Verschlüsselung von VoIP-Anschlüssen im Dienst DFNFernsprechen

Auf Wunsch können die VoIP-Verbindungen zwischen der VoIP-Telekommunikationsanlage eines Teilnehmers und der VoIP-Plattform im Wissenschaftsnetz verschlüsselt werden. Dazu werden die Protokolle **TLS** (Transport Layer Security) und **SRTP** (Secure Real-Time Protocol) eingesetzt. Die Signalisierung, d. h. Rufaufbau, Rufsteuerung und Rufabbau werden über TLS verschlüsselt. Die Verschlüsselung des Medienstroms - der eigentlichen Sprachdaten - erfolgt über SRTP. Mit der Verschlüsselung können Vertraulichkeit, Authentizität und Integrität der VoIP-Verbindungen auf dem Trunk gesichert werden.

Für die Verschlüsselung der Signalisierung über TLS werden Zertifikate der **DFN-Verein Community PKI** benötigt.

1 Zertifikate

Im TLS-Protokoll wird die **beidseitige Authentifizierung** über Zertifikate der DFN-PKI eingesetzt. Dabei authentifiziert sich die VoIP-TK-Anlage der Einrichtung und eine Komponente vor der VoIP-Plattform, ein sogenannter Session Border Controller (SBC), gegeneinander (auch als mutual authentication bezeichnet).

In der Einrichtung muss für die VoIP-TK-Anlage ein **Server-Zertifikat der DFN-Verein Community PKI** installiert werden. Informationen zu dieser PKI finden Sie unter https://www.pki.dfn.de/dfn-verein-community-pki

Das Zertifikat muss im eigenen Zugang zur DFN-Verein Community PKI unter dem **Zertifikatprofil "VoIP-Server"** beantragt werden. Für alle Fragen diesbezüglich steht die DFN-PCA unter dfnpca@dfn-cert.de zur Verfügung.

Das Zertifikat des SBC der VoIP-Plattform baut auf einem eigenen **Wurzelzertifikat** auf. Das Wurzelzertifikat muss in der VoIP-TK-Anlage der Einrichtung als **vertrauenswürdig** akzeptiert werden, damit die beidseitige Authentifizierung zwischen VoIP-TK-Anlage und SBC erfolgreich durchgeführt werden kann.

Wurzelzertifikat DFNFernsprechen VoIP-Verschlüsselung

Das Wurzelzertifikat des SBC ist hier zu erhalten:

https://doku.tid.dfn.de/de:dfnpki:dfnpki_root_certs#dfn_voip

Gültigkeit

- Dec 7 09:31:36 2010 GMT bis
- Dec 8 00:00:00 2030 GMT

Formate

- Text: Das Zertifikat in lesbarer Form (.txt)
- PEM: Das Zertifikat in ASCII-kodierter Form (.pem)

Fingerprint

SHA1 Fingerprint=95:92:AA:19:1C:11:3F:DF:AB:CA:DF:6C:E6:27:11:D2:52:15:66:5A

SHA256 Fingerprint = A7:43:19:FF:BA:50:5D:BE:14:AF:E8:64:D9:7A:FA:99:
DA:F5:43:6F:00:1D:F1:2C:65:16:8C:ED:B6:21:A3:CC

Bitte überprüfen Sie die Authentizität des Wurzelzertifikats über den Fingerprint wie unter https://www.pki.dfn.de/faqpki/faqpki-allgemein/#c15267 angegeben.

Der Inhalt dieses Dokuments befindet sich unter

https://www2.dfn.de/dienstleistungen/dfnfernsprechen/voip/verschluesselung und

https://www2.dfn.de/dienstleistungen/dfnfernsprechen/zertifikate