IBM Software Group

Host On-Demand Certificate Management

Casey Cooley and Russ Stancliffe

WebSphere software

WebSphere® Support Technical Exchange

ON DEMAND BUSINESS

Objectives

- Discuss Host On-Demand Certificate Management Tools
- Discuss Host On-Demand SSL Certificates
  - Known Certificate Authority Certificates
  - Unknown Certificate Authority Certificates
  - Self-Signed Certificates
  - Storing and Transferring Certificates
- Discuss additional usage tips and techniques

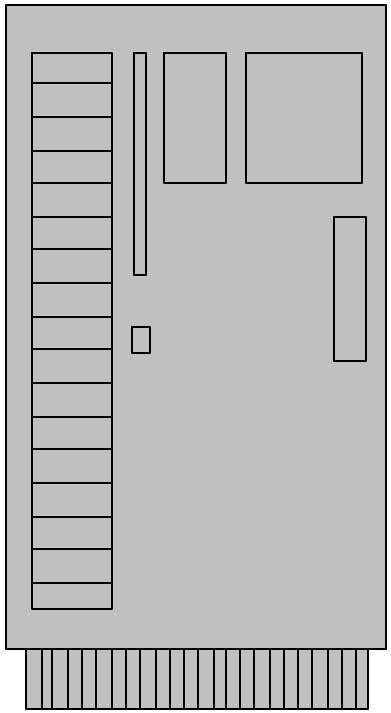
SSL with Host On-Demand

- Server Authentication
  - When enabled, the client, after making sure that the server's certificate can be trusted, checks whether the Internet name in the certificate matches the Internet name of the server. If they match, the SSL negotiation will continue. If not, the connection ends immediately.
- Client Authentication
  - You can only use client authentication when a server requests a certificate from a client. Not all servers support client authentication, including the Host On-Demand Redirector.
- Redirector
  - The Redirector sets security for each host. Security choices are no data-stream modification (pass-through), client-side encryption, host-side encryption, and encryption on all data flowing between the Host On-Demand emulator session and the secure server (both).

Host on Demand Server Certificate Management

- Servers
  - Windows
  - UNIX
  - Linux
  - i5/OS or OS/400
  - z/OS or OS/390

Certificate Management tools allow you to enable Secure Sockets Layer (SSL) communications between Host On-Demand Servers and Clients



Tools for HOD Certificate Management

- iKeyman (IBM Key Manager) on Windows and UNIX – GUI tool
- IKEYCMD on Windows and UNIX – command line tool
- Digital Certificate Manager on iSeries
- RACF and gskkyman on z/OS

Host On-Demand Server Key Database File

- HODServerKeyDb.kdb
- You must create this file as it is not shipped with Host On-Demand
- This database contains the server's private key and certificate as well as CA (signer) certificates.
- You can add certificates from unknown CAs and self-signed certificates to this database.
- On z/OS, the kdb name can be any name

iKeyman on Windows, AIX and Linux

- Packaged with Host On-Demand Server
- To start

On Windows:
Start>All Programs>IBM WebSphere Host On-Demand>Administration> Certificate Management

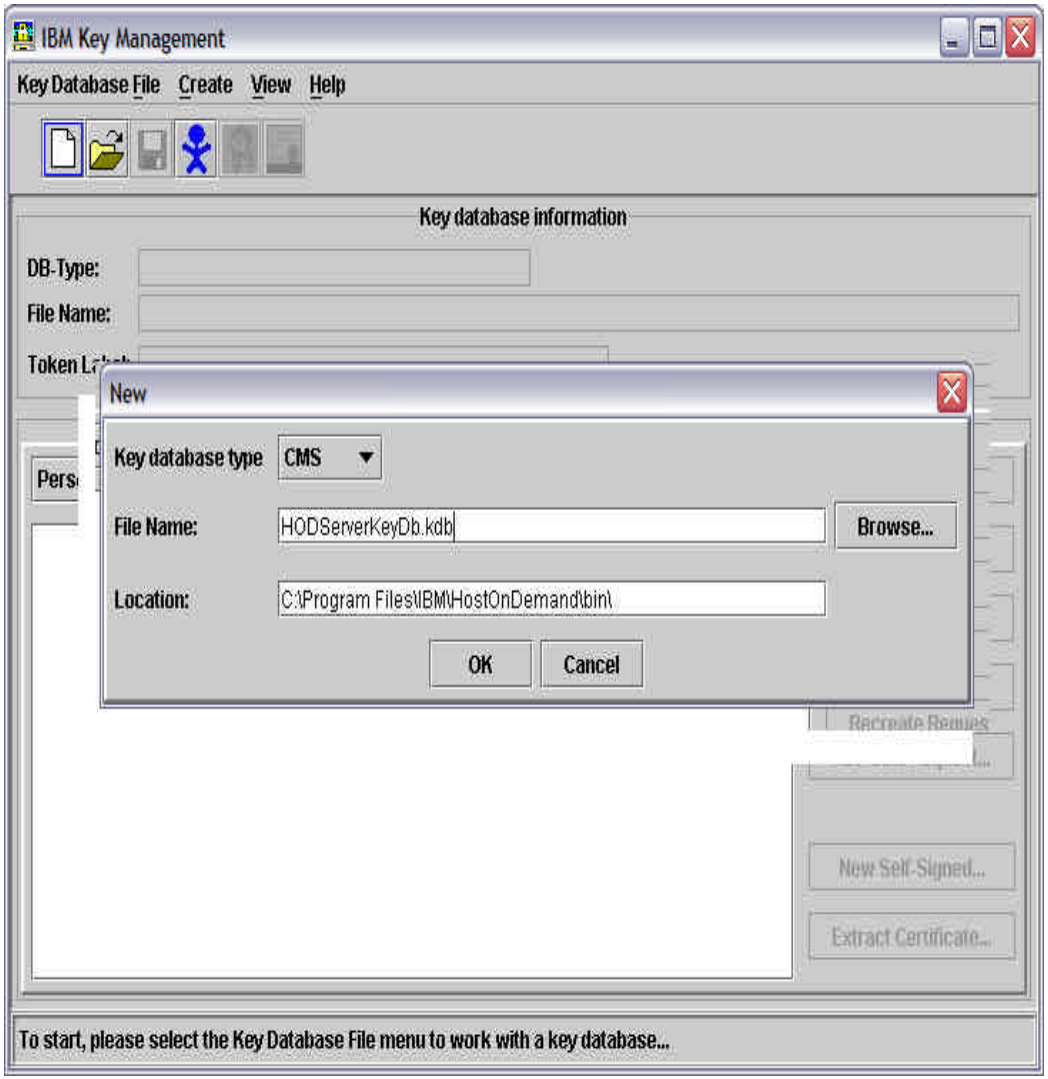
On both AIX and Linux:
The default install directory is /opt/IBM/HostOnDemand, so you would change to /opt/IBM/HostOnDemand/bin.

The file CertificateManagement is a command script file that launches the utility. Run the file as you would any other command script. For example, in Linux, you might run the file as follows:

```
./CertificateManagement &
```

iKeyman on Windows, AIX and Linux

1. Click on Key Database File
2. Click on New
3. Select CMS for key Database type
4. Type HODServerKeyDb.kdb for the file name
5. Default location is C:\Program Files\IBM\HostOnDemand\bin
6. Click OK



iKeyman on Windows, AIX and Linux cont…

Enter a password

Warning: when setting an expiration date on the password, your Host On-Demand SSL will stop working when the password expires.

Note: Stash the password to a file? Should be checked. Do NOT uncheck this, Host on-Demand requires that the password be stashed so the Host on-Demand server can access the key file.

The strength of your password is indicated by the bars at the bottom of the panel.

IKEYCMD on Windows, AIX and Linux

- Available only on Windows, AIX, and Linux (Intel and zSeries)
- Java based
- Environment settings: (all on one line per set or export)

Windows:

```
set PATH=c:\Program Files\IBM\HostOnDemand\hod_jre\jre\bin;%PATH%;
set CLASSPATH=c:\Program Files\IBM\GSK7\classes\cfwk.zip;C:\Program
  Files\IBM\GSK7\classes\gsk7cls.jar;%CLASSPATH%;
```

AIX and Linux:

```
EXPORT PATH=/opt/IBM/HostOnDemand/hod_jre/jre/bin:$PATH
EXPORT
  CLASSPATH=/usr/local/ibm/gsk7/classes/cfwk.zip:/usr/local/ibm/gsk7/cla
  sses/gsk7cls.jar:$CLASSPATH
```

IKEYCMD on Windows, AIX and Linux

- ikeycmd is functionally similar to Certificate Management GUI and run from the command line
- Called from native shell scripts and programs to be used when applications prefer to add custom interfaces to certificate and key management tasks.
- ikeycmd can create key database files for all of the types that the Certificate Management utility (iKeyman) currently supports.
- Ikeycmd can create certificate requests, import CA-signed certificates and manage self-signed certificates.
- To create a Host On-Demand key database file, enter at the command prompt: (all on one line, though it might wrap to the next line)

```
java com.ibm.gsk.ikeyman.ikeycmd -keydb –create -db
  your_install_directory\bin\HODServerKeyDb.kdb -pw
  <password> -type cms -expire <days> -stash
```

gskkyman on z/OS UNIX System Services

- From OMVS prompt, enter gskkyman
- Enter 1 to create a new database OR
- Enter 2 to open an existing database
- When creating a new kdb and prompted for the password expiration, just hit Enter for no expiration

Database Menu

1 - Create new database

2 - Open database

3 - Change database password

4 - Change database record length

5 - Delete database

6 - Create key parameter file

0 - Exit program

Enter option number:

===>

gskkyman – Store the password

If creating a new database, you must store the password of the database using option 10

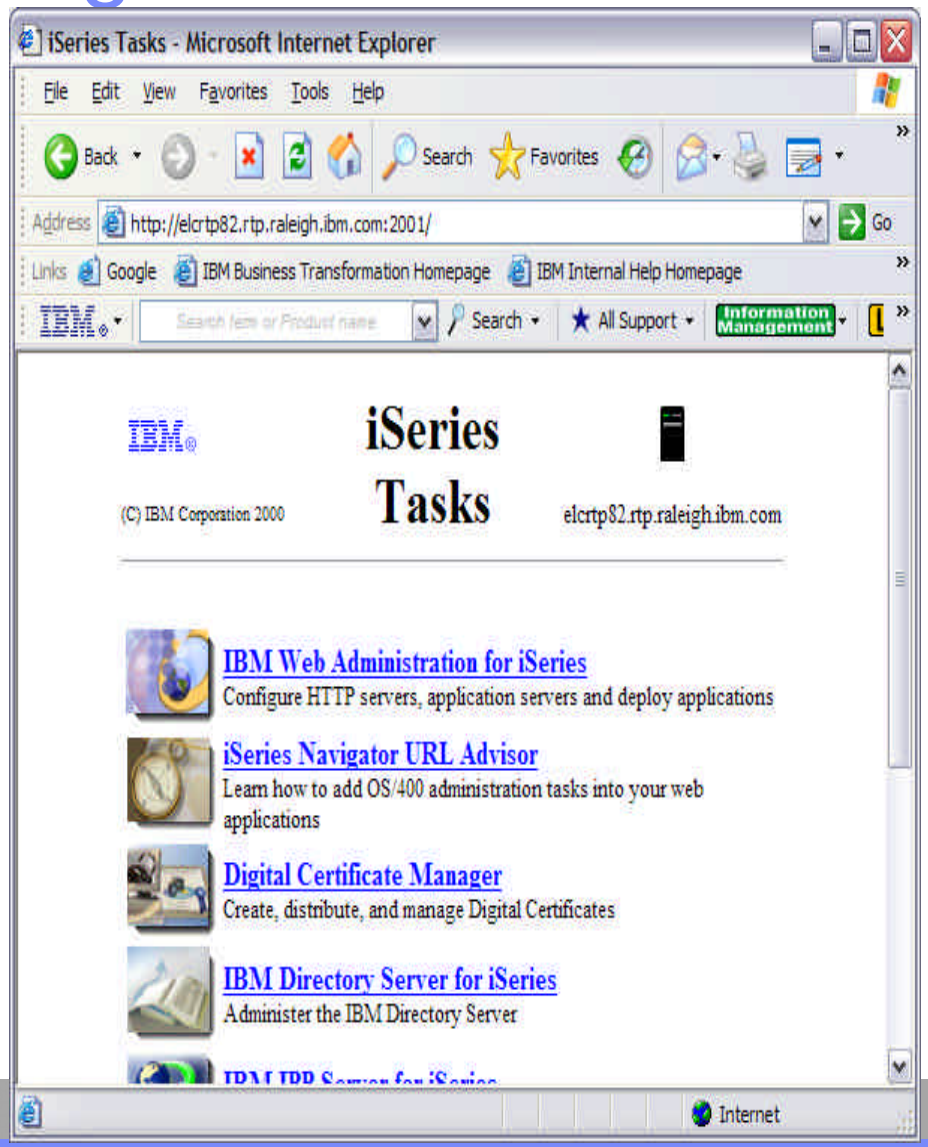
```
Key Management Menu

    Database: /u/user1/casey.kdb

  1 - Manage keys and certificates
  2 - Manage certificates
  3 - Manage certificate requests
  4 - Create new certificate request
  5 - Receive requested certificate or a renewal certificate
  6 - Create a self-signed certificate
  7 - Import a certificate
  8 - Import a certificate and a private key
  9 - Show the default key
 10 - Store database password
 11 - Show database record length

  0 - Exit program

Enter option number (press ENTER to return to previous menu):
 ===>
```

iSeries requirements for secure connections

- Digital Certificate Manager (DCM)
- TCP/IP Connectivity Utilities
- IBM HTTP server for AS/400
- One of the IBM Cryptographic Access Provider products.
- iSeries support should be contacted when creating certificates using DCM.

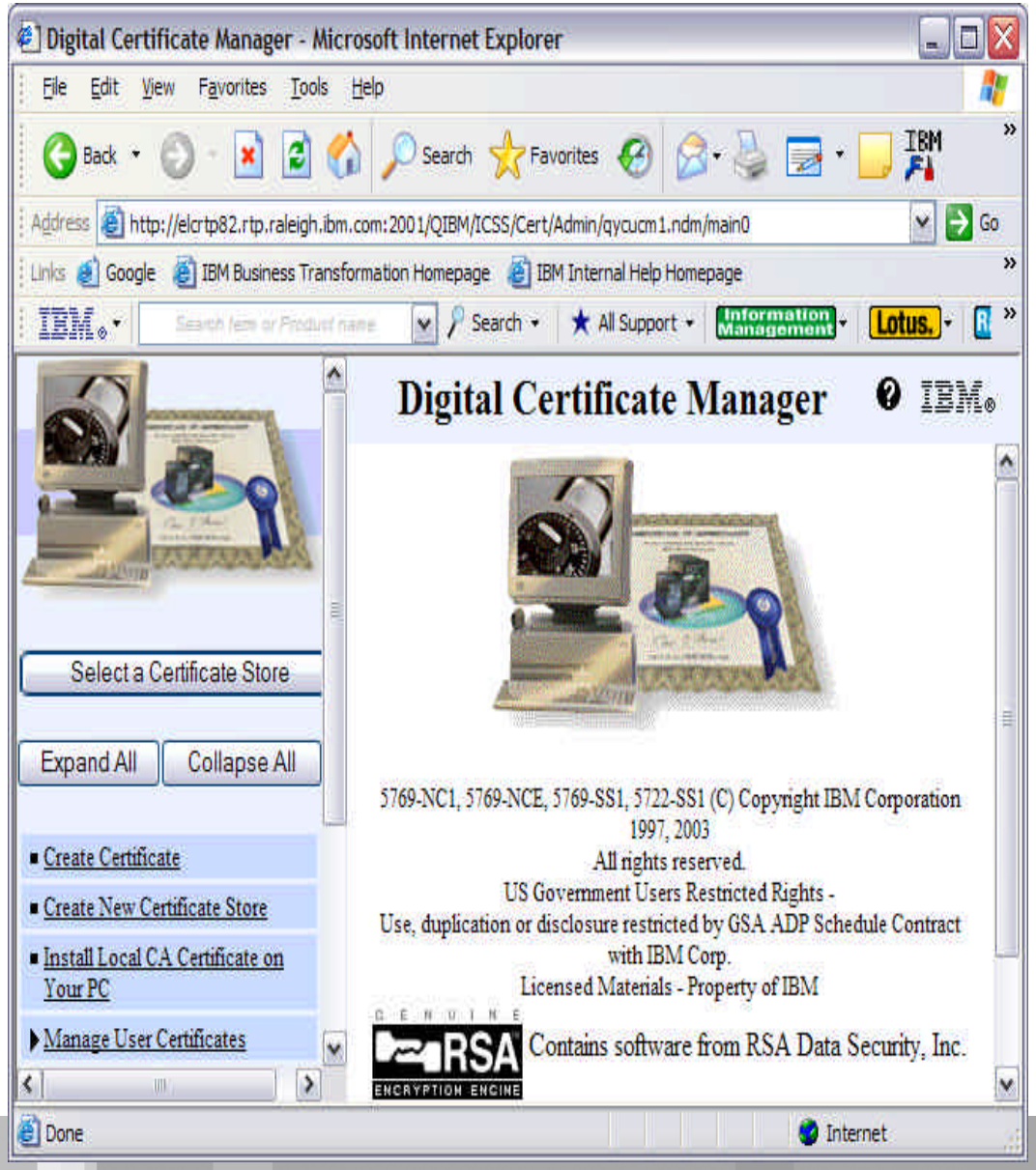
Digital Certificate Manager on iSeries

1. Access to DCM is via browser
2. Your.iSeries.ip.address:2001
3. You must be authorized
4. Click on Digital Certificate Manager



DCM on iSeries

- iSeries provides a default certificate store (key database)
- *SYSTEM



SSL Certificates for Host On-Demand

- A Certificate Authority (CA) certificate may be used
- A self-signed certificate may be used

Certificate Authority (CA) certificates

Trusted Certificate Authority

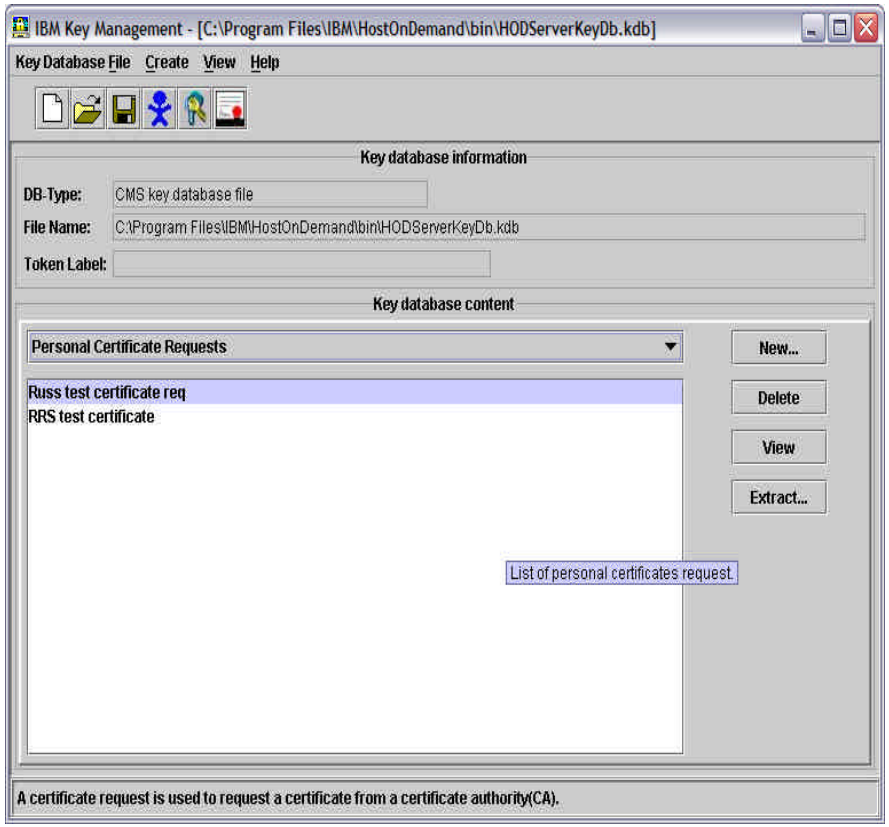
By default CA certificates are stored in the HODServerkeyDb.kdb key database and marked as trusted CA certificates, they are from:

IBM World Registry CA
Integrion CA Root
VeriSign
RSA
Thawte

WellKnownTrustedCAs.p12 is a file supplied by Host On-Demand that contains the public certificates of all the CAs that Host On-Demand trusts. You should not modify this file.

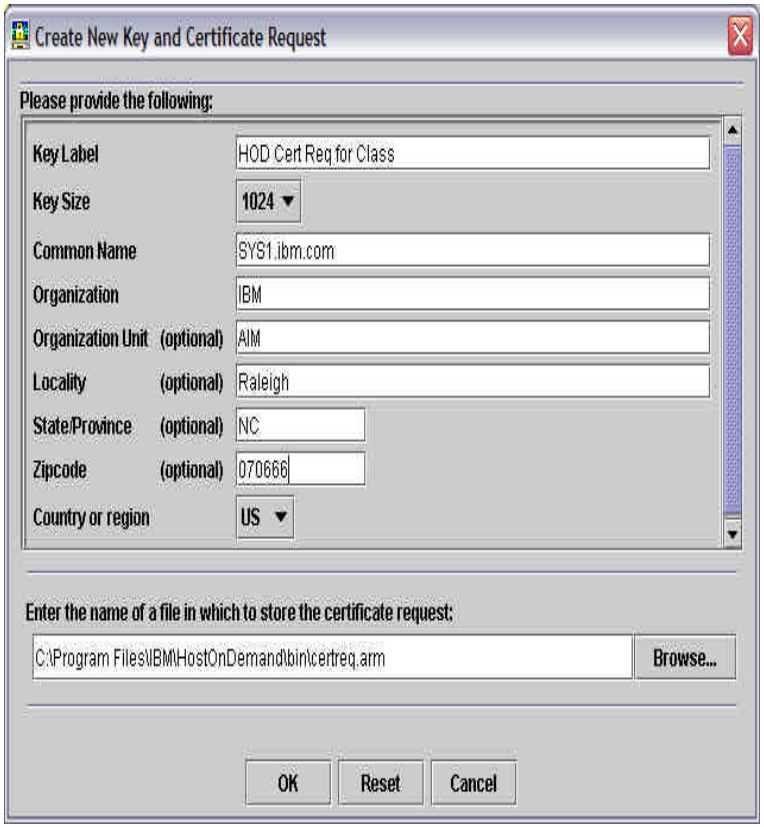
iKeyman: Create Certificate Request

- Click on Personal Certificate Requests from the drop-down list
- Click on Create, select New Certificate Request
- Enter your information in the panel that opens



iKeyman: Create keys and a Certificate request

- When you click OK, your information is processed and four files are produced or updated:
- HODServerKeyDb.kdb – key database file
- HODServerKeyDb.sth – key database password file
- HODServerKeydb.rdb – key database private key file
- Certificate_name – default name (certreq.arm) or name you gave the certificate request file, this is PKCS 12 type file in armored 64 format.
- DO NOT attempt to edit these files, you will corrupt them.

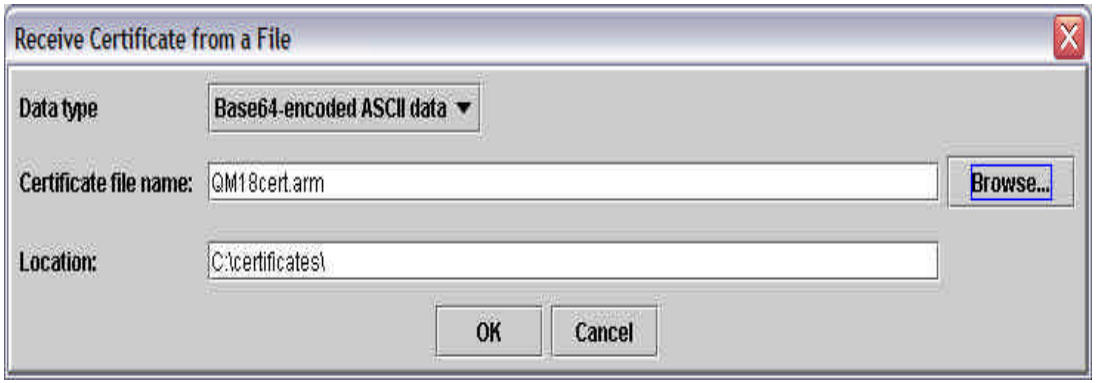


Send the Certificate request

- Start a Web Browser and access a CA's Web page.
- Follow the instructions provided to submit the certificate request.
- You can either e-mail the certificate request or incorporate the certificate request into the form or file provided by the CA.
- Well-known CAs:

  www.verisign.com
  www.thawte.com

Storing the server certificate



- After receiving the certificate from the CA, make a copy, then
- Choose Personal Certificates then click receive from a file
- Data type must be Base64-encoded ASCII data (armored 64 format)
- After receiving, highlight the certificate and click View/Edit , the option to set the key as default is on this panel.
- Stop and re-start the Host On-Demand Service Manager

Unknown Certificate Authority

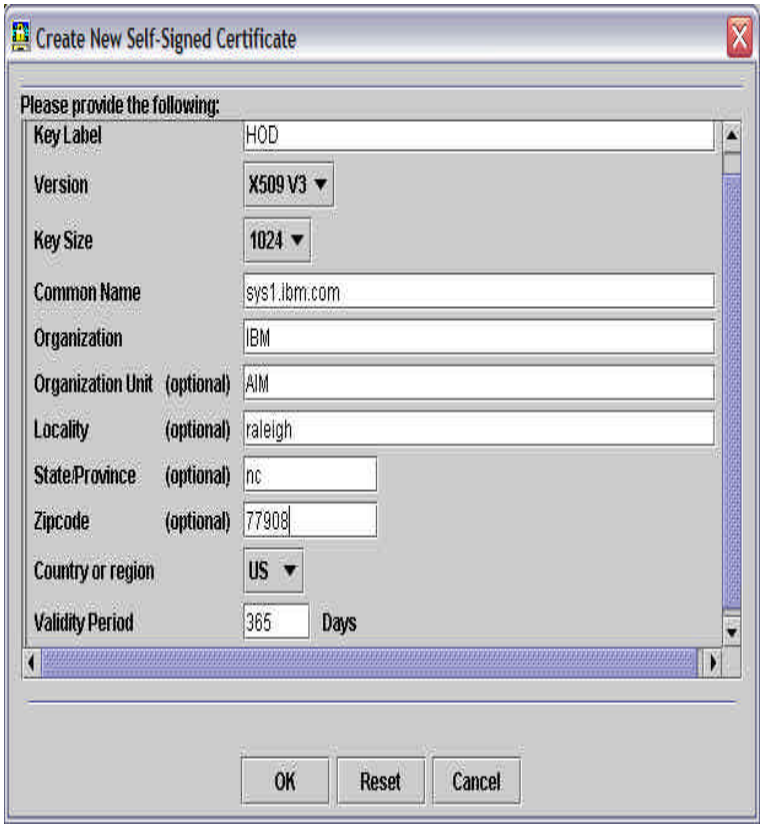
- CAs that are not already defined in the database
- Could be your iSeries or z/OS system
- Create the key pair and certificate request as before
- Submit the certificate request to the CA
- Obtain the CA's root certificate and your certificate and store them in the key database file

Unknown Certificate Authority cont.

- Store the CAs root certificate in the “Signer Certificates” location of the Key Database File, it will be marked as trusted when you click ok.
- Store your “applied-for Certificate” in the “Personal Certificates” location of the Key Database File, again click on View/Edit and check the box to to set it as default.
- Stop and re-start the Host On-Demand Service Manager.

Self-Signed Certificates

- Choose Personal Certificates from the drop down list in iKeyman
- Click “Create” then “New Self-signed certificate”
- Enter information to identify the certificate
- Be careful to set the number of days valid to a high enough value.
- Highlight the certificate and click View/Edit , then set it as default.
- Stop and re-start the Host On-Demand Service Manager.
- All certificates in HODServerkeyDb.kdb are available to the Host On-Demand server.



Making server certificates available to clients

- Three types of clients:
  - Locally Installed
  - Downloaded
  - Cached
- For Locally Installed clients, unknown CA root certificates or self-signed certificates must be extracted to a file, securely transferred to the client, then added to the Key Database File of the client machine.
- For Downloaded or Cached clients a CustomizedCAs.p12 or CustomizedCAs.class file in the Host On-Demand server publish directory is used.

Client Certificate Files

- CustomizedCAs.class and/or CustomizedCAs.p12 file contains the root certificates of unknown CAs and self-signed certificates.
- CustomizedCAs.p12 file is a newer version of the CustomizedCAs.class (Host On-Demand V7 and earlier) file.

Note: iSeries still uses CustomizedCAs.class file

Client Certificate Files cont.

- During SSL negotiations the server presents its certificate to the client.
- Client checks WellKnownTrustedCAs.p12 files first, followed by CustomizedCAs.p12 or CustomizedCAs.class files for a certificate signed by an authority the client trusts.
- Client will reject the connection if the server presents an unknown or no certificate

Creating CustomizedCAs.p12 or .class file

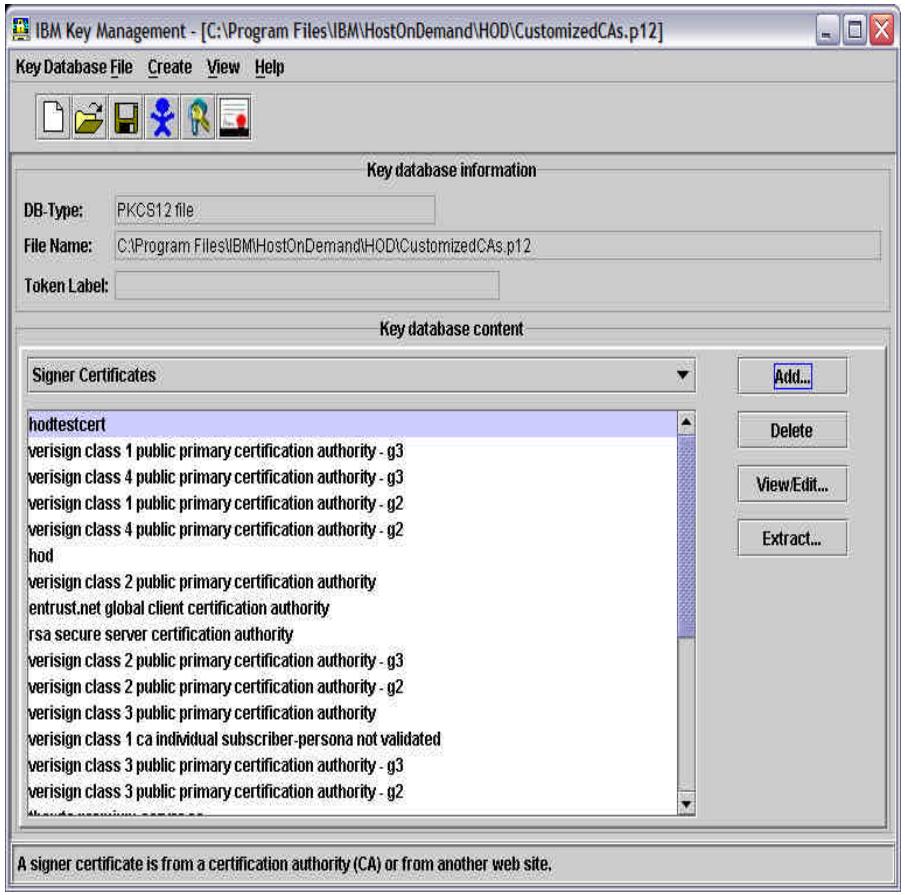
- Open the HODServerKeyDb.kdb as you have previously
- If using self-signed certificates, display the list of personal certificates, highlight the certificate used by your server, click Extract Certificate. OR
- If using an unknown CA, display the list of Signer Certificates, highlight the root certificate of the unknown CA that issued the site certificate for your server, click Extract.

Creating CustomizedCAs.p12 or .class file cont.

- Extract the certificate to a file, select data type BASE64 encoded ASCII data, you can name this file whatever you choose.
- Click Key Database File, click New, choose PKCS12 database type, the file name MUST be CustomizedCAs.p12 for Windows, AIX, and Linux and the location should be in the publish (HOD) directory of your server.
- Default location for Windows: C:\Program Files\IBM\HostOnDemand|HOD
- Default location for AIX and Linux: /opt/IBM/HostOnDemand/HOD
- Click OK, you will be prompted for the password, you MUST use the default password “hod” for this file. NOTE: the password is lowercase hod.
- On iSeries the file name is CustomizedCAs.class
- Now that the CustomizedCAs.p12 or .class file exists, you must add the previously extracted certificate to this CustomizedCAs file.

Adding a Certificate to the CustomizedCAs file

- iKeyman has the CustomizedCAs.p12 file open
- Using the ADD button on the right we can select our .arm certificate file name that we extracted previously
- Note the certificate named “hod” that was added to the CustomizedCAs.p12 file



gskkyman – creating CA certificate to sign requests

- Create a self-signed certificate, option 6 from main menu.
- For Certificate type, select option 1 – 4 for CA type certificate.
- Complete the information for the certificate

```
Certificate Type

 1 - CA certificate with 1024-bit RSA key
 2 - CA certificate with 2048-bit RSA key
 3 - CA certificate with 4096-bit RSA key
 4 - CA certificate with 1024-bit DSA key
 5 - User or server certificate with 1024-bit RSA key
 6 - User or server certificate with 2048-bit RSA key
 7 - User or server certificate with 4096-bit RSA key
 8 - User or server certificate with 1024-bit DSA key

Select certificate type (press ENTER to return to menu):
 ===>
```

gskkyman – Create certificate Request

- Select option 4 from the main menu to create a new certificate request
- Enter Certificate Type, option 1.
- Complete the certificate request.
- The request can then be sent to a known Certificate Authority (CA) OR
- Use gskkyman to be the CA and sign the certificate

```
Certificate Type

1 - Certificate with 1024-bit RSA key
2 - Certificate with 2048-bit RSA key
3 - Certificate with 4096-bit RSA key
4 - Certificate with 1024-bit DSA key

Enter certificate type (press ENTER to return to menu):
===>
```

gskkyman – signing the certificate

- To sign the certificate using the CA that was created, the gskkyman command must be issued from the command line with options, all on one line.

```
gskkyman -g -x num-of-valid-days
-cr certificate-request-file-name
-ct signed-certificate-file-name
-k CA-key-database-file-name
-l label-CA-cert
```

gskkyman – receive the signed certificate

- Select option 5 on the main menu, Receive requested certificate or a renewal certificate.
- Enter the certificate file name
- After adding the certificate to the kdb, make the certificate the default using option 1, Manage keys and certificates

```
Key Management Menu

Database: /u/user2/key.kdb

1 - Manage keys and certificates
2 - Manage certificates
3 - Manage certificate requests
4 - Create new certificate request
5 - Receive requested certificate or a renewal certificate
6 - Create a self-signed certificate
7 - Import a certificate
8 - Import a certificate and a private key
9 - Show the default key
10 - Store database password
11 - Show database record length

0 - Exit program

Enter option number (press ENTER to return to previous menu): 5
```

RACF – create self signed certificate

1. Create the keyring file
```
RACDCERT ID(IBMUSER) ADDRING(HODTN3270)
```

2. Create the certificate
```
RACDCERT ID(IBMUSER) GENCERT SUBJECTSDN
 (CN('MVS.RALEIGH.IBM.COM') OU('IBMHOD') C('US'))
 WITHLABEL('TN3270 SERVER') KEYUSAGE(HANDSHAKE)
```

3. Add the certificate to the keyring and make sure it is set as DEFAULT
```
RACDCERT ID(IBMUSER) CONNECT (ID(IBMUSER)
 LABEL('TN3270 SERVER') RING(HODTN3270) DEFAULT)
```

4. Check to make sure that this was successful by issuing the following command:
```
RACDCERT ID(IBMUSER) listring *
```

Java Commands for CustomizedCAs.p12 for z/OS

- For the following commands you must be in OMVS or UNIX system services:
- The password for the CustomizedCAs.p12 file must be 'hod'
- The command must be on one line if in a shell script. Can use continuation character if entering on command line
- You must enter the commands from the publish directory (HOD/hostondemand/HOD)

- To add a telnet certificate via connect option:

```
java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip
   com.ibm.hod5sslight.tools.P12Keyring CustomizedCAs connect IP:port
```

- To add certificate via add command (if unable to connect to telnet server, server down or network down. Need to have the certificate file on system where command is issued)

```
java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip
   com.ibm.hod5sslight.tools.P12Keyring CustomizedCAs add –site file.der
```

- To add an ftp certificate via connect option:

```
java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip
   com.ibm.hod5sslight.tools.P12Keyring CustomizedCAs connect IP:port ftp
```

- To add ftp certificate via add command (if unable to connect to ftp server, server down or network down. Need to have the certificate file on system where command is issued)

```
java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip
   com.ibm.hod5sslight.tools.P12Keyring CustomizedCAs add –site file.der ftp
```

- To verify the certificates in the p12 file:

```
java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip
   com.ibm.hod5sslight.tools.P12Keyring CustomizedCAs list
```

JAVA commands for CustomizedCAs.class file

- For the following commands you must be in OMVS or UNIX Systsm Services:
- When prompted for a password for the CustomizedCAs.class file, just press Enter.
- It is recommended you enter commands from the publish directory (HOD/hostondemand/HOD)

- To add a certificate for telnet via connect option:

```
java -classpath ../lib/sm.zip com.ibm.hodsslight.tools.keyrng
  CustomizedCAs connect IP:port
```

- To add a telnet certificate via add option (if unable to connect to server. Need to have the certificate file available):

```
java -classpath ../lib/sm.zip com.ibm.hodsslight.tools.keyrng
  CustomizedCAs add –site file.der IP:port
```

- To add a secure FTP certificate via connect option:

```
java -classpath ../lib/sm.zip com.ibm.hodsslight.tools.keyrng
  CustomizedCAs connect IP:port ftp
```

- To add an ftp certificate via add option (if unable to connect to server. Need to have the certificate file available):

```
java -classpath ../lib/sm.zip com.ibm.hodsslight.tools.keyrng
  CustomizedCAs add –site file.der IP:port ftp
```

- To verify the certificates in the class file:

```
java -classpath ../lib/sm.zip com.ibm.hodsslight.tools.keyrng
  CustomizedCAs verify
```

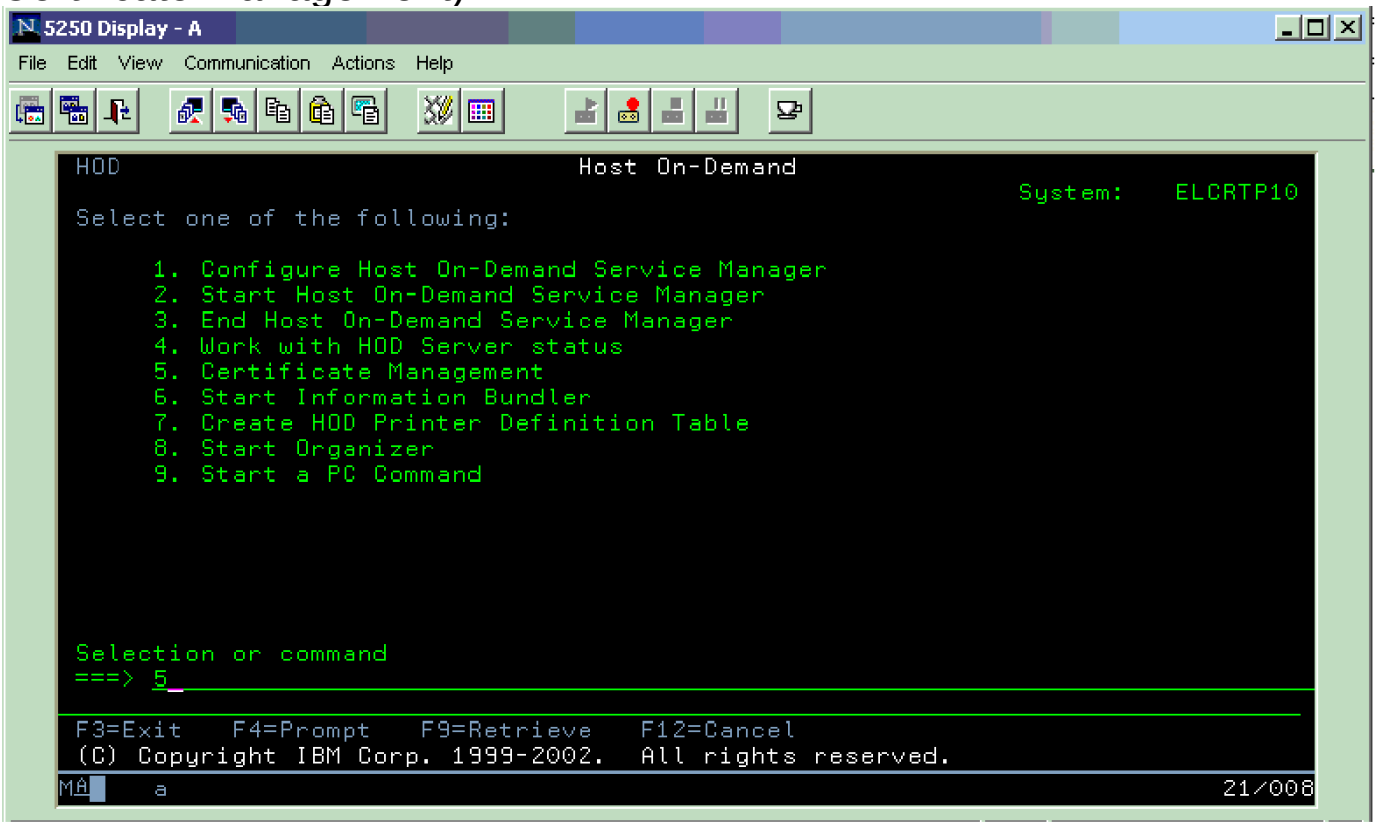
JAVA command to Convert .class file to .p12 z/OS

- To convert CustomizedCAs.class into CustomizedCAs.p12 with the file being in the hostondemand/HOD directory
- You must enter the command from the directory that the CustomizedCAs.class file resides, for example the publish directory (hostondemand/HOD)

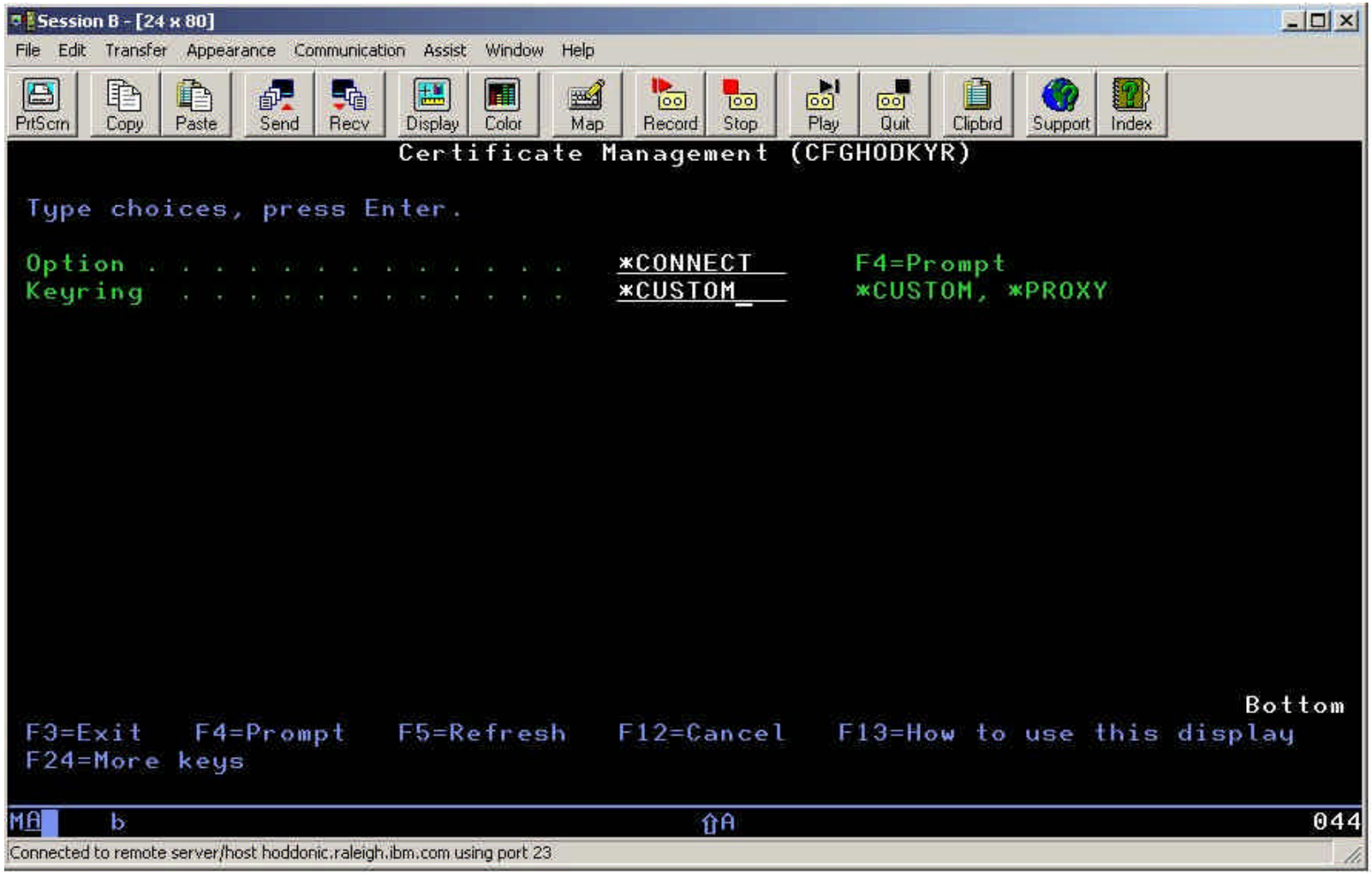
```
java -classpath ../lib/sm.zip
  com.ibm.eNetwork.HOD.convert.CVT2PKCS12
  CustomizedCAs.class hod
```

If you are using a self-signed certificate or a certificate from a signing agency that is NOT in the well known list, complete the following steps to configure a CustomizedCAs keyring on iSeries:

1. Type the following command: GO HOD.
2. Choose option 5 (Certificate Management).

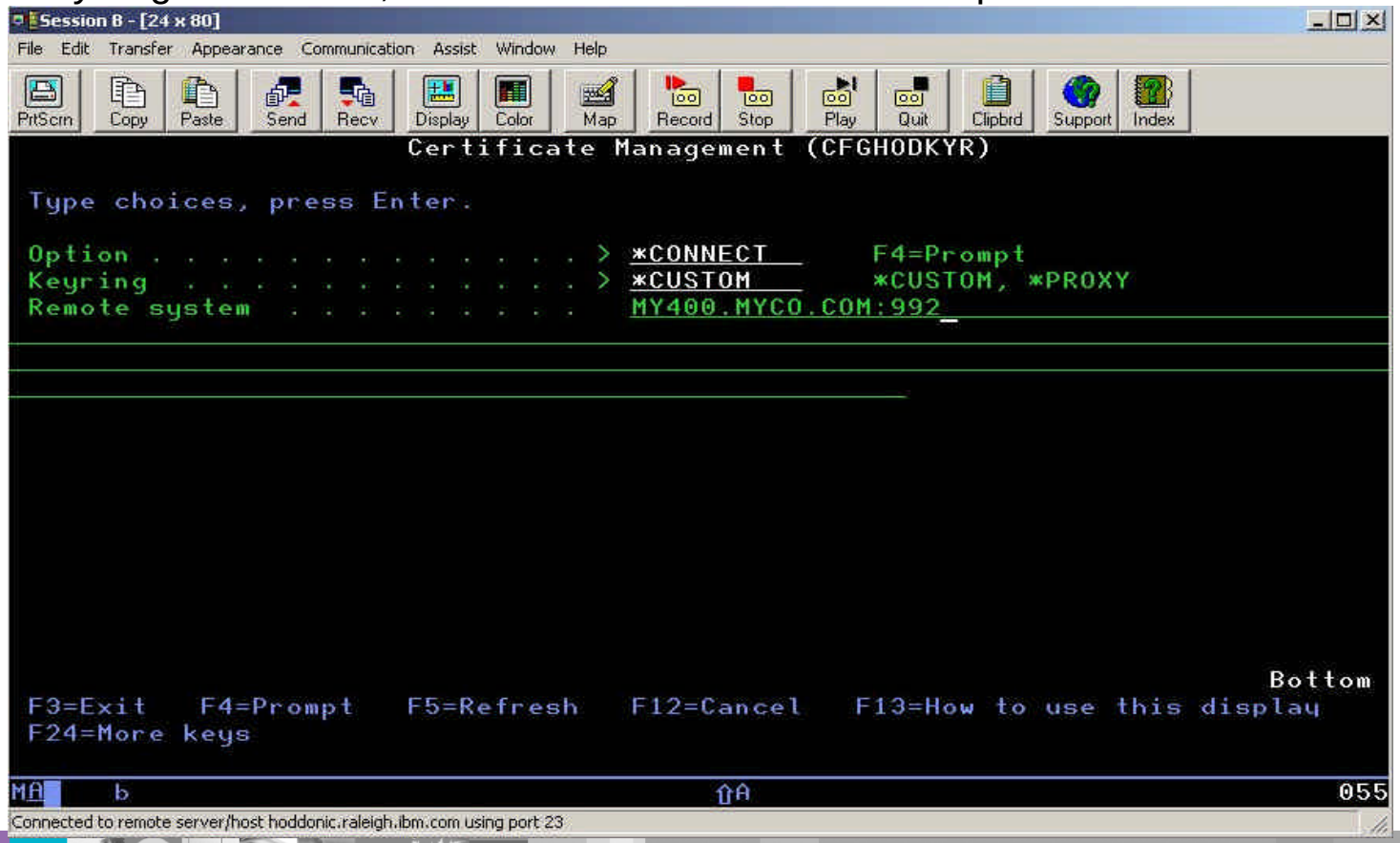


3. Enter *CONNECT for the option and *CUSTOM for the name of the keyring, then press the Enter key.



4. Type the TCP/IP name or IP address and port for the target server in the following format: server.name:port where server.name is the TCP/IP name of the target server (for example, my400.myco.com) and port is the port for the target server (for example, 992). This command can take a few minutes to complete. If you are prompted for a password, just press the Enter key. If this is the first certificate, a new CustomizedCAs object is created.

* Note: If you get an RC=1, check to see that the Java Group PTFs have been installed.



5. Select the certificate number that corresponds to the signer certificate that you want to add to the keyring. Usually this is 0, but, in some cases, 1.

To determine which certificate to add:

If 0 is the site certificate, adding this to the CustomizedCAs will allow clients to connect only to the server from which they receive the certificate (the server you are working on now or the one you connected to?).

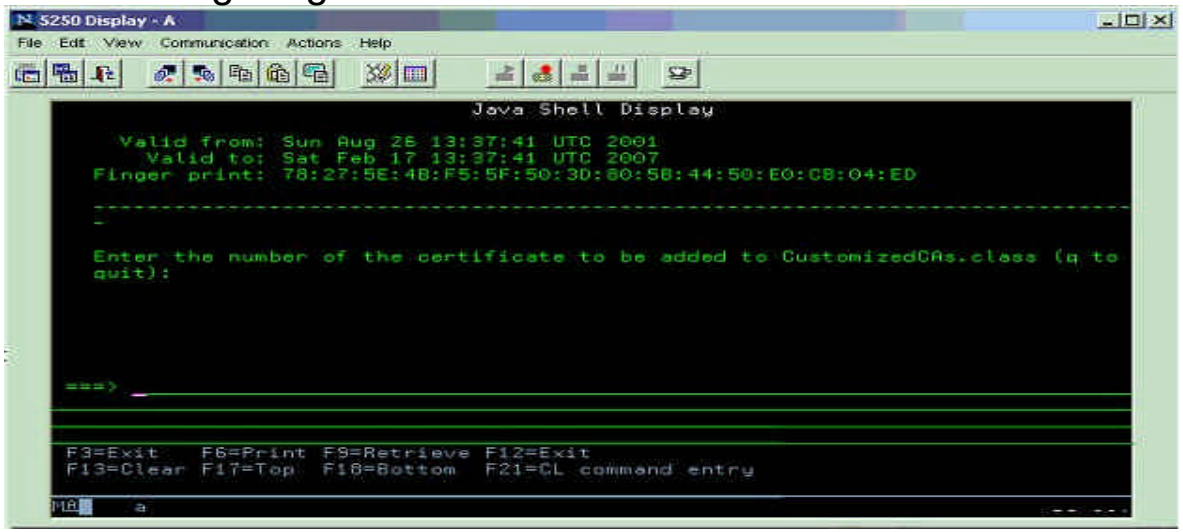
If you add certificate 0, you should get the message, "Adding the Site Certificate - 0 to CustomizedCas.class."

Adding certificate 1 or higher will allow clients to connect to any server whose certificate was signed by the same certificate authority. These are the CA certificates.

If you add certificate 1, you will get the message, "Adding the Signer Certificate - 1 to CustomizedCAs.class."

If the port is not responding, refer to Configuring iSeries servers for secure connection.

6. Repeat these steps for each target server.



Additional WebSphere Product Resources

- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at: http://www.ibm.com/developerworks/websphere/community/
- Learn about other upcoming webcasts, conferences and events: http://www.ibm.com/software/websphere/events_1.html
- Join the Global WebSphere User Group Community: www.websphere.org
- Access key product show-me demos and tutorials by visiting IBM Education Assistant: http://www.ibm.com/software/info/education/assistant
- Learn about the Electronic Service Request (ESR) tool for submitting problems electronically: http://www.ibm.com/software/support/viewlet/ESR_Overview_viewlet_swf.html
- Sign up to receive weekly technical My support emails: http://www.ibm.com/software/support/einfo.html
- Attend WebSphere Technical Exchange conferences or Transaction and Messaging conference: http://www.ibm.com/jct03001c/services/learning/ites.wss/us/en?pageType=page&c=a0011317

Questions and Answers