

Laufzeit- verlängerung

Vorstellung des technischen Ablaufs bei
secunet Konnektoren



Schritte zum neuen Zertifikat ...

Voraussetzung: gSMC-K Zertifikate vor 01.01.2021 ausgestellt

1. Aktualisierung der Firmware auf PTV5 WR3
 - voraussichtlich ab 08/2023 verfügbar
2. Einspielen der Laufzeitverlängerungs-Lizenz
3. Abruf der verlängerten Zertifikate vom TSP mittels ICCSN
 - Gültigkeit C.NK.VPN-Zertifikates < 180 Tage = Tägliche Abfragung nach verlängerten Zertifikaten
 - Offline-Szenario: Manueller Import von Zertifikaten
4. Re-Registrierung der neuen Zertifikaten beim VPN-ZugD
 - Default: Manueller Vorgang
 - Umstellung auf „automatisch“ möglich
5. Aktivierung neuer Zertifikate gegenüber Clientsystemen

- Die neuen, laufzeitverlängerten Zertifikate sind im sicheren Speicher der Konnektors und nicht mehr auf der gSMC-k gespeichert
- Der private Schlüssel wird nach wie vor von der gSMC-K bezogen
- Neue Zertifikate sind bis 31.12.2025 gültig

Durchführung in der Konnektor Oberfläche

Schritt-für-Schritt Anleitung

Durchführung secunet konektor – Teil 1

RU/TU

System konnektor

Laufzeitverlängerung

Im Rahmen der Laufzeitverlängerung stellt der TSP X.509 nonQES für Komponenten Zertifikate in der TI für den Abruf durch die Konnektoren bereit.

1. Schritt: Abruf der erneuerten Zertifikate vom TSP

Im Rahmen der Laufzeitverlängerung stellt der TSP X.509 nonQES für Komponenten Zertifikate in der TI für den Abruf durch die Konnektoren bereit. Der Konnektor kann die erneuerten Zertifikate für seine gSMC-K(s) abrufen und anschließend verwenden. Die Verwendung der alten Zertifikate bleibt bis zu ihrem Ablaufdatum möglich.

Der Konnektor startet 180 Tage vor Ablauf des aktuell verwendeten C.NK.VPN-Zertifikats automatisch den Zertifikatserneuerungsprozess. Solange die Zertifikate noch nicht vollständig erfolgreich erneuert wurden, versucht der Konnektor genau einmal täglich neue Zertifikate zu beziehen.

Der Zertifikatserneuerungsprozess kann optional manuell durch den Administrator angestoßen werden.

Zertifikate zur Laufzeitverlängerung aus der TI herunterladen ... **ERLEDIGT** ○

2. Schritt (optional): Manueller Import von Zertifikatspaketen aus lokaler Datenquelle

Es kann vorkommen, dass Konnektoren dauerhaft offline sind (z.B. Reserve insbesondere in Krankenhäusern).

In diesem Fall kann ein Administrator manuell neue gSMC-K-Zertifikate einbringen, auch wenn die ursprünglichen Zertifikate bereits abgelaufen sind.

Zip-Dateien zur Laufzeitverlängerung hochladen ... **ERLEDIGT** >

3. Schritt: Backup mit erneuerten Zertifikaten erstellen

Home
Netzwerk
Praxis
Diagnose
System
VPN
Module
Suche
Benutzer

Allgemein
Zertifikate
Zeit
Aktualisierungen
Backup
Version
Missbrauchserkennung
Laufzeitverlängerung

Durchführung secunet konektor – Teil 2

RU/TU

System konnektor

Laufzeitverlängerung

3. Schritt: Backup mit erneuerten Zertifikaten erstellen

Es wird empfohlen, nach erfolgreicher Erneuerung der Zertifikate ein Backup zu erstellen

Backup zu erstellen („System > Backup > Backup erstellen“) ... [🔗](#)

4. Schritt: Re-Registrierung der erneuerten Zertifikate beim VPN-Zugangsdienst

Für die Verwendung gegenüber dem VPN-Zugangsdienst ist dafür eine Re-Registrierung mit dem neuen NK.VPN-Zertifikat notwendig.

Re-Registrierung der erneuerten Zertifikate beim VPN-Zugangsdienst (siehe „VPN > VPN-Zugangsdienst“) ... **ERLEDIGT** [🔗](#)

5. Schritt: Auswahl des zu nutzenden Zertifikats gegenüber dem Clientsystem

Der Administrator muss die Verwendung von erneuerten C.AK.AUT-Zertifikaten für die Authentisierung des Konnektors gegenüber den Clientsystemen manuell aktivieren.

Eine Aktivierung ist nicht erforderlich, wenn der Konnektor ein Software-Zertifikat für die Authentisierung gegenüber den Clientsystemen verwendet.

Auswahl zu nutzendes Zertifikat gegenüber den Clientsystemen (siehe „Praxis > Clientsysteme > Clientsystem-Einstellungen“) ... **OFFEN** [🔗](#)

6. Schritt: Erneutes Backup mit erneuerten Zertifikaten erstellen

Durchführung secunet konektor – Teil 3

RU/TU

System
konnektor

Netzwerk

Praxis

Diagnose

System

VPN

Module

Suche

Benutzer

Laufzeitverlängerung

5. Schritt: Auswahl des zu nutzenden Zertifikats gegenüber dem Clientsystem

Der Administrator muss die Verwendung von erneuerten C.AK.AUT-Zertifikaten für die Authentisierung des Konnektors gegenüber den Clientsystemen manuell aktivieren.
Eine Aktivierung ist nicht erforderlich, wenn der Konnektor ein Software-Zertifikat für die Authentisierung gegenüber den Clientsystemen verwendet.

Auswahl zu nutzendes Zertifikat gegenüber den Clientsystemen (siehe „Praxis > Clientsysteme > Clientsystem-Einstellungen“ ...) **OFFEN**

6. Schritt: Erneutes Backup mit erneuerten Zertifikaten erstellen

Es wird empfohlen, nach vollständiger Aktivierung der laufzeitverlängerten Zertifikate erneut ein Backup zu erstellen

Backup zu erstellen („System > Backup > Backup erstellen“) ...

Verwendete Zertifikate

Nach der erfolgten Erneuerung der unten aufgeführten Zertifikate kann ein Neustart erforderlich sein, damit der Konnektor die erneuerten Zertifikate nutzen kann. Die unten angezeigten Werte zeigen den aktuellen Zustand an. Erneuerte Zertifikate werden evtl. erst nach erfolgreichem Neustart berücksichtigt.

C2C der Signaturanwendungskomponente mit den HBAs **C.SAK.AUTD_CVC_ECC | ERNEUERT**

Durchführung secunet konektor – Teil 4

RU/TU

System konnektor

Laufzeitverlängerung

6. Schritt: Erneutes Backup mit erneuerten Zertifikaten erstellen

Es wird empfohlen, nach vollständiger Aktivierung der laufzeitverlängerten Zertifikate erneut ein Backup zu erstellen

Backup zu erstellen („System > Backup > Backup erstellen“) ...

Verwendete Zertifikate

Nach der erfolgten Erneuerung der unten aufgeführten Zertifikate kann ein Neustart erforderlich sein, damit der Konektor die erneuerten Zertifikate nutzen kann. Die unten angezeigten Werte zeigen den aktuellen Zustand an. Erneuerte Zertifikate werden evtl. erst nach erfolgtem Neustart berücksichtigt.

C2C der Signaturanwendungskomponente mit den HBAs	C.SAK.AUTD_CVC_ECC ERNEUERT	
TLS zu den Kartenterminals	C.SAK.AUT_RSA ERNEUERT	C.SAK.AUT_ECC ERNEUERT
TI und SIS VPN-Tunnel	C.NK.VPN_RSA ERNEUERT	C.NK.VPN_ECC ERNEUERT
TLS zu den Clientsystemen	C.AK.AUT_RSA ORIGINAL	C.AK.AUT_ECC ORIGINAL

Die Darstellung entspricht: Strecke „Zertifikatstyp | Erneuerungsstatus“. Die Wertemenge für den Erneuerungsstatus ist ORIGINAL/ERNEUERT/SOFTWARE.

secunet