

Im Unterbereich *Häufigkeitsbeschränkung für Aufrufe der Operation GetAuthorization List* kann die Beschränkung per Radiobutton ein auf einmal täglich konfiguriert werden. Dies gilt pro Telematik-ID und Clientsystem-ID. Alternativ kann man diese Beschränkung ausschalten.

[118] Vgl. [gemSpec_FM_ePA] Kap. 6.1 „Allgemein“

6.7.5 Arzneimitteltherapiesicherheit (AMTS)

Das Fachmodul Arzneimitteltherapiesicherheit (FM AMTS) ist eine Softwarekomponente. Sie setzt den E-Medikationsplan (eMP) als integralen Bestandteil der KoCoBox 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.[119]

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.[120]

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 sekundengenauer Uhrzeit.

Im Unterbereich *Protokollierungskonfiguration* werden der *Log-Level*, die *Speicherdauer* sowie das *Performancelogging* konfiguriert.

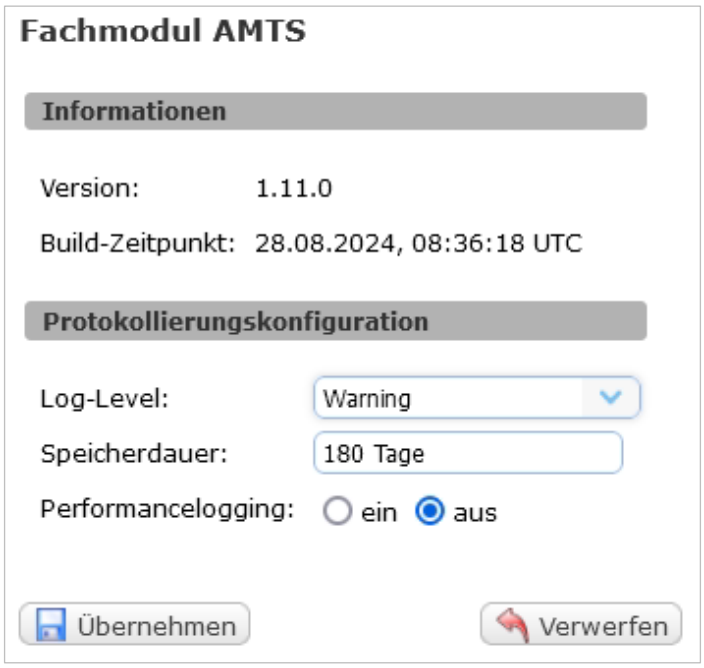


Abbildung 71: Konfigurationsbereich für das Fachmodul AMTS

[119] Vgl. [TR-03155], S. 6

[120] Vgl. [gemSpec_FM_AMTS], S.10

Legen Sie die *Protokollierungskonfiguration* wie folgt fest:

1 Zunächst ist der *Log-Level* (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*.

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 *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.

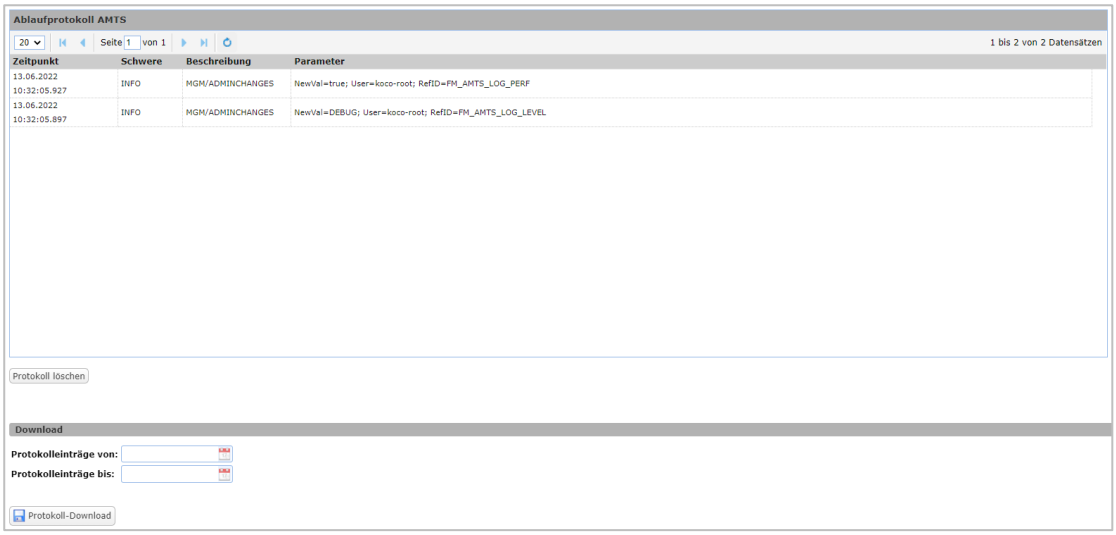


Abbildung 72: Exemplarische Ansicht zum Ablaufprotokoll AMTS mit Downloadfunktion

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 Moduls
Amount	Anzahl, wie oft die Meldung in diesem Logeintrag zusammengefasst ist[121]
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 AMTS

[121] Gleiche Logeinträge werden nach bestimmten, komplexen Regeln zusammengefasst.

7 Sicherheitsrelevante Szenarien

Im Folgenden finden Sie einen Überblick zu sicherheitsrelevanten Ereignissen in Zusammenhang mit dem Betrieb der KoCoBox.

7.1 Sicherheitskritische Fehlerzustände

In der Tabelle *Betriebszustandsmeldungen* auf der Status-Seite der Managementschnittstelle werden Fehlerzustände angezeigt.

Die Prüfung auf derartige Fehlerzustände erfolgt automatisch durch den Konnektor. Sie wird mit ihrem Ergebnis in den Protokolldaten vermerkt.[122]

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 identifizieren, folgen Sie umgehend den Handlungsanweisungen.

Zustandsmeldung auf Status-Seite	**Beschreibung**	**Handlungsanweisung**
EC_Random_Generator_Not _Reliable[123]	Der Zufallszahlengenerator kann die Anforderungen an die zu erzeugende Entropie nicht erfüllen.	Kontaktieren Sie umgehend Ihren Supportpartner.
EC_Secure_KeyStore_Not_Available	Der sichere Zertifikats- und Schlüsselspeicher des Konnektors (gSMC-K-Struktur oder Truststore) ist nicht verfügbar.	Starten Sie die KoCoBox neu. Ist dies nicht erfolgreich, kontaktieren Sie Ihren Supportpartner.
EC_Security_Log_Not_Writable	Das Sicherheitslog kann nicht geschrieben werden.	Starten Sie die KoCoBox neu. Ist dies nicht erfolgreich, kontaktieren Sie Ihren Supportpartner.
EC_Software_Integrity_Check_Failed	Eine oder mehrere konnektor-interne Integritätsprüfungen der aktiven Konnektorbestandteile sind fehlgeschlagen.	Starten Sie die KoCoBox neu. Ist dies nicht erfolgreich, kontaktieren Sie Ihren Supportpartner.

[122] Siehe dazu im Kapitel Inbetriebnahme / Konfiguration des Anwendungskonnektors den Abschnitt Protokollierungsdienst

[123] Diese Fehlerzustandsmeldung wird durch den Netzkonnektor nie ausgelöst.

Zustandsmeldung auf Status-Seite	Beschreibung	Handlungsanweisung
EC_TSL_Trust_Anchor_Out_Of_Date	Die Gültigkeit des Vertrauensankers ist abgelaufen.	Kontaktieren Sie Ihren Supportpartner.
EC_TSL_Out_Of_Date _Beyond_Grace_Period	Systemzeit t mit t>NextUpdate-Element der TSL + CERT_TSL_DEFAULT_GRACE_ PERIOD_DAYS und eine neue TSL ist nicht verfügbar	Spielen Sie über die Managementschnittstelle im Bereich *Zertifikatsdienst* die TSL manuell über den Button TSL importieren ein. Kontaktieren Sie zusätzlich Ihren Supportpartner, da dieses Problem mehrere Instanzen der KoCoBox HSK betreffen könnte.
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.[124] Beenden Sie den Fehlerzustand manuell über den Button EC_OTHER_ERROR_STATE zurücksetzen im Navigationsbereich *Verwaltung*. Der Konnektor nimmt automatisch einen Neustart vor. Alle Systemdienste des Konnektors werden neu initialisiert.
Operational State Error EC_OTHER_ERROR_STATE(2)	Herstellerspezifische Warnung	Der Protokollspeicher des Konnektors ist zu mehr als 80 Prozent belegt. Überprüfen Sie die Protokolle und informieren Sie bitte Ihren Supportpartner.

Folgen Sie den Anweisungen des Supportpartners, um die erforderlichen Sicherheitsanforderungen zu erfüllen.

[124] Siehe im Detail die ausführliche Fußnote oben im Abschnitt Verwaltung / Reset.

7.2 Außerbetriebnahme

Für den Fall, dass die KoCoBox HSK dauerhaft außer Betrieb genommen werden soll, muss sie einen Werksreset erfahren. Dies stellt den Datenschutz für die Rückgabe des Konnektors an den Betreiber sicher.

Gehen Sie dazu wie folgt vor:

1. Führen Sie einen Werksreset[125] (siehe Kapitel Konnektormanagement / Werksreset) durch.
2. Melden Sie anschließend Ihrem Supportpartner, dass der Konnektor außer Betrieb genommen wurde.

[125] Siehe oben im Abschnitt Konfiguration des Anwendungskonnektors / Verwaltung / Werksreset

8 Anhang

8.1 Herstellerspezifische Fehlermeldungen

Die folgende Tabelle gibt eine Übersicht sämtlicher herstellerspezifischer Fehlermeldungen.

Fehler-code	Schwe-regrad	Fehlertyp	Fehlermeldung	Kompo-nente	Auslösende Bedingung
20002	Error	Security	Erforderliche Rollen sind nicht im Zertifikat vorhanden	Konnektor	Eine notwendige Rolle zur Durchführ-ung einer Operation ist nicht im Zertifikat vorhanden.
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 ent-nommen werden sollen, stehen nicht bereit.
20009	Error	Technical	Das VersichertenDatenTemplate der KVK enthält ungültige Daten.	Konnektor	Die gesteckte KVK enthält nicht valide Versichertendaten.
20012	Error	Technical	Der Anzeigetext ist zu lang.	Konnektor	Der übergebene Dis-playText ist für das angesprochene Kar-tenterminal zu lang und muss kürzer sein. Hier ist eine Abstimmung mit dem Hersteller des Clientsystems erforderlich.
20014	Error	Technical	Der Kartentyp entspricht nicht der Vorbedingung der Operation ReadVSD.	Konnektor	Der Kartentyp ent-spricht nicht der Vor-bedingung der Operation ReadVSD.
20015	Error	Technical	Keine Response-APDU erhalten	Konnektor	Das durch den Kon-nektor gesendete Kommando an die Karte bzw. das Kar-tenterminal enthält keine Antwort.
20016	Error	Technical	Der Name der Gegenstelle kann nicht aufgelöst werden.	Konnektor	Die DNS-Adresse der Gegenstelle kann

Fehler-code	Schwe-regrad	Fehlertyp	Fehlermeldung	Kompo-nente	Auslösende Bedingung
					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.
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 <Karten-fehlercode 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 Operation ist überschritten.	Konnektor	Die Operation 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 unbekannte Information.	Konnektor	Die Zertifikatsprüfung schlägt bei der Prüfung von kritischen Zertifikats-erweiterungen fehl.
20029	Warning	Technical	MimeType des eingebetteten Dokuments kann nicht ermittelt	Konnektor	Falls bei einer CMS-Parallelsignatur der

Fehler-code	Schwe-regrad	Fehlertyp	Fehlermeldung	Kompo-nente	Auslösende Bedingung
			werden.		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 *Warning*.
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 Fehlertext 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 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.

Fehler-code	Schwe-regrad	Fehlertyp	Fehlermeldung	Kompo-nente	Auslösende Bedingung
20036	Error	Technical	Zugriff auf gSMC-K-Ressource des AK fehlgeschlagen.	Konnektor	Der Zugriff auf die gSMC-K-Struktur des Anwendungs-konnektors ist fehlgeschlagen.
20039	Error	Technical	Das Dokument enthält keine strukturell gültige CMS-Signatur.	Konnektor	Die im übergebenen Dokument enthal-tene CMS-Signatur ist strukturell ungeeig-net 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 unzuläs-sigen 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	OCSP-Informationen stehen nicht für die 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	Konnektor	Die XSD-

Fehler-code	Schwe-regrad	Fehlertyp	Fehlermeldung	Kompo-nente	Auslösende Bedingung
			Antwort des {0} ist fehlgeschlagen.		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}.
20056	Error	Security	Zertifikat enthält eine fehlerhafte Extension ({0})	Konnektor	Das Zertifikat enthält eine fehlerhafte Erweiterung ({0}).
20058	Error	Technical	Kein Schema für Signaturrichtlinie {0} im Konnektor hinterlegt	Konnektor	Es ist kein Schema für Signaturrichtlinie {0} im Konnektor hinterlegt.
20059	Warning	Security	Signerzertifikat konnte nicht eindeutig ermittelt werden.	Konnektor	Bei der Signaturprü-fung konnte unter den vorliegenden Zertifikaten kein eindeutiges Signerzertifikat 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-Adresskonfigu-ration an allen aktiven Netzwerk-adaptern.
20063	Error	Security	Signaturrichtlinie {0} nicht eingehalten.	Konnektor	Die im Dokument oder Request über-

Fehler-code	Schwe-regrad	Fehlertyp	Fehlermeldung	Kompo-nente	Auslösende Bedingung
					gebene Signatur-richtlinie wurde nicht vollständig einge-halten.
20064	Error	Technical	Keine Signaturrichtlinie zu URI {0} gefunden.	Konnektor	Die im Dokument oder Request über-gebene Signatur-richtlinie 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 Prü-fung der Signatur kann deswegen nicht durchgeführt werden.
20067	Error	Security	OCSP-Archive-Cutoff für geprüftes Zertifikat überschritten.	Konnektor	Ein OCSP-Responder hat für ein QES-Zer-tifikat angezeigt, dass er keine ver-lässlichen Statusin-formationen für die-ses 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 schwer-wiegenden Fehler bei der Signaturveri-fikation, i.d.R. bei unstimmigen Status-informationen zum Signaturzertifikat, wird die weitere Prü-fung gemäß Common-PKI abge-

Fehler-code	Schwe-regrad	Fehlertyp	Fehlermeldung	Kompo-nente	Auslösende Bedingung
					brochen. 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 Signatur hinterlegten MimeType {1} überein.	Konnektor	Der im Request übergebene MimeType {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 Formatierung, 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

Fehler-code	Schwe-regrad	Fehlertyp	Fehlermeldung	Kompo-nente	Auslösende Bedingung
					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.
20083	Error	Technical	Das ECC-Zertifikat kann nicht erzeugt werden, da kein ECC-fähiges Schlüsselmaterial auf der gSMC-K-Ressource vorhanden ist.	Konnektor	Für die Ausstellung von ECDSA-Zertifikaten ist eine gSMC-K-Struktur 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	Konnektor	Das End-Entity-Zertifikat wurde in

Fehler-code	Schwe-regrad	Fehlertyp	Fehlermeldung	Kompo-nente	Auslösende Bedingung
			falschen Algorithmus gehasht.		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, 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 Zertifikatsketten-prüfung 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.
20500	Info	Technical	Fehler in der Modulkonfiguration!	Konnektor	Eine Konfiguration ist fehlerhaft und wurde nicht übernommen.

Fehler-code	Schwe-regrad	Fehlertyp	Fehlermeldung	Kompo-nente	Auslösende Bedingung
20505	Error	Security	Fehler beim Prüfen des Admin-Flags	Konnektor	Das Admin-Flag konnte nicht erfolgreich geprüft werden.
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 Parame-ter 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.
20803	Error	Technical	Fehler beim Ausführen des Ping-Skriptes	Konnektor	Das Ausführen des Skripts, das die Netz-werkverbindung zu einem System prüft, wurde mit einem Fehler abgebrochen.
20807	Error	Technical	Fehler beim Validieren der FQDN	Konnektor	Die für den Erreich-barkeitstest angege-bene FQDN konnte

Fehler-code	Schwe-regrad	Fehlertyp	Fehlermeldung	Kompo-nente	Auslösende Bedingung
					nicht als gültig validiert werden.

8.2 Betriebszustandsmeldungen

Im Folgenden werden die Betriebszustandsmeldungen des Konnektors sowie die Handlungsanweisungen zu deren Behebung in einer Übersicht dargestellt.

Zustandsmeldungen auf Status-Seite	Beschreibung	Schwe-regrad	Handlungsanweisung
Operational State Error EC_CardTerminal_Soft-ware_Out_Of_Date ($ctId)	Software auf Kartenterminal ($ctId) ist nicht aktuell.	Info	Die Firmware der 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_Time_Sync_Not_Successful	Der letzte Synchronisations-versuch der Systemzeit war nicht erfolgreich.	Info	Der letzte Synchronisations-versuch der Systemzeit war nicht erfolgreich. Sollte sich der Konnektor über einen längeren Zeitraum in diesem Zustand befinden, informieren Sie bitte Ihren Supportpartner.
EC_TLS_Client_Certificate_Secu-rity	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.
EC_TSL_Expiring	Systemzeit t mit t > NextUpdate-Element der TSL – 7 Tage und t <= 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[126]) 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 Systemprotokolle gelöscht werden.
EC_Time_Sync_Pending_ Warning	Keine erfolgreiche Synchronisation der Systemzeit seit d Tagen und d > NTP_WARN_PERIOD und	Warnung	Die Verbindung zum Zeitdienst der TI ist gestört. Kontaktieren Sie Ihren Supportpartner.

[126] Siehe dazu den Abschnitt Benutzerverwaltung

Zustandsmeldungen auf Status-Seite	Beschreibung	Schwe-regrad	Handlungsanweisung
	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.		
EC_TSL_Out_Of_Date _Within_Grace_Period	Systemzeit t mit t > NextUpdate-Element der TSL und t <= NextUpdate-Element der TSL + CERT_TSL_DEFAULT_GRACE_PERIOD_DAYS und eine neue TSL ist nicht verfügbar	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 ($ctId)	Bekanntes Karten-terminal($ctId) ist nicht verfügbar.	Fehler	Überprüfen Sie das Kartenterminal.
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 Supportpartner.
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 Supportpartner.
Operational State Error EC_OTHER_ERROR_STATE(3)	SMC-B-Verifikation gescheitert	Warnung	Die PIN-Eingabe zur initialen SMC-B-Verifikation ist gescheitert. Prüfen Sie die PIN-Daten und informieren Sie ggf. Ihren Supportpartner.
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 Supportpartner.
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 Supportpartner.
EC_CRYPTOPERATION_ALARM	Gemäß TIP1-A_4597 wurde ein	Warnung	Es gibt eine auffällige Häufung

Zustandsmeldungen auf Status-Seite	Beschreibung	Schwe-regrad	Handlungsanweisung
	potenzieller Missbrauch einer Kryptooperation erkannt. Nur der Administrator kann die Alarmmeldung zurücksetzen.		von Aufrufen (der Alarmwert ist überschritten). Informieren Sie bitte Ihren Supportpartner.

8.3 Sicherheitsrelevante Fehlermeldungen der Fachmodule

Die folgende Tabelle gibt eine Übersicht fachmodulspezifischer sicherheitsrelevanter Fehlermeldungen.

Fehler-code	Schwe-regrad	Fehler-typ	Fehlermeldung	Kompo-nente	Auslösende Bedingung
101	Fatal	Security	Kartenfehler	Fach-module NFDM, ePA	Karte defekt, Austausch nötig
106	Fatal	Security	Zertifikat auf eGK ungültig	Fach-modul NFDM, ePA	Karte ungültig, Austausch nötig
107	Fatal	Security	Zertifikat auf eGK ungültig	Fachmodul NFDM	Karte ungültig, Austausch nötig
5002	Error	Security	Fachliche Rolle nicht berechtigt zur Ausführung	Fachmodul NFDM	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 NFDM	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 NFDM	Wahrscheinlich ein Lesefehler der eGK, Austausch nötig
5014	Error	Security	Das Primärsystem hat keine Zugriffsberechtigung auf die eGK.	Fachmodul NFDM	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 NFDM	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 NFDM	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 NFDM	Der Datensatz auf der eGK ist defekt, er ist neu anzulegen, ggf. ist ein Austausch der eGK nötig.

Fehler-code	Schwe-regrad	Fehler-typ	Fehlermeldung	Kompo-nente	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 anzu-legen, 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 wieder-holtem 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 anzu-legen, 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 ge-wechselt werden. Evtl. ist das Infomo-dell zu prüfen.

Fehler-code	Schwe-regrad	Fehler-typ	Fehlermeldung	Kompo-nente	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 Doku-mentenverwaltung 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 Verbin-dung 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 Kontext-schlüssels 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.

8.4 Ergänzende technische Informationen

In diesem Abschnitt finden Sie weitere Informationen zu technischen Details.

8.4.1 Startverhalten

Die KoCoBox HSK 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 des Konnektors beinhaltet, z.B. wenn die Protokollspeicher gefüllt sind und die ältesten Protokolleinträge rollierend gelöscht werden. Während dieser Zeit ist die Managementschnittstelle inaktiv. Zudem reagiert die KoCoBox nicht auf manuelle Eingaben.

Warten Sie das Ende des Vorgangs ab.

8.4.2 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.[127]

[127] Diese Versionsangabe muss nicht immer vorhanden sein.

8.4.3 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: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>
```

8.4.4 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>-->
<!-- 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>
	<!-- 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>
```

xmldsig_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/xmldsig#"
   >
   <!ENTITY dsig 'http://www.w3.org/2000/09/xmldsig#'>
   <!ENTITY % p ''>
   <!ENTITY % s ''>
]>
<!-- Schema for XML Signatures
   http://www.w3.org/2000/09/xmldsig#
   $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/xmldsig#"
        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:SPKIData"/>
        <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:KeyValueType"/>
<complexType name="KeyValueType" mixed="true">
    <choice>
        <element ref="ds:DSAKeyValue"/>
        <element ref="ds:RSAKeyValue"/>
        <any namespace="##other" processContents="lax"/>
    </choice>
</complexType>
<element name="RetrievalMethod" type="ds:RetrievalMethodType"/>
<complexType name="RetrievalMethodType">
    <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 PGPData -->
<!-- Schemahärtung -->
<!--<element name="PGPData" type="ds:PGPDataType"/>
<complexType name="PGPDataType">
  <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 PGPData -->
<!-- Begin SPKIData -->
<!-- Schemahärtung -->
<!--<element name="SPKIData" type="ds:SPKIDataType"/>
<complexType name="SPKIDataType">
  <sequence maxOccurs="unbounded">
    <element name="SPKISexp" type="base64Binary"/>
    <any namespace="##other" processContents="lax" minOccurs="0"/>
  </sequence>
</complexType>-->
<!-- End SPKIData -->
<!-- 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>
```

8.5 Anforderungen an Clientsysteme

8.5.1 TLS-Verbindungen zum Konnektor

1. Die Spezifikation der gematik sieht die Unterstützung von TLS v1.2 mit TLS-Cipher-Suites vor, deren Nutzdatenverschlüsselung auf AES-GCM und AES-CBC basiert. Der Einsatz von AES-CBC ist auf Grund fehlender AEAD[128] aus aktueller Sicht nicht mehr dem Schutzbedarf der Netzwerkverbindungen angemessen. Die Nutzung von TLS-Cipher-Suites mit AES-GCM ist umzusetzen; die Verwendung von AES-CBC ist für jegliche Verbindungen mit Konnektoren **zu vermeiden**.
2. Für Verbindungen zur Nutzung von SOAP- und LDAP-Diensten gilt: Das Clientsystem muss dem Benutzer den Verbindungsstatus anzeigen. Es muss klar erkennbar sein, wenn eine Verbindung unsicher ist. Hinweis: Die Anzeige könnte ähnlich wie in aktuellen Web-Browsern realisiert werden. Wenn in der Software keine sichere Verbindung implementiert ist, muss das im Handbuch des Clientsystems erklärt werden. Die Verbindung darf nur als sicher angezeigt werden, wenn folgende Bedingungen gleichzeitig erfüllt sind:
   - TLS-Verbindung wurde aufgebaut,
   - Konnektoridentität wurde erfolgreich geprüft (TLS-Server-Authentication).
3. Das Clientsystem muss den Konnektor bei einer TLS-Verbindung für CETP authentifizieren. Wenn die Zertifikatsprüfung fehlschlägt, muss die Verbindung beendet werden.
4. Für Verbindungen zur Nutzung von CETP gilt: Wenn ein Clientsystem CETP-Nachrichten abonniert, muss angezeigt werden, ob diese authentisch, integer und vertraulich empfangen werden. Die Anzeige kann analog wie in für die SOAP-Anbindung beschrieben erfolgen. Die Verbindung darf nur als sicher angezeigt werden, wenn folgende Bedingungen gleichzeitig erfüllt sind:
   - TLS-Verbindung wurde aufgebaut,
   - Konnektoridentität wurde erfolgreich geprüft (TLS-Client-Authentication)
5. Bezüglich der Konnektorspezifikation [gemSpec_Kon, TAB_KON_852] gelten nur SOAP1, DVD2, CETP1 und LDAP1 als sicher, und zwar ausschließlich mit **zusätzlicher Prüfung** des Konnektorzertifikats
   - bei SOAP (Konnektor = TLS-Server) und
   - bei DVD (Konnektor = TLS-Server) und
   - bei CETP (Konnektor = TLS-Client) sowie
   - bei LDAP (Konnektor = TLS-Server).

8.5.2 Verwendung von Signaturfunktionalität

1. Das Clientsystem muss dem Benutzer bei einem Signaturvorgang die Jobnummer anzeigen.
2. Im Benutzerhandbuch des Clientsystems muss der Benutzer dazu angehalten werden, zu prüfen, ob die Jobnummern in der Kartenterminalanzeige und im Clientsystem identisch sind. Bei einer Abweichung muss vor einem Angriff gewarnt werden, und eine PIN darf nicht eingegeben werden. Stattdessen müssen weitergehende Schritte zur Klärung des aufgetretenen Fehlverhaltens eingeleitet werden.
3. Bei Stapelsignaturen muss das Clientsystem den Signaturfortschritt basierend auf CETP-Events der zugehörigen KoCoBox anzeigen.
4. Bei Fehlern im Ablauf der Stapelsignaturerstellung, sofern diese nicht direkt durch eine Nutzeraktion

[128] Authenticated Encryption with Associated Data

verursacht wurden, muss der Benutzer gewarnt werden, dass eine Fehlfunktion bzw. ein Angriff vorliegt, vgl. [gemSpec_Kon, TAB_KON_192].

5. Der Verification Report muss immer durch das Clientsystem bereitgestellt werden können, und zwar vollständig/ausführlich.
6. Der Benutzer muss prüfen können, wer der Schlüsselinhaber des signierenden Zertifikats (Signaturinhaber) ist.
7. Aus der Verwendung von XAdES-Dokumenten sind diverse Angriffe bekannt. Neben anderen existiert, gerade in heterogenen Prozesslandschaften mit unterschiedlichen technischen Umsetzungen der XML/SAML-Funktionalitäten, eine Gruppe von Schwachstellen, die sich aus der Verwendung der Kommentarfunktionen ergibt, siehe

   https://duo.com/blog/duo-finds-saml-vulnerabilities-affecting-multiple-implementations

   Für zuverlässige Aussagen zur Signatur und zur Vermeidung des Einschleusens unerwünschter oder unzulässiger Dokumenteninhalte via XML-Kommentar ist unbedingt durchgängig die XML-Kanonisierungsmethode XML-C14N **ohne** Kommentare (wie über die gematik-Spezifikation bereits referenziert) zu nutzen, siehe

   http://www.w3.org/TR/xml-c14n

   Nur dann kann sich die verarbeitende Logik auf die Signaturaussage verlassen.
8. Die KoCoBox signiert und verifiziert PDF-Dokumente nach dem PAdES-Standard. Der Konnektor führt dabei eine robuste Analyse von PDF-Dokumenten durch. Das Ziel der Funktionalität ist, eine möglichst große Spanne von PDF-Dokumenten verarbeiten zu können.

   Der Konnektor ist nicht geeignet, Aussagen über die Standardkonformität von PDF-Dokumenten zu treffen; er ist kein PDF-Validierer.

   Das Clientsystem ist dafür verantwortlich, die übergebenen PDF-Dokumente auf Ihre Konformität zum PDF-Standard zu prüfen. Insbesondere MUSS das Clientsystem sicherstellen, dass die PDF-Start- und PDF-Endemarkierungen an den korrekten Positionen im Dokument stehen:

   - Die PDF-Startmarkierung „%PDF-1." muss an Position 0 der ersten Zeile des Dokuments stehen.
   - Die PDF-Endemarkierung „%%EOF" muss an Position 0 der letzten Zeile des Dokuments stehen. Die letzte Zeile soll nicht mehr als die PDF-Endemarkierung enthalten. Ein abschließender Zeilenumbruch wird toleriert.

   Wenn der Benutzer Dokumente in den Prozess einbringt, die diesen Vorgaben nicht entsprechen, MUSS das Clientsystem den Benutzer warnen. Der Hersteller empfiehlt, dass das Clientsystem selbst solche Dokumente ablehnt und dem Konnektor nicht zur Signatur oder Signaturverifikation vorlegt.

   Der Hersteller empfiehlt weiterhin, dass das Clientsystem das vom Konnektor signierte Dokument dem Benutzer anzeigt.
9. Wenn das Clientsystem die Operation ExternalAuthenticate verwendet, d.h. über die Dienstschnittstelle der KoCoBox aufruft, ist durch die Implementierung des Clientsystems sicherzustellen, dass diese Konnektoroperation **ausschließlich** zu Authentisierungszwecken unter Verwendung der Authentisierungsschlüssel des HBAx und des SM-B (SMC-B) verwendet wird.

10. Für die Verwendung der Komfortsignaturfunktionalität muss das zum Einsatz kommende Clientsystem pro Aktivierung der Komfortsignaturfunktion eine eindeutige UserID im Format UUID gemäß RFC4122 generieren. Hierzu muss durch das Clientsystem mithilfe eines qualitativ guten Zufallszahlengenerators (siehe z.B. AIS20/31 oder NIST SP800-90A/B/C) benötigter Zufall in einer Menge von 128 bits erzeugt, bereitgestellt und verwendet werden. Dieser Zufall muss damit praktisch unvorhersagbar sein (oder nur erratbar mit einer Wahrscheinlichkeit von 2^{-128}).
11. Jede UserID zur Verwendung der Komfortsignaturfunktionalität muss im Clientsystem eindeutig einem Benutzer (User) zugeordnet sein. Sie ist weiterhin durch das Clientsystem sowie den zugeordneten Benutzer vertraulich zu behandeln. Auf die Notwendigkeit der vertraulichen Behandlung der UserID ist in der Dokumentation des Clientsystems hinzuweisen.

8.6 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 HSK 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 HSK.

Die aktuelle Version dieser Datenschutzerklärung finden Sie auf der Administrationsoberfläche der KoCoBox HSK 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 HSK

KoCoBox HSK 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 bestimmbaren 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 HSK

- **Stammdaten der Administratoren**
- **Daten von eGK und HBA**
  - **Kartennummer (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 HSK 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 HSK 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 HSK beschrieben.

4.3 Verarbeitung von Praxisdaten und besonderen Arten personenbezogener Daten | Patientendaten in integrierten Modulen

Es werden keine integrierten Module zusammen mit der KoCoBox HSK standardmäßig installiert.

5. Datenübermittlung

Die KoCoBox HSK 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 Auskunftsersuchen 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.

8.7 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 so lange, 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 HSK]"
   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 gewonnen Informationen und der bearbeiteten Software ist hingegen nicht gestattet.
4. 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.”
5. Die damit verbundenen Lizenzinformationen finden Sie in der Managementschnittstelle im Bereich *Verwaltung* unter dem Button Lizenzbestimmungen anzeigen.

8.8 Tabellenverzeichnis

8.9 Stichwortverzeichnis

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

8.10 Glossar

Das folgende Glossar wurde in weiten Teilen in enger Anlehnung an das zentrale Projekt-Glossar der gematik[129] 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)
Administrator		Administrator des Konnektors 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.[130]
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.
andere Anwendungen des Gesundheitswesens ohne Zugriff	aAdG-NetG	Die Anwendungskategorie „andere Anwendungen des Gesundheitswesens ohne Zugriff auf Dienste der

[129] Vgl. [gemGlossar]

[130] Vgl. [gemGlossar], S. 7 sowie alle folgenden

Begriff	Synonym / Abkürzung	Erläuterung / Definition
auf Dienste der TI in angeschlossenen Netzen des Gesundheitswesens		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 (Rechteverwaltung). Im Kontext Gesundheitskarte wird der Begriff insbesondere im Sinne von § 291a, Abs. 5 SGB

Begriff	Synonym / Abkürzung	Erläuterung / Definition
		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 des Konnektors 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, sofern sie nicht durch gesetzlichen Auftrag zur Bereitstellung eines Dienstes verpflichtet sind.

Begriff	Synonym / Abkürzung	Erläuterung / Definition
Betriebsführungsbuch	BfB	Im BfB des Konnektors 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		Sie umfasst 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 Die externe Authentisierung mit Ausnahme von e verändert den Authentisierungsstatus der prüfenden Chipkarte.
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 Telematikinfrastruktur, andererseits aber auch Funktionen der Basisdienste des Konnektors als so genannte Basisanwendungen aufrufen. Die cetp-Schnittstelle ist ebenfalls Bestandteil der Clientsystem-Schnittstelle.

Begriff	Synonym / Abkürzung	Erläuterung / Definition
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.
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 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

Begriff	Synonym / Abkürzung	Erläuterung / Definition
		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 **ID**entification, **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).
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

Begriff	Synonym / Abkürzung	Erläuterung / Definition
		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 orientieren sich an der Nutzungsrichtlinie.
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	FW	Betriebssoftware eines Gerätes. Bei der KoCoBox HSK wird diese durch den bereitstellenden HSK definiert.
Fortgeschrittene elektronische Signatur		Sie erfüllt folgende Anforderungen: 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 unser 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

Begriff	Synonym / Abkürzung	Erläuterung / Definition
		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.
Highspeed-Konnektor	HSK	Der HSK ist eine hochperformante und skalierbare Variante des Konnektors für den Betrieb im Rechenzentrum. Er stellt Konnektoren als einzelne Instanzen zur Verfügung.
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-Protokoll 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

Begriff	Synonym / Abkürzung	Erläuterung / Definition
		(IIN) mit dem Branchen-hauptschlüssel, dem Länderkennzeichen 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 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. Beim Konnektor 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 Anwendungs-fälle der Fachanwendung VSDM, indem er

Begriff	Synonym / Abkürzung	Erläuterung / Definition
		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 ausgerichtetes 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

Begriff	Synonym / Abkürzung	Erläuterung / Definition
		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.
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 Netz-

Begriff	Synonym / Abkürzung	Erläuterung / Definition
		werkebene 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 deamon) 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.
Online-Prüfung der VSD		Gemäß § 291 SGB V gesetzlich vorgegebene Prüfung auf Gültigkeit und Aktualität der Versichertenstammdaten (VSD), beinhaltet folgende Schritte: - 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.
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

Begriff	Synonym / Abkürzung	Erläuterung / Definition
		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	Die Rechteverwaltung ist die konzeptionelle und

Begriff	Synonym / Abkürzung	Erläuterung / Definition
	Management	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. Beim Konnektor 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 beigestellt ist, und ein SGD 2 außer-halb 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 gegen-über anderen Komponenten der TI. Die Security Module Card Typ B ist ein Produkttyp.

Begriff	Synonym / Abkürzung	Erläuterung / Definition
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 Grenzrisiko 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

Begriff	Synonym / Abkürzung	Erläuterung / Definition
		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.
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.
Telematik		Telematik ist zusammengesetzt aus den Begriffen Telekommunikation und Informatik. Er beschreibt die Zusammenführung, Verarbeitung und Wei-

Begriff	Synonym / Abkürzung	Erläuterung / Definition
		tergabe 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 organisationsübergreifenden 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 Transportschichtsicherheit; 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

Begriff	Synonym / Abkürzung	Erläuterung / Definition
		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.
Versichertenstammdaten-management	VSDM	VSDM ist eine Fachanwendung der TI und realisiert 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 Gewähr-

Begriff	Synonym / Abkürzung	Erläuterung / Definition
		leistung von Datenschutz- und Informations-sicherheitseigenschaften. Dazu gehören z.B. - 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
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.

Begriff	Synonym / Abkürzung	Erläuterung / Definition
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.

8.11 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
CT-ID	Kartenterminal-ID
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System, Domain Name Service
DPE	Datensatz persönliche Erklärungen
DVD	Dienstverzeichnisdienst
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
HSK	**H**igh**s**peed-**K**onnektor
HSM-B	HSM-Variante einer Institutionskarte vom Typ B (Secure Module Card).

Abkürzung	Langform
	Das SM-B wird als virtuelle Karte verstanden, die in einem virtuellen Kartenterminal steckt.
http	Hypertext Transfer Protocol
https	Hypertext Transfer Protocol Secure
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	Lightweight Directory Access Protocol
LE	Leistungserbringer
MAC	Message Authentication Code
MB	Mega Byte (1024 x 1024 Bytes)
MTU	Maximum Transmission Unit
NFDM	Notfalldaten-Management
NTP	Network Time Protocol
OTP	One-Time-Passwort
PAP	Password Authentication Protocol
PAT	Port Address 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

Abkürzung	Langform
RFC	Request for Comments
SAK	Signaturanwendungskomponente
SER	Seriennummer
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
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	Telematikinfrastruktur
TLS	Transport Layer Security
TSL	Trust-service Status List
TSP	Trust Service Provider
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VAU	Vertrauenswürdige Ausführungsumgebung
VDG	Vertrauensdienstegesetz
VO	Verordnung
VSD	Versichertenstammdaten
VSDM	Versichertenstammdatenmanagement
VZD	Verzeichnisdienst
WA	Weitere Anwendungen
WAN	Wide Area Network
XAdES	XML Advanced Electronic Signature: ETSI-Standard zur Signatur von XML-Dokumenten
XML	Extensible Markup Language

Abkürzung	Langform
ZGDP	Zugangsdienstprovider
ZIS	Zugangs- und Integrationsschicht

8.12 Abbildungsverzeichnis

8.13 Referenzen

ID	Bezeichnung
[CAdES]	European Telecommunications Standards Institute. Electronic Si- gnatures 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/fileadmin/Fachportal/Glossar/gemGlossar_V5.2.0.pdf
[gemILF_PS]	gematik, Implementierungsleitfaden Primärsysteme – Telematikinfrastruktur (TI) (einschließlich VSDM, QES-Basisdienste, KOM-LE), gemILF_PS_V2.22.0.pdf, 23.02.2024, https://gemspec.gematik.de/docs/gemILF/gemILF_PS/gemILF_PS_V2.22.0/
[gemILF_PS_AMTS]	gematik, Implementierungsleitfaden Primärsysteme – elektronischer Medikationsplan/AMTS-Datenmanagement (Stufe A), gemILF_PS_AMTS_1.7.0.pdf, 12.11.2020, https://gemspec.gematik.de/docs/gemILF/gemILF_PS_AMTS/gemILF_PS_AMTS_V1.7.0/
[gemILF_PS_ePA]	Implementierungsleitfaden Primärsysteme - Elektronische Patientenakte (ePA) (ePA-Stufe 2.5), gemILF_PS_ePA_V2.52.0.pdf, 31.03.2023, https://gemspec.gematik.de/docs/gemILF/gemILF_PS_ePA/gemILF_PS_ePA_V2.52.0/
[gemILF_PS_NFDM]	gematik, Implementierungsleitfaden Primärsysteme – Notfalldaten-Management (NFDM), gemILF_PS_NFDM_1.5.0.pdf, 26.08.2022, https://gemspec.gematik.de/docs/gemILF/gemILF_PS_NFDM/gemILF_PS_NFDM_V1.5.0/
[gemRL_QES_NFDM]	gematik, Signaturrichtlinie QES Notfalldaten-Management (NFDM), gemRL_QES_NFDM_V1.4.1.pdf, 02.03.2020, https://gemspec.gematik.de/docs/gemRL/gemRL_QES_NFDM/gemRL_QES_NFDM_V1.4.1/
[gemSpec_FM_AMTS]	gematik, Elektronische Gesundheitskarte und Telematikinfrastruktur, Spezifikation Fachmodul AMTS, gemSpec_FM_AMTS_V1.4.0.pdf, 15.05.2019, https://gemspec.gematik.de/docs/gemSpec/gemSpec_FM_AMTS/gemSpec_FM_AMTS_V1.4.0/

[gemSpec_FM_ePA]	gematik, Elektronische Gesundheitskarte und Telematikinfrastruktur, Spezifikation Fachmodul ePA, gemSpec_FM_ePA_V1.53.0.pdf, 03.04.2023, https://gemspec.gematik.de/docs/gemSpec/gemSpec_FM_ePA/gemSpec_FM_ePA_V1.53.0/
[gemSpec_FM_NFDM]	gematik, Elektronische Gesundheitskarte und Telematikinfrastruktur, Spezifikation Fachmodul NFDM, gemSpec_FM_NFDM_V1.6.2.pdf, 30.06.2021, https://gemspec.gematik.de/docs/gemSpec/gemSpec_FM_NFDM/gemSpec_FM_NFDM_V1.6.2/
[gemSpec_FM_VSDM]	gematik, Einführung der Gesundheitskarte, Spezifikation Fachmodul VSDM, gemSpec_FM_VSDM_V2.8.0.pdf, 10.07.2023, https://gemspec.gematik.de/docs/gemSpec/gemSpec_FM_VSDM/gemSpec_FM_VSDM_V2.8.0/
[gemSpec_Karten_Fach_TIP]	gematik, Einführung der Gesundheitskarte, Befüllvorschriften für die Plattformanteile der Karten der TI, gemSpec_Karten_Fach_TIP_G2.1_3.1.0.pdf, 07.07.2023, https://gemspec.gematik.de/docs/gemSpec/gemSpec_Karten_Fach_TIP_G2_1/gemSpec_Karten_Fach_TIP_G2_1_V3.1.0/
[gemSpec_KT]	gematik, Elektronische Gesundheitskarte und Telematikinfrastruktur, Spezifikation eHealth-Kartenterminal, gemSpec_KT_V3.17.pdf, 12.02.2024, https://gemspec.gematik.de/docs/gemSpec/gemSpec_KT/gemSpec_KT_V3.17.0/
[gemSpec_Kon]	gematik, Elektronische Gesundheitskarte und Telematikinfrastruktur, Spezifikation Konnektor, gemSpec_Kon_V5.22.0.pdf, 13.06.2024, https://gemspec.gematik.de/docs/gemSpec/gemSpec_Kon/gemSpec_Kon_V5.22.0/
[gemSpec_PKI]	gematik, Elektronische Gesundheitskarte und Telematikinfrastruktur, Übergreifende Spezifikation PKI, gemSpec_PKI_V2.18.0.pdf, 17.05.2024, https://gemspec.gematik.de/docs/gemSpec/gemSpec_PKI/gemSpec_PKI_V2.18.0/
[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 Sgnatures 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