Ergänzungen zum Administratorhandbuch

KoCoBox HSK

Version 1

KoCo Connector GmbH
Dessauer Str. 28/29
10963 Berlin
info@kococonnector.com
www.kococonnector.com

Dokumentenversion:	1.0.0
Dokumentensprache:	deutsch (de)
zuletzt geändert:	30.07.2025

Inhaltsverzeichnis

1 Kontext des Dokuments

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

Die Ergänzungen beziehen sich ausdrücklich auf die Version 1 des Administratorhandbuchs.

Zielgruppe

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

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

2.3 Hinweise für die Anbindung von Primärsystemen

Kontext: Kap. 3.2

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 LDAP-Proxy-Verbindungsparameter

Kontext: Kap. 8.5.1

Die Verbindung zum LDAP-Proxy der KoCoBox HSK folgt in ihren Parametern weitgehend den Einstellungen zur Absicherung der Verbindung zwischen Clientsystem und Konnektor, siehe Kap. 6.5.1.1.

- Bei aktiviertem TLS für die Verbindung des Clientsystems kann eine LDAPS-Verbindung aufgebaut werden. Die KoCoBox HSK authentisiert sich hierbei über dasselbe Zertifikat wie bei einer Clientsystem-Verbindung.
- Die Verwendung von TLS-Client-Authentication wird dringend empfohlen.
- Wenn TLS-Client-Authentication aktiviert wurde, prüft die KoCoBox HSK das Zertifikat des LDAP-Clients (z.B. KIM-Client). Dieses Zertifikat wird analog zum Zertifikat für das Clientsystem erstellt und in der KoCoBox HSK verwaltet.
- Die Anforderung, den Nutzer über den Verbindungszustand zu informieren, ergibt sich aus dem Umstand, dass bei ANCL_CAUT_MANDATORY = Disabled nicht klar ist, ob die TLS-Verbindung authentisch erfolgt.

2.3.2 Regeln zur Wahl von Passwörtern

Kontext: Kap. 6.5.1.1

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.