FaaS HSM setup

HSM client installation

Installation of Luna SA client software is described in the section "Installation of required software" (step 5.) of the document "Initial creation of the template machine"

Certificate exchange

In order to created Network Trust Link between client and HSM appliance, appropriate certificates must be exchanged. This section describes steps that need to be taken.

1. Register Luna SA's certificate in the trust list on a client side.

   - Download HSM appliance certificate and store it in /usr/safenet/lunaclient/cert/server/

   - Add HSM appliance certificate to the trust list:

   ```
   vtl addServer -n se-tug-hsm1.sunet.se -c /usr/safenet/lunaclient/cert/server/se-tug-hsm1.sunet.se.crt
   ```

2. Verify that the Luna SA server is in the list of servers trusted by the client.

   ```
   vtl listservers
   ```

3. Generate client certificate and send it to NUNOC to register client's certificate.

   > Procedure for client certificate creation is described in the section "HSM access" of the document "Production and test instances deployment guide".

4. Verify partition visibility to the client.

   ```
   vtl verify
   ```

FaaS HSM-protected signing key

This section details the commands used to create the RSA key pair and X.509 certificate inside the HSM, used to sign all production SAML Metadata as part of the FaaS offering.

SafeNet Certificate Management Utility (cmu)

1. Generate an RSA key pair with a 4096bit-sized modulus (the maximum size in use in 2015) and label the created objects (private and public key) accordingly.

   ```
   cmu generatekeypair -keyType RSA -modulusBits=4096 -publicExp=65537 -sign=T -verify=T -startDate
   20150101 -endDate 20300630 -labelPublic faas-prod-public -labelPrivate faas-prod-private
   ```

2. Find out the "handles" of the newly created objects:

   ```
   cmu list
   ```

3. Create a self-signed X.509 certificate containing the public key created above, based on the handles discovered in the previous step:

   ```
   cmu selfSignCertificate -publichandle=56 -privatehandle=57 -startDate 20150101 -endDate 20300630 -CN
   "Federation Metadata Signer" -keyusage digitalsignature -keyusage keycertsign -sha256withrsa
   ```

4. Export the X.509 certificate from the HSM into the local file system, to be used to verify signed SAML metadata. This file needs to be communicated to the operators of FaaS-hosted federations, and they should rename and distribute that file to their communities as needed.

```
cmu export -handle=55 -outputFile=/root/handle55.pem
```

FaaS signature validation certificate

Attached federation-metadata-signer.pem and also produced in full below:

```
-----BEGIN CERTIFICATE-----
MIIE2DCCAsCgAwIBAgICNEEwDQYJKoZIhvcNAQELBQAwJTEjMCEGA1UEAxMaRmVk
ZXJhdGlvbiBNZXRhZGF0YSBTaWduZXIwHhcNMTUwMTAxMDAwMDAwWhcNMzAwNjMw
MDAwMDAwWjAlMSMwIQYDVQQDExpGZWRlcmF0aW9uIE1ldGFkYXRhIFNpZ25lcjCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAOJBqGjmFkaovgSJuwuusoHr
2b8zGQFv2qoG/1STHf13tiIyPmEwoO2fs9H2s9qvHWbqg9rYtezgIdiTTL9i2Kv3
daxXAm9/H+PHE52BMZfoAWJyknve+Cw2itsTaD95tzLVQ5yBMMH02XvypyoRSNwj
Agnl4D4f9Q6hWNFGPhME1bx+KSrAWX4bM+8kSco5IP3YEhsBQ5Y+pMVLqtYa8EKP
7BzVZadyF6lXe+gfKU+3+cZS2qwQQjrNfC3tE4jl8ejGDKcwBsn0g0xLmxx1JMJO
F25hwxKuuVVFdiEgTb0DpIZE/ycfNp+uI/fKDId0wWCX1OCGujW4eVWIo95iw9Ni
V2JBjHDHGbZZLA3z3UZ0rNZXWckGR8l8Tx7Mb5EqZ7fcPw2nefL91BatpAyPoZco
4Rs/ZNd4IoebbaFgo5L8JRw/VJn5t1k31lSnjYJxTqTRb2OSOM29/a2RKPecBnAG
hCxR4axo5e312YqvWT6PwqRkTOkgcM2LijvW5d0pxs004c8focvuo8YcNygjfMm/
yEAVoBArs8JMvXYOoTY+WUHgDQtdL1VdNj3cYcBXRg+V0fcwlAel4192B7gQ+UgI
9WQeFGRDyEyypL+tm3l5GGpFUUUxxbn/MJFxvvzupFGRQfFi1njkar92yNGJjnlG
326PmP08J77v8+mQeqbbAgMBAAGjEjAQMA4GA1UdDwEB/wQEAwIChDANBgkqhkiG
9w0BAQsFAAOCAgEATAn805/tWH5iqdUsGNnZFFddUUFiWBtp2Y+ung9D38NrTyMR
EhUfZtRBDKmblXltn+2dHiNac56OKpnDsnHz0zqiF4pygzn9XCQ9BpuLLbUBKY9P
KHwnSIWvCejGUQQJzTwhId1nCNwoZYJtPBIwCOkUlX4N+xBp1G4Han5mh0txwu/y
5CoDeo/EE7Cr0+kJdLGSV0L16UTE2Dv8FUGzbWroTTqoO1GlraBwCgfjey8cK1Kx
sZIF4W05an/ZA6kbHfNcDx/9g9v3daowcWyXWX1V2TaR3tnACU3YsHgxmGPOBvT2
VTBOAe9bEfJ4KNiPHxohN31i7PN2ACir7sjtbE7gzpxo/9JFLjXxFpbxB/n3TEqe
qsj8cw4p0b60T77Jlhv8VnHrLC25RqRK/7DhEVGyidv86KzMfvs2OmiYNQ1ffZJU
oI4r0n0JHpA8W1ebnExDj/sNve/4gSpdgKn7xtahfd0SoaL4TjEpuyRIKnfcf6lP
dVoygeDNPsaoqvFRvtCEZv5SzPAAG0gw8WO1kzVvndwtASd87TEYYJOB74KdYFvk
kpZqJ/uu5DX7jGhE0m+m1ighjNoYOTN97L0Gf4QpB7mjMDdLcXhKrXs4u/jDvpvT
ZwAT9nGACaxEYMTKWOfWLbVNX7M7nu74n5U9uIx048tAWmyXur5qUrgLJLw=
-----END CERTIFICATE-----
```

Verifying the authenticity with the cert's fingerprints

The SHA-1 and SHA-256 fingerprints for the FaaS certificate are:

```
SHA1 Fingerprint=B6:4B:43:75:5E:1D:24:DF:80:D1:BF:9A:A7:37:CD:D3:40:44:94:B1
SHA256 Fingerprint=3F:A3:6D:8E:B0:0B:44:C0:BA:65:97:03:E9:BA:32:E7:26:79:63:D4:79:02:EF:75:F1:1E:34:06:2C:E8:24:
C3
```

To be obtained with commands like (adjusting hash algorithm, `-sha1` or `-sha256`):

```
openssl x509 -noout -fingerprint -sha256 -in federation-metadata-signer.pem
```

HA setup

In order to provide high availability for the HSM signing, second HSM partition has been created on a different Luna SA appliance. This section describes steps that need to be taken in order to create high availability environment.

Certificate exchange

1. Register second Luna SA's certificate in the trust list on a client side.

   - Download second HSM appliance certificate and store it in /usr/safenet/lunaclient/cert/server/

   - Add HSM appliance certificate to the trust list:

```
vtl addServer -n se-fre-hsm1.sunet.se -c /usr/safenet/lunaclient/cert/server/se-fre-hsm1.sunet.se.crt
```

2. Verify that the Luna SA server is in the list of servers trusted by the client.

```
vtl listservers
```

3. Send client certificate to NUNOC in order to register client certificate on the second HSM appliance.
4. Verify partition visibility to the client.

```
vtl verify
```

> ⚠ Two partitions should be displayed.

HSM HA setup

1. Create HA group with first partition as a primary partition

```
vtl haAdmin newgroup -serialNum 462371008 -label faasHAgroup -password <password>
```

2. Add a second partition to the HA group

```
vtl haAdmin addMember -group 1462371008 -serialNum 462344017 -password <password>
```

3. Configure Client to show only HA virtual slots

```
vtl haAdmin HAOnly -enable
```