

How to Improve Secure Connectivity on Your z/VM TCP/IP Network

With a focus on SSL/TLS Controls

Brian W. Hugenbruch, CISSP
z/VM Security Design and Development
IBM: Endicott, NY, US



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:

*, IBM Systems, IBM System z10®, IBM System Storage®, IBM System Storage DS®, IBM BladeCenter®, IBM System z®, IBM System p®, IBM System i®, IBM System x®, IBM IntelliStation®, IBM Power Architecture®, IBM SureOne®, IBM Power Systems™, POWER®, POWER6®, POWER7®, POWER8®, Power @, IBM z/OS®, IBM AIX®, IBM i, IBM z/VSE®, IBM z/VM ®, IBM i5/OS®, IBM zEnterprise®, Smarter Planet™, Storwize®, XIV®, PureSystems™, PureFlex™, PureApplication™, IBM Flex System™, Smarter Storage

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

- **Overview: What is TCP/IP?**
 - And why is securing it important?

- **Introducing the SSL Server**

- **Managing Digital Certificates in the z/VM environment**

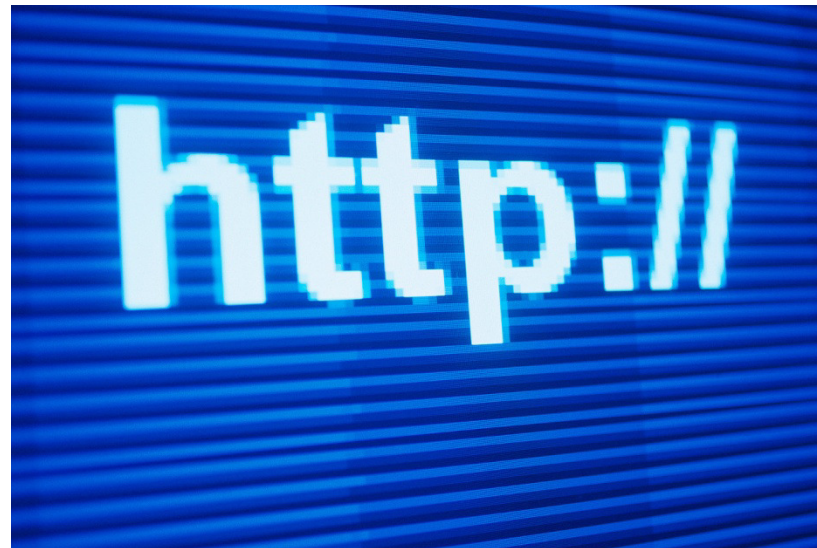
- **Configuring the SSL Server**
 - *And Configuring a 3270 Client for Secure Communication*

- **Frequently Asked Questions**

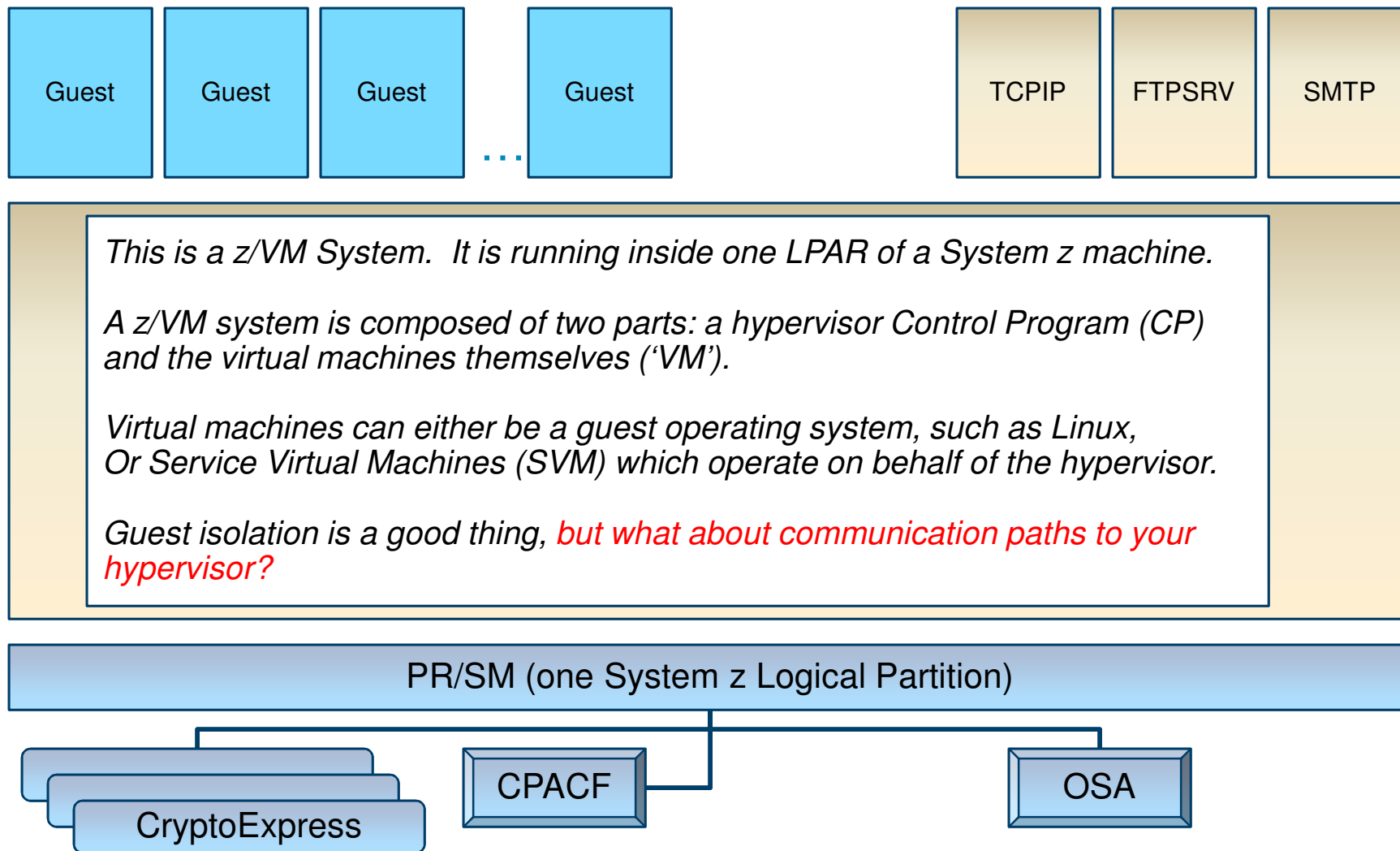
You received your magnifying glasses at conference registration, right?

AES	Advanced Encryption Standard	MAC	Message Authentication Code
ARL	Authority Revocation List	M	Message Detection Code
CA	Certification Authority	MD5	Message Digest 5
CBC	Cipher Block Chaining	OAEP	Optimal Asymmetric Encryption Padding
CCA	IBM Common Cryptographic Architecture	OCSF	OS/390 Open Cryptographic Services Facility
CCF	Cryptographic Coprocessor Facility	OCSF	Online Certificate Status Protocol
CDSA	Common Data Security Architecture	PCICA	PCI Cryptographic Accelerator
CEX2/3A	Crypto Express 2/3 Accelerator Mode	PCICC	PCI Cryptographic Coprocessor
CEX2/3C	Crypto Express 2/3 Coprocessor Mode	PCIXCC	PCI Cryptographic Coprocessor
CFB	Cipher Feedback	PKA	Public Key Architecture
CKDS	Cryptographic Key Data Set	PKCS	Cryptographic Standards
CRL	Certificate Revocation List	PKDS	Public Key Data Set
CRT	Chinese Remainder Theorem	PKI	Infrastructure
CVC	Card Verification Code	RA	Registration Authority
CVV	Value	RACF	Resource Access Control Facility
DES	Data Encryption Standard	RSA	Rivest-Shamir-Adleman
DSA	Digital Signature Algorithm	SET	Secure Electronic Transaction
DSS	Standard	SHA	Secure Hash Algorithm
ECB	Electronic Code Book	SLE	Session Level Encryption
FIPS	Federal Information Processing Standard	SSL	Secure Sockets Layer
GSS	Generalized Security Services	TKE	Trusted Key Entry
ICSF	Integrated Cryptographic Service Facility	TLS	Transport Layer Security
IETF	Internet Engineering Task Force	VPN	Virtual Private Network
IPKI	Internet Public Key Infrastructure		
KGUP	Key Generation Utility Program		
LDAP	Lightweight Directory Access Protocol		

Introduction: z/VM TCP/IP



Your goal is to protect this. All of this. From every angle.



What is z/VM TCP/IP?

- **TCP/IP (Transmission Control Protocol / Internet Protocol)** is a layer of communication infrastructure which serves as the circulatory system of the Internet.
- **z/VM TCP/IP** is a collection of Service Virtual Machines (SVMs) which facilitate communication to and from z/VM systems, and between virtual machines on the same / different systems.
- Service virtual machines handle protocols such as:
 - Telnet
 - FTP
 - SMTP and IMAP
 - REXECD
- *Not to be confused with:*
 - IUCV, APPC, or Virtual Networking
 - Though a TCP/IP stack will often have OSA connectivity



Names of Configuration Files used in this Presentation

- **PROFILE TCPIP** – controls TCP/IP operations and configuration
 - Sits on the TCPMAINT.198 disk, usually accessed at Filemode D
 - May have a different filename, will always be filetype TCPIP
 - ASSORTEDPARMS, INTERNALCLIENTPARMS, PORT, HOME, OBEY ...

- **IBM DTCPARMS** – controls the options and configurations of **Service Virtual Machines**
 - Often renamed as <yoursys>.DTCPARMS
 - Also on TCPMAINT.198
 - Different definitions for SSL configuration, what TLS protocols are allowed, explains where the certificate database is
 - For FTP, enables/disables anonymous access, turns on RACF exits

Why Does Securing z/VM TCP/IP Matter to Me?

- Managing security controls for the hypervisor is a fundamental part of enterprise security management

- This includes connectivity to the hypervisor layer
 - If your guests are secure, and your hypervisor is not ...
 - *... your guests are not as secure as they should be.*

- This line of thinking applies both to smaller shops and to larger shops
 - Controlling potential damage
 - Auditability of privileged commands
 - Restrictions on access to data
 - Enforcing scope of responsibility

- Additionally, encrypting traffic may be mandated by clients, partners, vendors, industry regulations, or governing bodies.

What can we do to secure z/VM TCP/IP?

- **Enable the SSL-TLS Server**
 - Allows (or requires) encrypted traffic to and from the hypervisor
 - For TN3270 connections, it requires a client certificate

- **Enable z/VM service virtual machines (SVMs) to use SSL-TLS as well**
 - Telnet, FTP, SMTP
 - Port-based controls for other services (REXECD, even SMAPI)

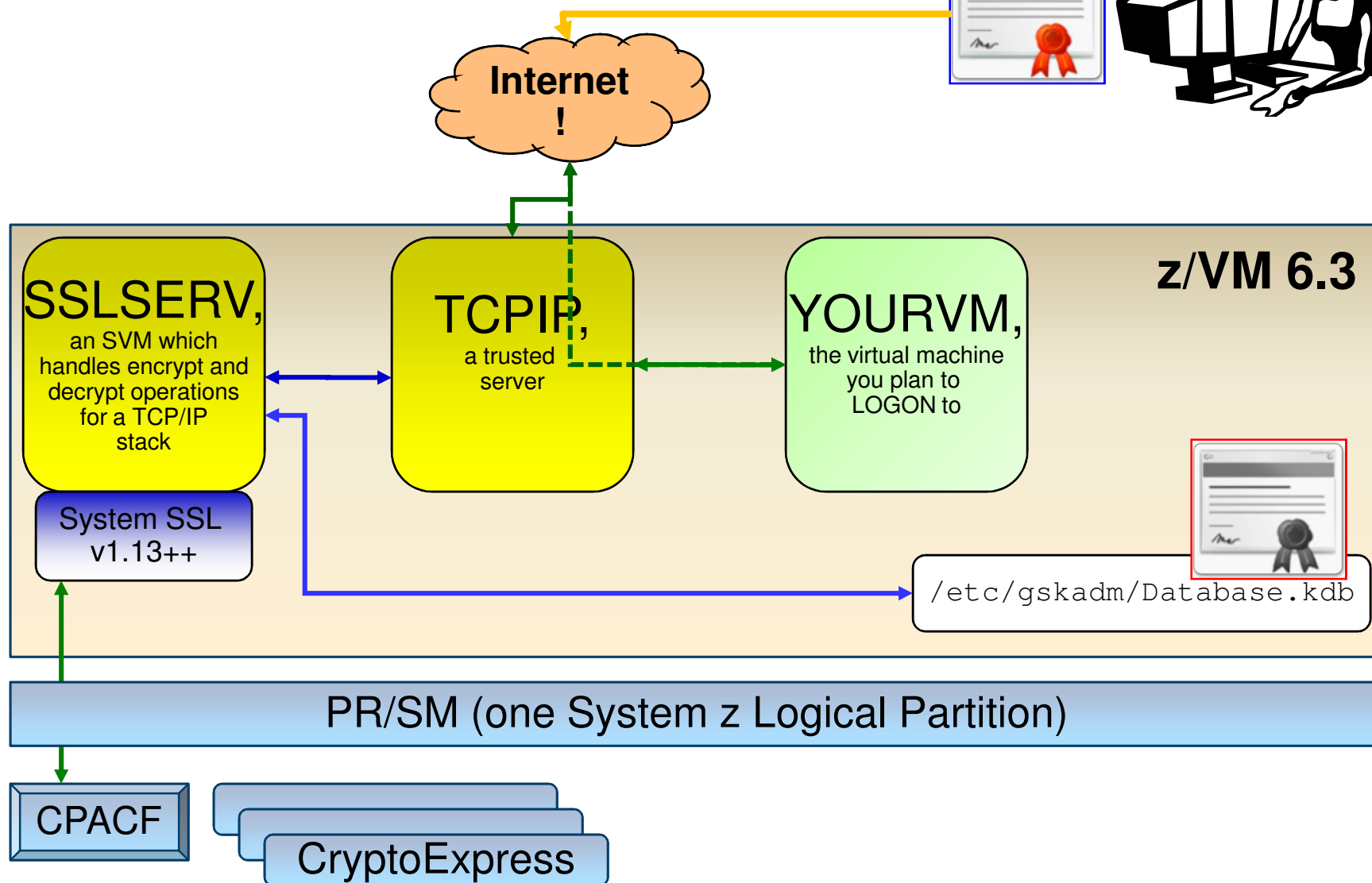
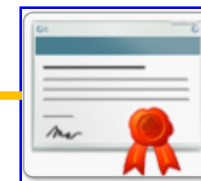
- **Adjust other controls as pertinent:**
 - TIMEMARK for timing out Telnet sessions (PROFILE TCPIP)
 - Disable Anonymous FTP if appropriate (SRVRFTP.CONFIG)
 - Make sure RESTRICTLOWPORTS is enabled (PROFILE TCPIP)
 - Remove unused TCP/IP Service Virtual Machines (NOLOG in USER DIRECT)
 - Enable services for RACFVM control
 - Security labeling for services if appropriate (or SYSNONE for TCPIP)
 - RACF configuration for SSLSERV later in this presentation

Introducing the z/VM SSL Server

(or, “We have an SVM for that”)



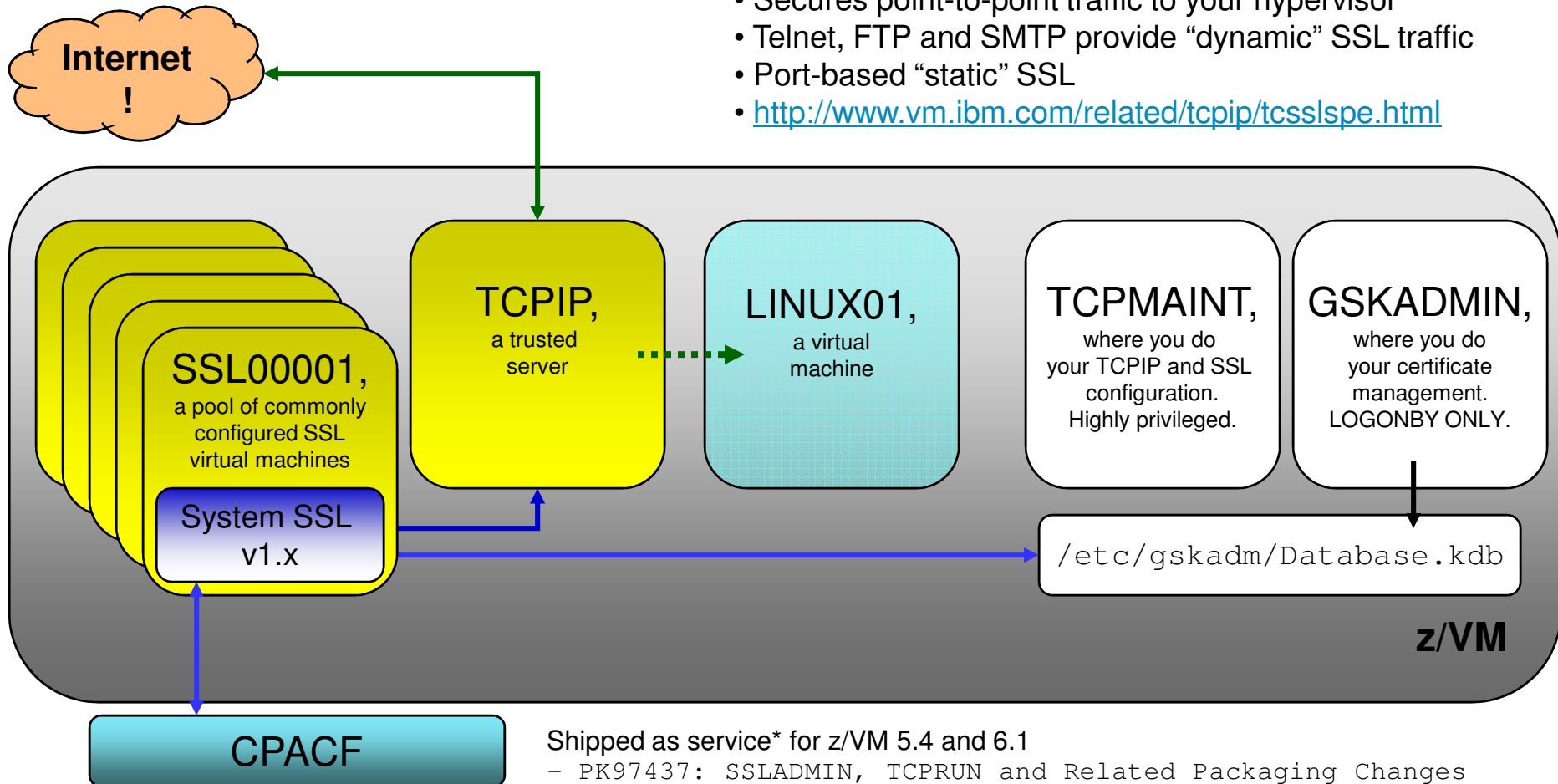
Connecting Securely to z/VM



The z/VM SSL Server

The z/VM SSL Server:

- A CMS-based server associated with the TCP/IP stack
- Secures point-to-point traffic to your hypervisor
- Telnet, FTP and SMTP provide “dynamic” SSL traffic
- Port-based “static” SSL
- <http://www.vm.ibm.com/related/tcpip/tcsslspe.html>



Shipped as service* for z/VM 5.4 and 6.1

- PK97437: SSLADMIN, TCPRUN and Related Packaging Changes
- PK97438: SSLSERV Module Updates
- PK75662: TCPIP Module Updates

Rapelcgvba rkvmfgf orpnhfr fbzrgvzrf
jr yvvr gb xrrc frpergf.

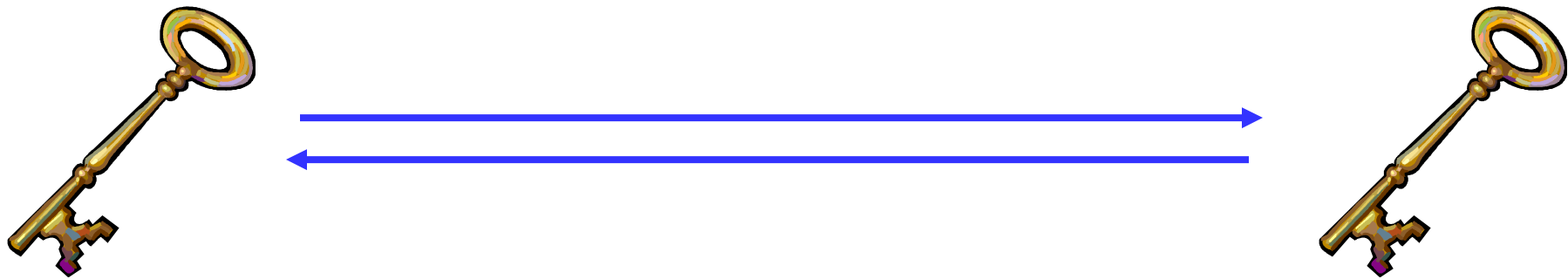


Encryption exists because sometimes
we like to keep secrets.

Cryptography is a mathematical function whereupon plaintext (“information in the clear”) is transmuted into a secret (“encrypted”) and can only be decrypted by someone who shares a common secret.

Symmetric keys (Examples: DES, Triple-DES, AES)

- A secret held in common by two parties
- Used to encrypt or decrypt a message in flight.
- Without the shared secret, a third party could not reasonably decrypt the message

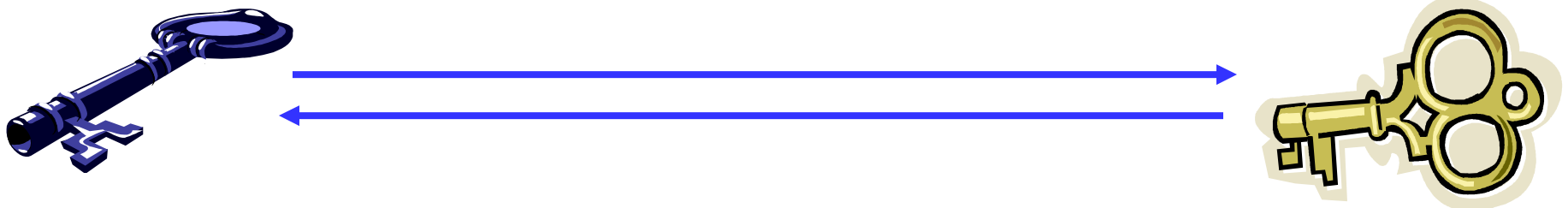


- Faster than asymmetric, but only provides confidentiality – not authentication or nonrepudiation.
- The problem: how does the secret key go from person A to person B?

Asymmetric keys

(Examples: Diffie-Hellman, RSA, DSA, Elliptic Curve)

- Corresponding secrets used to encrypt information
- Data encrypted by the private key can be encrypted by anyone with the public key
 - Only Alice has Alice's private key; if we can decrypt this message, we know it is from Alice.
 - If we encrypt the response with Alice's public key, we know only Alice will be able to read it.

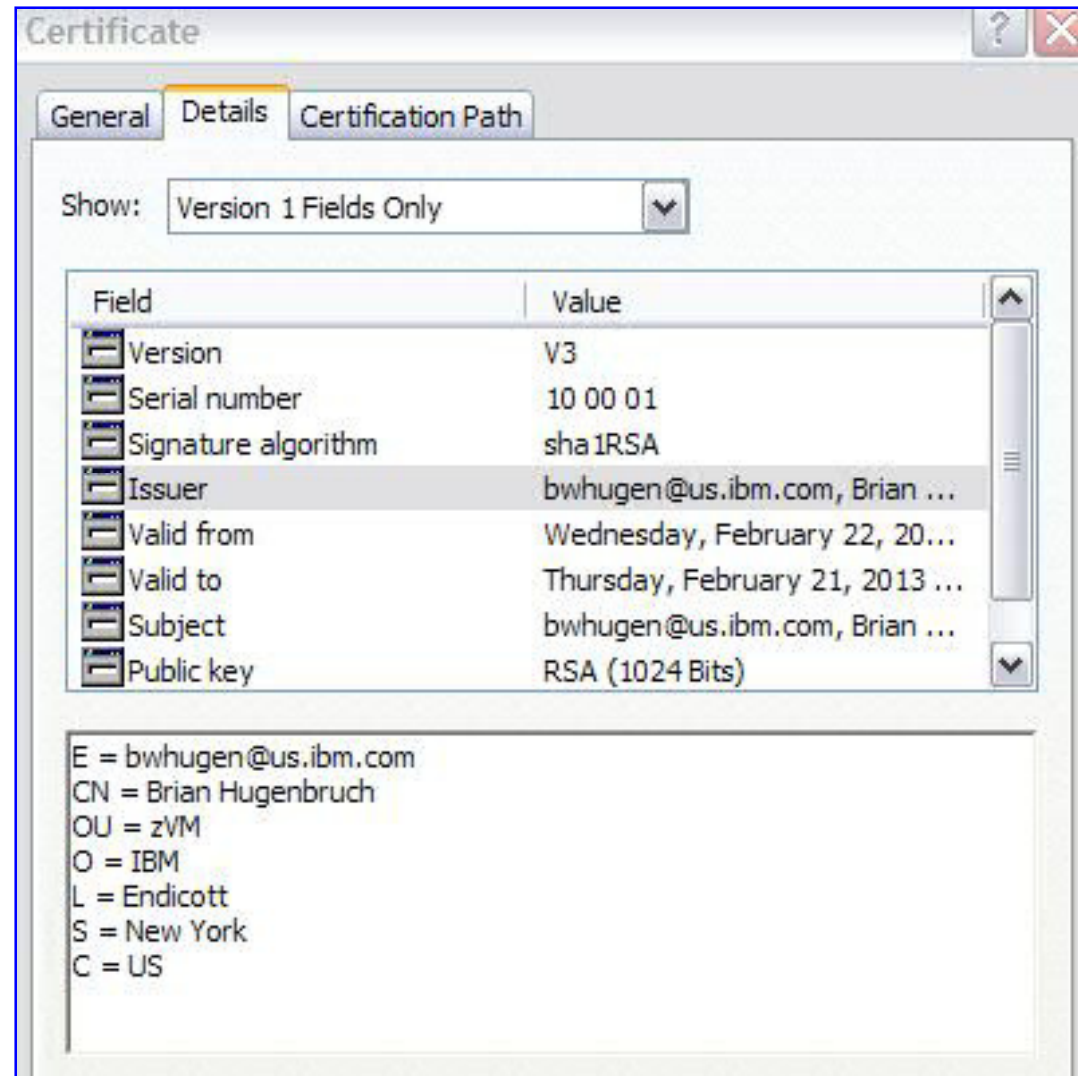


- Mathematically more intensive than symmetric (and therefore much slower)

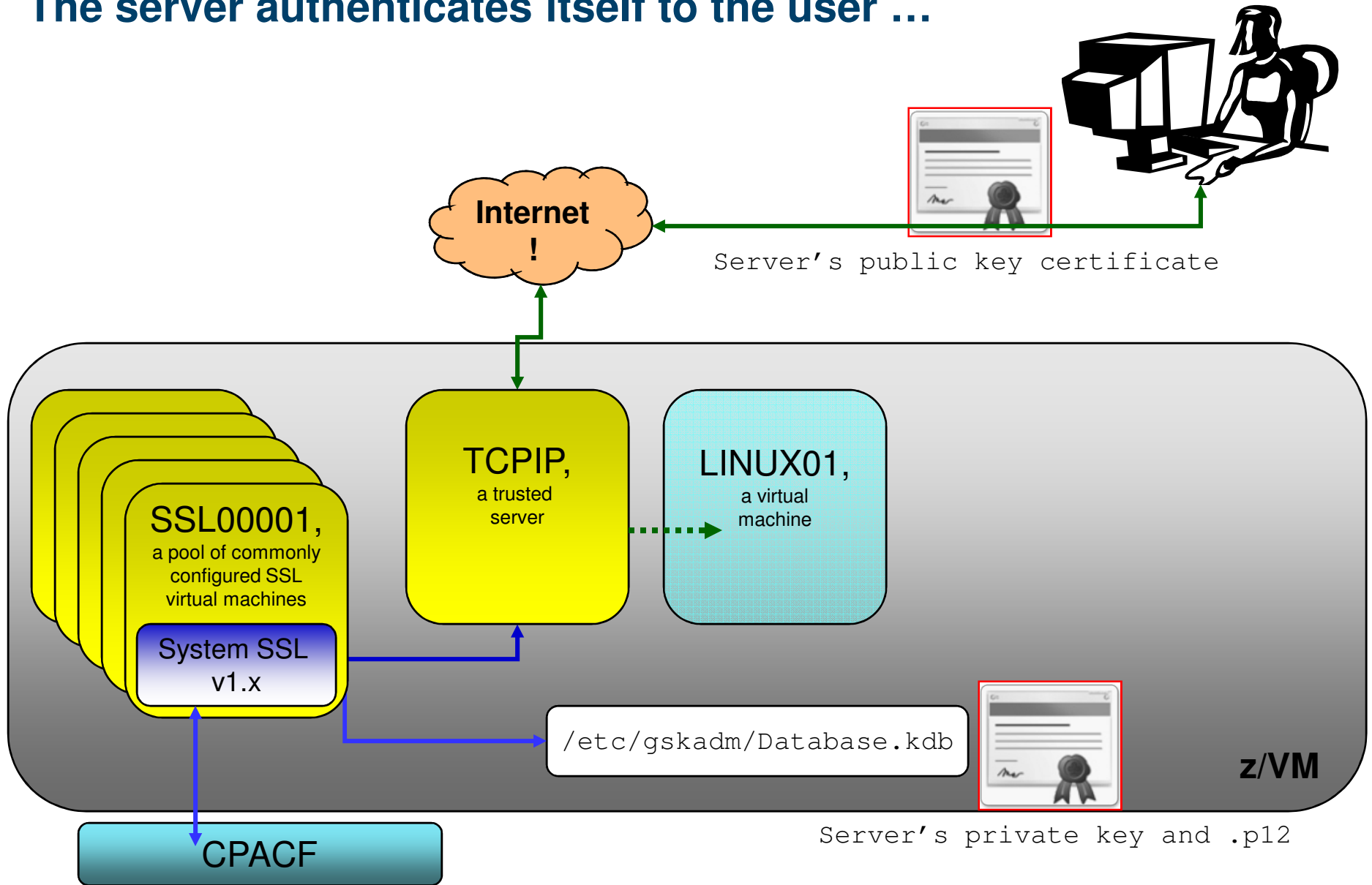
A digital certificate is a unique identifier

- Contains:
 - Public key
 - X.509 information
 - Digital signature

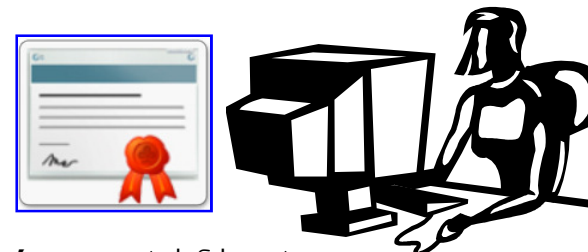
- A mechanism for authenticating identity when exchanging a cryptographic secret



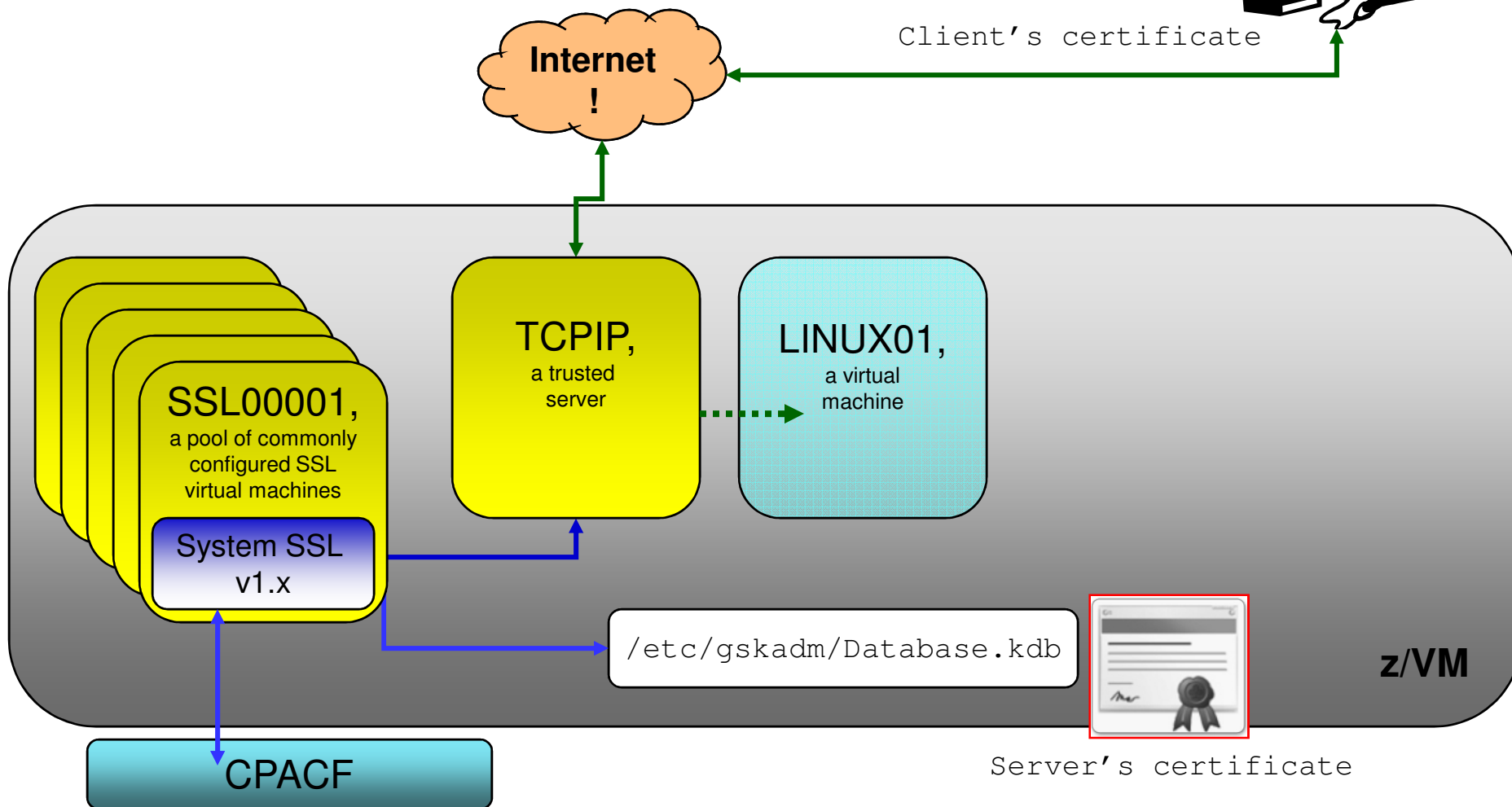
The server authenticates itself to the user ...



Of course, authentication goes both ways. (Dynamic TN3270 only)



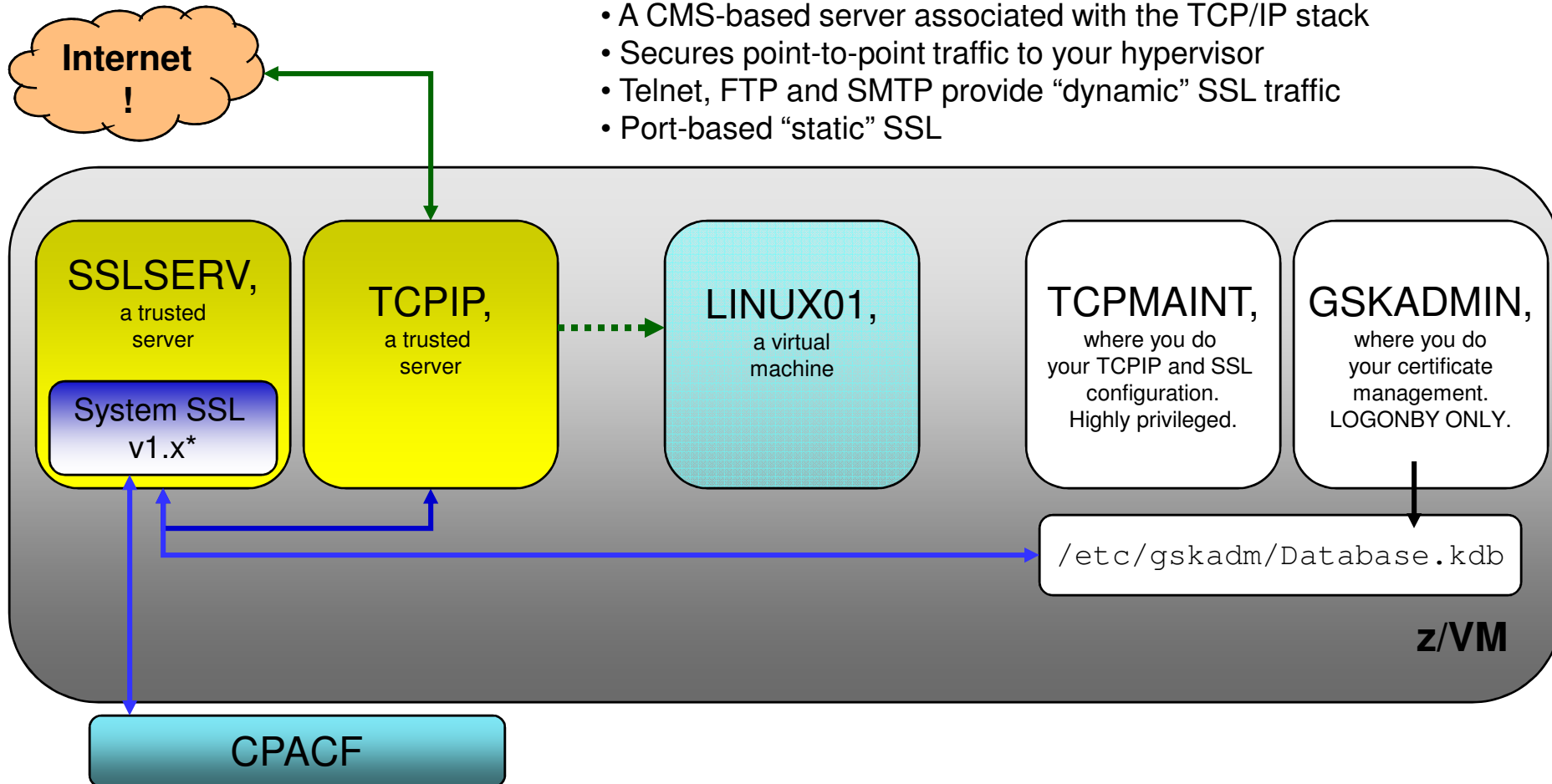
Client's certificate



Where in z/VM do we handle certificate management?

The z/VM SSL Server:

- A CMS-based server associated with the TCP/IP stack
- Secures point-to-point traffic to your hypervisor
- Telnet, FTP and SMTP provide “dynamic” SSL traffic
- Port-based “static” SSL



Managing Digital Certificates

(or, Updating the Party's Guest List)



Certificate Management

About *gskkyman*

- A command-line application for certificate management
 - Ported from z/OS; first made available in z/VM 5.3 (for LDAP)
 - Manages databases stored in a Byte-File System (BFS)
 - SSL Servers and LDAP Servers can share databases and certificates
-
- **GSKADMIN** userid manages *gskkyman* and SSL
 - Introduced in z/VM 5.4
 - Configured to be enrolled in default z/VM BFS filepools
 - Consult webpage for specifics

 - *The following examples assume that default settings are used, and commands are issued from GSKADMIN.*

GSKADMIN,
where you do
your certificate
management.
LOGONBY ONLY.

Certificate Management for z/VM SSL

Logging onto GSKADMIN:

```
Profile..: Setting up BFS environment...
Profile..: Determining what is currently mounted...
Nothing is mounted

Profile..: Mounting root file system...
Profile..: Mounting GSKSSLDB file space at: /etc/gskadm/
Profile..: Setting working directory to: /etc/gskadm/
Profile..: (for direct access to key database files)...
Profile..: Checking mounts...
Mount point = '/etc/gskadm'
Type Stat Mounted
BFS R/W '/../VMBFS:VMSYS:GSKSSLDB/'
Mount point = '/'
Type Stat Mounted
BFS R/W '/../VMBFS:VMSYS:ROOT/'

Profile..: Checking current directory content...
Directory = '/etc/gskadm'
[.....]
Profile..: Setup complete; Environment prepared for use of GSKKYMAN
```


Certificate Management for z/VM SSL

Looking around in GSKADMIN:

```
openvm listf
```

```
Directory = '/etc/gskadm'  
Update-Dt  Update-Tm Type  Links          Bytes Path name component  
02/02/2013 02:41:00   F      1              651 'certfips.arm'  
01/31/2013 19:45:47   F      1             1497 'mct210s1.cert'  
01/31/2013 19:46:09   F      1            120080 'Database_tcpip10.kdb'  
01/31/2013 19:46:09   F      1              80 'Database_tcpip10.rdb'  
01/31/2013 15:44:32   F      1             129 'Database_tcpip10.sth'  
02/06/2013 11:12:43   F      1            60088 'FipsDatabase_tcpip10.kdb'  
02/01/2013 08:23:04   F      1              88 'FipsDatabase_tcpip10.rdb'  
02/01/2013 08:22:55   F      1             129 'FipsDatabase_tcpip10.sth'  
01/31/2013 19:20:46   F      1             1112 'Mct2root.cert'  
01/31/2013 19:39:56   F      1             5109 'MCT210BH.cert'  
Ready; T=0.01/0.01 11:37:27
```

Certificate Management for z/VM SSL

Opening gskkyman:

```
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 for z/VM SSL

Creating a Certificate Database

– 1. Create new Database

```
Enter key database name (press ENTER to return to menu):
```

```
ForThisPresentation.kdb
```

```
Enter database password (press ENTER to return to menu):
```

```
Re-enter database password:
```

```
Enter password expiration in days (press ENTER for no expiration):
```

```
1000
```

```
Enter database record length (press ENTER to use 5000):
```

```
Enter 1 for FIPS mode database or 0 to continue:
```

```
1
```

```
Key database /etc/gskadm/ForThisPresentation.kdb created.
```

```
Press ENTER to continue.
```

Certificate Management for z/VM SSL

Database permissions

```
openvm listf (own
```

```
gskadmin    security    rw- --- --- F  'ForThisPresentation.kdb'  
gskadmin    security    rw- --- --- F  'ForThisPresentation.rdb'
```

- 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 for z/VM SSL

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
 - Default database location: `/etc/gskadm`
- Database should be located at mount point
- May require manual configuration if not using the defaults

Certificate Management for z/VM SSL

Key Management Menu

Database: /etc/gskadm/ForThisPresentation.kdb
Expiration: 2015/12/15 15:49:12

- 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 for z/VM SSL

Importing certificates

- Certificates can be imported into the certificate database through gskkyman.
- But first they need to be placed in the appropriate BFS directory.
- If possible, FTP directly into the BFS
 - `cd /.. /VMBFS:VMSYS:GSKSSLDB/`
- If not, transfer the certificate to GSKADMIN and then issue the following command:

```
openvm putbfs TESTCERT P12 A /etc/gskadm/testcert.p12 (bfsline none
```

or

```
openvm putbfs MYCACERT PEM A /etc/gskadm/mycacert.pem (bfsline nl
```

Certificate Management for z/VM SSL

- The difference in the previous examples is formatting. Standard certificates can be either Base64 or binary format – and `bfsl` none is for binary format only.
 - *If you can open it and read **any** of it, it's in Base64!*

Example: Base64 certificate

```
-----BEGIN CERTIFICATE-----  
MIIEOTCCA+OgAwIBAgIDEAAHMA0GCSqGSIb3DQEEBBQUAMIGcMQswCQYDVQQGEwJV  
UzERMA8GA1UECBMITmV3IFlvcmsxETAPBgNVBAcTCEVuZG1jb3R0MRgwFgYDVQQK  
Ew96Vk0gRGV2ZWxvcG1lbnQxDDAKBgNVBAsTA1NTTDEcMBoGA1UEAxMTQnJpYW4g  
Vy4gSHVnZW5icnVjaDEhMB8GCSqGSIb3DQEJARYSYndodWdlbkBlcy5pYm0uY29t  
MB4XDTEzMMDyNzE3NTMwOVowXDTE0MMDyNzE3NTMwOVowZjELMAkGA1UEBhMCMVVMx  
ETAPBgNVBAgTCE5ldyBZb3JrMRgwFgYDVQQKEw96Vk0gRGV2ZWxvcG1lbnQxDDAK  
BgNVBAsTA1NTTDEcMBoGA1UEAxMTQnJpYW4gVy4gSHVnZW5icnVjaDCCAiIwDQYJ  
KoZIHvcNAQEBAQADggIPADCCAgoCggIBAPb/rq0V3++X7lJ2N7xDcktOeSxjv1kA  
2n1HRnb3VC05HlROket1Oxd4QhBoLWL+GJgo2vY1jBM3fP/KX6lFYcCXj+zwUMIu  
+eGOB+DRmVfL4cZnVYEkwTgBnEKRLQEIJ+KmgGnJgtJYRjdZ54kaXlgB2obupCui  
099iYZDVkzdiizu/S1rM0dP3jz3p6MRWWRN4f9uf6a4bNd+bCI7HnVLsLvfp3wCW  
MUTKjAx6snZPAgMBAAGjezB5MAkGA1UdEwQCMAAwLAYJYIZIAyb4QgENBB8WHU9w  
ZW5TU0wgR2VuZXJhdGVkIENlcnRpZmljYXR1MB0GA1UdDgQWBBTWiatA5nzhUruN  
dS9/TJPz/F3PnTafBgNVHSMEGDAWgBT7hRhg6eCiBsJPY2+4DBIzqS8CEzANBgkq  
hkiG9w0BAQUFAANBAAwic+Z/IvzFImTcgvNC3PH99c9u8J0u5KiAT39c6ia+FuZZ  
i3tBDKoSBCfy2kBBc4k6CQNYazovVSUtJrJquQU=  
-----END CERTIFICATE-----
```

Example: Binary-format certificate with key

```
'b"Ñ""""b""""fçf7""""µb""b""b""b""""fçf7""""µb""b""b""b""""fçf7' . . .
```

- Key differences:
 - Binary format is one record (line), LRECL is comparatively huge
 - Binary format does not include the “Begin/End” certificate lines
- Your certificates may appear in *either* format
- .p12 files, the PKCS #12 format for a Certificate With Private Key, **is binary only.**

Certificate Management for z/VM SSL

- The difference in the previous examples is formatting. Standard certificates can be either Base64 or binary format – and bfsline none is for binary format only.
 - *If you can open it and read **any** of it, it's in Base64!*
- .p12 files, the PKCS #12 format for a Certificate With Private Key, is binary only.
- Once the key is in the BFS directory, access *gskkyman*. Open the database and select the following options:

```
1. Manage keys and certificates
7. Import a certificate
```

or

```
8. Import a certificate and a private key
```

Certificate Management for z/VM SSL

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 for z/VM SSL

```
                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
```

Certificate Management for z/VM SSL

A few final thoughts:

- When making changes to a certificate database in use by a running SSL Server virtual machine, be sure to issue an SSLADMIN REFRESH from a privileged userid.
- The server will reload its environment without interrupting existing secure connections.
- Important for when certificates need to be renewed, replaced or removed.
- SSLADMIN REFRESH will automatically be transmitted to all SSL servers in an SSL Pool.

Configuring the z/VM SSL Server

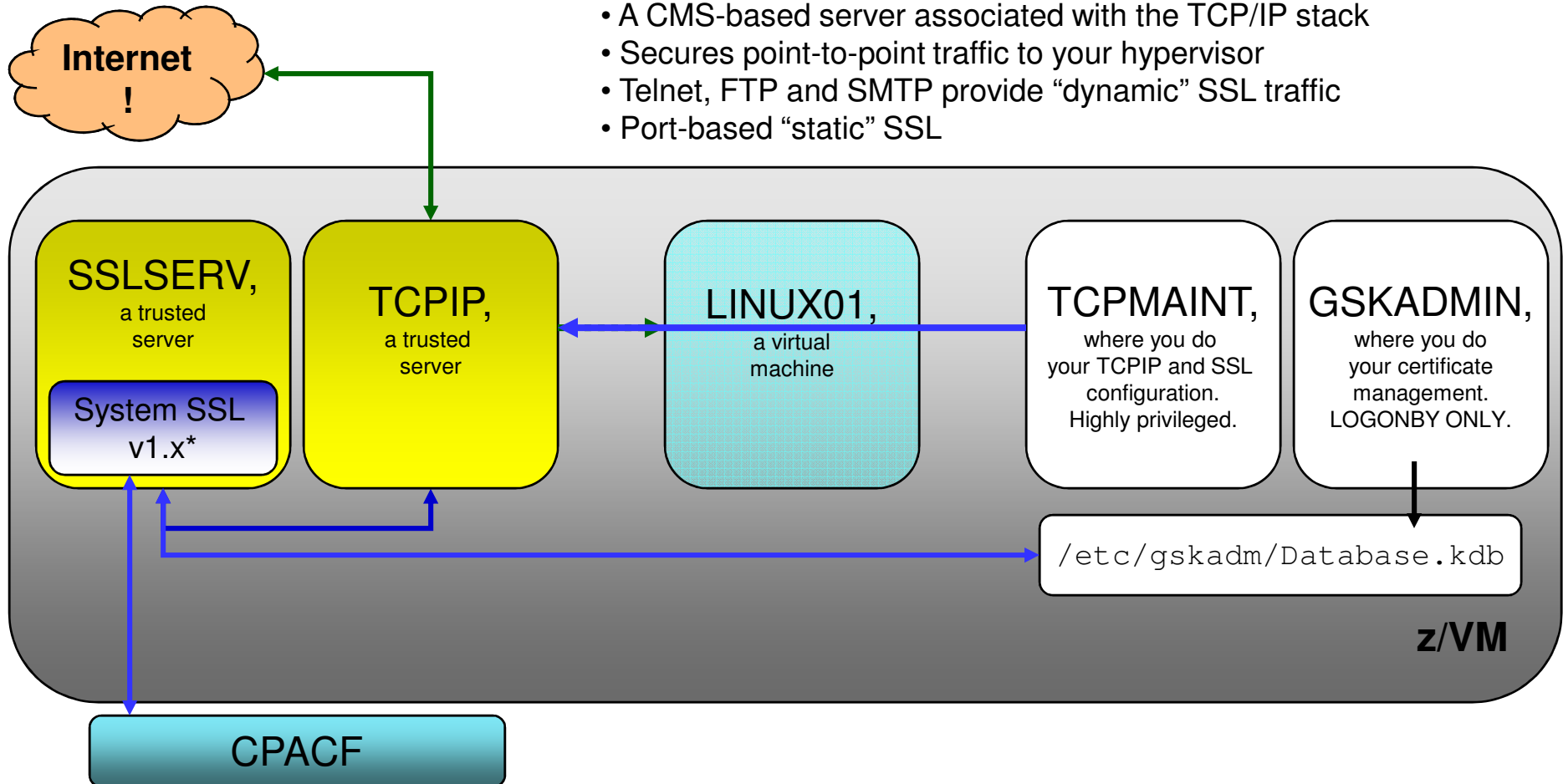
(or, "Tickets, please.")



Configuring Secure Connectivity

The z/VM SSL Server:

- A CMS-based server associated with the TCP/IP stack
- Secures point-to-point traffic to your hypervisor
- Telnet, FTP and SMTP provide “dynamic” SSL traffic
- Port-based “static” SSL



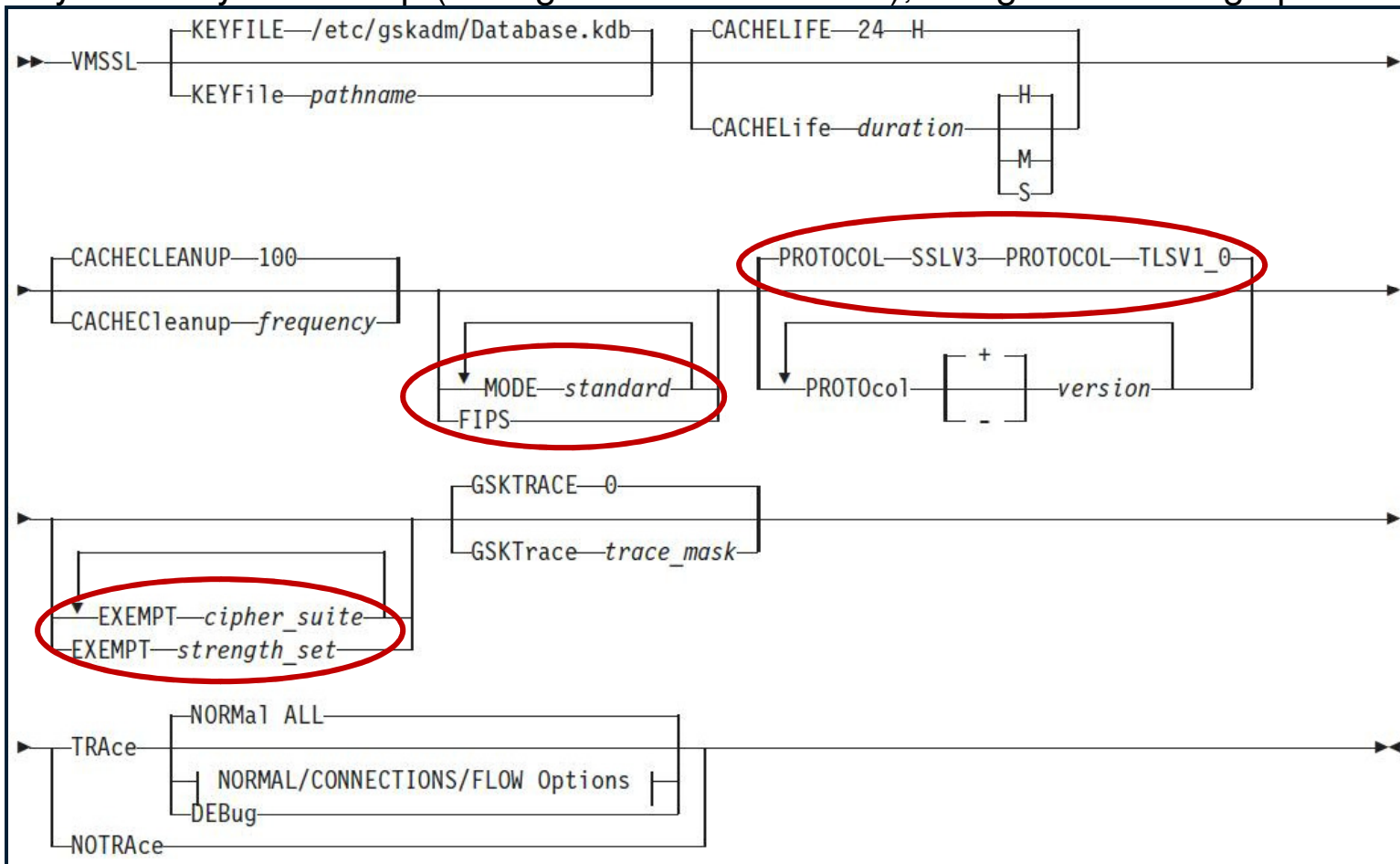
Configuring the SSL Server

- DTCPARMS values associated with your SSL Server:

:Admin_ID_list.	Userids authorized to execute privileged commands – e.g., SSLADMIN commands
:Mixedcaseparms.	Parameters are supported in mixed case
:Mount.	Certificate database location. Default is /etc/gskadm/
:Parms.	As per the VMSSL command
:Stack.	Associated TCPIP virtual machine <i>This tag is required; otherwise, the SSL server / pool cannot be identified during stack initialization!</i>
:Timestamp.	On/Off for timestamps on terminal messages and cmd responses
:Timezone.	Set timezone of server
:Vmlink.	Sets a Pool member's SFS space

z/VM SSL Server News – Protocol Selection

- Configuration can be done either statically (through the DTCPARMS file) or dynamically at start-up (through the VMSSL EXEC), using the following operands:



z/VM SSL Server Options

- Specified either on VMSSL (command-line exec) or DTCPARMS
- Persists for the run-time for a server or server pool. Must be consistent for all members of a server pool
- Options:
 - **KEYFILE** – BFS location of the certificate database
 - **CACHELIFE** – for secure connections, in hours, minutes, seconds
 - **CACHECLEANUP** – processed every n connections
 - **MODE** – sets a cryptographic compliance mode
 - **MODE FIPS-140-2**
 - **MODE NIST-800-131A**
 - **FIPS** – equivalent to **MODE FIPS-140-2**
 - **PROTOCOL** – enable or disable SSL/TLS levels.
 - **SSLV3** and **TLS 1.0** enabled by default
 - **Available protocols change based on MODE**
 - **EXEMPT** – disable particular cipher suites
 - **GSKTRACE** – enable System SSL tracing
 - **TRACE/NOTRACE** – enable SSL Server tracing
 - Can be dynamically manipulated via authorized commands

z/VM SSL Server Updates – TLS 1.2 Support

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	RSA_AES_128_SHA256	DH_DSS_DES	NULL_SHA256
DHE_RSA_3DES	DH_DSS_AES_128	DH_RSA_DES	
RSA_AES_256	DH_DSS_AES_128_SHA256	DHE_DSS_DES	
RSA_AES_256_SHA256	DH_RSA_AES_128	DHE_RSA_DES	
DH_DSS_AES_256	DH_RSA_AES_128_SHA256		
DH_DSS_AES_256_SHA256	DHE_DSS_AES_128		
DH_RSA_AES_256	DHE_DSS_AES_128_SHA256		
DH_RSA_AES_256_SHA256	DHE_RSA_AES_128		
DHE_DSS_AES_256	DHE_RSA_AES_128_SHA256		
DHE_DSS_AES_256_SHA256			
DHE_RSA_AES_256			
DHE_RSA_AES_256_SHA256			

Legend:
TLS 1.2 only
Not in TLS 1.2
Not in TLS 1.1 or 1.2

Note 1: Cipher suites can be exempted from processing based on either cipher name or by strength set, per the above (but not both).

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

Note 3: Ciphers are negotiated on a per-handshake basis and are protocol-dependent.

Configuring SSL: FIPS 140-2 Compliance



- **Requires both database support ...**
 - In *gskkyman*, the *Create New Database* option will prompt for FIPS mode

```
Enter 1 for FIPS mode database or 0 to continue:
```

```
1
```

```
Key database /etc/gskadm/ForThisPresentation.kdb created.
```

- **... and SSL Server Support**
 - DTCPARMS: **FIPS (or MODE FIPS-140-2)** or
 - VMSSL: **FIPS (or MODE FIPS-140-2)**

z/VM SSL Server Updates – Mode Selection

- **MODE FIPS-140-2**
 - Replaces ‘FIPS’ keyword
 - Minimum Protocol of TLS 1.0
 - Export ciphers restricted
 - Minimum key exchange value of 1024
 - FIPS-compliant database required
 - Integrity checking (HMAC-SHA256)
 - Known Answer Tests
- z/VM has been FIPS-compliant since V6R1
- ***NEW* MODE NIST-800-131A**
 - Minimum Protocol of TLS 1.2
 - Minimum key exchange value of 2048
 - DSA certificate usage prohibited!
 - Minimum hash of SHA2
 - No certificate database requirements
 - Integrity checking only (HMAC-SHA256)
 - Supersedes FIPS-140-2 where applicable
- Requires **APAR PM93363** (z/VM 6.3 only)
- When running in either mode, the cipher suites available adjust accordingly ...

“How To”: Select Protocols and Modes for your SSL Server

If we specify ...

[Default Settings]:
 PROTOCOL +TLSV1_0
 PROTOCOL +SSLV3

[New Protocols]:
 PROTOCOL +TLSV1_1
 PROTOCOL +TLSV1_2

MODE FIPS-140-2

MODE NIST-800-131A

EXEMPT MEDIUM

```
SSL00001 Enabled TLSV1_2
SSL00001 Disabled TLSV1_1 TLSV1_0 SSLV3 SSLV2

RSA_AES_256_SHA256 DH_RSA_AES_256_SHA256
DHE_RSA_AES_256_SHA256 RSA_AES_256 DH_RSA_AES_256
DHE_RSA_AES_256 DHE_RSA_3DES DH_RSA_3DES
```

- MODE FIPS-140-2 and MODE NIST-800-131A have additional restrictions:
 - Certificate key minimum of 1024 for FIPS, and FIPS-mode database required
 - Certificate key minimum of 2048 for NIST, and SHA-2 only
- MODE overrides specified PROTOCOL statements
 - FIPS requires a minimum protocol level of TLS 1.0
 - NIST requires a minimum protocol level of TLS 1.2
- Plan ahead if MODE support is a requirement for your configuration!

Configuring Secure Connectivity

■ TCPIP Configuration

- <http://www.vm.ibm.com/related/tcpip/tcpspesc.html>
- SSSLIMITS (determines volume of concurrent connections per server)
- SSLSERVERID (identifying the server to TCPIP)
 - If detected, TCPIP will autolog SSLSERV automatically
 - Use * for a pool of SSL machines – association happens in DTCPARMS

■ Implicit (“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 8 characters)
- Can use port ranges instead of a single port

Configuring TCP/IP Services for Secure Connectivity

- **Configuration File Updates (for “Dynamic” SSL)**
 - ▶ **TN3270:** INTERNALCLIENTPARMS (in PROFILE TCPIP)
 - SECURECONNECTION {**Required** | **Allowed** | **Never**}
 - ***new*** CLIENTCERTCHECK {**FULL** | **NONE**}
 - TLSLABEL <server_certificate_name>

 - ▶ **FTP:** SRVRFTP CONFIG (server); FTP DATA (client)
 - PASSIVEPORTRANGE
 - SECURECONTROL, SECUREDATA {**Required** | **Allowed** | **Never**}
 - TLSLABEL <server_certificate_name>

 - ▶ **SMTP:** SMTP CONFIG
 - TLS Statement {**Required** | **Allowed** | **Never**}
 - TLSLABEL <server_certificate_name>

- These can be adjusted dynamically (SMSG, NETSTAT OBEY)

Dynamic Reconfiguration of z/VM's TLS Settings

- z/VM Applications support SMSG
 - **SMSG FTPSERV QUERY SECURE**
 - **SMSG FTPSERV SECURE CONTROL REQUIRED**
 - **SMSG SMTP TLS NEVER**

- z/VM 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).

Running the SSL Server

Starting the Server

- When properly configured, SSLSERV or an SSL* pool will start when the TCPIP virtual machine is started
 - In a pool, the first pool member (e.g., SSL00001) is autologged first

- To bring a specific server online:
 - `SSLADMIN START (SSL SSL00004`

 - or

 - `NETSTAT SSL START SSL00004`

Running the SSL Server

SSLADMIN command

- Privileged command (:Admin_ID_list.)
- Reports information on SSL server status and connections
- Can route commands to specific SSL servers or TCPIP stacks

```

                                .-QUERY STATUS SUMMARY-.
>>--SSLADMIN---.-----'--command-----'--operands----->
                    '-diagnostic_op-'

>----->
    '-(--| Options |--.---.--'
                    '-)-'

Options:

|-----|
|          .-ALL----. | '-TCPserver--userid-' '-MONitor--seconds-'
|'-SSLserver--'-userid--'

```

- <http://www.vm.ibm.com/related/tcpip/tcspeca.html>

Running the SSL Server

SSLADMIN command

- **CLEAR** remove userid(s) set by SET
- **CLOSECON / LOG** retrieves console log
- **HELP** displays help information
- **QUERY**
 - Status Summary returns general server data
 - Status Details returns specific server data
 - Settings returns current command defaults
 - Cache returns cache data
 - Sessions returns data on active secure sessions
 - Trace returns trace settings
- **RESTART** quiesces and re-IPL's SSL server
- **REFRESH** reaccess certificate database
- **SET** sets default targets for SSLADMIN commands
- **START / STOP** starts / stops an SSL server
- **SYSTEM** used to issue CP or CMS commands
- **TRACE / NOTRACE** enables / disables tracing

Running the SSL Server

Tracing

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

```

                .-NORMAL ALL-----
>>--SSLADMIN--.-TRACE--+-----+-----X
      |          |--| NORMAL/CONNECTIONS/FLOW Options |--|
      |          |--DEBUG-----|
      '-NOTRACE-----'

NORMAL/CONNECTIONS/FLOW Options:
                                     (1)
    .-NORMAL----- .-ALL or ALL 20-----
    |-----+-----+-----+-----|
    |--NORMAL-----|          .-20-----| | | |
    |          .-NODATA-. |          .-ALL-----+-----|
    |--CONNECTIONS--+-----+-----|  |--ip_address-----|          (2)|
    |          '-DATA---'|          |--:--port-----|  |--length---|
    '-FLOW-----'          |--ip_address--:--port-|  '-ALL-----'
                          '-connection_number---'
    
```

Configuring Clients for Secure Connectivity *(or, How to Get There From Here)*

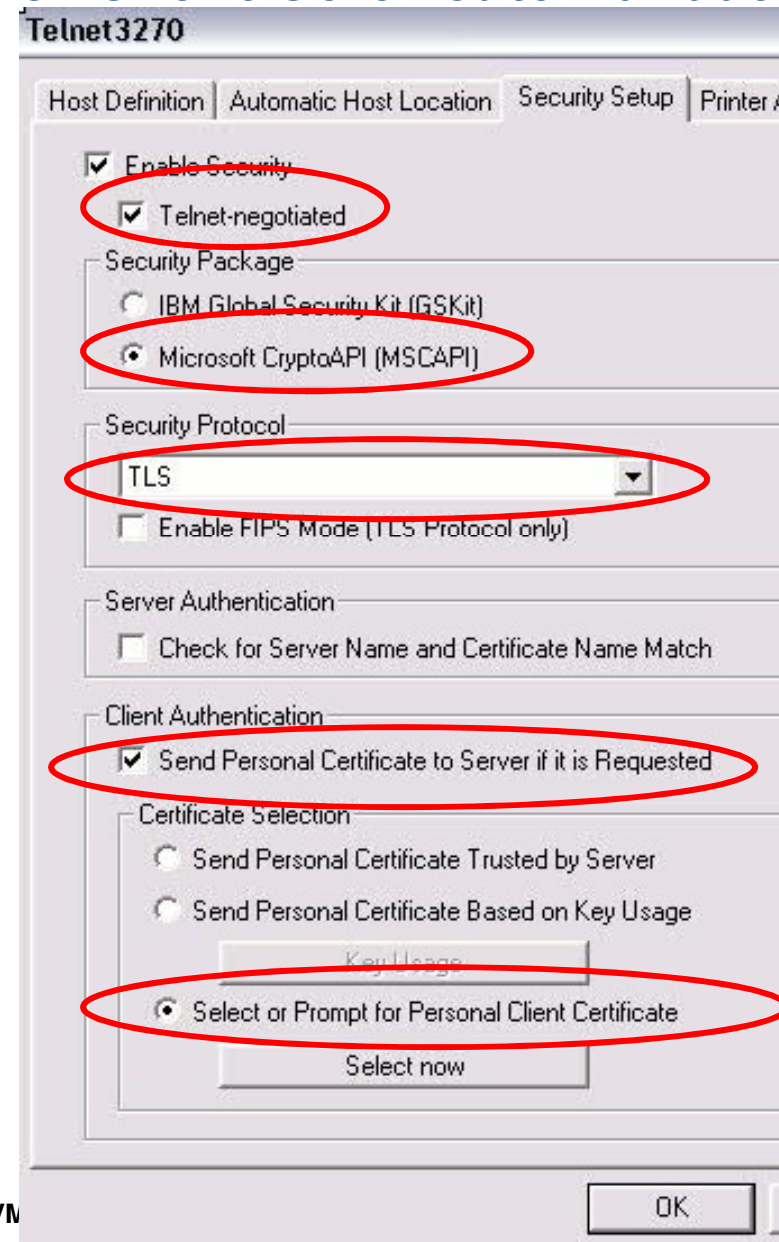


Configuring External Clients to Connect to z/VM

- The compatibility and capabilities of external clients will vary
 - Consult the TCP/IP service webpage for thoughts
 - <http://www.vm.ibm.com/related/tcpip/tcsl540.html>
- The terminology of external clients may vary (SSL vs TLS)
- The certificate management techniques for local clients will also vary (MSCAPI, GSKit, openSSL, x3270 ...)
- During the handshake, the external client will need to understand both the **server certificate** and (if enabled) the **client's certificate**
 - These may or may not be generated off the same root certificate
 - Installation into a local certificate database will be required

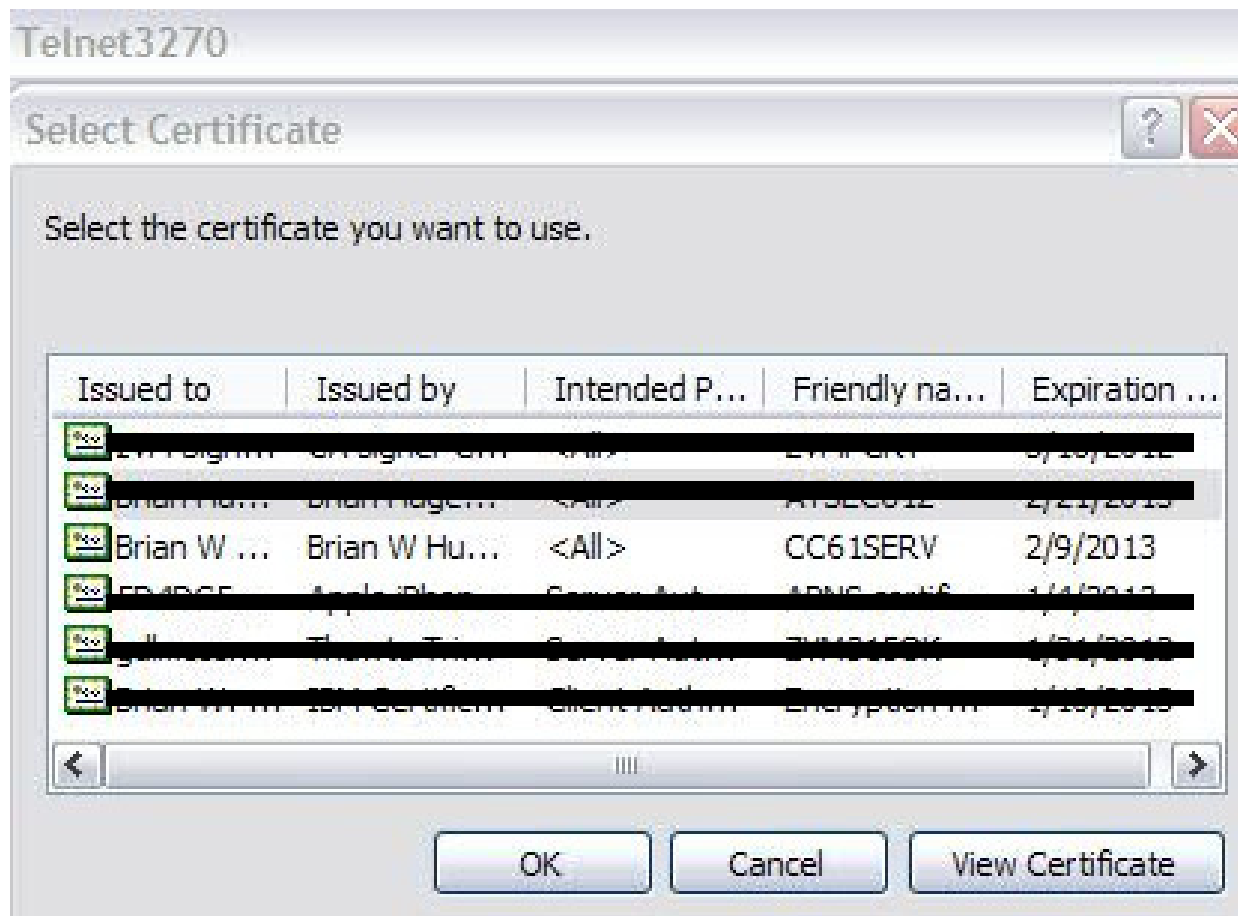
Example: Configuring PComm for Client Certificate Validation

- Telnet-negotiated: dynamic SSL
- MSCAPI: certificates are stored in Windows, rather than PComm's GSKit library.
- TLS: instead of SSLv3. FIPS mode disabled in this example. TLS 1.1 and TLS 1.2 available in later versions of the client
- "Personal Certificate" represents the client's identifying certificate. This will be sent if z/VM's Telnet server is configured for **CLIENTCERTCHECK FULL**.

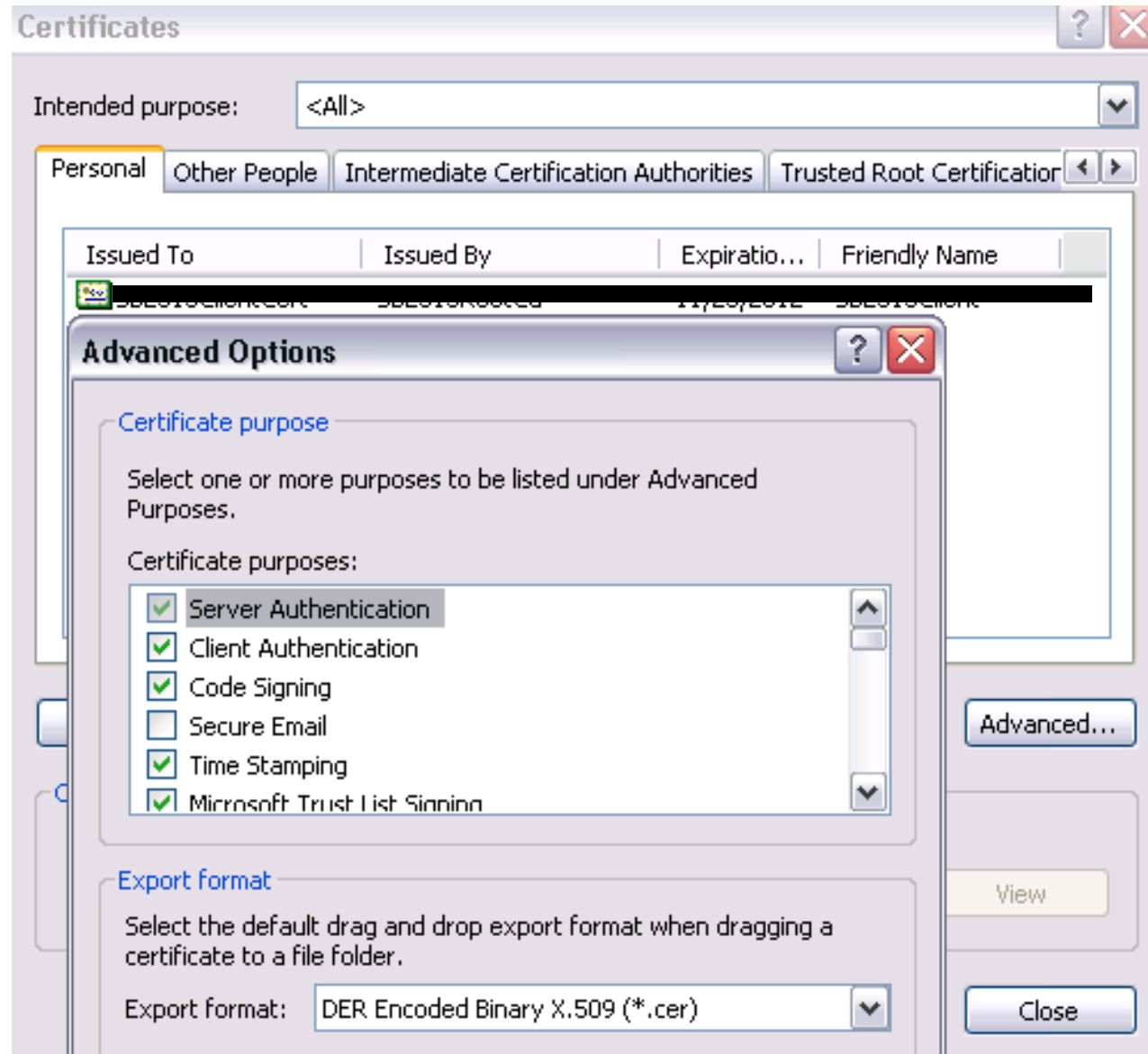


Example: Configuring PComm for Client Certificate Validation

- Example of certificates stored in MSCAPI:



- Note that certificates stored in MSCAPI will need to be assigned a particular purpose (in the case of our certificate, enabling for client authentication).



For Linux clients ...

- Linux tends to be a little easier – place appropriate certificate files into a local keystore (OpenSSL) and make sure the certificate and/or key files are available when executing OpenSSL or x3270 commands
- X3270 seems not to take P12 files; instead, you'll be using commands like:

```
x3270 -certfile mycert.cert -keyfile mykey.key -keypasswd  
string:mypwd -cafile MyRootCA.pem 192.168.0.1
```

Frequently Asked Questions

(or, Questions which are asked with some degree of regularity.)



Frequently Asked Questions

- **Does z/VM SSL use the Crypto Express Cards?**

Answer: No. While SSLSERV and LDAPSRV use CPACF if enabled, z/VM only virtualizes Crypto Express support for hosted operating systems. z/VM's CMS-based servers will not utilize them.

- **Why isn't RACFVM the keystore or certificate store for [insert function here]?**

Answer: RACFVM does not support RACDCERT or the DIGTCERT class, so it cannot provide that functionality.

- **Can SSL servers for different TCP/IP stacks share the same certificate database?**

Answer: Yes, as long as your security policy permits this. Bear in mind that this may require "wildcard" certificates which cover multiple subdomains on your network.

Frequently Asked Questions

- **Is FIPS Mode for SSLSERV the same as the Common Criteria certified configuration?**

Answer: No. FIPS 140-2 and Common Criteria, while analogous in their cipher requirements, are **not** the same – their cipher suite specifications vary. Additionally, FIPS mode may require changes to your certificate database.

Check your security policy; your environment configuration may require either, or both, or something even more stringent.

- **Can RACF and SSL be combined? What implications does this have for configuration?**

Answer: Yes! Just be certain that the SSL Server virtual machines have the authorities it needs in order to do its job. For example:

RACF: Reader access for SSL

- Authorize all users to send files to the SSL machine's reader.
- If there is already a SSL VMRDR profile defined, alter it, by entering:

```
– RAC RALTER VMRDR SSL00001 UACC (UPDATE)
```

```
– RAC RALTER VMRDR SSL00002 UACC (UPDATE)
```

```
– RAC RALTER VMRDR SSL00003 UACC (UPDATE)
```

```
– RAC RALTER VMRDR SSL00004 UACC (UPDATE)
```

```
– RAC RALTER VMRDR SSL00005 UACC (UPDATE)
```

```
– RAC RALTER VMRDR SSLDCSSM UACC (UPDATE)
```


RACF, SSL and VMSEGMENT

- If RACF is being used to control restricted segments with the VMSEGMENT class, give UPDATE authority for SSL to so SSL has shared write access to the DCSS.TCPIP segment.
 - RAC RDEFINE VMSEGMENT DCSS.TCPIP UACC(NONE)
 - RAC PERMIT DCSS.TCPIP CLASS(VMSEGMENT) ID(SSL00001)
ACCESS(UPDATE)
 - RAC PERMIT DCSS.TCPIP CLASS(VMSEGMENT) ID(SSL00002)
ACCESS(UPDATE)
 - RAC PERMIT DCSS.TCPIP CLASS(VMSEGMENT) ID(SSL00003)
ACCESS(UPDATE)
 - RAC PERMIT DCSS.TCPIP CLASS(VMSEGMENT) ID(SSL00004)
ACCESS(UPDATE)
 - RAC PERMIT DCSS.TCPIP CLASS(VMSEGMENT) ID(SSL00005)
ACCESS(UPDATE)
 - RAC PERMIT DCSS.TCPIP CLASS(VMSEGMENT) ID(SSLDCSSM)
ACCESS(UPDATE)

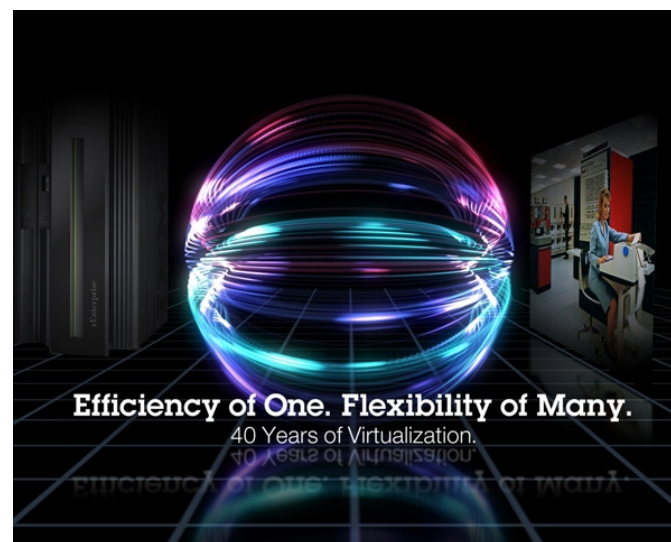
RACF, SSL, and RACROUTE

- To record activity in the RACF system audit trail, they must each be authorized. Enter:
 - RAC SETROPTS CLASSACT(FACILITY)
 - RAC RDEFINE FACILITY ICHCONN UACC(NONE)
 - RAC PERMIT ICHCONN CLASS(FACILITY) ID(SSL00001) ACCESS(UPDATE)
 - RAC PERMIT ICHCONN CLASS(FACILITY) ID(SSL00002) ACCESS(UPDATE)
 - RAC PERMIT ICHCONN CLASS(FACILITY) ID(SSL00003) ACCESS(UPDATE)
 - RAC PERMIT ICHCONN CLASS(FACILITY) ID(SSL00004) ACCESS(UPDATE)
 - RAC PERMIT ICHCONN CLASS(FACILITY) ID(SSL00005) ACCESS(UPDATE)

RACF, SSL, and Minidisk Access

- If RACF is being used to control minidisk access with VMMDISK class, enable minidisk access for any TCPIP userids that SSL uses.
 - RAC PERMIT 6VMTCP30.491 CLASS (VMMDISK) ID (SSLDCSSM) ACCESS (READ)
 - RAC PERMIT 6VMTCP30.492 CLASS (VMMDISK) ID (SSLDCSSM) ACCESS (READ)
 - RAC PERMIT TCPMAINT.591 CLASS (VMMDISK) ID (SSLDCSSM) ACCESS (READ)
 - RAC PERMIT TCPMAINT.198 CLASS (VMMDISK) ID (SSLDCSSM) ACCESS (READ)
 - RAC PERMIT 6VMTCP30.491 CLASS (VMMDISK) ID (SSL00001) ACCESS (READ)
 - RAC PERMIT 6VMTCP30.492 CLASS (VMMDISK) ID (SSL00001) ACCESS (READ)
 - RAC PERMIT TCPMAINT.591 CLASS (VMMDISK) ID (SSL00001) ACCESS (READ)
 - RAC PERMIT TCPMAINT.198 CLASS (VMMDISK) ID (SSL00001) ACCESS (READ)
 - (repeat for SSL00002, SSL00003 ...)

Summary




Summary

- Protecting connectivity to the hypervisor is a key part of a security policy
- z/VM offers you the controls to restrict ports, enable timeouts, and manage access
- The SSL-TLS server provides a scalable SVM for handling encrypted traffic to the hypervisor
- z/VM 6.3 delivers enhanced function:
 - Better protocol selection
 - Stronger cryptographic modes
 - More flexible certificate management
 - More resilient hashing
- Select the security policy that is right for you and your company

For More Information ...

- **Presentation: “Migrating to Multiple SSL Server Support” [PDF]:** <http://www.vm.ibm.com/devpages/hugenbru/SSLMULTI.PDF>
- **System z Security:** <http://www.ibm.com/systems/z/advantages/security/>
- **z/VM Security resources:** <http://www.vm.ibm.com/security>
- **Security for Linux on System z** (SG24-7728), IBM RedBooks
- **z/VM Secure Configuration Guide:** <http://publibz.boulder.ibm.com/epubs/pdf/hcss0b30.pdf>

Contact Information:

[Brian W. Hugenbruch](#), CISSP
z/VM Security Design and Development
[bwhugen at us dot ibm dot com](mailto:bwhugen@us.ibm.com)
+1 607.429.3660
 @Bwhugen



Dank u

Dutch

Merci

French

Спасибо

Russian

Gracias

Spanish

شكراً

Arabic

감사합니다

Korean

Tack så mycket

Swedish

धन्यवाद

Hindi

תודה רבה

Hebrew

Obrigado

Brazilian
Portuguese

谢谢

Chinese

Thank You

Dankon
Esperanto

ありがとうございます

Japanese

Trugarez

Breton

Danke

German

Tak

Danish

Grazie

Italian

நன்றி

Tamil

děkuji

Czech

ขอบคุณ

Thai

go raibh maith agat

Gaelic