

## gemSpec\_Kon

In Kapitel 3.4 wird eine neue Anforderung und unter diese neue Anforderung ein informativer Absatz hinzugefügt und im PTSB für den Konnektor dem funktionalen Test zugeordnet:

### A\_21224 - Authentifizierung für Verbindungen zwischen Konnektor und Clientsystemen bei LDAPS

Bei der Verwendung des LDAPS-Proxies im Konnektor, MUSS sich der Konnektor abhängig von der Stellung der Schalter ANCL\_TLS\_MANDATORY, ANCL\_CAUT\_MANDATORY und ANCL\_CAUT\_MODE gemäß der Tabelle TAB\_KON\_xyz verhalten.

**Tabelle 1: TAB\_KON\_860 Konfigurationsvarianten der Verbindungen zwischen Konnektor und Clientsystemen bei LDAPS**

Konfigurationsvariante	ANCL_TLS_MANDATORY	ANCL_CAUT_MANDATORY	ANCL_CAUT_MODE	Bedeutung
LDAPS1	Enabled	Enabled	CERTIFICATE	Der Konnektor akzeptiert vom Clientsystem nur Aufrufe über TLS. Der Konnektor verlangt beim TLS-Handshake die Authentisierung des Clientsystems per Zertifikat.
LDAPS2	Enabled	Enabled	PASSWORD	Der Konnektor akzeptiert vom Clientsystem nur Aufrufe über TLS. Der Konnektor nimmt keine Clientauthentifizierung vor.
LDAPS3	Enabled	Disabled	Irrelevant	Der Konnektor akzeptiert vom Clientsystem nur Aufrufe über TLS. Der Konnektor nimmt keine Clientauthentifizierung vor.
LDAPS4	Disabled	Irrelevant	Irrelevant	Der Konnektor akzeptiert vom Clientsystem sowohl Aufrufe ohne TLS als auch über TLS. Im zweiten Fall sollte der Konnektor das Clientsystem nicht authentifizieren, wenn er es aber für den Sonderfall ANCL_CAUT_MANDATORY=Enabled, ANCL_CAUT_MODE=CERTIFICATE aktuell tut, sehen wir das nicht als Fehler.

<==

Aus der Afo A\_21224 resultiert direkt, dass als Client-Authentisierung für LDAPS nur Client-Zertifikate unterstützt werden müssen. Die Authentisierung mit Username/Passwort wird bei LDAPS nicht unterstützt.

Es sei noch einmal betont, dass TIP1-A\_5009 sich nur auf SOAP und CETP bezieht und TIP1-A\_4516 das Basic-Authentication Verfahren nur für HTTP fordert.

---

## **gemILF\_PS**

---

In Kapitel 4.1.1 unter die Tabelle 3 wird folgender Text hinzugefügt:

Im speziellen Fall der Verwendung des LDAPS-Proxies im Konnektor muss der Konnektor nur die Clientauthentisierung mit Zertifikat (Stufe 4 in der Tabelle Tab\_ILF\_PS\_Konfigurationsvarianten\_HTTP) verpflichtend unterstützen. Die Authentisierung mit Username/Passwort (Stufe 3 in der Tabelle Tab\_ILF\_PS\_Konfigurationsvarianten\_HTTP) bei LDAPS wird für den LDAPS-Proxy im Konnektor nicht unterstützt.

---

## gemSpec\_CM\_KOMLE

---

In Kapitel 4.1.3 wird eine neue Anforderung hinzugefügt auch im PTSB für KIM CM dem funktionalen Test zugeordnet:

### **A\_21223 - Verbindungen mit dem Konnektor bei LDAPS**

Bei der Verwendung des LDAPS-Proxies im Konnektor MUSS das Clientmodul die Vorgaben aus [gemSpec\_Kon#3.4] erfüllen. <==

Die Authentisierung mit Username/Passwort bei LDAPS wird für den LDAPS-Proxy im Konnektor nicht unterstützt. Genaues Verhalten des Konnektors bei der Verwendung des LDAPS-Proxies ist in der Afo A\_21224 in der [gemSpec\_Kon] beschrieben.