Brian W. Hugenbruch, CISSP
z/VM Security Design and Development
bwhugen@us.ibm.com

Managing Digital Certificates in z/VM

Or, "The Care and Feeding of your z/VM SSL Server"

#WAVV #zVM #IBMSecurity

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

- **Dissecting a Digital Certificate**
- **Exploring the z/VM SSL Server**
- **Managing Digital Certificates in the z/VM environment**
  - ***Configuring the SSL Server***
  - ***Configuring a Client for Secure Communication***
- **Frequently Asked Questions**
- **Advanced Topics**

You received your magnifying glasses at conference registration, right?

AES	Advanced Encryption Standard	MAC	Message Authentication Code
ARL	Authority Revocation List	MDC	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	OCSP	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	PCIX 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		

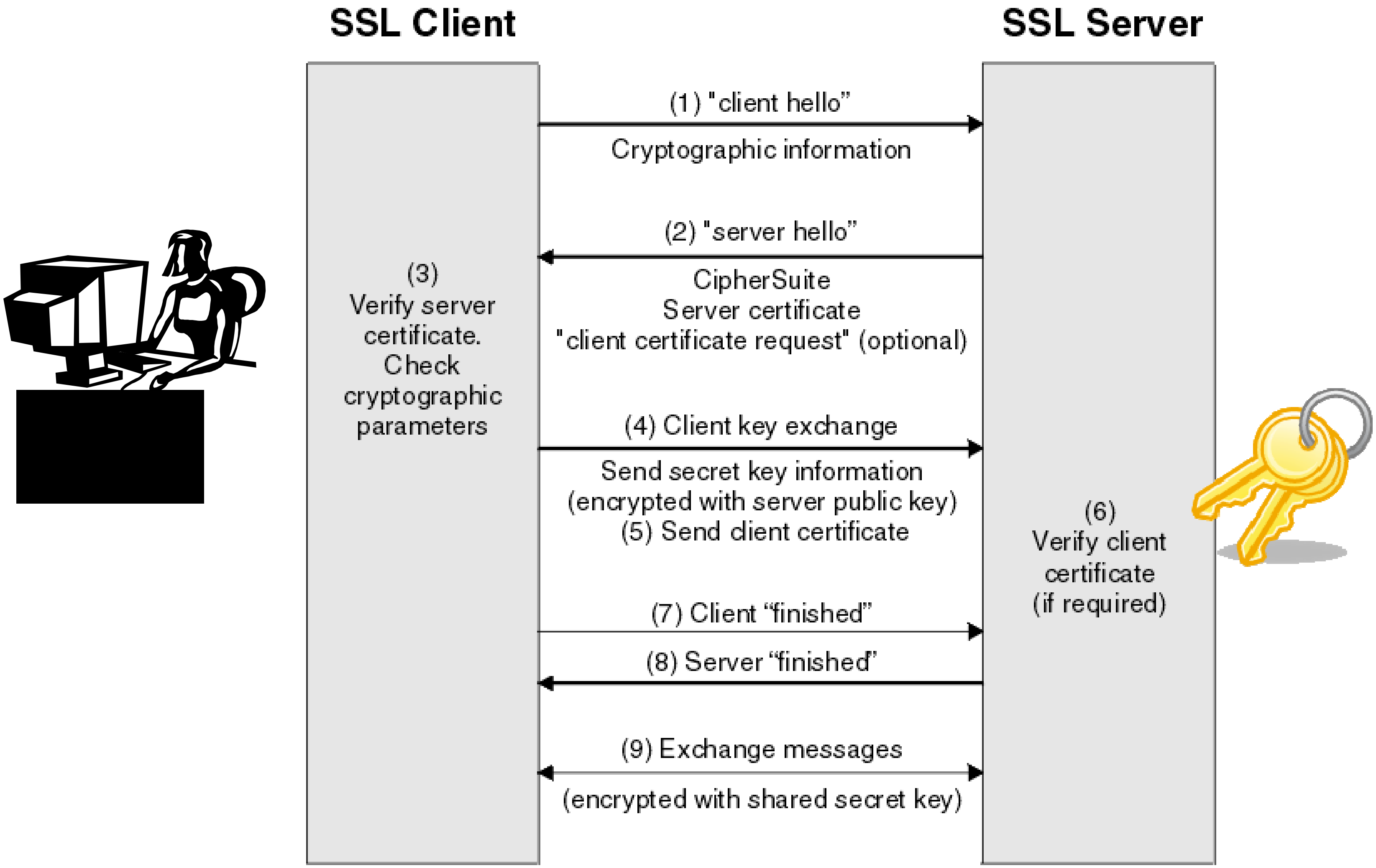
Dissecting a Digital Certificate

(or, The Importance of Being Secret)

(Actually, it’s written in ROT39, not ROT13.)

Vasbezngvba **frphevgl** qrcraqf hcba **pelcgbtencul** orpnhfr fbzrgvzrf vg’f uneq gb xrrc frpergf.

Information **security** depends upon **cryptography** because sometimes it’s hard to keep secrets.



SSL Client

SSL Server

(1) "client hello"

Cryptographic information

(2) "server hello"

CipherSuite
Server certificate
"client certificate request" (optional)

(3)
Verify server certificate.
Check cryptographic parameters

(4) Client key exchange

Send secret key information
(encrypted with server public key)
(5) Send client certificate

(6)
Verify client certificate
(if required)

(7) Client "finished"

(8) Server "finished"

(9) Exchange messages

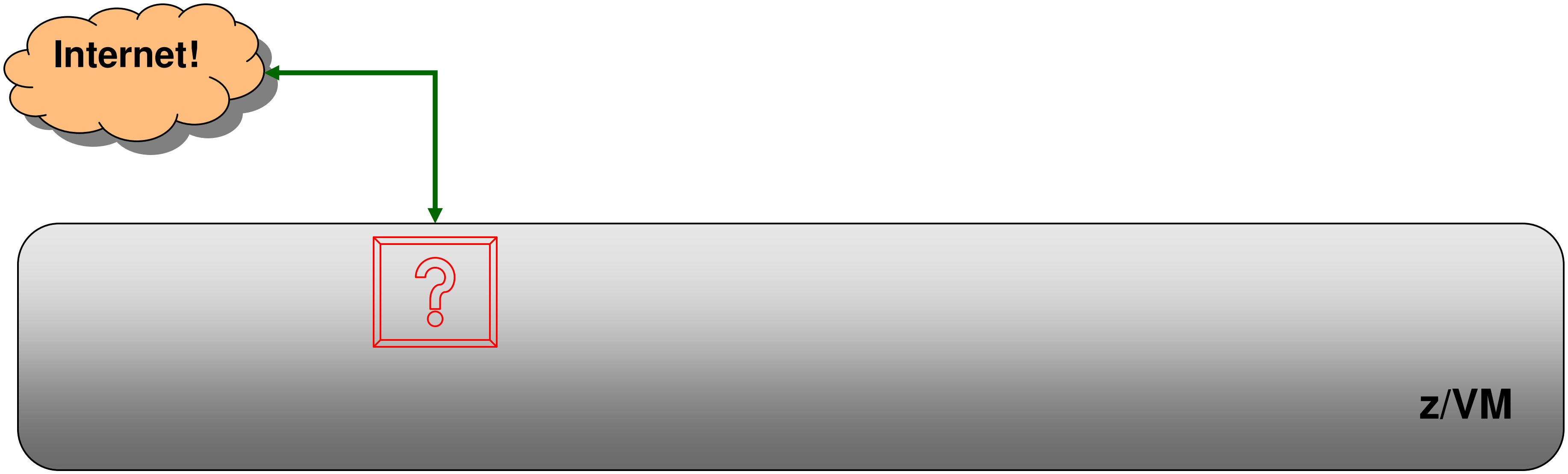
(encrypted with shared secret key)

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

How does this apply to System z Virtualization?



- **The mandate comes down: "secure all connections."**
  - Company policy, industry standards, federal regulations
  - Guests have security mechanisms, but what about the virtualization layer?

- What handles securing TCP/IP traffic?
  - Where do the certificates go?
  - What standards can be met?

Exploring the z/VM SSL Server

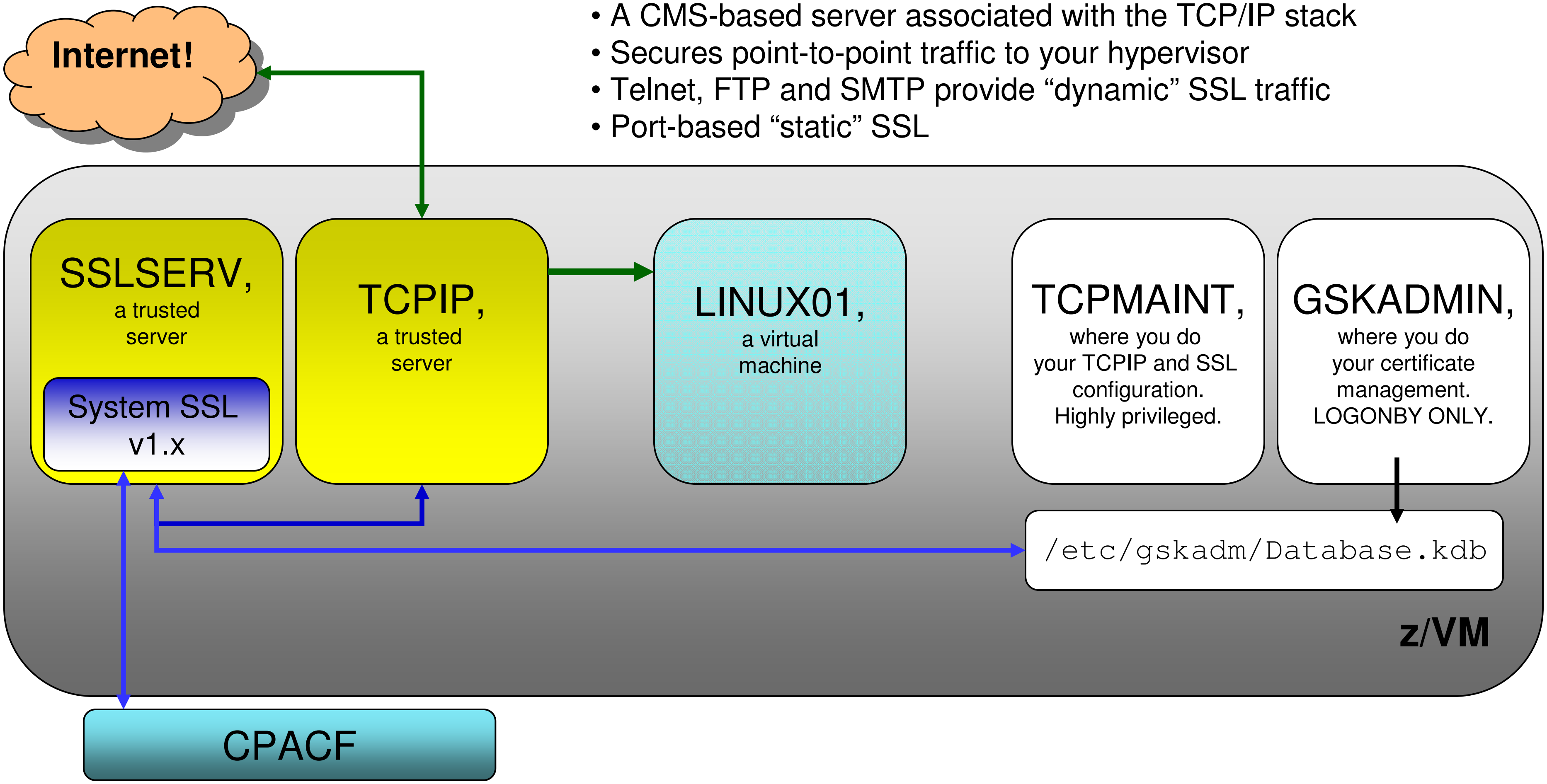
(or, “We have an SVM for that”)

[redacted]

The z/VM SSL Server

The z/VM SSL Server:

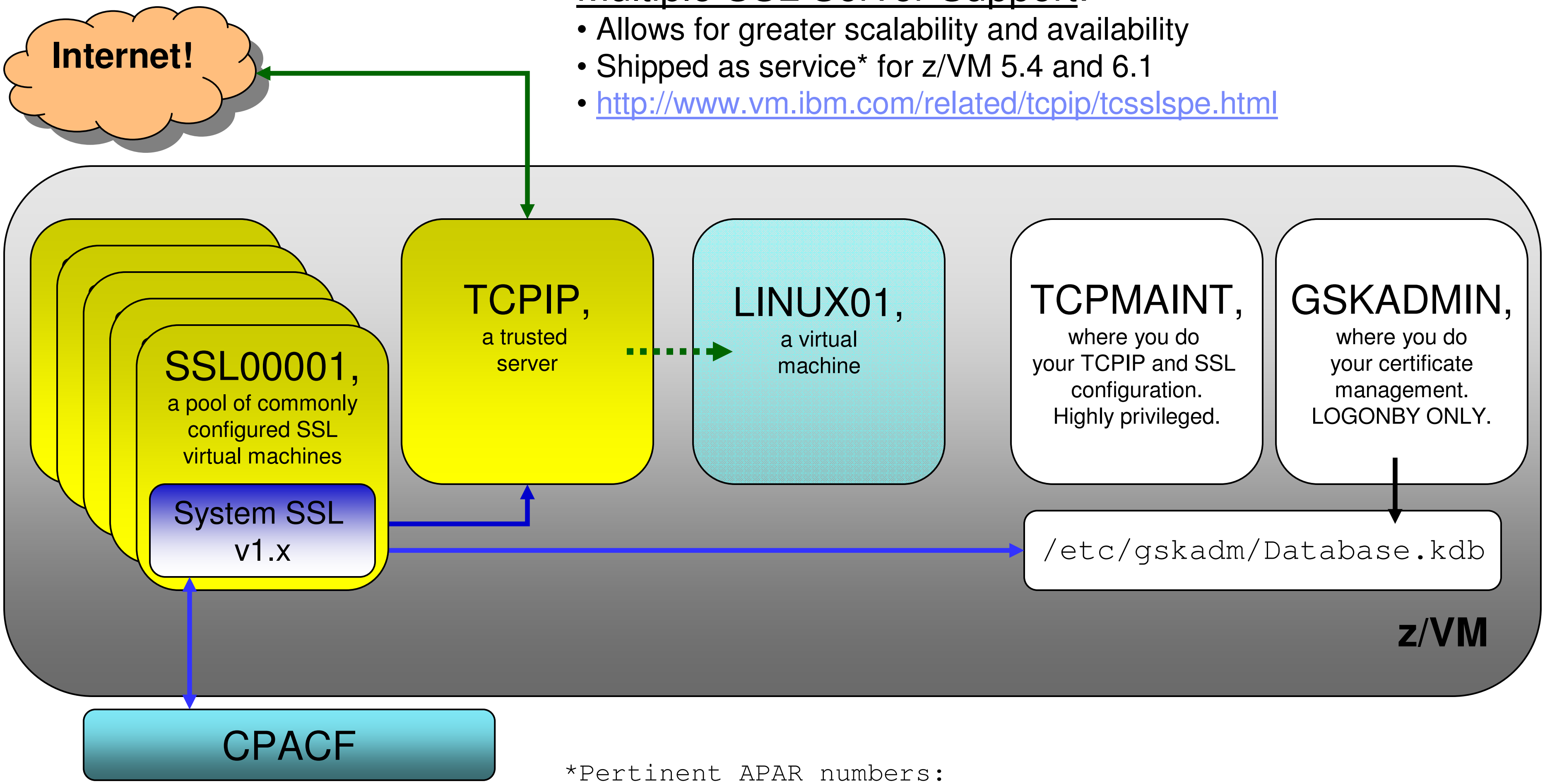
- A CMS-based server associated with the TCP/IP stack
- Secures point-to-point traffic to your hypervisor
- Telnet, FTP and SMTP provide “dynamic” SSL traffic
- Port-based “static” SSL



The z/VM SSL Server

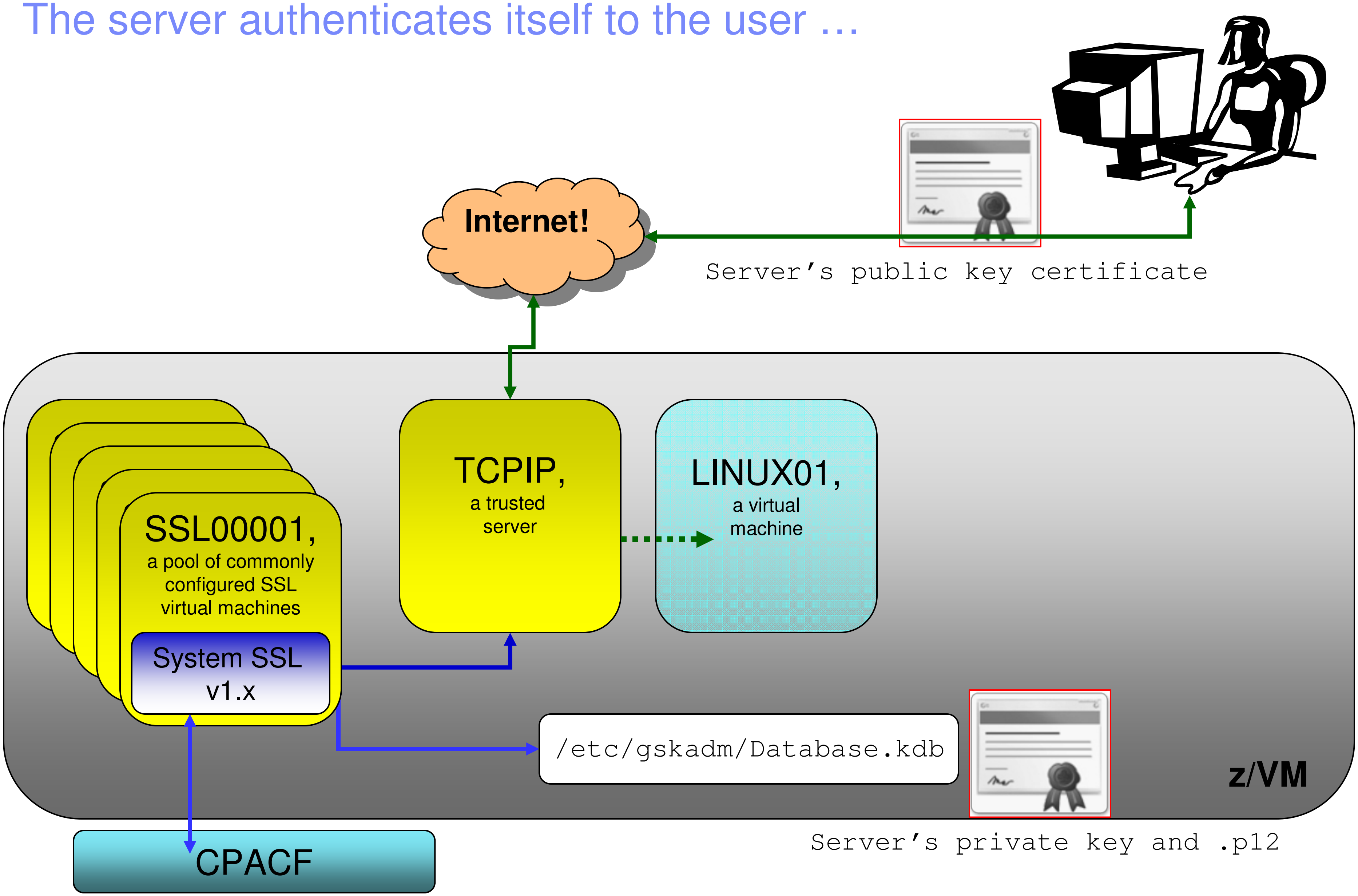
Multiple SSL Server Support:

- Allows for greater scalability and availability
- Shipped as service* for z/VM 5.4 and 6.1
- http://www.vm.ibm.com/related/tcpip/tcsslspe.html


Internet!
SSL00001,
a pool of commonly configured SSL virtual machines
System SSL v1.x
TCPIP,
a trusted server
LINUX01,
a virtual machine
TCPMAINT,
where you do your TCPIP and SSL configuration. Highly privileged.
GSKADMIN,
where you do your certificate management. LOGONBY ONLY.
/etc/gskadm/Database.kdb
z/VM
CPACF

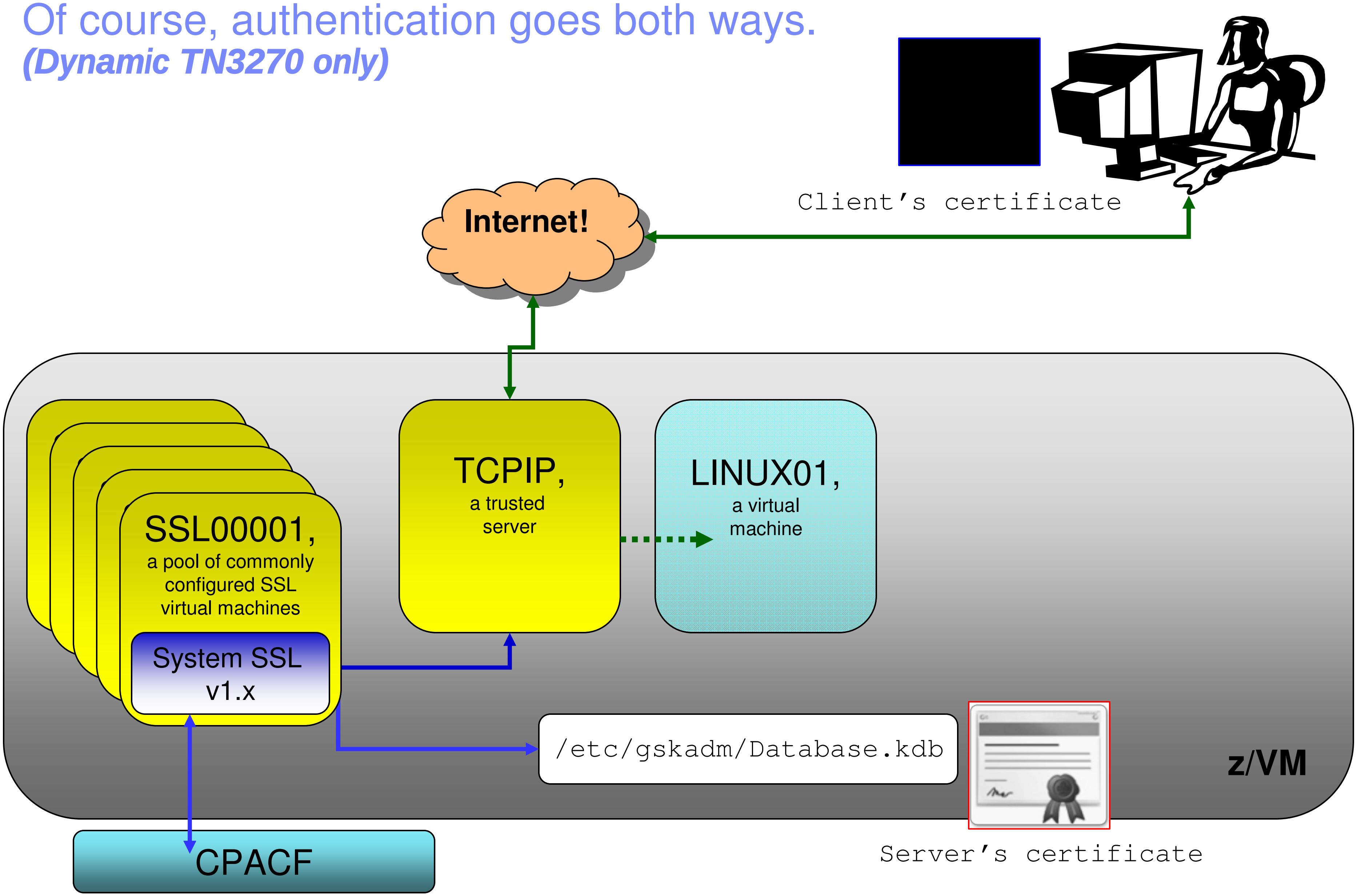
```
*Pertinent APAR numbers:
- PK97437: SSLADMIN, TCPRUN and Related Packaging Changes
- PK97438: SSLSERV Module Updates
- PK75662: TCPIP Module Updates
```

The server authenticates itself to the user …



Of course, authentication goes both ways.

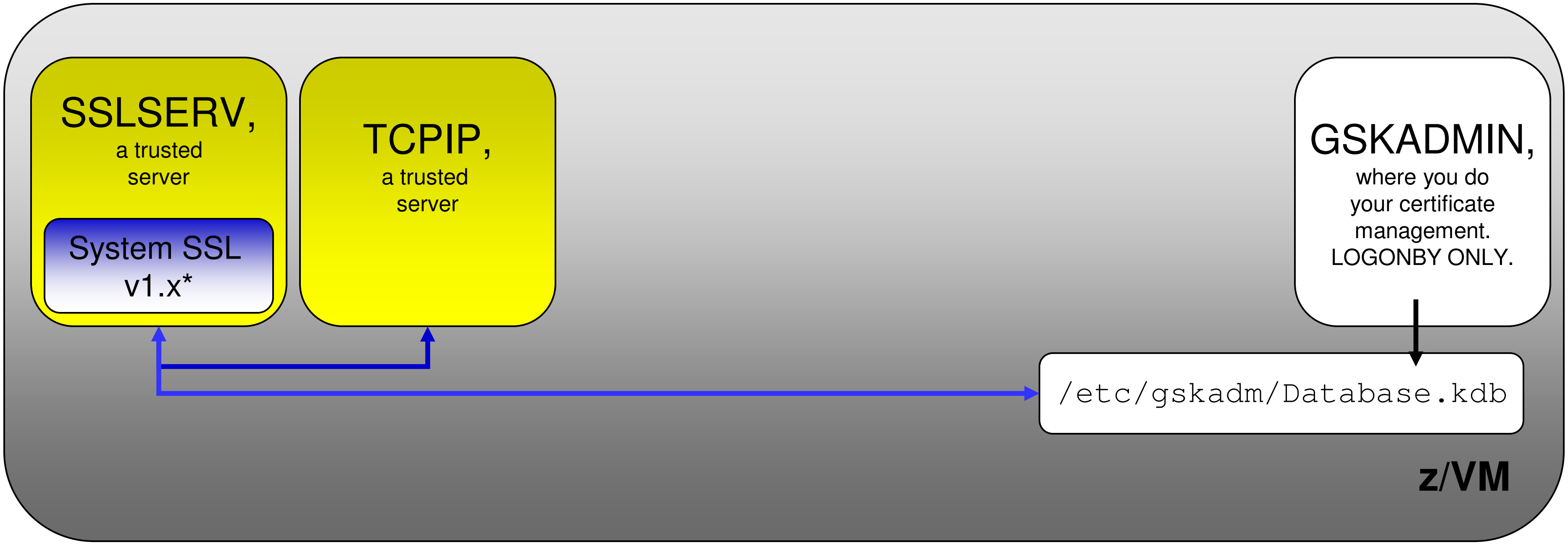
(Dynamic TN3270 only)



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 can manage ***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

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:

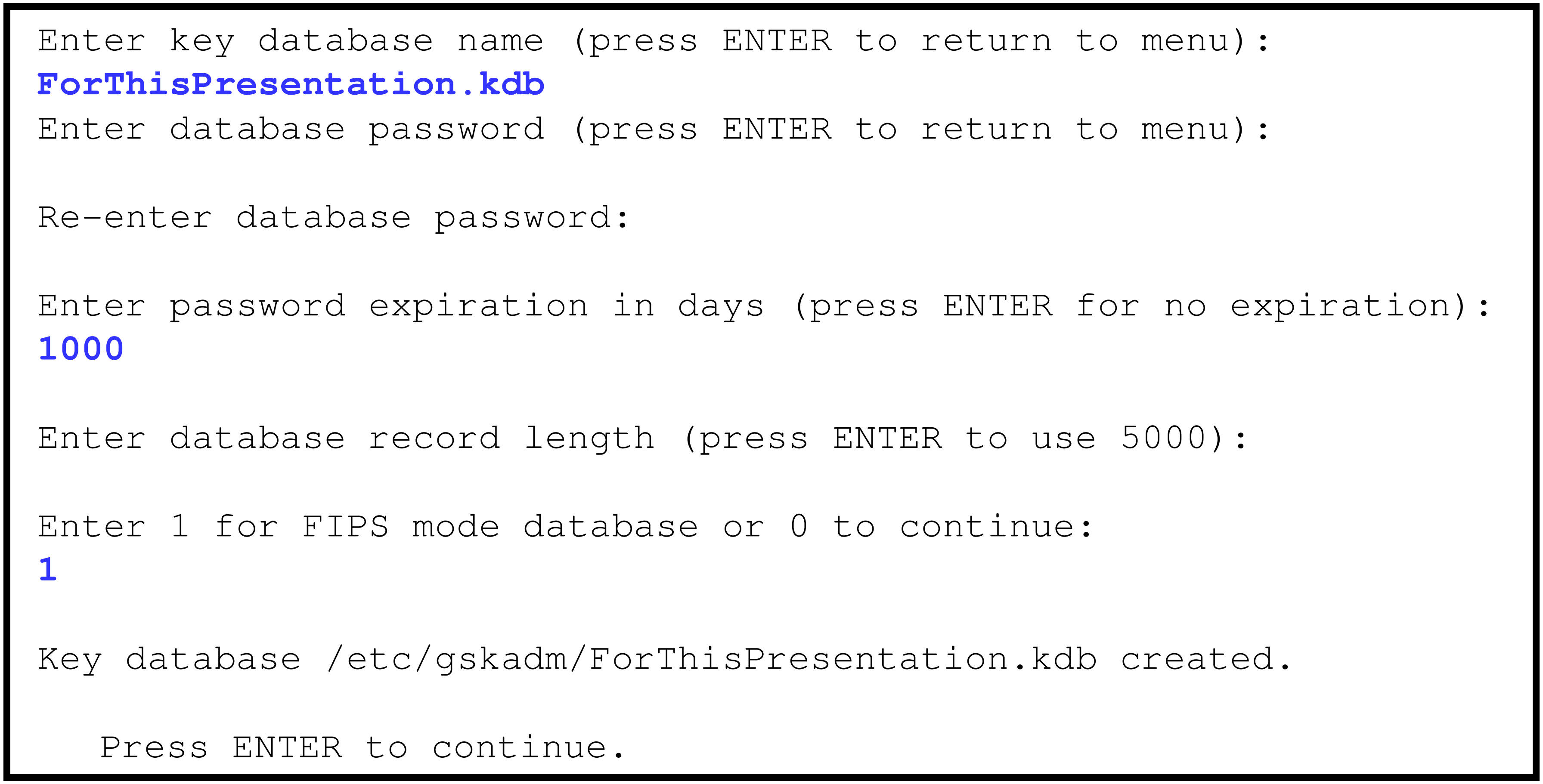
```
gskkyman
```

```
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.
```

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***

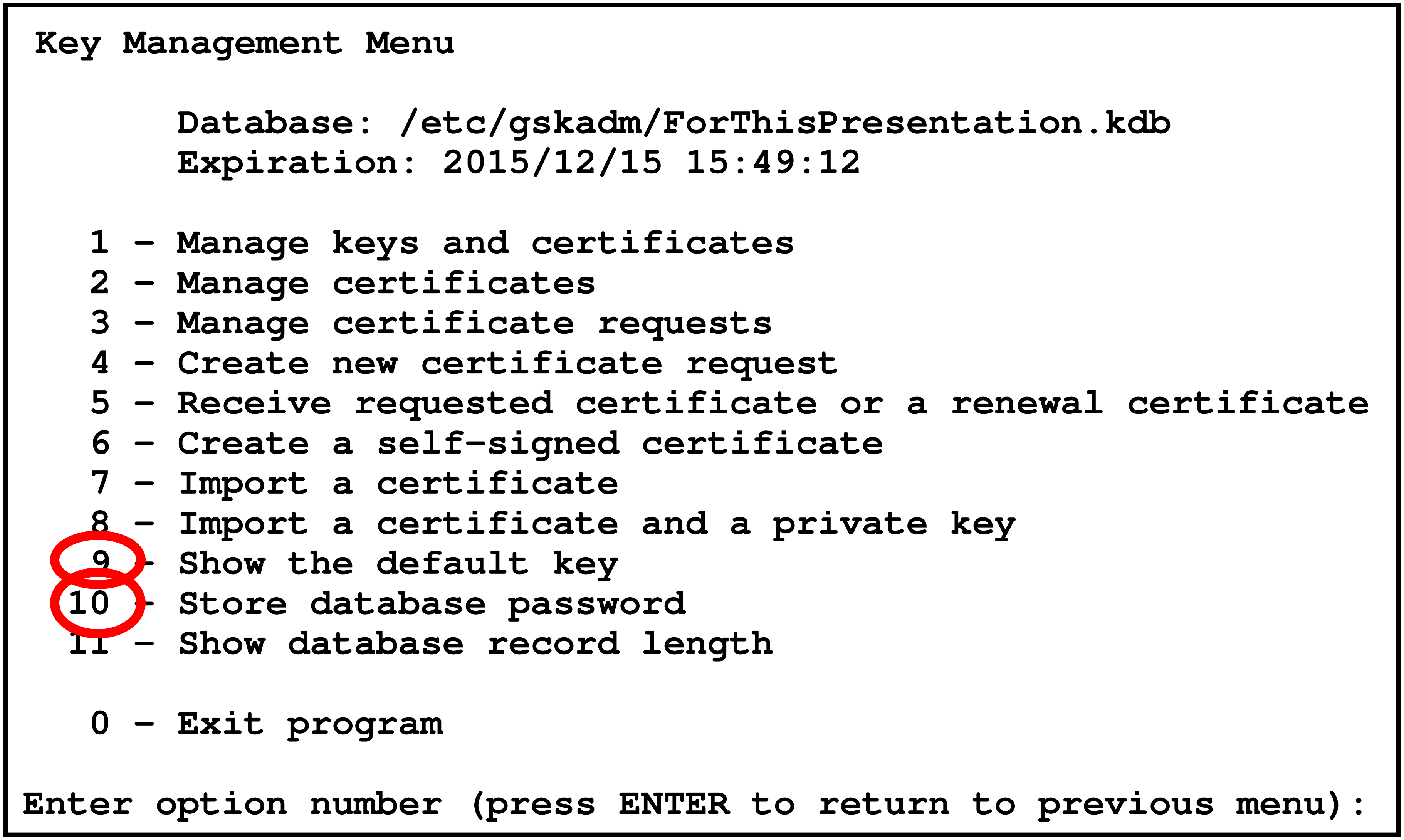
[redacted]

– 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 bfsline 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+OgAwIBAgIDEAAHMA0GCSqGSIb3DQEBBQUAMIGcMQswCQYDVQQGEwJV
UzERMA8GA1UECBMITmV3IFlvcmsxETAPBgNVBAcTCEVuZGljb3R0MRgwFgYDVQQK
Ew96Vk0gRGV2ZWxvcG1lbnQxDDAKBgNVBAsTA1NTTDEcMBoGA1UEAxMTQnJpYW4g
Vy4gSHVnZW5icnVjaDEhMB8GCSqGSIb3DQEJARYSYndodWdlbkB1cy5pYm0uY29t
MB4XDTEzMDMyNzE3NTMwOVoXDTE0MDMyNzE3NTMwOVowZjELMAkGA1UEBhMCVVMx
ETAPBgNVBAgTCE5ldyBZb3JrMRgwFgYDVQQKEw96Vk0gRGV2ZWxvcG1lbnQxDDAK
BgNVBAsTA1NTTDEcMBoGA1UEAxMTQnJpYW4gVy4gSHVnZW5icnVjaDCCAiIwDQYJ
KoZIhvcNAQEBBQADggIPADCCAgoCggIBAPb/rg0V3++X7lJ2N7xDcktOeSxjvlkA
2n1HRnb3VCO5HlROKet1Oxd4QhBoLWL+GJgo2vY1jBM3fP/KX6lFYcCXj+zwUMIu
+eGOB+DRmVfL4cZnVYEkWTgBnEKRLQEIJ+KmgGnJgtJYRjdZ54kaXlgB2obupCui
099iYZDVkzdiizu/SlrM0dP3jz3p6MRWMRN4f9uf6a4bNd+bCI7HnVLsLvfp3wCW
MUtKjAx6snZPAgMBAAGjezB5MAkGA1UdEwQCMAAwLAYJYIZIAYb4QgENBB8WHU9w
ZW5TU0wgR2VuZXJhdGVkIENlcnRpZmljYXRlMB0GA1UdDgQWBBTWiatA5nzhUruN
dS9/TJPz/F3PnTAfBgNVHSMEGDAWgBT7hRhg6eCiBsJPY2+4DBIzqS8CEzANBgkq
hkiG9w0BAQUFAANBAAwiC+Z/IvzFImTcgvNC3PH99c9u8J0u5KiAT39c6ia+FuZZ
i3tBDKoSBCfy2kBBc4k6CQNyazovVSUtJrJquQU=
-----END CERTIFICATE-----
```

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

[redacted]

Certificate Management for z/VM SSL

A few final thoughts:

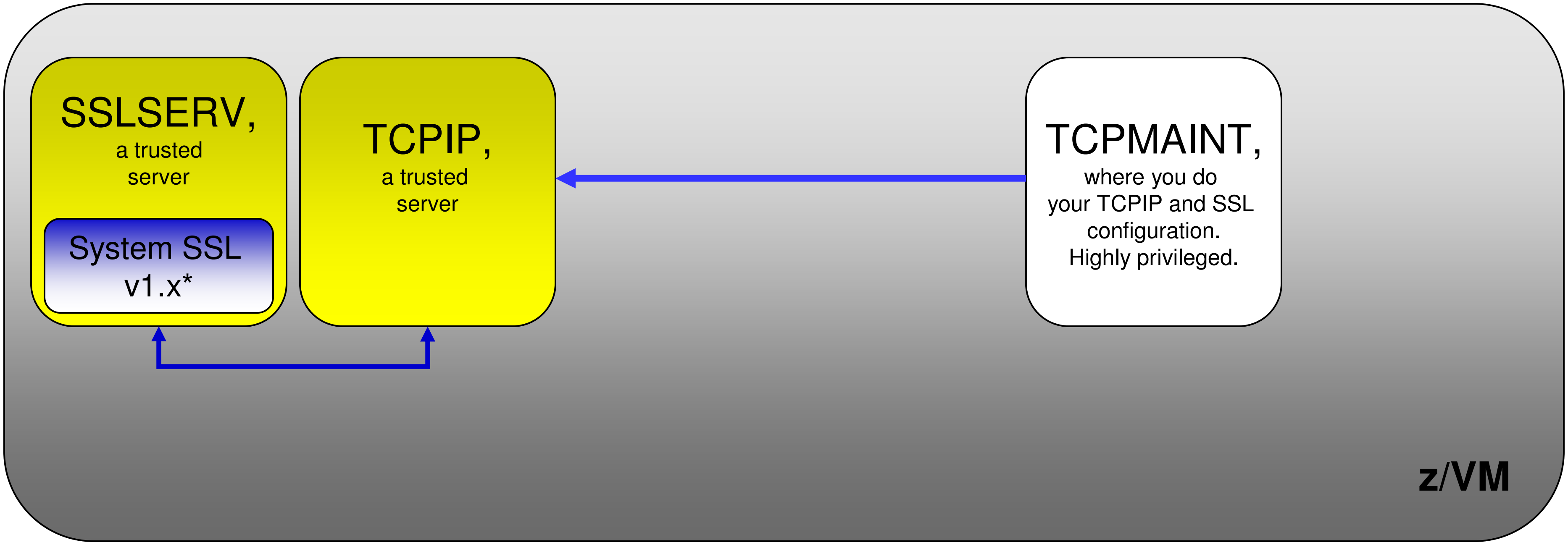
- When making changes to a certificate database in use by a running SSL Server virtual machine, be sure to issue an SSLADMIN REFRESH from a privileged userid.
- The server will reload its environment without interrupting existing secure connections.
- Important for when certificates need to be renewed, 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 ***This tag is required; otherwise, the SSL server / pool cannot be identified during stack initialization!***
:Timestamp.	On/Off for timestamps on terminal messages and cmd responses
:Timezone.	Set timezone of server
:Vmlink.	Sets a Pool member's SFS space

Configuring the SSL Server

- Configuration can be done either statically (through the `DTCPARMS` file) or dynamically at start-up (through the `VMSSL EXEC`). Either uses the same operands (see right)

- Settings are used for all servers in an SSL pool

- SSLSERV ***security policy*** cannot be fine-tuned dynamically; plan ahead for the security you will need!

Configuring the 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 strength set, per the above – but not both.

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

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.
```

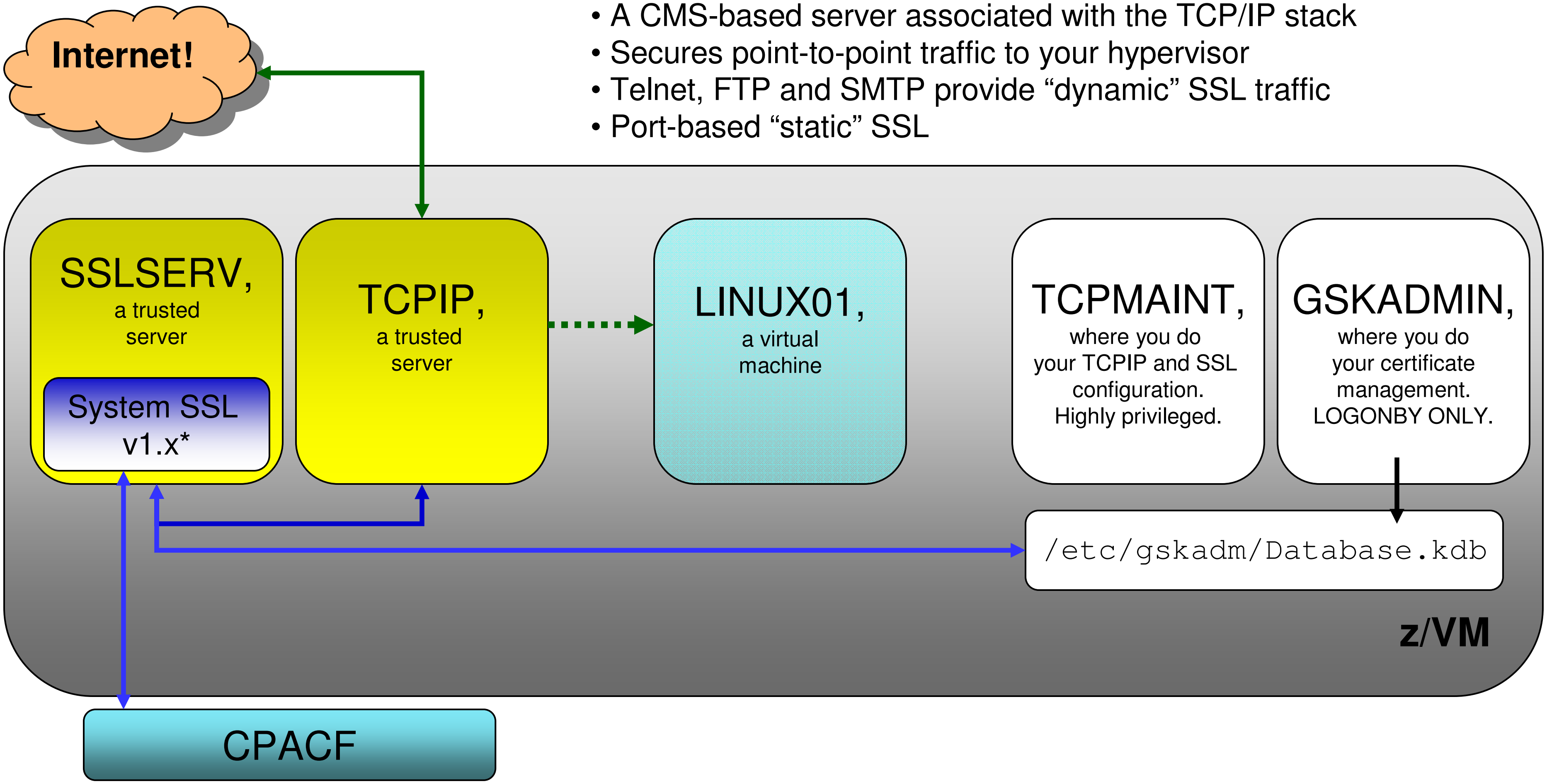
- **… and SSL Server Support**
  - DTCPARMS: **FIPS** or
  - VMSSL: **FIPS**

- Automatically configures required cipher suites to meet 140-2 standards.

Federal Information Protection Standard (FIPS) 140-2

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

If we specify ...

Default settings

```
RC4_128_SHA RC4_128_MD5 RSA_AES_256
DH_DSS_AES_256 DH_RSA_AES_256
DHE_DSS_AES_256 DHE_RSA_AES_256
RSA_AES_128 DH_DSS_AES_128
DH_RSA_AES_128 DHE_DSS_AES_128
DHE_RSA_AES_128 3DES_168_SHA
DHE_RSA_3DES DHE_DSS_3DES
DH_RSA_3DES DH_DSS_3DES  DES_56_SHA
DHE_RSA_DES DHE_DSS_DES DH_RSA_DES
DH_DSS_DES RC4_40_MD5 RC2_40_MD5
NULL_SHA NULL_MD5 NULL
```

Configuring the SSL Server

If we specify ...

Default settings

FIPS mode

```
RSA_AES_256
DH_DSS_AES_256
DH_RSA_AES_256
DHE_DSS_AES_256
DHE_RSA_AES_256
RSA_AES_128
DH_DSS_AES_128
DH_RSA_AES_128
DHE_DSS_AES_128
DHE_RSA_AES_128
3DES_168_SHA
DHE_RSA_3DES
DHE_DSS_3DES
DH_RSA_3DES
DH_DSS_3DES
```

Configuring the SSL Server

If we specify ...

Default settings

FIPS mode

EXEMPT MEDIUM

```
RSA_AES_256
DH_DSS_AES_256
DH_RSA_AES_256
DHE_DSS_AES_256
DHE_RSA_AES_256
3DES_168_SHA
DHE_RSA_3DES
DHE_DSS_3DES
DH_RSA_3DES
DH_DSS_3DES
```

Configuring Secure Connectivity

- **TCPIP Configuration**
  - http://www.vm.ibm.com/related/tcpip/tcspeslc.html
  - `SSLLIMITS` (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 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)

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

[redacted]

http://w3.vm.ibm.com/devpages/CIBULAMA/tcspecsa.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:

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 TCPIP 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

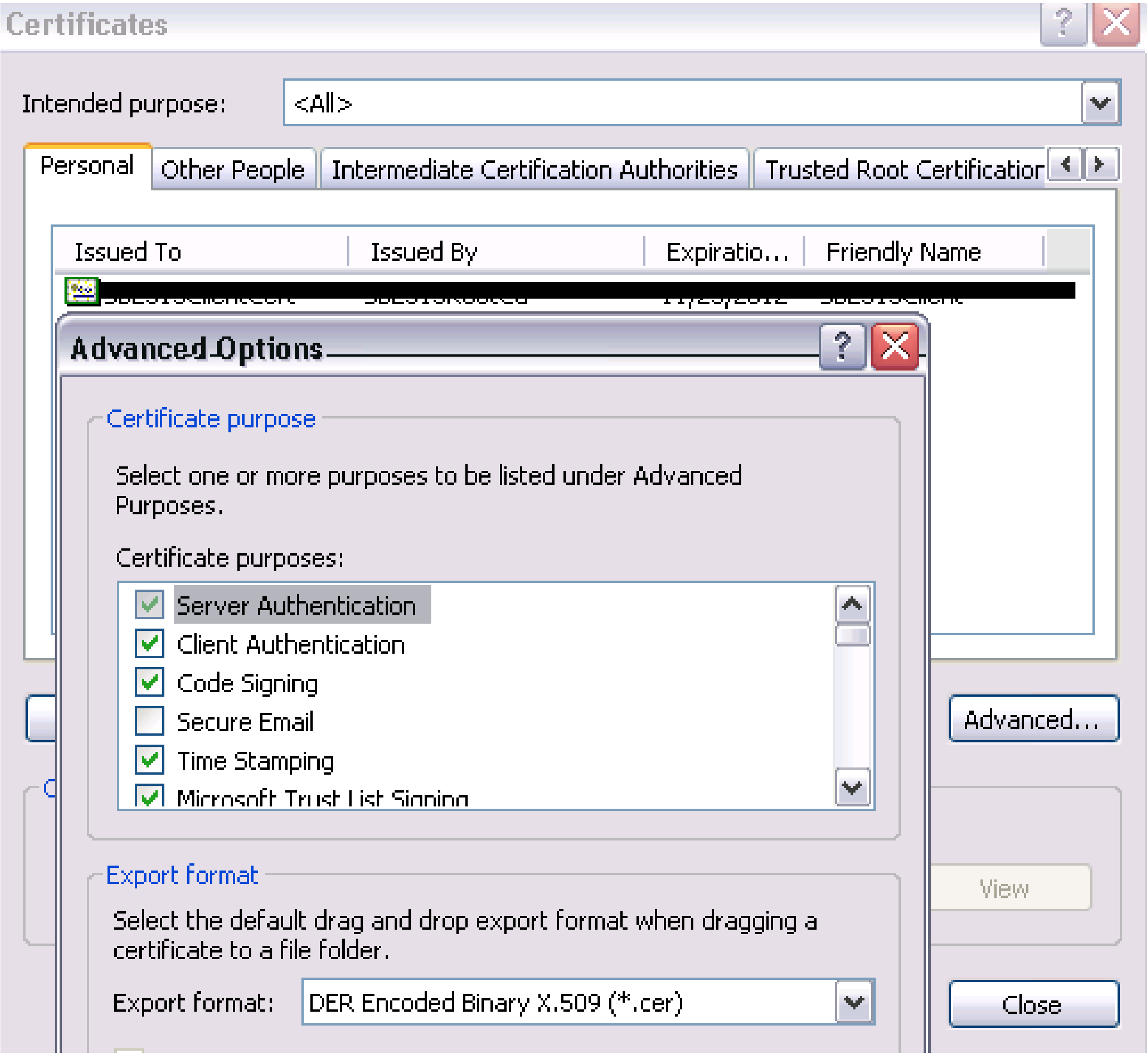
Example: Configuring PComm for Client Certificate Validation

- 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.
- “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).



Certificates

Intended purpose: <All>

Personal | Other People | Intermediate Certification Authorities | Trusted Root Certificatior

Issued To	Issued By	Expiratio...	Friendly Name
[redacted]			

Advanced Options

Certificate purpose

Select one or more purposes to be listed under Advanced Purposes.

Certificate purposes:

☑ Server Authentication
☑ Client Authentication
☑ Code Signing
☐ Secure Email
☑ Time Stamping
☑ Microsoft Trust List Signing

Export format

Select the default drag and drop export format when dragging a certificate to a file folder.

Export format: DER Encoded Binary X.509 (*.cer)

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.

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.

Frequently Asked Questions

- **Can I run both SSLSERV and an SSL pool for the same TCP/IP stack?**
  Answer: Not concurrently. Configuration requirements prevent this.

- **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.

- **Can’t I just migrate my z/OS certificate database into z/VM?**
  Answer: It may be technically feasible, but there may be unanticipated consequences from doing this …

For More Information …

- **System z Security:** http://www.ibm.com/systems/z/advantages/security/
- **z/VM Security resources:** http://www.vm.ibm.com/security
- ***z/VM Security*** (SG24-7471), IBM RedBooks
- ***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
+1 607.429.3660
Twitter: @Bwhugen

[redacted]

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

Dankon
Esperanto

Thank You

ありがとうございます
Japanese

Tak
Danish

Trugarez
Breton

Danke
German

Grazie
Italian

நன்றி
Tamil

děkuji
Czech

ขอบคุณ
Thai

go raibh maith agat
Gaelic

Advanced Topics

Because sometimes not everything fits in the main presentation.

1. **How do I export .p12 files from my z/VM 5.3 (Linux-based) SSL Server?**

2. **How can I use *gskkyman* to become my own Certificate Authority?**

3. **How do I migrate to Multiple SSL Server Support?**

How do I export .p12 files from z/VM 5.3's Old SSL Server?

1. How To Export .P12 Files from z/VM 5.3

- **History:** Prior to z/VM 5.4, the z/VM SSL Server's code ran inside of a Linux guest which communicated with the z/VM TCP/IP stack. The crypto and certificate management was structured on ***ikeyman*** instead of ***gskkyman***.

- **Problem**: z/VM 5.3's `SSLADMIN EXPORT` command did not allow for exporting certificates with associated keys … only certificate files.

- **Solution**: `APAR PK75661`
  - New .RPM files for both SSLSERV and GSKit
  - Adds new **`SSLADMIN EXPORT ... WITHKEY`** option

- **Helpful links:**
  - http://www.vm.ibm.com/related/tcpip/pk75661.html
  - http://www.vm.ibm.com/related/tcpip/tc53crmg.html

1. How To Export .P12 Files from z/VM 5.3

1. Install new .RPM files
   - Reconfigure Linux guest for alternate connectivity (modsymlinks)
   - Backup existing certificate database files
   - FTP .RPM files onto Linux guest
   - Uninstall old .RPM files (first SSL, then GSKit)
   - Install new .RPM files (first GSKit, then SSL)
   - Restore certificate database files
   - Reconfigure Linux guest for SSLSERV mode (modsymlinks)
   - Restart SSL server

2. Logon TCPMAINT

3. Disable SSL server tracing:

```
ssladmin notrace
```

1. How To Export .P12 Files from z/VM 5.3

4. Disable console spooling for this userid

5. Export certificate with associated key:

```
SSLADMIN EXPORT <filename> <filemode> CERTWKEY <tlslabel> <password>
```

Notes:

- <filename> and <filemode> represent the target CMS file to be created.
- The new file will be of filetype “P12”
- <tlslabel> represents the certificate label specified in your certificate database.
- The <password> will be associated with your new file.
- <password> is case-sensitive, and can be comprised of multiple tokens; leading and trailing blanks are removed.

6. Send your new file to your modern z/VM system (5.4 onward)

1. How To Export .P12 Files from z/VM 5.3

7. Store the P12 file in an appropriate BFS directory, e.g.

```
openvm putbfs CERTWKEY P12 A /etc/gskadm/certwkey.p12
     (bfsline none
```

8. Using gskkyman (as shown on previous slides), import the .p12 file into the certificate database

9. Update appropriate config files to use the new certificate label (e.g., PROFILE TCPIP, SRVRFTP CONFIG); or update servers dynamically / use SSLADMIN REFRESH

- Cleanup Notes:
  - <password> should no longer be required. If <password> is maintained, though, use appropriate measures to ensure it is adequately protected
  - Be certain that any console or other files that contain your certificate-with-key password(s) are properly discarded or erased

How Can I Use gskkyman to Become My Own Certificate Authority?

2. How To Be Your Own Certificate Authority

- **Problem**: Obtaining certificates from a trusted Certificate Authority is good for external-facing zones … but paying money for the privilege of an officially recognized certificate may be beyond the needs of your environment.

- **Solution**: Be your own Certificate Authority
  - Can answer certificate requests using ***gskkyman***
  - Useful for test-oriented or internal-only environments

- **References:**
  - ***z/VM TCP/IP Planning and Customization***, Chapter 18
  - ***z/VM TCP/IP LDAP Administrator's Guide***, Chapter 15

2. How To Be Your Own Certificate Authority

2. How To Be Your Own Certificate Authority

[redacted]

[redacted]

2. How To Be Your Own Certificate Authority

How Do I Migrate to Multiple SSL Server Support?

Multiple SSL Server Support

Installation and Migration

- PTFs:
  - **UK59535** – Release 540 (available 18 Aug 2010)
  - **UK59536** – Release 610 (available 18 Aug 2010)

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

- FIPS 140-2 Enablement was released as an APAR to z/VM 610 only
  - **PM10616** (and several Binder / CMS APARs for System SSL)

- ***All available as part of the base code of z/VM 6.2***

Multiple SSL Server Support

Installation and Migration

- If the SSL server is not currently in use on the system, service can be applied without the need for up-front configuration change

- If the SSL server **IS** in use, configuration must be done before issuing PUT2PROD or TCP2PROD
  - Otherwise, the SSL server will not properly initialize and will no longer function

Multiple SSL Server Support

Installation and Migration

- New server virtual machine: SSLDCSSM
  - **<u>Required</u>** whether using single-server support or multiple!
  - Must be defined in user directory
  - DTCPARMS definitions in new IBM DTCPARMS file

- New SSL pool: SSL*
  - Needed to run Multiple SSL Server Support
  - Should be defined in user directory
  - DTCPARMS definitions included in new IBM DTCPARMS file

- Standalone Server note:
  - The existing :nick.SSLSERV :type.server entry for the SSLSERV user ID now is listed in this file in comment form only

Multiple SSL Server Support

Installation and Migration

- `SSLPOOL SAMPEXEC`
  - generates planning information to assist with defining a "pool" of SSL server machines for a given TCP/IP stack virtual machine
    - Use the “NOPOOL” option for planning the new config of a single server
  - sample CP directory definitions, sample DTCPARMS file entries
  - Can also enroll subject server machines in a designated SFS file pool, and establish files and authorizations to facilitate their use
    - **VMSYS** filepool used by default

- Shipped as a sample exec

- Rename, move to 191 disk

- http://www.vm.ibm.com/related/tcpip/tcspecsp.html

Multiple SSL Server Support

Installation and Migration

[redacted]

- http://www.vm.ibm.com/related/tcpip/tcspecsp.html

For more information …

- For the full presentation on ‘Migrating to Multiple SSL Server Support,’ see the following presentation [PDF]:
  - http://www.vm.ibm.com/devpages/hugenbru/SSLMULTI.PDF

Bonus Slide!
Reconfiguring z/VM applications dynamically for TLS

- 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).

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

Dankon
Esperanto

Thank You

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