SMP/E Internet Service Retrieval Configuration

Katie Juhala (Katie.Juhala@Broadcom.com)
October 2022

BROADCOM

Hello and welcome to this presentation on SMP/E Internet Service Retrieval Configuration.

Disclaimer

Certain information in this presentation may outline CA's general product direction. This presentation shall not serve to (i) affect the rights and/or obligations of CA or its licensees under any existing or future license agreement or services agreement relating to any CA software product; or (ii) amend any product documentation or specifications for any CA software product. This presentation is based on current information and resource allocations as of 15th October 2021 and is **subject to change or withdrawal by CA at any time without notice**. **The development, release and timing of any features or functionality described in this presentation remain at CA's sole discretion**.

Notwithstanding anything in this presentation to the contrary, upon the general availability of any future CA product release referenced in this presentation, CA may make such release available to new licensees in the form of a regularly scheduled major product release. Such release may be made available to licensees of the product who are active subscribers to CA maintenance and support, on a when and if-available basis. The information in this presentation is not deemed to be incorporated into any contract.

THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY. Broadcom assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will Broadcom be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if Broadcom is expressly advised in advance of the possibility of such damages.

Please note the disclaimer.

SMP/E Internet Service Retrieval Overview

- Summary
  - What is SMP/E Internet Service Retrieval?
  - How does SMP/E Internet Service Retrieval work?
  - Obtain the Certificates for SMP/E Internet Service Retrieval
  - Create the Keyring and Add the Certificates
  - Setup User Access to Certificate and Keyring
  - Sample SMP/E RECEIVE ORDER JCL

Terms:
ESM refers to ACF2, Top Secret, RACF
Userid refers to ACF2 logonid, Top Secret acid and RACF userid
CA refers to Certificate Authority

BROADCOM

In this presentation, we will go over what SMP/E Internet Service Retrieval is in addition to a high level overview of how it works. We will show you where to obtain the digital certificates required for the configuration and give sample commands for creating a keyring to add the certificates to. There will also be sample commands for granting user access to the certificates and keyring. Lastly, we will go over the fields in the sample SMP/E Receive Order JCL and explain how to point to the keyring we created. Some terms we will be using include ESM which refers to ACF2, Top Secret, and RACF. UserID which refers to an ACF2 logonid, Top Secret ACID, and RACF userID. And CA which refers to a Certificate Authority. All commands and links in the presentation will be included in a text file available for download.

SMP/E Internet Service Retrieval Overview

What is SMP/E Internet Service Retrieval?

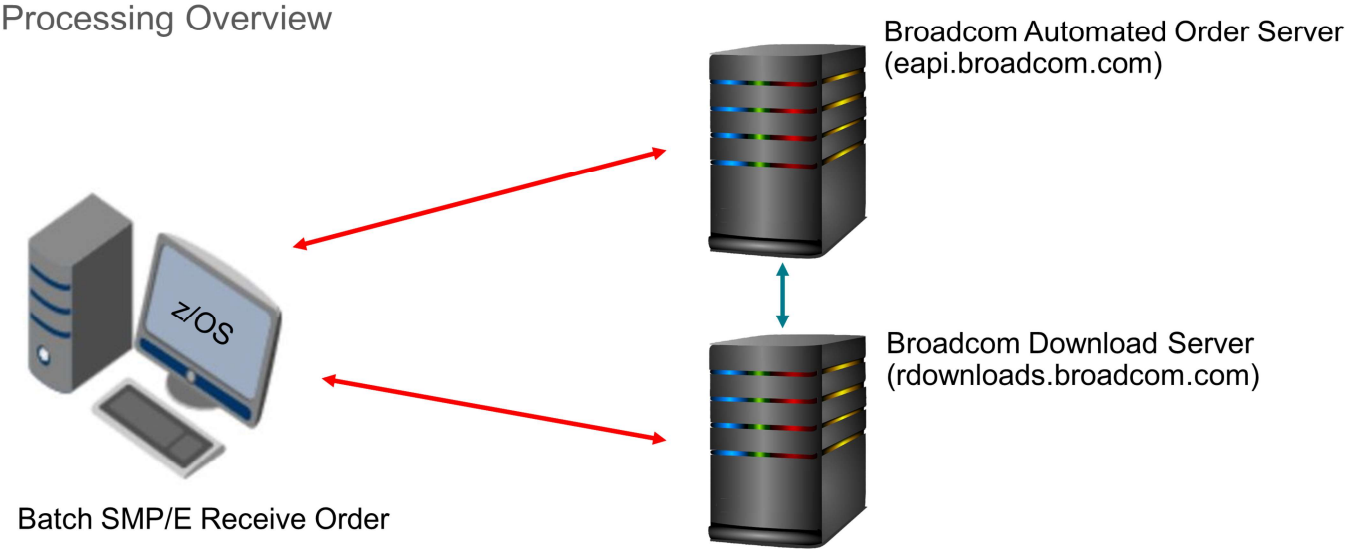
- Allows a site to obtain software service over the Internet.
- The SMP/E job uses a new form of the RECEIVE command to place a service request, waits for the request to be fulfilled and automatically downloads to the system, all in one step.
  - Order Types:
    a) All Missing PTFs
    b) HOLDDATA
    c) CRITICAL only
    d) Recommended Service
    e) Specific PTFS or APARs
- Service requests can be made on demand or scheduled SMP/E service request jobs can be used to automate the service delivery process.

BROADCOM

SMP/E Internet Service Retrieval allows a site to obtain maintenance from the internet by running an SMP/E job on the mainframe. The SMP/E job issues a new form of the RECEIVE command to place a service request to the order server, which then goes out to a download server that fulfills the request. This process appears all as one step to the end user. Various types of order requests can be made including missing PTFS, HOLDDATA, CRITICAL only, recommended service, and even specific PTFs or APARs can be requested. With SMP/E Internet Service Retrieval, service requests can be made on demand or can also be ran as scheduled jobs which allows for a more automated approach to downloading maintenance. Setting up SMP/E Internet Service Retrieval greatly simplifies the maintenance retrieval process and is a better method than manually going out to Broadcom's support website to download PTFs to then upload and apply to the Mainframe.

SMP/E Internet Service Retrieval Overview

Processing Overview



For a high level overview of how SMP/E works behind the scenes, on the left we have a terminal user who submits a batch SMP/E Receive order job. It communicates to the Broadcom Automated Order server which processes the request and stages package file to the Broadcom Download server. The order server provides SMP/E with the information to authenticate with the CA Download server and then download the package files. More specifically, the order server provides SMP/E with the Broadcom Download server host name and a temporary user ID and password for that server, which are unique for the specific package to be downloaded. SMP/E then goes out to the Broadcom Download Server to download the maintenance. Again, this process appears as all one step to the user submitting the job.

SMP/E Internet Service Retrieval Overview

Identity and Authentication using SSL

Three Certificates are Required:

1. User Certificate
2. Server Digicert Intermediate CA Certificate
3. Server Digicert Root CA Certificate

- User Certificate: Identifies the client (SMP/E Userid) to the Broadcom servers.
- Server CA certificates: Allow the client SMP/E application to confirm the identity of the Broadcom server application.

All communications between the client and the Broadcom order and download servers are performed using an SSL connection so the data is encrypted. To accomplish this, both the client (which is SMP/E) and the server use X.509 certificates. There are three certificates that are required. These include the user certificate which identifies the client (which is the SMP/E Userid) to the Broadcom Servers and two server Digicert certificates that serve to confirm the identity of the Broadcom server application. In the next slides, we will go over how to download these certificates.

SMP/E Internet Service Retrieval Overview

Obtain the Certificates for SMP/E Internet Service Retrieval

User Certificate for Client

Import a User Certificate from Broadcom Support Online.

1. Register at https://support.broadcom.com/
2. Go to the Broadcom Support Online Certificate site at https://eapi.broadcom.com/receiveorder/getSignedCert

   Note: This will need to be completed every year as the expiration date for the user certificate is exactly one year from download
3. A certificate dialog opens (see next slide).

To get started, you must be a registered user on Broadcom Support. If you are not already a registered user, you can become one by registering at support.Broadcom.com. After registering or if you are already registered, go to the Broadcom Support Certificate site. You will be prompted to log in if not already logged in. Enter the email and password you registered with for Broadcom Support.
This process will need to be completed every year because the user certificate has an expiration date of one year from download.
A certificate dialog window will open as shown on the next slide.

SMP/E Internet Service Retrieval Overview

Obtain the Certificates for SMP/E Internet Service Retrieval

User Certificate for Client

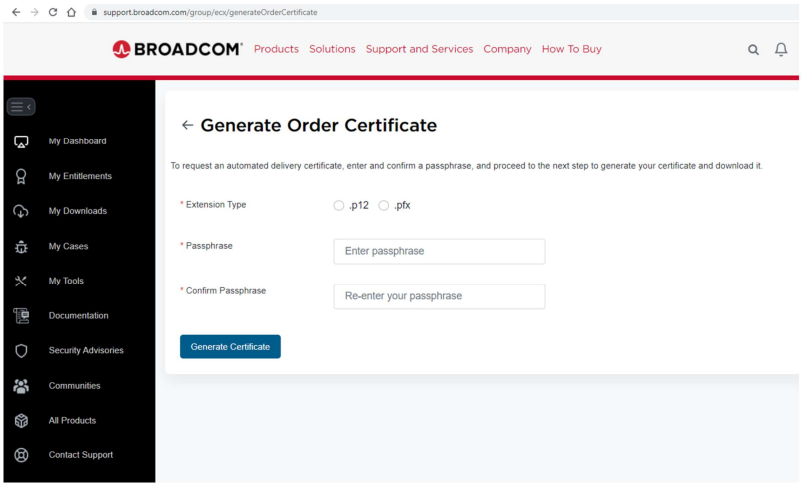
Complete the following tasks:

a) Select .p12 or .pfx for the download file type.

b) Enter an encryption passphrase.

Remember this passphrase as it must be specifed again later when adding the certificate to the ESM database.

c) Click Generate Certificate to download your user certificate.



BROADCOM

On the Generate Order Certificate page, Select the extension type. Either .p12 or .pfx can be selected.
Enter an encryption passphrase that will be used to encrypt the PKCS12 package that contains the user certificate and its associated private key.
*Remember this passphrase, y*ou must specify it again later when adding the certificate to your ESM database. Be mindful that this passphrase is case sensitive.
Click the **Generate Certificate** button to save the certificate to your workstation. Be sure to take note of the location of the certificate file on your workstation.

SMP/E Internet Service Retrieval Overview

Obtain the Certificates for SMP/E Internet Service Retrieval

Digicert Certificate Authority (CA) Intermediate and Root certificates to authenticate the Broadcom Automated Order Server

1. Download the Digicert CA Intermediate certificate:
   https://ftpdocs.broadcom.com/cadocs/0/certs/digi-inter-new/digicert_intermediate_2031.crt
2. Download the Digicert CA Root certificate:
   https://support.broadcom.com/cadocs/0/certs/eapi/digi-root.crt
3. Note the location of the files **digicert_intermediate_2031.crt** and **digi-root.crt** on your workstation where the certificate was downloaded.

Next, we will need to download the two server certificates by going to the two websites listed. These links will be provided in a text file that accompanies this presentation. Be sure to take note of the location of the certificate file on your workstation. It will make things easier during the upload process if all 3 certificates are in the same location.

https://ftpdocs.broadcom.com/cadocs/0/certs/digi-inter-new/digicert_intermediate_2031.crt
https://support.broadcom.com/cadocs/0/certs/eapi/digi-root.crt

SMP/E Internet Service Retrieval Overview

Obtain the Certificates for SMP/E Internet Service Retrieval

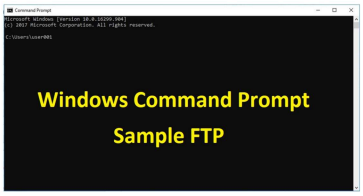
Upload the certificates to z/OS

Sample FTP commands:

FTP host.name
User (host.name:(none)): user1
331 Send password please.
Password: xxxxxxxx
ASCII
QUOTE SITE LRECL=84 RECFM=VB
PUT **ca-receive-order.cer** 'user.mvs.dataset.name'
PUT **digicert_intermediate_2031.crt** 'digiint.mvs.dataset.name'
PUT **digi-root.crt** 'digiroot.mvs.dataset.name'
quit

Important formatting parameters:

- RECFM=VB
- LRECL=84
- ASCII



BROADCOM

After downloading the 3 certificates, it is time to upload them to z/OS. You may choose whatever method you would like, but there are important formatting parameters to keep in mind. When uploading, be sure to specify rec fm = VB, lrecl = 84, and ASCII. Here we also give you sample FTP commands that can be used in your favorite workstation terminal. In your terminal, navigate to the directory where your certificates are stored and issue the following commands one at a time, substituting the blue fields for your own information.

SMP/E Internet Service Retrieval Overview

Create the Keyring and Add and CONNECT the Certificates Overview

Steps Overview:

- Create the Keyring
- Insert the certificates into the ESM database from the uploaded z/OS datasets
- Connect the certificates to the Keyring

Even though the exact commands differ for each security product, it is important to remember that the overall steps to accomplish are the same. In the following slides, we will cover how to create the keyring, insert the certificates into the database, and connect them to the keyring we created. We will do this for each security product.

SMP/E Internet Service Retrieval Overview

Create the Keyring and Add and CONNECT the Certificates with **ACF2**

* Create the Keyring
SET PROFILE(USER) DIV(KEYRING)
INSERT user1.ring RINGNAME(SMPERING)

Note: "user1" is the logonid that owns the keyring.

* Insert the certificates from the uploaded z/OS datasets
SET PROFILE(USER) DIV(CERTDATA)
INSERT certauth.digiroot DSN(digiroot.mvs.dataset.name) LABEL(Digicert Root CA) TRUST
INSERT certauth.digiint DSN(digiint.mvs.dataset.name) LABEL(Digicert Intermediate CA) TRUST
INSERT user1.cert DSN(user.mvs.dataset.name) LABEL(SMPE Client Certificate) **PASSWORD(xxxxxxxx)** TRUST

Note: Issue the following CHANGE command if the INSERT of "user1.cert" results with message 'ACF6D075 The signing certificate COULD NOT BE FOUND. Adding certificate with NOTRUST status'

CHANGE user1.cert TRUST

* Connect the certificates to the Keyring
SET PROFILE(USER) DIV(KEYRING)
CONNECT CERTDATA(user1.cert) KEYRING(user1.ring) USAGE(PERSONAL)
CONNECT CERTDATA(certauth.digiint) KEYRING(user1.ring) USAGE(CERTAUTH)
CONNECT CERTDATA(certauth.digiroot) KEYRING(user1.ring) USAGE(CERTAUTH)

BROADCOM

Here are the commands for ACF2. We start by creating a keyring. Please note on the insert of the keyring that the first qualifier (in this example user1) is the logonid that owns the keyring. After creating the keyring, add each of the 3 certificates that were uploaded in the previous section to the ACF2 database. Make a note of the certificate label for the user certificate (in this example "SMPE Client Certificate") as this will be needed later when setting up the SMP/E JCL. *Note the password that is specified on the INSERT of the user1 certificate., this password should be the same encryption password specified when the certificate was generated.* If during the add of the user certificate you receive a ACF2 message saying "The signing certificate COULD NOT BE FOUND. Adding certificate with NOTRUST status" issue the following change command. After the certificates have been inserted into the database, they are ready to be connected to the keyring using the ACF2 CONNECT command.

SMP/E Internet Service Retrieval Overview

Create the Keyring and Add and CONNECT the Certificates with **Top Secret**

Create the Keyring

```
TSS ADD(user1) KEYRING(SMPERING) LABLRING(SMPERING)
```

Note: "user1" is the ACID that owns the keyring. The information in the KEYRING and LABLRING parameters can be different. The information in KEYRING is needed for the connect step and if creating ring specific rules for validation. LABLRING is used when pointing to the keyring in the SMP/E RECEIVE ORDER JCL.

* Insert the certificates from the uploaded z/OS datasets

```
TSS ADD(CERTAUTH) DIGICERT(DIGIROOT) LABLCERT('Digicert Root CA') –
  DCDSN(digiroot.mvs.dataset.name) TRUST
TSS ADD(CERTAUTH) DIGICERT(DIGIINT) LABLCERT('Digicert Intermediate CA') –
  DCDSN(digiint.mvs.dataset.name) TRUST
TSS ADD(user1) DIGICERT(USERCERT) LABLCERT('SMPE Client Certificate') –
  DCDSN(user.mvs.dataset.name) PKCSPASS(xxxxxxxx) TRUST
```

Note: If you receive this message: 'TSS1573I THE CERTIFICATE <USERCERT> SIGNER NOT FOUND. ADDING CERTIFICATE WITH NOTRUST STATUS' when adding the user certificate, issue the corresponding REPLACE command for that certificate:

```
TSS REPLACE(user1) DIGICERT(USERCERT) TRUST
```

* Connect the certificates to the Keyring

```
TSS ADD(user1) KEYRING(SMPERING) RINGDATA(CERTAUTH,DIGIROOT) USAGE(CERTAUTH)
TSS ADD(user1) KEYRING(SMPERING) RINGDATA(CERTAUTH,DIGIINT) USAGE(CERTAUTH)
TSS ADD(user1) KEYRING(SMPERING) RINGDATA(user1,USERCERT) USAGE(PERSONAL)
```


BROADCOM

Here are the commands for Top Secret. We start by creating a keyring. Please note the TSS ADD parameter of the keyring is the ACID that owns the keyring. In this example, this keyring owner is user1. Also, the information in the KEYRING and LABLRING parameters can be different. Both parameters are case sensitive. The KEYRING parameter can only be 8 characters long and is needed for the connect step and if creating ring specific rules for validation. LABLRING can be up to 237 characters and is used when pointing to the keyring in the SMP/E RECEIVE ORDER JCL

After creating the keyring, add each of the 3 certificates that were uploaded in the previous section to the Top Secret database. *Note the PKCSPASS parameter that is specified on the TSS ADD of the user1 certificate. This password should be the same encryption password specified when the certificate was generated*.

Make a note of the LABLCERT parameter for the user certificate (in this example "SMPE Client Certificate") as this will be needed later when setting up the SMP/E JCL.

If during the add of the user certificate you receive a TSS message saying "SIGNER NOT FOUND. ADDING CERTIFICATE WITH NOTRUST STATUS" issue the following replace command. After the certificates have been added into the database, they are ready to be added to the keyring using a TSS ADD command with the RINGDATA parameter.

SMP/E Internet Service Retrieval Overview

Create the Keyring and Add and CONNECT the Certificates with **RACF**

* Create the Keyring
RACDCERT ID(user1) ADDRING(SMPERING)

Note: "user1" is the user id that owns the keyring.

* Insert the certificates from the uploaded z/OS datasets
RACDCERT ID(user1) ADD(user.mvs.dataset.name) WITHLABEL('SMPE Client Certificate') **PASSWORD(xxxxxxxx)** TRUST
RACDCERT CERTAUTH ADD(digiint.mvs.dataset.name) WITHLABEL('Digicert Intermediate CA') TRUST
RACDCERT CERTAUTH ADD(digiroot.mvs.dataset.name) WITHLABEL('Digicert Root CA') TRUST

* Connect the certificates to the Keyring
RACDCERT ID(user1) CONNECT(LABEL('SMPE Client Certificate') RING(SMPERING) +
USAGE(PERSONAL))
RACDCERT ID(user1) CONNECT(CERTAUTH LABEL('Digicert Intermediate CA ') RING(SMPERING) +
USAGE(CERTAUTH))
RACDCERT ID(user1) CONNECT(CERTAUTH LABEL('Digicert Root CA ') RING(SMPERING) +
USAGE(CERTAUTH))

BROADCOM

Here are the commands for RACF. We start by creating a keyring. Please note the ID parameter of the keyring is the user id that owns the keyring. In this example, this keyring owner is user1. After creating the keyring, add each of the 3 certificates that were uploaded in the previous section to the RACF database. *Note the password that is specified on the RACDCERT ADD of the user1 certificate. This password should be the same encryption password specified when the certificate was generated*. Make a note of the WITHLABEL parameter for the user certificate (in this example "SMPE Client Certificate") as this will be needed later when setting up the SMP/E JCL. After the certificates have been inserted into the database, they are ready to be added to the keyring with the RACDCERT CONNECT commands.

SMP/E Internet Service Retrieval Overview

Setup User Access to Certificate and Keyring

Rules for keyring access depend on:

- Type of access check
- User needing authorization

BROADCOM

Next we need to write rules to allow users access to the keyring we created. The rules to write depend on the type of access check you want to deploy. You can write either ring specific rules or global profile checking rules. You also need to decide what users need access to the keyring as the access level is different if the user is or is not the KEYRING or certificate owner. In the following slides, we will give you sample commands for each ESM. An in-depth explanation of the options presented is discussed in a previous video in this series titled Keyring and Certificate Security.

SMP/E Internet Service Retrieval Overview

Setup User Access to Certificate and Keyring

Grant ACF2 user permissions for shared and non-shared certificates:

- Global profile check:

```
$KEY(IRR) TYPE(FAC)
 DIGTCERT.LISTRING UID(user1_uid) SERVICE(READ) ALLOW
 DIGTCERT.LISTRING UID(user2_uid) SERVICE(UPDATE) ALLOW

F ACF2,REBUILD(FAC)
```

- Ring specific check:

```
$KEY(USER1) TYPE(RDA)
 SMPERING.LST UID(user1_uid) SERVICE(READ) ALLOW
 SMPERING.LST UID(user2_uid) SERVICE(UPDATE) ALLOW

 F ACF2,REBUILD(RDA)
```

Note: Type RDA must be resident

Here are the sample commands for ACF2. If you prefer to use ring specific checking, the resource name takes the format of ringowner.ringname.lst. In our example, USER1 is the ringowner and SMPERING is the RINGNAME. Please note that the RDATALIB resource must be resident in order to use ring specific checks.

SMP/E Internet Service Retrieval Overview

Setup User Access to Certificate and Keyring

Grant Top Secret user permissions for shared and non-shared certificates:

- Global profile check:

```
TSS PER(user1) IBMFAC(IRR.DIGTCERT.LISTRING) ACC(READ)
TSS PER(user2) IBMFAC(IRR.DIGTCERT.LISTRING) ACC(UPDATE)
```

- Ring specific check:

```
TSS PER(user1) RDATALIB(USER1.SMPERING.LST) ACC(READ)
TSS PER(user2) RDATALIB(USER1.SMPERING.LST) ACC(UPDATE)
```


Here are the sample commands for Top Secret. If you prefer to use ring specific checking, the resource name takes the format of ringowner.ringname.lst. In our example, USER1 is the ringowner and SMPERING is the RINGNAME.

SMP/E Internet Service Retrieval Overview

Setup User Access to Certificate and Keyring

Grant RACF user permissions for shared and non-shared certificates:

- Global profile check:

```
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(user1) ACCESS(READ)
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(user2) ACCESS(UPDATE)
SETROPTS RACLIST(FACILITY) REFRESH
```

- Ring specific check:

```
PERMIT USER1.SMPERING.LST CLASS(RDATALIB) ID(user1) ACCESS(READ)
PERMIT USER1.SMPERING.LST CLASS(RDATALIB) ID(user2) ACCESS(UPDATE)
SETROPTS RACLIST(RDATALIB) REFRESH
```

Note: RDATALIB must be active and RACLISTed

BROADCOM

Here are the sample commands for RACF. If you prefer to use ring specific checking, the resource name takes the format of ringowner.ringname.lst. In our example, USER1 is the ringowner and SMPERING is the RINGNAME. Please note that the RDATALIB resource must be active and RACLISTed in order to use ring specific checks.

SMP/E Internet Service Retrieval Overview

Sample SMP/E RECEIVE ORDER JCL and Commands

```
//jobname JOB ...,REGION=0M
//RECEIVE EXEC PGM=GIMSMP
//SMPCSI DD DSN=yourcsi,DISP=SHR
//SMPNTS DD PATH='/u/your/smpnts/directory',PATHDISP=KEEP
//SMPOUT DD SYSOUT=*
//SMPRPT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SMPCNTL DD *
 SET BDY(GLOBAL).
 RECEIVE ORDER(
        ORDERSERVER(ORDSRVR)
        CLIENT(CLIENT)
        CONTENT(RECOMMENDED)
         )
       DELETEPKG.
/*\
//ORDSRVR DD *
  <ORDERSERVER
    url=https://eapi.broadcom.com/receiveorder
    keyring="userid/keyring"
    certificate="SMPE Client Certificate">
 </ORDERSERVER>
/*
//CLIENT DD *
  <CLIENT
   javahome="/usr/lpp/java/J8.0"
   classpath="/usr/lpp/smp/classes"
   javadebugoptions="-Dcom.ibm.smp.debug=severe -showversion"
   downloadmethod="https">
 </CLIENT>
 /*
```

Required fields are in red.

SMPCSI DD specifies the Broadcom Product CSI

SMPNTS DD specifies the directory containing GIMZIP archive files and associated metadata files for all extracted PTFs, APARs, and HOLDDATA in the zip file. This directory can be used as the SMPNTS input to SMP/E RECEIVE FROMNTS processing.

CONTENT specifies the order type:

CONTENT(ALL)	Get ALL missing PTFs
CONTENT(HOLDDATA)	Get HOLDDATA only
CONTENT(CRITICAL)	Get CRITICAL only
CONTENT(RECOMMENDED)	Get Recommended Service
CONTENT(PTFS(RO12345,RO23456))	Get these PTFS and REQS
CONTENT(APARS(TR12345)	Get PTF that resolves APAR

ORDERSERVER and CLIENT fields continued...

BROADCOM

Next we'll go over the sample receive order JCL. This JCL can be found in the CA Common Services documentation and a link will be provided in the text document that accompanies this presentation. Everything in red is what needs to be modified to fit the environment. We'll start with the SMPCSI DD which will point to the Broadcom Product CSI. Next is the SMPNTS DD which points to the USS directory where the download order will be downloaded to before being received. You will either need to create your own HFS or zFS directory to point to or you can point to an existing USS directory that has enough space for the download. The next section is the CONTENT parameter in the RECEIVE ORDER section. This specifies the order type you wish to download. The majority of these order types are self explanatory, but if you specify CONTENT(ALL) it is important to note that all missing PTFs will be downloaded. For example, the first time you run SMP/E with this parameter it is going to receive all of the maintenance that has been published. The next time you run the SMP/E job with the CONTENT(ALL) parameter, it is only going to receive maintenance that has been published in the time since the last time you ran the job.

SMP/E Internet Service Retrieval Overview

Define the ORDERSERVER Input for RECEIVE ORDER

```
<ORDERSERVER
  url=https://eapi.broadcom.com/receiveorder
  inventory="all"
  keyring="userid/ringname"
  certificate="User certificate label">
 </ORDERSERVER>
```

- **Keyring** Identifies the key ring that contains the user certificate that is required for access to the order server.

  Ex. keyring="USER1/SMPERING"

- **Certificate** Specifies the label to identify the **User Certificate** that is used for access to the CA Automated Order Server.

  Ex. certificate="SMPE Client Certificate"

Note: the keyring and certificate fields are case sensitive

The next section to modify is the ORDERSERVER section. The SMP/E RECEIVE ORDER command uses the ORDERSERVER dataset to provide necessary information about the Broadcom Automated Order Server. The information appears with the <ORDERSERVER> tag. Do not change the parameters specified for URL and Inventory. URL specifies the URL for the order server and Inventory specifies that the generated CSI inventory file is to be in XML format. The CA Automated Order Server does not support the default format of inventory=ibm.

The parameters to focus on are keyring and certificate. KEYRING Identifies the key ring that contains the user certificate required for access to the order server. Where USER ID is the user id of the owner of the keyring and RINGNAME is the name given to identify the keyring. The user ID and key ring name must be separated by a forward slash. To continue using our example setup, keyring would equal "USER1/SMPERING".

Certificate specifies the label to identify the User Certificate that is used for access to the CA Automated Order Server. Following our example from the previous slides, the certificate label for the user certificate was SMPE Client Certificate.

It is important to note that both the KEYRING and the Certificate fields are case sensitive.

The following slides will show where to find the information required for the keyring and

certificate parameters in the event you need to backtrack to find the information.

SMP/E Internet Service Retrieval Overview

Correlate the Keyring/Certificate Fields with the ORDERSERVER Parameters

ACF2

```
SET PROFILE(USER) DIV(KEYRING)
LIST USER1.RING

KEYRING / USER1.RING LAST CHANGED BY USER2 ON 01/11/21-14:30
                     DEFAULT() RINGNAME(SMPERING)
The following certificates are connected to this key ring:
CERTDATA record    Label                           Usage
-----------------  ------------------------------  --------
USER1.CERT         SMPE Client Certificate         PERSONAL
CERTAUTH.DIGIINT   Digicert Intermediate CA        CERTAUTH
CERTAUTH.DIGIROOT  Digicert Root CA                CERTAUTH



<ORDERSERVER
 url="https://eapi.broadcom.com/receiveorder"
 inventory="all"
 keyring=" USER1/SMPERING"
 certificate="SMPE Client Certificate">
 </ORDERSERVER>
```


BROADCOM

In ACF2, issue a LIST command for the keyring. The color coded information corresponds to the parameters needed for the keyring and certificate fields.

SMP/E Internet Service Retrieval Overview

Correlate the Keyring/Certificate Fields with the ORDERSERVER Parameters

Top Secret

```
TSS LIST(USER1) KEYRING(SMPERING)

KEYRING =  USER1          ACCESSORID = USER1
   ADMIN BY= BY(ADMIN001 )     SMFID(SYSA)    ON(04/09/2021)  AT(12:21:10)

KEYRING LABEL = SMPERING
KEYRING HAS THE FOLLOWING CERTIFICATES CONNECTED:

  ACID(USER1)  DIGICERT(USERCERT)  DEFAULT(YES)  USAGE(PERSONAL)
  LABLCERT(SMPE Client Certificate)

  ACID(USER1)  DIGICERT(DIGIINT)  DEFAULT(YES)  USAGE(CERTAUTH)
  LABLCERT(Digicert Intermediate CA)

  ACID(USER1)  DIGICERT(DIGIROOT)  DEFAULT(YES)  USAGE(CERTAUTH)
  LABLCERT(Digicert Root CA)

<ORDERSERVER
 url="https://eapi.broadcom.com/receiveorder"
 inventory="all"
 keyring=" USER1/SMPERING"
 certificate="SMPE Client Certificate">
 </ORDERSERVER>
```


In Top Secret, issue a TSS LIST command for the keyring. The color coded information corresponds to the parameters needed for the keyring and certificate fields.

SMP/E Internet Service Retrieval Overview

Correlate the Keyring/Certificate Fields with the ORDERSERVER Parameters

RACF

```
RACDCERT ID(USER1) LISTRING(SMPERING)

Digital ring information for user USER1:

   Ring:
        >SMPERING<
   Certificate Label Name              Cert Owner     USAGE      DEFAULT
   --------------------------------    ------------   --------   -------
   SMPE Client Certificate             ID(USER1)      PERSONAL   NO
   Digicert Intermediate CA            ID(USER1)      CERTAUTH   NO
   Digicert Root CA                    ID(USER1)      CERTAUTH   NO


<ORDERSERVER
 url="https://eapi.broadcom.com/receiveorder"
 inventory="all"
 keyring=" USER1/SMPERING"
 certificate="SMPE Client Certificate">
 </ORDERSERVER>
```


In RACF, issue a RACDCERT LISTRING command for the keyring. The color coded information corresponds to the parameters needed for the keyring and certificate fields.

SMP/E Internet Service Retrieval Overview

Define the CLIENT Input for RECEIVE ORDER

Required fields are in red. Optional tags are in blue*.

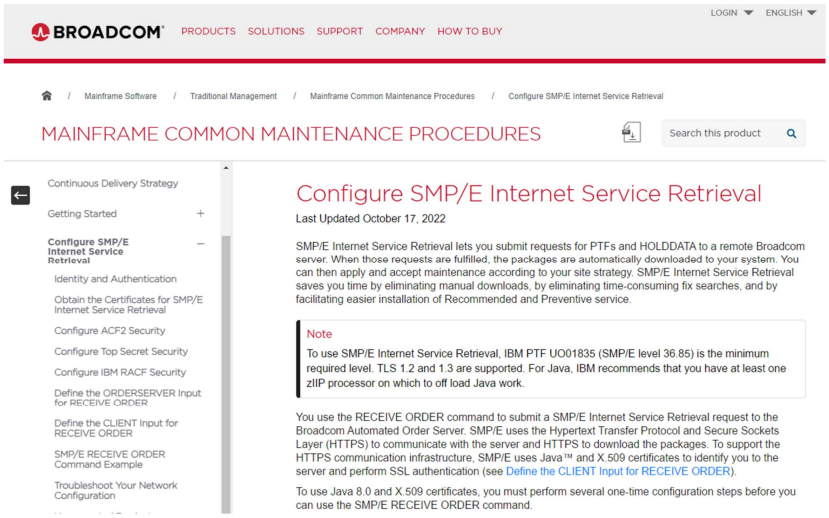
```
<CLIENT
 downloadmethod="https"
 javahome="/usr/lpp/java/J8.0"
 classpath="/usr/lpp/smp/classes"
 javadebugoptions="-Dcom.ibm.smp.debug=severe -showversion"
 >
 <HTTPPROXY host="local.httpproxy.com">
 </HTTPPROXY>
 <FIREWALL>
   <SERVER host="local.ftpproxy.com"> </SERVER>
   <FIRECMD>&REMOTE_USER;@&REMOTE_HOST;</FIRECMD>
   <FIRECMD>&REMOTE_PW;</FIRECMD>
 </FIREWALL>
</CLIENT>
```

- javahome specifies the location for the Java runtime to be used by SMP/E, which uses Java 8 for HTTPS operations.
- classpath specifies required SMP/E Java application classes.

Getting back to the SMP/E JCL, the last parameters that need to be specified are the javahome and classpath. Typically you can request this information from your systems programmer. The javahome parameter specifies the location for the Java runtime to be used by SMP/E and classpath specifies the required application classes for SMP/E. Everything in blue is optional and is listed in the event your site utilizes a proxy server or has additional firewall configurations to take into consideration.

SMP/E Internet Service Retrieval Overview

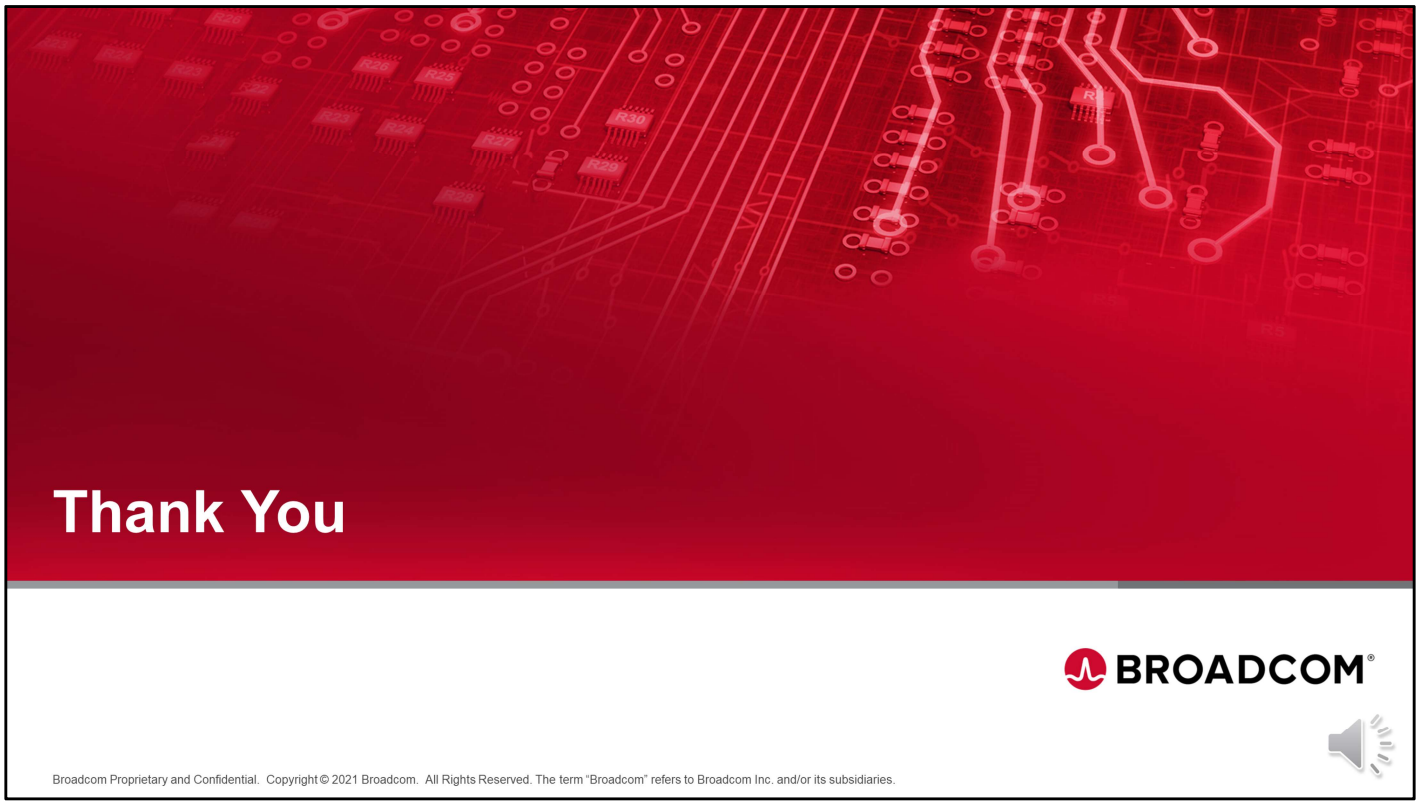
Documentation



Reference: [Mainframe Common Maintenance Procedures - Configure SMP/E Internet Service Retrieval]

BROADCOM

Additional documentation for SMP/E Internet Service Retrieval configuration can be found online at techdocs.Broadcom.com. A link to the documentation and course notes will be included in a text file available for download.



That concludes this presentation on configuring security for SMP/E Internet Service Retrieval. Thank you and have a wonderful day.


BROADCOM®
connecting everything®