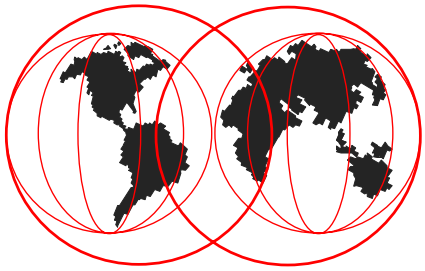
# SSL Enablement of OS/390 TN3270

Paul de Graaff IBM ITSO Poughkeepsie S/390 Security



IBM Technical Support

- 
- 
- Paul M. de Graaff is a Certified I/T Specialist at the International Technical Support Organization, Poughkeepse Center.  He writes extensively and teaches IBM classes worlwide on all areas of S/390 Security.  Before joining the ITSO, Paul worked with IBM Global Services in The Netherlands as a senior I/T Specialist

## Agenda

- SSL Support in R6 for Telnet
  - TN3270 SSL Server Authentication
  - Host on Demand
  - Personal Communications
- SSL Support in R8 for Telnet
  - TN3270 SSL Client Authentication
  - Use of RACF Digital Certificate Support
  - Host on Demand V4
- Future Focus Areas
  - RACF and LDAP Usage
  - SNA Use of Client Certificates

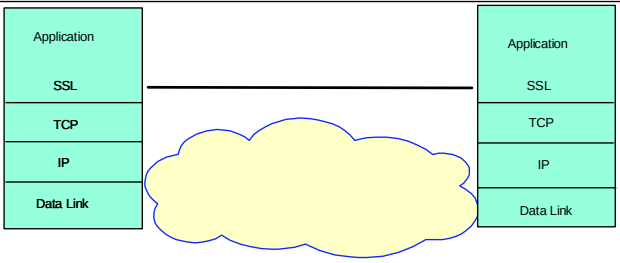
IBM Technical Support



- 
- The objectives for this session are to show past, present and future TELNET SSL features and enhancements. This will be accomplished by reviewing the introduction of SSL support in TELNET, OS/390 V2.6. Then the discussion will shift to enhancements that are available in TELNET for OS/390 V2.8, finally this presentation will touch on the future enhancements currently in the development pipeline.

# Support in OS/390 V2.R6

## Secure Sockets Layer - What is it?




- Provides authentication, integrity, and data privacy above TCP layer.
  - Protocol includes key exchange using public key cryptography and negotiation of security parameters
- Applications must be changed to use SSL
- Applications that use SSL:
  - Application Websphere
  - TN3270 Server

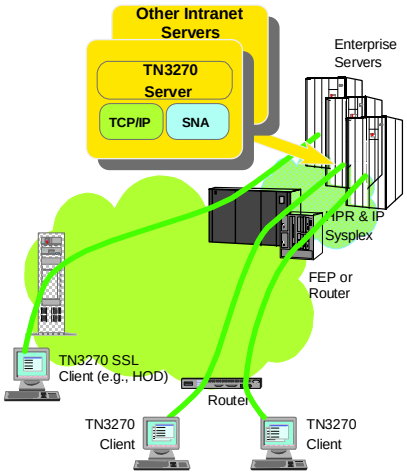
IBM Technical Support



- Before getting into the features of SSL used within TELNET a quick overview of what Secured Sockets Layer is and does is needed.
- 
- The objective of SSL is to provide a degree of authentication and integrity over a TCP/IP layer.
- 
- Briefly, the negotiation occurs as follows.
- 1)The client application initiates contact with the server application, the server answers back thus showing the application can be reached through this port.
- 2)The server application sends its certificate containing the server application's public key. At this point the client application can encrypt it's responses back to the server application using the server's public key. Secondarily the client can verify the server's certificate against the client's list of trusted certificate authorities (CAs) - this portion of the negotiation is server side authentication
- 3)If required the client would then pass its certificate containing the client's application's public key (encrypted using the server application's public key) to the server. The server decrypts using it's private key then checks the client's certificate against the server's list of trusted certificate authorities - this portion of the negotiation is client side authentication.
- 
- Additionally negotiation takes place to find an agreed upon cipher suite in which to encrypt the rest of the communication between the 2 applications. At any time either client or server may break the communication link.
- 
- Note that applications must be changed to use SSL.

## TCP/IP SSL Enabling for TN3270 (V2R6)

- **Secure TN3270 data exchange**
  - SSL server side authentication support using X.509 Certificates
  - Client authentication done with userid/password over encrypted session
  - Uses SSL protocols to authenticate and set up shared secrets for encryption of data
  - DES and Triple DES for data encryption
- **Direct TN3270 Support for SSL Clients**
  - Host on Demand , PComm
- **Allows Multiple TN3270 Ports per Server**
  - 255 max
  - Basic Ports
  - SSL-Only




IBM Technical Support



- This discussion will concentrate on the use of SSL within TN3270.
- In O/S390 V2R6 server side authentication was introduced in TELNET. This provided a secure TN3270 data exchange. The SSL support used within TN3270 uses X.509 certificates. The big advantage of the introduction of SSL is that the session now has encrypted data. Thus userid and password no longer flow in clear text over the network link. When using an unsecured link there is a need to encrypt data.
- Additionally the client application can verify that the connection has been setup with a legitimate server, since the server's certificate must be authenticated by the client, or the session will be terminated.
- DES and Triple DES are supported for data encryption.
- Currently Host on Demand and PComm are the 2 applications exploit server side authentication using SSL.
- TN3270 currently has the following limitations:
- 255 maximum ports and a port must be configured as SSL-only, SSL and non-SSL communication is not allowed over the same port at the same time.

## TELNET Parameters for SSL (V2.6)

### TCPIP Profile Enhancements :

```
TELNETPARMS
    SECUREPORT  2323 KEYRING  HFS /u/graaff/telnet.kdb
    ENCRYPT  SSL_DES_SHA  ENDENCRYPT
    SSLTIMEOUT  30  (time-out in seconds)
ENDTELNETPARMS


TELNETPARMS
    SECUREPORT  2323 KEYRING  MVS  graaff.telnet.kdb
    ENCRYPT  SSL_DES_SHA  ENDENCRYPT
    SSLTIMEOUT  30  (time-out in seconds)
ENDTELNETPARMS
```

IBM Technical Support



- This foil shows the parameters placed in the TCPIP profile definition. These enhancements enable the use of server side SSL authentication.
- In the first example port 2323 has been defined as a secure port and the KEYRING containing valid keys and certificates are located in an HFS file /u/graaff/telnet.kdb. This port will accept DES encryption across it's SSL link and the SSL session will wait a maximum of 30 seconds during the SSL handshake prior to breaking its communication link.
- The difference in the second TELNET parms is the use of an MVS file for the KEYRING rather than an HFS file.

## Supported Encryption Algorithms

| SSL V3 Cipher Suite | HTCP350 (base) | JTCP35T (RC2/4) | JTCP35L (DES) | JTCP35K (TDES) |
|---|---|---|---|---|
| SSL_NULL-Null | Y | Y | Y | Y |
| SSL_NULL_MD5 | Y | Y | Y | Y |
| SSL_NULL_SHA | Y | Y | Y | Y |
| SSL_RC4_MD5_EX | | Y | Y | Y |
| SSL_RC4_MD5 | | | | Y |
| SSL_RC4_SHA | | | | Y |
| SSL_RC2_MD5_EX | | Y | Y | Y |
| SSL_DES_SHA | | | Y | Y |
| SSL_3DES_SHA * | | | | Y |

IBM Technical Support



- Documentation APAR II11402 documents the encryption parameter and the supported encryption algorithms as shown in this table.
- * TDES only supported in Software !

## Key Management TELNET SSL (V2.6)

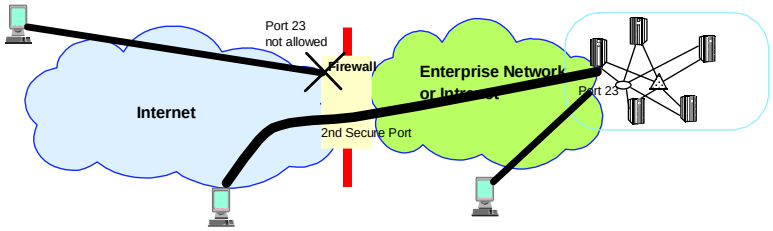
- Key Management functions performed by a utility called MKKF
  - Create KEYRING File
    - Loaded with Well known Certificate Authorities (e.g. Verisign)
  - Create Self Signed Certificate
  - Import Certificate Request signed by external Certificate Authority

IBM Technical Support



- In OS/390 V2.6 the key management functions are performed by a utility called MKKF. The MKKF utility can perform the following management functions against a KEYRING.
- 
- It can create a key ring - please note the OS/390 V2.6 is shipped with a default key ring which is already primed with known Certificate Authorities.
- 
- MKKF can create a self signed Certificate
- AND
- MKKF and import a certificate request signed by an external Certificate Authority.

## Separate Port For Secure Internet Access




One possible configuration using separate ports...

- SSL TN3270 negotiations are always initiated over a specified secure port
  - Can be a separate port
- Configuration flexibility
  - Can filter all non-SSL traffic at Firewall based on port
  - Firewall allows only SSL TN3270 traffic access based on secure port
  - Access to non-SSL port from intranet only

IBM Technical Support

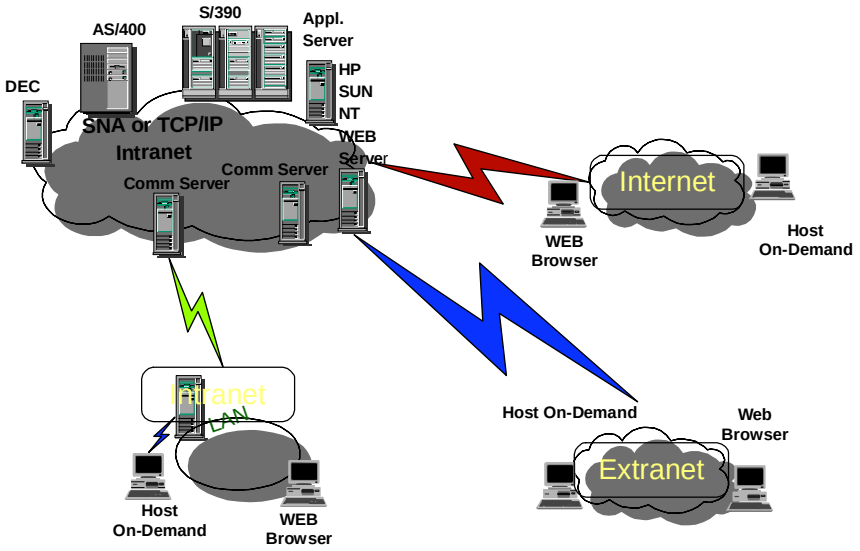


- This diagram shows one possible configure to allow for secure internet access via TN3270. In this example the '2nd Secure Port' is defined as a SECUREPORT using server side authentication SSL. Therefore any traffic coming from the internet must be using SSL or it will be rejected. However any TN3270 traffic on the INTRAnet may use the unsecured port 23.
- 
- This configuration ensures that access from the internet will be done over SSL lines only, thus traffic over the line will be encrypted.

# Host on Demand

## What is Host On-Demand ?

**A Java-based applet for browser access to 3270, 5250, VT100 and VT220 hosts.**




IBM Technical Support



- The official 25 work description
-
- IBM(R) eNetwork Host On-Demand Version 2 puts all your mission-critical data one click away from a standard browser. No installation or configuration required! No disk storage for application code! What could be simpler?
-

## Key Features of Host On-Demand

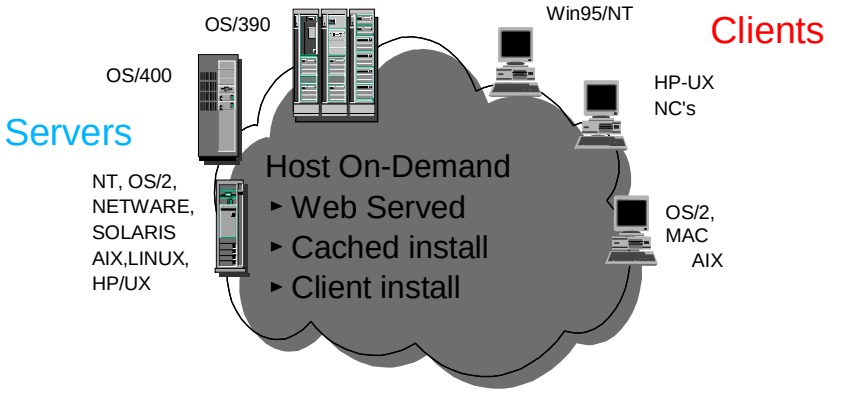
- Flexible client and server configurations
- Java based browser interface
- TN3270E support
- Full industry standard TNxxxx gateway support
- Secure enterprise data access
- Host Access Class Library
- TN5250 and VT52/100/220
- Web-based server configuration and administration

IBM Technical Support



- Server: 390,AS400,....
-
- TN370E =
  - Right Now - LU Pooling, Special Key support
    - in V3 - Host Print

## Flexible server and client configurations




IBM Technical Support

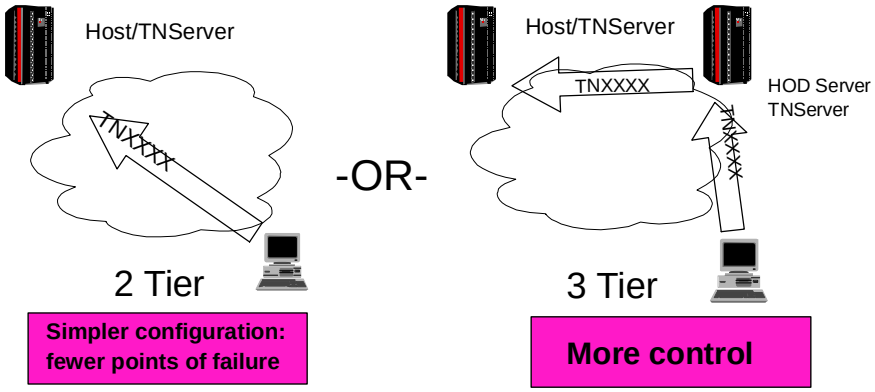


- HOD allows for a variety of server and client platforms. The supported server platforms are NT, OS/2, NETWARE, Solaris, AIX, LINUX, HP/UX, OS/400 and of course the best server platform the OS/390.
-
- Client platforms are WIN95, WINNT, HP/UX, OS/2, MAC and AIX

## Flexible Achitecture

Full support for standard TNXXXX protocol

- ➡ Delivers ability to communicate directly with any TN Server
  - TNXXXX protocol fully implemented at client
  - flexibility to use 2 or 3 tier network configuration




IBM Technical Support



- Reasons for using a 3 (or more) tier configuration
  - 1) Offload TN processing from Host
  - 2) Interface to a SNA backbone (rather than multi protocol)
  - 3) Firewall penetration
  - 4) Management of all functions combined in one box
  - 5) Load balancing, redundancy

## Host On-Demand security

- Server identification and Client authorization
  - Web Server access
    - Supports any password/security employed by your Web Server
  - HOD Server access
    - HOD Login ID and Password to gain access to a profile
  - Server authentication
    - Server authentication (Server sends x.509 certificates)
- Transport
  - SSL V3
    - Encryption support for the Encryption Algorithms mentioned earlier
    - Session data encrypted back to Secure HOD Server
  - Support for Firewall tunneling
- Host based security
  - Support for RACF, TopSecret or any host based security

IBM Technical Support



- Client/Server identification
- 1,2 - controls access to client software(ID and PW may not be encrypted)
- 3 - verifies to the client that the server is who it says he is. Most important if HOD is installed on the client. Requires the use of Certificates
- **Note - with HOD V3 and OS/390 V2.6 Client side authentication is not supported in other words the server does not verify who the client is - we leave this to the Host application - same as OCS.
- Transport
- Industry standard SSL V3.
- Firewalls are not a problem
- Host based Security
- support for any host based security mechanisms
-

## Server

- Host On-Demand server
  - Emulator configuration
    - Default sessions
  - User management
    - User IDs, passwords
  - Redirector
    - Lets clients connect to any Telnet server/host system with any browser
    - Supports SSL security - on Win32 and AIX
  - Express server
    - Provides compression (with Express Client)
  - Publications
    - Administrator's Guide, Helps, README
  - Host Access Class Library - Java API
- *Must* reside in the same machine as a web server
- *Can* co-reside with a communications server

IBM Technical Support



- The HOD server provides the following flexible functions. The ability to configure the emulator sessions the client will be using - and provide the client with a set of pre-configured default sessions.
- The server can control access to the specified pre-configured sessions via userids and passwords which are managed from the server HOD application.
- The use of the HOD Redirector allows clients to connect to any Telnet server/host system with any browser and it supports SSL security for WIN32 and AIX client platforms.
- By using Express server in conjunction with Express Client the ability to compress the JAVA applet is introduced.
-
- There are some minimum requirements. The HOD server must reside on the same machine as a web server, it *can* be on the same machine as a communications server, but this is not required.

## Clients

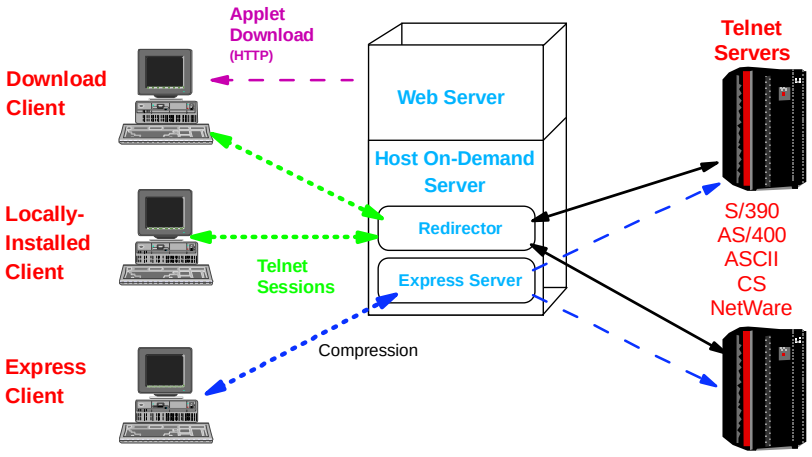
- Cached client (HODLocal.htm)
  - Downloaded from a server the first time
  - Cached on client workstation, loaded locally thereafter
  - Checks for updated version at each load
  - Strict browser requirements
- Downloaded client (HOD.htm)
  - From the server, every time
  - Needs only a browser - no code installed
- Locally-installed client
  - For remote sites, probably dial-in
  - Express provides compression = performance
  - Windows 95 & NT, AIX, HP UX

IBM Technical Support



- The HOD client can be run in 3 different configurations. It can be run as a cached client, a downloaded client or a locally installed client. You need to determine the best configuration for your installations requirements.
- 
- A cached client is downloaded from a server the first time it is used - from that point on the client is loaded locally from cache. The client checks for updated versions each time it loads.
- 
- A downloaded client is downloaded from the server every time. This is probably best done for LAN connected clients. The advantage is that there is no code installed on the client and the client only needs a web browser.
- 
- A locally installed client is a good option for remote or dial-in sites. The client is installed on the workstation so there is never a need to load the client code from a server. Using the Express Client further improves performance by using compression. The client platforms supported for a locally installed client are WIN95, WINNT, AIX and HP/UX.

## How It Works



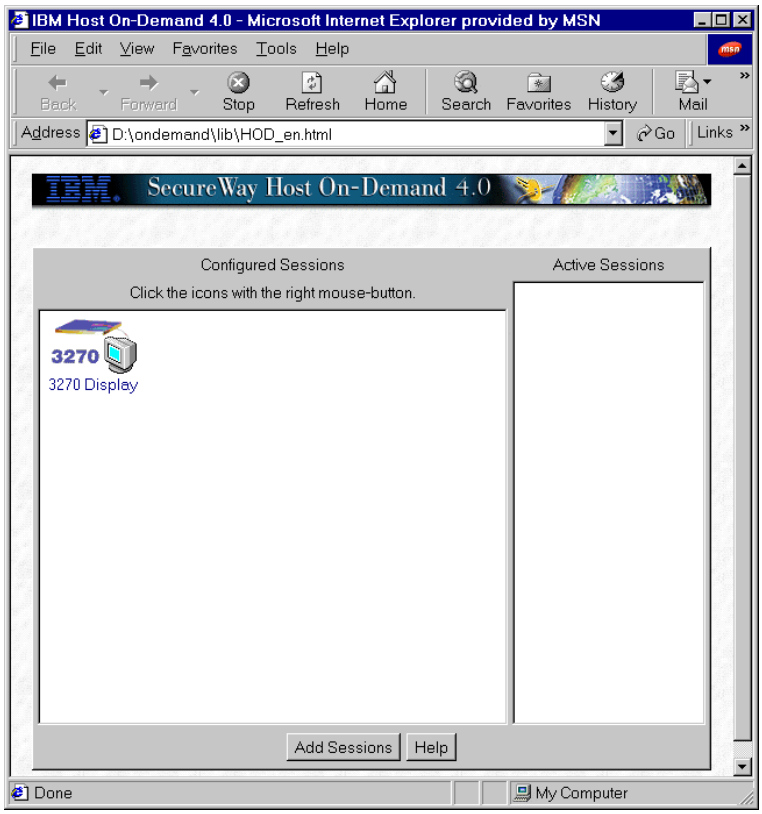

Clients (except Express) can connect directly to Telnet servers if they use a browser that has signed-applet support.

SSL Optional

IBM Technical Support

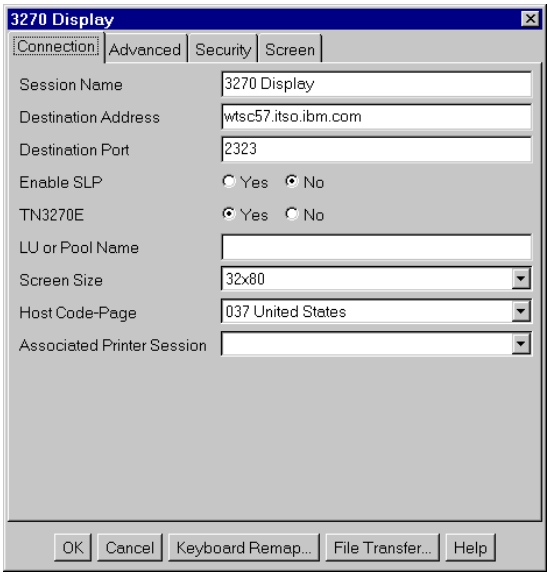


- If a client is using a browser which has signed-applet support, the client can connect directly to a Telnet server. (The exception to this is a client running Client Express).
- 
- As shown in this digram and already previously mentioned the Host On-Demand Server must run on the same machine as a Web Server.




- This foil shows a V4.0 Host On-Demand window.  Notice there is one pre-configured session defined and there are currently no active sessions.
- 
- By double clicking on the pre-configured session, the session will automatically 'start-up' and begin the process of negotiating a TN3270 session.

## HOD V4 Configuration




Connection Tab specifies :

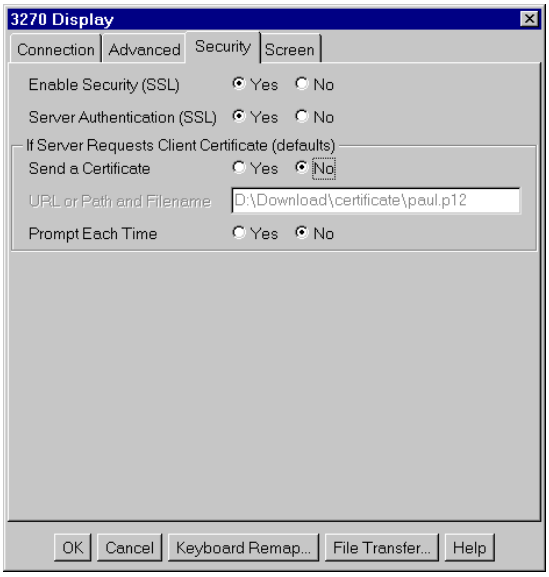
- Destination Address
- Destination Port
- LU name or Pool
- Screen Size





- This foil shows a Host On-Demand configuration window. Specifically the options available under the 'Connection Tab'.
- In this foil the name of the session will be 3270 Display, this corresponds to the name shown in the blue bar across the top of the window.
- The destination address is wtsc57.itso.ibm.com. That destination has a Host On Demand server and a Web Server up and running.
- The destination port is 2323. On an OS/390 platform this is the port specified in the profile definition for the TCPIP started task.
- This configuration will not be using SLP, and is defined as a TN3270E session.
- Since the LU/Pool Name has been left blank this session will be assigned the first available LU as defined in the TCPIP VTAMBEGIN parameters within the TCPIP profile definition.
- This session will have a 32x80 screen and will use USA English and has no associated printer.

## HOD V4 Configuration




Security Tab specifies :

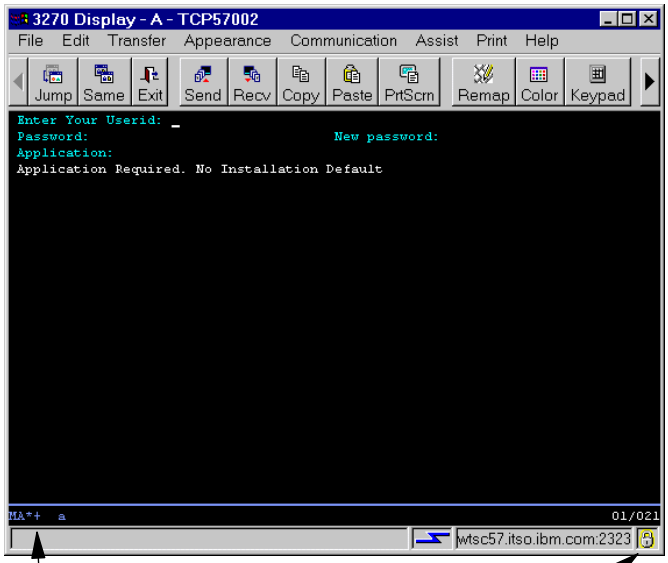
- SSL Enablement
- SSL Server Authentication
- SSL Client Authentication (discussed later)

IBM Technical Support



- This foil shows a Host On-Demand V4 configuration window specifically using the Security tab.
- 
- This session has enabled SSL Security and will be using server side authentication only. This session will not be using client authentication. This will be discussed later in this presentation during the OS/390 R2.8 features section.

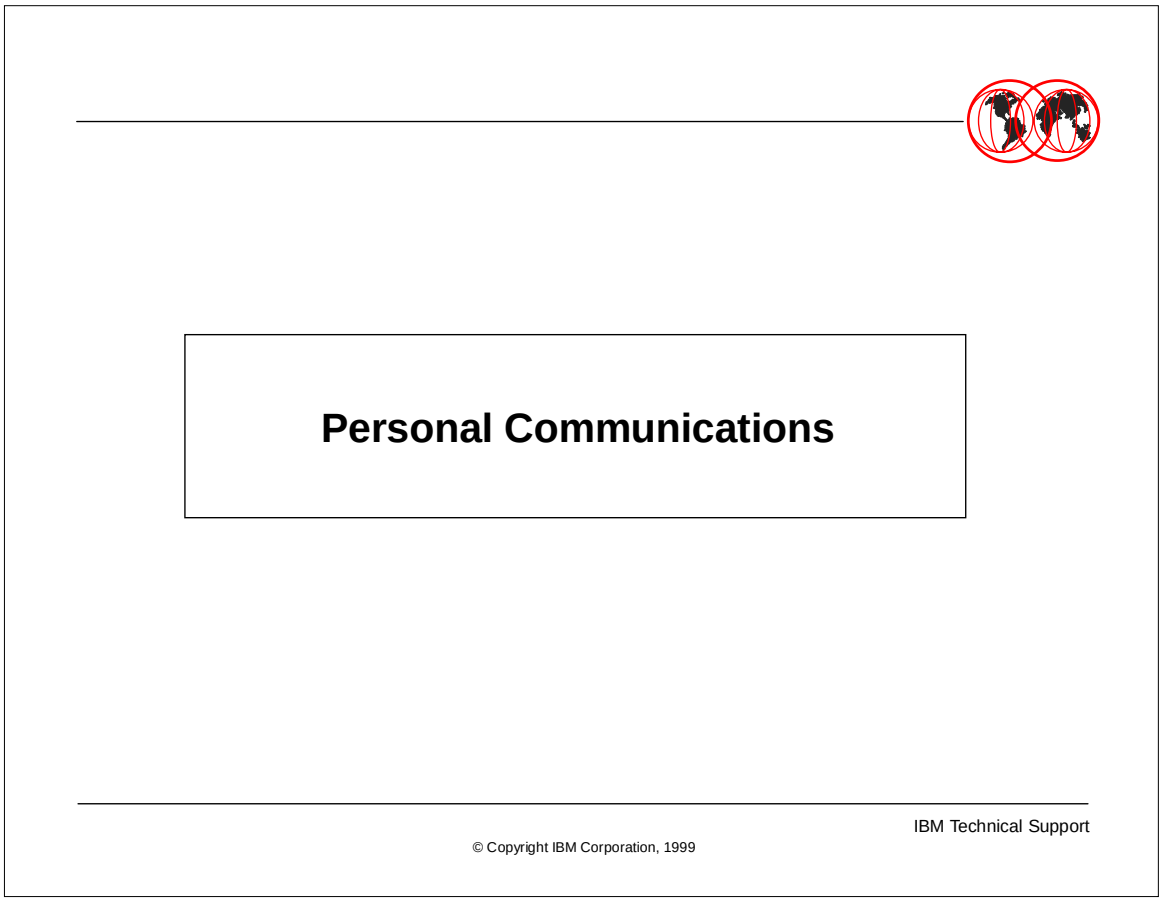
## 3270 Session Window Example




IBM Technical Support

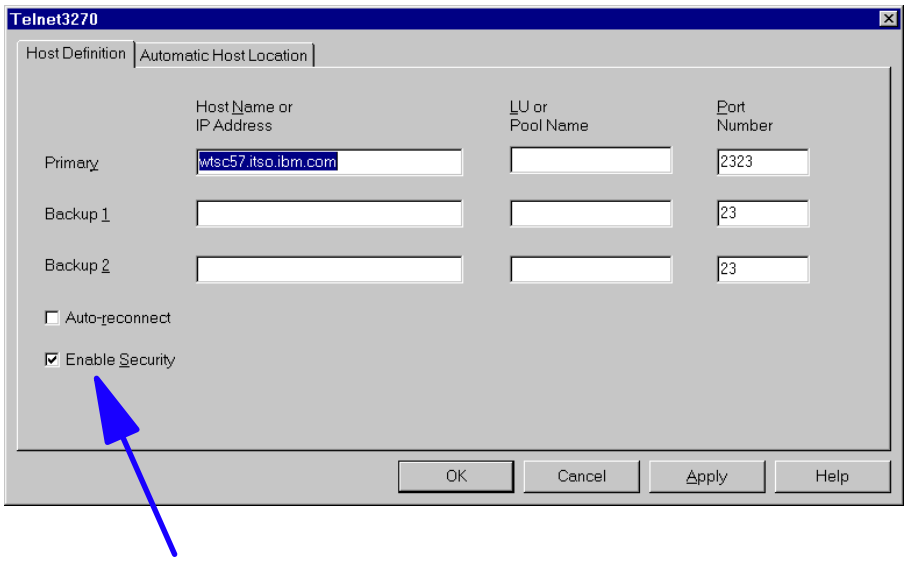


- This foil shows an active TN3270 session using the configuration set up from the previous foils.
- 
- Across the top blue bar you can see that this is the session called '3270 Display' and the 'A' indicates this is the first session started from this client. The LU name assigned from the TELNET host (since we did not request an explicit LU or pool) is TCP57002.
- 
- Across the bottom of the screen the + and the closed lock indicate this is a secured SSL connection. The lightning bolt indicates that this is an active session.




- The second exploiter of TELNET server side SSL authentication is PCOMM. You must be at PCOMM V4.3 to use SSL server side authentication.

## SSL Support in Personal Communications

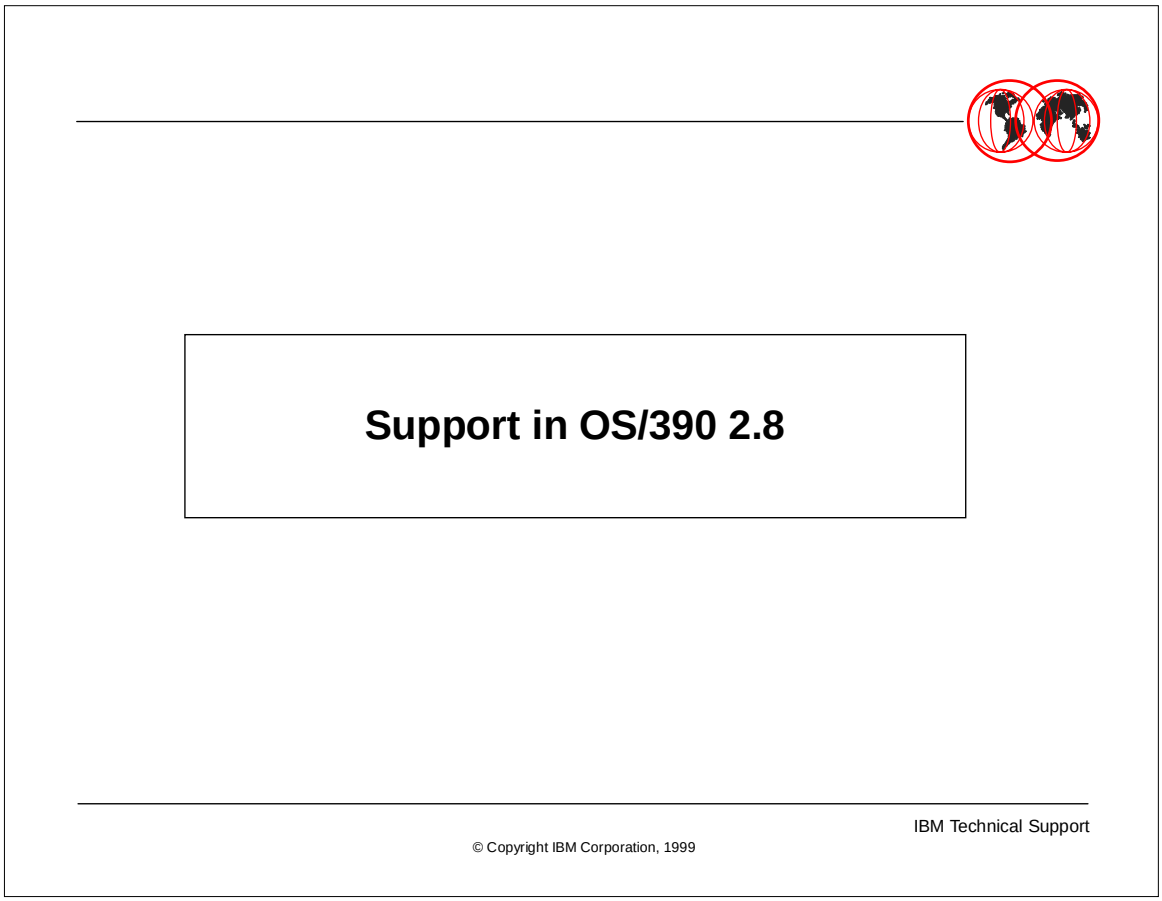



Note: SSL Support is in Personal Communications 4.3

IBM Technical Support



- Notice that we are again using port number 2323 for this example, and that the host name is wtsc57.itso.ibm.com
-
- However, the trickiest part of this setup is that SSL is not mentioned anywhere on this configuration panel. To enable SSL support for this PCOMM TN3270 session, click on the box called 'Enable Security'

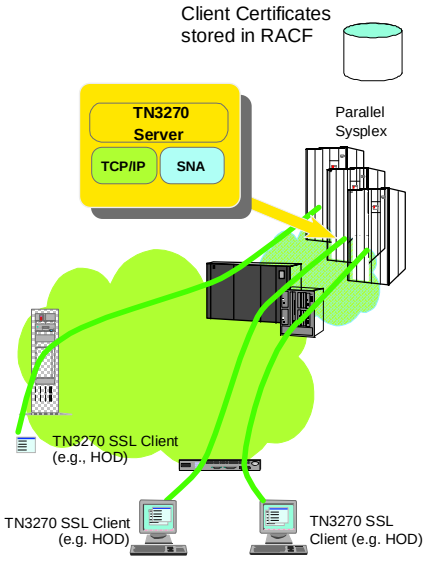



- Now we will concentrate our discussion on the features made available OS/390 2.8

# TN3270 SSL Client Authentication (V2R8)

- **Protects SNA and S/390 resources using digital certificate technology**
  - Tightens security for TN3270 access to corporate intranet
    - Client credentials are validated before USSMSG (logon screen) is sent
- **Security Levels Provided**
  - SSL Client Authentication
    - Provides authentication of client side certificates
  - Pre-login access control using RACF digital certificate support
    - Client certificate stored in RACF
    - New RACF Class for TN3270 access - SERVAUTH

      <Certificate mapped to RACF userid and userid must be permitted to use SERVAUTH TN3270 resource>
- **Client support in release 4 of Host on-Demand and Future release of PComm**




IBM Technical Support



- This diagram shows the new level of security available for client side SSL authentication. Additionally since the client has been authenticated with a valid Certificate we are now able to restrict access to certain TELNET ports.
- 
- The client support in Host On-Demand is available in HOD release 4, and will be exploited in a future release of PCOMM.
- 
- The Client's Certificate is stored in a Keyring defined to the Host On-Demand client. This Certificate is passed on to the HOD server and must be signed by a trusted CA, otherwise the SSL handshake does not complete and the connection is broken.
- 
- Additionally you can specify that the Certifcate must be already associated with a RACF USERID and that the port is a valid port for this RACF USERID to use. The PORT authentication is done by using the SERVAUTH class within the RACF database.

## TELNET Parameters for SSL (V2.8)

- New parameters in 2.8
  - CLIENTAUTH in support of SSL Client Authentication
    - NONE - No Client Authentication
    - SSLCERT - Verifies client has a certificate from a trusted Certificate Authority
    - SAFCERT - Verifies client certificate has an associated RACF userid before presenting the Telnet USSMSG screen.

      A additional Security Check is performed against a profile in the RACF CLASS SERVAUTH, to check if the associated RACF userid is authorized to open the port :

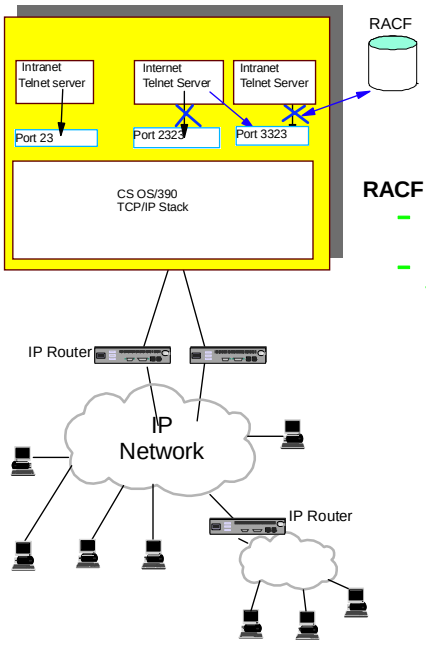
      EZB.TN3270.sysname.tcpname.PORTnnnnn

IBM Technical Support



- With OS/390 2.8 Telnet supports SSL V3 Client Authentication.
- There are two ways of requiring a client certificate :
  - SSLCERT - any valid client certificate is accepted without further checks performed
  - SAFCERT - the client certificate has to be mapped to a RACF userid (mapping profile added through RACDCERT or Self Registration in the DIGTCERT class) to receive the Telnet USSMSG screen and the RACF userid need to be authorized to a profile in the new SERVAUTH class to protect an unauthorized user from opening a Telnet port.
  - Profile example : EZB.TN3270.MVS.ITCPIP.PORT02323

## RACF Telnet Port Access Control




**RACF Telnet Port Controls**

- **user access to a Telnet port**
- **is considered a resource in the RACF SERVAUTH class**

IBM Technical Support



- This foil shows how the client authentication flow works. In this example the port used for Internet access has been defined as a SECURE port (2323) and is using the SERVAUTH. Therefore for the SSL handshake to be successful the HOD client must provide a valid certificate and the certificate must be associated with a valid RACF userid and the RACF userid must have access to the SERVAUTH facility for port 2323. To state another way the following must all be true:
- 1) Valid certificate signed by a trusted certificate authority
- 2) Valid certificate associated with a RACF userid
- 3) RACF userid must have access to the SERVAUTH profile EZB.TN3270.MVS.ITCPIP.PORT02323
-
- However if a Telnet user is behind the firewall, they can connect to unsecured port23, therefore they do not need to establish an SSL handshake and incur the overhead of encrypting all the traffic going over the IP connection.
-

## Supported Encryption Algorithms

| SSL V3 Cipher Suite | HCPT270 (base security) | JCPT27X (LEVEL1) | JCPT283 (LEVEL 2) | JCPT271 (LEVEL 3) |
|---|---|---|---|---|
| SSL_NULL-Null | Y | Y | Y | Y |
| SSL_NULL_MD5 | Y | Y | Y | Y |
| SSL_NULL_SHA | Y | Y | Y | Y |
| SSL_RC4_MD5_EX | | Y | Y | Y |
| SSL_RC4_MD5 | | | | Y |
| SSL_RC4_SHA | | | | Y |
| SSL_RC2_MD5_EX | | Y | Y | Y |
| SSL_DES_SHA | | | Y | Y |
| SSL_3DES_SHA | | | | Y |

IBM Technical Support



- Documentation APAR II11402 documents the encryption parameter and the supported encryption algorithms as shown in this table
- 
- For export version of HOD the highest level of encryption used is the SSL_RC4_MD5_EX. Therefore if you would only allow SSL_3DES_SHA encryption (triple DES) - those clients

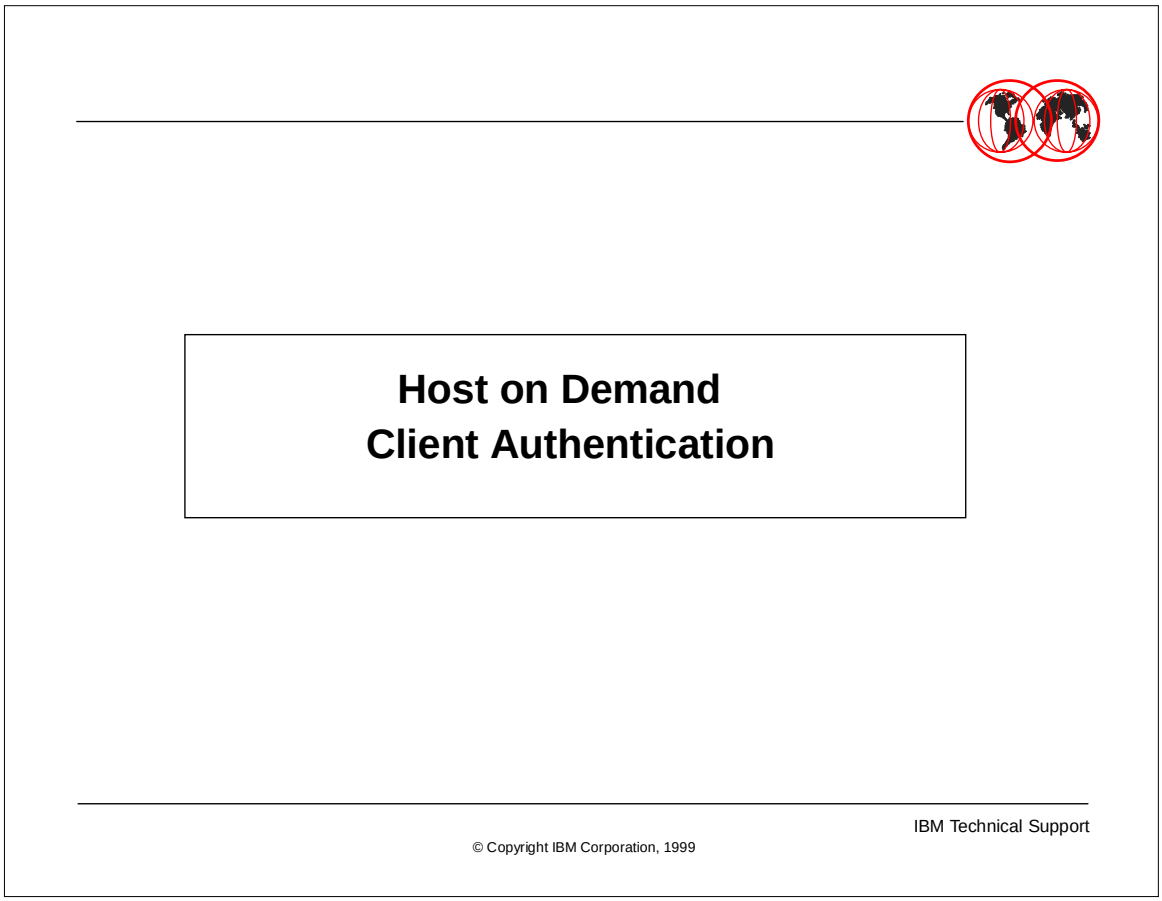
## Key Management TELNET SSL (V2.8)

- TN3270 Server utilizes System SSL in 2.8
- Key Management done through utility GSKKYMAN
  - Create/Migrate Keyring File
    - Loaded with Well known Certificate Authorities (e.g. Verisign)
  - Create Self Signed Certificate
  - Import Certificate Request signed by external Certificate Authority

IBM Technical Support

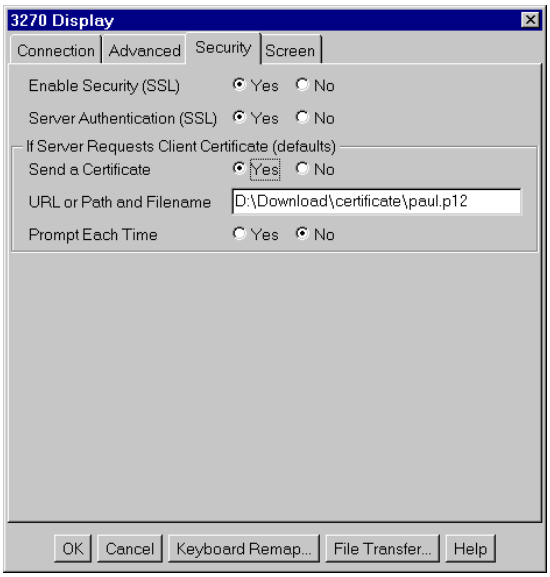


- In OS/390 V2.8 Telnet exploits System SSL. By using the TCPIP parms a Telnet secure port can be defined which points to a system managed keyring.
- The Keyring is managed through use of the GSKKYMAN utility. This utility is shipped with the OS/390 system and is run as a UNIX exec under the OS/390 UNIX shell. GSKKYMAN allows an installation to perform a number of management tasks against a Keyring. There is a 'pre-built' key-ring shipped with OS/390 which contains certificates from some Well known Certificate Authorities, such as Verisign.
- A couple of the functions provided through the use of GSKKYMAN are the ability to create a Self Signed Certificate and the ability to import Certificate Requests signed by an external Certificate Authority. These 2 functions are used extensively in setting up a 'valid' certificate for use by Telnet.
- The Self Signed Certificate is a useful tool for creating 'Test' certificates to test the SSL process. However, it is advisable to use an external Certificate Authority for use in a production SSL environment.




- This next section will walk through the panels and parameters needed to set-up Client Authentication for the Host On-Demand TN3270 application.
-
- This is for HOD V4.0.

## SSL Client Authentication - Configuration



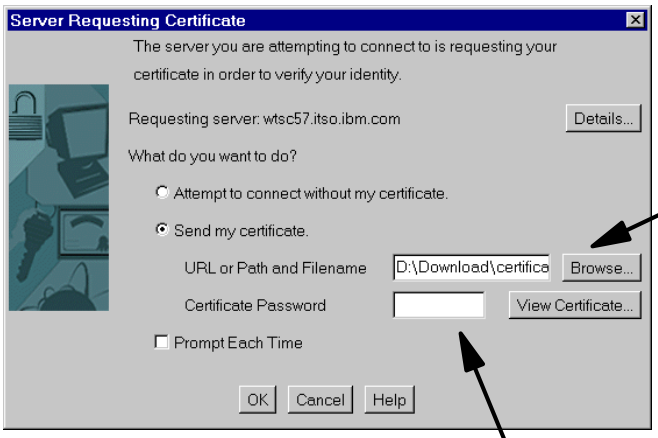

- New Security tab on Session configuration
- Identifies default location of client certificate
- Client may override on receipt of Server Requesting Certificate message

IBM Technical Support



- This security tab was shown earlier in this presentation during the Server Side SSL authentication. However note that the 'Yes' button for 'Send a Certificate' has been clicked. When this button is clicked you are also requested to enter a file name or a URL where your client certificate is located. This should point to a Key Ring which must contain a certificate which has been signed by a Trusted Certificate Authority.
- 
- Optionally you can request that a prompt is given for every time you request a connection to a SERVER.
- 
- Please note that HOD also has it's own Key Management set of GUI interfaces to allow you to import PKCS12 format keys into the keyring used here.

## SSL Client Authentication - Request




Client certificate stored in a file in a PKCS12 format

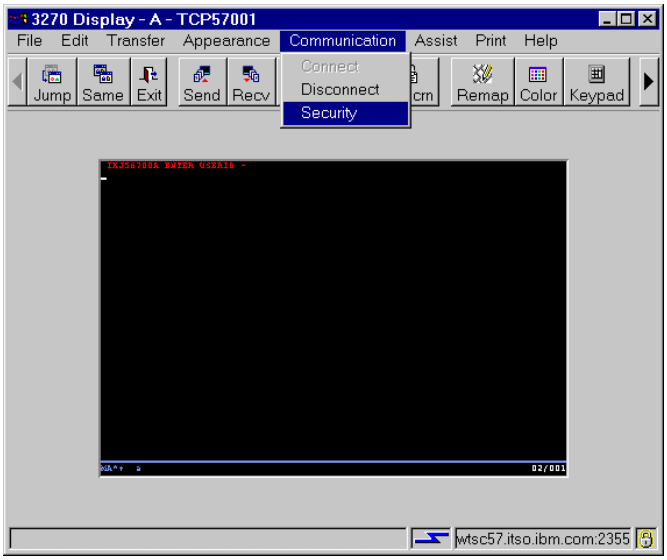
Password associated with the exported certificate

IBM Technical Support



- This screen is shown after you have requested to connect to the SERVER. You can change the file name where your keyring is located to something other than the default set up in the previous foil. Secondarily you need to enter the password associated with the PKCS12 certificate.
- 
- Note if you clicked the 'NO' button for the 'Prompt Each Time' shown on the previous foil - this panel will only show the first time you request a connection. All subsequent connect requests made while this window is open will not request you to enter a password. If you click the 'YES' button for the 'Prompt Each Time' you will need to enter your password for the PKCS12 key every time you connect.

## Security Item

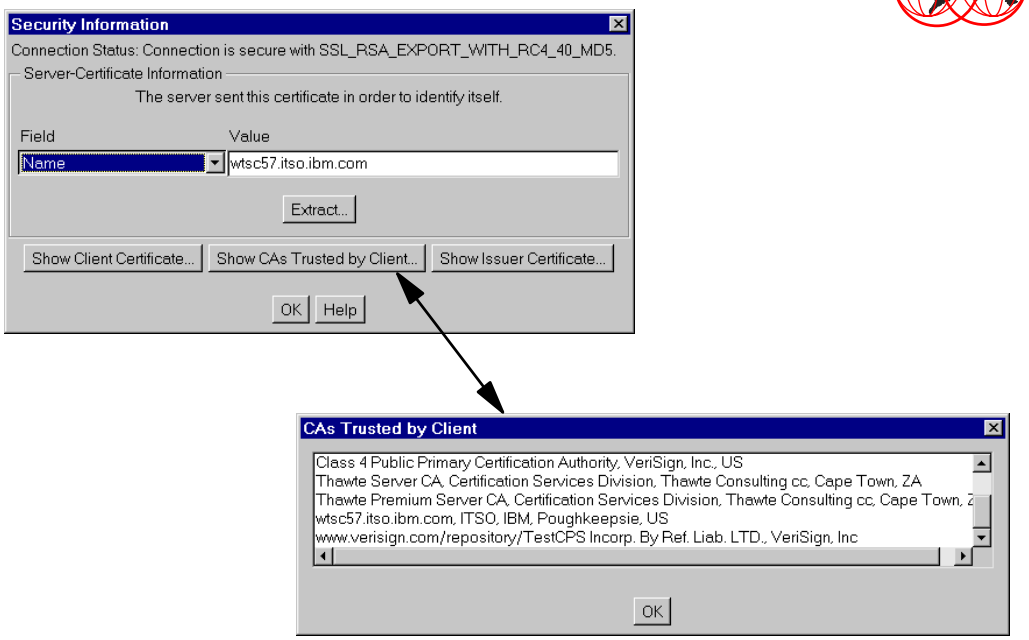



IBM Technical Support



- This is the screen which shows after you have requested a connection. At this point the SSL connection has been established. As noted earlier you can tell this is a secured SSL connection by the '+' in the lower left hand corner and the closed lock in the lower right hand corner.
- 
- Additionally we are going to look at what other security information is available to us on this TN3270 session.

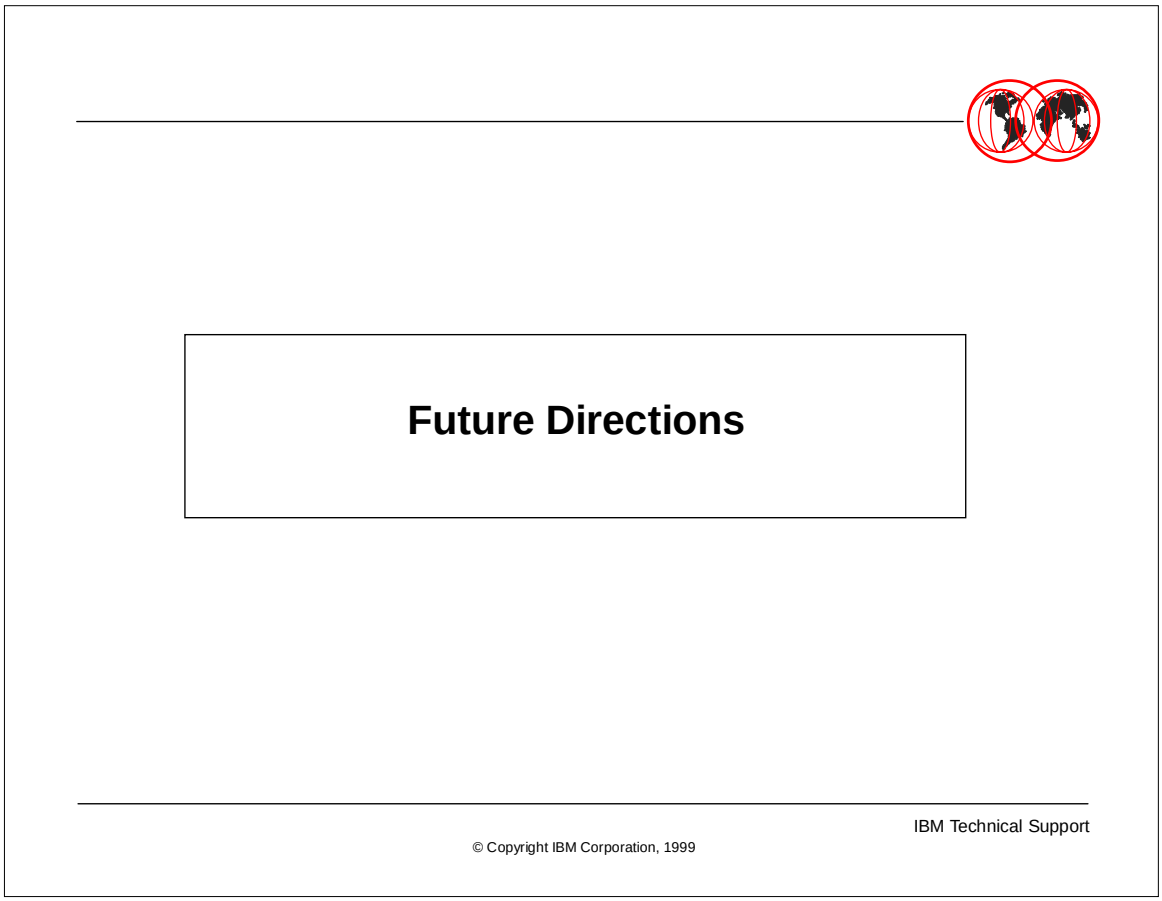
## Secure Connection - Security Window




IBM Technical Support



- This shows us the results of clicking on the security drop down tab.
-
- The Encryption information is shown across the top of the Security information box. The SSL session will attempt to establish the strongest encryption. In this case the encryption used for this SSL session is RC4 40 bit encryption.
-
- Further, by clicking on the button 'Show CAs Trusted by Client' we have a list of the Certificate Authorities which are trusted by this HOD client application. Therefore any server certificates which have been signed by these CAs will be considered valid certificates.




- Next we will touch on a few of the future enhancements expected in the TN3270 SSL area.

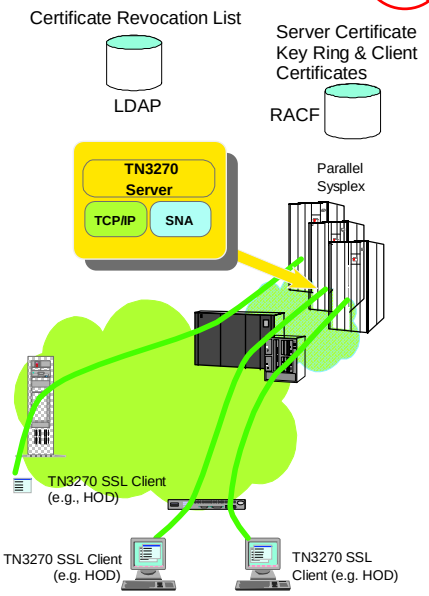
# TN3270 SSL Future Enhancements

**Access Server Certificate Key Ring stored in RACF**

- Currently kept in HFS
  - Allows both client and server certificates to be stored in RACF
- Use RACF Common Key Ring Support

**Certificate Revocation List Checking**

- CRL stored in LDAP
- Authenticated Client Certificate checked against CRL
  - If user on CRL, connection is broken

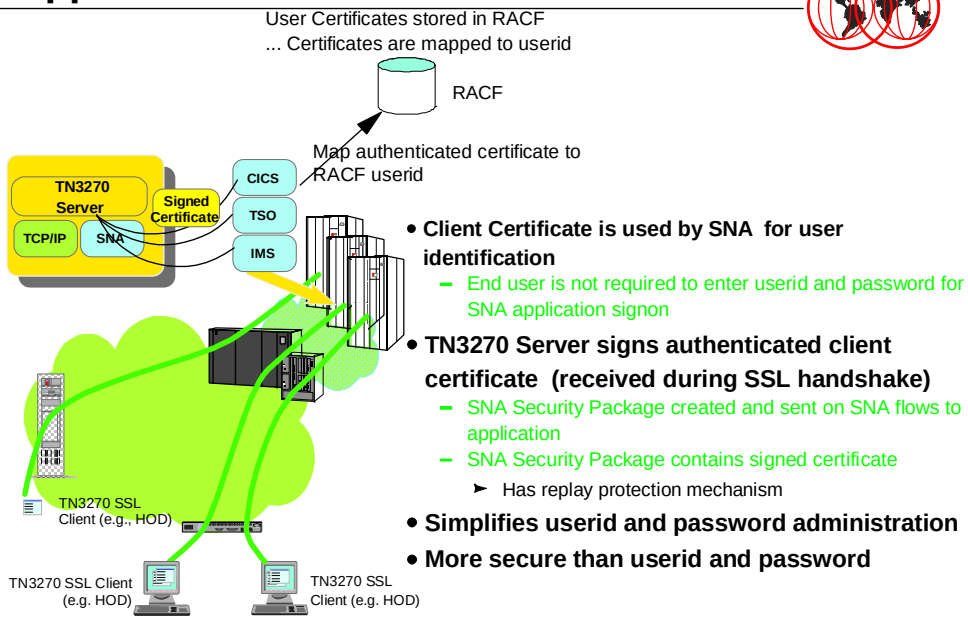



IBM Technical Support



- Currently the keyrings used by Telnet are kept in HFS files. These keyrings are easily maintain through the use of GSKKYMAN, but there is no correlation to the RACF database. You can expect to see TelNet using the RACF database as a repository for Keyrings. This will allow both the client and the server certificates to be stored in the RACF database.
- 
- Additionally there will be a Certificate Revocation list kept in LDAP. This will mean if a Certificate has been Revoked it will be considered an 'Invalid' certificate. Therefore no connections will be allowed for users on the 'revoked' list.

## SNA Application Use of Client Certificates



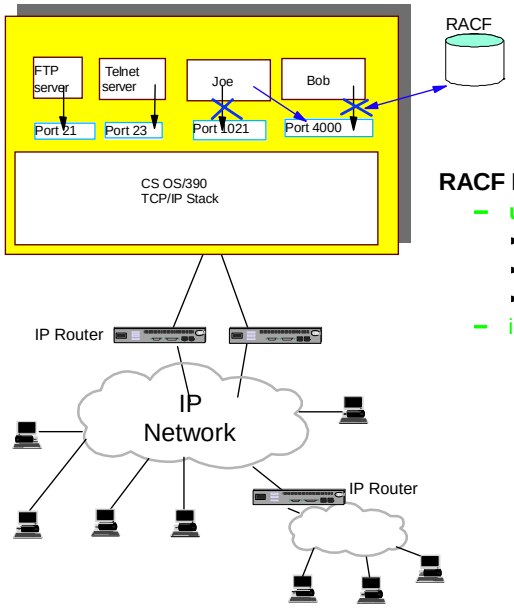

- **Client Certificate is used by SNA for user identification**
  - End user is not required to enter userid and password for SNA application signon
- **TN3270 Server signs authenticated client certificate (received during SSL handshake)**
  - SNA Security Package created and sent on SNA flows to application
  - SNA Security Package contains signed certificate
    - Has replay protection mechanism
- **Simplifies userid and password administration**
- **More secure than userid and password**

IBM Technical Support



- SNA application use of client certificates is an exciting new area. This will allow easy secured access to traditional SNA applications such as CICS, IMS and TSO. This mechanism will work by using the Client certificate to associated with a specific RACF USERID. Currently this is how access to a secured port is granted when the SAFCERT parameter is used on the CLIENTAUTH portion of the SECUREPORT TELNET.
- 
- Additionally the RACF ID which is associated with the Authenticated Client Certificate will be placed in the FMH5 security header on the SNA connection. Since this userid will be considered as having been authenticated there will be no need to 're-signon' to an SNA application. This means that once a Client has passed a valid certificate to Telnet, the person on the client TN3270 application will not need to signon explicitly to CICS, IMS or TSO. This will mitigate the need to reenter USERID and PASSWORD to signon to these SNA applications.

## RACF Local Port Access Control




**RACF Local Port Controls**

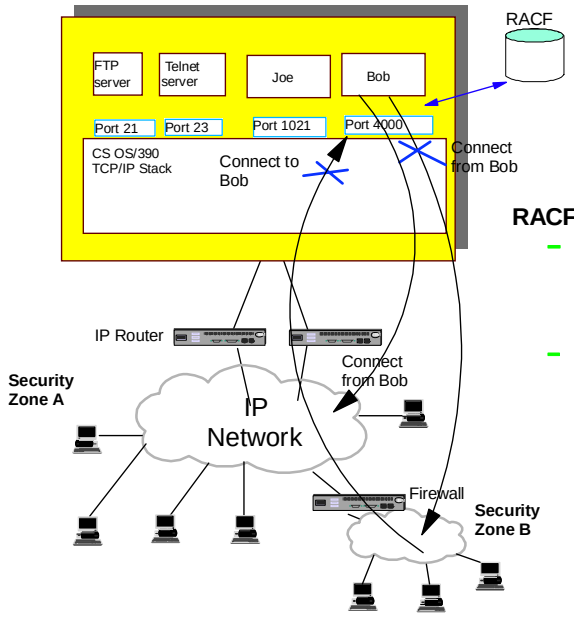
- **user access to a local port**
  - All ports
  - By port range (low / high)
  - Specific port
- is considered a resource

IBM Technical Support



- As in the last foil this is an exciting new area of security control. Coming soon will be the ability to control access to any TCPIP port, not just access to the Telnet ports. Being able to control points of access to the OS/390 TCP/IP is going to give a granularity and control which will be welcome.
- 
- Each port will be considered a resource and you will be able to grant individuals or groups access to each of these resources.
- 

## RACF Network Access Control




**RACF Network Access Controls**

- **local user access to network resources**
  - Network address
  - Specific host
- Network considered a resource

IBM Technical Support



- Another new area of security control will be the source or originating network.
- 
- The classic case is illustrated here where those users who are outside the firewall will be considered coming from an external network such as the internet and thus would only have access to certain TCP/IP ports, those inside the firewall could have access to certain other TCP/IP ports.
- 
- 