SSL, SSLv2, SSLv3

About

SSL encryption has been found broken in both SSLv2 and SSLv3 versions (SSLv1 was never released). So, because there is a little meaning in using a broken encryption, you're invited to remove SSL support from both your clients and your servers.

Disabling SSLv3 and SSLv2 in FreeSWITCH

It's long time we already ship with correct configuration, but you may want to check your settings.

You do not want to have sslv2 or sslv3 into tls-version parameter value.

Edit /usr/local/freeswitch/conf/vars.xml (or /etc/freeswitch/vars.xml if you installed from packages), and be sure this line reads as:

```
<X-PRE-PROCESS cmd="set" data="sip_tls_version=tlsv1,tlsv1.1,tlsv1.2"/>
```

Then check into all SIP profiles if they are using this same value. It can be taken from global variables as:

```
<param name="tls-version" value="$${sip_tls_version}"/>
```

SSL Certificates

Certificates have nothing to do with using SSL as encryption method, "SSL Certificate" is just the old way to call a security certificate (because was then used by SSL, but it can be used by TLS too, no problem, is always the same certificate).

Nothing to see here.