4.4 Authentication in SIP Trunks

As stated in the SIP Trunk introduction, from the authentication point of view there's no difference between encrypted or unencrypted SIP Trunks.

> ⊘ There's no way to perform an unauthenticated SIP INVITE on PrivateServer ! You can have different authentication models but you cannot choose to enable an unauthenticated SIP Trunk.

The two configurations are parallel meaning that the Authentication method is not related with the encryption of the Trunk itself.

Username	5353884
Password	••••••••
Register	☑

figure 1. Detail of the SIP Trunk form about the registration

 In figure 1. Detail of the SIP Trunk form about the registration you have a magnification of the SIP Trunk form that shows the registration fields. Usually in order to perform the authentication you have two ways, depending on the authentication type exposed by your peer PBX:

1. **SIP Accoun**t
2. **IP based**

4.4.1 SIP Account authentication

If your PBX peer on the other end of the Trunk has given to you a SIP Account to be used for the Authentication, then you need to insert login and password in **Username** and **Password** fields. Plus you should enable the **Register** option (check figure 1. Detail of the SIP Trunk form about the registration). The Register option force PrivateServer to act like a VoIP client and thus operate an explicit registration to the other end as soon as the internal Asterisk has been restarted.

Typically this configuration is used by public SIP providers because they can't rely just on the IP authentication (the customer's PBX could be behind an ADSL, for instance) and they need to be sure you're just the one who has the right to be connected despite the IP address you are using.

4.4.2 IP Address Authentication

In an enterprise scenarios the authentication is generally based on IP address, because inside enterprise's infrastructure all the structural elements use to have both private and static IP addresses.

Send keep alive	☑
Port	50

figure 2. Send Keep Alive field

In this case the IP address is most likely an internal one and it should be fixed: these features make it a reliable source for the authentication.

The IP Address Authentication is based on the **Host** field in the form of the Trunk creation.

Plus you need to enable the **Send keep alive** option (please see figure 2. Send Keep Alive field). This option is going to send to the other party a scheduled SIP OPTIONS message and would measure the roundtrip time to assess if the Trunk is fine or degraded or unable to carry messages.

> ⚠ The downside of this option is that there will be some more traffic on the socket (each passage of the request is 1.8 KiloByte, thus you can count almost 3.6 KB of traffic every 3 minutes)

The actual **default** value for the keep-alive **interval** is **60 seconds**. You can configure the general keep-alive timeout in the **NAT configuration** form. Please read PSAM 2.4 Advanced configurations to get informations about it.

> ⓘ Note that the keep alive option can be safely set up even on the SIP account authenticated trunk where it's optional. Instead it considered mandatory for an IP Address Authentication.info