Merkblatt Verschlüsselung von VoIP-Telefonaten

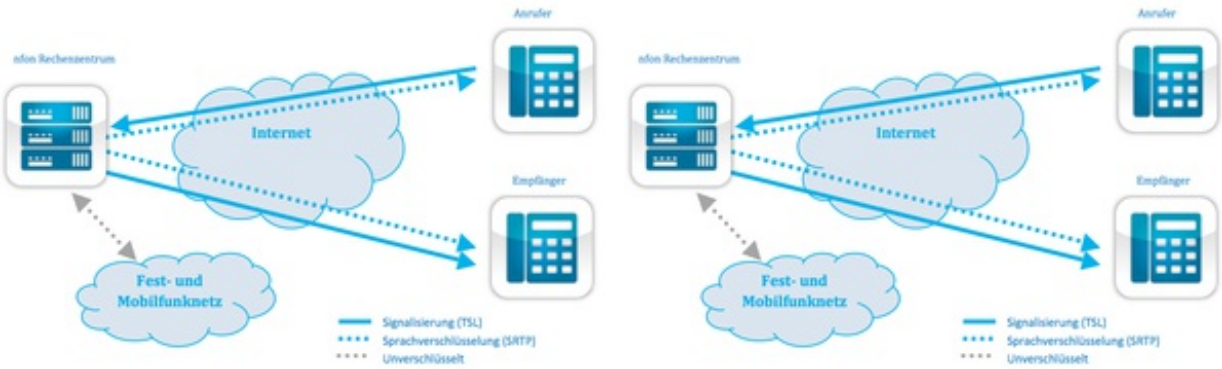
A. Funktionsbeschreibung VoIP-Verschlüsselung

nfon bietet Kunden die VoIP-Verschlüsselung von Signalisierung und Medienströmen an. Hierbei werden der Verbindungsaufbau und anschließend die Sprachdaten verschlüsselt. Dies erfolgt Ende-zu-Ende, also ab dem Telefon bis in das Rechenzentrum von nfon, in der Ihre Telefonanlage betrieben wird.

Im Zuge der Endgeräteprovisonierung werden Zertifikatsdaten zur Absicherung der SIP-Signalisierung via TLS auf die Endgeräte geladen. Die Endgeräte registrieren sich dann an dem für sie verantwortlichen Verschlüsselungsgateway, welches in den mehrfach gesicherten Rechenzentren von nfon betrieben wird.

Im Zuge des über TLS (256 Bit AES) gesicherten Gesprächsaufbaus werden die Schlüssel für die spätere Verschlüsslung der Medienströme ausgetauscht (mittels SDES). Diese werden einmalig zur Absicherung der Gespräche verwendet. Gesicherte Gespräche werden – falls vom Endgerät unterstützt – im Display als gesichert angezeigt.

Die Strecke zwischen Endgerät und nfon Rechenzentrum ist somit vollständig gesichert (also auch schon im LAN des Kunden). Das Verschlüsselungsgateway befindet sich im selben Netzwerk wie die nfon Telefonanlagenserver. Da die Verschlüsselung ausschließlich IP basiert funktioniert sind Verbindungen ab nfon Rechenzentrum in das öffentliche Telefonnetz (Fest und Mobilfunknetz) nicht verschlüsselt.



B. Kompatibilitätsliste

Die beschriebene Verschlüsselungslösung ist mit folgenden Endgeräten kompatibel:

- **Mitel 6730i, 6731i, 6753i*, 6755i*, 6757i***
- **snom 300, 320, 360*, 370*, 710, 715, 720, 760, 821*, 870***
- **Panasonic KX-UT248**
- **Unify (ehem. Siemens) OpenStage 15, 40, 60, 80***
- **Yealink T41P, Yealink T42G, Yealink T46G, Yealink T48G**

Weitere Endgeräte, die durch die Verschlüsselungslösung unterstützt werden:

- **Nsoftphone premium** (Softphone) ab Version 8.0.0

Endgeräte, die durch die Verschlüsselungslösung zwar unterstützt werden aber für die keinen Support übernommen wird:

- **Mitel UC360** (Konferenztelefon)

* Dieses Telefon wird nicht mehr vom Hersteller produziert und ist „End of Life“.

C. Konsequenz verschlüsselter Kommunikation

Dadurch das die Verschlüsselung der Signalisierung schon auf dem Endgeräten erfolgt, haben Edge-Router beim Kunden keine Möglichkeit mehr, die Signalisierung mitzuverfolgen und damit dynamisch Ports für die Medienströme zu öffnen und zu schließen.

In dieser Konsequenz ist ein breiter Bereich an UDP Ports für ausgehenden Verkehr zu öffnen, alle Medienströme laufen zwingend über die Internetanbindung.

Sobald für einen Kunden Verschlüsselung aktiviert wird, werden alle zur Verschlüsselung zertifizierten Geräte automatisch auf diese umgestellt. Es ist nicht möglich, einzelne Geräte dieses Typs selektiv zur Verschlüsselung freizugeben oder diese davon auszunehmen. Bei der Abrechnung werden immer nur die auch zur Verschlüsselung fähigen Geräte betrachtet.