Introduction to SSL/TLS Certificate Management in z/VM

James Vincent
July 2026

Agenda

- Overview & Terms
- Why secure your z/VM system
- Setting up for certificates and secure connections (z/VM SSL)
- Managing your certificates

Overview

Securing your system includes:
TCPIP, OpenExtensions/BFS, Secure Sockets, Cryptography, Data Encryption, Cipher Suites…

It is a *complicated* collection of topics!

- If you are planning to be a Cyber Security expert, then most will begin to make sense as you *learn all the details*
- If you are a z/VM System Admin, these topics can be a challenge at first and take time to learn to even understand the *basics*

Common Terms

Terms

SSL – Secure Sockets Layer
An encryption-based internet security protocol; the “original”

TLS – Transport Layer Security
Widely adopted and more modern security protocol

- TLS v1.3 is currently the latest version
- z/VM currently only supports up to TLS v1.2; v1.3 will be “soon”

SSL/TLS, SSL and TLS are most times used interchangeably to mean “secure” or “secure transport”

Terms

Certificates / **TLS/SSL Certificates** / **Secure Certificates** - Contains a one or more server / host / service identities and public key

Public Key – what remote device/apps will use to verify the server's identity

Certificate Authority (CA) – a **trusted** organization that confirms and verifies an organization requesting a certificate and public key

- If I asked for https://velocitysoftware.com, is it really, *really*, them?
- Just having a certificate doesn't verify the target host is trustworthy
- Validating the CA chain is important also

Terms

FIPS - Federal Information Processing Standards

NIST - National Institute of Standards and Technology

GSKADMIN (GSK) - IBM Global Security Kit; how the z/VM certificate key database is managed

GSKKYMAN – The main utility for managing your key database and certificates on GSKADMIN

CERTMGR – A VERY handy, new utility to report on and manage certificates on GSKADMIN

Why Secure?

Every system should set up for secure network access, including z/VM!

In today's world, HTTP**S**/FTP**S**/TLS-Telnet is nearly a requirement

Securing all data-in-flight is paramount to prevent people stealing corporate data – and login credentials!

Threats are not just external to your company. There are internal threats too!

z/VM SSL Services
Key Database Setup

GSKADMIN setup

"*z/VM 7.4 TCP/IP Planning and Customization*" is the manual to have on hand for reference!

- Chapter 15. Configuring the SSL Server

The GSKADMIN userid is provided on z/VM

- Default is LOGONBY and IBMVM1 is the userid to use
- The installed PROFILE EXEC will do the setup
  - GSKADMIN uses the Byte File System (BFS) for storage under OpenExtensions (OPENVM) – a Unix-like environment

Once logged on… 

GSKADMIN setup

1. Enter: GSKKYMAN
2. Select: “1 - Create new database”
3. Enter key database name: allcerts.kdb (for example)
4. Enter database password: (pick one you will remember! If you lose the password, you are going to start over!!)
5. Verify password…
6. Expiration in days: Unless you want it, just press ENTER TWICE
7. Enter database record length: just press ENTER TWICE
8. Enter 2 for database types, 1 for FIPS mode database or 0 to continue: ** your certificate requirements will dictate FIPS or not **

GSKADMIN setup

9. Key database /etc/gskadm/allcerts.kdb created. Press ENTER TWICE
10. Select: “10 - Store database password”
11. Database password stored in /etc/gskadm/allcerts.sth. Press ENTER TWICE
12. Select: “4 - Create new certificate request”
    Your following selections will depend on your certificate requirements! ECC is a good choice though
13. Select: “3 - Certificate with an ECC key”
14. Select: “1 - NIST recommended curve”

GSKADMIN setup

15. Select NIST recommended curve type
    secp256r1 (or higher) would be good
16. Enter request file name – pick a name to find later, like
    NEWCERT.REQ
17. Enter label – this is an eye-catcher label for the certificate, 1 to 8
    characters. Consider a system/cert name, like: SYS1CERT

You will then be prompted for details on the organization / host for the certificate authority to use to confirm that it is valid

GSKADMIN setup

20. Common name (required): Enter main IP or hostname
21. Organizational unit:
22. City:
23. State/Province:
24. Country/Region:
25. Enter 1 to specify subject alternate names or 0 to continue:
    If the system hosts other IP address or hostnames, use 1 and follow the prompts

GSKADMIN setup

When done entering any subject alternate names, you will see

- Please wait .....
- Certificate request created.
- Press ENTER to continue.

Prese ENTER TWICE

You could select: “3 - Manage certificate requests” and review the request

Select: 0 - Exit program

You now have a Certificate Request in your '/etc/gskadm’ directory

GSKADMIN setup

Enter: EXEC OPENVM LISTFILE /etc/gskadm/ (own
This will start OPENVM and run LISTFILE

On a new system, you would see four files. Three are for your key database and one is your new certificate request

```
Directory = '/etc/gskadm'
User ID    Group Name  Permissions Type  Path name component
gskadmin   security    rw- --- ---  F    'allcerts.kdb'
gskadmin   security    rw- --- ---  F    'allcerts.rdb'
gskadmin   security    rw- --- ---  F    'allcerts.sth'
gskadmin   security    rw- r-- r--  F    'NEWCERT.REQ'
```

GSKADMIN setup

Your SSL TCPIP servers will need to be able to access the key DB and saved password files – permissions need to be adjusted

- Permissions are very similar to Linux file permissions

Enter the following – assuming “allcerts.kdb” is your key DB:

EXEC OPENVM PERMIT /etc/gskadm/allcerts.kdb rw- r-- ---

EXEC OPENVM PERMIT /etc/gskadm/allcerts.sth rw- r-- ---

GSKADMIN setup

Enter: EXEC OPENVM LISTFILE /etc/gskadm/ (own

Confirm the permissions for .kdb and .sth files

```
Directory = '/etc/gskadm'
User ID    Group Name  Permissions Type  Path name component
gskadmin   security    rw- r-- ---   F    'allcerts.kdb'
gskadmin   security    rw- --- ---   F    'allcerts.rdb'
gskadmin   security    rw- r-- ---   F    'allcerts.sth'
gskadmin   security    rw- r-- r--   F    'NEWCERT.REQ'
```

VELOCITY SOFTWARE

Certificates

Certificates

You will need to ‘get’ that certificate request out of the BFS and to your GSKADMIN’s 191 disk

- Note! BFS is case-dependent; CASE MATTERS!

```
EXEC OPENVM GETBFS /../VMBFS:VMSYS:GSKSSLDB/NEWCERT.REQ NEWCERT REQ A
```

That will get the NEWCERT.REQ file and copy it to CMS as NEWCERT REQ A

NEWCERT REQ A content would look something like:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBPzCB5gIBADBZMQswCQYDVQQGEwJVUzELMAkGA1UECBMCT0gxFDASBgNVBAcT
C1dlc3RlcnZpbGxlMREwDwYDVQQKEwhTeXMgUHJvZzEUMBIGA1UEAxMLVGVzdCBT
eXN0ZW0wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQNscGyjcpnspDPRfBduDkY
YKCLj6+gOT0RbD/+AoaRZUaoRwMvnrLpzLzxuDoGp4NSgvhYGi7aYuzqQb3PLc9G
oCswKQYJKoZIhvcNAQkOMRwwGjAYBgNVHREEETAPgg1zb21ld2hlcmUuY29tMAoG
CCqGSM49BAMCA0gAMEUCIGFw9tmpe77B3DQwBL74T8sn6k01IvKByJ9WNPnjE5zL
AiEA99KjooDEAIDlIqGW0aNWE3v/u1oFXmnmqf/SzumXqgI=
-----END NEW CERTIFICATE REQUEST-----
```

Certificates

You can: XEDIT NEWCERT REQ A
and copy/paste the contents to an email or attachment to the Certificate Authority

- **Or**, download NEWCERT REQ A via your TN3270 and IND$FILE (or using FTP) and attach it to an email to the Certificate Authority

* Depending on your CA, they may accept an email/attachment or you will need to go to their web site and upload it

Certificates

The Certificate Authority will do their due-diligence and confirm the content of the request. Once completed and accepted, you will likely receive:

- A certificate and private key that satisfies the certificate request
- One or more CA certificates; these identify the signer of the provided certificate/key pair
  - Usually includes a CA ‘signer’ or intermediate certificate and a CA ROOT certificate
  - Most current systems sometimes include the major CA certs, such as Digicert, VeriSign – but some do not
    - If you are using an internal company CA, then you will need the CA certs!
  - Import the CA certs FIRST before importing your cert/key

Certificates

Certificates have a hierarchy to be aware of:

- Root Certificate – the “master” CA certificate
  “DigiCert Global Root G2”
  - Intermediate Certificate – signer/issuer of *your* certificate
    “DigiCert Global G2 TLS RSA SHA256 2020 CA1”
    - Your certificate/key

If you have a new ROOT certificate and a new Intermediate, the ROOT should be added first, then the Intermediate, and then your certificate

- Otherwise, GSKKYMAN will complain!

Certificates

The files you receive from the CA need to get to GSKADMIN

The content of the files dictates how you will get them uploaded. This is *actually the "hardest part" of the whole process*

If you view the files and they have starting/ending tags like:

```
-----BEGIN CERTIFICATE-----
   …data…
-----END CERTIFICATE-----
```

Then they are "plain text" and easier to transfer.

If you can't read the content, then it is Binary data

VELOCITY SOFTWARE

Certificates

Plain text

- Copy/paste the data into a file on GSKADMIN
  XEDIT MYCERT CRT A, add lines to the file and paste data
- Upload – use ASCII character translation

Binary text

- Upload – use BINARY - no character translations

Certificates

Once you get the files uploaded and to GSKADMIN's 191 disk, something like:

```
Cmd    Filename Filetype Fm Format Lrecl     Records      Blocks    Date      Time
       MYCERT   CRT      A1 V         1029          18           2 12/05/25  8:19:47
       DIGI_CA  CRT      A1 V           64          28           1 10/11/23 13:48:45
```

These need to be "put" into the BFS storage for GSKKYMAN to find

EXEC OPENVM PUTBFS MYCERT CRT A /../VMBFS:VMSYS:GSKSSLDB/MYCERT.CRT

EXEC OPENVM PUTBFS DIGI_CA CRT A /../VMBFS:VMSYS:GSKSSLDB/DIGI_CA.CRT

Once they are copied to the directory, it is time to import them to your key DB!

Certificates

1. Enter: GSKKYMAN
2. Select: “2 - Open database”
3. Enter key database name: allcerts.kdb (for example)
4. Enter database password: (enter the one you set)
5. Select: “7 - Import a certificate”
6. Enter import file name: enter your CA Cert file “DIGI_CA.CRT”
7. Enter label: Enter the CA cert title, like “DigiCert Global G2 CA”
8. “Certificate imported.” – Tap ENTER TWICE

Certificates

9. Select: “5 - Receive requested certificate or a renewal certificate”
10. Enter certificate file name: Enter your cert/key file “MYCERT.CRT”
    Once the certificate is imported it is matched with your pending certificate request; If they match, the certificate request is removed
11. Tap ENTER TWICE once imported
12. Select “1 - Manage keys and certificates” to review your cert
    Take note of the Label for your certificate/key! It will match your request label. This is what you will use to reference it for securing services. You can change the label if you wish to.
13. Select: “0 - Exit program” when you are done
14. Enter: LOGOFF
    You are done with GSKADMIN now!

Quiz!

What do you call the entity or signer of your certificate?

What TCPIP utility is used to manage your key DB and certificates?

Quiz!

What do you call the entity or signer of your certificate?

Certificate Authority

What TCPIP utility is used to manage your key DB and certificates?

GSKKYMAN

TCPIP Configuration

TCPIP and SSL

z/VM's TCPIP has SSL servers you can set up to reference the key DB you defined with your certs/keys

In the CP Directory, there is an SSL IDENTITY

```
IDENTITY SSL      LBYONLY   160M  256M G
POOL LOW 1 HIGH 5 PROFILE TCPSSLU
```

The TCPSSLU profile contains "POSIXINFO UID 7 GNAME security" which provides the authorization to access the key DB

Generally, these are "good as defined"

TCPIP and SSL

Add or confirm SSL statements in your “system TCPIP” config file:

SSLSERVERID * TIMEOUT 30

SSLLIMITS MAXSESSIONS 500 MAXPERSSLSERVER 100

Adjust as you see fit

In the PORT section, you can add the “SECURE *certname*” parm to services that accept it. Example:

443 TCP ZWSSL01 NOAUTOLOG SECURE *certname*

Protect TELNET in PORTS:

```
992  TCP INTCLIEN  SECURE certname
```

In INTERNALCLIENTPARMS:

```
PORT           992
SECURECONNECTION REQUIRED
TLSLabel       certname
```

TCPIP and SSL

Add SSL entries in DTCPARMS config:

```
:nick.ssl       :type.class
                :name.SSL daemon
                :command.VMSSL
                :runtime.C
                :timestamp.ON
                :diskwarn.YES
                :Admin_ID_list.TCPMAINT GSKADMIN
                :memory.160M
                :mixedcaseparms.YES
                :mount. /../VMBFS:VMSYS:ROOT/       /     ,
                        /../VMBFS:VMSYS:SSLSERV/    /tmp  ,
                        /../VMBFS:VMSYS:GSKSSLDB/   /etc/gskadm
                :Admin_ID_list.TCPMAINT GSKADMIN
                :parms.KEYFile /etc/gskadm/allcerts.kdb
                       PROTOCOL +TLSV1_2
                       PROTOCOL -TLSV1_1
                       PROTOCOL -TLSV1_0
                       PROTOCOL -SSLV3
                       PROTOCOL -SSLV2
                       EXEMPT LOW
                       EXEMPT MEDIUM
                       TRACE NORMAL

:nick.SSLDCSSM  :type.server   :class.ssl_dcss_agent
                :stack.TCPIP
                :TcpDataFile.TCPIP DATA
                :DCSS_Parms.<DEFAULT>
                :for.SSL*
```

TCPIP and SSL

Restart TCPIP after making all your configuration updates

- Do not restart from a TN3270 session!!

You should then see SSLDCSSM and SSL0001 through SSL0005 running

Confirm with: NETSTAT CONFIG SSL

```
VM TCP/IP Netstat Level 730        TCP/IP Server Name: TCPIP

SSL Server User ID: SSL00001   Status: Active   Connections: 0
SSL Server User ID: SSL00002   Status: Active   Connections: 0
SSL Server User ID: SSL00003   Status: Active   Connections: 0
SSL Server User ID: SSL00004   Status: Active   Connections: 0
SSL Server User ID: SSL00005   Status: Active   Connections: 0
Maximum Session System Limit:  500
Maximum Session Server Limit:  100
SSL Session High-Water Mark:   0
```

Network is Secure!

With your key DB, active certificate/key, and TCPIP configured, your system now has enabled SSL/TLS

If you secured TELNET, then connections would require Port 992 and specify security or SSL/TLS of TLS v1.2 (assuming DTCPARMS used the recommended settings)

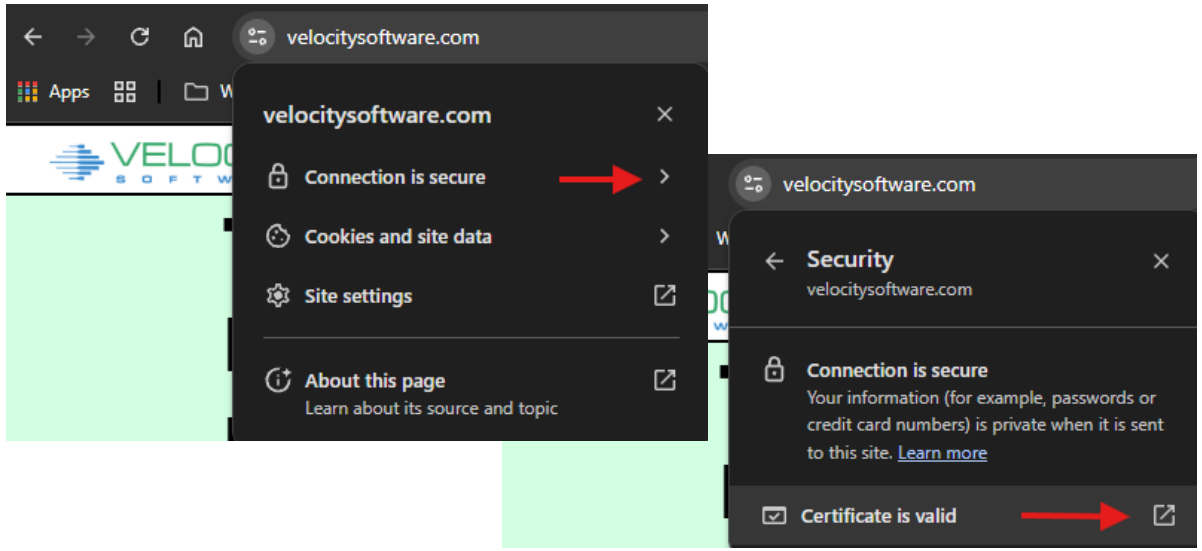
Web servers using SECURE *certname* will answer on **https** calls (port 443 normally)

If FTP servers are configured and TLSLABEL *certname* is defined, FTP services will be secured

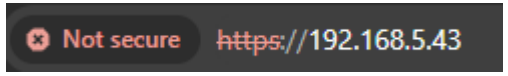
Network is Secure!

Validation via a Web Browser

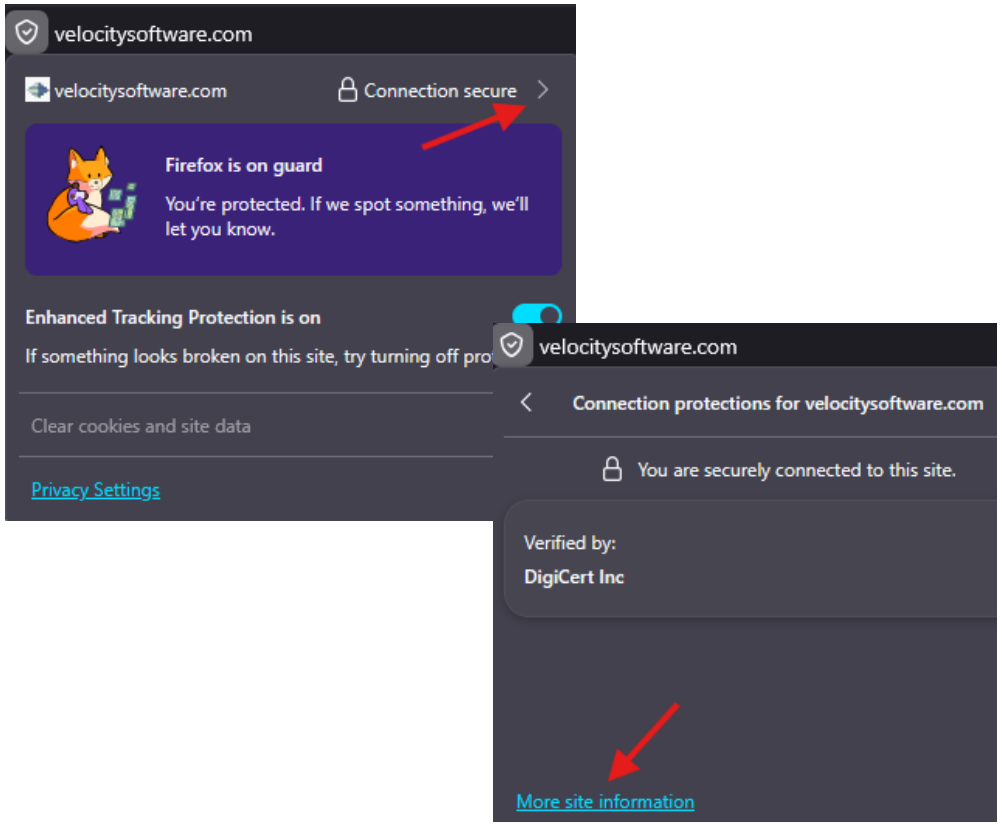
Chrome:



If you see this, then there's a problem!



Firefox:



VELOCITY SOFTWARE

CERTMGR Utility

CERTMGR

CERTMGR allows you to query *and now manage* your certificates without going through GSKKYMAN

- PTF PH68728 - z/VM 7.4 - TCPIP Feature 03 Fix 00
  https://www.ibm.com/support/pages/apar/PH68728

HELP CERTMGR for details on usage

- You may be prompted for the key DB password
- You can save the default key DB with DEFAULTS SET CERTMGR DATABASE /etc/gskadm/*dbname*.kdb

CERTMGR QUERY LABEL * (DATABASE /etc/gskadm/allcerts.kdb

```
Database /etc/gskadm/allcerts.kdb

Enter database password (press ENTER to cancel):

<----- Certificate ----> <- Key -> <-Signature-> Self
 Type    Expires   Trust Type Size Type   Hash    Sign            Label
------ ---------- ----- ---- ---- ----- ------- ---- -------------------------
Entity 04 Jan 2027  Yes  ECC   256 RSA   SHA-256 No   SYS1CERT
Root   01 Aug 2028  Yes  RSA  1024 RSA   SHA-1   Yes  VeriSign Class 1 Public Primary CA - G2
Root   01 Aug 2028  Yes  RSA  1024 RSA   SHA-1   Yes  VeriSign Class 2 Public Primary CA - G2
Root   01 Aug 2028  Yes  RSA  1024 RSA   SHA-1   Yes  VeriSign Class 3 Public Primary CA - G2
Root   01 Aug 2028  Yes  RSA  1024 RSA   SHA-1   Yes  VeriSign Class 4 Public Primary CA - G2
Inter  29 Mar 2031  Yes  RSA  2048 RSA   SHA-256 No   DigiCert Global G2 CA
Root   10 Nov 2031  Yes  RSA  2048 RSA   SHA-1   Yes  IBM DigitCert Global Root CA
Inter  01 Jan 2035  Yes  RSA  2048 RSA   SHA-256 No   IBM INTERNAL INTERMEDIATE CA
Root   03 Jan 2035  Yes  RSA  2048 RSA   SHA-256 Yes  IBM INTERNAL CA
Root   16 Jul 2036  Yes  RSA  2048 RSA   SHA-1   Yes  VeriSign Class 1 Public Primary CA - G3
Root   16 Jul 2036  Yes  RSA  2048 RSA   SHA-1   Yes  VeriSign Class 2 Public Primary CA - G3
Root   16 Jul 2036  Yes  RSA  2048 RSA   SHA-1   Yes  VeriSign Class 3 Public Primary CA - G3
Root   16 Jul 2036  Yes  RSA  2048 RSA   SHA-1   Yes  VeriSign Class 3 Public Primary CA - G5
Root   16 Jul 2036  Yes  RSA  2048 RSA   SHA-1   Yes  VeriSign Class 4 Public Primary CA - G3
Root   15 Jan 2038  Yes  RSA  2048 RSA   SHA-256 Yes  IBM DigitCert Global Root G2
```

CERTMGR QUERY (CHAIN DATABASE /etc/gskadm/allcerts.kdb

```
Database /etc/gskadm/allcerts.kdb

Enter database password (press ENTER to cancel):

  Expires                                  Label
-----------   ------------------------------------------------------------
15 Jan 2038   IBM DigitCert Global Root G2
29 Mar 2031     DigiCert Global G2 CA
04 Jan 2027       SYS1CERT

03 Jan 2035   IBM INTERNAL CA
01 Jan 2035     IBM INTERNAL INTERMEDIATE CA
```

Renewals

Renewals

Put the date of expiration of your certificates on your calendar!

Before your certificate expires,

- Create a new certificate request
  - Specify a NEW Label for the request!
  - For example, your original may be SYS1CERT. The new one could be SYS1RENW or SYS12027 – something that makes sense to you but it will be temporary
- Send the request to the CA and await the cert/key response

Renewals

When you have your new certificate / key:

- Import it in GSKKYMAN to satisfy the key request using "5 - Receive requested certificate or a renewal certificate"
- Once received, you will have two Certificate/Keys:
  - "1 - Manage keys and certificates" (GSKKYMAN)
    SYS1CERT (the active one) and SYS1RENW (the new one)
- Select SYS1CERT, "9 - Change label" and make it SYS12026
- Select SYS1RENW, "9 - Change label" and make it SYS1CERT

This allows you to start using the NEW certificate/key with all the services you set up to use the security/cert label of "SYS1CERT"

Renewals

Your key DB now contains the original/old cert/key along with the new one

z/VM SSL services do not yet have the **new** cert/key active though

- A refresh on the z/VM SSL servers is required for any key DB changes

To activate the new certificate in z/VM SSL

- Logon to TCPMAINT
- Enter: SSLADMIN REFRESH
  This refreshes the key DB data in the SSL servers; any new connection will use the new cert/key. It will not interrupt any current connections!
- HELP TCPIP SSLADMIN for more details on the command

Usual response from a refresh:

```
ssladmin refresh
DTCSSL2404I Sending command to server(s): SSL00001 SSL00002 SSL00003 SSL00004 SSL00005
SSL00001:  DTCSSL133I SSLADMIN request processed; RC: 0
SSL00002:  <*Same as for server SSL00001*>
SSL00003:  <*Same as for server SSL00001*>
SSL00004:  <*Same as for server SSL00001*>
SSL00005:  <*Same as for server SSL00001*>
```

Expiration Dates

Expiration Dates

There has been a lot of debate and discussion around how long TLS certificates should last

The maximum certificate lifetime is going to impact us all:

- Previously until March 15, 2026, the maximum lifetime was 398 days
- As of March 15, 2026, the maximum lifetime is 200 days
- As of March 15, 2027, the maximum lifetime will be 100 days
- As of March 15, 2029, the maximum lifetime will be 47 days

That means after 2029, you will be replacing your certificate every 47 days *or less*!! (You can thank Apple for this)

Reference: https://www.digicert.com/blog/tls-certificate-lifetimes-will-officially-reduce-to-47-days

Best Practices

Best Practices

Best Practices dictate that for each and every system you manage it should have its own certificate/key

- That very well could be dictated by your company's CSO also

Sometimes, especially in a test system cluster, you *may* want to share the cert/key or even the entire key DB

- "get" the key DB file(s) and send them to the target GSKADMIN
- "put" the files into the BFS for that system; build/refresh SSL

Backup your key DB!!

- I more than highly recommend this!
  - If you have a system backup product that covers the VMSYS file pool where the BFS file systems are, then good!
  - Otherwise, set something up to make a backup copy before changes are made
    - You need all three files; the .kdb, .rdb, and .sth
    - Copy them somewhere other than the BFS – GSKADMIN's 191 disk would be okay

Best Practices

Keep your key DB cleaned up

- As time goes on, you will collect old/expired certificates
- CERTMGR helps find them!
  - CERTMGR QUERY (CHAIN DATABASE /etc/gskadm/allcerts.kdb
  - An “E” after the expiration date shows you it is expired
- Go into GSKKYMAN to delete the certs/keys that are expired
  - Assuming they have been replaced!

Self-Signed Certificates

- **Don’t use** except for *very* short-term validation and testing

Homework!

You have some homework to do! Homework will be checked before the completion certificates are sent out after the end of the class.

Your task:

- On your browser, go to https://velocitysoftware.com
- Find the Certificate information/details
- Email to homework@velocitysoftware.com and include:
  - The Common Name (CN)
  - The Expiration Date of the certificate

That's it!

Thank you for attending!

More questions? Send to: questions@velocitysoftware.com

Training, Education and Information

https://velocitysoftware.com/educate/

Presentations and Handouts

https://velocitysoftware.com/pdfs/

VELOCITY SOFTWARE