Change of SAML-certificate

This guide describes how to change the security certificate for SAML messaging for Shibboleth and Haka metadata only. Also remember to renew the certificate from Tomcat / web server

Change of SAML-service (SP) certificate

The process described in this guide ensures uninterrupted certificate exchange with services that operate in accordance with the SAML specifications. There are SAML products on the market that do not support the key exchange process. Certificate exchange requires either manual action, scheduled certificate exchange, or service login does not work at all while two certificates are published in the metadata. Haka does not support scheduled certificate exchange without strong reasons, as it is impossible to agree on a common metadata update time for all services.

- Configure your SP to use both the new and old certificates in parallel so that the old certificate is used first, by default.

```
<CredentialResolver type="Chaining">
  <CredentialResolver type="File">
    <Key>
      <Name>OldKey</Name>
      <Path>/etc/shibboleth/old.key</Path>
    </Key>
    <Certificate>
      <Path>/etc/shibboleth/old.crt</Path>
    </Certificate>
  </CredentialResolver>
  <CredentialResolver type="File">
    <Key>
      <Name>NewKey</Name>
      <Path>/etc/shibboleth/new.key</Path>
    </Key>
    <Certificate>
      <Path>/etc/shibboleth/new.crt</Path>
    </Certificate>
  </CredentialResolver>
</CredentialResolver>
```

- In the Resource Register, add a new certificate to the registration information of your SP in addition to the old one.
- Wait 24 hours from the time the metadata is published for it to have time to update the IdPs. Then change the order of the certificates in the configuration of your SP so that the new certificate is the first and therefore becomes the default (see step 1 - change the order of these CredentialResolvers here in reverse.
- Remove the old certificate from the metadata in the Resource Register.
- Wait 24 hours for the metadata to update and remove the old certificate from your SP configuration.

Change the SAML authentication source (IdP) certificate

- In the Resource Register, add a new certificate in addition to the old one to your IdP registration information. Both certificates end up in the metadata.
- Wait for the metadata to be published and for it to update to the SPs. Then change your IdP in the configuration to a new certificate.
- Remove the old certificate from the metadata in the Resource Register.