
C_12413_Anlage

Inhaltsverzeichnis

1 Änderung in gemSpec_Kon.....	2
---------------------------------------	----------

1 Änderung in gemSpec_Kon

Anforderung A_21811-05 ersetzt Anforderung A_21811-04

A_21811-05 -Vorgaben für generierte und importierte Schlüssel und Zertifikate

Der Konnektor MUSS bezüglich selbst generierter und importierter Schlüssel und Zertifikate für die TLS-Authentisierung gegenüber Primärsystemen und für die Authentisierung des Clientsystems sowie für die Absicherung der Managementschnittstelle die kryptographischen Vorgaben aus [gemSpec_Krypt] durchsetzen und die Verfahren gemäß Tabelle TAB_KON_866 unterstützen.

Tabelle 1 : TAB_KON_866 Unterstützte Verfahren für generierte und importierte Schlüssel und Zertifikate

Verfahren	Neugenerierung bzw. -import	* Bereits generiert/importiert und in Benutzung * mit einem Konfigurationsbacku p importierte Zertifikate
RSA-2048	DARF NICHT generiert oder importiert werden	MUSS nutzbar sein
RSA-3072	MUSS generierbar und importierbar sein	MUSS nutzbar sein
ECC-256 mit NIST-Kurven	MUSS generierbar und importierbar sein	MUSS nutzbar sein
ECC-256 mit brainpool-Kurven	DARF NICHT generiert oder importiert werden	MUSS nutzbar sein

Die [gemSpec_Krypt] führt RSA-3072 nicht auf, macht jedoch allgemeine Vorgaben für RSA, die analog auf RSA-3072 anzuwenden sind.

RSA-2048 sowie Brainpool-Zertifikate dürfen nicht neu angelegt werden. Eine Weiternutzung von RSA-2048- sowie Brainpool-Zertifikaten muss auch nach dem Update der Konnektorfirmware möglich sein. Auch RSA-2048- / Brainpool-Zertifikate, die mit einem Konfigurationsbackup in den Konnektor kommen, müssen genutzt werden können. [\leq , Konnektor Highspeed, Konnektor PTV5Plus, Konnektor PTV6, funkt. Eignung: Test Produkt/FA]

A_21811-04 -Vorgaben für generierte und importierte Schlüssel und Zertifikate

Der Konnektor MUSS bezüglich selbst generierter und importierter Schlüssel und Zertifikate für die TLS-Authentisierung gegenüber Primärsystemen und für die Authentisierung des Clientsystems sowie für die Absicherung der Managementschnittstelle die kryptographischen Vorgaben aus [gemSpec_Krypt] durchsetzen und die Verfahren gemäß Tabelle TAB_KON_866 unterstützen.

Tabelle 2 : TAB KON_866 Unterstützte Verfahren für generierte und importierte Schlüssel und Zertifikate

Verfahren	Neugenerierung bzw. -import	Bereits generiert/importiert und in Benutzung
RSA-2048	DARF NICHT unterstützt werden	soll nicht verwendet werden
RSA-3072	MUSS unterstützt werden	MUSS unterstützt werden
ECC-256 mit NIST-Kurven	MUSS unterstützt werden	MUSS unterstützt werden
ECC-256 mit brainpool-Kurven	DARF NICHT unterstützt werden	soll nicht verwendet werden

Die [gemSpec_Krypt] führt RSA-3072 nicht auf, macht jedoch allgemeine Vorgaben für RSA, die analog auf RSA-3072 anzuwenden sind.

RSA-2048 sowie Brainpool-Zertifikate dürfen bei der neuen Anlage von Zertifikaten nicht verwendet werden. Eine Weiternutzung von RSA-2048 sowie Brainpool-Zertifikaten nach einem Update oder dem Import eines Konfigurationsbackups ist zulässig.

【<=,Konnektor Highspeed, Konnektor PTV5Plus, Konnektor PTV6,funkt. Eignung: Test Produkt/FA】