SIPS - Session Initiation Protocol Secure

By separating session and media, both data streams can also be encrypted independently of each other. SIP can be encrypted using the TLS protocol, also known as SIPS, and the media stream (voice data) can also be encrypted using the SRTTP protocol. Any combination of these is possible, but it does not make sense with regard to secure encryption.

For the purpose of secure encryption, both data streams (i.e. session and media) must be encrypted simultaneously. The symmetric keys of the media stream are exchanged via SDP (i.e. SIP) and would thus be attackable via an unencrypted SIP. Although the symmetric keys of TLS are exchanged at the beginning of the session, the mechanisms of the SSL certificates are effective here, in which the symmetric keys are encrypted by the asymmetric keys of the SSL certificates.

Since transmission via a connectionless network protocol makes more sense with SIP, DTLS was designed as a UDP-based counterpart to TLS, which is based on TCP. However, it is currently only implemented by a SIP stack (ReSiProcate).

Source: https://de.wikipedia.org/wiki/Session_Initiation_Protocol#Verschl%C3%BCsselung_und_Sicherheit

Further Information

- VoIP Essentials
- Visit the Snom Forum
- Open a support ticket
- Find a local partner

Related articles

- ADPCM - Adaptive Differential Pulse Code Modulation
- B2BUA - Back-to-Back-User-Agent
- Codec
- CSTA - Computer-supported telecommunications applications
- CTI - Computer Telephony Integration
- ENUM - Telephone Number Mapping
- Hot Desking
- IP-PBX
- IVR - Interactive Voice Response
- Jitter
- LLDP - Link Layer Discovery Protocol
- PBX - Private Branch Exchange
- PoP - Point of Presence
- RTP - Real-Time Transport Protocol
- SBC - Session Border Controller

Visit the Snom Forum
Open a support ticket
Find a local partner