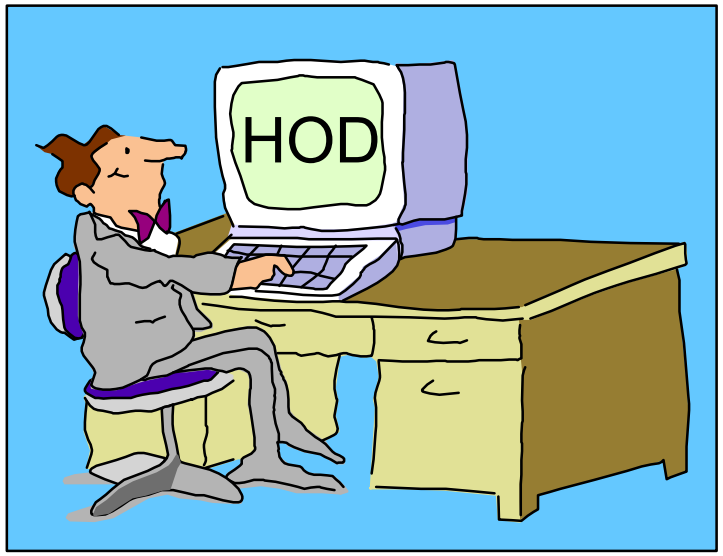
IBM®

TN3270E Secure Sockets Layer (SSL) and IBM WebSphere Host On-Demand V6 on OS/390 and z/OS



Linda Harrison
lharriso@us.ibm.com
05/06/02

Agenda

- TN3270E SSL and IBM HOD V6 on OS/390 and z/OS
  - Secure Sockets Layer (SSL)
  - Host On-Demand and SSL
  - SSL Optional Features
  - SSL Server Certificates
  - SSL Client Certificates
  - Using TN3270E SSL
  - OS/390 V2R6 and R7 MKKF Server Certficate
  - Migrate MKKF Certificate to IKEYMAN
  - OS/390 V2R8 GSKKYMAN Server Certificate
  - Make SSL Server Certficiate Available to HOD Clients
  - Client Certificate and Browser
  - Setup RACF for TN3270 Certificates
  - Migrate Certificate from GSKKYMAN to RACF
  - Create RACF Certificates
  - Use Express Logon Feature (ELF)

Agenda (cont.)

- Bibliography
- Web Sites

Abstract

Title: IBM Host On-Demand V6 for OS/390

Presenter: Linda Harrison supports OS/390 Host On-Demand in IBM Advanced Technical Support.

Audience: OS/390 Host On-Demand Installers

Abstract: Host On-Demand's browser-based access is the simplest way ever for users to reach critical host data because the user is not required to load or configure any software. Host On-Demand is a Java enabled Web based terminal emulation software supporting TN3270(E), TN5250, VT420, and IBM CICS Java Gateway. For users, Host On-Demand helps eliminate the confusing host and port names as all of the configuration is easily provided by the Administrator. From a web browser, users just click on a hyperlink that launches a session with the host. In addition to the usual web access, any number of sessions can be launched with multiple hosts at the same time. Since Host On-Demand installs on a server, maintenance, distribution, and upgrades are simplified. In the case of OS/390 Host On-Demand, the server that Host On-Demand installs onto is the OS/390 system, where most of today's enterprise mission-critical information still resides.

Secure Sockets Layer (SSL)

Key Pair

- Secure Sockets Layer (SSL) Certificate consists of a Key Pair:
  - Public Key - The key that is given to other hosts. The only key that can decrypt data that has been encrypted by the Private Key.
  - Private Key - The key that must never be given to other hosts. The only key that can decrypt data that has been encrypted by the Public Key.

SSL Server Authentication

1. The Client sends a connection request to the Server.
2. The Server sends the Server public key encrypted with a Signer's private key. The Signer is the Well-Known Certificate Authority (CA) or the Server if a Self Sign Certificate is used.
3. The Client has all Well-Known CA public keys (all browsers have preloaded Well- Known CA public keys). The Client must have the Server public key added if a Self Sign Certificate is used.
4. If the appropriate Signer's public key decrypts the Server public key then the session is approved for SSL encryption.
5. The Client encrypts a new randomly generated key pair with the Server public key (remember only the Server private key can decrypt data encrypted with the Server public key) and sends.
6. The Server and the client use this new randomly generated key pair for SSL session encryption.

SSL Client Authentication (Optional)

1. The Server Authentication is done and data is encrypted.
2. The Client sends the Client public key encrypted with a Signer's private key.
3. The Server must have the Well-Known CA public key or the Self Sign Certificate public key defined.
4. If appropriate Signer's public key decrypts the Client public key then the session is approved.

Negotiable SSL

- Telnet-negotiated Security (Negotiable SSL)
  - One OS/390 or z/OS TN3270 port supports secure and non-secure connections concurrently.
  - Communications Server for OS/390 V2R10+.
  - Supported on Host On-Demand 3270 display and printer sessions.
  - For more information about TN3270 SSL and Telnet-negotiated Security (IETF INTERNET-DRAFT TLS-based Telnet Security) see the "IP Configuration Guide, SC31-8725" Chapter 6 "Accessing Remote Hosts Using Telnet" section "Connection Security", the "IP Configuration Reference, SC31-8726" Chapter 11 "Telnet", the "System Secure Sockets Layer Programming Guide and Reference, SC24-5877-03" Chapter 6 "Certificate/Key Management", and the Host On-Demand "Planning and Installation Guide" also known as "Getting Started".

Host On-Demand and Secure Sockets Layer (SSL)

Host On-Demand and SSL

- There are multiple ways of using SSL with Host On-Demand.
  - SSL can be used on the HTTP session to port 80. Between Client Browser and HTTP Web Server. Please refer to HTTP Web Server documentation.
  - SSL can be used on the TN3270 session to port 23 (port number is customizable). Between the HOD Client and the TN3270 Server.
  - Not supported on OS/390 Host On-Demand Redirector, but supported on other HOD servers is the SSL encrypted Redirected HOD session.

SSL Optional Features

- SSL Optional Features Not Required
  - Secure connections can be made through an OS/390 or z/OS TN3270 secure port. When running with base TCP/IP, TN3270 connections accross ports defined as secure ports are protected only by way of MD5 or SHA hashing algorithms and support SSLV3 clients only. Encryption support by way of RC2, RC4, DES, or triple DES requires one of the optional features.

HOD Session Settings

- Secure Sockets Layer (SSL)
  - If "Enable Security (SSL)" is selected on the session Security tab the session will use SSL encryption with Server Authentication.
  - If "Server Authentication (SSL)" is selected on the session Security tab a DNS Server hostname verification is done. The hostname defined in the server certificate must match the hostname defined in the DNS.
  - If "Send a Certificate" is selected on the session Security tab the session will use Client Authentication.

Smart Card

- Smart Card Support
  - Store client certificate in the client's browser or in a dedicated security device such as a smart card.
    - Select "Certificate in browser or security device" on Security tab of session definition.
  - Store client certificate in a local or network-accessed file, in PKCS12 or PFX format, or in a URL, protected by a password.
    - Select "Certificate in URL or local file" on Security tab of session definition.
  - Add the browser's keyring to Host On-Demand client so that client will accept Certificate Authorities (CAs) trusted by the Microsoft Internet Explorer browser.
    - Select "Add MSIE browser's keyring" on Security tab of session definition.

Server Self Signed Certificate

- Distribute Self Signed Certificate
  - The OS/390 or z/OS TN3270 Server Self Signed Certificate public key can be defined to the Host On-Demand Server. If it is defined to the Host On-Demand Server it will be passed to each Host On-Demand Client. So even Self Signed Certificates or ones created by non-Well-Known CA's can be used without distributing the Signer's public key to each client manually.

HOD Express Logon Feature

- Express Logon Feature (ELF)
  - Enables a user, running a 3270 client session, to logon to an SNA host application (ie. TSO) using an SSL Client Digital Certificate defined to RACF instead of user ID and password.
  - Requires Communications Server for OS/390 V2R10+.
    - APAR PQ47742 / PTF UQ55691
  - Requires a session configured to use SSL client authentication with an express logon macro associated with it. When the session is launched the user is prompted to enter a PIN for the SSL client certificate.
  - The TSO password change has no effect since the password is never known to the client but the client certificate change is a manual process. Wherever the certificate is created, on the server or client, it must be updated to RACF at the same time that it is updated on the client workstation.

HOD ELF (cont.)

- Telnet-negotiated Security cannot be used at the same time as the Express Logon Feature.
- For more information about the Express Logon Feature see the White Paper "Setting up and Using the Express Logon Feature" that is available on the Library section of the Host On-Demand Home Page, and the Online Help Index items "express logon feature" and "express logon macro, recording".

Secure Sockets Layer (SSL)
Optional Features

SSL Requirements

OS 390	Product	Optional Feature Name	Function Provided
R5	Domino Go Webserv	DGW Export Security	HTTP SSL 56-bit
R5	Domino Go Webserv	DGW France Secure	HTTP SSL 40-bit
R5	Domino Go Webserv	DGW N America Secure	HTTP SSL 128-bit
R5	Comm Server	IP Security CDMF	IP Sec CDMF
R5	Comm Server	IP Security DES/CDMF	IP Sec DES/CDMF
R5	Comm Server	IP Kerberos DES	Kerberos DES 56-bit
R5	Comm Server	IP Kerberos non-DES	Kerberos non-DES
R6	Domino Go Webserv	DGW Export Security	HTTP SSL 56-bit
R6	Domino Go Webserv	DGW France Secure	HTTP SSL 40-bit
R6	Domino Go Webserv	DGW N America Secure	HTTP SSL 128-bit
R6	Comm Server	IP Security CDMF	IP Sec CDMF
			Telnet SSL RC2/RC4 40bit
R6	Comm Server	IP Security DES/CDMF	IP Sec DES/CDMF
			Telnet SSL DES 56bit
R6	Comm Server	IP Security TDES	IP Sec TDES
			Telnet SSL TDES
R6	Comm Server	IP Kerberos DES	Kerberos DES 56-bit
R6	Comm Server	IP Kerberos non-DES	Kerberos non-DES

SSL Requirements (cont.)

OS 390	Product	Optional Feature Name	Function Provided
R7	IBM HTTP Server	IBM HTTP Export Sec	HTTP SSL 56-bit
R7	IBM HTTP Server	IBM HTTP France Sec	HTTP SSL 40-bit
R7	IBM HTTP Server	IBM HTTP NA Secure	HTTP SSL 128-bit
R7	Comm Server	eNetwork CS Sec Lev 1	IP Sec CDMF
			Telnet SSL RC2/RC4 40bit
			Kerberos non-DES
R7	Comm Server	eNetwork CS Sec Lev 2	IP Sec DES/CDMF
			Telnet SSL DES 56bit
			Kerberos DES 56-bit
			SNMPV3 CBC DES 56-bit
R7	Comm Server	eNetwork CS Sec Lev 3	IP Sec TDES
			Telnet SSL TDES
			Kerberos DES 56-bit
			SNMPV3 CBC DES 56-bit

SSL Requirements (cont.)

OS 390	Product	Optional Feature Name	Function Provided
R8&9	IBM HTTP Server	IBM HTTP Export Sec	HTTP SSL 56-bit
R8&9	IBM HTTP Server	IBM HTTP France Sec	HTTP SSL 40-bit
R8&9	IBM HTTP Server	IBM HTTP NA Secure	HTTP SSL 128-bit
R8&9	Comm Server	SecureWay CS Sec Lev 1	IP Sec CDMF
			Telnet SSL RC2/RC4 40bit
			Kerberos non-DES
R8&9	Comm Server	SecureWay CS Sec Lev 2	IP Sec DES/CDMF
			Telnet SSL DES 56bit
			Kerberos DES 56-bit
			SNMPV3 CBC DES 56-bit
R8&9	Comm Server	SecureWay CS Sec Lev 3	IP Sec TDES
			Telnet SSL TDES
			Kerberos DES 56-bit
			SNMPV3 CBC DES 56-bit

SSL Requirements (cont.)

OS 390	Product	Optional Feature Name	Function Provided
R10&1	Crypto Services	Crypto Services base	HTTP SSL 40-bit
			HTTP SSL 56-bit
			Telnet SSL RC2/RC4 40bit
			Telnet SSL DES 56-bit
R10&1	Comm Server	IBM CS base	IP Sec CDMF
			IP Sec DES/CDMF
			SNMPV3 CBC DES 56-bit
R10&1	Comm Server	SecureWay CS Sec Lev 1	Kerberos non-DES
R10&1	Comm Server	SecureWay CS Sec Lev 2	Kerberos DES 56-bit
R10&1	Comm Server	SecureWay CS Sec Lev 3	IP Sec TDES
R10&1	IBM HTTP Server	IBM HTTP NA Secure	HTTP SSL 128-bit
R10&1	System SSL Sec	Sys SSL Security Lev 3	Telnet SSL TDES

(System SSL Sec does not need to be enabled unless Firewall is used)

SSL Requirements (cont.)

z/OS	Product	Optional Feature Name	Function Provided
R2&3	Crypto Services	Crypto Services base	HTTP SSL 40-bit
			HTTP SSL 56-bit
			Telnet SSL RC2/RC4 40bit
			Telnet SSL DES 56-bit
R2&3	Comm Server	SecureWay CS	Kerberos non-DES
			Kerberos DES 56-bit
R2&3	Comm Server	CS base	IP Sec CDMF
			IP Sec DES/CDMF
			SNMPV3 CBC DES 56-bit
R2&3	IBM HTTP Server	IBM HTTP NA Secure	HTTP SSL 128-bit
R2&3	System SSL Sec	Sys SSL Security Lev 3	Telnet SSL TDES
R2&3	Comm Server	SecureWay CS Sec Lev 3	IP Sec TDES

Secure Sockets Layer (SSL) Server Certificates

OS/390 and z/OS Certificate Tools

- To use OS/390 or z/OS TN3270 SSL create a Certificate Request and/or Server Public/Private Keys.
- There have been four Certificate Tools on OS/390 and z/OS. From the oldest to the newest: MKKF, IKEYMAN, GSKKYMAN, and RACF.

OS/390 V2R6 and R7 Certificate Tool

- The OS/390 V2R6 and V2R7 TCP/IP telnet servers require an MKKF format certificate.
  - The MKKF utility that ships as part of the OS/390 V2R6 and V2R7 LDAP server supports a 512-bit key size.
  - For OS/390 V2R6 and R7, how to create a private key and server certificate in the server's key ring file and a password stash file using MKKF is documented in "OS/390 Communications Server, IP Configuration, SC31-8513", Appendix D.
  - To use MKKF with certificate authority (CA) VeriSign, APAR OW39793 is required and a password for the keyringfile has to be 6 to 8 characters.

OS/390 V2R8 Certificate Tool

- The OS/390 V2R8 telnet server requires a certificate in the format of the GSKKYMAN utility.
  - GSKKYMAN utility is part of OS/390 V2R8+ System Secure Sockets Layer.
  - How to create the server key database using GSKKYMAN is documented in "OS/390 Communications Server, IP Configuration, SC31-8513", Appendix C, and the Redbook "IBM Host On-Demand 4.0: Enterprise Communications in the Era of Network Computing, SG24-2149-01".

OS/390 V2R10+ Certificate Tools

- The OS/390 V2R10+ telnet server requires a certificate in the format of the GSKKYMAN utility or RACF's Certificate Management Support.
  - The RACF RACDCERT command is detailed in the "OS/390 Security Server (RACF), Command Language Reference, SC28-1919".

Different Certificate Tools

- Some releases of the HTTP Web Server require an IKEYMAN format certificate.
  - A certificate created with MKKF can be migrated to an IKEYMAN format.
- An MKKF certificate can be migrated to GSKKYMAN and a GSKKYMAN database can be migrated to RACF.
  - Please see "OS/390 System SSL Programming Guide and Reference, SC24-5877".
- A certificate created with IKEYMAN can be exported using IKEYMAN and then a GSKKYMAN key database file can be created and the certificate can be imported into it.

Cryptography Library

- To start a TN3270 SSL port on an OS/390 or z/OS telnet server the Cryptography library must be defined to LINKLST.
  - I added the line:

    LNKLST ADD NAME(WSC.LINKLST) DSNAME(SYS1.CRYPTO.SGSKLOAD)

    to my **SYS1.PARMLIB(PROGF2)** member. Without this I received an **IEA995I SYMPTOM DUMP** with CODE=0C4. The dataset must also be program controlled. In RACF I changed the **CLASS=PROGRAM** with **PROFILE=***. I added '**SYS1.CRYPTO.SGSKLOAD**' to the member list.

Secure Sockets Layer (SSL) Client Certificates

SSL Client Authentication

- Create Client Certificate
  - Host On-Demand Locally Installed Client has a key-management utility that can be used to create a Client Certificate. This is detailed in the Redbook "SecureWay Communications Server for OS/390 V2R8 TCP/IP: Guide to Enhancements, SG24-5631-00", section "3.2.3.6 Working with the client certificate".

    http://www.redbooks.ibm.com
  - A Client Certificate can be obtained from a Well Known CA and exported in pkcs12 format from the browser through which it was received. The certificate can be stored on the local disk, network drive, or web server, from which the client can get it.
  - A Self Signed Client Certificate created on OS/390 using GSKKYMAN is only a V1 P12 file. HOD needs a V3 PKCS12 file so a browser can be used to convert the file.

Using TN3270E Secure Sockets Layer (SSL)

PROFILE.TCPIP TELNETPARMS

- TELNETPARMS SECUREPORT
  - On OS/390 V2R6+ TCP/IP uses the TELNETPARMS SECUREPORT statement to enable SSL Server Authentication.
- TELNETGLOBALS SECUREPORT
  - On OS/390 V2R10+ TCP/IP you can specify SECUREPORT in the TELNETGLOBALS block instead of the TELNETPARMS block.
- TELNETPARMS KEYRING SAF
  - On OS/390 V2R10+ TCP/IP uses the TELNETPARMS KEYRING SAF statement to define a RACF keyring to the telnet server.

TELNETPARMS (cont.)

- TELNETPARMS ENCRYPTION
  - On OS/390 V2R7+ the TELNETPARMS ENCRYPTION statement specifies a subset of the supported encryption algorithms to use for a port.
- TELNETPARMS CONNTYPE
  - On OS/390 V2R10+ the TELNETPARMS CONNTYPE can define Negotiable SSL (IETF INTERNET-DRAFT TLS-based Telnet Security) for TN3270 negotiation of SSL.
- TELNETPARMS EXPRESSLOGON
  - On OS/390 V2R10+ the TELNETPARMS ENCRYPTION statement specifies the Express Logon Feature.

TELNETPARMS and SERVAUTH

- TELNETPARMS CLIENTAUTH
  - On OS/390 V2R8+ use the TELNETPARMS CLIENTAUTH statement to enable SSL Client Authentication.
  - SSLCERT enables SSL Client Authentication only
  - SAFCERT enables SSL Client Authentication and checks that the user has a valid RACF userid assigned. The certificate must be defined to RACF with the RACDCERT command.
- SERVAUTH
  - On OS/390 V2R8+ use the RACF class SERVAUTH to limit access on a port basis.

OS/390 V2R6 and R7
MKKF Server Certificate

MKKF Server Certificate

Create Certificate with MKKF

1. Go to OMVS on OS/390, change the directory to the directory that you want the key ring to be in, and start MKKF:

   mkkf

2. Create and name the Server Keyring file (n for new):

   n

3. Input the key ring filename or press Enter for the default keyfile.kyr filename.

   This is the key ring filename to be used in the TCPIP PROFILE.

4. 'Work with keys and certificates':

   w

5. 'Create a key pair and request a certificate':

   c

6. Input the key ring password.
7. Input the password again for verification.

MKKF Server Certificate (cont.)

8. Select if the password will expire.

   To have the password expire, enter y and the number of days until it expires.

   To have the password not expire, enter n.

9. Request a server certificate or a CA certificate:

   s

10. Modify the key and certificate fields:

    m

11. Enter the Key Name label.
12. Select the Key Size.
13. Enter the Server Name; fully-qualified host name of the TN3270E server.

    If you select "Server Authentication" on your HOD session this Server Name must match the host name in the DNS for the IP address of the TN3270E server.

14. Enter the Organization Name.
15. Enter the Organization Unit Name.
16. Enter the Locality/City.
17. Enter the State/Province.

MKKF Server Certificate (cont.)

18. Enter the Postal Code.
19. Enter the two digit Country Code:

    US
20. Create the key pair and certificate request:

    r
21. Enter the certificate request filename.
22. Exit the Key menu:

    x
23. Create a stash file:

    c
24. Exit the Key Ring menu

    x
25. Save the key ring file and exit MKKF:

    y
26. If you are going to purchase a signed certificate from a Well Known Certificate Authority (CA), like VeriSign or Thawte, e-mail the certificate request to the CA and they will return it signed.

MKKF Server Certificate (cont.)

27. Start MKKF:

    mkkf

28. Open the key ring file:

    o

29. Enter the key ring filename from step 3.

30. Enter the password from step 6.

31. Receive the certificate into the key ring:

    r

32. Enter the certificate filename from step 21.

33. If you are receiving a self-signed certificate, confirm that you want to add the certificate to the key ring:

    y

34. If prompted, enter the certificate label for the signed certificate.

35. Exit the Key Ring Menu:

    x

36. Save the key ring file and exit MKKF:

    y

MKKF Server Certificate (cont.)

37. Start MKKF:

    mkkf

38. Open the key ring file:

    o

39. Enter the key ring filename from step 3.

40. Enter the password from step 6.

41. Work with keys and certificates:

    w

42. List the keys:

    l

43. Either select the key you want to make the default key:

    s

    Or display the next key:

    n

44. Make the key the default key in the key ring:

    f

MKKF Server Certificate (cont.)

45. Confirm the default key:

    y

46. Exit the Key Menu:

    x

47. Exit the Key Ring Menu:

    x

48. Save the key ring file and exit MKKF:

    y

Migrate MKKF Certificate to IKEYMAN

Migrate MKKF Certificate to IKEYMAN

Migrate the certificate from MKKF to IKEYMAN

1. Go to OMVS on OS/390, change the directory to the directory that has the certificate in it.
2. Set up the environment for IKEYMAN:

   ```
   export PATH=/usr/lpp/internet/bin:$PATH
   export LIBPATH=/usr/lpp/internet/bin:$LIBPATH
   export NLSPATH=/usr/lpp/internet/%L/%N:$NLSPATH
   ```

3. Convert kyr file to kdb format:

   ```
   ikeyman -m -r keyfile.kyr
   ```

   where keyfile is the name of the mkkf key ring file.
4. Enter password.

   File keyfile.kdb is created.
5. Start IKEYMAN:

   ikeyman
6. 'Open key database':

   2

Migrate MKKF Certificate (cont.)

7. Enter the key database name:

   keyfile.kdb

8. Enter password.

9. 'List/Manage keys and certificates':

   1

10. Select the number of the certificate you want to make available to HOD clients.

11. 'Copy the certificate of this key to a file':

    5

12. Select binary file type:

    2

13. Input filename:

    cert.der

    This is the certificate to be made available to the HOD clients.

14. Exit IKEYMAN:

    1

OS/390 V2R8+
GSKKYMAN Server Certificate

GSKKYMAN Server Certificate

Create Certificate with GSKKYMAN

1. Go to OMVS on OS/390, change the directory to the directory that you want the key ring to be in.

   My directory on my system is /u/harrisl.

2. You can display your environment settings, including STEPLIB:

   env

   I needed to add the C and Crypto library to my STEPLIB:

   export STEPLIB=$STEPLIB:SYS1.CRYPTO.SGSKLOAD:SYS1.CPP.SCLBDLL

3. Start GSKKYMAN:

   gskkyman

4. 'Create new key database':

   1

5. Input a database filename or press Enter for the default key.kdb filename.

   I input nm512.kdb and file ***/u/harrisl/nm512.kdb*** was created.

6. Input a password.

   I input *one0ssl* on my system.

GSKKYMAN Server Certificate (cont.)

7. Input password again for verification.
8. Select if the password will expire.

   I selected *1* so that the password would expire.

   Then I pressed *Enter* to default to a 60 day expiration.
9. Select to work with the database now:

   1
10. If you are going to purchase a signed certificate from a Well Known Certificate Authority (CA), like VeriSign or Thawte, select 3 'Create new key pair and certificate request'. If you are going to create a self-signed certificate, select 5 'Create a self-signed certificate'.

    I created a self-signed certificate:

    5
11. Select a version 3 Certificate:

    3
12. Input a certificate label name:

    I input *nmlow* for a certificate label name on my system.

GSKKYMAN Server Certificate (cont.)

13. Select key size.

    I selected *1* for 512 key size.

14. Input 'Common Name'; the fully-qualified host name of the TN3270E server.

    I input *mvsnm2*.

    If you select "Server Authentication" on your HOD session this 'Common Name' must match the hostname in the DNS for the IP address of the TN3270E server.

15. Input the 'Organization'.

    I input *IBM*.

16. Input the 'Organization Unit'.

    I input *nsc*.

17. Input the 'City'.

    I input *GBURG*.

18. Input 'State'.

    I input *MD*.

GSKKYMAN Server Certificate (cont.)

19. Input two digit 'Country'.

    I input *US*.

    Note: If you use USA then you get the following error when you try to save:

    Error: An asn.1 encoding/decoding error occurred.

20. Input number of days for certificate.

    I pressed *ENTER* to default to 365 days.

21. If you are purchasing a signed certificate, send the request to CA and after the request is returned select 4 'Receive a certificate issued for your request'.

22. Set key as the default key in the database:

    1

23. Save the certificate to a file:

    1

24. Save as a binary file:

    2

25. Input a filename or press Enter for the default name of cert.crt.

    I input *nmlow.crt* and file ***/u/harrisl/nmlow.crt*** was created.

GSKKYMAN Server Certificate (cont.)

26. Do not exit yet:

    0

27. 'Store encrypted database password':

    11

    I received a message back that password had been stored in

    /u/harrisl/nm512.sth.

28. Exit GSKKYMAN:

    1

Make SSL Server Certificate Available to HOD Clients

SSL Server Certificate

➢ Make the Certificate Available to the HOD Clients

1. Change to the root directory:

   cd /

2. Locate the HOD web-published directory:

   find . -name WellKnown TrustedCAs.class*

   The published directory on my system is the default

   /usr/lpp/HOD/hostondemand/HOD.

3. Copy the binary certificate into the published directory:

   cp /u/harrisl/nmlow.crt /usr/lpp/HOD/hostondemand/HOD/nmlow.crt

   Note: Copy as a binary file and no character conversion.

4. Locate the Host On-Demand server directory:

   find . -name sm.zip*

   The server directory contains the file archives used to run the Service Manager.

   The server directory on my system is /usr/lpp/HOD/hostondemand/lib.

5. Change to the HOD published directory:

   cd /usr/lpp/HOD/hostondemand/HOD

SSL Server Certificate (cont.)

6. Add the certificate to the CustomizedCAs.class file, using the keyrng Java Utility.

   For HOD V3 type the following, all on one line:

   `java -classpath .:HOD_SERVER_DIR/sm.zip:$CLASSPATH com.ibm.sslight.tools.keyrng CustomizedCAs add --certificatetype cert.der`

   For HOD V4 or V5 type the following, all on one line:

   `java -classpath .:HOD_SERVER_DIR/sm.zip:$CLASSPATH com.ibm.hodsslight.tools.keyrng CustomizedCAs add --certificatetype cert.der`

   where **`HOD_SERVER_DIR`** is the HOD server directory,

   `certificatetype` is **`ca`** if you are adding a CA root certificate

   or **`site`** if you are adding a site or self-signed certificate,

   and **`cert.der`** is the name of the file containing the binary certificate.

(continued on next page)

SSL Server Certificate (cont.)

6. (cont.)

Note: **CustomizedCAs** must be capitalized exactly as shown, there is a single hyphen before the classpath parameter, and a double hyphen before the certificate parameter. If the java command is typed in with incorrect syntax you will get the following error:

Unable to initialize Threads: Cannot find class /java/lang/Thread

If no CustomizedCAs.class file exists, keyrng prompts you for a password with which to encrypt the new class-file. However, CustomizedCAs.class must NOT be encrypted, so just ENTER at the password prompt.

I found I needed the following path to the java code:

```
export PATH=$PATH:/usr/lpp/java/J1.1/bin
```

I found this in the ServiceManager.sh script in /usr/lpp/HOD/hostondemand/lib.

I issued the following on my system:

```
java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip:\
/usr/lpp/java/J1.1/lib/classes.zip \
com.ibm.hodsslight.tools.keyrng CustomizedCAs add --site nmlow.crt
```

SSL Server Certificate (cont.)

6. (cont.)

For Java 2 (JDK 1.3) I needed the following:

export CLASSPATH=/usr/lpp/java/IBM/J1.3/lib

export PATH=/usr/lpp/java/IBM/J1.3/bin:$PATH

java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip:
**$CLASSPATH com.ibm.hodsslight.tools.keyrng **

CustomizedCAs add --site nmlow.crt

JDK 1.3 requires more memory than 1.1.8 so I got the following error:
Exception in thread "main"

until I changed my logon TSO memory size to 9000.

SSL Server Certificate (cont.)

7. Check to see if the certificate was added.

   For HOD V3 type the following, all on one line:

   java -classpath .:HOD_SERVER_DIR/sm.zip:$CLASSPATH

   com.ibm.sslight.tools.keyrng CustomizedCAs verify

   For HOD V4 or V5 type the following, all on one line:

   java -classpath .:HOD_SERVER_DIR/sm.zip:$CLASSPATH

   com.ibm.hodsslight.tools.keyrng CustomizedCAs verify

   This should be followed by something similar to the following:

   ```
   --------Key ring entry:  1 -------------------
   Entry type:  Site Certificate
   Key:  RSA/512 bits
   Subject:  aix-f26.raleigh.ibm.com,ibm,US
   Issuer:  aix-f26.raleigh.ibm.com,ibm,US
   Valid from:  Fri Aug 13 2:21:29 EDT 1999
   Valid to:  Sun Aug 13 12:21:29 EDT 2000
   Finger print: D7:2D:E9:6B:66:00:54:04:44:DE:02:E4:4E:1C:80:85
   ```

   The last certificate shown should be the one just added.

(continued on the next page)

SSL Server Certificate (cont.)

7. (cont.)

   I issued the following on my system:

   java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip:
   **/usr/lpp/java/J1.1/lib/classes.zip **
   com.ibm.hodsslight.tools.keyrng CustomizedCAs verify

   Note: The CustomizedCAs.class file does not remove any previous information but instead adds the new certificate information so the file may be corrupted if an error occurs when trying to use SSL like the following:

   keyrng: Cannot retrieve key ring data: com.ibm.hodsslight.SSLException

   or

   EZZ6021I TELNET PROFILE UPDATE FAILURE FOR PORT 723 on the system log,

   EZZ6029I PROFILE ERROR ON PORT 723, SSL NOT AVAILABLE

   If this happens try deleting the CustomizedCAs.class file from the publish directory and issuing the above java command again.

8. Exit OMVS.

SSL Server Certificate (cont.)

9. Create HOD session with "Enable Security (SSL)" selected.

   Note: If you select "Server Authentication (SSL)" on your HOD session the 'Common Name' input when creating the certificate must match the host name in the DNS for the IP address of the TN3270E server.

10. On OS/390 TN3270E server create TELNET SECUREPORT statement and BEGINVTAM PORT statement in TCPIP PROFILE:

```
TELNETPARMS
   SECUREPORT 723 KEYRING HFS /u/harrisl/nm412.kdb
   ...
ENDTELNETPARMS
BEGINVTAM
   PORT 723
   ...
ENDVTAM
```

11. Recycle HOD and TCP/IP servers and you're done!

Client Certificate and Browser

GSKKYMAN Client Certificate

Create Client Certificate with GSKKYMAN

1. Create a new key database and self-signed certificate with GSKKYMAN, just like the server certificate. This is the client key database and public key.
2. Add this client certificate (public key) to the Server key database.
3. Use GSKKYMAN to export the key by using option "9 Export keys" to create a p12 file.
4. FTP p12 file (in binary) to the client workstation.
5. Use the workstation browser to upgrade the p12 certificate.

Client Certificate and TN3270 Server

- Add Client Public key to Server Key Database

1. Start GSKKYMAN:

   gskkyman

2. Open Server key database:

   nm512.kdb

3. Enter password:

   one0ssl

4. Store a CA certificate:

   6

5. Enter certificate file name:

   lin512.crt

6. Enter label:

   lin512

7. Exit GSKKYMAN:

   1

Client Certificate and Netscape

Client Certificate and Netscape Browser

- Netscape Communicator 4.72 - On the Netscape Communicator window:
  1. Select Communicator, Tools, Security Info
  2. Select Yours under Certificates
  3. Select Import a Certificate
  4. Enter the password of the file to import it
  5. Select file that you FTPed from OS/390
  6. Enter password
  7. Select the P12 file that just appeared under "These are your certificates"
  8. Select Export
  9. Enter new password for the new file
  10. Enter the location to save the new file (to be used by HOD)

Client Certificate and Internet Explorer

Client Certificate and Internet Explorer Browser

- Internet Explorer V5 - On the Internet Explorer window:
  1. Select Tools, Internet Options
  2. Select the Content tab
  3. Select Certificates
  4. Select Import
  5. Enter filename to import it
  6. Enter the password of the file
  7. Select the P12 file that just appeared under "Issued To"
  8. Select Export
  9. Enter new password for the new file
  10. Enter the location to save the new file (to be used by HOD)

Client Certificate and PComm

- Optionally Add Client Certificate to Personal Communications (same as adding server certificate)
- Personal Communications - WorkStation Program V5:
  1. FTP lin512.crt in binary to workstation.
  2. Copy lin512.crt to directory
     "C:\Program Files\Personal Communications\private".
  3. Start PComm Certificate Management.
  4. Open PcommClientKeyDb.kdb, default password pcomm (which it tells you if you enter the wrong one).
  5. Click on Add.
  6. Change Data Type to "Binary DER data" and Certificate File Name to "lin512.crt".
  7. Click OK.
  8. Close PComm Certificate Management.
  9. Change session to use SSL port and enable security.

Setup RACF for TN3270 Certificates

Setup RACF for TN3270 Certificates

- Use the following commands to setup RACF to store SSL Certificates:

```
RDEFINE FACILITY IRR.DIGTCERT.ADD UACC(NONE)
RDEFINE FACILITY IRR.DIGTCERT.ADDRING UACC(NONE)
RDEFINE FACILITY IRR.DIGTCERT.CONNECT UACC(NONE)
RDEFINE FACILITY IRR.DIGTCERT.DELETE UACC(NONE)
RDEFINE FACILITY IRR.DIGTCERT.GENCERT UACC(NONE)
RDEFINE FACILITY IRR.DIGTCERT.GENREQ UACC(NONE)
RDEFINE FACILITY IRR.DIGTCERT.LIST UACC(NONE)
RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE)
RDEFINE FACILITY IRR.DIGTCERT.REMOVE UACC(NONE)
SETROPTS RACLIST(FACILITY) REFRESH
```

Setup RACF for Certificates (cont.)

- Use the following commands to authorize TN3270 access to the RACF SSL Certificates:

```
PERMIT IRR.DIGTCERT.ADD CLASS(FACILITY) ID(TCPIPUX) ACC(CONTROL)
PERMIT IRR.DIGTCERT.ADDRING CLASS(FACILITY) ID(TCPIPUX)
   ACC(CONTROL)
PERMIT IRR.DIGTCERT.CONNECT CLASS(FACILITY) ID(TCPIPUX)
   ACC(CONTROL)
PERMIT IRR.DIGTCERT.DELETE CLASS(FACILITY) ID(TCPIPUX)
   ACC(CONTROL)
PERMIT IRR.DIGTCERT.GENCERT CLASS(FACILITY) ID(TCPIPUX)
   ACC(CONTROL)
PERMIT IRR.DIGTCERT.GENREQ CLASS(FACILITY) ID(TCPIPUX)
   ACC(CONTROL)
PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ID(TCPIPUX) ACC(CONTROL)
```

(cont. on next page)

Setup RACF for Certificates (cont.)

```
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(TCPIPUX)
    ACC(CONTROL)
PERMIT IRR.DIGTCERT.REMOVE CLASS(FACILITY) ID(TCPIPUX)
    ACC(CONTROL)
SETROPTS RACLIST(FACILITY) REFRESH
SETROPTS CLASSACT(DIGTCERT)
SETROPTS CLASSACT(DIGTRING)
SETROPTS RACLIST(DIGTCERT) REFRESH
SETROPTS RACLIST(DIGTRING) REFRESH
```

Note: In the above commands the userid associated with my TCP/IP started task is TCPIPUX.

Note: Without these settings I received the following error:

```
EZZ6030I TELNET SSL UNAVAILABLE, UNABLE TO INITIALIZE SSL
    INTERFACE, RSN =FF9D
```

Migrate Certificate from GSKKYMAN to RACF

Migrate from gskkyman

- Migrate Certificate(s) from gskkyman to RACF
  - Using gskkyman export server and optionally client certificate to a PKCS12 file.

    gskkyman

    2 - Open key database

    Enter database name and password.

    1 - List/Manage keys and certificates

    Select certificate.

    9 - Export the key to a file

    Enter filename.p12 and password.
  - Binary copy the PKCS12 file(s) from HFS to data set.

Migrate from gskkyman (cont.)

- Use the following commands to create a RACF key ring and add the certificates:

```
RACDCERT ID(TCPIPUX) ADDRING(ELFTEST)
RACDCERT ID(TCPIPUX) ADD('HARRISL.SSL.NMLOWP12')
   TRUST WITHLABEL('NMLOW') PASSWORD('one0ssl')
RACDCERT ID(TCPIPUX) CONNECT(ID(TCPIPUX)
   LABEL('NMLOW') RING(ELFTEST) DEFAULT)
RACDCERT ID(HARRISL) ADD('HARRISL.SSL.SSLOWP12')
   TRUST WITHLABEL('SSLLOW') PASSWORD('one0ssl')
RACDCERT ID(TCPIPUX) CONNECT(ID(HARRISL)
   LABEL('SSLLOW') RING(ELFTEST))
```

Note: In the above commands the userid associated with my TCP/IP started task is TCPIPUX and the userid associated with the optional client certificate is HARRISL.

Migrate from gskkyman (cont.)

- Define the RACF SSL key ring to the TN3270 Server and optionally define the Client authentication in the PROFILE.TCPIP TELNETPARMS:

  KEYRING SAF ELFTEST

  CLIENTAUTH SSLCERT

Create RACF Certificates

Create RACF Certificate(s)

- Create Certificate(s) with RACF
  - Use the following commands to create a RACF key ring and certificates:

```
RACDCERT ID(TCPIPUX) ADDRING(ELFTEST2)
RACDCERT ID(TCPIPUX) GENCERT SUBJECTSDN(CN('ELFSERV')
   T('NETCENT') OU('COMMSERV') O('ATS') L('GBURG') SP('MD')
   C('US')) SIZE(512) WITHLABEL('ELFSERV')
   KEYUSAGE(DATAENCRYPT)
RACDCERT ID(HARRISL) GENCERT SUBJECTSDN(CN('ELFCLNT')
   T('NETCENT') OU('COMMSERV') O('ATS') L('GBURG') SP('MD')
   C('US')) SIZE(512) WITHLABEL('ELFCLNT')
   KEYUSAGE(CERTSIGN)
```

(cont. on next page)

Create RACF Certificate(s) (cont.)

```
RACDCERT ID(TCPIPUX) CONNECT(ID(TCPIPUX) LABEL('ELFSERV')
   RING(ELFTEST2) DEFAULT)
RACDCERT ID(TCPIPUX) CONNECT(ID(HARRISL) LABEL('ELFCLNT')
   RING(ELFTEST2))
RACDCERT ID(TCPIPUX) EXPORT(LABEL('ELFSERV'))
   DSN('HARRISL.SSL.ELFSERV')
   FORMAT(CERTDER) PASSWORD('one0ssl')
RACDCERT ID(HARRISL) EXPORT(LABEL('ELFCLNT'))
   DSN('HARRISL.SSL.ELFCLNT')
   FORMAT(PKCS12DER) PASSWORD('one0ssl')
```

Note: In the above commands the userid associated with my TCP/IP started task is TCPIPUX and the userid associated with the optional client certificate is HARRISL.

Create RACF Certificate(s) (cont.)

- Binary copy certifcate(s) from data set to HFS file(s).
- Using java add command add the server certificate to the CustomizedCAs:

export PATH=/usr/lpp/java/IBM/J1.3/bin:$PATH

```
java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip:\
$CLASSPATH com.ibm.hodsslight.tools.keyrng \
CustomizedCAs add --site elfserv.p12
```

JDK 1.3 requires more memory than 1.1.8 so I got the following error:

```
Exception in thread "main"
```

until I changed my logon TSO memory size to 9000.

- Optionally binary FTP the client certificate to the workstation and define it to the Host On-Demand session.

Create RACF Certificate(s) (cont.)

- Define the RACF SSL key ring to the TN3270 Server and optionally define the Client authentication in the PROFILE.TCPIP TELNETPARMS:

  KEYRING SAF ELFTEST2

  CLIENTAUTH SSLCERT

Use Express Logon Feature (ELF)

Express Logon

- Use Host On-Demand Express Logon Feature
  - Store server and client SSL certificates in RACF.
  - Define the RACF SSL key to the TN3270 Server and the RACF Client authentication in the PROFILE.TCPIP TELNETPARMS:

    KEYRING SAF ELFTEST

    CLIENTAUTH SAFCERT
  - Use the following RACF commands to define pass ticket support in RACF:

    SETROPTS CLASSACT(PTKTDATA)

    SETROPTS RACLIST(PTKTDATA)

Express Logon (cont.)

- Use the following RACF commands to define the application(s) (ie. TSO) to the RACF pass ticket support:

```
RDEFINE PTKTDATA TSONM2
   SSIGNON(KEYMASKED(E1E2E3E4E5E6E7E8)) UACC(NONE)
SETROPTS RACLIST(PTKTDATA) REFRESH
SETROPTS RACLIST(DIGTCERT) REFRESH
SETROPTS RACLIST(DIGTRING) REFRESH
```

Note: In the above commands NM2 is the SMF system ID defined in SMFPRMxx member of SYS1.PARMLIB and the KEYMASKED parameter is a hex string of your choice.

Express Logon (cont.)

- Create the Host On-Demand Express Logon Macro:
  1. Start Host On-Demand session and connect to a host.
  2. Click on Record Macro to start macro recording.
  3. Enter macro name (ie. ELF_TSO), description, check Express Logon Feature, and click OK.
  4. Enter the application ID defined to RACF (ie. TSONM2), and click OK.
  5. Navigate Host On-Demand session until a userid field is presented.
  6. Click Next> to indicate that the screen is not an alternate start screen.
  7. Click Next> to indicate that the screen contains a userid field.
  8. Click Current and enter the logon userid (ie. HARRISL).

Express Logon (cont.)

9. Click No and Next> to indicate that the screen does not contain a password field.
10. Navigate Host On-Demand session until a password field is presented.
11. Click OK to indicate that the screen contains a password field.
12. Click Current and enter the logon password.
13. Click OK.
14. Click Stop Macro to stop the macro recording.
15. Click Yes and OK to have the macro run automatically at session startup.

- Define Express Logon to the TN3270 Server in the PROFILE.TCPIP TELNETPARMS:

  EXPRESSLOGON

Bibliography

Bibliography

- Announcement Letters:
  - 200-324 IBM Host Access Client Package V1R0
  - 201-053 IBM Host Access Client Package V1R1
  - 201-267 IBM Host Access Client Package V2R0
  - 200-262 IBM Host Publisher V2R2
- Program Directories:
  - GI10-3175-00 IBM Host On-Demand Version 5 for System/390
  - GI10-3191-00 IBM Host On-Demand Version 6 for System/390
  - GI10-3176-00 IBM Screen Customizer Version 2.05 for System/390
  - GI10-3207-00 IBM Screen Customizer Version 2.0.60 for System/390

Bibliography

- The following three documents are available after Host On-Demand installation (where 9.82.1.100 is the IP address of the OS/390 system where HOD is installed) and they are also available on the HOD Library page off of the Host On-Demand Home page:
  - Host On-Demand Readme

    http://9.82.1.100/hod/en/doc/readme/readme.html
  - Planning and Installation Guide (also known as "Getting Started")(also available in pdf as install.pdf)

    http://9.82.1.100/hod/en/doc/install/install.html
  - Host Printing Reference

    http://9.82.1.100/hod/en/doc/hostprint/hostprintref.html
- The following four documents are available from the "IBM Host Access Toolkit" directory after Toolkit installation:
  - Getting Started (also available from the Toolkit CD panel)
  - Host Access Class Library Reference
  - Host Access Beans for Java Reference
  - Open Host Interface Objects Reference

Bibliography

- The following two documents are available after Screen Customizer installation (where 9.82.1.100 is the IP address of the OS/390 system where Screen Customizer is installed) and they are also available on the Screen Customizer Library page off of the Screen Customizer Home page:
  - Screen Customizer Readme

    http://9.82.1.100/hod/en/doc/custom/readme/readme.html
  - Planning and Installation Guide (also known as "Getting Started")(also available in pdf as installation.pdf)

    http://9.82.1.100/hod/en/doc/custom/install/installation.html

Bibliography

- The following Redbooks are available at http://www.redbooks.ibm.com:
  - IBM SecureWay Host On-Demand 4.0: Enterprise Communications in the Era of Network Computing, SG24-2149-01
  - IBM WebSphere Host On-Demand: Version 5 Enhancements, SG24-5989
  - IBM SecureWay Communications Server for OS/390 V2R8 TCP/IP: Guide to Enhancements, SG24-5631
  - IBM Web-to-Host Integration Solutions, SG24-5237
  - IBM Host Integration in a Secure Network: A Practical Approach, SG24-5988
- IBM OS/390 manuals:
  - Communications Server for OS/390, IP Configuration, SC31-8513
  - Communications Server for OS/390, IP Configuration Guide, SC31-8725
  - Communications Server for OS/390, IP Configuration Reference, SC31-8726
  - System Secure Sockets Layer (SSL) Programming Guide and Reference, SC24-5877
  - OS/390 Security Server (RACF) Command Language Reference, SC28-1919

Web Sites

Web Sites

- Host On-Demand Product Information site:

  http://www.ibm.com/software/webservers/hostondemand

  Select Support from the above Home Page to get to the Support Page.

  Select Library from the above Home Page to get to the Library page.

- Screen Customizer Product Information site:

  http://www.ibm.com/software/network/screencustomizer

  Select Support from the above Home Page to get to the Support Page.

  Select Library from the above Home Page to get to the Library page.

- This and other presentations are available on web site:

  http://www.ibm.com/support/techdocs

  PRS351 "IBM WebSphere Host On-Demand V6 for OS/390 and z/OS"

  "TN3270E Secure Sockets Layer (SSL) and IBM WebSphere Host On-Demand V6 on OS/390 and z/OS"

  PRS352 "IBM WebSphere Host Publisher V2R2 for OS/390 and z/OS"

Web Sites (cont.)

- IBM HTTP Server Product Information site:

  http://www.ibm.com/software/webservers/httpservers
- IBM HTTP Server SSL Examples:

  http://www.ibm.com/software/webservers/httpservers/gskkyman.htm