

Änderung in gemSpec_Kon

geänderte Anforderung

TIP1-A_4517-03 - Schlüssel und X.509-Zertifikate für die Authentisierung des Clientsystems erzeugen und exportieren sowie X.509-Zertifikate importieren

Der Konnektor MUSS die Erstellung und den Export von Schlüsselpaaren und dazugehörigen X.509-Zertifikaten für Clientsysteme durch den Administrator über das Managementinterface ermöglichen. Hierbei MUSS der Konnektor dem Administrator die Möglichkeit geben, das kryptographische Verfahren gemäß Tabelle TAB_KON_866 auszuwählen. Als Exportformat MUSS PKCS#12 verwendet werden. Die so erstellten Zertifikate werden zu ANCL_CCERT_LIST angefügt.

Zur Sicherung der PKCS#12-Datei MUSS der Konnektor ein intern generiertes starkes Passwort anbieten, jedoch alternativ auch die Vergabe des Passwortes durch den Administrator ermöglichen. Soll vom Administrator ein alternatives Passwort gewählt werden, MUSS der Konnektor dazu Hinweise bzgl. Passwortlänge und Komplexität geben, DARF dahingehend aber NICHT technischen Einschränkungen durchsetzen.

Der Konnektor MUSS dem Administrator ferner den Import von konnektorfremden X.509-Zertifikaten für Clientsysteme über das Managementinterface ermöglichen. Die so importierten Zertifikate werden zu ANCL_CCERT_LIST angefügt.

[<=]

+ informativer Text unter TIP1-A_4517-03

Hintergrund für die Möglichkeit zur uneingeschränkten Vergabe des Passwortes sind ggf. sehr einengende Vorgaben auf Seiten der Primärsysteme, die die PKCS#12 Datei importieren.

Eine valide Umsetzung zur Vergabe des Passwortes für zu exportierende PKCS#12-Dateien wäre ein Input-Feld für den Administrator, welches jegliche Werte akzeptiert, jedoch mit einem starken Passwort vorbefüllt ist.

Da die exportierte PKCS#12-Datei unter der Kontrolle des Administrator ist, liegt die konkrete Passwortstärke für das konnektorgenerierte Passwort im Ermessen des Herstellers. Dabei sollen dennoch der Stand der Technik und die Tatsache, dass mit der exportierten Datei grundsätzlich leicht Brute-Force-Angriffe durchlaufen werden können, berücksichtigt werden.

Die Zuordnungen der obigen Anforderung zu Prüfverfahren bleiben bestehen.

Änderung in gemILF_PS

In Kapitel

1.1.1.1 Client-Authentisierung

(...)

Für die zertifikatsbasierte Client Authentication (mittels konnektoreigenen Zertifikaten) wird im Konnektor ein Zertifikat sowie ein privater Schlüssel erzeugt und exportiert. Es liegt als standardisiertes Format (p12) [PKCS#12] vor, wobei der Schlüsselspeicher und ist durch eine PIN Passwort geschützt ist.

Am Konnektor-Managementinterface erzeugte und von dort exportierte Clientzertifikate ([gemSpec_Kon#3.4], TIP1-A_4517) werden in die Clientsysteme importiert. Das PS importiert und verwaltet das Client-Zertifikat und den dazugehörigen privaten Schlüssel aus der p12-Datei. Dazu muss während des Import-Vorgangs das PIN Passwort des Zertifikats eingegeben werden (Transportsicherung). Anschließend hat das Primärsystem Zugriff auf den für den TLS-Verbindungsaufbau benötigten privaten Schlüssel.

Während des Import-Vorgangs soll das importierte Zertifikat keiner CA-Prüfung unterzogen werden, da es selbstsigniert oder nur über eine PKI des Konnektor-Herstellers prüfbar ist.

...)