InCommon®

InCommon Certificate Manager

Authentication at Web Service API

InCommon
c/o Internet2
1000 Oakbrook Drive, Suite 300
Ann Arbor MI, 48104

Introduction to Authentication at Web Service API

InCommon CM offers two ways to authenticate users accessing its various services via SOAP API and REST API services. The authentication methods are:

- Authentication via Login and Password
- Authentication via Login and a Client Certificate

Authentication via Login and Password

Prerequisite

- Users should have InCommon CM login credentials and the correct customer login URI
- For the Web Service API, access must be enabled for the customer by InCommon and for each org/dept by admins on the client side.

The URIs for the login/password authentication method are:

SOAP API Service

- https://host:port/ws/[Service name]

REST API Service (for Code Signing on Demand)

- https://host:port/api/csod/v1/requests

Authentication is performed by sending the AuthData parameter to the web service API. This includes the login, password and Customer URI. After successful authentication, the admin can proceed to the InCommon CM management interface. If authentication is not successful (login and/or password are incorrect, password has expired), the admin will see an error and will be denied access to the Web Service API. The same admin could, however, still authenticate themselves via a client certificate (refer to the next section).

Authentication via Login and a Client Certificate

Prerequisite

- Admins should have the Customer URI
- For the Web Service API, access must be enabled for the customer by InCommon and for each org/dept by admins on the client side.
- Admins should have 'WS API use only' privilege enabled
- Admins should have 'Certificate Auth' enabled. The authentication certificate must requested and issued via InCommon CM and active at the moment of authentication.

The URIs for the login/certificate authentication method are:

SOAP API Service

- https://host:port/private/ws/[Service name]

REST API Service (for Code Signing on Demand)

- https://host:port/private/api/csod/v1/requests

The certificate must be provided by the admin's client at the time of login. After receiving the authdata parameter (customer URI and login), InCommon CM will verify that the certificate matches the one specified in the 'Certificate Auth' area of the admin's profile. After successful authentication, the admin can proceed to the InCommon CM management interface. If authentication is not successful (login and/or password are incorrect, certificate is not correct/revoked), the admin will see an error and will be denied access to the Web Service API. The same admin could, however, still authenticate themselves using the login and password method (see previous section).