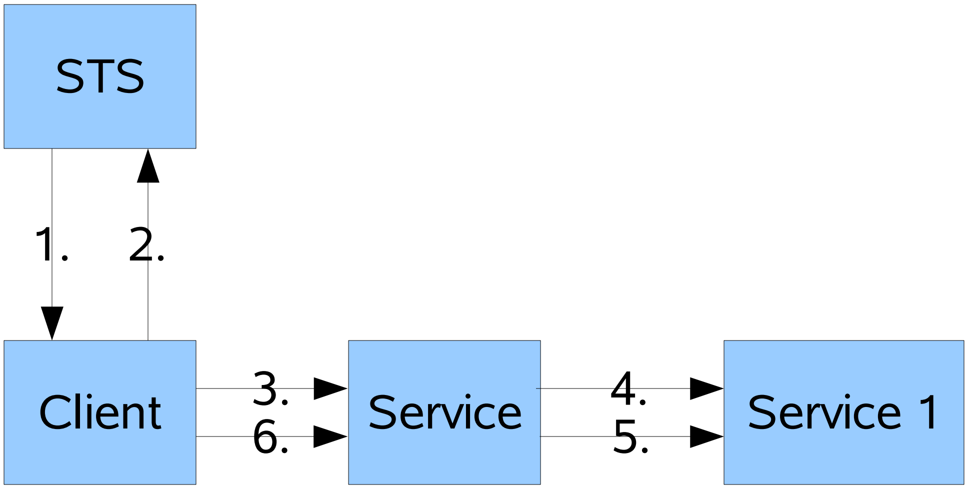

1. The Client send a request to the STS. The request message carries the username/password of the user and is secured with the STS certificate.

2. The STS issues an SAML assertion containing the username (e.g. Alice) as subject id and role attribute (see src\common\SampleSTSAttributeProvider). Then it send a response message with the issued token to the Client.

3. The client send a request to the Service. The message carries the SAML assertion from the previous step for authentication and secured (signed and encrypted) with the Service certificate.

4. The Service sand a request to the Service 1. The message carries the SAML from the previous step and is secured (signed and encrypted) with the Service 1 certificate. The Service 1 check the SAML assertion (see src\common\SampleSamlValidator.java).

5. The Service 1 send a response to the Service.

6. The Service sends a response to the Client.