X.509 troubleshooting - Send X.509 Certificate in HTTP Header

Author : Tobias Hofmann

Date : July 20, 2020

In many cases a proxy is placed between the end user and the SAP backend, like a Web Dispatcher.

User --> Proxy (intermediate) --> SAP

The proxy / intermediate receives the user certificate, extracts and adds it to HTTP header SSL_CLIENT_CERT. When a connection to the SAP backend is opened, the intermediate authenticates itself (warning: this is complex too) and sends the user certificate inside the header. The SAP backend receives the header and extracts the user certificate. For more information on this topic: SAP Help.

In this scenario, the X.509 certificate needs to be forwarded as a HTTP header. As the SAP backend expects in that use case additional security measures to be considered, this scenario is not simple, aka:

several problems may occur. I'll try to detail some of them and their possible solutions.

Problem

A trust relationship between the intermediate that is forwarding the user certificate and SAP must be established. If not, the certificate sent in the header SSL_CLIENT_CERT is rejected. ICM will show an error in its log.

The log message details the error and why it failed:

```
HttpModIsReverseProxyTrustworthy: no trust relationship to intermediary specif
ied (see documentation for parameter "icm/HTTPS/trust_client_with_issuer" or "
icm/trusted_reverse_proxy") HttpHandleCertificate: intermediary is NOT trusted
 ... Forwarded Client certificate: subject="CN=test1, O=blog, L=Karlsruhe, SP=
BW, C=DE", issuer="CN=intermediate, O=blog, SP=BW, C=DE" ... HttpModGetDefRule
s: intermediary is NOT trusted -> remove SSL header fields HTTP request [5/79/
3] Reject untrusted forwarded certificate (received via HTTPS without certific
ate): subject="CN=test1, O=blog, L=Karlsruhe, SP=BW, C=DE", issuer="CN=interme
diate, O=blog, SP=BW, C=DE"
```

Root cause

ICM received the user certificate in the http header but is not accepting it. This is because the intermediate is authenticating itself with a certificate at the SAP backend, but this certificate is not trusted.

Solution

Trust the certificate of the intermediate. This is done by configuring ICM and adding the subject line of the intermediate client certificate as trusted.

```
icm/HTTPS/trust_client_with_issuer =  icm/HTTPS/trust_client_with_subject =
```

To find out the values that need to be added, you can use openssl. For instance, my client certificate contains the following information:

```
openssl x509 -in tobias.crt.pem -text -noout
```

```
Issuer: C=DE, ST=BW, O=blog, CN=intermediate Subject: C=DE, ST=BW, L=Karlsruhe
, O=blog, CN=tobias
```

Based on this, the ICM parameters are:

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

Won’t work

The order shown in openssl output is not the same as ICM is seeing it. The parameters must be configured to match the order of how ICM sees the issuer and subject. While OpenSSL output indicates that the subject line starts with C=DE, for ICM the line starts with CN=test1.

Possible but dangerous

Use a wildcard for the issuer and subject line. This way, all certificates are validated successfully.

```
icm/HTTPS/trust_client_with_issuer = * icm/HTTPS/trust_client_with_subject = *
```

Test

To see if the logon works, you can use ICM log or e.g. STAD.

```
Tx SMICM
```

Set trace level to 3 and check the log files if the user certificate is accepted.

```
Forwarded Client certificate: subject="CN=test1, O=blog, L=Karlsruhe, SP=BW, C
=DE", issuer="CN=intermediate, O=blog, SP=BW, C=DE" HttpModGetDefRules: interm
ediary is trusted -> forward SSL header fields HTTP request [0/8/4] Accept tru
sted forwarded certificate (received via HTTPS without certificate): subject="
CN=test1, O=blog, L=Karlsruhe, SP=BW, C=DE", issuer="CN=intermediate, O=blog,
SP=BW, C=DE" HttpModGetDefRules: determined the defactions: COPY_CERTHEADER_TO
_MPI (2) HttpModHandler: decode SSLCERT from header
```

You can also check which user called a transaction.

```
Tx: STAD
```

The test1 X.509 is mapped to user X509TEST.