4.2 ENCRYPTED SIP Trunks ZRTP

Create SIP Trunk

Name	new_pbx
Failover Group	NONE ▾
IP / Hostname *	new_pbx.hostname.com
Port	5061
Transport Protocol	TLS ▾
Outboundproxy	
Register	☐
Username	
Password	
Virtual Phone Number	
SIP OPTIONS Ping	☑
Enable SIPS URIs	▾
SRTP Encryption	☑
SRTP Crypto Suite	DEFAULT ▾
Secure RTCP	▾
Insecure Call Treatment	Reject ▾
Max Concurrent Calls *	10
NAT	NO ▾
Direct Media	☑
Send Remote-Party-ID	☑
Codecs	amr:100
Announcement	No ▾
DTMF Signaling Method	SIP INFO ▾
Trusted	☑

Create

figure 1. "Edit Sip Trunk" form

In you can see an example configuration for creating a SECURE ZRTP SIP Trunk. The mandatory values are:

- **NAME:** a meaningful name for this trunk
- **IP / HOSTNAME**: IP address/hostname of the SIP server provided by ITSP
- **PORT**: this is **5061** by RFC
- **TRANSPORT PROTOCOL**: TLS
- **SRTP ENCRYPTION**: check it disabled

We do also suggest the following values to be set:

- **ANNOUNCEMENT:** No audio tones
- **DTMF SIGNALING METHOD**: choose your values considering the PBX on the other end of the Trunk. Usually we suggest to choose the value **IN FO**
- **DIRECT MEDIA**: enabled (checked)
- **SEND REMOTE-PARTY-ID**: enabled (checked)
- **CODECS**: amr:100
- **TRUSTED**: enabled (checked)

Other fields in the form depend by your network topology and by the features on the other end PBX.

When you are done with your changes, commit them by clicking on the **Update** icon.

4.2.1 Certificate Management

In order to validate a TLS peer for establishing an Encrypted SIP Trunk, you generally have to import the other party CA Root. This is important because the peer TLS certificate could not match PrivateServer actual Certificate Chain and thus the validation would fail.

> ⓘ   PrivateServer comes with a bundle of the most known CA Roots certificates ready to be used. So this section is useful for minor certificate authorities and/or for self signed certificates.

Please read to understand how to import a new CA Root certificate.