TEST/Eval Certificates for CableLabs Remote PHY Interop Authentication Testing

These test certificates are intended for development and testing purposes. They are not issued from the real CA chain. PEM and DER cert encodings are provided in their respective subdirectories

Installation Instructions:

The TEST_CableLabsRootCA_Cert is installed in the AAA server, CCAP Core, and RPD as a root trust anchor certificate for validating received certiciates from other devices.

The TEST_CableLabsDeviceCA_Cert is installed in the RPD along with the RPD device cert and private key. It should be sent with the RPD device cert during authentication messaging.

The TEST_CableLabsServiceProviderCA_Cert is installed in the AAA server along with the AAA server cert and private key. It should be sent with the AAA server cert during authentication messaging.

The TEST_CableLabsServiceProviderCA_Cert is installed in the CCAP Core along with the CCAP Core server cert and private key. It should be sent with the CCAP Core server cert during authentication messaging.

Generating an RPD TEST Cert & private key using OpenSSL:

1.Download and configure OpenSSL to work in current environment from https://www.openssl.org/

2.Create a configuration text file for the certificate signing request (CSR). Name the file "csr_config.txt" and put the following information into the file (<> characters indicate information to be entered by company):

```
[ req ]
default_keyfile       = TEST_Device_PrivateKey.pem
default_md      = sha256
prompt                = no
string_mask           = nombstr
distinguished_name    = req_DN

# Certificate Distinguished Name
[ req_DN ]
C               = <2 Digit Country Code>
O               = <Company Name>
OU              = <Manufacturing Location>
CN              = <MAC Address, see spec for format>
```

3.Create a CSR and a new private key for the TEST RPD device cert using the csr_config.txt file. Enter the following OpenSSL command at the command

prompt:

```
Openssl req -newkey rsa:2048 -config csr_config.txt -out csr.pem
-nodes
```

4.Create a extension text file for the TEST RPD device cert. Name the filE "ext.txt" and put the following information into the file:

```
keyUsage=critical,digitalSignature,keyEncipherment
authorityKeyIdentifier=keyid
```

5.Create a TEST RPD device certificate. Enter the following OpenSSL command at the command prompt:

```
Openssl x509 -req -days 7305 -in csr.pem -CA
TEST_CableLabsDeviceCA_Cert.pem -CAkey
TEST_CableLabsDeviceCA_PrivateKey_pkcs8.pem -CAcreateserial
-extfile ext.txt -sha256 -out TEST_RPD_DEVICE_Cert.pem
```

NOTE: The test certificate created in step #5 (TEST_RPD_DEVICE_Cert.pem) along with the private key created in step #3 (TEST_Device_PrivateKey.pem) is installed into the RPD along with the TEST_CableLabsDeviceCA_Cert for authentication testing.

Generating a AAA or CCAP Core server TEST Cert & private key using OpenSSL:

1.Download and configure OpenSSL to work in current environment from https://www.openssl.org/

2.Create a configuration text file for the certificate signing request (CSR). Name the file "csr_config.txt" and put the following information into the file (<> characters indicate information to be entered by company):

```
[ req ]
default_keyfile       = TEST_Server_PrivateKey.pem
default_md      = sha256
prompt                = no
string_mask           = nombstr
distinguished_name    = req_DN

# Certificate Distinguished Name
[ req_DN ]
C               = US
O               = CableLabs
CN              = <server FQDN>
```

3.Create a CSR and a new private key for the TEST server cert using the csr_config.txt file. Enter the following OpenSSL command at the command prompt:

Openssl req -newkey rsa:2048 -config csr_config.txt -out csr.pem -nodes

4.Create a extension text file for the TEST server cert. Name the filE "ext.txt"□and put the following information into the file:

```
keyUsage=critical,digitalSignature,keyEncipherment
authorityKeyIdentifier=keyid
subjectKeyIdentifier=hash
subjectAltName=DNS:<server FQDN>
```

5.Create a TEST server certificate. Enter the following OpenSSL command at the command prompt:

```
Openssl x509 -req -days 730 -in csr.pem -CA
TEST_CableLabsServiceProviderCA_Cert.pem -CAkey
TEST_CableLabsServiceProviderCA_PrivateKey_pkcs8.pem
-CAcreateserial -extfile ext.txt -sha256 -out TEST_Server_Cert.pem
```

NOTE: The test certificate created in step #5 (TEST_Server_Cert.pem) along with the private key created in step #3 (TEST_Server_PrivateKey.pem) is installed into a AAA or CCAP Core server along with the TEST_CableLabsServiceProviderCA_Cert for server authentication.

WARNING: Test certificates provide no security. Therefore, when you use the test certificates you are agreeing to use the test certificates only for development, testing and evaluation purposes and not to use the test certificates in production devices. You are also agreeing that: (1) CableLabs is providing the test certificates and all related documentation AS IS and without any warranty expressed, implied or by law, and (2) CableLabs is not liable for any damages arising from or related to your use of the test certificates and all related documentation.