

---

C\_12622\_Anlage

---

Inhaltsverzeichnis

1 Änderungsbeschreibung.....2

2 Änderung in gemSpec\_VPN\_ZugD.....3

---

## 1 Änderungsbeschreibung

---

Im Rahmen der Registrierung der Konnektoren beim VPN-Zugangsdienst werden die C.VPN.NK Zertifikate und die C.HCI.OSIG Zertifikate in einer Datenbank im Registrierungsserver gespeichert. Der VPN-Zugangsdienst prüft zyklischen die gespeicherten C.VPN.NK und der C.HCI.OSIG Zertifikate in der Datenbank auf Gültigkeit und Laufzeit. Die bei dieser Überprüfung ermittelten ungültigen Zertifikate werden aus der Datenbank entfernt. Zudem werden die zu dieser Registrierung vorhandenen IPsec-Verbindungen beendet. Dadurch verliert der Konnektor die TI-Verbindung und kann auch keine neue gesicherte Verbindung etablieren.

Es gibt bis einschließlich PTV5 Konnektorprodukte, die die Registrierungen in der Kombination ECC-basiertes C.VPN.NK Zertifikat mit RSA-basierter SMC-B-Signatur durchgeführt haben. Dadurch besteht das Risiko, dass zum Zeitpunkt der Sperrung der RSA-basierten C.HCI.OSIG Zertifikate im Rahmen der RSA2ECC Migration, diese Registrierungen durch die zyklische Prüfung im VPN-Zugangsdienst als ungültig erkannt und entsprechend der implementierten Abläufe entfernt werden.

Daher soll die zyklische Prüfung modifiziert werden, so dass die Prüfung der Zertifikate nach den Parametern Revoke und zeitliche Laufzeit konfigurativ ein und ausgeschaltet werden kann. Durch diese Schalter ist es dann möglich die zyklische Prüfung auszusetzen, so dass Registrierungen mit einem RSA-basierten C.HCI.OSIG Zertifikat nicht aus der Registrierungsdatenbank entfernt werden.

Eine im Bedarfsfall notwendige Sperrung des TI-Zugangs wird in diesem Fall über organisatorische Maßnahmen durchgesetzt.

## 2 Änderung in gemSpec\_VPN\_ZugD

*Im Kapitel 4.1.6 werden die folgenden neuen Anforderungen aufgenommen.*

### **A\_28812 -VPN-Zugangsdienst, zyklische Zertifikatsprüfung von C.NK.VPN und C.HCI.OSIG**

Ist die Zertifikatsprüfung durch Konfigurationsschalter gemäß [A\_28825] aktiviert, MUSS der VPN-Zugangsdienst die Gültigkeit aller bei ihm im Rahmen von Konnektorregistrierungen verwendeten C.NK.VPN (SMC-K-Zertifikat) und C.HCI.OSIG (SM-B-OSIG-Zertifikat) gemäß TUC\_PKI\_002 und TUC\_PKI\_006 einmal täglich prüfen. Die Prüfung der Zertifikate muss gleichmäßig verteilt über das Prüfintervall erfolgen.  
[<=,Zugangsdienst,funkt. Eignung: Test Produkt/FA]

### **A\_28813 -VPN-Zugangsdienst, Konfigurationsparameter der zyklische Prüfung**

Der VPN-Zugangsdienst MUSS für die zyklische Prüfung von Zertifikaten zwei technisch voneinander unabhängige Konfigurationsparameter (Schalter) bereitstellen, um die Prüflöge zu steuern:

- Schalter 1: Steuert die Prüfung der zeitlichen Gültigkeit
- Schalter 2: Steuert die Prüfung des Revocation-Status

Die Schalter MÜSSEN jeweils zwischen den Zuständen "aktiv" (ein) und "inaktiv" (aus) umschaltbar sein. Der jeweils eingestellte Zustand MUSS persistent gespeichert werden.  
[<=,Zugangsdienst,funkt. Eignung: Test Produkt/FA]

### **A\_28825 -VPN-Zugangsdienst, Kombination der Schalter und Standardeinstellung**

Der VPN-Zugangsdienst MUSS auf Grundlage der in [A\_28813] definierten Schalter die zyklische Prüfung gemäß [A\_28812], [A\_25743 und [A\_25864] durchführen, dabei sind die Fallunterscheidungen und Kombination der Schalterzustände zu beachten. In der Standardeinstellung MÜSSEN sich Schalter 1 und Schalter 2 im Zustand "aktiv" befinden.

**Table 1 Kombination\_Zustände\_Schalter\_Prüfungen**

Schalter 1	Schalter 2	Standardeinstellung	Prüfung
aktiv	inaktiv	./.	zeitlichen Gültigkeit gemäß TUC_PKI_002
inaktiv	aktiv	./.	Revocation-Status gemäß TUC_PKI_006
aktiv	aktiv	Default	zeitlichen Gültigkeit gemäß TUC_PKI_002 und Revocation-Status gemäß

			TUC_PKI_006
<b>inaktiv</b>	inaktiv	./.	keine Prüfung

61  
62 **[<=,Zugangsdienst,funkt. Eignung: Test Produkt/FA]**

63 **A\_28840 -VPN-Zugangsdienst, Anweisung zur Konfiguration der Schalter**

64 Der VPN-Zugangsdienst MUSS die Konfiguration der Schalter nach Weisung und gemäß  
65 den Einstellvorgaben der gematik anpassen. **[<=,Zugangsdienst,funkt. Eignung:**  
66 **Herstellererklärung]**

67  
68 *Im Kapitel 4.1.6 entfällt die Anforderung TIP1-A\_5389 und wird aus der gemSpec\_VPN-*  
69 *Zugangsdienst entfernt.*

70 **TIP1-A\_5389 -VPN-Zugangsdienst, zyklische Prüfung der C.NK.VPN und**  
71 **C.HCI.ÖSIG Zertifikate**

72 Der VPN-Zugangsdienst MUSS die Gültigkeit aller bei ihm im Rahmen von  
73 Konnektorregistrierungen verwendeten C.NK.VPN (SMC-K-Zertifikat) und C.HCI.ÖSIG (SM-  
74 B-ÖSIG-Zertifikat) gemäß TUC\_PKI\_002 und TUC\_PKI\_006 einmal täglich prüfen.  
75 Die Prüfung der Zertifikate muss gleichmäßig verteilt über das Prüfintervall erfolgen.  
76 **[<=,Zugangsdienst,funkt. Eignung: Test Produkt/FA]**