Generating a new metadata certificate

This should only be necessary if the private key of your existing metadata certificate becomes compromised - e.g. if you accidentally sent both the public and private keys to the federation you are joining.

To generate a new self-signed certificate and install it:

1. Access a runtime using the maint account
2. Navigate to the `/usr/share/atacama-platform/keys/` directory

   ```
   cd /usr/share/atacama-platform/keys/
   ```

3. Rename the old certificate as a backup

   ```
   sudo mv idp.yourdomain.com.pem idp.yourdomain.com.pem.backup
   ```

4. Run the `gen_self_signed_sert.sh` script passing it your server address and name

   ```
   sudo ./gen_self_signed_cert.sh idp.yourdomain.com 'Your Organisation Name'
   ```

5. This will generate .pem file containing a pair of certificates something like this:

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCnoX/8OGqv3vBJ
VdN+eSbeYeFqgnjhzgz8PMFnUifxnF45BxvOTnR+FpC8dRXj+DfzmQzX83zHz0yt
1hXl1hkRGuz1+UPIGWzJKlTW8ZLjXzyA/fS8VGq1CJWP9++dWnQfylK1PyHHPA1q
Ngo44p6Qtc6TxL20qq6vd0aXf1lzkdv8y80gMHyI00HlgAKNlEiPd3V8Y5zy1227
mIWTPvh0J7VTG2VLsewKmYh2HbPqagoUPTz1VO7esorKDRMWwAPKmV+FS/Aqsri2
diFFCVqU4Cvu0G1ex0HkQyS7JPkipLCspQBMajcMbL2rYkvaE3525iNkp7SQXMmj
NpVc+Hh/AgMBAAECggEAF0QLB26tIAvJPeRznjIieusK5kWFkZGPq9Ki5Tw53wbc
7P1XlqK8+GMZY468ow9odJ7hcXeR8gmLkvULxQKaKA2cpecayUL+Hk2JyOtuf7BQ
LXcR6LGuvcGbQIgg8a4EQAVMxWslvQlQs1Ucxhht+ZfCPDAqRFEMPb5IRe6e87Mp
XBKhTeW/aginR0/D8/pLzLC+ybSNvJeZiitd8xGXca7DlD8luv+57/tN9P3hvInO
q5jMSRd16zalAO1fkslffvpMMPGIqTHIS3jHMa4oyq5Brl2T4844x0HQ+1ZbUqO7
7IJ0L1cGp0ukBbAlASR384LAZIvWEwISg5DsrkplQQKBgQDQNu92IqUoxHANcLat
8McrwZEMyV9PC3YcwG9EGp6AULlzzFAKEw1WF0CJwkBALhqCuEZUzBKIWKhWHE3/
ouHnCsTSBSwT69/R11Xlf4b1FXg7C3e3SHPWYQ5ROBa5dZSmBvKXWzyvzigqeHG9
3OAWqGXf4C0ZCMNI362pIqC3FQKBgQDOGi5eoXukYN4aHTp9tdezdfZMCSgeltmZ
4ZSmm/0pd7BNmextBCJOz2aP6yUWOoWzVlnAtL/WzNW9Ik8pEBkJ05flq2sELoaz
l0eOG9FbHfDv23ysJDnZO8Jw+YFXEGHQGbJj8C/WGCb8iJslQZsrsO4Ha9FxgOME
l07Te6nWQwKBgQCLLi2jqkT8m1LLqSxz2R9KAHoVMgajr+WkEn5N5/1LiKpu3VIA
ZDTl92UMsOyB+k9+Ue+xfzhkK99asFDzMM4QwwIN4ac1KdbTTj38yuJLsa5Myb2c
prHH+9i2Mef+0LoswTgoNLS8T/JJcXmWkK66dpaisBd1RIZFkD9lb+A+gQKBgA3j
NbyqpOounMilr4tI9X/iMvZsp4doIsF7sciIOkbRCdAwzv2JicZFs2N/NMCKsPek
meeiRkrzAnP8G9lofEdtOo7/PfbKK8luKCQrO7AoFFQVNhFjX4KDxFZYeZ6kO/MJ
yDtzs8V5WycpDUs1YH9RLLjTSwma5bEpgOY/LvKBAoGAQUzClYppv3asE5Gq+S3L
Q8tTMWOXGiHnxPPtXR1dNpsWd7nzrJ6C4SL+JmBylkkr1YDTJ7Pfi294ghlfe3g9
mKzFPLAyTKzwZqnCUonrWfB68ezOG91ubXuT9qVTL1Se7mVcsISiVhI3asuLpzDK
O4Nc+aIpfCMT9+EZIxSW/cU=
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDIzCCAgugAwIBAgIJALKKW3OWfIikMA0GCSqGSIb3DQEBBQUAMCgxDjAMBgNV
BAoMBWJhbGxzMRYwFAYDVQQDDA1pZLAuYmFsbHMuY29tMB4XDTE2MDMxNDE1MTUy
M1oXDTI2MDMxMjE1MTUyM1owKDEOMOwGA1UECgwFYmFsbHMxFjAUBgNVBAMMDWlk
cC5iYWxscy5jb20wggEiMA0GCSqGSVb3DQEBAQUAA4IBDwAwggEKAoIBAQCnoX/8
OGqv3vBJVdN+eSbeYeFqgnjhzgz8PEFnUifxnF45BxvOTnR+FpC8dRXj+DfzmQzX
83zHz0yt1hXl1hkRGuz1+UPIGWzJKPTW8ZLjXzyA/fS8VGq1CJWP9++dWnQfylK1
PyHHPA1qNgo44p6Qtc6TxL20qq6vdIaXf1lzkdv8y80gMHyI00HlgAKNlEiPd3V8
Y5zy1227mIWTPvh0J7VTG2VLsewKmZh2HbPqagoUPTz1VO7esorKDRMWwAPKmV+F
S/Aqsri2diFFCVqU4Cvu0G1ex0HkQZS7JPkipLCspQBMajcMbL2rYkvaE3525iNk
p7SQXMmjNpVc+Hh/AgMBAAGjUDBOMA0GA1UdDgQWBBSt9hMIrztae6Y0yi2Ahk/f
7NtUhTAfBgNVHSMEGDAWgBSt9hMIrztae6Y0yi2Ahk/f7NtUhTAMBgNVHRMEBTAD
AQH/MA0GCSqGSIb3DQEBBQUAA4IBAQA7RMfxiYVMGn1/QC4QpdkgchYB059/mUtO
G4MeBsOjeV0dQF/ccTrML8jxUvsFB3K8VjH2zWqpk4W+n4+eFkWRYdK1IbmogQ4A
AR5znmRmsVmGYVGiz2HhsL3rvUrh6cQoIoRlH8vinZ9Xea8jeKj4Xg4QUQcIafJh
sFY5WgQJDuoss/nTi3XhfwtbLNR1qGlv91CAadN5I4V+Y8zRl8UcFCv/KqOmdoiV
dXo7oHVl0DfAvQmq47gTT2K8iFxhsahtGhdMXWcRE7dQhEUx9Mvxc8hfckQq6wKn
DqgchL2+XkgDZxuHcxQ2wu9ovRHtqtPsooEBw49gU8HfS3zCZIQN
-----END CERTIFICATE-----
```

6. The first of the two is your private key - never share that with anyone or you will have to go through this again.

7. The second one is what you may have to copy to another file and send to a federation operator (or upload to a non-federated SAML SP you are connecting to such as Google)
8. Finally restart Apache for the change to take effect. If this is a live service you may want to postpone this for another time (see below).

```
sudo service httpd restart
```

9. Once you are sure all is well, you can return and remove the old certificate that you renamed:

```
sudo rm idp.yourdomain.com.pem.backup
```

Anything to watch our for?

If you are doing this on a live service, there will be some time when resources are not accessible because there will be a mismatch between the certificate in your metadata and your entry in a federation's aggregated metadata (or the version of that metadata cached by a resource). To minimise this time:

- Pass your new certificate to the federation operator ahead of time and arrange a date for them to publish the change. Explain that this is a change to a live service so they will not expect to be able to see that certificate in your metadata immediately.
- Once they publish the change, it will take up to 24 hours for resources to pick up that change. As they update, they will become unavailable because your SAML responses will not be signed with the certificate they're expecting.
- At some point between some becoming unavailable and all becoming so, do step 8 (restart apache) to make the change live.

If you publish a new configuration from the administration console, Apache will be restarted and the new certificate will come into play at that time. You may like to take steps to mitigate this.