



IBM Systems and Technology Group

Using CMS-based SSL Support for z/VM TCP/IP

Brian W. Hugenbruch
IBM Corporation
Endicott, NY

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States, other countries, or both.

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*, AS/400®, e business (logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Disclaimer

The information contained in this document has not been submitted to any formal IBM test and is distributed on an "AS IS" basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used; any functionally equivalent program may be used instead.

Any performance data contained in this document was determined in a controlled environment and, therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environments.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM products, programming or services in your country.

Agenda

- About SSL for zVM
- Configuring Your SSL Server
- Gathering SSL Status
- Certificate Management
- The “How-To” Section
- References

About SSL for zVM

“What it is, what it does, where it’s going”

About SSL for zVM

- SSL was developed by Netscape to provide secure communications
 - ▶ Connection is trusted
 - Certificates authenticate identity
 - ▶ Connection is private
 - Cryptographic parameters established during handshake
 - ▶ Connection is reliable
 - *Message digest is sent with message*
- Standardized by RFC 2246 (Transport Layer Security - TLS)

About SSL for zVM

Supported Features

- Support for SSL 3.0, TLS 1.0
- Provides security functions for any server
- SSL for zVM TCP/IP clients
- Client authentication
- Certificate database management

About SSL for zVM

What's Not Supported

- Some forms of hardware encryption
- IPv6 Support

New for zVM 5.4.0.

- **SSL Server operating in a CMS environment**
 - No need for Linux distributions
 - GSKKMAN for standardized certificate management
 - Certificate database maintained in a BFS
 - New cipher suites for stronger encryption
 - Removal of FIPS 140-2 Support

- **Support provided by** PTFs for APARs PK65850, PK73085, PK75268, VM64540, VM64519, and VM64570.

Configuring Your SSL Server

For specific steps for server configuration, see:
zVM TCPIP Planning and Customization 5.4.0, Chapter 22

*zVM TCPIP LDAP Administration Guide,
Chapter 15*

Configuring Your SSL Server

1. Configure PROFILE TCPIP

- XAUTOLOG statement
- **SSLSERVERID** *userid* **TIMEOUT** *seconds*

*No need for Admin Port 9999 in zVM 5.4

Configuring Your SSL Server

2. Configure DTCPARMS – new tags

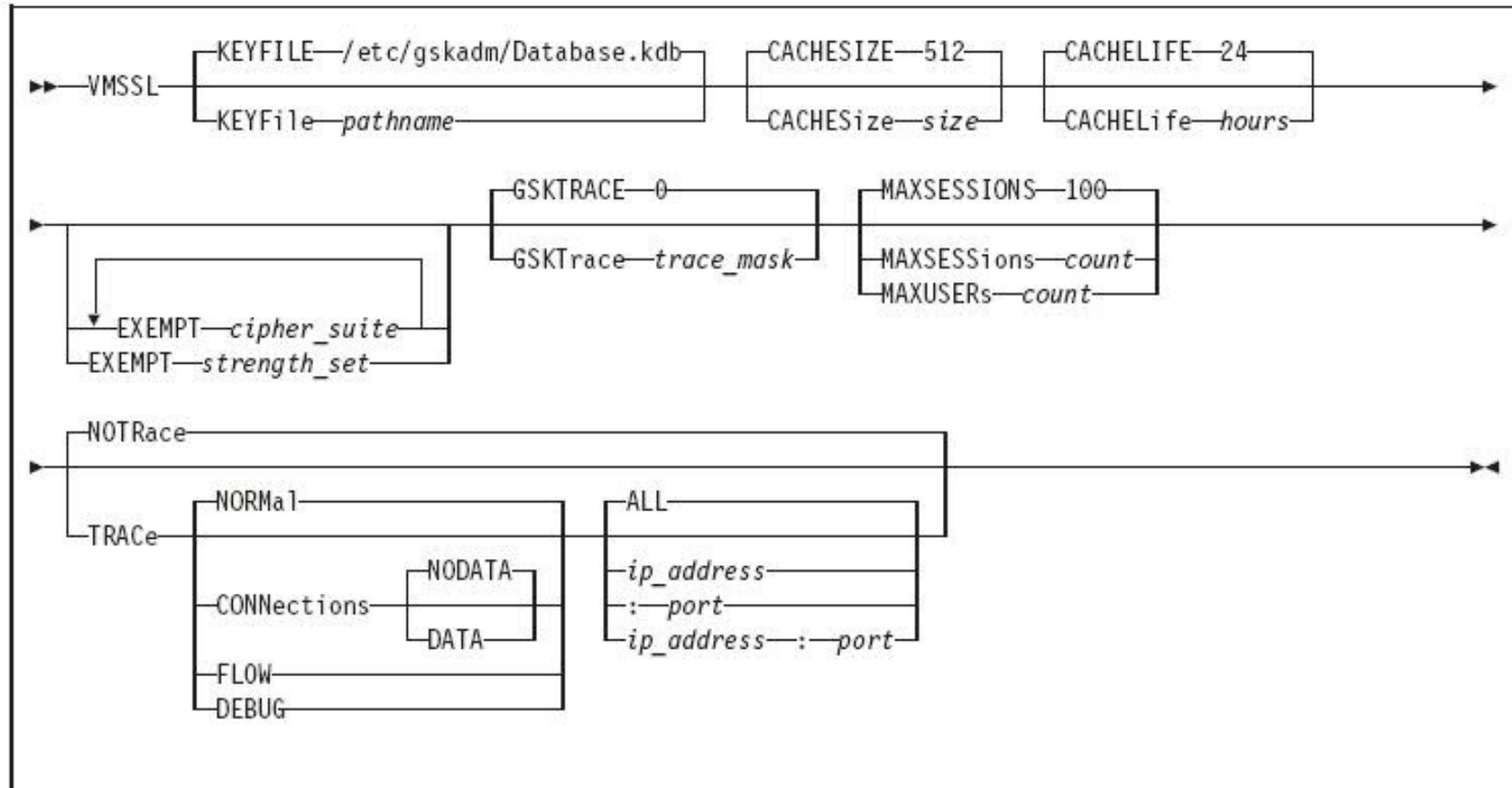
- **:Admin_ID_List.** – indicates which privileged users may use SSLADMIN for administrative commands
- **:Timezone.**
- **:Mount.** – the location of the certificate database in your BFS environment
 - Default is /etc/gskadm/

3. Set up Certificate Database – more on this to follow

4. Start the SSL Server with the VMSSL command

- In DTCPARMS or on the command line

Configuring Your SSL Server



Configuring Your SSL Server

High	Medium	Low	None
3DES_168_SHA	RC4_128_SHA	RC2_40_MD5	NULL
DH_DSS_3DES	RC4_128_MD5	RC4_40_MD5	NULL_SHA
DH_RSA_3DES	RSA_AES_128	DES_56_SHA	NULL_MD5
DHE_DSS_3DES	DH_DSS_AES_128	DH_DSS_DES	
DHE_RSA_3DES	DH_RSA_AES_128	DH_RSA_DES	
RSA_AES_256	DHE_DSS_AES_128	DHE_DSS_DES	
DH_DSS_AES_256	DHE_RSA_AES_128	DHE_RSA_DES	
DH_RSA_AES_256			
DHE_DSS_AES_256			
DHE_RSA_AES_256			

Note 1: Cipher suites can be exempted from processing based on either cipher name or by cipher strength, per below – but not both.

Note 2: Exempting by strength automatically exempts a lower strength!

Configuring Your SSL Server

```
netstat allconn
VM TCP/IP Netstat Level 540      TCP/IP Server Name: TCPIP10

Active IPv4 Transmission Blocks:

User Id  Conn   Local Socket           Foreign Socket          State
-----  ---   -
FTPSRV10 1006   *..FTP-C               *..*                   Listen
SMTP10   1005   *..SMTP                *..*                   Listen
SMTP10   UDP    *..1024                *..*                   UDP
INTCLIEN 1003   *..TELNET              *..*                   Listen
INTCLIEN 1004   *..1123                *..*                   Listen
SSLSRV10 1000   127.0.0.1..1024       *..*                   Listen
SSLSRV10 1001   127.0.0.1..1024       127.0.0.1..1025       Established
SSLSRV10 1002   *..1026                *..*                   Listen

Active IPv6 Transmission Blocks: None

Ready; T=0.01/0.01 03:07:18
```

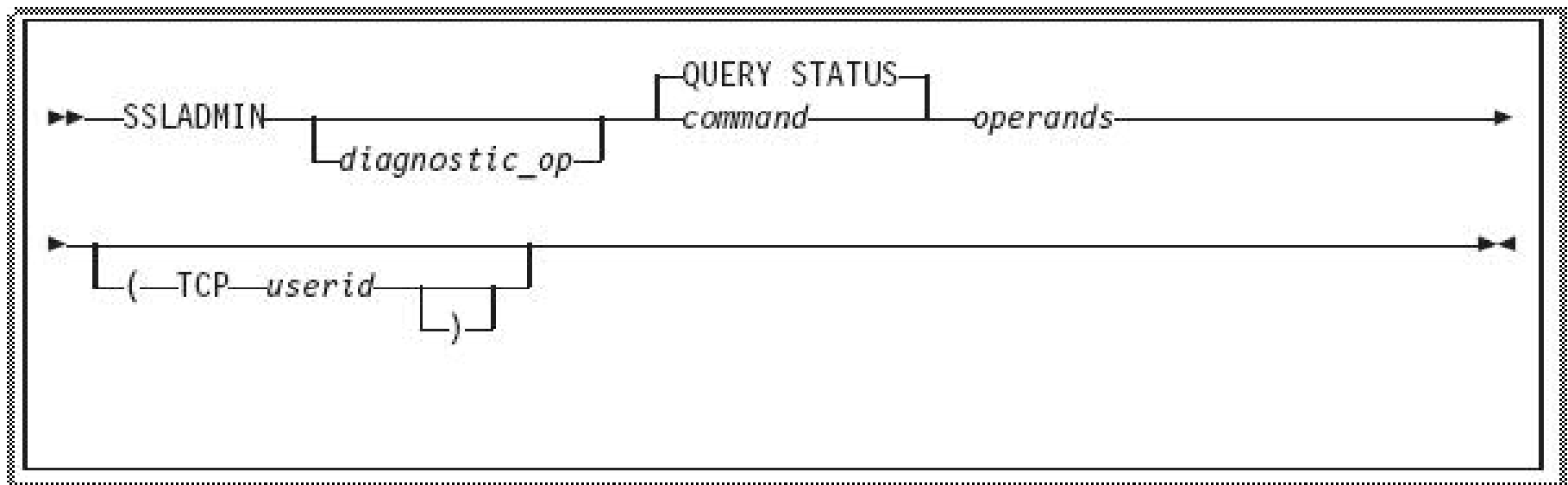
Note: Three connections should appear at SSLSERV start-up, to indicate communication with the TCPIP stack.

Gathering SSL Status

“It’s up and running; now what?”

Gathering SSL Status

SSLADMIN command



- Privileged command (:Admin_ID_list.)
- Reports information on SSL server status and connections
- Used to enable tracing and retrieve log files

Gathering SSL Status

SSLADMIN QUERY STATUS

```
ssladmin
DTCSSL2404I Sending command to server SSLSRV10
Maximum number of sessions: 100
Number of active sessions: 0
Cipher suites included :   RC4_128_SHA   RC4_128_MD5   3DES_168_SHA   RC2_128_MD5
RC4_40_MD5   RC2_40_MD5   NULL_SHA   NULL_MD5   NULL   DH_DSS_DES   DH_DSS_3DES   DH_RS
A_DES   DH_RSA_3DES   DHE_DSS_DES   DHE_RSA_DES   DHE_RSA_3DES   RSA_AES_128   DH_DSS_
AES_128   DH_RSA_AES_128   DHE_DSS_AES_128   RSA_AES_256   DH_DSS_AES_256   DH_RSA_AE
S_256   DHE_DSS_AES_256   DHE_RSA_AES_256
Cipher suites exempted :   DES_56_SHA   DHE_DSS_3DES   DHE_RSA_AES_128

Trace Settings:
  Normal: OFF
  Connections: OFF
  Flow: ON
  Address: 255.255.255.255:0
  Connection: 0

Ready; T=0.01/0.01 03:28:43
```

Gathering SSL Status

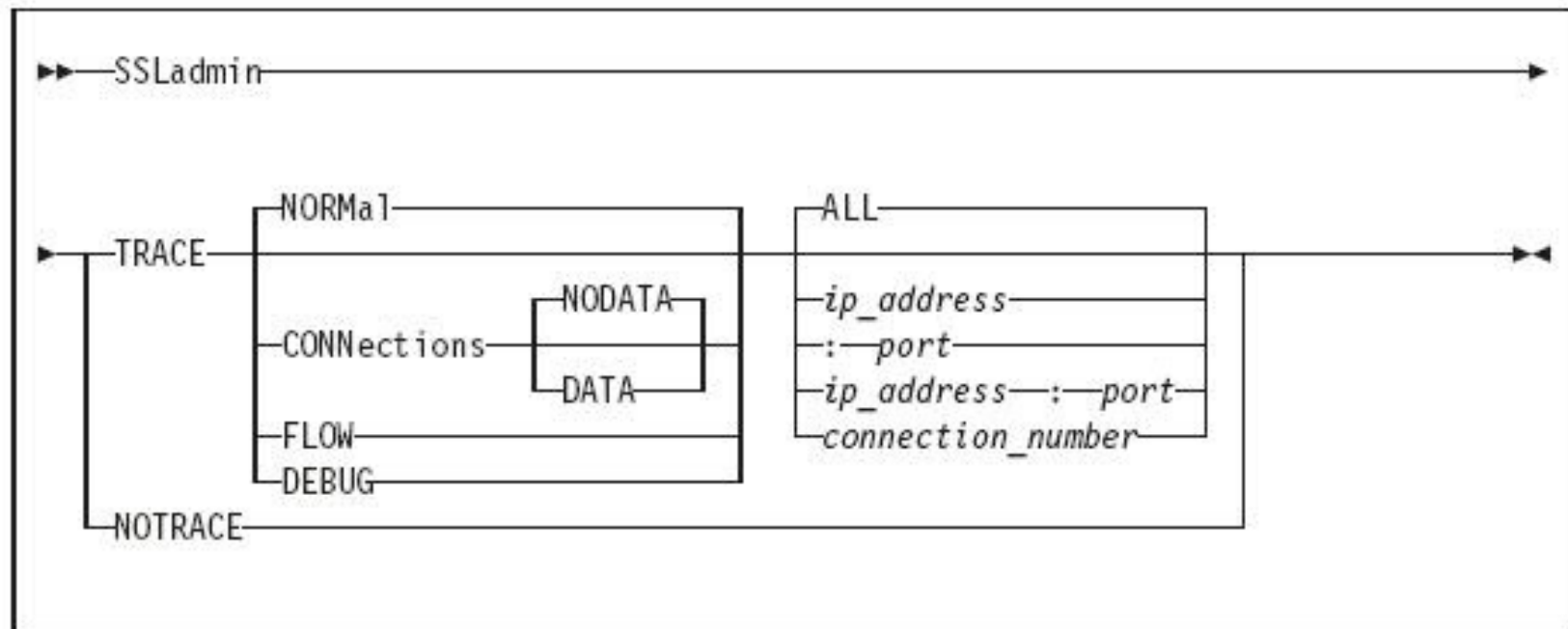
SSLADMIN command

- CLOSECON / LOG retrieves console log
- HELP displays help information
- QUERY Status returns general server data
- QUERY Cache returns cache data
- QUERY Sessions returns data on active secure sessions
- RESTART quiesces and re-IPL's SSL server
- REFRESH reaccess certificate database
- STOP stops the SSL server
- SYSTEM used to issue CP or CMS command
- TRACE / NOTRACE enables / disables tracing

Gathering SSL Status

Tracing

- Configured at start-up through DTCPARMS or VMSSL
- Can be turned on/off with SSLADMIN:



Gathering SSL Status

Tracing – SSLADMIN options

- Normal: records successful connections
 - All: indicates tracing for all incoming connections
 - This can be delimited by an ip address, port number or connection number
- Connections: records state changes and handshake results.
 - Data: displays the first 20 bytes of send/receive entries
 - NoData

Gathering SSL Status

Tracing – SSLADMIN options

- Flow: traces the flow of control and system activity
- Debug: extensive tracing for all control and system activities as well as data on ALL connections
 - **Usage note:** both Trace Flow and Trace Debug generate a lot of data; this not only causes major performance impact but will fill up spool space more quickly.

- NoTrace: turns off **all** tracing.

Gathering SSL Status

Example: TRACE FLOW ALL

```
0001      PEEK      A0  V 133  Trunc=133 Size=2102 Line=1979 Col=1 Alt=0
File (none) (none) from SSLSRV10 at GDLGCT2 Format is CONSOLE.
03:05:17 Info      setupToDo ended; t: 3DA70028
03:05:17 Info      fillToDoStr() started
03:05:17 Info      fillToDoStr() ended
03:05:17 Admin     CQshowAToDo() started
03:05:17 Admin     displaySockSSL() started
03:05:17 Admin     displaySockSSL()
03:05:17 Admin     fromIP: 0.0.0.0:0 Len: 0 ConNum: 0 Z:""
03:05:17 Admin     toIP: 0.0.0.0:0 Fam: 2 Tcb: 0 Lbl:""
03:05:17 Admin     origTCBptr: 0
03:05:17 Admin     displaySockSSL() ended
03:05:17 Admin     CQshowAToDo() ended
03:05:17 Info      placeInToDoList() started
03:05:17 Info      placeInToDoList() ended
03:05:17 Info      signalWorker() started
03:05:17 Info      signalWorker() ended
03:05:17 2         getFirstToDo() started; ToDoList: 3DA70028
03:05:17 Info      adkQueryAns() ended
```

Certificate Management

Certificate Management

About gskkyman

- First available in zVM 5.3.0. – LDAP server
- Came to zVM by way of zOS
- Manages databases stored in a Byte-File System
- SSL Servers and LDAP Servers can share databases and certificates
- GSKADMIN userid created to manage gskkyman

Certificate Management

Accessing gskkyman

1. Log onto GSKADMIN (or other configured id)
2. >> gskkyman

```
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
7 - Display certificate file (Binary or Base64 ASN.1 DER)

0 - Exit program

Enter option number:
```

Certificate Management

Creating a new certificate database

- From starting menu, select option 1:

```
Enter option number:  
1  
  
Enter key database name (press ENTER to return to menu):  
TemporaryDB.kdb  
Enter database password (press ENTER to return to menu):  
  
Re-enter database password:
```

Certificate Management

Creating a new certificate database

```
Enter password expiration in days (press ENTER for no expiration):  
365  
  
Enter database record length (press ENTER to use 5000):  
  
Key database /var/ssl/TemporaryDB.kdb created.  
  
Press ENTER to continue.
```

Certificate Management

Key Management Menu

Database: /var/ssl/TemporaryDB.kdb

Expiration: 2009/09/30 01:19:48

- 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):

Certificate Management

Opening a Certificate Database

- 2. Open Database

```
Enter key database name (press ENTER to return to menu):  
Database.kdb  
Enter database password (press ENTER to return to menu):
```

- GSKADMIN automatically mounts and accesses the database's directory
- Database should be located at mount point
- May require manual configuration if not using the defaults

Certificate Management

Key Management Menu

Database: /var/ssl/Database.kdb

Expiration: None

- 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):

Certificate Management

Database permissions

```
openvm listf (owner
Directory = '/var/ssl'
User ID      Group Name  Permissions Type  Path name component
gskadmin     ssl        rw- r-- r--  F    'rsa4096.arm'
gskadmin     ssl        rw- r-- r--  F    'rsa4096s.arm'
gskadmin     ssl        rw- r-- r--  F    'tcpip0b.arm'
gskadmin     ssl        rw- r-- r--  F    'tcpip0bs.arm'
gskadmin     ssl        rw- r-- r--  F    'tcpip99s.arm'
gskadmin     ssl        rw- r-- r--  F    'testcert.arm'
gskadmin     ssl        rw- r-- ---  F    'Database.kdb'
gskadmin     ssl        rw- r-- ---  F    'Database.rdb'
gskadmin     ssl        rw- r-- ---  F    'Database.sth'
gskadmin     ssl        rw- --- ---  F    'MacTest.kdb'
gskadmin     ssl        rw- --- ---  F    'MacTest.rdb'
gskadmin     ssl        rw- --- ---  F    'MacTest.sth'
gskadmin     ssl        rw- --- ---  F    'TemporaryDB.kdb'
gskadmin     ssl        rw- --- ---  F    'TemporaryDB.rdb'
gskadmin     ssl        rw- r-- r--  F    '2kselc.arm'
gskadmin     ssl        rw- r-- r--  F    '2ktelnet.arm'
gskadmin     ssl        rw- r-- r--  F    '4ktelnet.arm'
GSKADMIN..Ready; T=0.01/0.01 21:27:34
```


Certificate Management

Database permissions

- Changes made with BFS commands (openvm)
- openvm permit Database.kdb rw- r-- --- (replace
 - Executes against specified file
 - Grants read, write and/or execute authority
 - Upon creating a new database, permissions should be adjusted for <name>.kdb, <name>.rdb and <name>.sth

Certificate Management

Importing certificates

- Certificates can be imported into the certificate database through *gskkyman*.
- First, place certificate file in appropriate BFS directory
 - Without key: *tlslabel.arm*
 - With key: *tlslabel.p12* (PKCS #12 format)
- Access *gskkyman*:
 1. Manage keys and certificates
 7. Import a certificate

Certificate Management

Importing certificates

```
Enter import file name (press ENTER to return to menu):  
tcpip0bs.arm  
  
Enter label (press ENTER to return to menu):  
SSLTST01  
  
Certificate imported.  
  
Press ENTER to continue.
```

Certificate Management

Certificate Information

```
Label: SSLTST01
Record ID: 28
Issuer Record ID: 27
Trusted: Yes
Version: 3
Serial number: 48693053000f2864
Issuer name: CA certificate for TCPIP Development Usage
             SSL Development
             TCPIP Development
             Endicott
             NY
             US
Subject name: Server certificate for TCPIP0B system
             TCPIP Development
             SSL development
             Endicott
             NY
             US
```

The “How To” Section

Wherein we answer all those other questions!

How to Designate a Secure Port

- Explicit (“static”) SSL
 - Establish a permanently secure port for secure connectivity
 - Standardized in RFC 2228
- PROFILE TCPIP: PORT statement

PORT

```
21      TCP FTPSERV SECURE tlslabel
```

- *Tlslabel* – name of certificate in database (max. of eight characters)
- Can use port ranges instead of a single port

How to Set Up zVM Applications for SSL

- Configuration File Updates
 - ▶ **TN3270:** INTERNALCLIENTPARMS (in PROFILE TCPIP)
 - SECURECONNECTION
 - TLSLABEL

 - ▶ **FTP:** SRVRFTP CONFIG (server); FTP DATA (client)
 - PASSIVEPORTRANGE
 - SECURECONTROL, SECUREDATA
 - TLSLABEL

 - ▶ **SMTP:** SMTP CONFIG
 - TLS Statement
 - TLSLABEL

How to Change Set-up Dynamically

- zVM Applications support SMSG
 - **SMSG** FTPSERV **QUERY** SECURE
 - **SMSG** FTPSERV **SECURE CONTROL** REQUIRED
 - **SMSG** SMTP **TLS** NEVER

- zVM Telnet – NETSTAT OBEY / OBEYFILE
 - Adjust INTERNALCLIENTPARMS

- SSL Server
 - Operating parameters (DTCPARMS) **cannot** be dynamically changed
 - Certificate database changes can be seen by issuing **SSLADMIN REFRESH** from GSKADMIN (or another authorized userid).

How to Configure non-VM Clients for SSL

A bit about non-VM clients

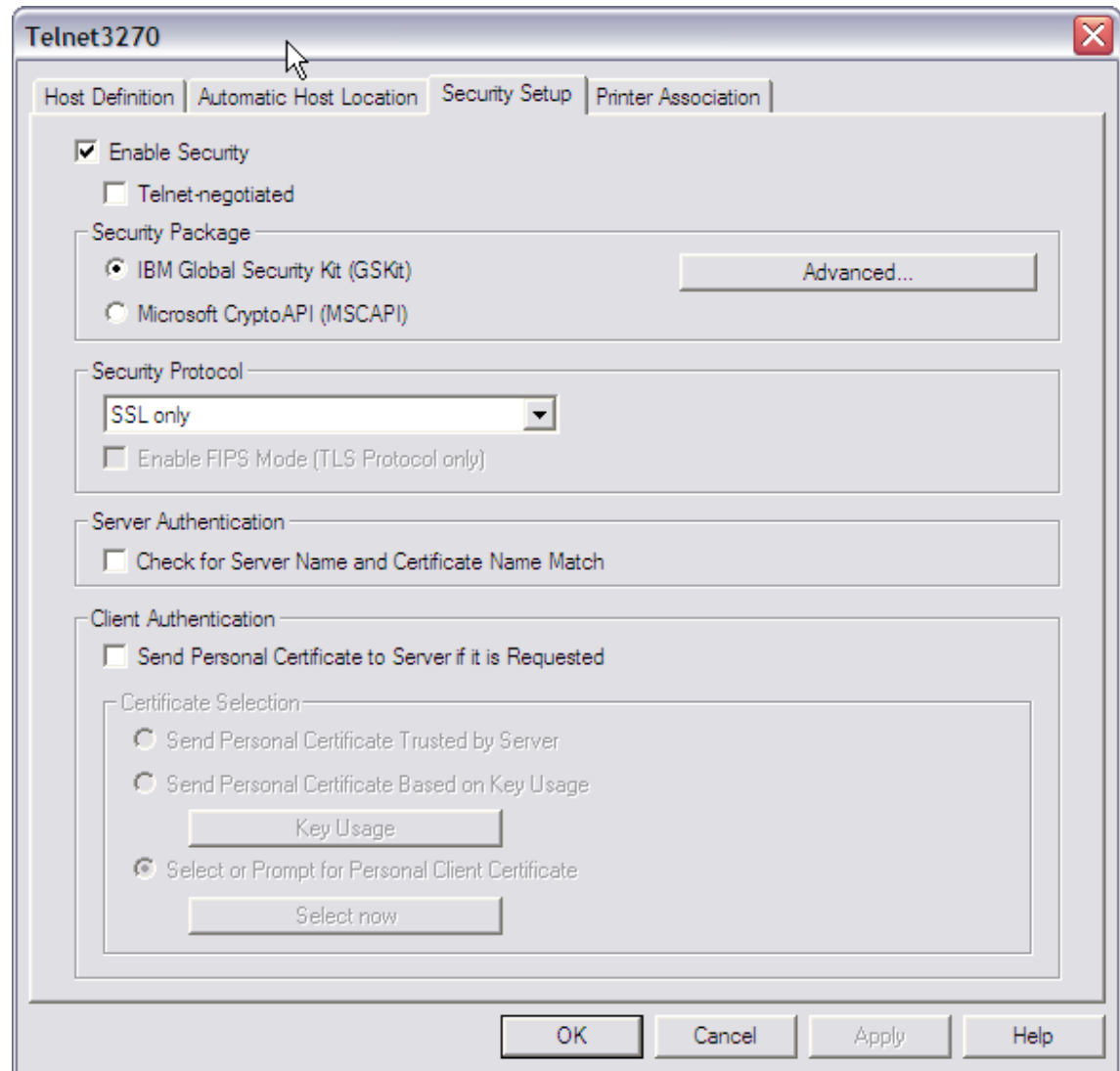
- Clients have varying options and capabilities
- Most will refer to explicit SSL as “SSL” and implicit as “TLS”
- All require a certificate from the database stored locally

Example clients

- Telnet: PComm 5.9 supports both explicit and implicit SSL
- FTP: CoreFTP, Filezilla, Attachmate, Bluezone
- SMTP: Eudora v7.0.1.0 for TLS

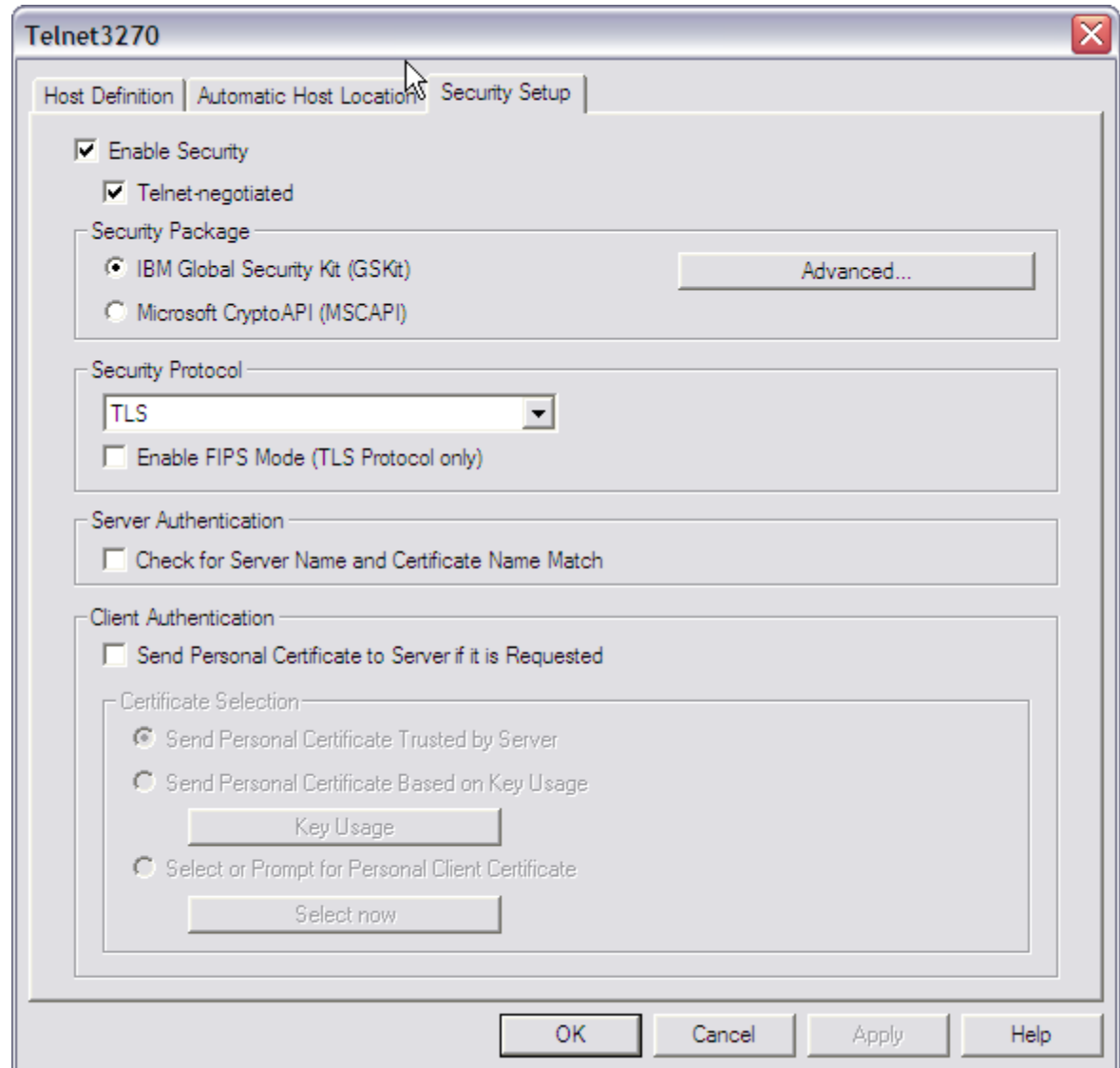
How to Configure non-VM Clients for SSL

- PComm 5.9
- Explicit SSL



How to Configure non-VM Clients for SSL

- PComm 5.9
- Implicit SSL



How to Be Your Own Certificate Authority

- **Certificate Authorities** – traditionally, third-parties who provided assurance that your certificates and keys are secure.
- With zVM 5.4 and the use of *gskkyman*, you can be your own Certificate Authority
- Allows a sysadmin to bypass going to places like Thawte or Verisign to answer certificate requests ... and having to pay money for the privilege.
- Process involves several steps

TCPIP LDAP Administrator's Guide, Chapter 15

How to Be Your Own Certificate Authority

Certificate Authority (System A)	Server or Client (System B)
Step 1 - Create a key database	
<p>Create a key database using the gskkyman command:</p> <ul style="list-style-type: none"> From the Database Menu, select option 1 - Create new database <p>See "Creating, Opening and Deleting a Key Database File" on page 203 for details.</p>	<p>Create a key database using the gskkyman command:</p> <ul style="list-style-type: none"> From the Database Menu, select option 1 - Create new database <p>See "Creating, Opening and Deleting a Key Database File" on page 203 for details.</p>
Step 2 - Create a Root Certificate Authority certificate	
<p>Create a Certificate Authority certificate:</p> <ul style="list-style-type: none"> From the Key Management Menu, select option 6 - Create a self-signed certificate From the Certificate Type menu, select one of the CA values for your certificate type <p>See "Creating a Self-Signed Server or Client Certificate" on page 208 for details.</p>	<p>No action required.</p>
Step 3 - Create a certificate request	
<p>No action required.</p>	<p>Create a certificate request:</p> <ul style="list-style-type: none"> From the Key Management Menu, select option 4 - Create new certificate request From the Certificate Type menu, select one of the certificate types <p>See "Creating a Certificate Request" on page 211 for details.</p>

How to Be Your Own Certificate Authority

Step 4 - Send the certificate request to the CA

No action required.

Send the certificate request to the CA: See [“Sending the Certificate Request”](#) on page 217.

Step 5 - Sign the certificate request

To sign the certificate request, the **gskkyman** command must be issued using command-line options (see [“GSKKYMAN Command Line Mode Syntax”](#) on page 237 for a description of the options). The **gskkyman** command must be issued with the following parameters:

```
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
```


How to Be Your Own Certificate Authority

Step 6 - Send the signed CA certificate and the newly signed certificate to the requestor	
Export the signed CA certificate (created in Step 2) to a Base64 file (DER or PKCS #7) See "Copying a Certificate Without its Private Key" on page 222. Send (for example, without its private key ftp) the Base64 file and the newly signed certificate (created in Step 4) to the requestor.	No action required.
Step 7 - Import the CA certificate	
No action required.	Import the CA certificate. See "Importing a Certificate from a File as a Trusted CA Certificate" on page 231.
Step 8 - Receive the signed certificate	
No action required.	Receive the signed certificate. See "Receiving the Signed Certificate or Renewal Certificate" on page 217. Note: Depending upon the SSL application, you may need to either send the CA certificate to the client, or the server application may actually present the certificate to the client for them during SSL session setup.

Questions?



(references on next slide)

References

- SSL web page
 - ▶ <http://www.vm.ibm.com/related/tcpip/vmsslinf.html>

- Author: Brian Hugenbruch (bwhugen@us.ibm.com)
 - ▶ <http://www.vm.ibm.com/devpages/hugenbru>

- ▶ Acknowledgements
 - ▶ Will Roden Jr (retired), Mark Cibula and Alan Altmark:
IBM Endicott Programming Lab

Bonus Features

... because not everything fits inside
the main presentation.

Service

zVM 5.4.0

- PK65850/PK73085 (UK40952)
- PK75268 (UK41626)
- VM64540 (UM32541)
- VM64569 (UM32592)
- VM64570 (UM32594)

zVM 5.3.0

- PK52298 – connection constraint relief for SSLSERV
 - SLES 9 SP3 and RHEL4 – *64-bit only*
- PK53928 – related SSLADMIN changes
- PK53932 – related TCPIP changes

Linux Support in zVM 5.2 and 5.3

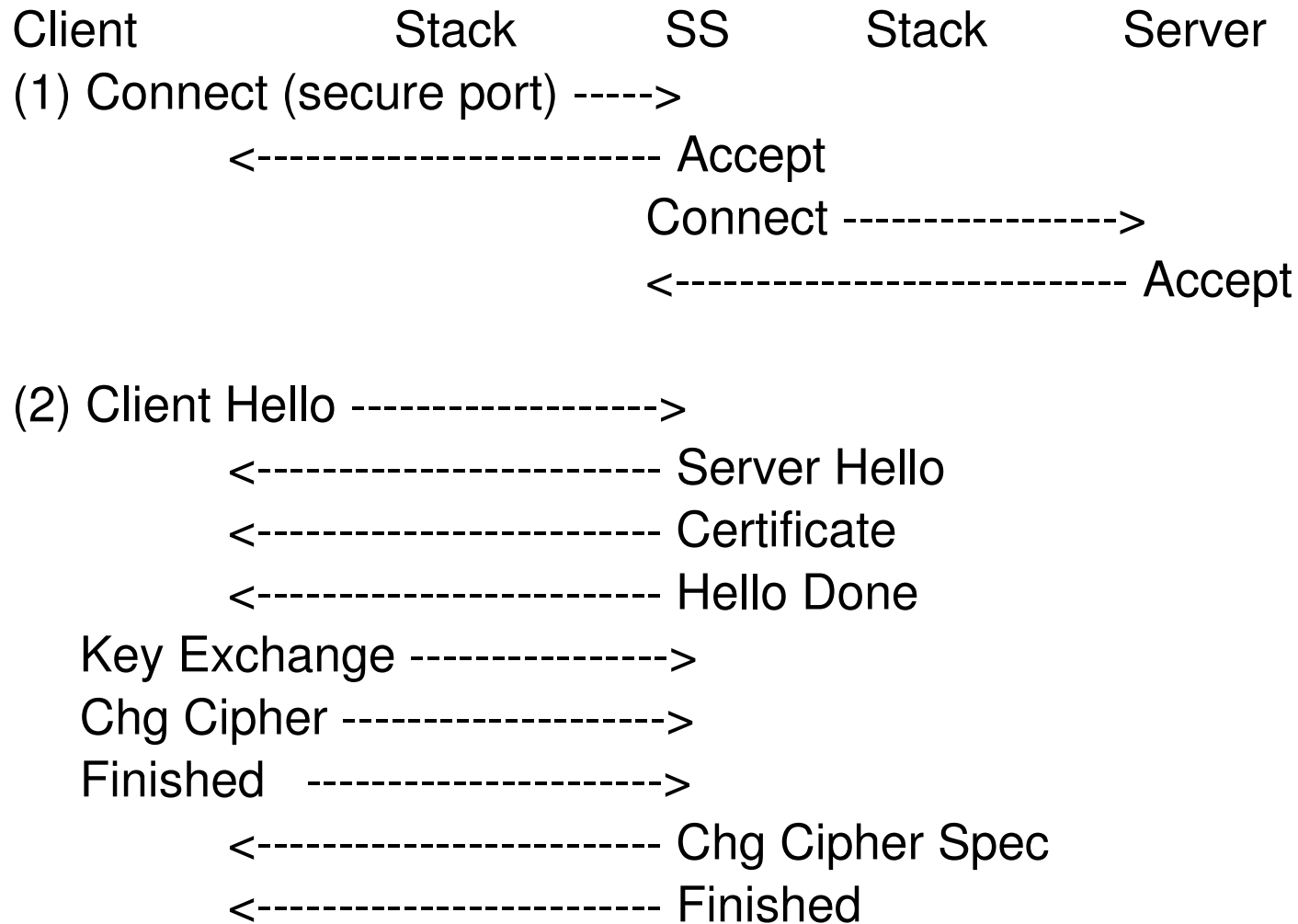
■ SuSE

- ▶ SLES 8 31 bit - 5.2.0. only
- ▶ SLES 9 31 bit
- ▶ SLES 9 64 bit

■ Red Hat Enterprise

- ▶ AS3 31 bit - 5.2.0. only
- ▶ AS3 64 bit - 5.2.0. only
- ▶ AS4 31 bit
- ▶ AS4 64 bit

Example: a Secure Handshake (1)



Example: a Secure Handshake (2)

