Release Notes: KoCoBox MED+

KoCoBox MED+ Firmware:	5.5.16
Gültig für Hardwareversion:	2.0.0 und 4.0.0
Produkttypsteckbrief Konnektor:	5.54.1-0 (PTV5+ mit LZV & ePA 2.5)
Stand:	28.05.2025

1 Einleitung

Die KoCoBox MED+ Konnektor Version 5.5.16 ist die Produktversion gemäß PTV5+. Sie basiert auf der Produkttypsteckbriefversion 5.54.1-0.

Damit sind gegenüber der Konnektorversion 5.1.8:2.0.0 bzw. 5.1.10:4.0.0 weitere Funktionen gemäß des Produkttypsteckbriefes *gemProdT_Kon_PTV5Plus_5.54.1-0_V1.0.0.pdf* hinzugekommen.

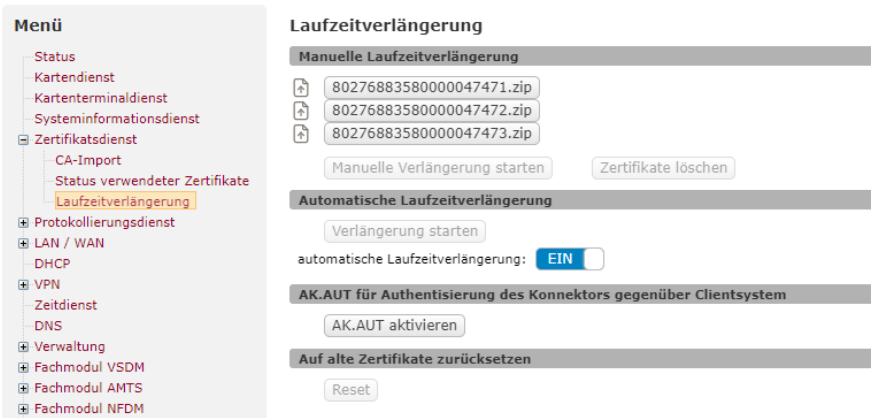
Bei der Firmware 5.5.16 handelt es sich um eine Weiterentwicklung der Vorgängerversion 5.5.12. Die Änderungen hierzu werden im Kapitel 3 beschrieben.

2 Neue Funktionen

Laufzeitverlängerung gSMC-K

Der Konnektor unterstützt die Laufzeitverlängerung (automatisch und manuell). 180 Tage vor Ablauf der Konnektorzertifikate geht dieser in den Betriebszustand *EC_NK_Certificate_Expiring*, welcher auf dem Display und der Managementoberfläche angezeigt wird und auch als Event an das Primärsystem übergeben wird. In diesem Zustand lädt der Konnektor **automatisch**, sofern vorhanden, die neuen Zertifikate (RSA & ECC) vom Downloadpunkt in der TI herunter und verwendet diese nach erfolgreicher Prüfung. Abschließend führt der Konnektor mit den neuen Zertifikaten eine Re-Registrierung am VPN-Zugangsdienst durch. Das neue C.AK.AUT zur Authentisierung des Konnektors gegenüber Clientsystem muss manuell aktiviert werden.
Die Laufzeitverlängerung kann jederzeit **manuell** via Download der Zertifikate aus der TI oder durch lokalen Upload (z.B. nach Ablauf der Gerätezertifikate) ausgeführt werden.
Im Fehlerfall kann die Laufzeitverlängerung zurückgesetzt und die automatische Verlängerung deaktiviert werden.

Aktuell liegen auf dem Downloadpunkt neue Zertifikate für Konnektoren bis einschließlich Seriennummer 80276003640001038O2 mit einer Zertifikatslaufzeit bis zum 31.12.2025.



ePA 2.5 - Anbindung *Digitaler Gesundheitsanwendungen (DiGA)* an die elektronische Patientenakte

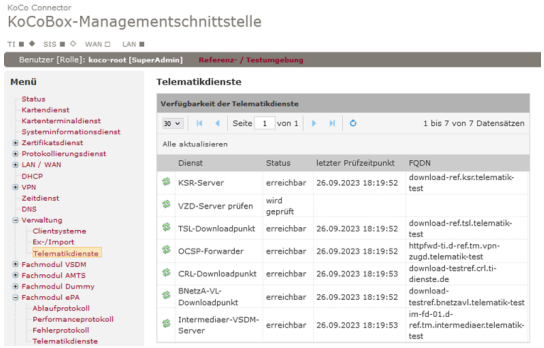
Zusätzlich zur ePA 1.0 und ePA 2.0 ist die ePA 2.5 umgesetzt.

Neue Operationen im Konnektor:

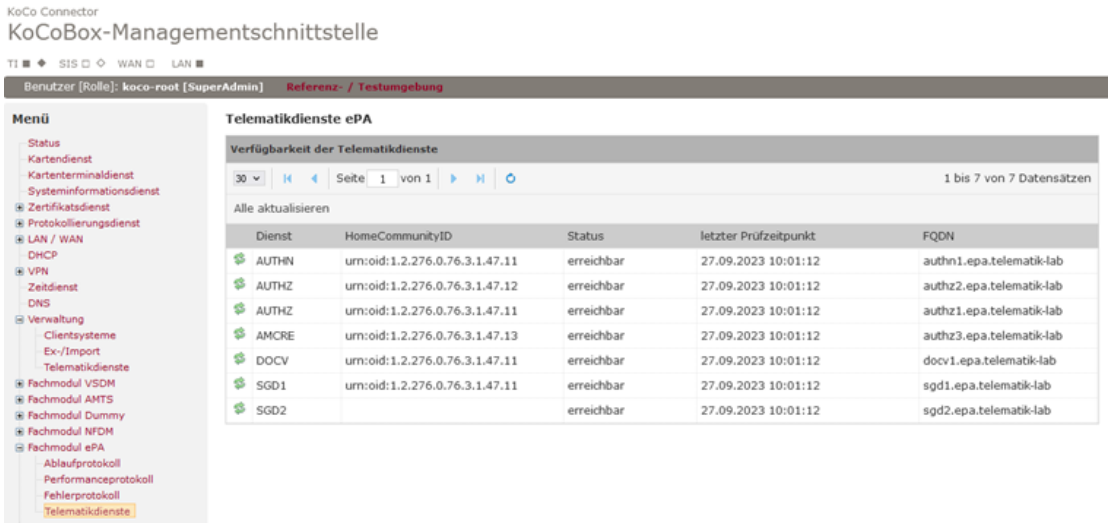
- Datenübermittlung aus einer DiGA in eine ePA
- Erstellung einer ad-hoc Berechtigung für DiGA in der Leistungserbringerumgebung
- Einsehen der DiGA-Daten durch einen Leistungserbringer

Diagnose, Download CRL/TSL und Betriebsdaten [gematik C_11268]

Um sowohl bei der Inbetriebnahme als auch bei der Entstörung den Anwender zu unterstützen, wurden folgende Hilfsfunktionen implementiert:**Prüfung der Erreichbarkeit von Systemen:**



Über die Management-Oberfläche wird die Verfügbarkeit der einzelnen TI-Dienste angezeigt (KSR, VZD, TSL/CRL/BNetzA-VL-Downloadpunkte, OCSP-Forwarder, Intermediär-VSDM, ePA).



Manueller Download der CRL, TSL und BNetzA-VL
Über die Management-Oberfläche im Bereich Zertifikatsdienst kann die sofortige Aktualisierung der CRL, TSL und BNetzA-VL gestartet werden.

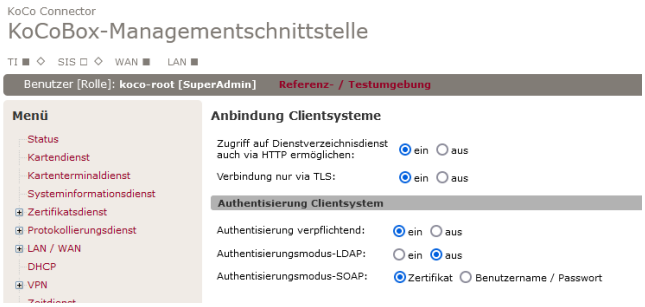
Manueller Versand der Betriebsdaten
Über die Management-Oberfläche kann der sofortige Versand der Betriebsdaten ausgelöst werden.

Zielführendere Fehlermeldung am PS für Zugriffsberechtigungsdienst [gematik C_10978]

Die allgemeine Fehlermeldung des Konnektors zum PS "Prüfung der Zugriffsberechtigung fehlgeschlagen" wird durch die detaillierten Fehlermeldungen des Zugriffsberechtigungsdienstes abgelöst. Die Meldung gibt Auskunft, wo ggf. eine fehlerhafte Konfiguration vorliegt (Konnektor/PS).

TLS-Client-Auth - Schalter für LDAP [gematik C_11118]

Über die Management-Oberfläche kann die verpflichtende LDAP-Authentifizierung der Clientsysteme zur Nutzung des LDAP-Proxys aktiviert bzw. deaktiviert werden.



Aktualisierung SOG-IS-Katalog [gematik C_11325]

Damit auch in der Vergangenheit signierte Objekte vom Konnektor verarbeitet werden können, prüft der Konnektor die verwendeten kryptografischen Algorithmen nicht mehr auf ihre zeitliche Zulässigkeit. Für neu zu erstellende Signaturen regelt die gematik die Anwendung von kryptografischen Algorithmen über die TSL.

Mindestanzahl von Zertifikaten für Verschlüsselung [gematik C_11042]

Um die Anwendung KIM adäquat zu unterstützen, sind bei der hybriden Verschlüsselung nun bis zu 2.000 Empfänger-Zertifikate möglich.

Härtung von Vorgaben zu XML-Dokumenten und Nachrichten [gematik C_11022]

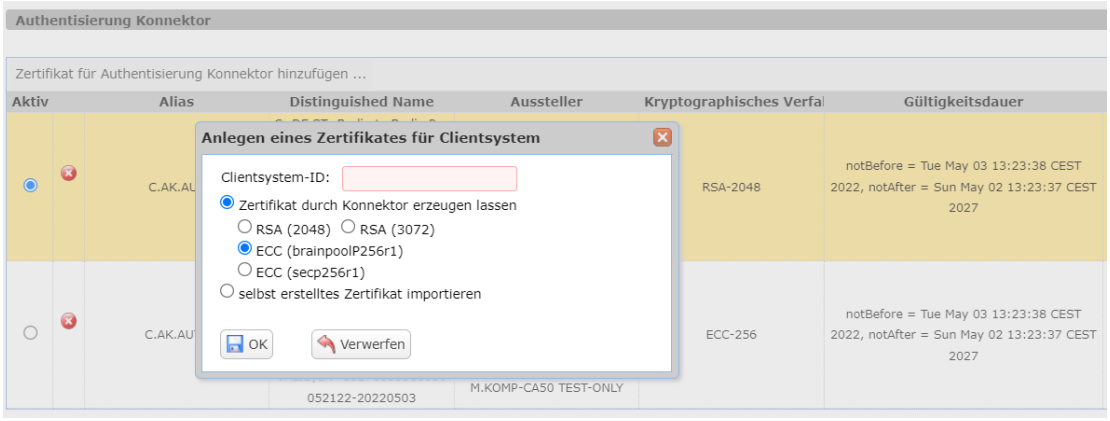
Basierend auf Rückmeldungen der Hersteller und Zertifizierungsverfahren hat die gematik Korrekturen an gehärteten Schemata und Anforderungen zur Verarbeitung von XML-Dokumenten und Nachrichten vorgenommen. Das hat Auswirkung auf die Validierung, Verschlüsselung, Entschlüsselung, Signatur und Signaturprüfung von XML-Dokumenten und Nachrichten.

Entfall der Prüfung von CV-Zertifikaten der Generation 1 [gematik C_11113]

Nach Wegfall der Anforderung GS-A_4668 (Änderungsliste P18.1/2019) wurde nun der TUC_KON_042 so angepasst, dass die Prüfung von CV-Zertifikaten der Generation 1 nicht länger möglich ist.

ECC-Nutzung an der Schnittstelle zu Primärsystemen [gematik C_11034]

Soll zur Authentifizierung gegenüber dem Clientsystem das Zertifikat von der gSMC-K genutzt werden, so kann zwischen dem RSA- oder ECC-Zertifikat (sofern vorhanden) gewählt werden. Es können nun RSA-3072-Authentifizierungszertifikate sowohl erzeugt als auch importiert werden. Beim Import eines Zertifikats wird nun vom Konnektor geprüft, dass dieses nicht länger gültig ist als die Konnektorzertifikate selbst (max. 5 Jahre).



Dokumente >25MB bei Verify-, Sign-, Encrypt- und DecryptDocument [gematik C_11091]

Überschreitet ein Dokument bzw. Aufruf für die Operationen signDocument, verifyDocument, encryptDocument, decryptDocument die zulässige Größe, quittiert der Konnektor dieses mit dem Fehler „4283 Dokument zu groß“. Überschreitet der Request die Größe von 335 MB, antwortet der Konnektor weiterhin mit dem HTTP-Fehler 413.

Betriebsdaten: Anpassung der verpflichtend zu senden Daten [gematik C_11076]

Konnektoren können sich in Zuständen befinden, in denen nicht alle der im Schema OperatingData.xsd geforderten Daten verfügbar sind. Da solche Daten dennoch als "verpflichtend" markiert sind, führt das in der Folge zu Fehlern. Nun wurde das Schema dahingehend angepasst, dass möglicherweise betroffene Daten als optional deklariert sind.

VSDM: Fehlerhierachie bei gesperrter eGK [gematik C_11138]

Durch Anpassung der Prüfhierarchie wird sichergestellt, dass bei einer gesperrten eGK der fehlende Versicherungsschutz zuverlässig sichtbar wird. Bisher war es durch eine unklare Fehlerhierarchie möglich, dass beim Einlesen der Karte (ReadVSD) weitere Fehler erkannt und in der Folge als Ergebnis Prüfnachweis-3 "technischer Fehler" gemeldet wurde.

3 Änderungen und behobene Fehler

3.1 Seit Version 5.5.12

Zugriff auf connector.sds nicht möglich / Keine LDAPS Verbindung möglich / TLS-Session-Cache voll
Der Konnektor MUSS TLS Session Resumption mittels Session-ID gemäß RFC5246 für TLS-gesicherte Verbindungen zum Clientsystem unterstützen, um für den wiederholten Aufbau von TLS-Verbindungen die bereits ausgehandelten TLS-Session wiederzuverwenden und damit den TLS-Handshake abzukürzen.
Wurden binnen 24h mehr als 20.400 neue TLS-Sessions aufgebaut, kam es zu einem Fehler im Session Cache, der dazu führte, dass keine neuen TLS-Verbindungen aufgebaut werden konnten. Das zeigte sich unter anderem an dem Fehler: Kein Zugriff auf die connector.sds oder keine LDAPS Verbindung möglich. Dieser Fehlerzustand konnte nur durch einen Neustart behoben werden.

In der Konnektor-Firmware 5.5.16 wurden Anpassungen am Cache Handling vorgenommen, so dass beim Überschreiten des Limits von 20.400 TLS-Verbindungen die älteste Sitzung zugunsten einer neuen Sitzung überschrieben wird.

Log-Download nicht möglich
Durch einen Change im Firefox, war es ab der Browserversion v128 nicht mehr möglich, Dateien vom Konnektor runterzuladen (Logs, Konfig & Zertifikate).

Mit der Konnektor-Firmware 5.5.16 ist der Dateidownload nun wieder in allen aktuellen Browserversionen inkl. Firefox möglich.

TSL und CRL wird mehrfach täglich heruntergeladen
Bei der Prüfung des letzten Downloadzeitpunktes bzgl. der TSL und CRL konnte es zu einem Fehler kommen, so dass binnen 24 Stunden die TSL und CRL mehrfach heruntergeladen werden konnte.

Mit der Konnektor-Firmware 5.5.16 wurde die Prüfung so modifiziert, dass der Download nur noch einmal am Tag erfolgt.

IP-Pakte von KIM werden von der Konnektor-Firewall geblockt
Speziell bei einer intensiveren Nutzung von KIM konnte es dazu kommen, dass von der Firewall im Konnektor beim Überschreiten eines Grenzwertes kurzzeitig IP-Pakete blockiert wurden.

In der Konnektor-Firmware 5.5.16 wurden Anpassungen in der Firewall vorgenommen, um das Verhalten zu beheben.

GetSubscription direkt nach dem Firmwareupdate nicht möglich
Nach einem Firmware-Update konnte es dazu kommen, dass der Konnektor Anfragen nach CETP-Abonnements (Aufruf: GetSubscription) nicht beantwortet.

In der Konnektor-Firmware 5.5.16 wurden Anpassungen vorgenommen, welche das Problem beheben.

falscher CRL-Download-Endpunkt
Im Rahmen der gematik-Testwoche zum RSA-Phase-Out wurde bei RU-Testkonnektoren (RU: Referenzumgebung) beobachtet, dass vereinzelt Konnektoren den CRL-Downloadpunkt nicht korrekt aus der TSL übernehmen.

In der Konnektor-Firmware 5.5.16 wurden Anpassungen vorgenommen, welche das Problembeheben.

Fehler bei HBA-Gültigkeitsprüfung
Im Rahmen der Umstellung bei der HBA-Personalisierung bei IDEMIA ist es zu einer Inkompatibilität bei der Gültigkeitsprüfung im Konnektor gekommen, der Aufruf CheckCertificateExpiration läuft auf den Fehler 4001. Es ist nur eine kleine Gruppe von HBAs betroffen.

In der Konnektor-Firmware 5.5.16 wurden Anpassungen vorgenommen, welche das Problem beheben.

Komfortsignatur nach Laufzeitverlängerung mit neuem HBA nicht möglich
Das erstmalige Aktivieren der Komfortsignatur mit einem neuen HBA bei einem Konnektor nach erfolgter Laufzeitverlängerung schlägt fehl, wenn der HBA und die laufzeitverlängerten Zertifikate unter der gleichen CVC-Root-CA erstellt wurden.

In der Konnektor-Firmware 5.5.16 wurden Anpassungen vorgenommen, welche das Problem beheben.

Neues Schema und Signatur der BNetzA-VL
Mit der Anhebung der ETSI TS 119 612 von V2.1.1 auf V2.3.1 wird neben dem Schema (version 6) auch das XAdES-Profil der Signatur der Vertrauensliste von XAdES BES/EPES nach ETSI TS 101 903 auf XAdES-B-B nach ETSI EN 319 132-1 geändert.

In der Konnektor-Firmware 5.5.16 wurden Anpassungen vorgenommen, um das neue Schema und das geänderte Signaturverfahren zu unterstützten.

3.2 Seit Version 5.1.8/5.1.10/5.5.2

Es werden behobene Fehler zum Release 5.1.8/5.1.10 bzw. 5.5.2 der KoCoBox MED+ gelistet.

KIM1.0 Client Modul konnte keine Verbindung zum Konnektor aufbauen

Gemäß dem gematik Change C_11325 (siehe weiter oben) sind folgende Ciphersuiten, welche für KIM 1.0 relevant sind, entfallen:
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Dadurch war keine Verbindung mehr zwischen KIM1.0 Client Modul und Konnektor möglich.

KIM1.5 war davon nicht betroffen.

In der aktuellen Konnektor-Firmware-Version werden die Ciphersuiten wieder unterstützt.

4 Allgemeine Hinweise

Unterstützung von TLS 1.2

Seit Version 4.2.22/24 (PTV4+) unterstützt der Konnektor ausschließlich TLS-Verbindungen mit TLS 1.2.

5 Bekannte Fehler

keine

6 Hinweise zum Update auf PTV5+

Update in Zwischenschritten

Beim Update von PTV3 (FW-Version 2.3.24) bzw. beim Update von PTV4 (FW-Version 4.x.x) auf PTV5+ (FW-Version 5.5.x) ist zwingend als Zwischenschritt ein Update auf PTV4 (FW-Version 4.2.22/24) und/oder PTV5 (FW-Version 5.1.x) notwendig.

Sperrung von Firmwareversionen nach Zulassungsende

Es dürfen nur Konnektoren und Kartenterminals mit von der gematik zugelassenen Firmwareversionen an der Telematikinfrastruktur teilnehmen. Bei Zuwiderhandlung ist der VPN-Zugangsdienstbetreiber verpflichtet, diese entsprechend zu behandeln und in letzter Konsequenz den Zugang zur TI zu sperren.

Wir empfehlen daher entweder die Aktivierung der Autoupdate-Funktion im Konnektor oder alternativ die regelmäßige Prüfung auf neue Firmwareversionen auf dem KSR.

Ablauf der Firmware PTV3 & PTV4

Seit dem 01.01.2025 sind die Softwarestände PTV3 (FW-Version 2.3.24) und PTV4 (FW-Version 4.x.x) nicht mehr Bootfähig.

***Disclaimer:** Alle Angaben ohne Gewähr. Änderungen vorbehalten.*