

Workaround Update CA

Ausgangslage:

Konnektor ist frisch installiert, Verbindung zum Internet besteht.

Initialpasswort wurde geändert. Der Hostname wurde geändert.

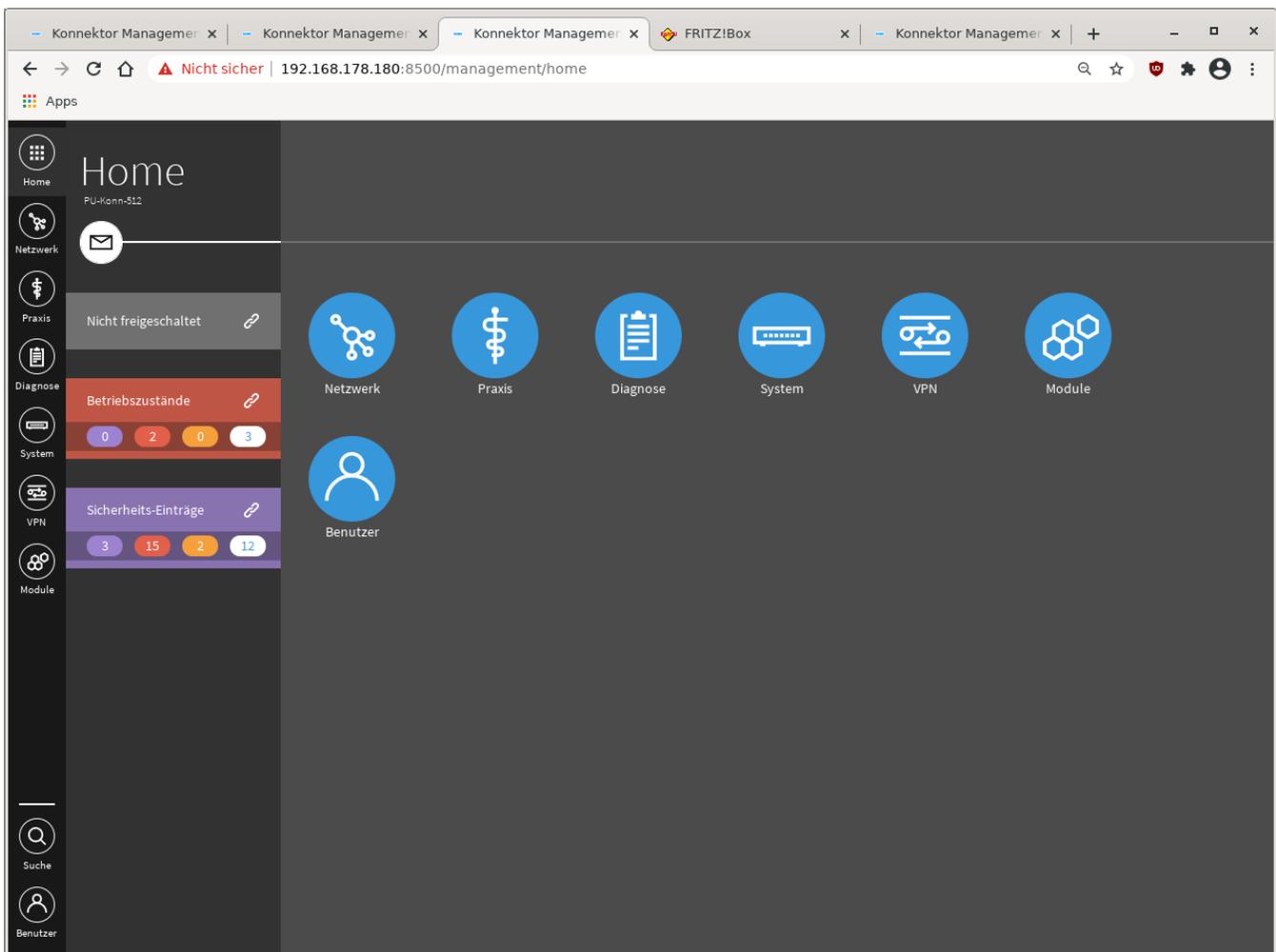
WAN-DHCP-Client deaktiviert, WAN deaktiviert, LAN-DHC deaktiviert und feste IP-Adresse gesetzt. (optional)

Der Konnektor wurde dann neu gestartet, um alle Änderungen zu übernehmen und die Anzeige "Betriebszustände" zu aktualisieren.

Die CA-Wechsel-TSL und die aktuelle TSL müssen offline bereit liegen.

Als CA-Wechsel-TSL kommen infrage: Sequenz-Nr 461, gültig bis 13.01.2023 bis Nr 464, gültig bis 27.02.2023.

Die TSL 461 kann unter folgendem Link heruntergeladen werden: <https://download.tsl.ti-dienste.de/tsl-va-wechsel/>



Hinweis: Die Bilder sind teilweise auf RU-Konnektoren entstanden, wo der CA-Wechsel früher stattgefunden hat. In der PU steht er zum Zeitpunkt der Erstellung dieses Dokumentes noch bevor. Kalenderdaten und Sequenznummern sind daher fiktiv.

Nach dem ersten Start zeigt sich folgendes Bild:

Diagnose Status

Home
Netzwerk
Praxis
Diagnose
System
VPN
Module

Status
Protokolle
Gespeicherte Suchen
Berichte
Abonnements
Administration
Diagnose-Kit

Betriebszustände

20.01.2023 12:23:43	Vertrauensanker abgelaufen ...	Schwerwiegend	Sicherheit
20.01.2023 12:23:10	CRL abgelaufen ...	Schwerwiegend	Sicherheit
20.01.2023 12:23:10	Keine Online-Verbindung ...	Fehler	Technisch
20.01.2023 12:23:12	Keine SIS Verbindung ...	Fehler	Technisch
20.01.2023 12:23:12	Keine TI Verbindung ...	Fehler	Technisch
20.01.2023 12:23:10	IP-Adressen fehlen ...	Fehler	Sicherheit
20.01.2023 12:23:43	TSL-Aktualisierung fehlgeschlagen ...	Info	Technisch

Diagnose Status Vertrauensanker abgelaufen

Home
Netzwerk
Praxis
Diagnose
System
VPN
Module

Status
Protokolle
Gespeicherte Suchen
Berichte
Abonnements
Administration
Diagnose-Kit

Gültigkeit des Vertrauensankers ist abgelaufen.

zum Bereich: Zertifikate ...

Auswirkungen

Die Kommunikation mit Kartenterminals sowie der Aufbau von VPN-Verbindungen in die TI/SIS werden unterbunden.

Handlungsanweisungen

Aktualisieren Sie den Trustanchor.

Details

Fehlerschlüssel EC_TSL_Trust_Anchor_Out_Of_Date

Letzte Änderung 17.02.2023 11:19:37

Schweregrad Schwerwiegend

Art des Fehlers Sicherheit

Bedeutung Gültigkeit des Vertrauensankers ist abgelaufen

ExpiringDateTrustAnchor 17.02.2023 10:18:48.000 UTC

Die Einträge im System- und Sicherheitslog zeigen, dass die aktuelle TSL nicht akzeptiert wird:

Protokolle

1

2

3

4



Suchfilter anpassen ...

Operative Einträge (SYSTEM)

Info

20.01.2023 14:55:43

Suche wiederholen



Suche speichern ...



Zeit	Level	Nachricht	
20.01.2023 18:03:14.513	ERROR	code=42033;name=CANT_IMPORT_BNETZA_VL_FILE;text=Import der BNetzA-VL-Datei fehlgeschlagen;Vorgangsnummer=90ba15db-a76a-4763-be23-d5d6d6b4567f	>
20.01.2023 18:03:14.513	ERROR	code=1006;name=TSL_DOWNLOAD_ERROR;text=TSL-Downloadadressen wiederholt nicht erreichbar;detail=Konnektor ist nicht mit der TI Verbunden;Vorgangsnummer=90ba15db-a76a-4763-be23-d5d6d6b4567f	>
20.01.2023 18:03:14.501	ERROR	code=42039;name=TSL_SIGNATURE_INTERNET_INVALID;text=Signatur der Internet-TSL ist ungültig bgzw. konnte nicht erfolgreich geprüft werden;Vorgangsnummer=90ba15db-a76a-4763-be23-d5d6d6b4567f	>
20.01.2023 18:02:14.641	ERROR	code=42033;name=CANT_IMPORT_BNETZA_VL_FILE;text=Import der BNetzA-VL-Datei fehlgeschlagen;Vorgangsnummer=90ba15db-a76a-4763-be23-d5d6d6b4567f	>
20.01.2023 18:02:14.641	ERROR	code=1006;name=TSL_DOWNLOAD_ERROR;text=TSL-Downloadadressen wiederholt nicht erreichbar;detail=Konnektor ist nicht mit der TI Verbunden;Vorgangsnummer=90ba15db-a76a-4763-be23-d5d6d6b4567f	>
20.01.2023 18:02:14.626	ERROR	code=42039;name=TSL_SIGNATURE_INTERNET_INVALID;text=Signatur der Internet-TSL ist ungültig bgzw. konnte nicht erfolgreich geprüft werden;Vorgangsnummer=90ba15db-a76a-	>

Protokolle

1

2

3



Suchfilter anpassen ...

Sicherheitseinträge

Info

20.01.2023 14:55:43

Suche wiederholen



Suche speichern ...



Zeit	Level	Nachricht	
20.01.2023 18:04:15.114	ERROR	code=4127;name=CANT_IMPORT_TSL_FILE;text=Import der TSL-Datei fehlgeschlagen;Vorgangsnummer=90ba15db-a76a-4763-be23-d5d6d6b4567f	>
20.01.2023 18:04:15.114	WARNING	code=1009;name=VALIDITY_WARNING_2;text=Überschreitung des Elements NextUpdate um TSL-Grace-Period;Vorgangsnummer=90ba15db-a76a-4763-be23-d5d6d6b4567f	>
20.01.2023 18:04:15.114	ERROR	code=1024;name=CERTIFICATE_NOT_VALID_MATH;text=Zertifikats-Signatur ist mathematisch nicht gültig.;Vorgangsnummer=90ba15db-a76a-4763-be23-d5d6d6b4567f	>
20.01.2023 18:03:14.501	ERROR	code=4127;name=CANT_IMPORT_TSL_FILE;text=Import der TSL-Datei fehlgeschlagen;Vorgangsnummer=90ba15db-a76a-4763-be23-d5d6d6b4567f	>
20.01.2023 18:03:14.501	WARNING	code=1009;name=VALIDITY_WARNING_2;text=Überschreitung des Elements NextUpdate um TSL-Grace-Period;Vorgangsnummer=90ba15db-a76a-4763-be23-d5d6d6b4567f	>
20.01.2023 18:03:14.501	ERROR	code=1024;name=CERTIFICATE_NOT_VALID_MATH;text=Zertifikats-Signatur ist mathematisch nicht gültig.;Vorgangsnummer=90ba15db-a76a-4763-be23-d5d6d6b4567f	>
20.01.2023 18:02:14.626	ERROR	code=4127;name=CANT_IMPORT_TSL_FILE;text=Import der TSL-Datei fehlgeschlagen;Vorgangsnummer=90ba15db-a76a-4763-be23-d5d6d6b4567f	>

FW 5.1.2 nach erstem Start:

The screenshot shows the 'Diagnose' status page. The left sidebar contains navigation options: Home, Netzwerk, Praxis, Diagnose (selected), System, VPN, and Module. The main content area is titled 'Status' and 'Betriebszustände'. It displays a list of operational states with columns for timestamp, description, severity, and security level.

Timestamp	Description	Severity	Security Level
22.01.2023 16:02:11	TSL Vertrauensanker abgelaufen ...	Schwerwiegend	Sicherheit
22.01.2023 16:01:42	CRL abgelaufen ...	Schwerwiegend	Sicherheit
22.01.2023 16:01:42	Keine Online-Verbindung ...	Fehler	Technisch
22.01.2023 16:01:44	Keine SIS Verbindung ...	Fehler	Technisch
22.01.2023 16:01:44	Keine TI Verbindung ...	Fehler	Technisch
22.01.2023 16:01:42	IP-Adressen fehlen ...	Fehler	Sicherheit
22.01.2023 16:01:44	Sicherheitsniveau des RSA-TLS-Server-Zertifikats gering ...	Info	Sicherheit
22.01.2023 16:02:11	TSL-Aktualisierung fehlgeschlagen ...	Info	Technisch

Die TSL wird wegen des abgelaufenen Vertrauensankers nicht aktualisiert, die CRL hingegen schon:

The screenshot shows the 'System' certificates page. The left sidebar contains navigation options: Home, Netzwerk, Praxis, Diagnose (selected), System, VPN, and Module. The main content area is titled 'Zertifikate' and 'TSL Informationen'. It displays details for a specific TSL certificate, including its ID, type, sequence number, validity period, and download URIs.

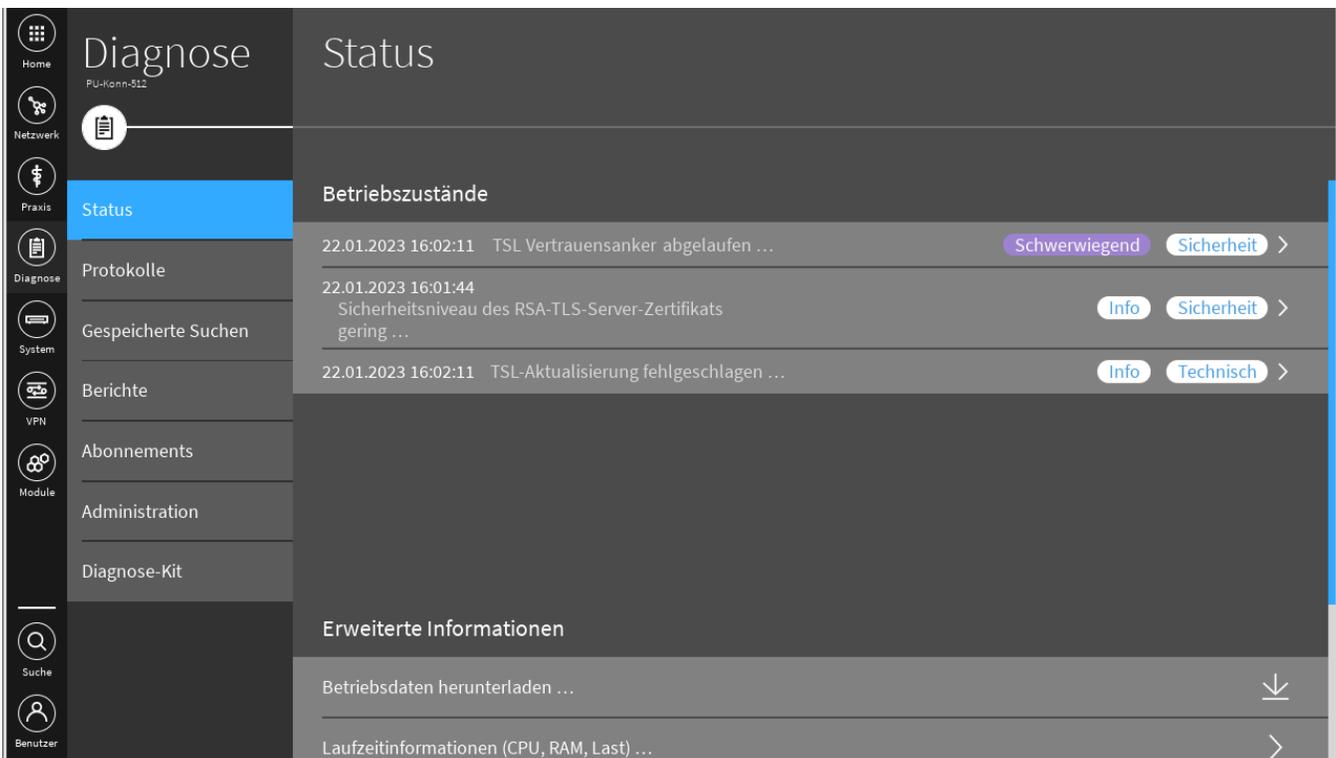
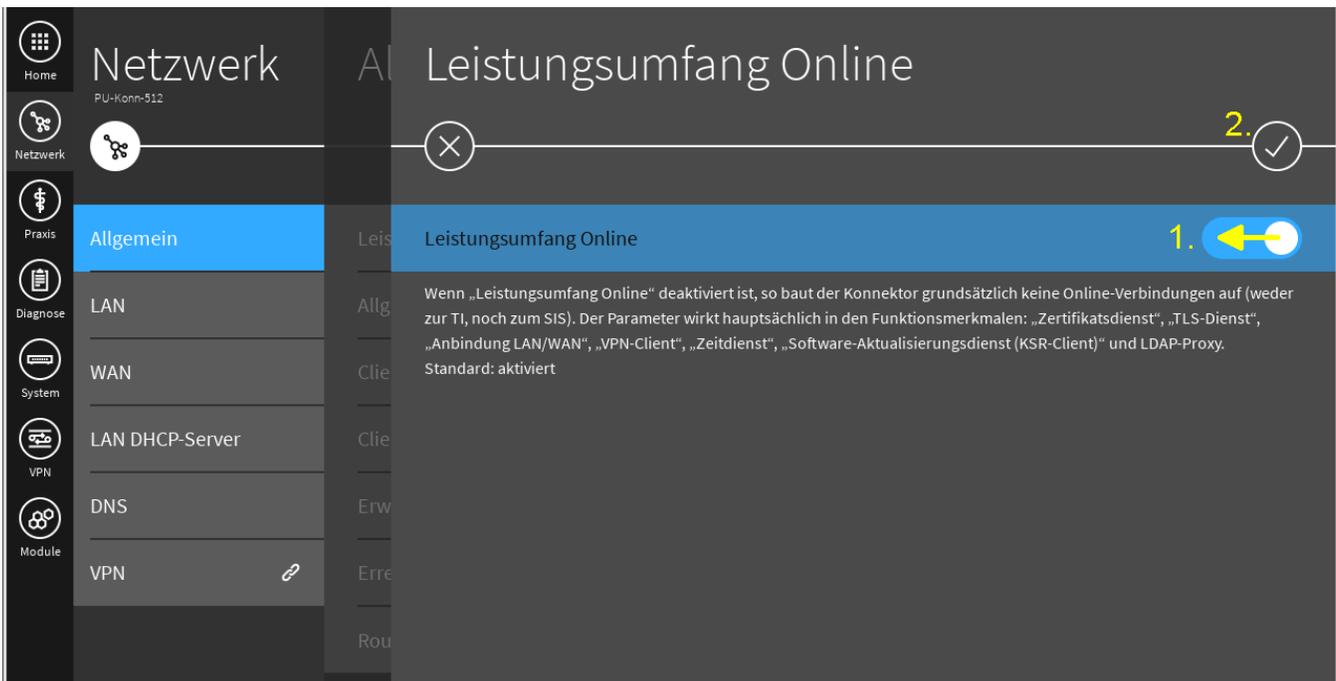
Field	Value
TSL herunterladen	ID345420220827230001Z ...
TSL-Typ	RSA
Sequenznummer	454
Gültig-Bis-Zeitpunkt der TSL	27.09.2022 1:00:01
Top-Level-Domain Namensraum TI	telematik.
CRL Download URI	http://download.crl.ti-dienste.de/crl/vpnk-ca1.crl
Primäre TSL Download URI	http://download.tsl.telematik/TSL.xml
Backup TSL Download URI	http://download-bak.tsl.telematik/TSL.xml
Feste Backup TSL Download URI im Internet (Hostname)	http://download.crl.ti-dienste.de/TSL-RSA/TSL
Feste Backup TSL Download URI im Internet (IP-Adresse)	http://84.17.168.212/TSL-RSA/TSL



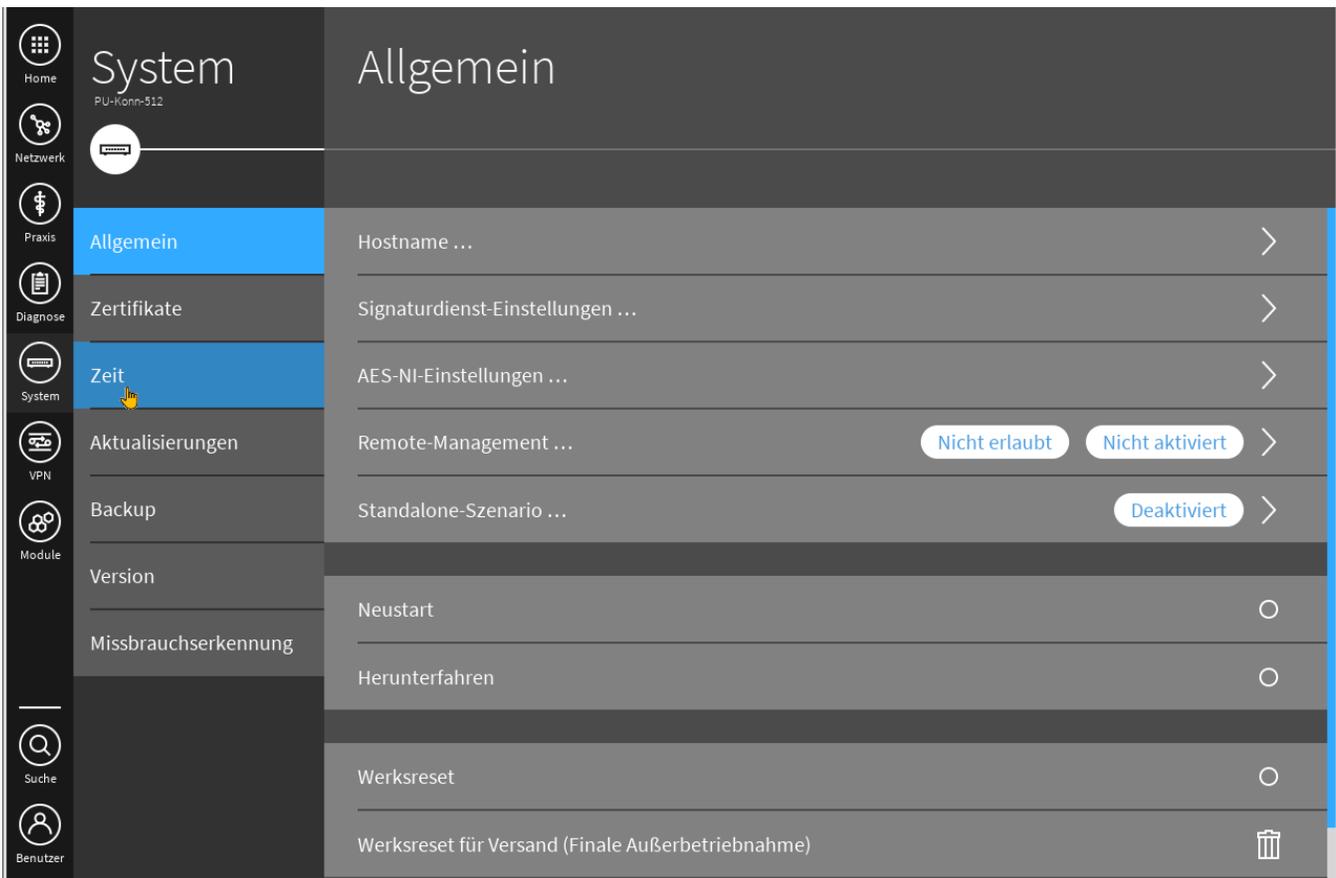
TSL für den CA-Wechsel einbringen:

Um die TSL manuell hochladen zu können, muss der "Leistungsumfang" offline geschaltet werden:





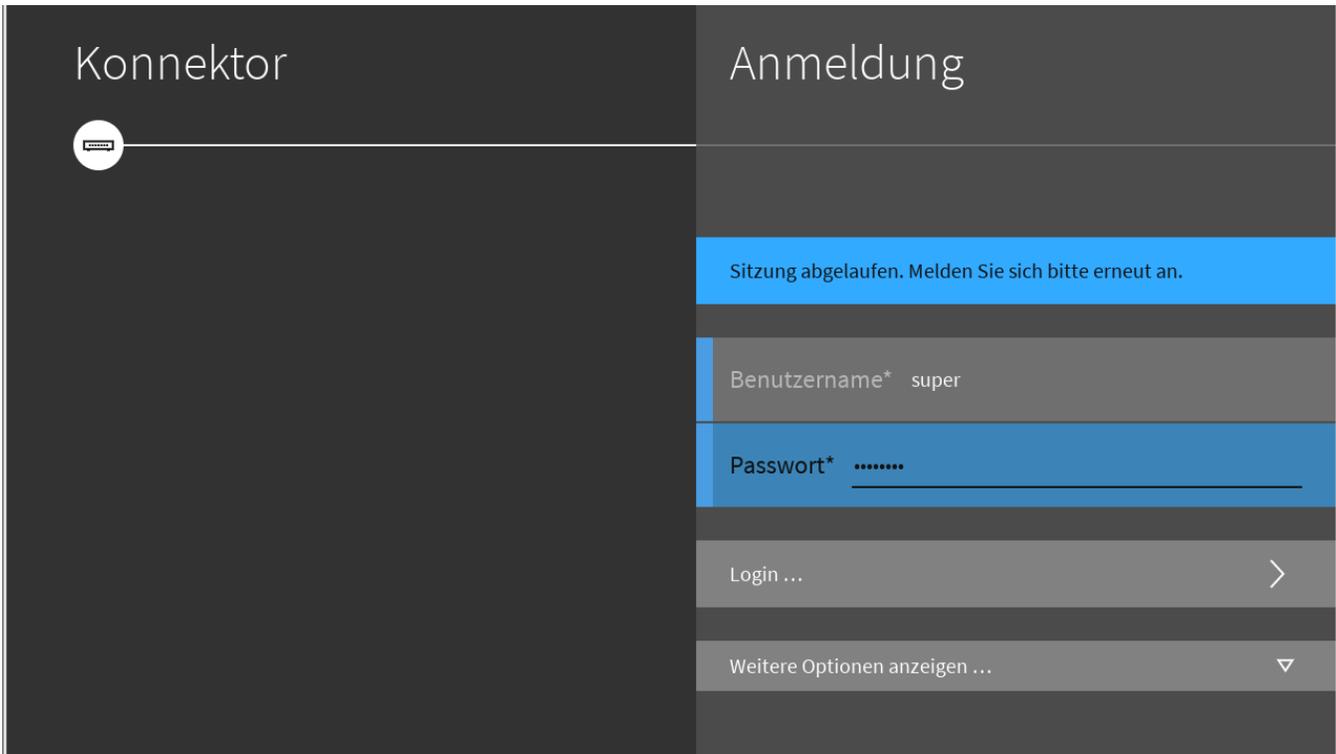
Zunächst muss die Systemzeit der Konnektors zurückgestellt werden, um diese TSL aktivieren zu können:



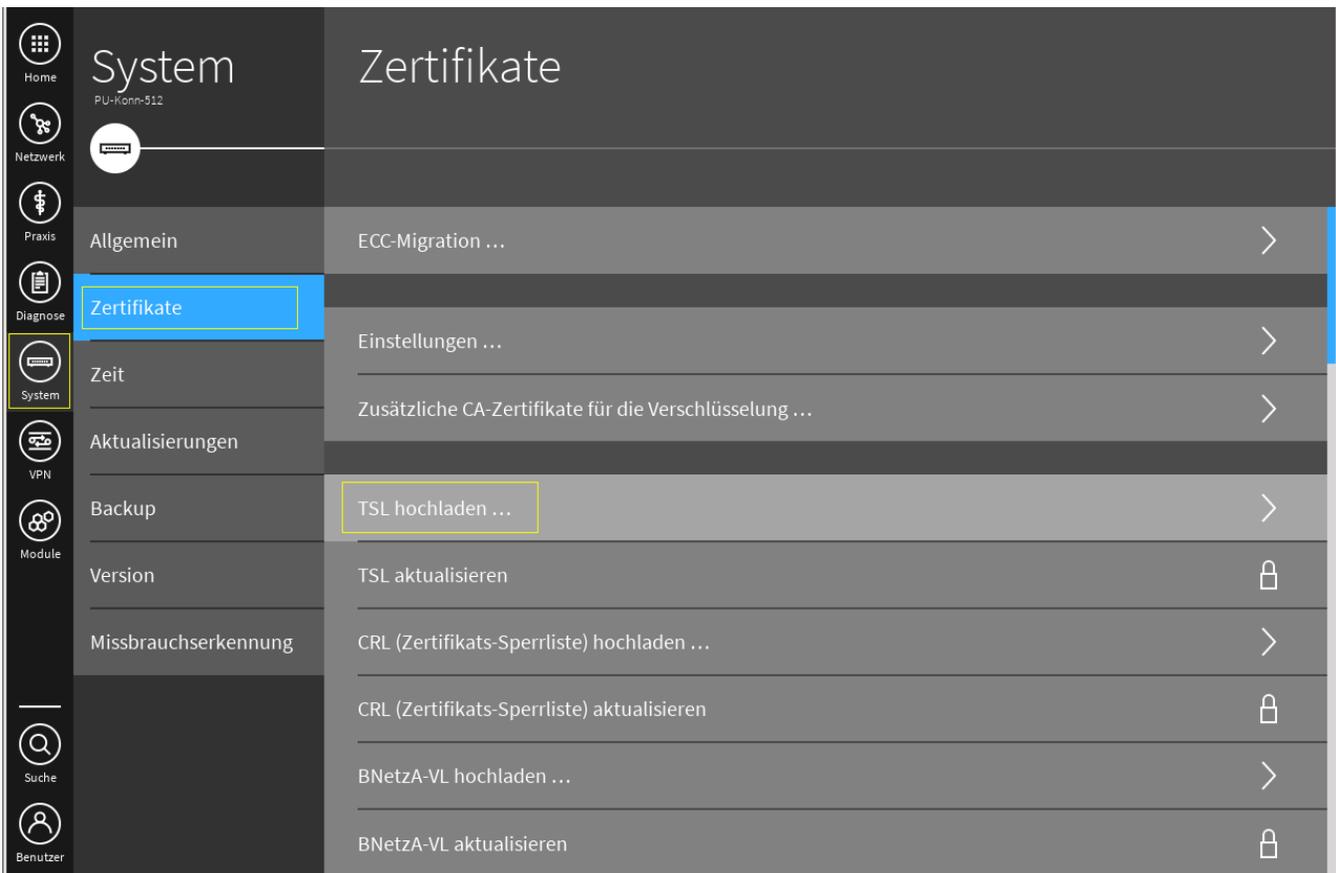
Den Konnektor auf ein Datum innerhalb der Gültigkeitsfrist der TSL und des alten Vertrauensankers einstellen:

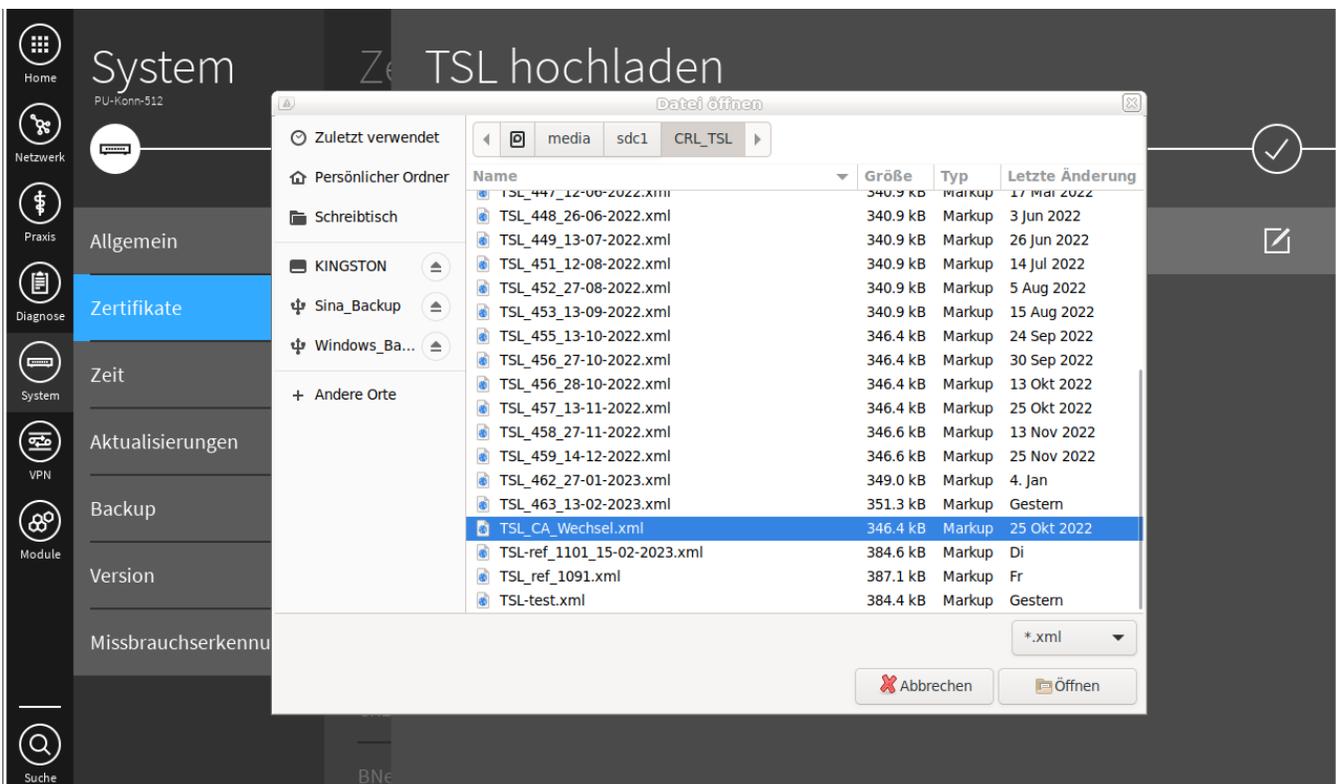
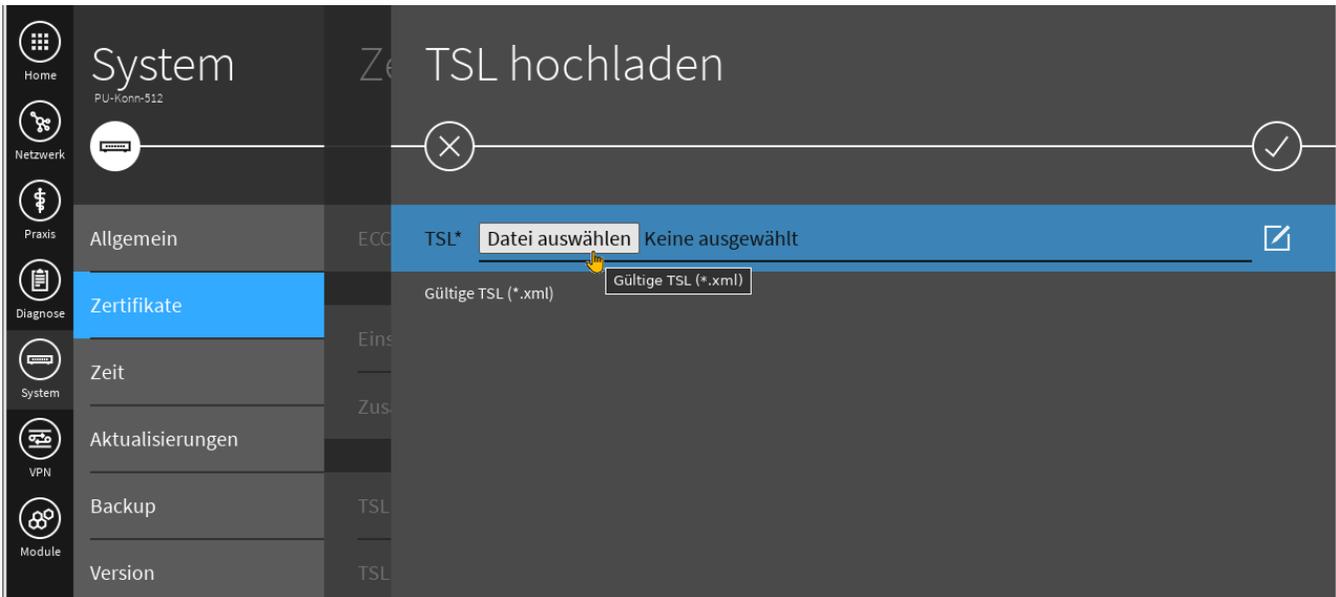


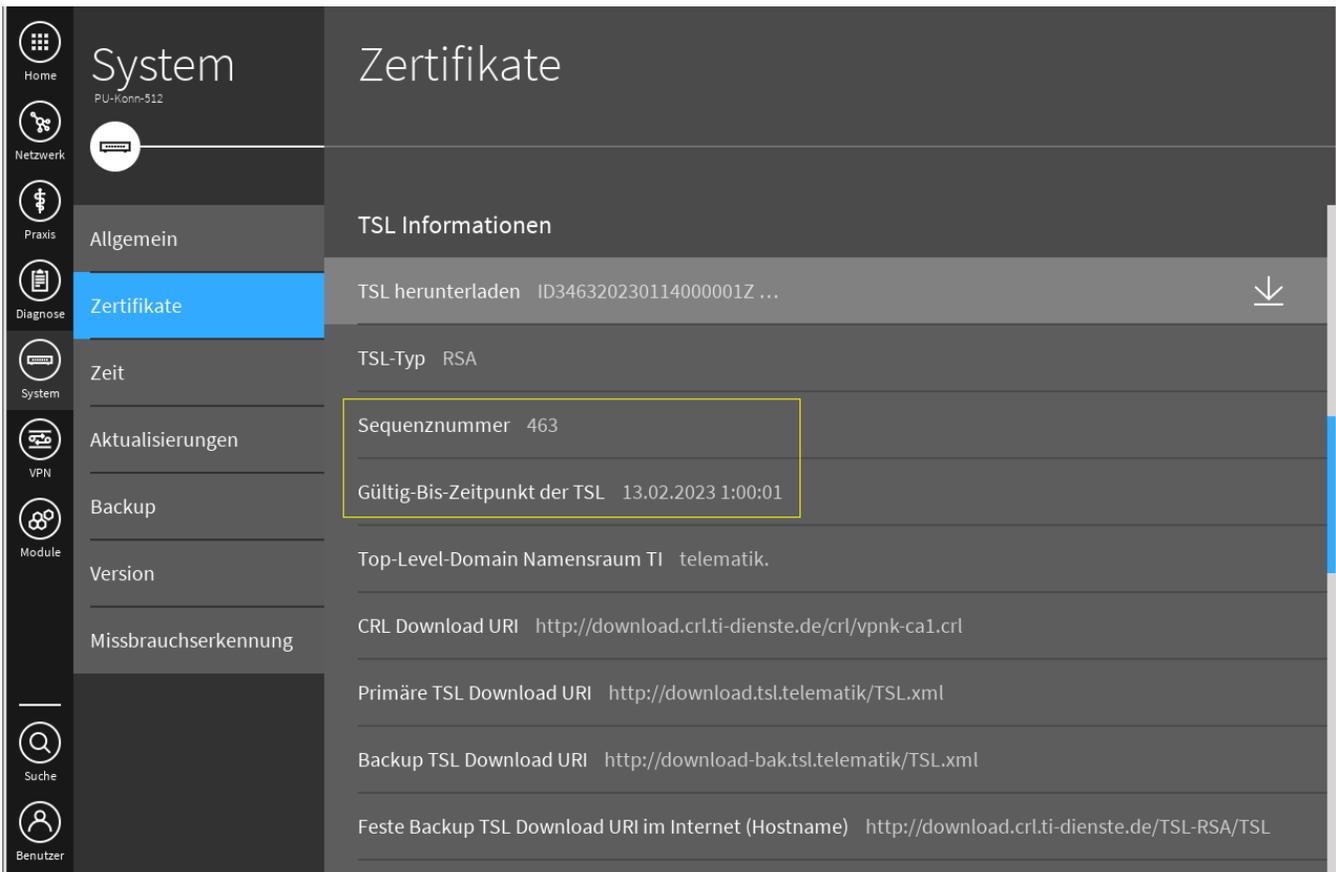
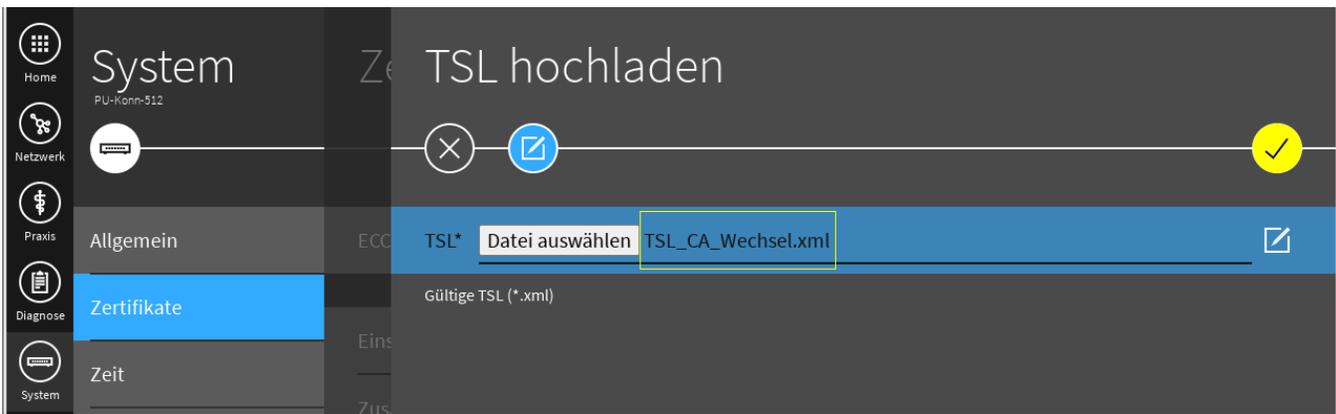
Anschließend muss man sich erneut anmelden. Danach kann die CA-Wechsel-TSL hochgeladen werden.



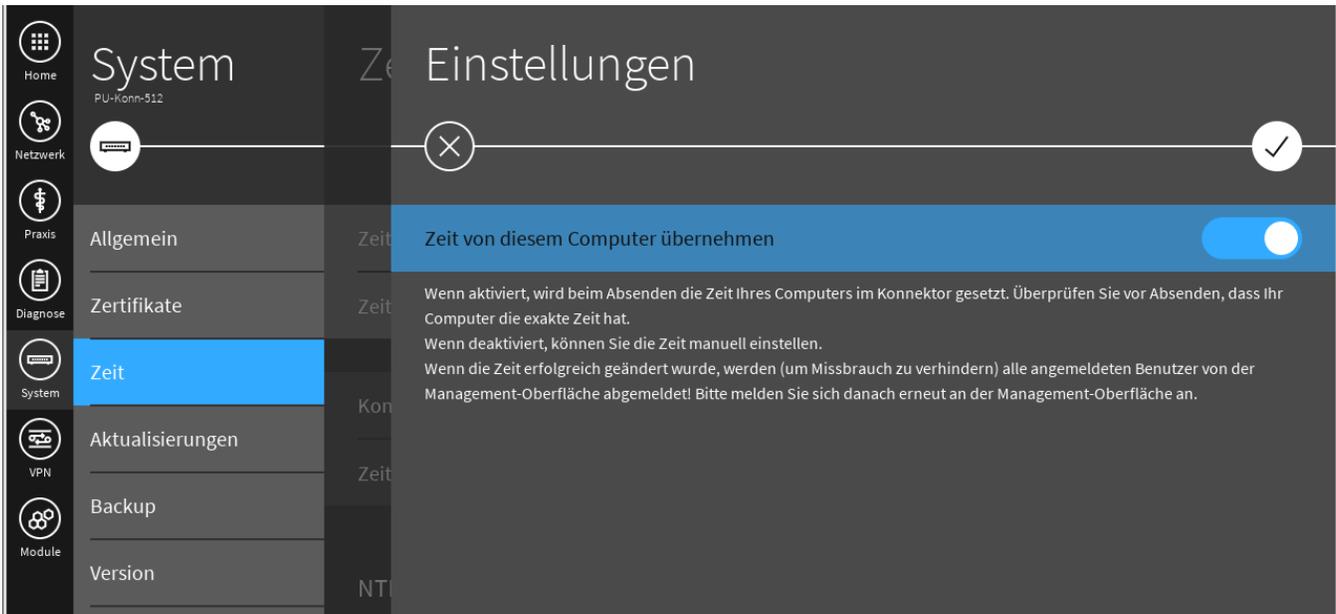
Man kann nun die neue TSL über "System", "Zertifikate" manuell hochladen:



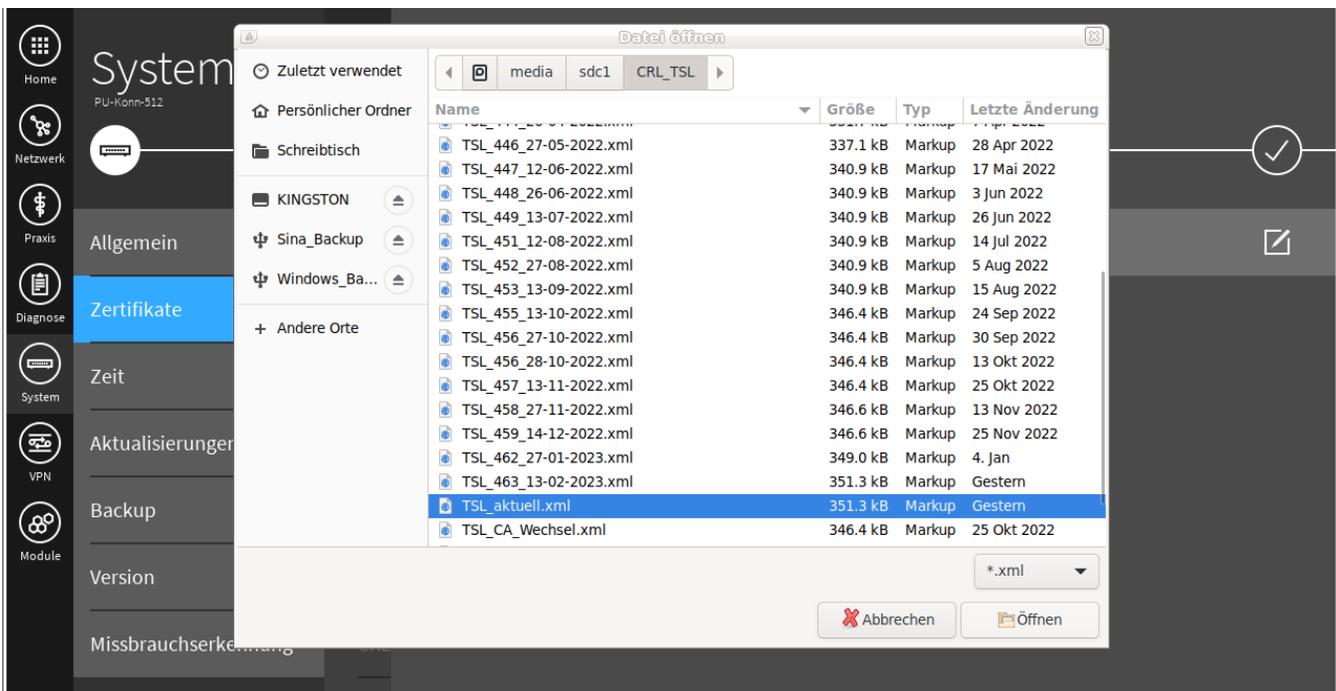


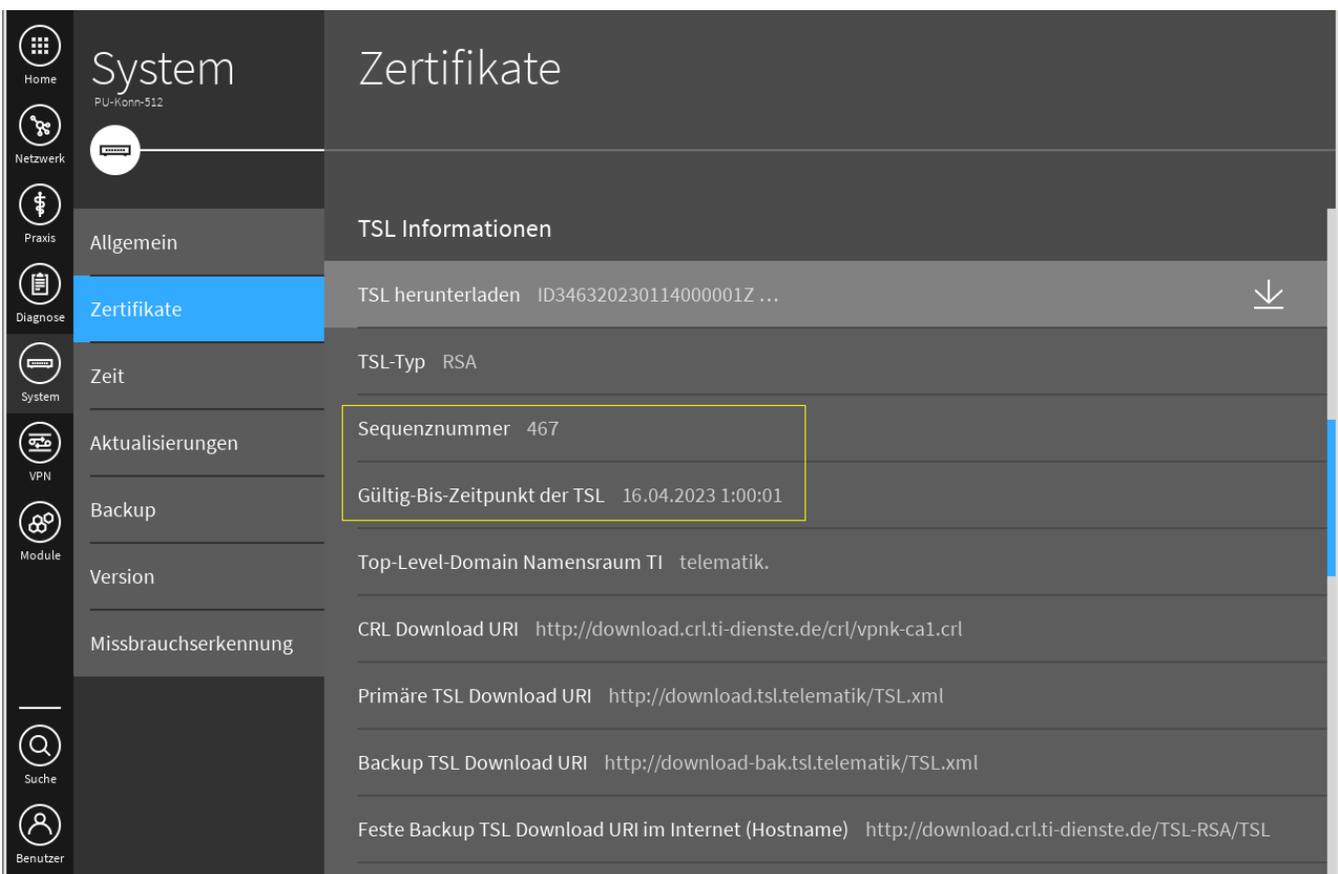
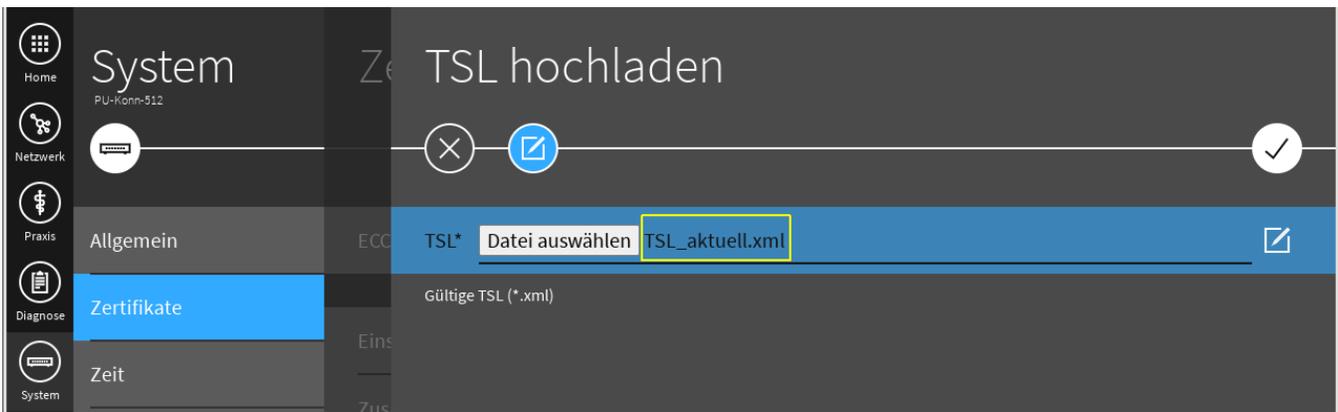


Die Systemzeit muss nun wieder korrigiert werden (im einfachsten Fall wird sie mit der PC-Zeit synchronisiert):

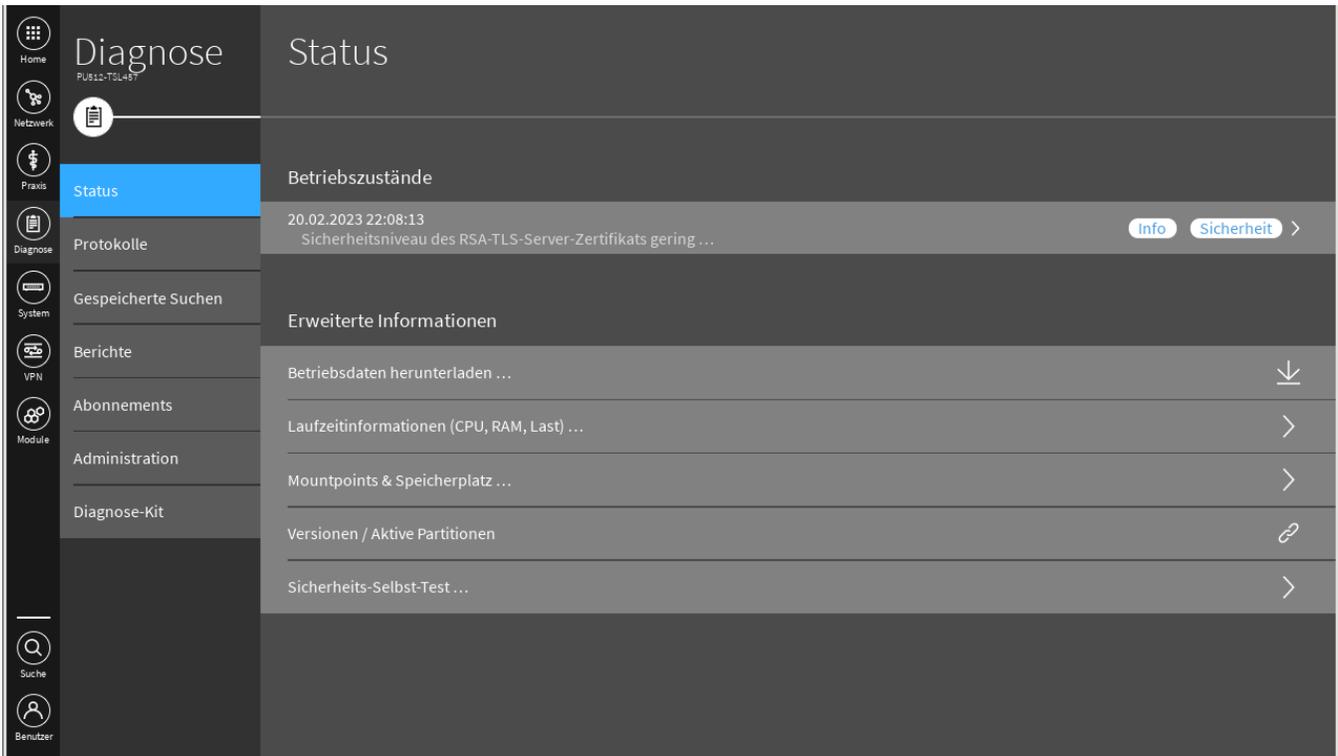


Nun muss als letzter Schritt die aktuelle TSL eingebracht werden:





Die Meldung zum abgelaufenen Vertrauensanker wurde damit aus den Betriebszuständen gelöscht:



Der "Leistungsumfang" wird anschließend wieder online geschaltet:



Der Konnektor kann nun eingerichtet werden.