SMP/E Internet Service Retrieval and FTP with SSL changes

With CA Support integration into the Broadcom Support portal, customers using SMP/E Internet Service Retrieval (RECEIVE ORDER) or customers who transfer files via FTP with SSL will need to make the following updates.

SMP/E Internet Service Retrieval

1. Download and install the new Digicert CA certificate:
    a. Download new certificate.
    b. Upload new certificate to z/OS.
    c. Add Digicert CA certificate to a key ring in CA ACF2, CA Top Secret, or IBM RACF as applicable.
2. Allow firewall access to the CA Automated Order Server and CA Download Server:
    a. Replace **eapi.ca.com** with **eapi.broadcom.com**.
    b. Replace **apidev.ca.com** with **rdownloads.broadcom.com**.
3. Update the ORDERSERVER XML in your RECEIVE ORDER JCL as follows:

    Replace url="https://**eapi.ca.com**/receiveorder" with url="https://**eapi.broadcom.com**/receiveorder"
4. If you created a new keyring, you will update the certificate name in the RECEIVE ORDER JCL.

FTP with SSL

1. Download and install the new Digicert CA certificate:
    a. Download new certificate.
    b. Upload new certificate to z/OS.
    c. Add Digicert CA Certificate for SSL Connection to CA ACF2, CA Top Secret, or IBM RACF as applicable.

For a complete list of URL and IP address changes, click here.

Download New Certificate

Download the new Digicert CA certificate.

Important! If you have used Receive Order prior to the migration, you ***do not*** need to download a new User certificate. ***You can use your existing User certificate.***

The GeoTrust Global certificate and GoDaddy certificate are no longer used by Receive Order.

Follow these steps:

1. Use the following link to download the Digicert CA certificate for SMP/E Internet Service Retrieval:

   https://casupport.broadcom.com/cadocs/0/certs/eapi/digi-intermediate.crt

2. Note the location of the file on your workstation where the certificate was downloaded.

Upload the Certificate to z/OS

Upload the Server certificate you saved to your workstation to z/OS.

Follow these steps:

1. Upload the Certificate as text data to your z/OS system in RECFM=VB and LRECL>=84 format.

   Note: When uploading the certificate to z/OS, be sure the appropriate WRAP parameter is specified so that the data is wrapped to the next record if no new line character is encountered before the logical record length of the receiving file is reached.

2. If you use FTP, use the following FTP commands to avoid truncation:

```
ASCII
QUOTE SITE WRAP LRECL=256 RECFM=VB
PUT cert_file_name 'your.mvs.dataset.name' (REPLACE
quit
```

Add Digicert CA Certificate to Key Ring

Configure CA ACF2, CA Top Secret, or IBM RACF security as applicable to add the EAPI Digicert Server certificate to a key ring.

Note: These procedures assume that you are going to use your existing Receive Order key ring. If you create a new key ring, you will add your existing User certificate and the new EAPI Digicert Certificate Authority certificate.

CA Top Secret

1. Add the Digicert CA certificate to the CA Top Secret database:

```
TSS ADD(CERTAUTH) DIGICERT(yourcertname) LABLCERT(yourcertname)-
    DCDSN('your.mvs.dataset.name') TRUST
```

2. Connect the certificate to the user keyring:

```
TSS ADD(user1) KEYRING(yourRingName) RINGDATA(CERTAUTH,yourcertname)-
USAGE(CERTAUTH)
```

CA ACF2

1. Add the Digicert CA certificate to the CA ACF2 database:

```
SET PROFILE(USER) DIV(CERTDATA)
INSERT certauth.yourcertname DSN('your.mvs.dataset.name') -
  LABLCERT(your label description)
```

2. Connect the certificate to the user key ring:

```
SET PROFILE(USER) DIV(KEYRING)
PROFILE
CONNECT CERTDATA(CERTAUTH.yourcertname) KEYRING(yourRingname) USAGE(CERTAUTH)
```

RACF

1. Add the Digicert CA certificate to RACF:

```
RACDCERT CERTAUTH ADD('your.mvs.dataset.name') +
WITHLABEL('your label description') TRUST
```

2. Connect the certificate to the key ring:

```
RACDCERT ID(ring-owner) CONNECT(CERTAUTH LABEL('your certificate name') +
RING(yourRingname) USAGE(CERTAUTH))
```

Add Digicert CA Certificate for SSL Connection

A Certificate Authority certificate is required to validate the SSL connection. The supportftp.broadcom.com server uses a server certificate signed by Certificate Authority (CA).

Use the following commands to add the new certificate:

CA Top Secret

```
TSS ADD(CERTAUTH) DIGICERT('yourcertname') LABLCERT('yourlabelname') -
       DCDSN('your.mvs.dataset.name') TRUST

TSS PER(userid) IBMFAC(IRR.DIGTCERT.LISTRING) ACC(UPDATE)
```

CA ACF2

```
SET PROFILE(USER) DIV(CERTDATA)

INSERT CERTAUTH.yourcertname DSN('your.mvs.dataset.name') LABEL(yourlabelname) TRUST

$KEY (IRR.DIGTCERT.LISTRING) TYPE(FAC) UID(userid) SERVICE(UPDATE) ALLOW
```

RACF

```
RACDCERT CERTAUTH ADD('your.mvs.dataset.name') WITHLABEL('yourlabelname') TRUST

PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(userid) ACCESS(UPDATE)
```