Verschlüsselung Sprache

phone total bietet optional die **Verschlüsselung** von **Signalisierung** und **Medienströmen** an. Hierbei werden der Verbindungsaufbau und anschließend die Sprachdaten verschlüsselt. Die **Strecke zwischen Endgerät und Rechenzentrum**, in dem phone total mehrfach abgesichert gehostet wird, ist damit **vollständig gesichert**. Dh. eine Verschlüsselung erfolgt auch im lokalen Netzwerk (LAN) des Nutzers.

Ende- zu- Ende Verschlüsselung

Die phone total **Verschlüsselungssysteme** sind redundant installiert und unterstützen bis zu **1000 parallele Gespräche**.

Eine Verschlüsselung ist für die komplette phone total Anlage aktivierbar. Der monatliche Aufpreis beträgt **1,33 € pro aktiver Nebenstelle**.

Eine Übersicht zu kompatiblen phone total Endgeräten finden Sie http:// phonetotal.planet33.com/ index.php? id=14692#hier.

Funktionsbeschreibung

Im Zuge des **Plug&Play** der **Endgeräte** bzw. deren Provisionierung werden **Zertifikatsdaten** zur Absicherung der SIP- Signalisierung via TLS auf die Endgeräte geladen.

Nach dem Laden der Zertifikatsdaten registrieren sich die Endgeräte an dem für sie verantwortlichen **Verschlüsselungsgateway**, welches in mehrfach gesicherten Rechenzentren betrieben wird.

SRTP Verschlüsselung

Bei **Gesprächsaufbau** (Sicherung über TLS 256 Bit AES) werden Schlüssel für die spätere **Verschlüsslung der Medienström** e mittels SDES ausgetauscht. Diese werden einmalig zur Absicherung der Gespräche verwendet.

Gesicherte Gespräche (**SRTP** mit AES-128 Bit) werden **im Display als gesichert angezeigt**.

Da die Verschlüsselung ausschließlich **IP- basiert** funktioniert, sind Verbindungen ab dem phone total Rechenzentrum in das **öffentliche Telefonnetz** (Festnetz und Mobilfunk) **nicht verschlüsselt**.

Konfiguration Firewall

Für die Kommunikation mit der Telefonanlage müssen die Endgeräte über bestimmte **Netzwerk- Ports** ausgehend kommunizieren. Es sind **keine eingehenden Port- Forwardings** notwendig. Das **UDP- NAT- Timeout** muss aber auf **mehr als 65s** eingestellt sein.

Da die Verschlüsselung der Signalisierung bereits auf dem Endgerät erfolgt, haben Edge- Router keine Möglichkeit mehr, die Signalisierung mitzuverfolgen und damit dynamisch Ports für die Medienströme zu öffnen und zu schließen. Daher ist ein **breiter Bereich an UDP- Ports für ausgehenden Verkehr zu öffnen**.

Für eine vollständige Liste der notwendigen Port- Freigaben wenden Sie sich bitte an den technischen Vertrieb.

planet 33 AG - telecommunications internet security

planet 33 besitzt mehr als **10- jährige Erfahrung** in **Konzeption und Umsetzung von ITK- Sicherheit**. Durch umfassende technische Lösungskompetenz erhalten Sie **Service für Ihre gesamte Bürokommunikation aus einer Hand**.