4.1 ENCRYPTED SIP Trunks

figure 1. "Edit Sip Trunk" form

In figure 1. "Edit Sip Trunk" form you can see an example configuration for creating a SECURE 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 enabled

We do also suggest the following values to be set:

- **ANNOUNCEMENT**: **ON EARLY MEDIA** works fine with the Cisco Unified Communications Manager.
- **DTMF SIGNALING METHOD**: choose your values considering the PBX on the other end of the Trunk. Usually we suggest to choose the value **RF C2833**

- **DIRECT MEDIA**: enabled (checked)
- **SEND REMOTE-PARTY-ID**: enabled (checked)
- **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 **Create** icon.

4.1.1 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 2.3.3 Add certification authority to understand how to import a new CA Root certificate.

4.2 ENCRYPTED SIP Trunks ZRTP