

How to use self-signed certificates for HTTPS communication

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/>).
 - 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 **openssl.ini** is specified in **Appendix A**. Save the contents as openssl.ini and modify the file based on your organization requirement.
 - a. Organization wide certificate: A common certificate can be generated and installed on all DASH systems in the organization (by giving Common Name as *.myorg.com). For an organization wide option, under "alt_names" section, add the key "DNS.1" Eg,

```
DNS.1    = *.myorg.com
```
 - b. 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.2    = dash-system  
IP.1     = 10.10.10.100
```
3. NIC Management Constroller specific requirements are mentioned in **Section D**

Note: The steps below are tested with OpenSSL 1.1.1i 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 certificate 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

- i. Copy DASHCA.crt to DASH Console.
- ii. 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

2. Ubuntu OS system with DASH Console

- i. Copy DASHCA.crt to DASH Console

```
sudo mkdir /usr/share/ca-certificates/extra
sudo cp DASHCA.crt /usr/share/ca-certificates/extra
sudo dpkg-reconfigure ca-certificates
```
- ii. A new UI window will be open -> Select YES
- iii. Give space to select the DASHCA.crt in Trusted certificates

```
sudo update-ca-certificates
```

3. Fedora OS system with DASH Console

- i. Copy DASHCA.crt to DASH Console

```
sudo cp DASHCA.crt /etc/pki/ca-trust/source/anchors
sudo update-ca-trust
```

Section C: Generate organization-wise or 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
```

4) Convert to DER format

```
openssl rsa -in key.pem -inform PEM -out DASHKey.der -outform DER
```

```
openssl x509 -in cert.pem -inform PEM -out DASHCert.der -outform DER
```

Section D: Import certificate on the DASH System

Executing the commands below will over-write the existing certificate details. Procedure to install certificate on a DASH System varies based on Management Controller:

1) Realtek Management Controller

Note: Sample **config.xml** is specified in Appendix B

- i) Ensure **DASHConfigRT** folder is present in your DASH Application folder
- ii) Copy DASHConfigRT folder to the DASH System
- iii) Copy the files 'DASHKey.der' & 'DASHCert.der' to DASH System
- iv) Copy the file config.xml to the same folder as DASHConfigRT.exe and update config.xml as required.
- v) Using DASHConfigRT, install the certificate files with one of the commands:

- (1) Configure username, password and install certificate

```
DASHConfigRT.exe -xf:config.xml -cert:DASHCert.der -priv:DASHKey.der
```

- (2) Only to update the certificates

```
DASHConfigRT.exe -cert:DASHCert.der -priv:DASHKey.der
```

2) Broadcom Management Controller

Note: Sample config.xml is specified in Appendix C

- i) Ensure **DASHConfig** folder is present in your DASH Application folder
- ii) Copy DASHConfig folder to the DASH System
- iii) Copy the files 'DASHKey.der' & 'DASHCert.der' to DASH System
- iv) Copy the file config.xml to the same folder as DASHConfig.exe and update config.xml as required.
- v) Using DASHConfig, install the certificate files with the commands:

```
DASHConfig.exe -xf:config.xml
```

3) Marvell Management Controller

- 1) Ensure **DASHAgent** folder is present in your DASH Application folder
- 2) Copy DASHAgent folder to the DASH System
- 3) Copy the files 'cert.pem' & 'key.pem' to DASH System
- 4) Configure the NIC

1. Shared mode

Command: Configure Shared Mode

```
AqDashConfig0.27 <mode> <username> <password> <certificate> <key>
```

Example:

```
AqDashConfig0.27 shared admin adminpass cert.pem key.pem
```

2. Exclusive mode with MAC 00:17:B6:00:00:08 and IP 10.138.135.159

Command: Configure Exclusive Mode

```
AqDashConfig0.27 <mode> <username> <password> <certificate> <key>  
--mac <MAC IC> --ip <IPAddress>
```

Example:

```
AqDashConfig0.27 exclusive admin adminpass cert.pem key.pem --mac  
00:17:B6:00:00:08 -ip 10.138.135.159
```

5) Install Aquantia DASH Agent

1. Launch the command prompt as Administrator and get into DASHAgent folder
2. If service is already running uninstall and then install

Command: Uninstall DASH Agent

```
AqDashAgent0.27 uninstall
```

Command: Install DASH Agent

```
AqDashAgent0.27 install
```

Section E: Verification

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

1) Via browser

Open the link <https://dash-system.myorg.com:664/> in either Chrome or Internet Explorer. The browser must report the site as secure and the TLS certificate must match with that generated in **Section A**.

2) 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
```

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 = 1024
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
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----
```

Appendix B - Sample config.xml for Realtek Management Controller

```
<?xml version="1.0" encoding="utf-8" ?>
<DASHPROVISIONSETTINGS>
  <MANAGEMENTTARGET>
    <GLOBAL>
      <HTTPS>
        <ENABLESUPPORT>true</ENABLESUPPORT>
        <TCPIPPORT>664</TCPIPPORT>
      </HTTPS>
      <HTTP>
        <ENABLESUPPORT>true</ENABLESUPPORT>
        <TCPIPPORT>623</TCPIPPORT>
      </HTTP>
    </GLOBAL>
    <USERS>
      <USER>
        <USERID>admin</USERID>
        <PASSWORD>adminPass</PASSWORD>
        <ENABLE>true</ENABLE>
        <ROLES>
          <ROLE>Administrator Role</ROLE>
        </ROLES>
      </USER>
    </USERS>
  </MANAGEMENTTARGET>
</DASHPROVISIONSETTINGS>
```

Appendix C - Sample config.xml for Broadcom Management Controller

```

<?xml version="1.0" encoding="utf-8" ?>
<DASHPROVISIONSETTINGS>
  <MANAGEMENTTARGET>
    <GLOBAL>
      <HTTPS>
        <ENABLESUPPORT>true</ENABLESUPPORT>
        <TCPIPPORT>664</TCPIPPORT>
        <HTTPREALM>Broadcom Management Service</HTTPREALM>
        <HTTPSTARGETTOCONSOLE>
          <CERTIFICATEPATH>DASHCert.der</CERTIFICATEPATH>
        </HTTPSTARGETTOCONSOLE>
      </HTTPS>
      <HTTP>
        <ENABLESUPPORT>true</ENABLESUPPORT>
        <TCPIPPORT>623</TCPIPPORT>
      </HTTP>
    </GLOBAL>
    <USERS>
      <USER>
        <USERID>admin</USERID>
        <PASSWORD>adminPass</PASSWORD>
        <ENABLE>true</ENABLE>
        <ROLES>
          <ROLE>Administrator Role</ROLE>
        </ROLES>
      </USER>
    </USERS>
  </MANAGEMENTTARGET>
</DASHPROVISIONSETTINGS>

```