Ergänzungen zum Administratorhandbuch

KoCoBox MED+

Version 5

KoCo Connector GmbH
Dessauer Str. 28/29
10963 Berlin
Tel.: +49 (0) 30 24 64 90-0
info@kococonnector.com
www.kococonnector.com

Dokumentenversion:	1.3.4
Dokumentensprache:	deutsch (de)
zuletzt geändert:	17.07.2024

Inhaltsverzeichnis

1 Kontext des Dokuments

Diese Ergänzungen zum Administratorhandbuch der KoCoBox MED+ beschreiben zusätzliche Aspekte und Verfahren, die zur Umsetzung des sicheren Betriebs der KoCoBox MED+ notwendig sind.

Die Ergänzungen beziehen sich ausdrücklich auf die Version 5 des Administratorhandbuchs.

Zielgruppe

Zielgruppe dieser Ergänzungen zum Handbuch sind Administratoren und Integratoren der KoCoBox MED+ sowie Hersteller von Primärsystemen, die für den Einsatz mit der KoCoBox MED+ vorgesehen sind.

2 Zusätzliche Sicherheitshinweise

Dieses Kapitel enthält notwendige, zusätzliche Sicherheitshinweise. In den jeweiligen Abschnitten ist der Kontext des Administratorhandbuchs anhand der Kapitelnummer explizit aufgeführt.

2.1 Hinweise für die Netzwerkanbindung im LAN

Kontext: Kap. 3.2, 5

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/

zur Verfügung gestellt.

2.2 Hinweise für die Entwicklung von Primärsystemen

Kontext: Kap. 1 Abschnitt „Weitere Dokumente“

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/

Die Primärsysteme werden im Kontext der Verwendung der KoCoBox MED+ auch als Clientsystem bezeichnet.

2.3 Hinweise für die Anbindung von Primärsystemen

Kontext: Kap. 3.2

Die Spezifikation der gematik stellt den Herstellern und Anwendern von Primärsystemen (Clientsystemen) prinzipiell frei, wie die Verbindung zwischen dem Clientsystem und der zu verwendenden KoCoBox MED+ abgesichert wird. Eine ungeschützte Verbindung stellt jedoch ein erhebliches Sicherheitsrisiko für die Datenübertragung im Praxisnetz dar.

Der Implementierungsleitfaden der gematik trifft keine direkte Aussage über Grundsätze, Auswahl und Anwendung kryptografischer Verfahren bzgl. der Clientsysteme, obwohl dies in der gematik-Spezifikation an anderer Stelle erfolgt. Die Clientsysteme interagieren jedoch mit Komponenten der Telematik-Infrastruktur und unterliegen daher den Empfehlungen und Anforderungen aus der Technischen Richtlinie TR-03116-1 „Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1“ des BSI. Deren Einhaltung und Umsetzung sind durch den

Hersteller des Clientsystems einzuhalten; relevant sind insbesondere die Festlegungen zur RSA-Schlüssellänge. Es gilt der Dokumentenstand, der zum Zeitpunkt des Inverkehrbringens des Clientsystems vorliegt. Der aktuelle Stand der Richtlinie ist unter

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116.html

verfügbar.

Zur Konfiguration geschützter Verbindungen enthalten die folgenden Unterkapitel wichtige Informationen.

2.3.1 TLS-Verbindungsparameter

Kontext: Kap. 7.5.1 Abschnitt „Clientsysteme“

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[1] 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 2. 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)

Hierbei ist zu beachten:

[1] Authenticated Encryption with Associated Data

a) Bezüglich der Konnektorspezifikation [gemSpec_Kon, TAB_KON_852] gelten nur (SOAP1 oder SOAP2 sowie DVD2) und CETP1 als sicher, und zwar ausschließlich
   - mit zusätzlicher Prüfung des Konnektorzertifikats (Konnektor = TLS-Client) bei CETP und
   - mit zusätzlicher Prüfung des Server-Zertifikats bei SOAP sowie
   - mit zusätzlicher Prüfung des Server-Zertifikats bei DVD.

b) Die Anforderung, den Nutzer über den Verbindungszustand zu informieren, ergibt sich besonders aus dem Umstand, dass bei ANCL_TLS_MANDATORY = Disabled nicht klar ist, ob eine TLS-Verbindung besteht oder nicht. ANCL_CAUT_MANDATORY sorgt ebenfalls für Unklarheit.

2.3.2 LDAP-Proxy-Verbindungsparameter

Kontext: Kap. 7.5.8

Die Verbindung zum LDAP-Proxy der KoCoBox MED+ folgt in ihren Parametern weitgehend den Einstellungen zur Absicherung der Verbindung zwischen Clientsystem und Konnektor, siehe Kap. 7.5.1 Abschnitt „Clientsysteme“.

- LDAPS auf Basis von TLS ist aus Sicherheitsgründen gegenüber LDAP bevorzugt zu konfigurieren.
- Bei aktiviertem TLS für die Verbindung des Clientsystems kann eine LDAPS-Verbindung aufgebaut werden. Die KoCoBox MED+ authentisiert sich hierbei über dasselbe Zertifikat wie bei einer Clientsystem-Verbindung. Basic-Authentication wird nicht unterstützt, weshalb hier die Authentisierung mittels Zertifikats anzuwenden ist.
- Die Verwendung von TLS-Client-Authentication wird dringend empfohlen.
- Wenn TLS-Client-Authentication aktiviert wurde, prüft die KoCoBox MED+ das Zertifikat des LDAP-Clients (z.B. KIM-Client). Dieses Zertifikat wird analog zum Zertifikat für das Clientsystem erstellt und in der KoCoBox MED+ verwaltet.

Hierbei ist zu beachten:

a) Bezüglich der Konnektorspezifikation [gemSpec_Kon, TAB_KON_865] gilt nur LDAP1 als sicher, und zwar ausschließlich mit zusätzlicher Prüfung des Server-Zertifikats.

b) Die Anforderung, den Nutzer über den Verbindungszustand zu informieren, ergibt sich besonders aus dem Umstand, dass bei ANCL_TLS_MANDATORY = Disabled nicht klar ist, ob eine TLS-Verbindung besteht oder nicht. ANCL_CAUT_MANDATORY sorgt ebenfalls für Unklarheit.

2.3.3 Regeln zur Wahl von Passwörtern

Kontext: Kap. 7.5.1 Abschnitt „Clientsysteme“

1. Wenn das Clientsystem eine passwortbasierte Authentisierung implementiert, muss es eine Passwortlänge von mindestens 17 Zeichen unterstützen und die Eingabe der

folgenden Zeichen unterstützen:

- Groß-Kleinbuchstaben (A-Z, a-z),
- Ziffern (0-9),
- Leerzeichen, Punkt, Klammern, Unterstrich.

2. Im Handbuch des Clientsystems muss darauf hingewiesen werden, dass auf unterschiedlichen Clientsystemen, d.h. solchen mit verschiedenen Clientsystem-IDs, unterschiedliche Passwörter verwendet werden müssen. Hierdurch soll für den Fall eines Passwort-Leak die unmittelbare Kompromittierung mehrerer Clientsysteme verhindert werden.

2.3.4 Verwendung von Signaturfunktionalität

Kontext: Kap. 7.5.7

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 MED+ anzeigen.
4. Bei Fehlern im Ablauf der Stapelsignaturerstellung, sofern diese nicht direkt durch eine Nutzeraktion 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 MED+ 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 MED+ 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.