# Release Notes: KoCoBox MED+

| | |
|---|---|
| KoCoBox MED+ Firmware: | 5.1.8 |
| Gültig für Hardwareversion: | 2.0.0 und 4.0.0 |
| Produkttypsteckbrief Konnektor: | 5.1.0-0 (PTV5 mit ePA 2.0) |
| Stand: | 01.06.2023 |

## 1 Einleitung

Die KoCoBox MED+ Konnektor Version 5.1.8 ist die Produktversion gemäß PTV5. Sie basiert auf der Produkttypsteckbriefversion 5.1.0-0.

Damit sind gegenüber der Konnektorversion 4.2.22:4.0.0 bzw. 4.2.24:2.0.0 weitere Funktionen gemäß des Produkttypsteckbriefes gemProdT_Kon_PTV5_5.1.0-0_V1.0.1.pdf hinzugekommen. Im Folgenden sind die darüber hinausgehenden Änderungen von PTV4+ (4.2.22:4.0.0 bzw. 4.2.24:2.0.0) zu PTV5 (5.1.8:2.0.0 bzw. 5.1.8:4.0.0) beschrieben

Die Version 5.1.8 basiert auf der 5.1.6, jedoch erweitert um den Hotfix gemäß Punkt 2. Bis auf den Hotfix sind die Versionen 5.1.6 und 5.1.8 funktionsgleich.

## 2 Hotfix 5.1.8

Infolge der Bekanntgabe des **CVE-2023-29469** wurde bei der Betrachtung der Reichweite des Problems festgestellt, dass bestimmte Funktionalitäten des Konnektors betroffen sind. Konkret sind dies hierbei die über SOAP-Aufrufe nutzbaren Funktionen EncryptDocument und DecryptDocument des EncryptionService, ausschließlich für übergebene XML-Dokumente.

Die erkannte Schwachstelle wurde durch Aktualisierung der Linux-Pakete geschlossen.

Die Version 5.1.8 besitzt den gleichen Funktionsumfang wie die 5.1.6, lediglich im Stand der Linux-Pakete unterscheiden sich die Versionen.

## 3 Neue Funktionen

### Elektronische Patientenakte – ePA 2.0

Zusätzlich zur ePA 1.0 ist die ePA 2.0 umgesetzt.

Neue Operationen für ePA 2.0:

- removeMetadata – Löschen von Dokumenten auch in Ordnern
- getAutorisationState – Abfrage der Berechtigungen

Angepasste Operationen:

- RequestFacilityAuthorization – Berechtigungsvergabe wurde angepasst
- getAutorisationList – soll nur noch einmal am Tag ausgeführt werden
- getHomeCommunityID – Anpassung der Abfrage zur Steigerung der Perfomance
- ValidTo – Angabe der Gültigkeitszeitpunkte in Events erfolgt nur noch tagesgenau

Operationen stehen in ePA 2.0 nicht mehr zur Verfügung:

- updateDocumentSet – Ändern der Metadaten von Dokumenten

- removeDocument – wird durch removeMetadata ersetzt

**ECC-Migration**

Umstellung folgender VPN- und TLS-Verbindungen auf ECC:

- VPN-Zugangsdienst
- Kartenterminals
- Primärsystem
- Intermediär
- zentrale Dienste der TI

Der Konnektor bevorzugt beim TLS-Verbindungsaufbau die Verwendung von ECC-Ciphersuiten. Das gilt für Konnektoren ab SN 8027600364000095102, welche mit dualpersonalisierten Gerätekarten (gSMC-K mit RSA+ECC) ausgestattet sind.

**ECC-Migration VPN:** Eine auf Basis RSA bestehende VPN-Registrierung versucht der Konnektor automatisch auf ECC umzustellen. Generell wird der Konnektor bei jedem VPN-Aufbau immer zuerst versuchen, ein ECC-basiertes VPN aufzubauen. Wenn dies scheitert, fällt er auf RSA-basiertes VPN zurück.

**ECC-Migration Kartenterminals:** RSA-Kartenterminalpairings bleiben bestehen und können durch Neu-Pairing auf ECC umgestellt werden, sofern das Kartenterminal dies unterstützt.

**ECC-Migration Primärsystem:** Konfigurierte RSA-Primärsystemverbindungen bleiben bestehen, können nun aber auf ECC umgestellt werden. Zusätzlich kann die Konnektorauthentisierung frei konfiguriert werden, neben ECC Brainpool wird auch ECC NIST unterstützt.

**Abgrenzung:**
ECC-Verfahren werden **nicht** bei der Konfigurationsschnittstelle (Managementschnittstelle) unterstützt.

**Betriebsdatenmeldedienst**

Der Konnektor übermittelt täglich die gemäß Spezifikation geforderten Betriebsdaten an den VPN-Zugangsdienst, wobei dieser vor der Weitergabe an die gematik das einzige personenbezogene Datum - die Contract-ID - entfernt.

**Zertifikatsablauf: Anzeige des Zertifikats-Status und Ablaufdatum**

Über die Managementschnittstelle wird im Zertifikatsdienst der Status der verwendeten Zertifikate, inkl. Ablaufdatum angezeigt (z.B. gSMC-K). Über den Ereignisdienst kann der Zustand: „Das Zertifikat der gSMC-KT im Kartenterminal läuft in weniger als 5 Wochen ab.“ vom Primärsystem abonniert werden. Das Primärsystem kann über die Operation CheckCertificateExpiration die Laufzeit des Kartenterminalzertifikats (gSMC-KT) abfragen.

Folgende Betriebszustände wurden hinzugefügt: EC_NK_Certificate_Expiring, EC_NK_Certificate_Expired und EC_CardTerminal_gSMC-KT_Certificate_Expires_Soon

**Operation VerifyCertificate**

Zur Unterstützung des eRezeptes können jetzt zusätzlich die Zertifikatsprofile oid_fd_sig, oid_fd_osig, oid_zd_sig verifiziert werden.

### Alternativer TSL Download konfigurierbar

Als Reaktion auf den großflächigen Ausfall von Konnektoren, aufgrund einer fehlerhaften TSL, wurde eine Möglichkeit geschaffen, auch ohne VPN Verbindung zur Telematikinfrastruktur eine gültige TSL aus dem Internet von einem alternativen Downloadpunkt zu laden. Die KoCoBox MED+ war von diesem Ausfall nicht betroffen.

## 4 Änderungen und behobene Fehler

Es werden behobene Fehler zum Release 4.2.22:4.0.0 bzw. 4.2.24:2.0.0 der KoCoBox MED+ gelistet.

### Gültigkeitsdauer für Zugangszertifikate für Clientsysteme verlängert

Bisher waren vom Konnektor erstellte Zertifikate für die sichere Verbindung mit dem Clientsystem nur 1 Jahr gültig. Dieses wurde nun so geändert, dass das Ablaufdatum der ausgestellten Zertifikate dem der Konnektor-Smartcard (gSMC-K) entspricht. Damit ist eine Laufzeit von bis zu 5 Jahren möglich.

### Komfortsignatur und Stapelsignatur

Bei Konnektoren mit aktuellen Gerätekarten (gSMC-K) konnte es dazu kommen, dass die Komfortsignatur und/oder Stapelsignatur gestört waren. Durch Anpassung in der Kommunikation zum Kartenterminal wird sichergestellt, dass dieser Fehler nicht mehr auftritt.

### Anzeige und Meldung von Firmwareständen angeschlossener Kartenterminals

Die Abfrage von Firmwareständen angeschlossener Kartenterminals wurde dahingehend verbessert, dass immer die tatsächlich installierte Firmwareversion erfasst, auf der Managementoberfläche angezeigt und auch an den KSR übertragen wird.

## 5 Allgemeine Hinweise

### Unterstützung von TLS 1.2

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

### Transfer von großen Dokumenten in die ePA

Um den Up- und Download von größeren Dokumenten speziell bei geringen Übertragungsbandbreiten in ein Aktensystem zu ermöglichen, wurde der Wertebereich für das Verbindungstimeout auf 15 Minuten (900s) erweitert. Der Defaultwert wurde auf 4 Minuten (240s) erhöht.

## 6 Bekannte Fehler

### Falscher Fehlercode bei zu großen Dokumenten

Das Einstellen von zu großen Dokumenten in die ePA (Operation putDocuments) wird zwar korrekt verhindert, jedoch statt mit dem Fehlercode 7211 (Einzeldokument > 25 MB) bzw. 7212 (mehrere Dokumente > 250MB) mit HTTP-Status 413 beantwortet.

### Event gSMC-KT_Certificate_Expires_Soon($ctId)

Beim Abonnieren des Events gSMC-KT_Certificate_Expires_Soon($ctId) muss das gewünschte Kartenterminal explizit ausgewählt werden. Das Abonnieren aller Kartenterminalevents über einen Aufruf ist nicht möglich.

Dabei muss die Angabe zwingend ohne Leerzeichen erfolgen.

Beispiel: OPERATIONAL_STATE/EC_CardTerminal_gSMC-KT_Certificate_Expires_Soon(CT_ID_0027)

**connector.sds über HTTP nicht verfügbar, wenn TLS aktiviert**

Aus Sicherheitsgründen soll die Kommunikation der Primärsysteme mit dem Konnektor verschlüsselt erfolgen (ANCL_TLS_MANDATORY=Enabled). Der Konnektor MUSS bei gesetzter Variable ANCL_TLS_MANDATORY=Enabled den Verbindungsversuch von Primärsystem ohne TLS ablehnen. Jedoch soll in diesem Zustand noch die connector.sds über HTTP verfügbar sein, welches der Konnektor nicht unterstützt.

Als Workaround kann im Bedarfsfall vorübergehend die Kommunikation zum Primärsystem auf unverschlüsselt gesetzt werden (ANCL_TLS_MANDATORY=Disabled) und dann die connector.sds über HTTP abgerufen werden.

**Verbindungsverlust zu Aktensystem**

Wenn das Aktensystem die TLS-Verbindung zum Konnektor nach z.B. 5-minütiger Inaktivität einseitig beendet, ohne ein TLS-Close-Notify an den Konnektor zu senden, kann es zu Problemen bei der Weiterverwendung des etablierten VAU-Kanals kommen. Der dann folgende Aufruf schlägt fehl und muss wiederholt werden.

# 7 Hinweise zum Update auf PTV5

**Update in Zwischenschritten**

Beim Update von PTV3 (FW-Version 2.3.24) auf PTV5 (FW-Version 5.1.6) ist zwingend als Zwischenschritt ein Update auf PTV4 (FW-Version 4.2.22/24) 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.

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