USING PRIVATE SIGNED CERTIFICATES WITH EEM

CA WORKLOAD AUTOMATION

This document describes how to use private (internally signed) certificates with EEM. Commercial Certificate Authorities (CA) like Verisign and Comodo no longer issue signed certificates for internal networks. Therefore a prerequisite to using this procedure is to have an internal CA setup. Clients (e.g. web browsers) should have the root and any intermediate certificates imported into their certificate store.

Note: It may be necessary to regenerate application certificates if the CA EEM server certificates are modified.

Steps

1. Login to the EEM host as the EEM software owner (typically root)
2. Change directory to $IGW_LOC (default: /opt/CA/SharedComponents/iTechnology)
3. Stop the iGateway service

```
./S99igateway stop
```

4. Set EIAM_HOME environment variable

```
export EIAM_HOME=/opt/CA/SharedComponents/EmbeddedEntitlementsManager
```

5. Change directory to $EIAM_HOME/bin
6. Run the eiam-clustersetup utility to generate a new 2048 key and SHA-2 certificates

```
java -jar eiam-clustersetup.jar
```

7. Enter 'Y' to continue

```
Are you sure you want to continue? [Y/N]:Y
```

8. At the prompt, run the modifycerts command

```
[<host>]> modifycerts
```

9. Select the certificate key length

```
INFO  - Enter Certificate Key Length [default = 1024]
INFO  -    [1] 1024
INFO  -    [2] 2048
INFO  -    [3] 4096
Select key length from [1 - 3] : 2
```

Warning: selecting a key length greater than 2048 may impact performance

10. Select the Digest Algorithm [default = SHA256]

```
INFO  - Enter Digest Algorithm [default = SHA256]
INFO  -    [1] SHA1
INFO  -    [2] SHA256
INFO  -    [3] SHA384
INFO  -    [4] SHA512
Select Digest algorithm from [1 - 4] : 2
```

11. Enter 'Y' to continue

```
=========================================================
INFO  - Summary
=========================================================
INFO  - Upgrading all certificates to key length: [2048]
INFO  - Upgrading all certificates to [digest algorithm : SHA256]
---------------------------------------------------------
Are you sure you want to continue? [Y/N]:Y
```

12. Enter 'exit' to close the eiam-clustersetup utility
13. Change directory to $IGW_LOC (default: /opt/CA/SharedComponents/iTechnology)
14. Generate a certificate signing request (CSR) based on the new key & certificate

```
openssl x509 -x509toreq -in igateway.cer -out igateway.csr \
-signkey igateway.key
```

15. Backup the existing certificate

```
mv igateway.cer igateway.cer.bak
```

16. Have the certificate request signed by your internal CA

    They will need to return the following in PEM format:

    a. the private (signed) certificate generated from the CSR

17. Put the new private (signed) certificate in place of the old igateway.cer file.

```
cp /root/igateway-myeemhost.pem $IGW_LOC/igateway.cer
```

18. Restart the iGateway service

```
./S99igateway start
```