IBM® Sterling Connect:Express ® for z/OS®

SSL Guide

Copyright

Before using this information and the product it supports, read the information in

Notices, on page 43.

IBM® Sterling Connect:Express® for z/OS®

Table of Contents

Table of Contents

Sterling Connect:Express for zOS and SSL/TLS support

This functionality integrates with the Sterling Connect:Express architecture via a SSL handler through which the monitor network services (the ANM) interface using z/OS Cryptographic Services System SSL, part of z/OS Cryptographic Services.

See https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.4.0/com.ibm.zos.v2r4.csf/csf.htm)

SSL activation is independent of the transfer protocol used (PeSIT or Odette).

The functionality is available in client or server mode.

IMPORTANT NOTE: The SSL option does not apply to FTP transfers processed in the AFM.

Configuring SSL

Before using SSL, you should configure the components involved in a secure transfer:

- The monitor;
- the ANM, network manager.

Configuring the Monitor

Monitor setup allows you to define its local characteristics as an SSL monitor:

- handler activation;
- default certificate specification;
- default SSL options.

All parameters are defined in the SYSIN file.

General principles include the following:

- By default, the SSL handler is inactive;
- SSL access over TCP/IP are characterized by a specific port for incoming traffic;
- SSL default values are z/OS System SSL Services default values;
- The SSL parameters values defined in the SYSIN are also known as configuration 00 (SSLCFG00);

Additionally, the SSL handler can't work with the HPNS interface. You must therefore modify the monitor setup to use the Open Edition interface of z/OS.

```
Change TCPORG=(HPNS, tcpipJob) to TCPORG=(SOE).
```

Monitor SYSIN File

The table below describes the parameters that characterize the Sterling Connect:Express SSL service. Some of the parameters allow lowercase characters: enter data carefully because most SYSIN parameters are exclusively upper case, key words in particular.

To use the SSL service, the following parameters are required:

- SSLOPT=Y
- SSLKRG=Name of a RACF keyring;
- or SSLDTTB and SSLPSW name and password of the certificates HFS database;
- SSLPRT=TCP/IP port for incoming traffic (Clients).

Field	Range or Values	Description	*Type*
TCPORG	(SOE)	This value selects the z/OS Open Edition interface for the TCP handler. This is required to make the SSL and TCP/IP handlers work together.	*Required*
SSLOPT	Y/N	Activation of the SSL handler. N is the default value.	*Optional*
SSLCFG	Y/N	ANM SSL can use more than one configuration. N is the default value. Y requires an ANMSSL file defined and allocated to the ANM. With more than one configuration it becomes possible to manage client or server profiles with SSL characteristics different from the default 00 configuration.	***Optional***
SSLKRG	1–44 chars mixed case	Name of the RACF keyring associated with the ANM. This field is mutually exclusive of SSLDTB and SSLPSW. Example: SSLKRG=TOM4.KEYRING GSK Reference: GSK_KEYRING_FILE	***Required***
SSLDTB	1–44 chars mixed case	Name of the HFS database in which certificates are stored. This field is associated with SSLPSW and is mutually exclusive of SSLKRG. GSK Reference: GSK_KEYRING_FILE	***Required***
SSLPSW	1–16 chars mixed case	Password allowing access to the HFS database in which certificates are stored. GSK Reference: GSK_KEYRING_PW	***Required***
SSLPRT	1–5 numeric chars	TCP/IP port number for incoming PeSIT SSL calls. Range from 1 to 65535.	***Required***
SSLPRO	1–5 numeric chars	TCP/IP port number for incoming Odette SSL calls. Ranges from 1 to 65535.	***Required only for Odette***
SSLCER	1–34 chars mixed case	Label of the default certificate referenced in the certificate database or in the RACF keyring. May include blanks. If not declared, the default certificate defined in the database is used by System SSL. Example: SSLCER=Label of Paris 2 server GSK Reference: GSK_KEYRING_LABEL	*Optional*
SSLTRC	0/1	Default trace option. 0 is the default value. 1 activates the environment trace of the SSL handler. This trace is written to an ANM SYSPRINT file.	*Optional*

Field	Range or Values	Description	*Type*
SSLTIM	1–6 numeric chars	Retention duration of the SSL session identifier, in seconds. Default is the System SSL default value. GSK Reference: GSK_V3_SESSION_TIMEOUT	*Optional*
SSLT13	Y/N	TLS V1.3 support. The default is ‘Y’. GSK Reference: GSK_PROTOCOL_TLSV1_3 (GSK_PROTOCOL_TLSV1_3_ON, GSK_PROTOCOL_TLSV1_3_OFF)	*Optional*
SSLT12	Y/N	TLS V1.2 support. The default is ‘Y’. GSK Reference: GSK_PROTOCOL_TLSV1_2 (GSK_PROTOCOL_TLSV1_2_ON, GSK_PROTOCOL_TLSV1_2_OFF)	*Optional*
SSLT11	Y/N	TLS V1.1 support. The default is ‘N’. GSK Reference: GSK_PROTOCOL_TLSV1_1 (GSK_PROTOCOL_TLSV1_1_ON, GSK_PROTOCOL_TLSV1_1_OFF)	*Optional*
SSLTL1	Y/N	TLS V1 support. The default is ‘N’. GSK Reference: GSK_PROTOCOL_TLSV1 (GSK_PROTOCOL_TLSV1_ON, GSK_PROTOCOL_TLSV1_OFF)	*Optional*
SSLAUT	Y/N/C	N is the default value. In server mode, with Y, client authentication will be required but no certificate can be provided by client. In server mode, C will reject client authentication with no certificate provided. GSK Reference: GSK_CLIENT_AUTH_TYPE(GSK_CLIENT_AUTH_FULL_TYPE, GSK_CLIENT_AUTH_PASSTHRU_TYPE). GSK_CLIENT_AUTH_ALERT (GSK_CLIENT_AUTH_NOCERT_ALERT_ON, GSK_CLIENT_AUTH_NOCERT_ALERT_OFF)	*Optional*
SSLCIP	Up to 64 chars	Default ciphers suite in numerical format and preference order. Depending on SSLCIL, up to 32 2 characters ciphers (SSLCIL=2) or 16 4 characters ciphers can be provided. Default value is the System SSL default value. Refer to the System SSL documentation for current default. Example: SSLCIP=09060504 GSK Reference: GSK_V3_CIPHER_SPECS (2), GSK_V3_CIPHER_SPECS_EXPANDED (4)	*Optional*

Field	Range or Values	Description	*Type*
SSLCIL	2/4	Length of cipher values provided in SSLCIP. Note: For TLS1.3 usage, SSLCIL must be set to 4. Default value is 2. GSG Reference: GSK_V3_CIPHERS (GSK_V3_CIPHERS_CHAR2, GSK_V3_CIPHERS_CHAR4)	*Optional*
SSLBIA	IPV4 or HOST	IPV4 address or hostname (resolved to an IPV4 address) the monitor will listen for incoming PeSIT SSL calls. Default is 0.0.0.0	*Optional*
SSLBIO	IPV4 or HOST	IPV4 address or hostname (resolved to an IPV4 address) the monitor will listen for incoming PeSIT SSL calls. Default is 0.0.0.0	*Optional*
SSLBOA	IPV4 or HOST	IPV4 address or hostname (resolved to an IPV4 address) the monitor will bind to when connecting to a remote PeSIT SSL server. Default is the default interface.	*Optional*
SSLBOO	IPV4 or HOST	IPV4 address or hostname (resolved to an IPV4 address) the monitor will bind to when connecting to a remote Odette SSL server. Default is the default interface	*Optional*
SSLSAP	Up to 64 chars	Specifies the list of hash and signature algorithm pair specifications that are supported by the client or server as a string consisting of 1 or more 4-character values in order of preference for use in digital signatures of X.509 certificates and TLS handshake messages. The signature algorithm pair specifications are sent by either the client or server to the session partner to indicate which signature/hash algorithm combinations are supported for digital signatures in X.509 certificates and TLS handshake messages. If the SSLCAP setting is specified, the SSLSAP setting is only used to indicate the signature/hash algorithm combinations supported for digital signatures in TLS handshake messages. The signature algorithm pair specification only has relevance for sessions using TLS V1.2 or higher protocols. Default value is System SSL default. GSK Reference: GSK_TLS_SIG_ALG_PAIRS	
SSLCAP	Up to 64 chars	Specifies the list of hash and signature algorithm pair specifications that are supported by the client or server as a string consisting of one or more 4-character values in order of preference for use in digital signatures of X.509 certificates. The certificate signature algorithm pair specifications are sent by either the client or server to the session partner to indicate which signature/hash algorithm combinations are supported for digital signatures in X.509 certificates. The SSLCAP setting overrides the SSLSAP setting when checking the digital signatures of the remote peer's X.509 certificates. The certificate signature algorithm pair specification only has relevance for TLS V1.2 client or TLS V1.3 client and server sessions. Default value is System SSL default. GSK Reference: GSK_TLS_CERT_SIG_ALG_PAIRS	

Field	Range or Values	Description	*Type*
SSLECL	Up to 64 chars	List of elliptic curves or supported groups that are supported by the client as a string consisting of 1 or more 4-character decimal values in order of preference for use. For TLS V1.0, TLS V1.1, and TLS V1.2 protocols, this list is used by the client to guide the server to the elliptic curves that are preferred when using ECC-based cipher suites. For the TLS V1.3 protocol, this list is used by the client to guide the server to the elliptic curves that are preferred and guide group selection to encrypt and decrypt TLS V1.3 handshake messages. Default value is System SSL default. GSK Reference: GSK_CLIENT_ECURVE_LIST	
SSLSKS	Up to 64 chars	List of groups or curves that are supported by the server when doing a TLS V1.3 handshake. Default value is System SSL default. GSK Reference: GSK_SERVER_TLS_KEY_SHARES	
SSLCKS	Up to 64 chars	List of groups or curves that are supported by the client when doing a TLS V1.3 handshake. Default value is System SSL default. GSK Reference: GSK_CLIENT_TLS_KEY_SHARES	
SSLHTO	0 to 30 seconds	Handshake timeout delay to limit handshake. Default is 0, no timeout, except TCP timeout.	
SSLMCM	Y/N	Specifies if the TLS V1.3 handshake process ought to use or tolerate handshake messages in a manner compliant with earlier TLS protocols to alleviate possible issues with middleboxes or proxies. Specify Y if the TLS V1.3 handshake process ought to use or tolerate handshake messages in a manner compliant with earlier TLS protocols to alleviate possible issues with middleboxes or proxies. Specify N if the TLS V1.3 handshake process ought to use the pure TLS V1.3 handshake message format. Default value is N. GSK Reference: GSK_MIDDLEBOX_COMPAT_MODE (GSK_MIDDLEBOX_COMPAT_MODE_ON, GSK_MIDDLEBOX_COMPAT_MODE_OFF)	

Configuring the ANM

Sterling Connect:Express receives the default SSL parameters via its SYSIN and transmits them to the ANM during initialization. If SSLCFG parameter is equal to 'N', the ANM loads the default configuration from the SYSIN file.

```
02.21.42 STC07965  ANMSSL03 SSL CONFIGURATION LOADED FROM SYSIN
02.21.42 STC07965  SSL0023I SSL HANDLER STARTING
02.21.42 STC07965  SSL0014I CONFIGURATION FILES PROCESS COMPLETED
```

If SSLCFG parameter is equal to 'Y', the ANM loads the configuration files from the ANMSSL file also.

```
06.17.46 STC00505  ANMSSL03 SSL CONFIGURATION LOADED FROM SYSIN
06.17.46 STC00505  SSL0023I SSL HANDLER STARTING
06.17.46 STC00505  SSL0010I STARTING CONFIGURATION FILES PROCESS
06.17.46 STC00505  SSL0014I SSLCFG01 PROCESSED SUCCESSFULY
06.17.46 STC00505  SSL0014I SSLCFG10 PROCESSED SUCCESSFULY
06.17.46 STC00505  SSL0014I SSLCFG12 PROCESSED SUCCESSFULY
06.17.46 STC00505  SSL0014I SSLCFG13 PROCESSED SUCCESSFULY
06.17.46 STC00505  SSL0014I SSLCFG14 PROCESSED SUCCESSFULY
06.17.46 STC00505  SSL0014I SYSSSL   PROCESSED SUCCESSFULY
06.17.46 STC00505  SSL0014I CONFIGURATION FILES PROCESS COMPLETED
```

ANMSSL File

The SSL profiles file is defined in the JCL of the ANM, using the ANMSSL DD card. This is a PDS file, fixed record format with record length less or equal to 300 bytes.

The following example shows a typical ANMSSL content.

```
  Menu  Functions  Confirm  Utilities  Help
------------------------------------------------------------------------------
VIEW              TOMC.ANMSSL                          Row 0000001 of 0000009
Command ===>                                                Scroll ===> CSR
           Name     Prompt       Size   Created          Changed          ID
_________ DNCFG01                 13  2012/03/28  2016/04/11 08:26:10  USR0009
_________ DNCFG05                 19  2009/02/18  2015/09/08 08:02:04  USR0009
_________ DNCFG06                 18  2009/02/18  2009/03/05 10:47:38  USR0008
_________ SSLCFG01                11  2009/01/21  2020/02/21 11:20:23  USR0003
_________ SSLCFG10                13  2020/02/26  2020/02/26 09:38:39  USR0003
_________ SSLCFG12                13  2020/02/26  2020/02/26 09:24:37  USR0003
_________ SSLCFG13                18  2020/02/20  2020/02/24 04:27:21  USR0003
_________ SSLCFG14                18  2020/02/26  2020/02/26 09:42:30  USR0003
_________ SYSSSL                  22  2015/09/21  2020/02/26 10:28:33  USR0003
          **End**
```

Members prefixed by string ‘DN’ are used for DN control (See DN Control on page 25), members prefixed by string ‘SSLCFG’ define SSL profiles, from number 01 to 99 (See Working with SSL Profiles on page 13), SYSSSL file is used for profile selection during an inbound session (See Server Mode on page 26 – *SYSSSL File*’).

Any other member is ignored.

Other SSL related DD NAMES

ANM JCL should also include the following SYSOUT DD:

- SYSCFG SSL configuration read from ANM and printed out;
- SYSDNCTL DN Control output. Only required if a DN Control trace is necessary;
- SYSPRINT SSL handler trace;
- CEEMOUT Language environment;
- CEEMSG Language environment;
- CEEDUMP Language environment dump.

SSL Default Configuration

When ANM starts, SYSLOG shows the list of default parameters.

```
 ISFPCU41 UT DISPLAY PSRANC   STC00505  DSID   105 LINE 0       COLUMNS 02- 133
 COMMAND INPUT ===>                                            SCROLL ===> CSR
******************************** TOP OF DATA *********************************
TCPORG=(SOE)
TCPPRT=51703
TCPPRO=00000
SSLOPT=Y
SSLPRT=51803
SSLCIL=00004
SSLCIP=130113021303003902F
SSLCER=PSRANMD2
SSLTRC=1
SSLKRG=psranm.keyring
TCPBIA=010.120.131.073
TCPBIO=000.000.000.000
SSLBIA=010.120.131.074
SSLBIO=000.000.000.000
SSLTL1=N
SSLT11=N
SSLT12=Y
SSLT13=Y
SSLMCM=N
SSLSKS=
SSLCKS=
SSLAUT=N
SSLCFG=Y
APLPFX=TOMCAP
STDMSG=32
MAXEXT=(64,32)
```

Working with SSL Profiles

SSL profiles are processed by the ANM, during inbound or outbound SSL handshake. Profiles enable to apply various policies to partners.

Definition

An SSL profile is defined in a member of the ANMSSL file. Its name follows the syntax shown below:

```
SSLCFGnn                    'nn' from 01 to 99
```

You can override one or several SSL parameters from the configuration 00 (monitor SYSIN) with new values defined in profile nn. Profile nn is a merge between configuration 00 and configuration nn.

Some SSL parameters can't be modified in a profile and value remains the same for all profiles; others can be modified; some are new and only available in configuration profile.

Non-modifiable parameters

TCPORG	This value selects the z/OS Open Edition interface for the TCP handler. This is required to make the SSL and TCP/IP handlers work together.
SSLOPT	Activation of the SSL handler. N is the default value.
SSLCFG	ANM SSL can use more than one configuration. N is the default value. Y requires an ANMSSL file defined and allocated to the ANM. With more than one configuration it becomes possible to manage client or server profiles with SSL characteristics different from the default 00 configuration.
SSLKRG	Name of the RACF keyring associated with the ANM. This field is mutually exclusive of SSLDTB and SSLPSW. Example: SSLKRG=TOM4.KEYRING GSK Reference: GSK_KEYRING_FILE
SSLDTB	Name of the HFS database in which certificates are stored. This field is associated with SSLPSW and is mutually exclusive of SSLKRG. GSK Reference: GSK_KEYRING_FILE
SSLPSW	Password allowing access to the HFS database in which certificates are stored. GSK Reference: GSK_KEYRING_PW
SSLPRT	TCP/IP port number for incoming PeSIT SSL calls. Range from 1 to 65535.
SSLPRO	TCP/IP port number for incoming Odette SSL calls. Ranges from 1 to 65535.

SSLTIM	Retention duration of the SSL session identifier, in seconds. Default is the System SSL default value. GSK Reference: GSK_V3_SESSION_TIMEOUT
SSLBIA	IPV4 address or hostname (resolved to an IPV4 address) the monitor will listen for incoming PeSIT SSL calls. Default is 0.0.0.0
SSLBIO	IPV4 address or hostname (resolved to an IPV4 address) the monitor will listen for incoming PeSIT SSL calls. Default is 0.0.0.0
SSLBOA	IPV4 address or hostname (resolved to an IPV4 address) the monitor will bind to when connecting to a remote PeSIT SSL server. Default is the default interface.
SSLBOO	IPV4 address or hostname (resolved to an IPV4 address) the monitor will bind to when connecting to a remote Odette SSL server. Default is the default interface
SSLHTO	Handshake timeout delay to limit handshake. Default is 0, no timeout, except TCP timeout.

Modifiable parameters

Field	Description
SSLCER	Label of the default certificate referenced in the certificate database or in the RACF keyring. May include blanks. If not declared, the default certificate defined in the database is used by System SSL. Example: SSLCER=Label of Paris 2 server GSK Reference: GSK_KEYRING_LABEL
SSLTRC	Default trace option. 0 is the default value. 1 activates the environment trace of the SSL handler. This trace is written to an ANM SYSPRINT file.
SSLTIM	Retention duration of the SSL session identifier, in seconds. Default is the System SSL default value. GSK Reference: GSK_V3_SESSION_TIMEOUT
SSLT13	TLS V1.3 support. The default is ‘Y’. GSK Reference: GSK_PROTOCOL_TLSV1_3 (GSK_PROTOCOL_TLSV1_3_ON, GSK_PROTOCOL_TLSV1_3_OFF)
SSLT12	TLS V1.2 support. The default is ‘Y’. GSK Reference: GSK_PROTOCOL_TLSV1_2 (GSK_PROTOCOL_TLSV1_2_ON, GSK_PROTOCOL_TLSV1_2_OFF)
SSLT11	TLS V1.1 support. The default is ‘N’. GSK Reference: GSK_PROTOCOL_TLSV1_1 (GSK_PROTOCOL_TLSV1_1_ON, GSK_PROTOCOL_TLSV1_1_OFF)

Field	Description
SSLTL1	TLS V1 support. The default is ‘N’. GSK Reference: GSK_PROTOCOL_TLSV1 (GSK_PROTOCOL_TLSV1_ON, GSK_PROTOCOL_TLSV1_OFF)
SSLAUT	N is the default value. In server mode, with Y, client authentication will be required but no certificate can be provided by client. In server mode, C will reject client authentication with no certificate provided. GSK Reference: GSK_CLIENT_AUTH_TYPE(GSK_CLIENT_AUTH_FULL_TYPE, GSK_CLIENT_AUTH_PASSTHRU_TYPE). GSK_CLIENT_AUTH_ALERT (GSK_CLIENT_AUTH_NOCERT_ALERT_ON, GSK_CLIENT_AUTH_NOCERT_ALERT_OFF)
SSLCIP	Default ciphers suite in numerical format and preference order. Depending on SSLCIL, up to 32 2 characters ciphers (SSLCIL=2) or 16 4 characters ciphers can be provided. Default value is the System SSL default value. Refer to the System SSL documentation for current default. Example: SSLCIP=09060504 GSK Reference: GSK_V3_CIPHER_SPECS (2), GSK_V3_CIPHER_SPECS_EXPANDED (4)
SSLCIL	Length of cipher values provided in SSLCIP. Note: For TLS1.3 usage, SSLCIL must be set to 4. Default value is 2. GSG Reference: GSK_V3_CIPHERS (GSK_V3_CIPHERS_CHAR2, GSK_V3_CIPHERS_CHAR4)
SSLSAP	Specifies the list of hash and signature algorithm pair specifications that are supported by the client or server as a string consisting of 1 or more 4-character values in order of preference for use in digital signatures of X.509 certificates and TLS handshake messages. The signature algorithm pair specifications are sent by either the client or server to the session partner to indicate which signature/hash algorithm combinations are supported for digital signatures in X.509 certificates and TLS handshake messages. If the SSLCAP setting is specified, the SSLSAP setting is only used to indicate the signature/hash algorithm combinations supported for digital signatures in TLS handshake messages. The signature algorithm pair specification only has relevance for sessions using TLS V1.2 or higher protocols. Default value is System SSL default. GSK Reference: GSK_TLS_SIG_ALG_PAIRS
SSLCAP	Specifies the list of hash and signature algorithm pair specifications that are supported by the client or server as a string consisting of one or more 4-character values in order of preference for use in digital signatures of X.509 certificates. The certificate signature algorithm pair specifications are sent by either the client or server to the session partner to indicate which signature/hash algorithm combinations are supported for digital signatures in X.509 certificates. The SSLCAP setting overrides the SSLSAP setting when checking the digital signatures of the remote peer’s X.509 certificates. The certificate signature algorithm pair specification only has relevance for TLS V1.2 client or TLS V1.3 client and server sessions. Default value is System SSL default. GSK Reference: GSK_TLS_CERT_SIG_ALG_PAIRS

Field	Description
SSLECL	List of elliptic curves or supported groups that are supported by the client as a string consisting of 1 or more 4-character decimal values in order of preference for use. For TLS V1.0, TLS V1.1, and TLS V1.2 protocols, this list is used by the client to guide the server to the elliptic curves that are preferred when using ECC-based cipher suites. For the TLS V1.3 protocol, this list is used by the client to guide the server to the elliptic curves that are preferred and guide group selection to encrypt and decrypt TLS V1.3 handshake messages. Default value is System SSL default. GSK Reference: GSK_CLIENT_ECURVE_LIST
SSLSKS	List of groups or curves that are supported by the server when doing a TLS V1.3 handshake. Default value is System SSL default. GSK Reference: GSK_SERVER_TLS_KEY_SHARES
SSLCKS	List of groups or curves that are supported by the client when doing a TLS V1.3 handshake. Default value is System SSL default. GSK Reference: GSK_CLIENT_TLS_KEY_SHARES
SSLHTO	Handshake timeout delay to limit handshake. Default is 0, no timeout, except TCP timeout.
SSLMCM	Specifies if the TLS V1.3 handshake process ought to use or tolerate handshake messages in a manner compliant with earlier TLS protocols to alleviate possible issues with middleboxes or proxies. Specify Y if the TLS V1.3 handshake process ought to use or tolerate handshake messages in a manner compliant with earlier TLS protocols to alleviate possible issues with middleboxes or proxies. Specify N if the TLS V1.3 handshake process ought to use the pure TLS V1.3 handshake message format. Default value is N. GSK Reference: GSK_MIDDLEBOX_COMPAT_MODE (GSK_MIDDLEBOX_COMPAT_MODE_ON, GSK_MIDDLEBOX_COMPAT_MODE_OFF)

New parameters

Field	Description
SSLCFG	Free text treated as a comment.
STATUS	Configuration status. E, configuration is enabled; H disabled.
SSLIPH	Set this parameters to Y if remote partner uses Application Transparent Transport Layer Security (AT-TLS).
SSLDNC	Optional name of the DN control member.

Syntax Rules

A line starting by character '*' is a comment line, a blank line is ignored.

A line starting by characters '/*' stops the process (End of file).

You must define at least one active parameter in a profile. The SSLCFG parameter is not an active one.

Keywords are unique and upper case.

The SSL handler initialization fails if one syntax error is found.

Profile Example

```
EDIT       TOMC.ANMSSL(SSLCFG13) - 01.09                        Columns 00001 00080
Command ===>                                                      Scroll ===> CSR
****** ********************************* Top of Data ***********************************
000001 SSLCFG=TLS 1.3 ONLY
000002 SSLTRC=1
000003 SSLCER=CXZOSCERT
000006 SSLTL1=N
000007 SSLT11=N
000008 SSLT12=N
000009 SSLT13=Y
000010 SSLCIL=4
000011 SSLCIP=130113021303
000012 SSLECL=00290030
000013 SSLCKS=00290030
000014 SSLSKS=00290030
000015 SSLSAP=080408050806040305030603
000016 SSLCAP=060106030501050304010403040203010303030202010203020201 01
000017 SSLAUT=Y
000018 SSLIPH=N
****** ******************************** Bottom of Data ********************************
```

SSL Profiles Load or Refresh

The SSL handler loads the profiles during initialization. Any update of a profile must be followed by a stop and start of the handler or a refresh command. See Refresh the SYSSSL configuration on page 33.

WTO messages are issued to indicate that an error has been detected in a profile. The SSL handler initializes successfully if no error has been found. The message SSL0011E indicates that errors have been detected: one or several SSL0012E messages have been issued before.

The SYSCFG file shows the list of profiles that have been loaded. Errors are marked with a '!' in column 2. Rejected profiles are identified with the " ======REJECTED=====" message.

Normal profiles load

WTO messages on JESMSGLG

```
06.17.46 STC00505  SSL0010I STARTING CONFIGURATION FILES PROCESS
06.17.46 STC00505  SSL0014I SSLCFG01 PROCESSED SUCCESSFULY
06.17.46 STC00505  SSL0014I SSLCFG10 PROCESSED SUCCESSFULY
06.17.46 STC00505  SSL0014I SSLCFG12 PROCESSED SUCCESSFULY
06.17.46 STC00505  SSL0014I SSLCFG13 PROCESSED SUCCESSFULY
06.17.46 STC00505  SSL0014I SSLCFG14 PROCESSED SUCCESSFULY
06.17.46 STC00505  SSL0014I SYSSSL   PROCESSED SUCCESSFULY
06.17.46 STC00505  SSL0014I CONFIGURATION FILES PROCESS COMPLETED
```

SYSCFG SYSOUT

```
…
       ======SSLCFG12======
SSLCFG=SSLTL2
SSLTRC=1
SSLCER=CXZOSCERT1
SSLTL1=N
SSLT11=N
SSLT12=Y
SSLT13=N
SSLCIL=2
SSLCIP=353637
SSLAUT=Y
SSLIPH=N
       ======SSLCFG13======
SSLCFG=TLS 1.3 ONLY
SSLTRC=1
SSLCER=CXZOSCERT3
SSLTL1=N
SSLT11=N
SSLT12=N
SSLT13=Y
SSLCIL=4
SSLCIP=130113021303
SSLECL=00290030
SSLCKS=00290030
SSLSKS=00290030
SSLSAP=080408050806040305030603
SSLCAP=060106030501050304010403040203010303030202010203020201
SSLAUT=Y
SSLIPH=N
       ======SSLCFG14======
SSLCFG=ALL TLS
SSLTRC=1
SSLCER=CXZOSCERT2
SSLTL1=Y
SSLT11=Y
SSLT12=Y
SSLT13=Y
…
```

Profiles load with errors

WTO messages on JESMSGLG

```
11.58.31 STC00603  SSL0010I STARTING CONFIGURATION FILES PROCESS
11.58.31 STC00603  SSL0014I SSLCFG01 PROCESSED SUCCESSFULY
11.58.31 STC00603  SSL0014I SSLCFG10 PROCESSED SUCCESSFULY
11.58.31 STC00603  SSL0014I SSLCFG12 PROCESSED SUCCESSFULY
11.58.31 STC00603  SSL0012E 16 BUILD    SSLCFG13 KVAL SSLTRC=
11.58.31 STC00603  SSL0013I SSLCFG13 CONFIGURATION FILE, ERROR DETECTED
11.58.31 STC00603  SSL0014I SSLCFG14 PROCESSED SUCCESSFULY
11.58.31 STC00603  SSL0014I SYSSSL   PROCESSED SUCCESSFULY
11.58.31 STC00603  SSL0011I ERRORS HAVE BEEN DETECTED DURING PROCESS
11.58.31 STC00603  SSL0011E ANMSSL PROCESS ERROR, CHECK SSL MESSAGES / SYSCFG FILE
```

SYSCFG SYSOUT

```
       ======SSLCFG13======
SSLCFG=TLS 1.3 ONLY
!SSLTRC=3
SSLCER=CXZOSCERT
SSLTL1=N
SSLT11=N
SSLT12=N
SSLT13=Y
SSLCIL=4
SSLCIP=130113021303
SSLECL=00290030
SSLCKS=00290030
SSLSKS=00290030
SSLSAP=080408050806040305030603
SSLCAP=060106030501050304010403040203010303030202010203020201 01
SSLAUT=Y
SSLIPH=N
       ======REJECTED======
```

The following codes identify errors:

Code	Explanation	Action
DUPK	Duplicate keyword	Modify the profile
INVK	Invalid keyword	Modify the profile
KVAL	Invalid value of a keyword	Modify the profile
LREC	Invalid record length of the ANMSSL file	Allocate the ANMSSL file with a record length up to 300.
NLEV	At least one SSL/TLS protocol should be enabled but none is selected after the merge between SYSIN and the configuration file. Parameters SSLTL1, SSLT11, SSLT12, SSLT13, SSLVE3 and SSLVE2 are all set to N.	Modify the profile
NULL	No active parameter for the profile	Modify the profile
LINK	Process error	Contact support

Code	Explanation	Action
OPEN	File open error	Contact support
STOR	Storage error	Contact support

Client Mode

There are many ways to enable SSL for a transfer:

- Provide a SSL profile number in the partner definition;
- Provide a SSL profile number in the file definition;
- Provide a SSL profile number with the transfer request parameters;
    - Using SSL CONFIG. in the transfer extension screen of the TSO/ISPF interface;
    - Using SEC= parameter of the utility P1B2PRQ2;
    - Using EX1SSECN field of program L0B2Z20.

SSL Profile in Partner Definition

```
 Directories  Monitor  Tables  Requests  Help  Caps (OFF)              4.3.0.11

                 Partner    CXM30751  of TOMC     - Mode View
Option ===> _____________________________________________ Scroll ===> PAGE

TYPE: TOM PESIT-E

                               Dpcsid Alias .. CXM30751
TOM Password .......... PSWC   Dpcpsw Alias .. PSWC
Initialisation State .. E      APM Reception Class  B
Partner Type .......... T
RACF User  Group ...... PSRUSR     SYS1

Protocol  Table Number  5   2           SSL Profile 14
Presentation .......... -  (01-24)     DN Control  -
Automatic Restart ..... Y              Sessions T I O    128 064 064

PI99 Connection ....... _____________________________________________________
                        ----+----1----+----2----+----3----+----4----+----5----
PI99 ACK Connection ... _____________________________________________________
                        ----+----1----+----2----+----3----+----4----+----5----
Network Link Type ..... I   Multi .. -
 IP Addr .. -                Port .. 51703
    Host .. ZVIPA_3073.USTXLAB.COM
            ----+----1----+----2----+----3----+----4----+----5----+----6----+-
Bnd Addr .. _________________
    Host .. _____________________________________________________________
            ----+----1----+----2----+----3----+----4----+----5----+----6----+-
 FTP  PASV  - Profile   -
 SNA  LUName -        LOGMode -        LOGData -        Disc N
Note _________________________________________________________________________
Last update USR0003 20/03/02 10:29:41
```

SSL Profile in File Definition

```
Directories  Monitor  Tables  Requests  Help  Caps (OFF)              4.3.0.11

                  File     CXM30751  of TOMC     - Mode View
Option ===> _____________________________________________ Scroll ===> PAGE


Initialisation State .. E          E: In-Service H: Hold
Notification Level .... 0          From 0 to 7
Direction ............. *          T:Transmit    R:Receive  *:Both Directions
Receiving Partner ..... *          'NAME'  #LIST   *:$$ALL$$  $$API$$
Sending Partner ....... *          'NAME'  #LIST   *:$$ALL$$  $$API$$
Priority .............. 2          0:Urgent 1:Fast   2:Normal 3:Slow
DSN Allocation Type ... D          D:Dynamic   F:Fix
Allocation Rule ....... 1          0:Create Replace  1:Prealc. 2:To Create
                                   3:Exit A:Application Server
File Type ............. S          S H M P PU V VU UU SU TU HU
Presentation .......... 01         Compression  Data Type (01-24)
Unload Reload Member .. -          Optional
SSL Profile ........... 14         Optional

PI 99 Selection ....... ____________________________________________________
                        ----+----1----+----2----+----3----+----4----+----5----
PI 99 ACK Selection.... ____________________________________________________
                        ----+----1----+----2----+----3----+----4----+----5----
Last update USR0003 20/03/09 06:13
```

SSL Profile in Request Extension

```
Directories  Monitor  Tables  Requests  Help  Caps (OFF)              4.3.0.11

                              Transfer Extension
Option ===> _____________________________________________ Scroll ===> PAGE



Monitor .... TOMC ACTIVE GLOBAL STANDALONE IRVO
File ....... CXM30751              Partner .... CXM30751
Direction .. T DSN  PSR$REC.PS.B80

Alias ...... ________ Alias Psw ... ________
Origin ..... ________ Destination . ________

RACF Group . ________ SSL Config .. 11
           (EN AN I)(F R)(B C S)                    (YES NO)
FTP T S M .. __       _    _          Store Unique .. _
Remote DSN . ____________________________________________

S  Detail
_ Api .....  ____________________________________________________________
```

SSL Profile in P1B2PRQ2 BATCH Utility

```
 000450 //SYSIN    DD  *
 000451 BBLOCK
 000452 SEND SFN=FICTST                SYMBOLIC FILE NAME
 000453      SPN=PARTNER3              SYMBOLIC PARTNER NAME
 000454      TYP=N                     REQUEST TYPE
 000455      CLS=A                     REQUEST CLASS
 000457      PRT=1                     REQUEST PRTY
 000458      SEC=12                    REQUEST SECURITY
 000460      DSN= PSR$REC.PS.F080.SHORT
 000466 EBLOCK
```

When a call is received inbound on one of the secured access points - defined in the SYSIN by SSLPRT or SSLPRO for TCP/IP- it is processed by the SSL handler. The default used configuration is the monitor SYSIN configuration, configuration 00.

To select a different profile than the default it is necessary to define rules based on incoming address, hostname or IP. The SYSSSL member of the ANMSSL file is used to select a configuration profile number from some address criteria.

Syntax Rules

- A line starting by character '*' is a comment line a blank line is ignored.
- A line starting by characters '/*' stops the selection process (End of file).
- Keywords are unique and uppercase.
- Each line defines some criteria and the associated profile number separated by a comma in any order.

```
LT=criteria,CF=nn[,DN=member]
```

The criteria indicates the link type *L* (I=TCP/IP) the type of address *T* (A=Address H=Host name). The value can be a specific address or a pattern. The parameter CF= provides the profile number to use. Alternatively, you can also provide a DN member for this address. The DN member will override the DN member declared in the configuration profile.

Optionally, a DN control member can be associated with a rule entry. This DN control member will override any DN control member defined in profile or in partner definition.

Processing of TCP/IP Addresses

- '12.24' is equivalent to '12.24.*' is processed as '012.024.*'
- '12.24*' is processed as '012.24*'.

The address '12.241.20.1' meets criteria '12.24*' but not criteria '12.24' .

The following example illustrates the syntax of the SYSSSL file. Note that host names must be uppercase.

```
  File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help
-------------------------------------------------------------------------------
ISREDDE2   TOMC.ANMSSL(SYSSSL) - 01.42                  Columns 00001 00072
Command ===>                                              Scroll ===> CSR
000019 *
000020 * IP
000021 *
000022 IH=XBF.OFF*,CF=02               GROUP 2
000023 IH=MVS*,CF=10                   GROUP 3
000024 IA=12.24,CF=04                  (=012.024.*)
000025 IA=10.24*,CF=13,DN=DN03         (=010.24*)
000026 IA=10.2,CF=14                   (=010.002.*)
000027 IA=10.2*,CF=15                  (=010.2*)
000028 IA=10.20.129.3,CF=06            EXACT MATCH
000029 IA=010.020.129.002,CF=06        EXACT MATCH
000030 IH=MVSB.XBF.COMPANY.COM,CF=05   EXACT MATCH
000031 /*
000032 *
```

Selection Algorithm

The exact image of the SYSSSL file is loaded in an internal table.

There are to types of process: the host name process and the address process. The handler starts with the host name process and looks up IH criteria. As soon as some IA criteria is found the process changes to address process.

The table is looked up entirely for an exact match: if no exact match is found the more precise match is used. The precision of the match is determined by the length on which the match is found.

If no match is found the default profile from the SYSIN is used. If the selected profile doesn't exist, the SSL session fails.

Below are the three scenarios:

1. All TCP/IP criteria are of type H: the process stops when an exact match is found. If no exact match is found the more precise match is used.
2. All TCP/IP criteria are of type A: the process changes to address process and stops when an exact match is found. If no exact match is found the more precise match is used.
3. Criteria are both of type A and H: the process starts with host name until an exact match is found or some address criteria is found. If the process changes to address mode it stops when an exact match is found either on the host name or on the address. If no exact match is found the more precise match on the address is used.

In the SYSSSL example above the partner with host name `MVSB.XBF.COMPANY.COM with address 12.24.54.3` will be processed with the SSL profile number `05` because an exact match is found for the host name although IA=12.24 criteria does match in address mode.

Profile Error

The SSL handler retrieves the requested configuration from parameters loaded during initialization or refresh. If the profile doesn't exist, the transfer fails with a session error. The NRC code SCF0nn is issued. 'nn' is the profile number. Message SSL0015W is issued.

Monitor SYSLOG

```
09/03/05 02:30:34 REQUEST 00000001 SESSION ERROR : SSLINI    NRC=SCF099 000000
```

ANM JESMSGLG

```
02.30.34 STC99845  SSL0015W CONFIGURATION FILE 99 NOT FOUND
```

Handshake Data

Information about handshake can be retrieved in monitor SYSLOG, Journal and ANM trace (see Working with traces on page 31).

Information available are:

- Selected profile
- Protocol (TLSV1.n)
- Cipher
- Key Share (TLSV1.3 only)
- DN member
- Type of authentication
- AT-TLS format used (IPH)
- Certificate

Handshake data in Monitor SYSLOG

```
OXBL004I REQUEST 00001715 COMMUNICATION OPENED (O) WITH CXMTL132 (I,010.120.131.074   ) APM 01  EFF 07 PESIT   S13
OXBL142I REQUEST 00001715 TLSV1.3 CIP 1301 KS 0029 DN          AUTH Y IPH N CERT CXZOSCERT
```

Handshake data in Monitor Journal

```
  Directories  Monitor  Tables  Requests  Help  Caps (OFF)              4.3.0.11

                            Journal  TOMC PSR$TST.PLEX.TOMC.SYSJNL
 Option ===> ____________________________________________________ Scroll ===> PAGE
                                                                    More:     +

 Request  00001715 IRVO     TOMC
 File     LOCALOOP DSN  PSR$TST.CXMTL132.LOCALOOP.D200327.A0001708
 TRC      -        PRC  -        SRC  -        Restarts  -
 Part Typ O File Type S   Data Type E          TRF-ID X:0006B3 00001715
        PI99
 Cnx In                                                        + Lrecl  ---80
 Cnx Out                                                       + Blksz  27920
 Sel In                                                        + Recfm  FB
 Sel Out                                                       +
                Dem  PSRAPC
 Dir     T      Part CXMTL132    R.U. A.ID          Service  N
 Notif   0      Org  CXMTL132    Type      N        Access   O
                Dest CXMTL132

 Addr    010.120.131.074        Host ZVIPA_3074.USTXLAB.ARICENT.COM
 Link    I      SPR  5F
 SSLCfg  13     Prot TLSV1.3  Cipher 1301     Key Share 0029     DN -
 Auth    Y      IPH  N        Certif CXZOSCERT

 Prio    1      PPR  01       Compres -
```

DN Control

This chapter describes how to implement certificate control.

Definition

DN control provides one more authentication level. After the end of handshake the SSL handler can control the information inside the certificates that have been authenticated by the z/OS SSL services. This control is based on control files created in the ANMSSL file.

The process is different for inbound and outbound communications.

The name of a control file is prefixed by 'DN'. The control file is processed only when required. Updates to these members can be considered as dynamic.

implementing DN Control

DN control is executed at the end of successful handshake. For an outbound connection (client mode) the partner is identified for an inbound connection (server mode) only the network address is known.

Client Mode

In client mode you can configure the DN control in the partner definition or in the SSL configuration file. In the following example partner CXM30751 uses SSL configuration SSLCFG05. This profile SSLCFG05 is associated with the control file DNCFG05 but for this partner the DN control is based on the DN0001 file.

```
 Directories  Monitor  Tables  Requests  Help  Caps (OFF)              4.3.0.11

                 Partner    CXM30751  of TOMC     - Mode View
Option ===> ____________________________________________________ Scroll ===> PAGE

TYPE: TOM PESIT-E

                                Dpcsid Alias .. CXM30751
TOM Password .......... PSWC    Dpcpsw Alias .. PSWC
Initialisation State .. E       APM Reception Class  B
Partner Type .......... T
RACF User  Group ...... PSRUSR     SYS1

Protocol  Table Number  5   2           SSL Profile 05
Presentation .......... -  (01-24)      DN Control  DN0001
Automatic Restart ..... Y               Sessions T I O    128 064 064

PI99 Connection ....... ____________________________________________________
                        ----+----1----+----2----+----3----+----4----+----5----
PI99 ACK Connection ... ____________________________________________________
                        ----+----1----+----2----+----3----+----4----+----5----
Network Link Type ..... I   Multi .. -
 IP Addr .. -                Port .. 51703
    Host .. ZVIPA_3073.USTXLAB.COM
            ----+----1----+----2----+----3----+----4----+----5----+----6----+-
Bnd Addr .. ________________
    Host .. ____________________________________________________________
            ----+----1----+----2----+----3----+----4----+----5----+----6----+-
 FTP  PASV  - Profile   -
 SNA  LUName -        LOGMode -        LOGData -        Disc N
Note ____________________________________________________________________
Last update USR0003 20/03/02 10:29:41
```



```
======SSLCFG05======
SSLCFG=*** PRODUCTION CONFIGURATION ***
SSLCER=Certificate for production
SSLCIP=3R
SSLTL1=Y
SSLVE3=N
SSLDNC=DNCFG05
```

Server Mode

In server mode the DN control is always defined in the SSL configuration file selected from the SYSSSL selection file. In the following example the partner whose host name is MVSB.XBF.COMPANY.COM will be associated to profile SSLCFG05 and DN control executed using DN0001 file because DN member override occurred in the SYSSSL rule.

```
====== SYSSSL ======
IH=XBF.OFF* CF=02                GROUP 2
IH=MVS* CF=10                    GROUP 3
IA=12.24 CF=04                   (=012.024*)
IA=10.2* CF=15                   (=010.02*)
IA=10.20.129.3 CF=06             EXACT MATCH
IH=MVSB.XBF.COMPANY.COM CF=05 DN=DN0001 EXACT MATCH
```

Processing DN Control

The SSL handler performs the DN control at the end of a successful handshake.

Syntax Rules

- A line starting by character '*' is a comment line. a blank line is ignored.
- A line starting by characters '/*' stops the process for the profile (End of file).
- A blank line is rejected.
- Blanks at the beginning of a line are ignored.

Four certificates can be controlled.

- The local certificate: LDN
- The local certificate issuer certificate: LISSDN
- The remote certificate: RDN
- The remote certificate issuer certificate: RISSDN

Each control must be described using a <TAG> </TAG> syntax. TAG value is LDN LISSDN RDN RISSDN. Each group of tag must be unique.

Any field in the certificate can be controlled using the keyword=value syntax. Patterns are allowed. The keyword fields can be 1 or 2 characters.

Characters '?' and '*' are processed this way :

- '?' means any character at this place.
- '*' must be placed at the end and means any string after.

```
   File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help
------------------------------------------------------------------------------
 EDIT       PROD.CEXPRESS.ANMSSL(DNCFG05) - 01.03           Columns 00001 00072
 Command ===>                                                 Scroll ===> CSR
 ****** ***************************** Top of Data ******************************
 000001 * LOCAL CONTROL
 000002 <LDN>
 000003   CN=AN4*
 000004   OU=TEST
 000005   C=*
 000006 </LDN>
 000007 <LISSDN>
 000008   CN=*
 000009   OU=T??T*
 000010 </LISSDN>
 000011 * REMOTE CONTROL
 000012 <DN>
 000013   CN=AN?CERT*
 000014   OU=TES*
 000015 </DN>
 000016 <ISSDN>
 000017   CN=AN8CERT
 000019 </ISSDN>
```

Performing DN Control

The DN control is performed if requested for the partner or for the profile. In case of error a WTO message SSLDN03E is issued by the ANM. it shows the request number and the involved control file along with the type of error. In the log of the monitor the return code indicates that the error is from DN Control for example NRC=SDC008 for an outbound call or SRC=SD08 for an inbound call. The return code 8 in the example points to one of the lines of the table below

```
Log of the monitor
09/03/05 02:58:10 REQUEST 00000001 SESSION ERROR : SSLINI    NRC=SDC004 000000
09/03/05 10:05:20 REQUEST 00000001 SESSION ERROR : SSLINI    NRC=SDC008 000000

09/03/05 10:49:54 INCOMING REQUEST REJECTED 00000020 -SSL-I  SRC=SD08 TRC=2154



Jesmsglg of the ANM
02.58.10 STC08024 SSLDN03E DN CONTROL  ERROR DETECTED R=00000001 DNCFG05  ALLODNCT
10.05.20 STC00428 SSLDN03E DN CONTROL  ERROR DETECTED R=00000001 DNCFG05  REJECTED "UNIT"^"Tes
```

Errors are identfied by the following codes and keywords

Code	Keyword	Explanation	Action
1	OPANMSSL	Open error on the ANMSSL file	Check the code - Contact support
2	NOMEMBER	Member not found	Check your configuration
3	LDYALINK	System error	Contact support
4	ALLODNCT	Error when allocating the DN file	Add parameter SSLCFG=Y in the SYSIN file of the monitor and ANMSSL DD card in the JCL of the ANM
5	OPENDNCT	Error when opening the DN file	Check the code - Contact support

Code	Keyword	Explanation	Action
6	LRECDNCT	Invalid ANMSSL record length	Allocate the ANMSSL file with a record length of 300 characters maximum
7	SYNTDNCT	Syntax error	Modify the DN file
8	REJECTED	Control failed	Check the certificate
9	DNINVKEY	Invalid tag	Modify the DN file
10	DNKEYACT	End of DN file was detected but an end tag is required	Modify the DN file

Working with traces

2 types of traces are available. DN control traces and System SSL handshake traces.

System SSL handshake traces are written to SYSPRINT DD.

DN control traces output is written to SYSDNCTL DD.

```
//SYSPRINT DD SYSOUT=&OUT
//SYSDNCTL DD SYSOUT=&OUT
```

SYSPRINT Information

The SYSPRINT file provides information about System SSL environment profile used and handshake data.

The SSL handler includes an internal trace viewable in the ANM SYSPRINT file. This trace shows data as it moves in the network and is processed by the protocol with additional characteristic information.

There are three levels of information : environment SSL session (handshake) and exchange of data. The trace can be activated at monitor startup by the parameter SSLTRC=1 of the SYSIN. This parameter activates by default environment and session levels.

The trace can be activated by the SSL configuration SSLTRC parameter. The table below shows the SSLTRC values.

SSLTRC = 0	No trace for this profile
SSLTRC = 1	Session trace is active for this profile
SSLTRC = 2	All data exchanged is traced for this profile

Environment information is displayed only if SSLTRC=1 in the SYSIN file.

Reading the SSL Trace

The trace is displayed in format close to XML format with each field defined by a tag. Each field is tagged with a timestamp and a process id.

```
</0102033D></Wed Mar 25 17:14:33 2020></SslServices>
```

There are multiple parts in the trace file each related to a specific phase. The most useful parts are <openClient> and <openServer> sections with configuration applied to the session the handshake section with exchanged buffers (<NetOData> <NetIData>) when handshake is successful the <handshakeValues> showing cipher and protocol selected the <CliCer> and <SrvCer> for detailed information about certificates.

```
</0102033D></Wed Mar 25 17:15:41 2020><HandshakeValues>
</0102033D></Wed Mar 25 17:15:41 2020><SessionID>AQIDPQAAAAAAAAAAAAAAAAAAAAAAAAAAXnuRvQAAAAE=</SessionID>
</0102033D></Wed Mar 25 17:15:41 2020><SecType>TLSV1.3</SecType>
</0102033D></Wed Mar 25 17:15:41 2020><Cipher>1301</Cipher>
</0102033D></Wed Mar 25 17:15:41 2020><KeyShare>0029</KeyShare>
</0102033D></Wed Mar 25 17:15:41 2020></HandshakeValues>
```

SYSDNCTL Information

The SYSDNCTL file provides a trace of the DN control process performed from the DN file and the certificates received during handshake.

The following example shows the control of the DN and the ISSDN of the remote partner from the DNCFG06 file:

```
   File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help
------------------------------------------------------------------------------
 EDIT       PROD.CEXPRESS.ANMSSL(DNCFG06) - 01.03           Columns 00001 00072
 Command ===>                                                 Scroll ===> CSR
 ****** ***************************** Top of Data ******************************
000011 * CONTROL REMOTE:
000012 <DN>
000013   CN=AN?CERT*
000014   OU=TES*
000015 </DN>
000016 <ISSDN>
000017   CN=IssCERT
000018   OU=Tes
000019 </ISSDN>
------------------------------------------------------------------------------
```

The DN is : CN=AN8CERT OU=TEST C=SSL

The ISSDN is : CN=IssCERT OU=UNIT C=SSL

```
SSLDN02I DN CONTROL PROCESS STARTED   R=00000001 DNCFG06
 DNCFG06 > <DN>
 PROCESSING REMOTE DN    L=0024 CN=AN8CERT OU=TEST C=SSL
 DNCFG06 >   CN=AN?CERT*
 CN=MATCH FOUND
 DNCFG06 >   OU=TES*
 OU=MATCH FOUND
 DNCFG06 > </DN>
 REMOTE DN    CONTROL SUCCESSFUL
 DNCFG06 > <ISSDN>
 PROCESSING REMOTE ISSDN L=0024 CN=IssCERT OU=UNIT C=SSL
 DNCFG06 >   CN=IssCERT
 CN=MATCH FOUND
 DNCFG06 >   OU=Tes
SSLDN03E DN CONTROL ERROR DETECTED    R=00000001 DNCFG06 REJECTED "UNIT"^"Tes"
SSLDN04I DN CONTROL PROCESS ENDED     R=00000001 DNCFG06
```

The control fails because ‘UNIT’ is different from ‘Tes’.

Changing line 18 of the DNCFG06 file ‘*OU=Tes*’ changed to ‘*OU=UNIT*’ the example shows a successfull control:

```
SSLDN02I DN CONTROL PROCESS STARTED   R=00000001 DNCFG06
 DNCFG06 > <DN>
 PROCESSING REMOTE DN    L=0024 CN=AN8CERT OU=TEST C=SSL
 DNCFG06 >   CN=AN8CERT*
 CN=MATCH FOUND
 DNCFG06 >   OU=TES*
 OU=MATCH FOUND
 DNCFG06 > </DN>
 REMOTE DN    CONTROL SUCCESSFUL
 DNCFG06 > <ISSDN>
 PROCESSING REMOTE ISSDN L=0024 CN=AN8CERT OU=UNIT C=SSL
 DNCFG06 >   CN=AN8CERT
 CN=MATCH FOUND
 DNCFG06 >   OU=UNIT
 OU=MATCH FOUND
 DNCFG06 > </ISSDN>
 REMOTE ISSDN CONTROL SUCCESSFUL
 DNCFG06 > END OF FILE
SSLDN04I DN CONTROL PROCESS ENDED     R=00000001 DNCFG06
```

Monitor console commands related to SSL

Enable/Disable the SSL handler

```
/F TOMJOB SSL=ON      activates the SSL handler
/F TOMJOB SSL=OFF     deactivates the SSL handler
```

Handler status can be controlled on ISPF using option 2.1

```
Directories  Monitor  Tables  Requests  Help  Caps (OFF)              4.3.0.11

                      Monitor Management           MO   NAMES INITIALIZED    |
Option ===> ____________________________________________________ Scroll ===> PAGE

TOMC

           F (ID)  Files       B  Bypass    N  Network    G  Global
           P (ID)  Partners    C  Coupling  T  Transfers  Z  Activity
           R (ID)  Requests    S  Shared  s * - A H I U   Mode

Monitor .... TOMC ACTIVE GLOBAL STANDALONE IRVO
Exit UEXJNL  L1B2PDIX ENABLED

                     S  Detail E  Enable     H Disable

_ Files              64      ENABLED _ Partners         618          ENABLED
_ Requests            8      ENABLED   Usage Percentage          3
_ Shared              -     DISABLED
_ Network                    ENABLED
  SSL                        ENABLED
_ Transfers  - Servers Used Allocated       -  48
```

Enable/Disable SSL Trace

```
/F TOMJOB SSLTRC=ON  enables the SSL handler trace
/F TOMJOB SSLTRC=OFF disables the SSL handler trace
```

Refresh the SYSSSL configuration

```
/F TOMJOB REF SYSSSL ANM is requested to refresh its SSL configuration
```


SSL Return Codes

SSL return codes are associated with messages shown in the ANM SYSPRINT file with the tag <GskError>.

Return code (hex)	Return code (decimal)	Constant	Explanation
0x00000000	0	GSK_OK	The task completes successfully. Issued by every function call that completes successfully.
0x00000001	1	GSK_INVALID_HANDLE	The environment or SSL handle is not valid. The specified handle was not the result of a successful open() function call.
0x00000002	2	GSK_API_NOT_AVAILABLE	The dynamic link library (DLL) was unloaded and is not available (occurs on Microsoft Windows systems only).
0x00000003	3	GSK_INTERNAL_ERROR	Internal error. Report this error to IBM Software Support.
0x00000004	4	GSK_INSUFFICIENT_STORAGE	Insufficient memory is available to complete the operation.
0x00000005	5	GSK_INVALID_STATE	The handle is not in a valid state for operation such as completing an init() operation on a handle twice.
0x00000006	6	GSK_KEY_LABEL_NOT_FOUND	Specified key label is not found in key file.
0x00000007	7	GSK_CERTIFICATE_NOT_AVAILABLE	Certificate is not received from the partner.
0x00000008	8	GSK_ERROR_CERT_VALIDATION	Certificate validation error.
0x00000009	9	GSK_ERROR_CRYPTO	Error processing cryptography.
0x0000000a	10	GSK_ERROR_ASN	Error validating ASN fields in certificate.
0x0000000b	11	GSK_ERROR_LDAP	Error connecting to user registry.
0x0000000c	12	GSK_ERROR_UNKNOWN_ERROR	Internal error. Report this error to IBM Software Support.
0x0000000d	13	GSK_INVALID_PARAMETER	Invalid parameter.
0x0000000e	14	GSK_ERROR_UNEXPECTED_INT_EXCEPTION	Invalid parameter. Report this error to IBM Software Support.

Return code (hex)	Return code (decimal)	Constant	Explanation
0x00000065	101	GSK_OPEN_CIPHER_ERROR	Internal error. Report this error to IBM Software Support.
0x00000066	102	GSK_KEYFILE_IO_ERROR	I/O error reading the key file.
0x00000067	103	GSK_KEYFILE_INVALID_FORMAT	The key file does not have a valid internal format. Recreate the key file.
0x00000068	104	GSK_KEYFILE_DUPLICATE_KEY	The key file has two entries with the same key.
0x00000069	105	GSK_KEYFILE_DUPLICATE_LABEL	The key file has two entries with the same label.
0x0000006a	106	GSK_BAD_FORMAT_OR_INVALID_PASSWORD	The key file password is used as an integrity check. Either the key file is corrupted or the password ID is incorrect.
0x0000006b	107	GSK_KEYFILE_CERT_EXPIRED	The default key in the key file has an expired certificate.
0x0000006c	108	GSK_ERROR_LOAD_GSKLIB	An error occurred loading one of the GSK dynamic link libraries. Check that GSK was installed correctly.
0x0000006d	109	GSK_PENDING_CLOSE_ERROR	Indicates that a connection is trying to be made in a GSK environment after the GSK_ENVIRONMENT_ CLOSE_OPTIONS was set to GSK_DELAYED_ ENVIRONMENT_CLOSE and gsk_environment_close() function was called.
0x000000c9	201	GSK_NO_KEYFILE_PASSWORD	Both the password and the stash-file name were not specified. The key file is not initialized.
0x000000ca	202	GSK_KEYRING_OPEN_ERROR	Unable to open the key file. Either the path was specified incorrectly or the file permissions did not allow the file to be opened.
0x000000cb	203	GSK_RSA_TEMP_KEY_PAIR	Unable to generate a temporary key pair. Report this error to IBM Software Support.
0x000000cc	204	GSK_ERROR_LDAP_NO_SUCH_OBJECT	A user name object was specified that is not found.
0x000000cd	205	GSK_ERROR_LDAP_INVALID_CREDENTIALS	A password that is used for an LDAP (lightweight directory access protocol) query is not correct.

Return code (hex)	Return code (decimal)	Constant	Explanation
0x000000ce	206	GSK_ERROR_BAD_INDEX	An index into the Fail Over list of LDAP servers was not correct.
0x000000cf	207	GSK_ERROR_FIPS_NOT_SUPPORTED	This installation of GSKit does not support FIPS mode of operation.
0x0000012d	301	GSK_CLOSE_FAILED	Indicates that the GSK environment close request was not properly managed. Cause is most likely due to a gsk_secure_socket*() command that is attempted after a gsk_close_environment() call.
0x00000191	401	GSK_ERROR_BAD_DATE	The system date was not set to a valid value.
0x00000192	402	GSK_ERROR_NO_CIPHERS	The SSLv2 and the SSLv3 are not enabled.
0x00000193	403	GSK_ERROR_NO_CERTIFICATE	The required certificate was not received from the partner.
0x00000194	404	GSK_ERROR_BAD_CERTIFICATE	The received certificate was formatted incorrectly.
0x00000195	405	GSK_ERROR_UNSUPPORTED_CERTIFICATE_TYPE	The received certificate type was not supported.
0x00000196	406	GSK_ERROR_IO	An I/O error occurred on a data read or write operation.
0x00000197	407	GSK_ERROR_BAD_KEYFILE_LABEL	The specified label in the key file is not found.
0x00000198	408	GSK_ERROR_BAD_KEYFILE_PASSWORD	The specified key file password is incorrect. The key file cannot be used. The key file also might be corrupt.
0x00000199	409	GSK_ERROR_BAD_KEY_LEN_FOR_EXPORT	In a restricted cryptography environment the key size is too long to be supported.
0x0000019a	410	GSK_ERROR_BAD_MESSAGE	An incorrectly formatted SSL message was received from the partner.
0x0000019b	411	GSK_ERROR_BAD_MAC	The message authentication code (MAC) was not successfully verified.
0x0000019c	412	GSK_ERROR_UNSUPPORTED	Unsupported SSL protocol or unsupported certificate type.
0x0000019d	413	GSK_ERROR_BAD_CERT_SIG	The received certificate contained an incorrect signature.

Return code (hex)	Return code (decimal)	Constant	Explanation
0x0000019e	414	GSK_ERROR_BAD_CERT	Incorrectly formatted certificate is received from the partner.
0x0000019f	415	GSK_ERROR_BAD_PEER	Did not receive a valid SSL protocol from the partner.
0x000001a0	416	GSK_ERROR_PERMISSION_DENIED	Report this error to IBM Software Support.
0x000001a1	417	GSK_ERROR_SELF_SIGNED	The self-signed certificate is not valid.
0x000001a2	418	GSK_ERROR_NO_READ_FUNCTION	The read() failed. Report this error to IBM Software Support.
0x000001a3	419	GSK_ERROR_NO_WRITE_FUNCTION	The write() failed. Report this error to IBM Software Support.
0x000001a4	420	GSK_ERROR_SOCKET_CLOSED	The partner closed the socket before the protocol completed.
0x000001a5	421	GSK_ERROR_BAD_V2_CIPHER	The specified V2 cipher is not valid.
0x000001a6	422	GSK_ERROR_BAD_V3_CIPHER	The specified V3 cipher is not valid.
0x000001a7	423	GSK_ERROR_BAD_SEC_TYPE	Report this error to IBM Software Support.
0x000001a8	424	GSK_ERROR_BAD_SEC_TYPE_COMBINATION	Report this error to IBM Software Support.
0x000001a9	425	GSK_ERROR_HANDLE_CREATION_FAILED	The handle cannot be created. Report this error to IBM Software Support.
0x000001aa	426	GSK_ERROR_INITIALIZATION_FAILED	Initialization failed. Report this internal error to service.
0x000001ab	427	GSK_ERROR_LDAP_NOT_AVAILABLE	Not able to access the specified user registry when a certificate is being validated.
0x000001ac	428	GSK_ERROR_NO_PRIVATE_KEY	The specified key did not contain a private key.
0x000001ad	429	GSK_ERROR_PKCS11_LIBRARY_NOTLOADED	A failed attempt was made to load the specified PKCS11 shared library.
0x000001ae	430	GSK_ERROR_PKCS11_TOKEN_LABELMISMATCH	The PKCS #11 driver failed to find the token that is specified by the caller.

Return code (hex)	Return code (decimal)	Constant	Explanation
0x000001af	431	GSK_ERROR_PKCS11_TOKEN_NOTPRESENT	A PKCS #11 token is not present in the slot.
0x000001b0	432	GSK_ERROR_PKCS11_TOKEN_BADPASSWORD	The password/pin to access the PKCS #11 token is not valid.
0x000001b1	433	GSK_ERROR_INVALID_V2_HEADER	The SSL header received was not a properly formatted SSLv2 header.
0x000001b2	434	GSK_CSP_OPEN_ERROR	Cannot open the hardware-based cryptographic service provider. Either the CSP name is not specified correctly or a failed attempt was made to access the specified CSP certificate store.
0x000001b3	435	GSK_CONFLICTING_ATTRIBUTE_SETTING	Attribute setting conflict between PKCS11 CMS key database and Microsoft Crypto API.
0x000001b4	436	GSK_UNSUPPORTED_PLATFORM	The requested function is not supported on the platform that the application is running. For example the Microsoft Crypto API is not supported on platforms other than Windows 2000.
0x000001b6	438	GSK_ERROR_INCORRECT_SESSION_TYPE	Incorrect value is returned from the reset session type callback function. Only GSKit gsk_sever_session gsk_sever_session_with_cl_auth or gsk_sever_session_with_cl_auth_crit is allowed.
0x000001f5	501	GSK_INVALID_BUFFER_SIZE	The buffer size is negative or zero.
0x000001f6	502	GSK_WOULD_BLOCK	Used with nonblocking I/O. Refer to the nonblocking section for usage.
0x00000259	601	GSK_ERROR_NOT_SSLV3	SSLv3 is required for reset_cipher() and the connection uses SSLv2.
0x0000025a	602	GSK_MISC_INVALID_ID	A valid ID was not specified for the gsk_secure_soc_misc() function call.
0x000002bd	701	GSK_ATTRIBUTE_INVALID_ID	The function call does not have a valid ID. This issue might also be caused by specifying an environment handle when a handle for an SSL connection should be used.
0x000002be	702	GSK_ATTRIBUTE_INVALID_LENGTH	The attribute has a negative length which is not valid.

Return code (hex)	Return code (decimal)	Constant	Explanation
0x000002bf	703	GSK_ATTRIBUTE_INVALID_ENUMERATION	The enumeration value is not valid for the specified enumeration type.
0x000002c0	704	GSK_ATTRIBUTE_INVALID_SID_CACHE	A parameter list that is not valid for replacing the SID cache routines.
0x000002c1	705	GSK_ATTRIBUTE_INVALID_NUMERIC_VALUE	When a numeric attribute is set the specified value is not valid for the specific attribute that is being set.
0x000002c2	706	GSK_CONFLICTING_VALIDATION_SETTING	Conflicting parameters were set for additional certificate validation.
0x000002c3	707	GSK_AES_UNSUPPORTED	The AES cryptographic algorithm is not supported.
0x000002c4	708	GSK_PEERID_LENGTH_ERROR	The PEERID does not have the correct length.
0x000002c5	709	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OFF	The particular cipher is not allowed when FIPS mode of operation is off.
0x000002c6	710	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON	No approved FIPS ciphers are selected in FIPS mode of operation.
0x00000641	1601	GSK_TRACE_STARTED	The trace started successfully.
0x00000642	1602	GSK_TRACE_STOPPED	The trace stopped successfully.
0x00000643	1603	GSK_TRACE_NOT_STARTED	No trace file was previously started so it cannot be stopped.
0x00000644	1604	GSK_TRACE_ALREADY_STARTED	Trace file is started so it cannot be restarted.
0x00000645	1605	GSK_TRACE_OPEN_FAILED	Trace file cannot be opened. The first parameter of gsk_start_trace() must be a valid full path file name.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products services or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product program or service is not intended to state or imply that only that IBM product program or service may be used. Any functionally equivalent product program or service that does not infringe any IBM intellectual property right may be used instead. However it is the user's responsibility to evaluate and verify the operation of any non-IBM product program or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries in writing to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk NY 10504-1785

U.S.A.

For license inquiries regarding double-byte character set (DBCS) information contact the IBM Intellectual

Property Department in your country or send inquiries in writing to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14 Shimotsuruma Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND EITHER EXPRESS OR IMPLIED INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF NON-INFRINGEMENT MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions therefore this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged should contact:

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose CA__95141-1003

U.S.A.

Such information may be available subject to appropriate terms and conditions including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of 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.

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

This information is for planning purposes only. The information herein is subject to change before the products described become available. This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible the examples include the names of individuals companies brands and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy the photographs and colour illustrations may not appear.

Trademarks

IBM the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corp. registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

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.

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

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.

Linux is a registered trademark of Linus Torvalds 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.

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.

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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.

Linear Tape-Open LTO the LTO Logo Ultrium and the Ultrium Logo are trademarks of HP IBM Corp. and Quantum in the U.S. and other countries.

Connect:Express® Connect Control Center® Connect:Direct® Connect:Enterprise Gentran® Gentran:Basic® Gentran:Control® Gentran:Director® Gentran:Plus® Gentran:Realtime® Gentran:Server® Gentran:Viewpoint® Sterling Commerce™ Sterling Information Broker® and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce Inc. an IBM Company.

Other company product and service names may be trademarks or service marks of others.