

## Release Notes: KoCoBox MED+

KoCoBox MED+ Firmware: 6.0.8  
 Gültig für Hardwareversion: 2.0.0 (G3) und 4.0.0 (G4)  
 Deadline-Date: 2.0.0 (G3): 10.11.2027 / 4.0.0 (G4): 24.11.2027  
 Produkttypsteckbrief Konnektor: 6.0.2-0 (PTV6 mit RSA Phase-Out, PoPP, ECC-LZV, ECC\_only eGK)  
 Stand: 13.05.2026

### 1 Einleitung

Die KoCoBox MED+ Konnektor Version 6.0.8 ist die Produktversion gemäß PTV6. Sie basiert auf der Produkttypsteckbriefversion 6.0.2-0

Damit sind gegenüber der Konnektorversion 5.5.16:2.0.0 bzw. 5.5.16:4.0.0 weitere Funktionen gemäß des Produkttypsteckbriefes *gemProdT\_Kon\_PTV6\_6.0.2-0\_V1.1.0.pdf* hinzugekommen.

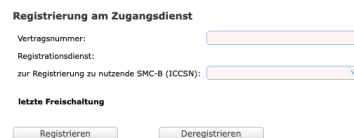
Im Rahmen des Updates auf PTV6 führt der Konnektor eine interne Umschlüsselung des sicheren Speichers durch. Bitte trennen Sie den Konnektor in dieser Zeit (längstens für 30 Minuten) nicht von der Spannung.

### 2 Neue Funktionen

#### RSA Phase-Out [gematik C\_11676]

Mit PTV6 wurde das Verhalten des Konnektors so angepasst, dass nach Möglichkeit RSA-2048 Zertifikate nicht mehr verwendet werden. Bei kartenbasierten Zertifikaten wird, sofern verfügbar, das ECC-Brainpool Zertifikat verwendet. Bei selbsterstellten Zertifikaten wird neben RSA-3072 auch ECC-NIST unterstützt.

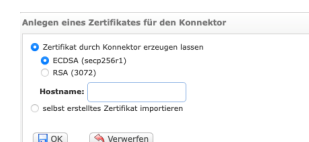
- **VPN-Zugangsdienst:** Ein dual-personalisierter Konnektor verwendet nur noch das C.NK.VPN2 (ECC) zur Verbindung zum VPN-Zugangsdienst. Eine Neuregistrierung erfolgt nur noch mit dem C.NK.VPN2 (ECC).



- **Clientsystem-Zertifikat zur Authentisierung:** Bei der Generierung bzw. dem Import von **neuen** Clientsystem-Zertifikaten wird nur noch ECC-NIST oder RSA-3072 unterstützt. Bereits konfigurierte Clientsystem-Zertifikate sind davon nicht betroffen, bleiben bis zum zeitlichen Ablauf gültig.



- **Konnektor-Zertifikat zur Authentisierung:** Bei der Generierung bzw. dem Import von **neuen** Server-Zertifikaten, wird nur noch ECC-NIST oder RSA-3072 unterstützt. Die bestehende Konfiguration behält auch nach dem Update ihre Gültigkeit, jedoch kann nicht mehr auf das C.AK.AUT (RSA-2048) zurück gewechselt werden. Zur Authentisierung im Browser wird vom Konnektor auf Basis von ECC-NIST ein Zertifikat selbst generiert und anstelle vom C.AK.AUT verwendet.



- **Kartenterminalverbindung (Pairing):** Bestehende RSA-Kartenterminal-Pairings werden vom Konnektor über ein Wartungspairing automatisch auf ECC umgestellt, sofern das Kartenterminal über eine dualpersonalisierte gSMC-KT (RSA&ECC) verfügt. Dieser Vorgang wird beim Verbindungsaufbau zum Kartenterminal automatisch durchgeführt.  
(ORGA 6141 online und ORGA Neo ab Kartenterminal-Firmware-Version > 3.9.0.)
- **crypt Parameter** – Verschlüsselung & Signaturerstellung erfolgen unabhängig von Client-systemvorgaben, sofern verfügbar, nur noch mit ECC. Bei G2.0-Karten werden RSA-Zertifikate verwendet, da keine ECC-Zertifikate vorhanden sind. Einzig die Operation ReadCardCertificate liefert das per crypt Parameter angeforderte Zertifikat aus.
- **HBA-Vorläuferkarten:** HBA-qSig und ZOD\_2.0 werden nicht mehr unterstützt. Die Karten werden als *unknown* ausgewiesen.
- **G2.0 HBA und SMC-B:** Beim Stecken einer G2.0 Karte wird im Konnektor für 7 Tage folgender Betriebszustand ausgelöst und auf der Statusseite angezeigt:

Betriebszustand	Bedeutung
<i>EC_G2_HBA_USED(\$pseudonym)</i>	Die HBA mit dem angegebenen Pseudonym verfügt nicht über Zertifikate mit 120 bit-Sicherheitsniveau und muss vor dem 01.01.2026 getauscht werden.
<i>EC_G2_SMCB_USED(\$pseudonym)</i>	Der SMC-B mit dem angegebenen Pseudonym verfügt nicht über Zertifikate mit 120bit-Sicherheitsniveau und muss vor dem 01.01.2026 getauscht werden.

Dieser Betriebszustand bleibt bestehen, unabhängig davon, ob die Karte noch gesteckt ist oder nicht. Ist nach 7 Tagen keine G2.0 Karte mehr gesteckt, endet der Betriebszustand. Der Betriebszustand wird nicht über einen Neustart des Konnektors erhalten. Dieser Betriebszustand kann als Event abonniert werden.

- **G2.1 HBA und SMC-B:** Von diesen Karten werden nur noch die ECC-Zertifikate verwendet.
- **Signaturprüfung - verifyDocument (QES):** Seit 01.01.2026 werden Dokumente mit valider RSA-Signatur, welche vor 2026 erstellt wurden, als VALID geprüft und mit ResultMessage "veraltete Signatur mit vermindertem Beweiswert" im VerificationReport ausgegeben.
- **Export Konfigurationsdaten:** Konfigurationsdateien werden vom Konnektor, sofern verfügbar, mit dem ECC-Zertifikat der SMC-B signiert. Sobald die RSA-CA der SMC-B aus der TSL entfernt wird, können nur noch ECC-signierte Konfigurationen importiert werden. Alte, nicht unter PTV6 erstellte Konfigurationsdateien sind dann nicht mehr verwendbar.

**Zusammenfassung:** Mit dem Einspielen des PTV6-Updates führt der Konnektor automatisch den RSA-Phase-Out durch. **Es ist keine zusätzliche Nutzeraktion erforderlich.** Kartenterminal-Pairings stellt der Konnektor, soweit möglich, automatisch auf ECC um. Bestehende Konfigurationen bleiben weiter gültig, selbst wenn dabei RSA-2048-Zertifikate verwendet werden. Erst bei Anpassung der Konfiguration entfällt die Wahlmöglichkeit von RSA-2048 und teilweise ECC-Brainpool – als Alternative werden RSA-3072 und ECC-NIST angeboten.

**PoPP** [gematik C\_11814]

Der PoPP-Service (Proof of Patient Presence) im Konnektor wird von einem PoPP-Client aufgerufen, um im Zusammenspiel mit der EGK und dem zentralen PoPP-Dienst einen kryptografisch gesicherten Token zu generieren, welcher den Gesundheitseinrichtungen einen ortsunabhängigen Zugriff auf Versichertendaten und damit auf TI-Anwendungen, wie die elektronische Patientenakte (ePA) oder das E-Rezept, ermöglicht.

**ECC-Laufzeitverlängerung** [gematik C\_11814]

Als Anpassung zur bisherigen Laufzeitverlängerung wird der Prozess vollständig auf die ECC-Zertifikate umgestellt. Es ist nun nicht mehr notwendig, dass auch RSA-Zertifikate verlängert bereitgestellt werden.

**Einbetten von OCSP-Antworten bei nonQES-Signaturen ermöglichen** [gematik C\_11346]

Im Kontext der Anwendung E-Rezept ist zur Unterstützung des Anwendungsfalls "Signieren des Abgabedatensatzes in der Apotheke" die Möglichkeit geschaffen worden, OCSP-Antworten auch im nonQes-Fall in Signaturen einzubinden.

Damit wird die Prüfung der Abgabedatensätze bei den Kassen erleichtert.

**Automatische Aktivierung AK.AUT nach Laufzeitverlängerung**

Gemäß gematik-Spezifikation ist vorgesehen, dass nach der Laufzeitverlängerung das AK.AUT manuell aktiviert werden muss. Um zu verhindern, dass der Konnektor ein abgelaufenes AK.AUT-Zertifikat verwendet, wird das laufzeitverlängerte AK.AUT-Zertifikat am letzten Tag der Gültigkeit des alten Zertifikats automatisch aktiviert.

**ECC\_only eGK** [gematik C\_11772]

Mit PTV6 unterstützt der Konnektor die korrekte Verarbeitung von eGKs, die nur noch mit ECC-Zertifikaten ausgestattet sind.

**ePA-Fachmodul entfernt** [gematik C\_11810]

Das Fachmodul ePA konnte aus dem Konnektor entfernt werden, da seit Anfang 2025 mit der Einführung der ePA 3.0 – *ePA für alle* – die Aufrufe nun direkt aus dem Primärsystem erfolgen und ein Fachmodul im Konnektor dazu nicht länger notwendig ist.

**Bei erfolgreicher OCSP-Prüfung Warnung 1050 unterdrücken** [gematik C\_11309]

Wenn im Rahmen einer QES-Signaturprüfung mit eingebetteter OCSP-Response diese verworfen und eine frische OCSP-Antwort (Status GOOD) eingeholt wird, wird dem Anwender keine Warnung gemeldet und die eingebettete OCSP-Antwort aktualisiert. Da es noch ein bis zwei Jahre dauern wird, bis die Konnektoren verwertbare OCSP-Antworten einbetten, würde so lange die Warnmeldung 1050 "PROVIDED\_OCSP\_RESPONSE\_NOT\_VALID" zum Regelfall. Regelmäßige Warnmeldungen müssen vermieden werden, um die Aufmerksamkeit des Anwenders für Warnmeldungen zu erhalten.

**Anpassung Clientauthentifizierung** [gematik C\_11600]

Es ist nun möglich, für die Clientsystem-Schnittstelle unterschiedliche Zertifikate zu erstellen und zu verwalten. Diese Zertifikate besitzen eine Gültigkeit von 5 Jahren ab Erstellung.

Die Zertifikate können über die Management-Oberfläche eingesehen werden. Zusätzlich wird bei Aktivierung eines Zertifikats zur Konnektorauthentisierung ein CETP-Event (sofern abonniert) versendet und ein entsprechender Eintrag im Systemprotokoll vorgenommen.

Zertifikat für Authentisierung Clientsystem hinzufügen ...						
	Clientssystem	Distinguished Name	Aussteller	Kryptographisches Verfahren	Gültigkeitsdauer	SHA256-Fingerabdruck
	CS3	C=DE,ST=NRW,O=design,OU=level,CN=Test	C=DE,ST=NRW,O=design,OU=level,CN=Test	ECDSA (secp256r1)	notBefore = Thu Feb 23 18:09:49 CET 2023, notAfter = Wed Feb 23 18:09:49 CET 2028	12 4A A2 95 97 6F 0A A4 03 2D 29 CE 39 23 E1 81 A1 80 82 24 6B 30 99 AA BA 85 54 33 84 83 7B
	CS2	C=DE,ST=NRW,O=design,OU=level,CN=Test	C=DE,ST=NRW,O=design,OU=level,CN=Test	ECDSA (secp256r1)	notBefore = Thu Feb 23 18:09:49 CET 2023, notAfter = Wed Feb 23 18:09:49 CET 2028	12 4A A2 95 97 6F 0A A4 03 2D 29 CE 39 23 E1 81 A1 80 82 24 6B 30 99 AA BA 85 54 33 84 83 7B
	CS1	C=DE,ST=NRW,O=design,OU=level,CN=Test	C=DE,ST=NRW,O=design,OU=level,CN=Test	ECDSA (secp256r1)	notBefore = Thu Feb 23 18:09:49 CET 2023, notAfter = Wed Feb 23 18:09:49 CET 2028	12 4A A2 95 97 6F 0A A4 03 2D 29 CE 39 23 E1 81 A1 80 82 24 6B 30 99 AA BA 85 54 33 84 83 7B
	test	CN=Test	CN=LU-Box-5-12	ECDSA (secp256r1)	notBefore = Tue Mar 04 13:45:17 CET 2025, notAfter = Mon Mar 04 13:45:17 CET 2030	91 52 95 7A A7 FD 98 29 AF EB 72 D3 22 7B 9F 03 48 16 4C 3E 53 FD 6A 86 AE 62 12 73 D6 DA 65 F6

Zertifikat für Authentisierung Konnektor

Zertifikat für Authentisierung Konnektor hinzufügen ...						
Aktiv	Alias	Distinguished Name	Aussteller	Kryptographisches Verfahren	Gültigkeitsdauer	SHA256-Fingerabdruck
	C.AK.AUT2	C=DE,ST=NRW,Westfalen,LU=Nephen,PostalCode=57250,ST=REIT,Unternehmensname=20,0=Deutsche Telekom Security GmbH - G2 TEST-ONLY - NOT,VALID,CN=80276883580000050792-20211121	C=DE,O=gematik GmbH NOT,VALID,OU=Komponenten-CA der Telemedizininfrastruktur,CN=GEM_KOMP-CAS4 TEST-ONLY	ECDSA (brainpoolP256r1)	notBefore = Fri Nov 26 15:20:33 CET 2021, notAfter = Wed Nov 25 15:20:33 CET 2026	A1 08 71 C9 1F 52 8D 99 D5 F0 8B 2A 50 8F 14 6A A2 85 3E 79 77 18 18 15 84 4A DD 97 C6 83 94
	test	CN=Test	CN=Test	ECDSA (secp256r1)	notBefore = Tue Mar 04 13:46:21 CET 2025, notAfter = Mon Mar 04 13:46:21 CET 2030	6B F9 4B EE 32 12 E1 1A BE 3F 67 AB 20 FD 6D 01 07 C1 FA 9D 80 6E F2 9D 18 41 90 32 D6

## Download des AK.AUT

Über die Management-GUI kann nun das AK.AUT als PEM-Datei heruntergeladen werden.

Authentisierung Konnektor						
Zertifikat für Authentisierung Konnektor hinzufügen ...						
Aktiv	Alias	Inhaber	Aussteller	Kryptographisches Verfahren	Gültigkeitsdauer	SHA256-Fingerabdruck
<input checked="" type="radio"/>	C.AK.AUT	C=DE,ST=Berlin,L=Berlin,PostalCode=10963,STREET=Deussauer Str. 28/29,OU=KoCo Connector GmbH TEST-ONLY - NOT-VALID,CN=80276883580000050792-2020204	C=DE,O=gematik GmbH NOT-VALID,OU=Komponenten-CA der Telemedizininfrastruktur,CN=GEM_KOMP-CAS4 TEST-ONLY	RSA (2048)	notBefore = Fri Feb 04 17:48:26 CET 2022, notAfter = Wed Feb 03 17:48:25 CET 2027	088D 483F 1581 A15E 737D 977A 2394 404F 247D 6A7E 3664 C673 242A 4881 58A3 308B
<input type="radio"/>	C.AK.AUT2	C=DE,ST=Berlin,L=Berlin,PostalCode=10963,STREET=Deussauer Str. 28/29,OU=KoCo Connector GmbH TEST-ONLY - NOT-VALID,CN=80276883580000050792-2	C=DE,O=gematik GmbH NOT-VALID,OU=Komponenten-CA der Telemedizininfrastruktur,CN=GEM_KOMP-CAS4 TEST-ONLY	ECDSA (brainpoolP256r1)	notBefore = Fri Feb 04 17:48:38 CET 2022, notAfter = Wed Feb 03 17:48:29 CET 2027	38C4 88A7 3471 4229 728A 25CC A66A 688C A6BA C277 2794 AAC 3F16 3055 67C8 133F

## Beschleunigter Download für adHoc-TSL [gematik C\_11794]

Für den Fall, dass eine Störung durch eine adHoc-TSL behoben werden muss, wird nun bei jedem Neustart des Konnektors die TSL aktualisiert, unabhängig davon ob in den letzten 24h bereits eine TSL-Aktualisierung stattgefunden hat.

## Konkretisierung NFDM - andere Heilberufe [C\_11774]

Bezüglich der Nutzung des Fachmoduls NFDM gab es einige Anpassungen, welche Berufsgruppen / professionOID berechtigt sind, auf die Notfalldaten zuzugreifen.

## Neues CETP-Event MGM/TLS\_CERT

Der Konnektor stellt bei der Aktivierung eines an der Clientsystemschnittstelle verwendeten TLS-Zertifikats den Fingerprint (SHA-256 Hashwert) des neu konfigurierten Zertifikats mit dem neuen CETP-Event „MGM/TLS\_CERT“ (sofern abonniert) zur Verfügung.

Die Informationen dieses Events werden auch im Systemprotokoll des Konnektors mit der Severity=Info protokolliert. Diese Verfügbarmachung erfolgt auch für die Aktivierung eines im Zuge der Laufzeitverlängerung heruntergeladenen erneuerten C.AK.AUT-Zertifikats.

Systemprotokoll				
20	1	Seite 1 von 708	1 bis 20 von 14152 Datensätzen	
Zeitpunkt	#	Schwere	Beschreibung	Parameter
21.06.2024 09:47:44.812	1	INFO	MGMADMINCHANGES	NewVal=C.AK.AUT2; User=koco-root; RefID=ANCL_CERTIFICATE_USED
21.06.2024 09:47:44.793	1	INFO	MGM/TLS_CERT	Fingerprint=B093 D28C 5C9C 845D 3722 2C77 58A1 13E1 F04D 4C73 43A8 033F 708D 0858 51B4 255D; Interface=CS_ITF
21.06.2024 09:47:00.397	1	INFO	MGMADMINCHANGES	NewVal=test; User=koco-root; RefID=ANCL_CERTIFICATE_USED
21.06.2024 09:47:00.376	1	INFO	MGM/TLS_CERT	Fingerprint=0218 78ED D15E 0556 2403 32C5 7A41 E9D0 3A7B 90FE 6621 97EE AEA2 9427 E123 F8D1; Interface=CS_ITF
21.06.2024 09:46:14.135	1	INFO	MGMADMINCHANGES	NewVal=C.AK.AUT; User=koco-root; RefID=ANCL_CERTIFICATE_USED
21.06.2024 09:46:14.101	1	INFO	MGM/TLS_CERT	Fingerprint=B168 6C9B B9A3 DE8D 1147 F43C 33E9 109C 06AD 48DF BE83 3311 1705 CE73 88DA; Interface=CS_ITF
21.06.2024 09:45:38.117	1	INFO	BOOTUP/BOOTUP_COMPLETE	TSLStatus=true

### eIDAS Anpassungen Signaturdienst [gematik C\_11276]

Im Rahmen der eIDAS-Konformität seitens des Konnektors wurden im SignatureService drei neue Signaturdienst-Endpunkte hinzugefügt.

- Version="7.4.3"
- Version="7.5.6"
- Version="7.5.7"

**ACHTUNG:** Zukünftig sollen ausschließlich die Versionen v7.5.6, v7.4.3 unterstützt werden.

### eIDAS-Konformität bei QES [gematik C\_11276]

Im Rahmen der eIDAS-Konformität seitens des Konnektors gab es Anpassungen im zeitlichen Ablauf der OSCP-Prüfung der HBA-Zertifikate bei der Erstellung einer qualifizierten elektronischen Signatur (QES).

### Anpassung der Fingerprintanzeige

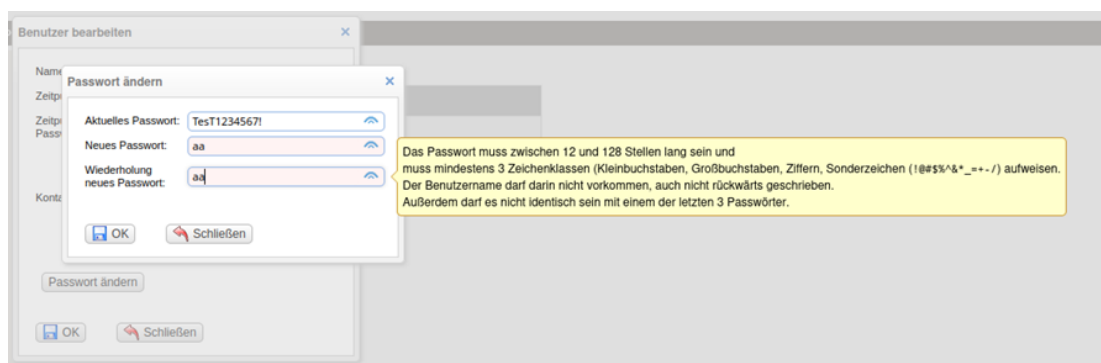
Zur besseren Übersicht und Vergleichbarkeit werden mit der Konnektor-Firmware 6.0.6 die Fingerprints der konfigurierten TLS-Zertifikate im Bereich „Clientsysteme“ angezeigt. Die Anzeige erfolgt fest mit 4 Zeilen à 4 Blöcke mit je 4 Hex-Werten.

Zertifikat für Authentisierung Konnektor hinzufügen ...						
Aktiv	Alias	Distinguished Name	Aussteller	Kryptographisches Ver	Gültigkeitsdauer	SHA256- Fingerabdruck
<input checked="" type="checkbox"/>	C.AK_AUT2	C=DE,ST=Berlin,L=Berlin,P=C=DE,O=gematik GmbH NOT-V	ECDSA (brainpoolP256r1)	notBefore = Thu Aug 24 14:11:16 CEST 2023, notAfter = Tue Aug 22 14:11:15 CEST 2028		3EBB 3C77 CE60 38D9 FABD 7088 9699 96A9 ED49 AA53 D71A A1F1 02FE 5B7E E665 8D10

### Admin-Passwortwechselzwang entfernt [C\_11515]

Ab sofort muss das Admin-Passwort der Management-GUI zwischen 12 und 128 Zeichen lang sein und mind. 3 Zeichenklassen (Kleinbuchstaben, Großbuchstaben, Ziffern, Sonderzeichen) enthalten. Im Gegenzug entfällt der Zwang, zyklisch das Admin-Passwort zu wechseln. Sollte das bisherige Passwort nicht der neuen Konvention entsprechen, wird der Nutzer beim erstmaligen Anmelden nach dem Update aufgefordert, ein neues Passwort zu erstellen, welches dann zeitlich unbefristet gültig ist.

Folglich entfällt die Einstellmöglichkeit der Passwortdauer auf der Benutzeroberfläche.



### PopUp mit Hinweismeldung: Hinweis Sicherheitslogeinträge

Das PopUp, welches den Anwender darauf hinweist, dass neue Einträge im Sicherheitsprotokoll vorliegen, wurde umgewandelt in einen Hinweis auf der Status-Seite. Damit ist kein Wegklicken der Meldung mehr notwendig.

### Reduktion Displayanzeigen

Es werden nur Betriebszustände mit Severity „Error“ und „Fatal“ auf dem Konnektor-Display angezeigt. Die Darstellung der Betriebszustände EC\_LOG\_OVERFLOW und EC\_OTHER\_ERROR\_STATE(2) – „Protokollspeicher zu mehr als 80% gefüllt.“ auf dem Display entfällt. Als Statusmeldung auf der Managementoberfläche und im Log werden die Betriebszustände unverändert ausgegeben.

### Außerbetriebnahme des Konnektors

Der Konnektor kann nun sowohl über die Management-GUI als auch über das Display außer Betrieb genommen werden. Dabei wird der Konnektor irreversibel gelöscht, die gSCM-Ks im Konnektor unbrauchbar gemacht. Zukünftig wird im Zuge der Außerbetriebnahme der Konnektor durch Laden einer neuen Firmware in eine KoCoBox VPN umgewandelt und kann zur Verbindung mit dem TI-Gateway verwendet werden.

### Gültigkeitsprüfung beim Kartenstecken

Nach dem Stecken einer SMC-B oder HBA wird der Status des entsprechenden AUT-Zertifikats geprüft und im Falle einer negativen Prüfung ein Event versendet. Zusätzlich wird der Status im Kartendienst auf der Management-GUI angezeigt. Folgende Zustände sind möglich: Invalid, Inconclusive, Unknown, Revoked, Valid.

## 3 Änderungen und behobene Fehler

### 3.1 Seit Version 5.5.16

#### Entschlüsselung von KIM-Nachrichten bei gleichzeitig aktivierter Komfortsignatur

Wenn die KIM-Adresse auf den HBA registriert wurde, war es nicht möglich, bei einer aktiven Komfortsignatursitzung gleichzeitig den HBA zur Entschlüsselung von KIM-Nachrichten zu verwenden.

Mit der Konnektor-Firmware 6.0.4 wurden Anpassungen vorgenommen, so dass bei Verwendung unterschiedlicher *ClientSystemID* und unterschiedlicher *userID* mit dem gleichen HBA sowohl Komfortsignatur als auch Entschlüsselung funktionieren.

#### Probleme beim Löschen von Entitäten im Infomodell

Beim Löschen von verknüpften Entitäten im Infomodell kann es vorkommen, dass nicht alle Verknüpfungen gelöscht werden. Hierzu mussten bisher die Verknüpfungen manuell gelöst und das Infomodell neu gespeichert werden. Dieser Vorgang muss ggf. mehrfach wiederholt werden.

Mit der Konnektor-Firmware 6.0.4 wurden Anpassungen vorgenommen, welche das Problem beheben.

#### Abbruch beim Import von Konfigurationsdateien

Bei Konfigurationsexporten, welche einen individuellen Alias für das Authentifizierungszertifikat AK.AUT beinhalten, konnte es zum Abbruch des Importvorgangs mit Fehlercode 4001 kommen.

Mit der Konnektor-Firmware 6.0.4 wurden Anpassungen vorgenommen, welche das Problem beheben.

### **Fehlerhafte Rückgabe bei CheckCertificateExpiration**

Bei der Rückgabe der SOAP-Operation "CheckCertificateExpiration" gab der Konnektor den Wert "Nachname" des ausgewählten Zertifikats zurück anstelle des CommonName.

Mit der Konnektor-Firmware 6.0.4 wird bei der Rückgabe der Operation der CommonName des ausgewählten Zertifikats zurückgegeben.

### **Anpassungen beim TLS-Handling**

Bei einer großen Anzahl von TLS-Verbindungen zum Konnektor kam es zu Beeinträchtigungen der genutzten Schnittstelle, was die weitere Nutzung verhinderte. Hier wurden Anpassungen vorgenommen, um die Stabilität zu gewährleisten.

### **Anpassungen Managementoberfläche**

Es wurden einige Anpassungen an der Konnektoroberfläche vorgenommen. So werden im Fehlerfall mehr Hinweise zur Ursache geliefert. Zudem wurde u.a. der Werksreset-Button deutlicher vom Neustart-Button getrennt, das Verhalten bezüglich neuer Sicherheitsprotokolleinträge angepasst und die Konfiguration der Bestandsnetze überarbeitet.

### **Download AUT-Zertifikaten möglich**

Im Bereich „Verwaltung“ – „Clientsysteme“ ist es nun möglich, das Authentisierungszertifikat des Konnektors als \*.pem-Datei herunterzuladen.

### **Protokollierung fehlgeschlagener Authentisierung**

Im Sicherheitsprotokoll werden nun auch fehlgeschlagene Authentisierungen protokolliert. Dies beinhaltet fehlgeschlagene Anmeldeversuche an der Managementoberfläche.

### **Fehlversuch-Sperre bei Login funktioniert nicht korrekt**

Im Handbuch ist beschrieben, dass nach einem fehlerhaftem Loginversuch an der Managementoberfläche ein weiterer Loginversuch erst nach 3 Sekunden möglich ist. Nach 3 Fehlversuchen erfolgt eine Sperre von 60 Sekunden. Durch einen Fehler wurde die 60 sekündige Sperre erst nach dem vierten Loginversuch aktiviert. Dies wurde nun korrigiert.

## **3.2 Seit Version 6.0.4**

### **Verbesserung bei PoPP**

Im Rahmen der PoPP-Testung wurden beim Fehlerhandling sowie bei der Interoperabilität Anpassungen erforderlich, die mit Version 6.0.6 umgesetzt wurden.

## **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 PTV6

### Update in Zwischenschritten

Beim Update von PTV5 (FW-Version 5.1.x) auf PTV6 (FW-Version 6.0.8) ist zwingend als Zwischenschritt ein Update auf PTV5+ (FW-Version 5.5.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.

*Änderungen vorbehalten.*