This document outlines the steps required to configure DASH systems for HTTPS communication using self-signed certificates.

**Requirements**

1. Download and install the latest available OpenSSL package ([http://www.openssl.org/](https://community.amd.com/external-link.jspa?url=http%3A%2F%2Fwww.openssl.org%2F)).

a. Ensure openssl.exe is in **%PATH%**

b. Ensure that the environment variables has the variable “OPENSSL\_CONF”

**OPENSSL\_CONF**

**C:\Program Files\OpenSSL-Win64\bin\cnf\openssl.cnf**

2. Sample **ini** is specified in **Appendix A**. Save the contents as openssl.ini and modify the file based on your organization requirement.

Size must be set to 2048. All other sizes are unsupported.

**default\_bits = 2048**

a. Per device certificate: A per device certificate can be generated and installed on that particular device (Eg: dash-system.myorg.com). Per device certificate can be generated on alternate names of the systems and also on IP address. For per per device option, under “alt\_names” section, add value for key “DNS.1”, “DNS.2 and “IP.1”. Eg,

**DNS.1   = dash-system.myorg.com <DNS name of DASH system>**

**DNS.2   = dash-system**

**IP.1    = 10.10.10.100 <IP address of DASH system, e.g. 192.168.1.10>**

3. NIC Management Controller specific requirements are mentioned in **Section D**

**Note:** The steps below are tested with OpenSSL 1.1.1d version.

**Section A: Generate Root certificate**

A Root certificate is common to the whole organization. It is generated only once and installed in the certificate store.

**1)    Create folders & copy openssl.ini**

**mkdir DASHCert**

**cd DASHCert**

**copy ..\openssl.ini DASHCert**

**mkdir newcerts private**

**2)    Create requisite files**

**echo 01 > serial**

**copy /y nul index.txt**

**3)    Create root certificate**

**Note:** For ‘Common Name’, specify the name of the root authority. For instance like 'DASH Root Authority'.

**openssl genrsa -out private/cakey.pem 1024**

**openssl req -new -x509 -extensions v3\_ca -key private/cakey.pem -out cacert.pem -days 3650 -sha256 -config ./openssl.ini**

**openssl x509 -in cacert.pem -out DASHCA.crt**

**Section B: Add root certificate to certificate store on the system with DASH Console**

Root certicate must be installed in the certificate store on all console systems where DASH applications like DASH CLI, AMD Management Console and AMPS are installed.

**1. Windows OS system with DASH Console**

1. Copy DASHCA.crt to DASH Console.

2. Import to certificate store:

a. Right click on DASHCA.crt and select 'Install Certificate'

b. Select “Local Machine” as Store Location

c. Click Next and select 'Place all certificates in the following store'

d. Click Browse and select 'Trusted Root Certification Authorities'

e. Click Next & Finish

**Section C: Generate per-device certificate**

**Continuation of the steps from Section A.**

**1)    Create certificate signing request**

**Note:** For ‘Common Name’, specify the generic (Eg: \*.myorg.com).

**openssl req -new -nodes -out req.pem -sha256 -extensions v3\_req -config ./openssl.ini**

**2)    Sign certificate**

**openssl ca -out cert.pem -extensions v3\_req -config ./openssl.ini -infiles req.pem**

**3)    Strip readable text**

**move cert.pem tmp.pem**

**openssl x509 -in tmp.pem -out cert.pem**

**Section D: Import certificate on the DASH System**

Executing the commands below will over-write the existing certificate details.

For shared mode use the following command:

**AqDashConfig.exe shared admin adminpass cert.pem key.pem**

For exclusive mode use the following command:

**AqDashConfig.exe exclusive admin adminpass cert.pem key.pem --mac 00:17:B6:10:10:10 --ip 192.168.1.10**

**Section E: Verification**

To verify the certificate installed correctly and DASH HTTPS is working.

**1)    Via DASH CLI**

Run a DASH CLI https command without -C option. DASH CLI must provide the output without any error.

**dashcli -h dash-system.myorg.com -p 664 -S https -a digest -u admin -P adminpass -t computersystem[0] power status**

**dashcli -h 192.168.1.10 -p 664 -S https -a digest -u admin -P adminpass -t computersystem[0] power status**

**Appendix A - Sample openssl.ini**

**# OpenSSL configuration file.**

**#----Begin----**

**# Establish working directory.**

**dir = .**

**[ ca ]**

**default\_ca = CA\_default**

**[ CA\_default ]**

**serial = $dir/serial**

**database = $dir/index.txt**

**new\_certs\_dir = $dir/newcerts**

**certificate = $dir/cacert.pem**

**private\_key = $dir/private/cakey.pem**

**default\_days = 3650**

**default\_md = sha256**

**preserve = no**

**email\_in\_dn = no**

**nameopt = default\_ca**

**certopt = default\_ca**

**policy = policy\_match**

**[ policy\_match ]**

**countryName = match**

**stateOrProvinceName = match**

**organizationName = match**

**organizationalUnitName = optional**

**commonName = supplied**

**emailAddress = optional**

**[ req ]**

**default\_bits = 2048**

**default\_keyfile = key.pem**

**default\_md = sha256**

**string\_mask = nombstr**

**distinguished\_name = req\_distinguished\_name**

**[ req\_distinguished\_name ]**

**# Variable name Prompt string**

**#---------------------- ----------------------------------**

**0.organizationName = Organization Name (company)**

**organizationalUnitName = Organizational Unit Name (department, division)**

**emailAddress = Email Address**

**emailAddress\_max = 40**

**localityName = Locality Name (city, district)**

**stateOrProvinceName = State or Province Name (full name)**

**countryName = Country Name (2 letter code)**

**countryName\_min = 2**

**countryName\_max = 2**

**commonName = Common Name (hostname, IP, or your name)**

**commonName\_max = 64**

**# Default values for the above, for consistency and less typing.**

**# Variable name Value**

**#------------------------------ ------------------------------**

**0.organizationName\_default       = MyOrg Inc**

**organizationalUnitName           = IT**

**countryName\_default              = IN**

**stateOrProvinceName\_default      = KA**

**localityName\_default             = Bangalore**

**emailAddress\_default             =**[**it@myorg.com**](mailto:it@myorg.com)

**organizationalUnitName\_default   = IT Department**

**commonName\_default               = \*.myorg.com**

**[ alt\_names ]**

**# Hostname of target with FQDN can also be entered in the form \*.domain.com**

**DNS.1      = \*.myorg.com**

**#DNS.2     = dash-system.myorg.com**

**#DNS.3     = dash-system**

**# IP address can be allowed with the IP Key**

**#IP.1      = 10.10.10.100**

**[ v3\_ca ]**

**basicConstraints = CA:TRUE**

**subjectKeyIdentifier = hash**

**authorityKeyIdentifier = keyid:always,issuer:always**

**keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign**

**subjectAltName = @alt\_names**

**[ v3\_req ]**

**basicConstraints = CA:FALSE**

**keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign**

**subjectAltName = @alt\_names**

**#----End----**