

Zertifikatsumstellung bei Plusnet/QSC IPFonie Extended Connect mit Verschlüsselung

Datum: 02.06.2019
Autor: Henning Techel, Swyx Solutions GmbH, TAP
Mail: tap@swyx.com

Kurzbeschreibung, wie mit das Root-Zertifikat für den TLS Verbindungsaufbau bis spätestens zum 27.07.2019 zu installieren ist

1 Allgemeines

1. Die SwyxWare nutzt zur Zertifikatsverwaltung den Certificate-Store des Windows Betriebssystems
2. Auf einem Windows-OS sind nach einer Neu-Installation mit anschliessender Installation aller Windows-Update-Pakete ist nicht unbedingt das notwendigen Root Zertifikat installiert. Dieses muss daher ggf. nachinstalliert werden.
3. Bis zum 27.07.2019 muss zum erfolgreichen Aufbau einer TLS-Verbindung im Certificate-Store des Windows Betriebssystems das DigiCert Global Root G2 Zertifikat installiert sein.

Download:

<https://www.digicert.com/digicert-root-certificates.htm>

2 Installation des Zertifikats

1. Öffnen einer CMD Shell im im Administratormodus
2. Aus der Shell heraus die mmc starten.
3. In der mmc: Menüpunkt File->Add/Remove Snap-in... , dann im Dialog links Certificates auswählen und als Computer Account hinzufügen
In der mmc ist jetzt die Administration zum Certificate Store geladen.
4. Im linken Fenster unter Trusted Root Certificates Authorities kann jetzt das benötigte Zertifikat importiert werden.

3 Sonstiges

1. Die Installation des Zertifikats sollte vor dem Anlegen des Trunks erfolgen.
2. Wenn ein Trunk bereits eingerichtet und aktiviert wurde, bevor das Zertifikate installiert wurde, muss der Trunk zunächst deaktiviert werden. Danach muss der LinkMgr-Dienst neu gestartet werden.

Die obige Beschreibung wurde auf frisch installierten Windows 2012, Windows2012 R2, Windows 2016 und Windows 2019 mit jeweils aktuellen Patch-Stand verifiziert.