Release Notes

KoCoBox MED+ Konnektor

Version 4.2.24
(Ausbaustufe PTV4+ ePA Stufe 1.1 und Komfortsignatur)

Version:	3.0.17
Stand:	09.08.2022
Status:	Freigegeben
Klassifizierung:	vertraulich
Referenzierung:	[KoCoConnector_PTV4_Releasenote_Konnektor_V4.2.22.docx]

Inhaltsverzeichnis

1 UMGESETZTE ANFORDERUNGEN 3
1.1 BASISFUNKTIONEN: 3
1.1.1 QES / nonQES Umsetzung 4
1.2 FACHMODULE: 5
1.3 HINWEISE 6
2 NICHT ODER ANDERS ALS SPEZIFIZIERT UMGESETZTE ANFORDERUNGEN 6
3 HINWEISE ZUR UMSETZUNG GEMATIK-ANFORDERUNGEN 7
4 ÜBER DIE ANFORDERUNGEN DER SPEZIFIKATION HINAUSGEHENDE ÄNDERUNGEN 7
5 ÄNDERUNGEN UND BEHOBENE FEHLER 8
6 OFFENE UND BEKANNTE FEHLER UND DEREN BEEINTRÄCHTIGUNG 8

1 Umgesetzte Anforderungen

Die KoCoBox MED+ Konnektor Version 4.2.24 ist die Produktversion gemäß PTV4. Sie basiert auf der Produkttypsteckbriefversion 4.80.3-0.

1.1 Basisfunktionen:

Kürzel	Titel	Beschreibung
QES / nonQES	qualifizierte und nicht-qualifizierte elektronische Signaturen	Erstellen und Prüfen von qualifizierten und nicht-qualifizierten elektronischen Signaturen; Ver- und Entschlüsseln von definierten Dokumententypen
KIM (ehemals KOM-LE)	Sichere Kommunikation im Medizinwesen	Vertraulicher und sicherer Austausch von Nachrichten und medizinischen Dokumenten zwischen den Teilnehmern der Telematikinfrastruktur – über alle Sektoren und Berufsgruppen hinweg. Operationen für diese Lösung werden vom Konnektor unterstützt.
KomfSig	Komfortsignatur	Die Komfortsignatur ermöglicht es dem Leistungserbringer die PIN-Eingaben für Signaturen zu reduzieren. Zu signierende Dokumente sind z.B. eAU oder eRezept. Am Konnektor kann der Modus „Komfortsignatur“ eingestellt werden. Details bitte dem Admin-Handbuch entnehmen. **Hinweis**: Wenn der Modus „Komfortsignatur“ aktiviert ist, dann muss für die Clientsystemschnittstelle des Konnektors verpflichtend TLS mit Clientauthentisierung konfiguriert sein.
AutoUpdate	A_18390 - Automatisches Auslösen der durchzuführenden Updates	Der Konnektor unterstützt die automatische Aktualisierung der Firmware für Kartenterminals und Konnektor. Diese Funktion ist im Standard aktiviert. Es kann am Konnektor eingestellt werden, ob und wann ein neues Update für ein Kartenterminal und / oder Konnektor automatisch installiert wird. Der Zeitpunkt wird über Parameter im Konnektor gesteuert. Standardeinstellung ist mittwochs um 01:00 Uhr. Siehe TIP1-A_4835-02 in Kapitel 2 Details bitte dem Admin-Handbuch entnehmen.
ECC-Migration	Umstellung auf ECC-Zertifikate	Unter ECC - Migration versteht man den Wechsel von RSA-Verfahren zu ECC-Verfahren bei kryptografischen Operationen. ECC steht für Elliptic Curve Cryptography. Grob gesagt basieren ECC-Verfahren auf Operationen mit Punkte-Paaren auf bestimmten elliptischen Kurven und bietet den Vorteil kürzere Schlüssellängen zu verwenden. Die Umstellung enthält das Laden der neuen TSL(ECC-RSA) zu erkennen an der Sequenznummer der TSL > 10.000. Die ECC-Verfahren sind bei geforderten internen Operationen, zum Aufbau des VAU-Kanals für die ePA und bei kartenbasierter Verschlüsselung und Signatur verfügbar z.B. bei KIM, wenn der HBA ECC unterstützt. **Abgrenzung:** Nicht umgesetzte Anforderungen sind in Kapitel 2 gelistet.

Kürzel	Titel	Beschreibung
		ECC-Verfahren werden **nicht** unterstützt bei Verbindungen vom Konnektor • zum VPN-Zugangsdienst (IPsec (VPN)), • zum Clientsystem, • zum Kartenterminal • zum Intermediär Die Clientzertifikate, die der Konnektor ausstellt, basieren auf RSA (kein ECC).

1.1.1 QES / nonQES Umsetzung

Das Basis modul QES / nonQES unterstützt folgende Funktionen.

PAdES- Signaturen erstellen und verifizieren. Die Verifikation dann für unterschiedliche Prüfzeitpunkte (Zeitpunkt der Signaturerstellung, zur Systemzeit, zu einem via Parameter übergebenen Zeitpunkt)
PDF/A-1 und PDFA/A-2 wird unterstützt, PDF/A-3 wird abgelehnt.
Es wird die qualifizierte und nicht-qualifizierte elektronische Signatur unterstützt.

CMS-Signaturen: Erstellen und Verifizieren unterschiedlichster Formate, S/MIME, XML, Text, Tiff, ...
Es wird die qualifizierte und nicht-qualifizierte elektronische Signatur unterstützt.

XAdES-Signaturen: Erstellen von Signaturen mit Signaturrichtlinie. Derzeit liegt ausschließlich für NFD eine Signaturrichtline vor.
Es wird nur die qualifizierte elektronische Signatur hier unterstützt.
XAdES-Signaturen verifizieren: Signaturen mit Signaturrichtlinie. Derzeit liegt ausschließlich für NFD eine Signaturrichtline vor und ist nur im qualifizierten Kontext möglich.

Bei der **Stapelsignatur** gibt es lediglich die Größenbeschränkung von 25 MB plain (base64 - decoded), Anzahl der Dokumente im Stapel ist dadurch nicht begrenzt.

Parallelsignaturen:
XML-Signatur:
Parallele Signaturen werden durch je ein ds:signature-Element pro Signatur abgebildet.
Für die Signaturvariante „enveloping“ werden parallele Signaturen nicht angeboten.
Aufgrund der Beschränkung auf NFD: de facto keine XAdES-Gegensignaturen.

CMS-Signatur:
Parallele Signaturen werden durch je einen SignerInfo-Container pro Signatur realisiert.

PDF-Signatur:
Parallele Signaturen werden nicht angeboten.

Dokumentexcludierende Gegensignaturen:
XML-Signatur

Die Implementierung erfolgt mittels Countersignature gemäß [XAdES], Kapitel 7.2.4. Jede vorhandene Parallel-Signatur wird gegensigniert.
Aufgrund der Beschränkung auf NFD: de facto keine XAdES-Gegensignaturen.

CMS-Signatur:
Die Implementierung erfolgt mittels der Countersignature gemäß CMS-Spezifikation [RFC5652].
Jede vorhandene Parallel-Signatur wird gegensigniert.

PDF-Signatur:
Dokumentexkludierende Gegensignaturen werden nicht angeboten.

1.2 Fachmodule:

Kürzel	Titel	Beschreibung
VSDM	Versichertenstammdaten-management	Die Fachanwendung VSDM prüft die Daten auf der eGK auf Aktualität und Gültigkeit. Ggf. werden die Stammdaten aktualisiert.
NFDM	Notfalldatenmanagement	Fachanwendung der eGK enthält zwei separate Datensätze: NFD (Notfalldatensatz), das sind notfallrelevante medizinische Daten DPE (Datensatz Persönliche Erklärungen), enthält den Ablageort von Willenserklärungen des Versicherten.
AMTS	Arzneimitteltherapiesicherheit.	Fachanwendung der eGK enthält den Datensatz für den elektronischen Medikationsplan (eMP) Arzneimitteltherapiesicherheit (AMTS) ist die Gesamtheit der Maßnahmen zur Gewährleistung eines optimalen Medikationsprozesses mit dem Ziel, Medikationsfehler und damit vermeidbare Risiken für den Patienten bei der Arzneimitteltherapie zu verringern.
ePA	Elektronische Patientenakte	Fachanwendung zur Bereitstellung von gesundheitsbezogenen Daten und Dokumente in einer elektronischen Patientenakte (ePA) gemäß SGB V §291a. Die Beteiligten am medizinischen Behandlungsprozess erhalten einen Einblick in den Verlauf der bisherigen Behandlung, womit eine individuellen Therapieentscheidung unterstützt wird. Die Nutzung der ePA ist freiwillig und kostenfrei. Die Dokumente in der ePA sind bundesweit verfügbar und können einrichtungs- und sektorenübergreifend ausgetauscht werden. Es ist die ePA Stufe 1.1 umgesetzt. Das Berechtigungskonzept beinhaltet: • Berechtigungen für Institutionen erteilen • Einstellen und Herunterladen von Dokumenten durch den Versicherten • Einstellen und Herunterladen von Dokumenten durch den Leistungserbringer

1.3 Hinweise

Der Hersteller empfiehlt als Webbrowser Mozilla Firefox. Dieser wird für die Betriebssysteme Windows (ab Microsoft Windows 7), Linux und macOS (ab Version 10.9) bereitgestellt. Firefox ist in seinem Zusammenspiel mit der KoCoBox MED+ qualitätsgesichert.
Weitere Browsertypen sind unter Umständen ebenfalls geeignet. Für eine sichere und vollständige Funktion derartiger Browser zur Administration der KoCoBox MED+ kann jedoch keine Gewährleistung übernommen werden.

2 Nicht oder anders als spezifiziert umgesetzte Anforderungen

Afo-ID	Titel	Beschreibung
TIP1-A_4717	Konfigurationswerte des Protokollierungsdienstes	**SECURITY_LOG_SIZE** ist statisch gesetzt und kann nicht verändert werden.
TIP1-A_5005	Protokollierung in der Managementschnittstelle	Die Konfigurationsänderungen an den Fachmodulen NFDM und AMTS werden im Ablaufprotokoll des jeweiligen Fachmodules protokolliert.
TIP1-A_4672	QES-Dokumentensignatur prüfen	Der Konfigurationsparameter MGM_LU_SAK wirkt nur für Erstellung und Prüfung einer QES. Wird durch ein Fachmodul eine QES-Signaturerstellung oder -prüfung aufgerufen, so wird bei MGM_LU_SAK=disabled mit Fehler 4125 abgebrochen.
TIP1-A_4655	Dokument QES signieren	
TIP1-A_5505	Kryptographische Prüfung der XML-Dokumentensignatur	
C_6574	Redaktionelle Korrektur	C_6574 nicht umgesetzt Publikation importierter DTD datatypes.dtd und XMLSchema.dtd
TIP1-A_4517	Schlüssel und X.509-Zertifikate für die Authentisierung des Clientsystems erzeugen und exportieren sowie X.509-Zertifikate importieren	Die Auswahl der kryptografischen Verfahren RSA-2048 oder ECC-256 wird an dem Administrator über das Managementinterface dargestellt. Die Funktion für ECC-256 ist nicht implementiert, damit hat die Auswahl keine Wirkung. Es wird Fehler EC4001 gemeldet.
A_17094, A_17221, A_18624,	Anforderungen zur ECC Migration	Die Anforderungen zur ECC-Migration werden mit der nächsten Version umgesetzt und sind nicht enthalten.
TIP1-A_4835-02	Automatische Softwareupdates	Der Default-Wert von **MGM_KSR_AUTO_UPDATE_TIME** wurde auf **Mittwoch** geändert.
A_18605	Option Basisdienst TBAuth	Basisdienst zur Token basierten Authentisierung ist optional und wurde nicht umgesetzt.
A_15559 A_15560 A_15571 A_15572	Operationen von TBAuth	Diese Operationen stehen nicht zur Verfügung, da der Basisdienst TBAuth nicht implementiert ist.
TIP1-A_4518	Konfiguration der Anbindung Clientsysteme	Die CC-Prüfstelle fordert, dass ein höchstmögliches Sicherheitsniveau erreicht werden soll. Diese Forderung wurde vom BSI bestätigt. Wählt der Administrator als Verbindung zu einem Clientsystem „nur via TLS“, dann wird für die Abfrage des Dienstverzeichnisdienstes (DVD) auch

Afo-ID	Titel	Beschreibung
		TLS genutzt. Die Einstellung der Zugriffsart für DVD wird ignoriert. **siehe Hinweis im Admin-Handbuch, Kap. 7.5.1**: "Der Dienstverzeichnisdienst ist grundsätzlich immer über https erreichbar. Zusätzlich kann man auch eine Erreichbarkeit über http konfigurieren – jedoch nicht, wenn die Verbindung außerdem über TLS geschützt werden soll."

3 Hinweise zur Umsetzung gematik-Anforderungen

Die Spezifikation der gematik lässt dem Hersteller Freiheiten für die Umsetzung und es besteht auch ein Interpretationsspielraum für die Umsetzung der Spezifikation. Hier werden Hinweise zur Umsetzung in der KoCoBox MED+ gegeben.

Afo-ID	Titel	Beschreibung
TIP1-A_4796	Grundlagen des Namensdienstes	Der Konnektor unterbindet DNS-Zonentransfer. **Begründung:** Die Spezifikation fordert gegenüber früheren Versionen die Verhinderung des Zonentransfers nicht mehr und überlässt diese Entscheidung dem Hersteller. Der Konnektor behält die bisherige Regel bei.
GS-A_5530	TLS-Verbindungen, Version 1.1	Der Konnektor unterstützt TLS1.1. nicht mehr. Er unterstützt aktuell ausschließlich TLS1.2. **Begründung.** Das BSI weist darauf hin TLS1.1 nicht zu verwenden, da es aufgrund der SLOTH-Attacke (Bhargavan et al. 2016) im allgemeinen Einsatz nicht mehr sicher ist.
A_18467	TLS-Verbindungen, Version 1.3	TLS1.3 ist optional und wird vom Konnektor nicht unterstützt.
	Token basierte Authentisierung	Dieser Basisdienst ist optional und wird in dieser Version nicht unterstützt.

4 Über die Anforderungen der Spezifikation hinausgehende Änderungen

ID	Titel	Beschreibung
	keine	

5 Änderungen und behobene Fehler

Es werden behobene Fehler zum Release 4.2.16 der KoCoBox MED+ gelistet.

ID	Titel	Beschreibung
	keine	

6 Offene und bekannte Fehler und deren Beeinträchtigung

ID	Titel	Beschreibung
	keine	