X.509 troubleshooting - Enabling trust between NetWeaver and intermediate server

Author : Tobias Hofmann

Date : July 21, 2020

ICM in NetWeaver ABAP is not reading the HTTP header and accepting the transmitted X.509 certificate simply like that. I'll show here a picture that shows what an intermediate server is sending to NetWeaver.

You can see that two certificates are transmitted to SAP: the user X.509 as well as the proxy / intermediate certificate. There are two parameters that need to be enabled in ICM configuration to accept the provided certificate.

```
icm/HTTPS/trust_client_with_issuer = CN=intermediate, * icm/HTTPS/trust_client
_with_subject = C=DE, ST=BW, L=Karlsruhe, O=blog, *
```

In case the intermediate server is not authenticating itself with a certificate matching these values, the certificate in the HTTP header is ignored. A BASIS person must add the correct values to the SAP NetWeaver profile.

An additional level of security is added by how ICM is validating certificates. Just adding the above parameters won’t enable an arbitrary certificate that contains these values to be accepted. The CA certificate provided by trust_client_with_issuer must be added to the server’s PSE for its role as an HTTPS server.

Without this additional level of validation, you could create a CA and a client certificate with the same values on your own. In that case, you can fake the client certificate send to ICM and it would accept, as the issuer line matches. But as the CA certificate must be included in the PSE, this kind of attack is not working.

Client certificate must be trusted by SSL Server

If the certificate send by the client is not trusted by the SSL Server (added to its PSE), then the logon won't work. For instance, assume that your HTTPS client uses a self-signed certificate.

Certificate validation fails