ADSS RA Service

Table of Contents

How does ADSS RA Service process the certification requests?

ADSS RA Service is capable of issuing certificates through multiple channels, i.e. SCEP, Web services and Face to Face meetings. The certificates issuance requests can either be Synchronous or Asynchronous. SCEP is always synchronous while Web services interface can be synchronous or asynchronous based on configurations. Synchronous requests are auto processed without user intervention while asynchronous requests are set to pending state and require reviewing by the RA Operators before forwarding them to the ADSS CA Server for issuance.

- **Request via SCEP**

  Network devices, mobile devices, servers, firewalls, etc. can use SCEP to send certificate issuance requests to ADSS RA Service. In this regard, the operator has to configure upfront the Subject DN and a Challenge password for each device in the "Device Certificates" section of ADSS RA Service. The SCEP requests must then exactly match with the configured Subject DN and Challenge Password for the respected device. In case of any mismatch in Subject DN or Challenge Password, the request will be rejected.

- **Request via Web Service (For Devices)**

  The certificate issuance request for a device via web service can either be Synchronous and Asynchronous. The operator has to configure upfront the Subject DN and a Challenge password for each device in the "Device Certificates" section of ADSS RA Service. The request must exactly match with the configured Subject DN attributes and Challenge Password of the particular device, otherwise the request will be rejected. However, in case of asynchronous request, the RA Operator can review the certificate request before forwarding the request to the ADSS CA Server.

- **Request via Web Service (For End-Users)**

  The certificate issuance request for an end-user via web service can also be Synchronous and Asynchronous. The operator can configure Subject DN in the 'RA Profiles' section. The synchronous requests are processed right away. However, in case of asynchronous request, the RA Operator can review the certificate request before forwarding the request to the ADSS CA Server. See the below KB (*How the Subject DN sent via the ADSS RA Web Service processed*) to know more about how the received Subject DN is checked both in the case of synchronous or asynchronous requests.

- **Request via Face to Face Meeting**
  The RA Operator can set the values for the required Subject DN attributes in a Face to Face meeting with the end user, before forwarding the request to the ADSS CA Server. As a result, digital certificates are issued right away.

How to make the certification requests received over the RA web service interface to be processed synchronously?

Synchronous processing method is used to issue digital certificates against incoming certificate requests without any manual user intervention.To enable certification request to be processed synchronously,

- Stop RA service from ADSS RA Service > Service Manager.
- Browse ADSS RA Service> RA Profiles.
- Open the respective RA profile.
- Enable the "Allow auto-approval for web based requests (no manual approval required)" option.
- Click "Update" button.
- Start RA service from ADSS RA Service > Service Manager.

Now all the certification requests that will use this RA profile will be processed synchronously and certificates will be issued right away.

> **Note**
> SCEP based certification requests are always processed synchronously.

How the Subject DN sent via the ADSS RA Web Service processed?

ADSS RA web service processes the certification requests as per the following rules:

- If a request contains multiple attributes e.g. Two OU attributes are sent in the request, whereas the RA Profile was configured with only one, then the request will be rejected. For this scenario to work, the RA Profile must have multiple OUs e.g.OU=$OU, OU=$OU. The dollar sign symbolizes that the value of this attribute can be provided externally.
- If an attribute is fixed in the RA Profile e.g. OU=Security then any OU attribute value sent in the request is ignored and the certificate is issued with OU=Security. The same will be true when no OU is sent in the request.
- If a request contains an attribute e.g. OU=CPC which is not identified in the RA Profile, then such a request will be rejected.
- If a request contains an attribute e.g. OU=CPC, whereas the RA Profile was configured with two e.g.OU=$OU, OU=$OU then such a request will be rejected.