Certificate Validation (Verification, XKMS and SCVP)

Table of Contents

What is the difference between Basic Validation and Advanced Validation in SCVP, XKMS and Verification profiles?

Basic Validation is not PKIX compliant and policy extensions are not checked in the certificates. Instead path validation is performed using Ascertia's custom built algorithm, which is much faster, but only the following checks are performed:

1. Name Chaining
2. Signature Verification
3. Basic Constraints Verification
4. Key Usages and Extended Key Usages Verification
5. Revocation Status Check using CRL or OCSP

Advanced Validation is PKIX compliant and the following checks are performed during certification validation:

1. Checks mentioned in Basic Validation
2. initial-policy-set
3. initial-explicit-policy
4. initial-policy-mapping-inhibit
5. initial-inhibit-any-policy

How to ensure seamless processing of signature/ certificate validation request, when the CA chain is already registered in Trust Manager?

It is often observed that CAs are registered in Trust Manager but they are not made available in the verification profile. Consequently, the validation request gets failed as certificate path could not be properly built. To resolve this:

1. Edit the required policy/profile
2. Go to the Trust Anchor tab
3. Put those CAs in the Allowed CAs List that will be used to build the path
4. Save the settings
5. Restart the relevant service component from the Service Manager module and send the request; it will then be processed successfully.

XKMS Service returns with profile not allowed or inactive

This means either the profile does not exist with the specified profile id or the profile is not allowed in Client Manager. In order to allow the profile, follow the steps below:

1. Go to Client Manager
2. Edit your required client
3. Go to the XKMS Service tab
4. Put your required profile in the allowed profiles list
5. Send the XKMS request with the required profile and client and it will be processed against your requested profile.

How to invoke an XKMS profile for non-registered CAs?

When the target certificate chain is built up to the registered self-signed Root CA certificate, and the intermediate CA certificate(s) are not registered within the Trust Manager module, then the revocation of such non-registered CAs is discovered by using a non registered CA policy (configured within the XKMS profile). ADSS Server also provides the flexibility to choose a certificate validation mechanism from CDP, AIA and configured OCSP addresses. The XKMS profile can be configured through XKMS Service> XKMS Profiles> Advanced Settings tab.

How to invoke an SCVP policy for non-registered CAs?

When the target certificate chain is built up to the registered self-signed Root CA certificate, and the intermediate CA certificate(s) are not registered within the Trust Manager module, then the revocation of such non-registered CAs is discovered by using a non registered CA policy (configured within the SCVP policy). ADSS Server also provides the flexibility to choose a certificate validation mechanism from CDP, AIA and configured OCSP addresses. The SCVP policy can be configured through SCVP Service> Validation Policies> Advanced Settings tab.