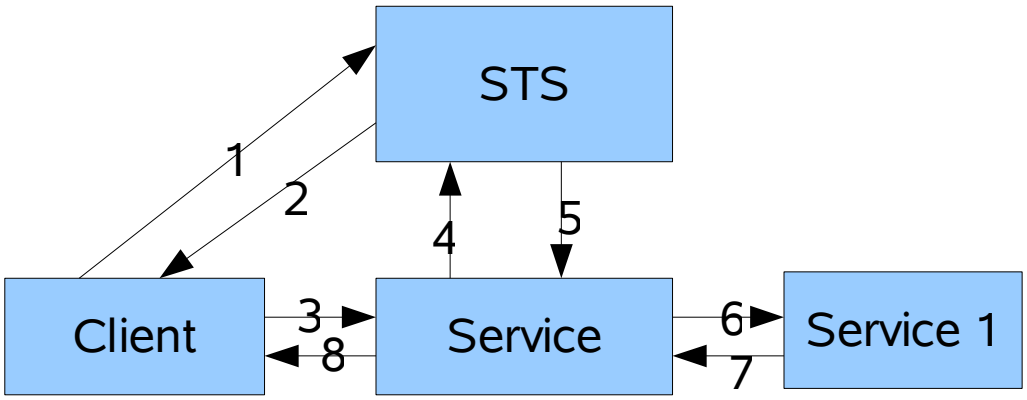

1. The Client send a request to the STS. The request message carries the username/password of the user and is secured with the STS certificate.
2. The STS issues an SAML assertion containing the username (e.g. Alice) as subject id and role attribute (see src\common\SampleSTSAttributeProvider). Then it 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 with the Service certificate.
4. The Service send a request to the STS. The message contains the username/password (bob/bob) of the Service, the SAML assertion received from the user in the previous step in an ActAs element in the body (RST), and is secure with the STS certificate (see src\fs\ simple\server\FSImpl.java. The ActAs token is injected into the request using the STSIssuedTokenFeture). It means to ask for an issued token with it the Service can access the Service 1, acting as the user.
5. The STS issues an (act as) SAML assertion which contains the Service id (bob) in the Subject, and attribute ActAs with the user name (e.g. Alice), and role attribute for the user (see src\common\SampleSTSAttributeProvider). It then send a response message with the issued token to the Service.
6. The Service sand a request to the Service 1. The message carries the act as SAML from the previous step and is secured with the Service 1 certificate. The Service 1 check the act as SAML assertion (see src\common\SampleSamlValidator.java) and understands it is the Service who made the request act as the user.
7. The Service 1 send a response to the Service.
8. The Service sends a response to the Client.