Connect:Express® z/OS

SSL Option

Version 4.2.3

Sterling Commerce
An IBM Company

Connect:Express z/OS SSL Option
Version 4.2.3
First Edition

Contents

Activating the SSL Option

This document complements the Connect:Express z/OS version 4.2.3 documentation. It describes the use of the SSL option.

Prerequisites

The SSL functions are linked to the SSL services of z/OS, which should be installed. They invoke the UNIX system services of z/OS (POSIX), which should thus be installed and configured.

To perform internal tests, you should configure two monitors.

License Key

The SSL option is specified in the license key: the license key should contain the SSL option. You can verify this parameter using the 0.O option in the ISPF interface.

```
TOM4230-------------- OPTIONS ------------------------------------------------
 OPTION ===>                                              X EXIT, -PF3- END

MONITOR  => TOM4 / PSRTOM4M  CSGA ACTIVE GLOBAL
             AP BROWSE ASSET-PROTECTION.       RACFCN= S ADHOCN= Y UPRFCT= Y
                0=OPTION NOT AUTHORIZED, CPUID=000194BA2064
 ACT       04 : 1       AUTHORIZATIONS FOR FTP-HTML.
 BSC       02 : 1       LINK VIA BSC (ETEBAC1/2).
 CICS      10 : 1       CICS INTERFACE.
 ETEBAC3   05 : 1       LINK VIA ETEBAC3.
 FTP       03 : 1       LINK VIA FTP.
 IMS       16 : 1       IMS INTERFACE.
 LOCAL     09 : 1       LOCAL MONITOR.
 LU6.2     06 : 1       LINK VIA LU6.2.
 MBO       12 : 1       MAILBOX OPTION.
 ODETTE    11 : 1       LINK VIA ODETTE.
 PAC       08 : 1       EXPLOITATION PACKAGE.
 PESIT     01 : 1       LINK VIA PESIT (FRENCH).
 SYSPLEX   19 : 1       SYSPLEX INTERFACE.
 TCP-IP    15 : 1       LINK VIA TCP-IP.
           14 : 0
 SSL       20 : 1       SSL INTERFACE.
```

Asset Protection: Using the AP option, you can display the Asset Protection file:

```
M OPERATING-SYSTEM OS390
B PESIT
B FTP
B ETEBAC3
B ODETTE
B TCPIP
B LU-6.2
B LU-2
B MANAGEMENT-TOOLS
B LOCAL
B CICS
B IMS
B ETEBAC1/2
B DIFFUSION
B ETEBAC5
B SSL
```

Using the SSL Option

The SSL option uses the SSL services of z/OS, which can be associated with the Integrated Cryptographic Service Facility (ICSF). Certificate management is accomplished either with the SSL utility *gskkyman* or with the specific RACF functions recommended and described in this document.

This functionality integrates with the Connect:Express architecture via an SSL handler through which the network services of the monitor (the ANM) interface with z/OS SSL services.

SSL activation is independent of the transfer protocol used (PeSIT, Etebac, or Odette), and of the network used (TCP/IP, X25). Some configuration parameters may differ.

The functionality is available in client or server mode.

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

Security Concepts

Cryptography is the science of keeping messages private. A cryptographic system uses encryption keys between two trusted communication partners. These keys encrypt and decrypt information so that the information is known only to those who have the keys.

There are two kinds of cryptographic system: symmetric key and asymmetric key. Symmetric key (or secret key) systems use the same secret key to encrypt and decrypt a message. Asymmetric key (or public key)
systems use one key (public) to encrypt a message and a different key (private) to decrypt it. Symmetric key systems are simpler and faster, but two parties must somehow exchange the key in a secure way, because if the secret key is discovered by outside parties security is compromised. Asymmetric key systems avoid this problem because the public key may be freely exchanged but the private key is never transmitted.

Cryptography provides information security as follows:

Authentication verifies that the entity on the other end of a communications link is the intended recipient of a transmission.
Non-repudiation provides undeniable proof of origin of transmitted data.
Data integrity ensures that information is not altered during transmission.
Data confidentiality ensures that data remains private during transmission.

The SSL Option enables you to select one of two security protocols to use to secure data during electronic transmission: Transport Layer Security protocol (TLS) and Secure Sockets Layer protocol (SSL) .

Secure Sockets Layer Protocol (SSL) and Transport Layer Security Protocol (TLS)

The SSL and the TLS protocols use certificates to exchange a session key between the node that initiates the data transfer and the node that receives the data. A certificate is an electronic document that associates a public key with an individual or other entity. It enables you to verify the claim that a given public key belongs to a given entity. A certificate authority (CA) is the entity responsible for issuing and revoking these certificates. The CA validates an applicant's identity, creates a certificate, and then signs the certificate, thus vouching for an entity's identity.

The SSL and TLS protocols provide three levels of security:

The first level of security is activated when a trading partner connects to a Connect:Express server. After the initial handshake, the Connect:Express server sends its digital certificate to the trading partner. The trading partner checks that it has not expired and that it has been issued by a Certification Authority the trading partner trusts. The trading partner must have a trusted root file that identifies the Certificate Authority. If the security fails on any one of these checks, the trading partner is notified that the site is not secure and the connection fails.

- The second level of security, called client authentication, requires that the trading partner send its own certificate. If enabled, the Connect:Express server requests certificate information from the trading partner after it returns its certificate information. If the client certificate is signed by a trusted source, the connection is established. In order to perform this security check, the trading partner must have a key certificate file available at its site and the Connect:Express server must have a trusted root file that validates the identity of the Certificate Authority (CA) who issued the key certificate.

- The third level of security is defined in client authentication and requires that a certificate common name be defined in the receiver certificate. The Connect:Expres server searches the certificate file it receives from the trading partner and looks for a certificate common name. If the server cannot find the certificate common name, communication fails.

To communicate using the SSL or TLS protocol, you must have both an X.509 certificate and a private key. The SSL and TLS protocols provide data security in the following areas:

- Strong authentication—Because the CA went through an established procedure to validate an applicant's identity, users who trust the CA can be sure the key is held by the owner. The CA prevents impersonation and provides a framework of trust in associating an entity with its public and private keys.
-
- Proof of data origin and data integrity validation—The certificate provides proof of origin of electronic transmission, and encryption validates data integrity. Encrypting the private key ensures that the data is not altered.
-
- Data confidentiality—Cipher suites encrypt data and ensure that the data remains confidential. Sensitive information is converted to an unreadable format (encrypted) by the sender before being sent to the receiver. The receiver then converts (decrypts) the information back into a readable format. Both the SSL protocol and the TLS protocol manage secure communication in a similar way. However, TLS provides a more secure method for managing encryption.

Both the SSL protocol and the TLS protocol manage secure communications in a similar way. However, TLS provides a more secure method for managing authentication and exchanging of messages, using the following features:

- While SSL provides keyed message authentication, TLS uses the more secure Key-Hashing for Message Authentication Code (HMAC) to ensure that a record cannot be altered during transmission over an open network such as the Internet.
- TLS defines the Enhanced Pseudorandom Function (PRF), which uses two hash algorithms to generate key data with the HMAC. Two algorithms increase security by preventing the data from being changed if only one algorithm is compromised. The data remains secure as long as the second algorithm is not compromised.
- While SSL and TLS both provide a message to each node to authenticate that the exchanged messages were not altered, TLS uses PRF and HMAC values in the message to provide a more secure authentication method.
- To provide more consistency, the TLS protocol specifies the type of certificate which must be exchanged between nodes.
- TLS provides more specific alerts about problems with a session and documents when certain alerts are sent.

Configuring the SSL Option

Before using the SSL option, you should configure the components involved in secured transfer: the TOM monitor, the ANM, and the database in which SSL certificates are stored. It is recommended to use the RACF functions for managing certificates.

You should associate the ANM with a RACF keyring to which you will connect the Connect:Express key certificate files and the trusted root files that validate the identity of the certificate authorities (CA) .

Configuring the Monitor

Monitor setup allows you to define its local characteristics as an SSL monitor : handler activation, definition of access by clients, default certificate specification, and 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 specific ports.
- SSL access over X25 are characterized by X25 user data or by subaddresses.
- Default values are z/OS SSL services defaults.
- Sysin values are default values for ANM configuration files
- The SSL profile defined in the SYSIN is SSL profile number zero (SSLCFG00)

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

TCPORG=(HPNS, jobtcpip) changed to TCPORG=(SOE)

The table below describes the parameters that characterize the 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.

SYSIN File

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

SSLOPT=Y
SSLKRG=Name of RACF keyring (or combination SSLDTTB + SSLPSW)
SSLPRT=TCP/IP port listening for SSL clients
And/or
SSLUDF=X25 user data for which SSL clients are waiting

Field	Range of Values	Description	Type
TCPORG	(SOE)	This value determines use of the z/OS Open Edition interface. It is required to be able to make the SSL and TCP/IP handlers work together.	Required
SSLOPT	Y/N	Activation of the SSL handler. N is the default value. Y requires at minimum the following SSL configuration parameters.	Optional
SSLCFG	Y/N	ANM SSL configuration files used. N is the default value. Y requires that the ANMSSL file is defined and allocated to the ANM.	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	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.	Required
SSLPSW	1–16 chars mixed case	Password allowing access to the HFS database in which certificates are stored.	Required
SSLCER	1–34 chars mixed case	Label of the default certificate (SSLCFG00 profile) referenced in the certificate database or in the RACF keyring. May include blanks. If absent, the default certificate defined in the database is used. Example : SSLCER=Label of Paris 2 server	Optional
SSLPRT	1–5 numeric chars	TCP/IP port number listening for calls under SSL. Range from 1 to 65535.	Min.
SSLUDF	1–16 hex chars	X25 user data expected from SSL clients. The number of characters should be even, for a maximum of eight pairs. Example : SSLUDF=AB02	Min.
SSLSAD	1–4 numeric chars	X25 subaddress expected from SSL clients.	Min.
SSLPRO	1–5 numeric chars	TCP/IP port number listening for Odette calls under SSL. Ranges from 1 to 65535.	Min.
SSLUDO	1–16 hex chars	X25 user data expected by Odette SSL clients. The number of characters should be even, for a maximum of eight pairs. Example : SSLUDF=AB04	Min.
SSLSAO	1–4 numeric chars	X25 subaddress expected from Odette SSL clients.	Min.
SSLTRC	0/1	Default trace option (SSLCFG00 profile) . Zero is the default value. One activates the trace environment of the SSL handler. This trace is written to an ANM SYSPRINT file.	Optional
SSLTIM	1–6 numeric chars	Retention duration of the SSL session identifier, in seconds. By default, the value is equal to 86,400 seconds.	Optional
SSLTL1	Y/N	Default support of TLS V1 (SSLCFG00 profile). The default is ‘Y’	Optional
SSLVE3	Y/N	Default support of SSL V3 (SSLCFG00 profile). The default is ‘Y’	Optional
SSLVE2	Y/N	Default support of SSL V2 (SSLCFG00 profile). The default is ‘N’	Optional
SSLAUT	Y/N	N is the default value. Y indicates that in server mode, client authentication will be required.	Optional
SSLCIP	1–32 hex chars	Default cipher suite (SSLCFG00 profile). Indicates the order of preference of numerical options, among the options supported by the z/OS SSL services. The number of characters should be even, for a maximum of eight pairs. Example : SSLCIP=09060504.	Optional

		(continued) The values provided are not controlled at the time of initialization; make sure they are valid. By default the list used by z/OS is as follows : 050435363738392F303132330A1613100D0915120F0C0306020100 <u>The list below comprises the values supported by z/OS for SSL version 3 and TLS :</u> 00 No encrypt. or message authentication and RSA key exchange 01 No encrypt with MD5 message authentication and RSA key exchange 02 No encrypt with SHA-1 message authentication and RSA key exchange 03 40-bit RC4 encrypt with MD5 message authentication and RSA key exchange 04 128-bit RC4 encrypt with MD5 message authentication and RSA key exchange 05 128-bit RC4 encrypt with SHA-1 message authentication and RSA key exchange 06 40-bit RC2 encrypt with MD5 message authentication and RSA key exchange 09 56-bit DES encrypt with SHA-1 message authentication and RSA key exchange 0A 168-bit Triple DES encrypt with SHA-1 message authentication and RSA key exchange 0C 56-bit DES encrypt with SHA-1 message authentication and fixed Diffie-Hellman key exchange signed with a DSS certificate 0D 168-bit Triple DES encrypt with SHA-1 message authentication and fixed Diffie-Hellman key exchange signed with a DSS certificate 0F 56-bit DES encrypt with SHA-1 message authentication and fixed Diffie-Hellman key exchange signed with an RSA certificate 10 168-bit Triple DES encrypt with SHA-1 message authentication and fixed Diffie-Hellman key exchange signed with an RSA certificate 12 56-bit DES encrypt with SHA-1 message authentication and ephemeral Diffie-Hellman key exchange signed with a DSS certificate 13 168-bit Triple DES encrypt with SHA-1 message authentication and ephemeral Diffie-Hellman key exchange signed with a DSS certificate 15 56-bit DES encrypt with SHA-1 message authentication and ephemeral Diffie-Hellman key exchange signed with an RSA certificate 16 168-bit Triple DES encrypt with SHA-1 message authentication and ephemeral Diffie-Hellman key exchange signed with an RSA certificate 2F 128-bit AES encrypt with SHA-1 message authentication and RSA key exchange 30 128-bit AES encrypt with SHA-1 message authentication and fixed Diffie-Hellman key exchange signed with a DSS certificate 31 128-bit AES encrypt with SHA-1 message authentication and fixed Diffie-Hellman key exchange signed with an RSA certificate 32 128-bit AES encrypt with SHA-1 message authentication and ephemeral Diffie-Hellman key exchange signed with a DSS certificate 33 128-bit AES encrypt with SHA-1 message authentication and ephemeral Diffie-Hellman key exchange signed with an RSA certificate 35 256-bit AES encrypt with SHA-1 message authentication and RSA key exchange 36 256-bit AES encrypt with SHA-1 message authentication and fixed Diffie-Hellman key exchange signed with a DSS certificate 37 256-bit AES encrypt with SHA-1 message authentication and fixed Diffie-Hellman key exchange signed with an RSA certificate 38 256-bit AES encrypt with SHA-1 message authentication and ephemeral Diffie-Hellman key exchange signed with a DSS certificate 39 256-bit AES encrypt with SHA-1 message authentication and ephemeral Diffie-Hellman key exchange signed with an RSA certificate For SSL version 2, the list is always taken to be equal to the default z/OS list; namely: 713642 <u>The list below comprises the values supported by z/OS, for SSL version 2 :</u> 1 128-bit RC4 encryption with MD5 message authentication (128-bit secret key) 2 128-bit RC4 export encryption with MD5 msg. authentication (40-bit secret key) 3 128-bit RC2 encryption with MD5 message authentication (128-bit secret key) 4 128-bit RC2 export encryption with MD5 msg. authentication (40-bit secret key) 6 56-bit DES encryption with MD5 message authentication (56-bit secret key) 7 168-bit Triple DES encryption with MD5 msg. authentication (168-bit secret key)	

MVS commands to the Monitor

The SSL handler can be enabled or disabled: Its status is displayed in the following general screen, TSO/ISPF option 2.1.

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

```
TOM4220     OPERATIONS CONTROL    ID=          MODE= *
 OPTION ===> !

            ^ F (ID)       - FILES.           B   - BYPASS.       PSR0008
              P (ID)       - PARTNERS         C   - COUPLING.     07/01/26
              R (ID)       - REQUESTS....     S   - SHARED.       03:41
              N            - NETWORK.         G   - GLOBAL.       CSGA
              T            - TRANSFERS.       Z   - ACTIVITY.     CSGPLEX
              */-/A/H/I/U  - 'mode'.

       MONITOR   ===> TOM4 / CSGA  ACTIVE   GLOBAL    STANDALONE
       EXIT UEXJNL  : L1B2PAEX     ENABLED

  ----------- S DISPLAY DETAILS, E ENABLE, H DISABLE
                                    V
  _   1077     FILES        - RESOURCE   : ENABLED
  _   591      PARTNERS     - RESOURCE   : ENABLED
  _   -        REQUESTS     - RESOURCE   : ENABLED      IN USE AT -  %
  _   -        SHARED       - RESOURCE   : DISABLED
  _            NETWORK      - SEE DETAIL : ENABLED
  _            TRANSFERS    - SEE DETAIL, EFFECTORS USED/ALLOC. : -   /  32
              SSL          - RESOURCE   : ENABLED
            X EXIT, -PF3- END, -ENTER- CONTINUE, -PF10/11- SCROLL
```

Configuring the ANM

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  SSL0014I CONFIGURATION FILES PROCESS COMPLETED
02.21.43 STC07965  ANMSSL02 SSL HANDLER IS ACTIVE
```

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

```
SSLCFG=Y
```

```
09.30.50 STC97322  SSL0010I STARTING CONFIGURATION FILES PROCESS
09.30.50 STC97322  SSL0014I SSLCFG01 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0014I SSLCFG02 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0014I SSLCFG03 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0014I SSLCFG05 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0014I SSLCFG07 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0014I SSLCFG08 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0014I CONFIGURATION FILES PROCESS COMPLETED
09.30.50 STC97322  ANMSSL02 SSL HANDLER IS ACTIVE
```

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, record length less equal 300 bytes.

The following example shows the ANMSSL members.

```
   Menu  Functions  Confirm  Utilities  Help
------------------------------------------------------------------------------
 EDIT              PROD.CEXPRESS.ANMSSL                    Row 00001 of 00014
 Command ===>                                                 Scroll ===> CSR
            Name     Prompt       Size   Created          Changed          ID
 _________ README                   25  2009/02/18  2009/02/25 02:53:45  USER008
 _________ DNCFG05                  19  2009/02/18  2009/02/25 02:53:45  USER008
 _________ DNCFG06                  18  2009/02/18  2009/02/24 09:16:55  USER008
 _________ DN000001                 16  2008/11/17  2009/02/18 06:15:12  USER008
 _________ DN000002                 16  2008/11/17  2009/02/18 06:15:12  USER008
 _________ SSLCFG01                  1  2009/01/21  2009/01/21 08:25:54  USER008
 _________ SSLCFG02                  2  2009/01/21  2009/01/21 07:50:52  USER008
 _________ SSLCFG03                  2  2009/01/21  2009/02/09 00:57:35  USER008
 _________ SSLCFG04                  3  2009/01/13  2009/01/21 04:08:01  USER008
 _________ SSLCFG05                  9  2008/11/17  2009/03/02 10:11:41  USER008
 _________ SSLCFG06                  8  2008/11/17  2009/03/02 09:48:17  USER008
 _________ SSLCFG07                  3  2009/01/13  2009/01/21 04:06:28  USER008
 _________ SYSSSL                   49  2008/12/29  2009/03/02 10:11:09  USER008
           **End**
```

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

Any other member, ‘README’ for example, the name of which doesn’t respect the rules above, is ignored.

SSL Default Configuration

The ANM SYSLOG file shows the list of default parameters.

JCL Procedure

Specific files for SSL options are shwn below :

- LOADSSL library is in STEPLIB
- ANMSSL library is allocated using ANMSSL DD card
- The SYSOUT file SYSPRINT displays SSL traces
- The SYSOUT file SYSCFG is a report of the SSL configuration files load procedure
- The SYSOUT file SYSDNCTL provides a trace of the DN control process

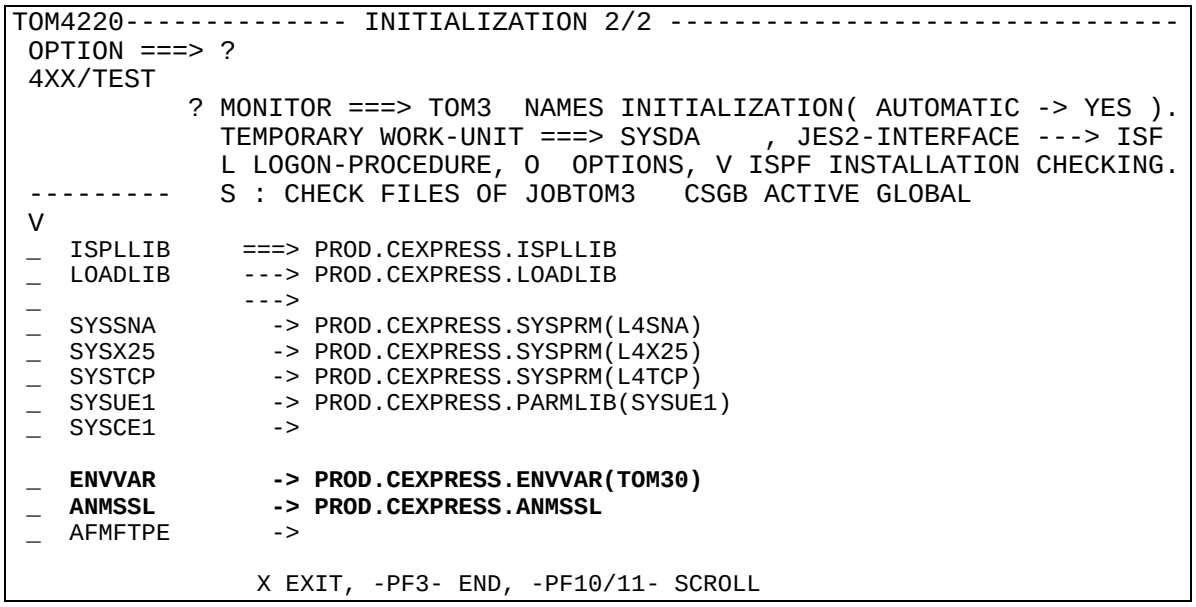
Using the TCP/IP Opend Edition interface may require the addition of a card to determine which IP stack to use. If it is absent, all the computer's stack IPs are used equally, and this can disrupt the processing of address and host name control.

```
//TOM3ANM PROC OUT=X
//TOMV422 EXEC PGM=P1ANM000,REGION=0M,TIME=1440,
// PARM=('SSN=&SSN','MSN=&MSN','LHM=&LHM','HSS=&HSS','ISN=&ISN')
//*-------------------------------------------------------------------
//* perform group must be the same as VTAM (for X25 treatment).
//* region must be at least : (effectors count x 68k)
//* (32 x 68k) = 2200k
//* region size must be increased if using large buffer size.
//*-------------------------------------------------------------------
//* ANM PROCEDURE (AUXILIARY NETWORK MANAGER)
//*
//* Note : if Connect:Express LOADLIB is in LINKLIST
//* the following //STEPLIB card
//* can be suppressed for ANM procedure.
//* But the APM needs always a SYSLIB.
//*-------------------------------------------------------------------
//BPXTCAF EXEC PGM=BPXTCAFF,PARM=LCTCPB2
//*-------------------------------------------------------------------
//STEPLIB  DD DISP=SHR,DSN=PROD.CEXPRESS.LOADSSL
//         DD DISP=SHR,DSN=PROD.CEXPRESS.LOADLIB
//SYSUDUMP DD SYSOUT=&OUT
//SYSDUMP  DD SYSOUT=&OUT
//SYSMSG   DD SYSOUT=&OUT
//SYSLOG   DD SYSOUT=&OUT
//SYSPRINT DD SYSOUT=&OUT
//SYSIN DD DISP=SHR,DSN=index1.TOMV422.PARMLIB(PARMANM3) IN
//SYSTCPD  DD DISP=SHR,DSN=SYS.TCPIP.PARMS(TCPDATA)
//CEEDUMP  DD SYSOUT=&OUT
//CEEMOUT  DD SYSOUT=&OUT
//CEEMSG   DD SYSOUT=&OUT
//ENVIRON  DD DSN=PROD.CEXPRESS.SSLTCFG,DISP=SHR
//ANMSSL   DD DSN=PROD.CEXPRESS.ANMSSL,DISP=SHR
//SYSCFG   DD SYSOUT=&OUT
```

The card ENVIRON DD can be activated to get a trace on the SSL services of z/OS. The language environment configuration file $$SSLTRC$$ is described in the section of this document called "Trace gskssl."

The ANMSSL file is available through option 0 of the TSO/ISPF operator interface. Use option 'S' to edit the file. Update the file and stop-start the SSL handler using the following commands :

```
/F jobtom,SSL=OFF
/F jobtom,SSL=ON
```



```
TOM4220-------------- INITIALIZATION 2/2 -------------------------------
 OPTION ===> ?
 4XX/TEST
           ? MONITOR ===> TOM3  NAMES INITIALIZATION( AUTOMATIC -> YES ).
             TEMPORARY WORK-UNIT ===> SYSDA    , JES2-INTERFACE ---> ISF
             L LOGON-PROCEDURE, O  OPTIONS, V ISPF INSTALLATION CHECKING.
 ---------   S : CHECK FILES OF JOBTOM3   CSGB ACTIVE GLOBAL
 V
 _  ISPLLIB     ===> PROD.CEXPRESS.ISPLLIB
 _  LOADLIB     ---> PROD.CEXPRESS.LOADLIB
 _              --->
 _  SYSSNA        -> PROD.CEXPRESS.SYSPRM(L4SNA)
 _  SYSX25        -> PROD.CEXPRESS.SYSPRM(L4X25)
 _  SYSTCP        -> PROD.CEXPRESS.SYSPRM(L4TCP)
 _  SYSUE1        -> PROD.CEXPRESS.PARMLIB(SYSUE1)
 _  SYSCE1        ->

 _  ENVVAR        -> PROD.CEXPRESS.ENVVAR(TOM30)
 _  ANMSSL        -> PROD.CEXPRESS.ANMSSL
 _  AFMFTPE       ->

                 X EXIT, -PF3- END, -PF10/11- SCROLL
```

Using SSL Profiles

SSL profiles are processed by the ANM, during inbound or outbound SSL handshake. Profiles enable you 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' different from '00'

The two numeric characters 'nn', different from '00', identify the profile. SSLCFG00 is ignored by the SSL handler, according to the rules defined in the paragraph before.

You can define one or several parameters in a profile. The SSL profile defined in the monitor SYSIN is configuration number 00 (SSLCFG00). For an active session the SSL profile used is merged from values in the following order:

1. Values from SSLCFG profile
2. Values from SYSIN
3. Default values from z/OS

The following table shows the list of SSL configuration parameters and where they can be defined :

Parameter	**z/OS**	**Sysin**	**SSLCFG**
SSL handler activation		SSLOPT (Y/N)	
Name of the RACF keyring allocated to the ANM		SSLKRG	
Name of the HFS database Password		SSLDTB SSLPSW	
Listen port, sub address …. ….. for TCP/IP or X25 for PeSIT or odette		SSLPRT SSLPRO SSLSAD SSLSAO SSLUDF SSLUDO	
Client authentication	No	SSLAUT (Y/N)	
SSL session ID retention	86400 seconds	SSLTIM	
Local certificate label	Default certificate	SSLCER	SSLCER
SSL version (for compatibility)	30	SSLLEV (31,30,20)	
Support of SSL V2	No	SSLVE2 (Y/N)	SSLVE2 (Y/N)
Support of SSL V3	Yes	SSLVE3 (Y/N)	SSLVE3

Parameter	z/OS	Sysin	SSLCFG
			(Y/N)
Support of TLS V1	Yes	SSLTL1 (Y/N)	SSLTL1 (Y/N)
Cipher liste	050435363738392F303132330A16 13100D0915120F0C0306020100	SSLCIP	SSLCIP
Trace option for the SSL handler		SSLTRC (0/1)	SSLTRC (0/1/2)
DN Control			SSLDNC
Profile description			SSLCFG
Profile status			STATUS

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 active, except SSLCFG=$DUMMY$, that is used for compatibility with version 4.2.0.
Keywords are unique and upper case.

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

Example of profile :

```
   File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help
-------------------------------------------------------------------------------
 EDIT       PROD.CEXPRESS.ANMSSL(SSLCFG05) - 01.26         Columns 00001 00072
 Command ===>                                                 Scroll ===> CSR
 ****** ***************************** Top of Data ******************************
 000001 SSLCFG=*** PRODUCTION CONFIGURATION ***
 000002
 000003 STATUS=E               E/H
 000004 SSLCER=Certificat 05                     END OF FIELD
 000005 * No trace in production
 000006 SSLTRC=0               0/1/2  (NO, SHORT, FULL)
 000007 SSLCIP=0A
 000008 SSLTL1=Y               Y/N
 000009 SSLVE2=N               Y/N
 000010 SSLVE3=N               Y/N
 000011 SSLDNC=DNCFG05         DN......
 ****** **************************** Bottom of Data ****************************
```

The table below gives the list of parameters that you can use in a profile, with their description and type. The default values are those defined in the monitor SYSIN.

Champ	Lg/Val	Description	Type
SSLCFG	Depends on LRECL	Description of the profile. Example : SSLCFG=*** Special Configuration *** SSLCFG=$DUMMY$: this profile is equivallent to profile 00 (SYSIN) and this parameter must be unique.	Inactive Active
STATUS	E/H	Defines the status of the profile. The defeult is 'E'=Enable. You can disable the profle using STATUS=H.	Active
SSLCER	1 à 34 car. M+m	Label of the local certificat, defined in the certificates data base or in the RACF keyring : blanks, upper and lower case characters are valid. Example : SSLCER=Lable of special certificat	Active
SSLTRC	0/1 /2	'0' disable the trace. '1' activate the trace for handshake only. '2' activate the ful trace, handshake and data flow. The trace is writtent in the SYSPRINT file of ANM.	Active
SSLCIP	1 à 32 c. hex.	Cipher suite : define the preferred order of cipher algorithm among z/OS supported options. The number of characters must be even, 1 to sixteen pairs of hexadecimal numbers. Example SSLCIP=090605040A.	Active
SSLTL1	Y/N.	Support of TLS V1	Active
SSLVE2	Y/N.	Support of SSL V2	Active
SSLVE3	Y/N.	Support of SSL V3	Active
SSLDNC	DN….	The name of a DN control file. Refer to section '*DN Control*'	Active

Loading SSL Profile

The SSL handler loads the profiles durig initalization. Any update of a profile must be followed by stop and start of the handler.

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.

```
09.30.50 STC97322  SSL0010I STARTING CONFIGURATION FILES PROCESS
09.30.50 STC97322  SSL0014I SSLCFG01 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0014I SSLCFG02 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0014I SSLCFG03 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0014I SSLCFG05 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0014I SSLCFG07 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0012E 16 BUILD    SSLCFG08 INVK SSLCIq=
09.30.50 STC97322  SSL0013I SSLCFG08 CONFIGURATION FILE, ERROR DETECTED
09.30.50 STC97322  SSL0011I ERRORS HAVE BEEN DETECTED DURING PROCESS
09.30.50 STC97322  SSL0011E ANMSSL PROCESS ERROR, CHECK SSL MESSAGES / SYSCFG FILE
09.30.50 STC97322  ANMSSL01 SSL HANDLER TERMINATED
```

The SYSCFG file shows the list of profiles that have been loaded : it shows errors with a character '!' in column 2. It shows that a profile has been rejected by the line ======REJECTED===== as for profile SSLCFG08 in the example below.

```
       ======SSLCFG01======
 SSLCFG=$DUMMY$   SYSIN CONFIG USED
       ======SSLCFG02======
 SSLCFG=*** TRACE HANDSHAKE ONLY ***
 SSLTRC=1
       ======SSLCFG03======
 SSLCFG=*** TRACE ALL (HANDSHAKE + DATA) ***
 SSLTRC=2
       ======SSLCFG05======
 SSLCFG=*** CONFIGURATION DE PRODUCTION ***
 STATUS=E
SSLCER=Certificat de production
SSLCIP=0A                        168-bit Triple DES -SHA-1 -RSA
SSLTL1=Y
SSLVE2=N
SSLVE3=N
       ======SSLCFG06======
SSLCFG=*** TLS ET SSL ***
STATUS=E
SSLCIP=0A01020304052F
SSLCER=Certificat
SSLTRC=2
SSLTL1=Y
SSLVE3=Y

       ======SSLCFG08======
SSLCFG=*** SPECIAL CRYPTO ***
!SSLCIq=052F
SSLCER=Certificat spécial
       ======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 of 300 characters maximum.
NLEV	Combination of the parameters SSLTL1, SSLVE3 and SSLVE2, after merging with SYSIN values, results in a null value.	Modify the profile
NULL	No active parameter for the profile	Modify the profile
LINK	Process error	Contact support
OPEN	File open error	Contact support
STOR	Storage error	Contact support

The normal sequence of messages is shown below.

```
09.30.50 STC97322  SSL0010I STARTING CONFIGURATION FILES PROCESS
09.30.50 STC97322  SSL0014I SSLCFG01 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0014I SSLCFG02 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0014I SSLCFG03 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0014I SSLCFG05 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0014I SSLCFG07 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0014I SSLCFG08 PROCESSED SUCCESSFULY
09.30.50 STC97322  SSL0014I CONFIGURATION FILES PROCESS COMPLETED
09.30.50 STC97322  ANMSSL02 SSL HANDLER IS ACTIVE
```

Client Mode

You can activate SSL process, for a transfer, in different ways :

- Use SSL CONFIGURATION field in the partner definition: provide a configuration profile number.

```
TOM4220     PARTNER OF TOM3 TO  VIEW       (2/4)
 OPTION ===>                          -ENTER- : GO ON, -PF3- : CANCEL   X : EXIT
 TYPE: TOM,PESIT-D
 MOD: PSR0008  09/03/13 04:52:32      119
 SYMBOLIC NAME          : PARTNER3            DPCSID ALIAS           : -
 TOM PASSWORD           : PSR                 DPCPSW ALIAS           : -
 INITIAL STATE          : E                   APM RECEPTION CLASS    : A
 RACF USER              : TOMPSR              RACF GROUP             : -

 PARTNER TYPE           : T
 SESSION PROT.NUM.-T.   : 5    : 2            SSL CONFIGURATION      : 06
 AUTOMATIC RESTART      : NO                  DN CONTROL MEMBER      : -

 LINK TYPES             : M    : IX
 EFF. TOTAL/IN/OUT      : 256  : 001  : 128  FLOW CONTROL T.   SLD  : -

 SNA: LUNAME  : -         LOGMODE    : -        LOGDATA   : -         DISC  : N
 X25: MCHMSC  : A     REM.ADDR.  : 3110214506054    LOC.ADDR  : -
      CUG     : -     UDF        : ABCD             CHARGE    : 1
      FACILITIES      : -
 IP : ADDR.   : -               PORT  : 21009 FTP PASV  : - PROF.   : -
      HOST    : MVSB.<HOST>                          'S': - RIGHTS  : -
 NOTE  :
```

- Use SSL CONFIGURATION field in the file definition: provide a configuration profile number.

```
TOM4220--------------- FILES ATTRIBUTES (2/5) ---------------------------- -
 OPTION ===>
 TMSG RELOAD(VERSION)
 SYMBOLIC NAME              : F1HFS        MODE: NORMAL

 INIT STATE ............    : E            E: IN-SERVICE H: HOLD

 DIRECTION .............    : *            T:TRANSMIT R:RECEIVE *:TRANS./REC.
 RECEIVING PARTNER .....    : *            'NAME', £LIST, */$$ALL$$ OR $$API$$
 SENDING PARTNER .......    : *            'NAME', £LIST, */$$ALL$$ OR $$API$$

 PRIORITY ..............    : 1            0:URGENT 1:FAST 2:NORMAL 3:SLOW
 DSN DEFINITION TYPE ...    : D            D:DYNAMIC F:FIXED
 ALLOCATION RULE .......    : 0            0:CREATE/REPLACE 1:PREALL. 2:CREATE
                                           3:EXIT A:APPLICATION SERVER
 FILE TYPE .............    : H            S/H/M/P/PU/V/VU/UU/SU/TU/HU
 PRESENTATION ..........    : 01           COMPRESS.,DATA TYPE (01-24)
 UNLOAD/RELOAD MEMBER ..    : -            OPTIONNAL
 SSL CONFIGURATION......    : 02           OPTIONNAL

 OPTION  : VIEW                            UPDATE: 09/03/25 11:08 PSR0008
 -ENTER- : NEXT SCREEN                     -PF3- : CANCEL
```

- Provide a SSL configuration profile number with the transfer request parameters :

  - Use SSL CONFIG. in the transfer extension screen of the TSO/ISPF interface

```
TOM4220     TRANSFER EXTENSION                          NAMES INITIALIZED    !
 OPTION ===>                                                          CSGB

 4XX/TEST

 SUB-SYSTEM .  :   TOM3
 FILE .......  :   F1HFS                                          ENABLED
 DIRECTION ..  :   T         (T/R)          <- *
 PARTNER ....  :   PARTNER3                 <- $$ALL$$  52        ENABLED
 DSN LOCAL ..  :   <CEXP>/toto.txt                                DYNAMIC
               <- &EXTDSN                                    -    HFS
 Rdsn/Pi99 .. --->                                          <    *1
              <-
 FTP T/S/M .. ---> '' ---> '  ---> '   <- I   -  -      STOU   ---> '    <- N
 RACF-GROUP . ---> ''''''''                             ('VALUE'/'BLANK')
 Org.-Dest. . --->          < --->          <            *1
 AND ONLY IF TOM IS UP :
 SSL CONFIG.  ---> 05                                   ('VALUE'/'BLANK')
 Alias id/psw --->          < --->          <            *1
 V----- S : DETAIL
 '' Api ....  --->
                     <                              *1 ('VALUE'/'value'/'BLANK')
             X EXIT, -ENTER- CONFIRM, -PF1- HELP TRC, -PF3- PREVIOUS
```

- Use SEC= parameter of the utility P1B2PRQ2

```
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=06,                    REQUEST SECURITY
000460      DSN= PSR$REC.PS.F080.SHORT
000466 EBLOCK
```

- Use EX1SSECN field of program L0B2Z20

The SSL handler retreives the corresponding configuration file from this parameter, from the table loaded during initialization. If the profile doesn't exist, the transfer fails with a session error: the code NRC=SCF0xx is issued. 'xx' represents the profile number that did not correspond to a definition. Message SSL0015W is issued.

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

Jesmsglg of ANM
02.30.34 STC99845  SSL0015W CONFIGURATION FILE 99 NOT FOUND
```

Server Mode –SYSSSL File

When a call is received inbound on one of the secured access points - defined in the SYSIN by SSLPRT or SSLPRO for TCP/IP, SSLSAD, SSLUDF, SSLSAO or SSLUDO for X25 - it is processed by the SSL handler. The default configuration used is the SYSIN configuration: this is SSL configuration 00.

The SYSSSL member of the ANMSSL file is used to select a configuration profile number from an 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.

```
'CRITERIA',CF='profile number'

 CRITERIA : 'LT='Value to check'
```

Each line defines a criteria and the associated profile number, separated by a comma , in any order.
The criteria indicates the link type *L* (X=X25, I=TCP/IP), the type of address *T* (A=Address, H=Host name) - valid combinations are XA, IA and IH – and the value of address to check. The value can be a specific address or a generic address on the form '*generic**'. The parameter CF= provides the profile number to use, two numeric characters from00 to 99.

Processing of TCP/IP Addresses

For TCP/IP addresse always consider the full representation ‘xxx.xxx.xxx.xxx’.

For example :

‘12.24’, is equivallent to‘12.24.*’, is procesed like this: ‘012.024.*’
‘12.24*’ is processed like this ‘012.24*’.

The address ‘12.241.20.1’ meets criteria ‘12.24*’, 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   PROD.CEXPRESS.ANMSSL(SYSSSL) - 01.42          Columns 00001 00072
Command ===>                                                Scroll ===> CSR
000014 *
000015 * X25
000016 *
000017 XA=01935622013,CF=01             COMPANY 1
000018 XA=012345678*,CF=03              GROUP 1
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                  (=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 a table.

A profile is selected during network session establishment. For X25, the SSL handler looks up XA criterias . For TCP/IP 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 criterias. As soon as a 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 I used. If the profile that has been selected doesn't exist, the connection fails, with messages and codes shown below:

```
Monitor Log
09/03/05 07:55:48 INCOMING REQUEST REJECTED 00000006 -SSL-I  SRC=SC99 TRC=2154

Jesmsglg of the ANM
07.55.48 STC00065  SSL0015W CONFIGURATION FILE 99 NOT FOUND
```

TCP/IP Example

For TCP/IP, the handler looks up host names first, but changes to address process at first IA criteria found. Below are the three scenarios :

1. All TCP/IP criterias 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 criterias 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 an address crieria 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`, `address 12.24.55.3`, will be processed with the SSL profile `number` CF=05, because an exact match is found for the host name, although IA=12.24 criteria does match in address mode.

Loading SYSSSL

The SSL handler loads the SYSSSL file during initalization. Any update of this file must be followed by stop-start of the SSL handler.

When an error is detected a WTO message is issued. The handler initialization fails if an error is detected. Message SSL0011E indicates that one or several errors have been detected. One or several messages SSL0012E are issued before.

```
08.13.50 STC00127  SSL0014I SSLCFG05 PROCESSED SUCCESSFULY
08.13.50 STC00127  SSL0014I SSLCFG06 PROCESSED SUCCESSFULY
08.13.50 STC00127  SSL0014I SSLCFG07 PROCESSED SUCCESSFULY
08.13.50 STC00127  SSL0012E 16 BUILD    SYSSSL   INVK ID=      L=023
08.13.50 STC00127  SSL0012E 16 BUILD    SYSSSL   INVR ID=CSGB. L=023
08.13.50 STC00127  SSL0013I SYSSSL   CONFIGURATION FILE, ERROR DETECTED
08.13.50 STC00127  SSL0011I ERRORS HAVE BEEN DETECTED DURING PROCESS
08.13.50 STC00127  SSL0011E ANMSSL PROCESS ERROR, CHECK SSL MESSAGES / SYSCFG FILE
08.13.50 STC00127  ANMSSL01 SSL HANDLER TERMINATED
```

The SYSCFG file shows the SYSSSL information: it indicates syntax errors with an exclamation mark in column 2.

```
       ======SSLCFG07======
SSLCIP=052F
SSLCFG=*** SPECIAL CRYPTO ***
SSLCER=Certificat de TOM8
       ====== SYSSSL ======
XA=0193562,CF=01              BNP,SG,CEDI
XA=012345678*,CF=03           SOFINCO
CF=03,XA=012345678*
!ID=CSGB.OFF*,CF=02            DEVELOPMENT
IH=XBF.OFF*,CF=02                 GROUP 2
IH=MVS*,CF=10                     GROUP 3
IA=12.24,CF=04                    (=012.024.*)
IA=10.24*,CF=13                   (=010.24*)
IA=10.2,CF=14                     (=010.002.*)
IA=10.2*,CF=15                    (=010.02*)
IA=10.20.129.3,CF=06              EXACT MATCH
IA=010.020.129.002,CF=06          EXACT MATCH
IH=MVSB.XBF.COMPANY.COM,CF=05     EXACT MATCH
```

Errors are identified by the following codes:

Code	Explanation	Action
DUPK	Duplicate keyword – the line number is indicated	Change the line
INVK	Invalid keyword – the line number is indicated	Change the line
KVAL	Invalid value of a keyword	Change the line
NOCF	No profile is defined – the line number is indicated	Change the line
INVR	Invalid record , check errors	Fix errors
MAXR	The maximum of possible definitions has been reached. The line number where the process stopped is indicated	Delete unused lines
LREC	Invalid record length of the ANMSSL file	Allocate the ANMSSL file with a record size of 300 characters maximum
NULL	No valid specification in the SYSSSL file	Fix errors
LINK	Allocation error	Contact support
OPEN	Open error	Contact support
STOR	Getmain error	Contact support

DN Control

This chapter describes how to implement certficate 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 neen authenticated by the z/OS SSL services. The control is based on control files that you create in the ANMSSL file, and that you can reference from their name. The process is different for inbound and outbound communications.

The names of the control files are prefixed by ‘DN’. The control file is processed only when required : updates can be considered as dynamic.

You can access to the DN files by option 0 of the SO/ISPF operator interface

```
TOM4220-------------- INITIALIZATION 2/2 -----------------------------------
 OPTION ===> ?
 4XX/TEST
             ?  MONITOR ===> TOM3  NAMES INITIALIZATION (AUTOMATIC ---> YES).
               TEMPORARY WORK-UNIT ===> SYSDA    , JES2-INTERFACE ---> ISF
              L LOGON-PROCEDURE, O  OPTIONS, V ISPF INSTALLATION CHECKING.
 ---------  S : CHECK FILES OF JOBTOM3   CSGB ACTIVE GLOBAL
 V
 _  ISPLLIB     ===> PROD.CEXPRESS.ISPLLIB
 _  LOADLIB     ---> PROD.CEXPRESS.LOADLIB
 _              --->
 _  SYSSNA        -> PROD.CEXPRESS.SYSPRM(L4SNA)
 _  SYSX25        -> PROD.CEXPRESS.SYSPRM(L4X25)
 _  SYSTCP        -> PROD.CEXPRESS.SYSPRM(L4TCP)
 _  SYSUE1        -> PROD.CEXPRESS.PARMLIB(SYSUE1)
 _  SYSCE1        ->

 _  ENVVAR        -> PROD.CEXPRESS.ENVVAR(TOM30)
 _  ANMSSL        -> PROD.CEXPRESS.ANMSSL
 _  AFMFTPE       ->

                 X EXIT, -PF3- END, -PF10/11- SCROLL
```

```
   Menu  Functions  Confirm  Utilities  Help
-------------------------------------------------------------------------------
 EDIT              PROD.CEXPRESS.ANMSSL                    Row 00001 of 00014
 Command ===>                                                 Scroll ===> CSR
            Name     Prompt       Size   Created          Changed           ID
 __________ README                 25  2009/02/18  2009/02/25 02:53:45  USER008
 __________ DNCFG05                19  2009/02/18  2009/02/25 02:53:45  USER008
 __________ DNCFG06                18  2009/02/18  2009/02/24 09:16:55  USER008
 __________ DN000001               16  2008/11/17  2009/02/18 06:15:12  USER008
 __________ DN000002               16  2008/11/17  2009/02/18 06:15:12  USER008
 __________ SSLCFG01                1  2009/01/21  2009/01/21 08:25:54  USER008
 __________ SSLCFG02                2  2009/01/21  2009/01/21 07:50:52  USER008
 __________ SSLCFG03                2  2009/01/21  2009/02/09 00:57:35  USER008
 __________ SSLCFG04                3  2009/01/13  2009/01/21 04:08:01  USER008
 __________ SSLCFG05                9  2008/11/17  2009/03/02 10:11:41  USER008
 __________ SSLCFG06                8  2008/11/17  2009/03/02 09:48:17  USER008
 __________ SSLCFG07                3  2009/01/13  2009/01/21 04:06:28  USER008
 __________ SYSSSL                 49  2008/12/29  2009/03/02 10:11:09  USER008
            **End**
```

Implementing DN Control

DN control is processsed at the end of successfull handshake : for an outbound connection (client mode) the partner is identified, for an inbound connection (server mode) only the network address is known. The process is different in the two modes.

Client Mode

In client mode, you can cofigure the DN control in the partner definition or in the SSL configuration file. In the following example, PARTNER 3 is called with SSL configuration SSLCFG05. This profile is associated with the control file DNCFG05 but, for this partner, the DN control is based on the DN0001 fle.
En mode demandeur le contrôle peut être paramétré au niveau de la définition du partenaire, ou dans le profil

```
TOM4220     PARTNER OF TOM3 TO  VIEW       (2/4)
 OPTION ===>                          -ENTER- : GO ON, -PF3- : CANCEL   X : EXIT
 TYPE: TOM,PESIT-D
 MOD: PSR0008  09/03/13 04:52:32      119
 SYMBOLIC NAME         : PARTNER3           DPCSID ALIAS           : -
 TOM PASSWORD          : PSR                DPCPSW ALIAS           : -
 INITIAL STATE         : E                  APM RECEPTION CLASS    : A
 RACF USER             : TOMPSR             RACF GROUP             : -

 PARTNER TYPE          : T
 SESSION PROT.NUM.-T.  : 5    : 2           SSL CONFIGURATION      : 05
 AUTOMATIC RESTART     : NO                 DN CONTROL MEMBER      : DN0001

 LINK TYPES            : M    : IX
 EFF. TOTAL/IN/OUT     : 256  : 001  : 128  FLOW CONTROL T.   SLD  : -

 SNA: LUNAME  : -         LOGMODE    : -        LOGDATA   : -         DISC  : N
 X25: MCHMSC  : A     REM.ADDR.  : 3110214506054    LOC.ADDR  : -
      CUG     : -     UDF        : ABCD             CHARGE    : 1
      FACILITIES       : -
 IP : ADDR.   : -                PORT  : 21009 FTP PASV  : - PROF.   : -
      HOST    : MVSB.<HOST>                          'S': - RIGHTS  : -
 NOTE  :
```

```
      ======SSLCFG05======
SSLCFG=*** PRODUCTION CONFIGURATION ***
SSLCER=Certificate for production
SSLCIP=0A                        168-bit Triple DES -SHA-1 -RSA
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 connected with profile SSLCFG05, and DN control executed from DNCFG05 file.

```
====== SYSSSL ======
XA=0193562,CF=01             BNP,SG,CEDI
XA=012345678*,CF=03          SOFINCO
CF=03,XA=012345678*
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    EXACT MATCH
```

Processing DN Control

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

The syntax is similar to XML. The following example shows the structure of the DN control file.

You can control four certificates :

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

```
   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 * CONTROL LOCAL:
 000002 <LDN>
 000003   CN=AN4*      TOUS LES CERTIF TOM4
 000004   OU=TEST
 000005   C=*
 000006 </LDN>
 000007 <LISSDN>
 000008   CN=*
 000009   OU=T??T*     TEST*, TIOT*
 000010 </LISSDN>
 000011 * CONTROL REMOTE:
 000012 <DN>
 000013   CN=AN?CERT*
 000014   OU=TES*
 000015 </DN>
 000016 <ISSDN>
 000017   CN=AN8CERT
 000019 </ISSDN>
-------------------------------------------------------------------------------
```

Four tags are valid: <LDN>, <LISSDN>, <DN> and <ISSDN>, and unique in the file.
If a start tag exists, the corresponding end tag is required.
You can control any field of the certificate, the field keyword can be any 1 or 2 characters string.
Characters ‘ ?’ and ‘*’ are processed this way :

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

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 control file involved, 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 fle	Check the code - Contact support
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 detecetd , but a end tag is required	Modify the DN file

Use available traces to analyse problems.

Traces

Trace tools available are :

- The SYSPRINT file used to trace SSL operations, controlled by the SSLTRC parameter.
- The SYSDNCTL file used to trace DN control operations, controlled by the SSLTRC parameter.

These to files must be defined in the JCL of the ANM.

```
//TOM3ANM PROC OUT=X
//TOMV423 EXEC PGM=P1ANM000,REGION=0M,TIME=1440,
// PARM=('SSN=&SSN','MSN=&MSN','LHM=&LHM','HSS=&HSS','ISN=&ISN')
//*-------------------------------------------------------------------
//* perform group must be the same as VTAM (for X25 treatment).
//* region must be at least : (effectors count x 68k)
//* (32 x 68k) = 2200k
//* region size must be increased if using large buffer size.
//*-------------------------------------------------------------------
//* ANM PROCEDURE (AUXILIARY NETWORK MANAGER)
//*-------------------------------------------------------------------
//BPXTCAF EXEC PGM=BPXTCAFF,PARM=LCTCPB2
//*-------------------------------------------------------------------
//STEPLIB  DD DISP=SHR,DSN=PROD.CEXPRESS.LOADSSL
//         DD DISP=SHR,DSN=PROD.CEXPRESS.LOADLIB
//SYSUDUMP DD SYSOUT=&OUT
//SYSDUMP  DD SYSOUT=&OUT
//SYSMSG   DD SYSOUT=&OUT
//SYSLOG   DD SYSOUT=&OUT
//SYSIN DD DISP=SHR,DSN=index1.TOMV422.PARMLIB(PARMANM3) IN
//SYSTCPD  DD DISP=SHR,DSN=SYS.TCPIP.PARMS(TCPDATA)
//CEEDUMP  DD SYSOUT=&OUT
//CEEMOUT  DD SYSOUT=&OUT
//CEEMSG   DD SYSOUT=&OUT
//ENVIRON  DD DSN=PROD.CEXPRESS.SSLTCFG,DISP=SHR
//SYSPRINT DD SYSOUT=&OUT
//ANMSSL   DD DSN=PROD.CEXPRESS.ANMSSL,DISP=SHR
//SYSCFG   DD SYSOUT=&OUT
//SYSDNCTL DD SYSOUT=&OUT
```

SYSPRINT Information

The SYSPRINT file provides information about context, profile and results of the SSL handshake. The context provides the request number, the profile provides the DN control file name and which local certificate is used, the results display the certificates exchanged. For request number '*nnnnnnn'*, look for the following tags:

Tag	**Description**
<Req>nnnnnnn</Req>	Information are linked to the request number
<Cfg>06</Cfg>	Number of the profile SSLCFG06
<DnCtl>DNCFG06 </DnCtl>	DN control file, blank if not requested
<Cer>CERTZOS</Cer>	Local certificat label
<SrvCer> <DN> <IssDN>	Certificate of the SSL server DN of the server, used for control DN of the issuer of the server DN, used for control
<CliCer> <DN> <IssDN>	Certificate of the SSL client DN of the client, used for control DN of the issuer of the client DN, used for control

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

In the trace, the records from the DN file are preceeded by the name of the file, DNCFG06 in the example :

```
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
```

Certificate Management with RACF

Certificate management is performed by means external to Connect:Express. If the certificate to use is not the one defined by default for the ANM in the certificate database, it can be set by the parameter Certificate Label indicated in the monitor configuration (SSLCER). This label can be typed in mixed case and can include a maximum of 34 characters.

The local certificate (the default one or any other) and the certificates of authorities involved in expected exchanges should be connected to the ANM keyring. They are not themselves necessarily associated to the ANM (parameter ID of the RACDCERT command). You don't need to connect partner certificates to the keyring.

Note: In the case of autosigned certificates, the local and the partner certificates should both be present in the keyring.

In this beta version, you can associate only one certificate: you can provide it in the SYSIN file.

SSLCER=Server Label Paris 2 <maximum size = 34 characters

For the initial tests, you can use autosigned certificates, or create your own authority and create certificates authenticated by this authority. Under normal conditions, you have to submit a certificate request to an authority. The authority returns the authenticated certificate, which must then be added to the database.

A certificate can be created locally or added to the database by means of a file received.
The command TSO RACDCERT and the RACF ISPF interface allows you to accomplish all these operations:

- Create a keyring
- Create a certificate
- Autosigned
- Of type authority
- Of type user
- Request a certificate
- Extract a certificate from a file
- Add a certificate to the database from a file
- Connect a certificate to a keyring

The RACDCERT Command

The examples below illustrate certificate management: The parameter *withlabel* is the information used in the configuration of Connect:Express (SSLCER).

Autosigned Certificate

An autosigned certificate suffices by itself, but certain systems don't allow its use. This certificate should be connected to the keyring of the ANM.

This operation can be performed using the ISPF interface.

```
RACDCERT id(psran8) GENCERT subjectsdn(cn('AN8CERT') or('TEST') c('SSL'))trust
size(1024) withlabel('CRACAN8')
```

Certificate Authority

A certificate authority (CA) allows you to sign certificates of type user. This certificate should be connected to the ANM keyring if the certificates used in the course of testing are signed by this authority.

```
RACDCERT CERTAUTH GENCERT subjectsdn(OU('Paris labs Certificate Authority')
O('Sterling France, Inc') C('FR')) withlabel('Local PKI CA')
NOTBEFORE(DATE(2006/03/01)) NOTAFTER(DATE(2021/03/01))
```

Connecting a Certificate to a Keyring

This operation can be done through the ISPF interface.

```
RACDCERT ID(PSRAN4) CONNECT(CERTAUTH LABEL('Local PKI CA') RING(psran4.keyring)
USAGE(PERSONAL) DEFAULT)
```

Exporting a Certificate in a File

This operation allows you to transmit the certificate to a partner. The operation can be done through the ISPF interface.

```
RACDCERT CERTAUTH EXPORT(LABEL('Local PKI CA')) DSN('_RACF.PRIVATE.KEY.P12BIN')
FORMAT(PKCS12DER) PASSWORD('MVPKI02')
```

ISPF Menus

All the operations involved in creating a certificate of type authority can be done via the ISPF interface.

```
           RACF - Digital Certificates and Related Services
OPTION ===>

  Select one of the following:

     Digital Certificate Services
        1. Generate a certificate and a public/private key pair.
        2. Create a certificate request.
        3. Write a certificate to a data set.
        4. Add, Alter, Delete, or List certificates or
           check whether a digital certificate has been added to
           the RACF database and associated with a user ID.
        5. Renew, Rekey, or Rollover a certificate.

     Key Ring Services
        6. Create, List, or Delete an entire key ring or
           Connect or Remove a certificate to/from a key ring.

     Certificate Name Filtering Services
        7. Add, Alter, Delete, or List certificate name filters
           associated with a user ID.
```

Here is a typical sequence of operations:

1. Create a keyring, option 6.
2. Create an autosigned certificate, option 1.
3. Create a certificate signed by an existing authority :
   a. Identify the certificate: option 1.
   b. Create the certificate request: option 2.
   c. Have the authority sign the certificate: option 1 again.
4. Connect the certificate to the keyring : option 6.
5. Export the certificate: option 3.
6. Import a certificate: option 4.

Specific Return Codes and Message

Specific Return Codes

New TRC codes have been added, and SSL error messages are displayed in SRC or NRC fields depending on the context.

TRC Codes

TRC=2163 : The SSL handler is disabled.
TRC=2164 : SSL prohibited for this partner.
TRC=2165 : SSL required for this partner.
TRC=A7AS : The SSL handler abended.
TRC=A7ES : The SSL handler terminated due to an error detected by z/OS SSL services. Check SRC return code.

SSL Return Codes

The SSL return codes are contained in the list provided in the table below. They are displayed in decimal format in the NRC field in the format NRC=Sxxxxx, or in the SRC field in the format SRC=Sxxx.

Display in the SRC field is done exclusively in the case of rejected incoming requests.

Examples:

Incoming request rejected : the client request is made through the TCP/IP SSL port, but comes from PeSIT without SSL :

```
INCOMING REQUEST REJECTED 00000015 -SSL-I  SRC=S406 TRC=2154  PRC=0000 PESIT   GFIPSR8SPSR
```

Incoming request rejected : the client request is made on X25 with user data expected for SSL, but is made via PeSIT without SSL :

```
INCOMING REQUEST REJECTED 00000015 -SSL-X  SRC=S406 TRC=2154  PRC=0000 PESIT   GFIPSR8SPSR
```

Outgoing request rejected : error during SSL handshake :

```
REQUEST 00000556 SESSION ERROR : SSLINI    NRC=S00406 000000
```

Specific Messages

Added SSL functionality appears in the SYSMSG and SYSLOG files of TOM, and the JESMSGLG file of ANM.

Messages of the SSL Handler

SSL handler messages, as seen in the JESMSGLG file of the ANM, signal environment errors and should be flagged for analysis by Support.

```
SSL0001E : INIT LE ERROR - TEST RC=8.
SSL0002E : INIT LE FAILURE RC IS NOT 8.
SSL0003E : SSL INITIALIZATION FAILED

SSL0004W : SSL TERMINATION SSL FAILED
SSL0005W : LE TERMINATION FAILED
```

ANM Messages

Two new messages appear when the SSL handler is activated or stopped.

```
ANMSSL02 SSL HANDLER IS ACTIVE
ANMSSL01 SSL HANDLER TERMINATED
```

TOM Messages

Monitor messages indicate if a connection is running under SSL: Here, ‘PESIT SSL’ replaces ‘PESIT’ in connection messages.

```
COMMUNICATION NOT OBTAINED GFIPSR4S RETRY IN 01 MIN (I,010.020.129.002)          PESIT   SSL
COMMUNICATION OPENED (O) WITH GFIPSR4S (I,010.020.129.002) APM 01 EFF 01 PESIT   SSL
```

New messages are used with specific data:

Abend of SSL handler: TRC=A7AS

```
ANM HANDLER ABNORMALLY TERMINATED   SRC=0008 TRC=A7AS  PRC=0000
```

Errors and rejections in the connection phase:

```
INCOMING REQUEST REJECTED 00000829 -SSL-X  SRC=0414 TRC=2154  PRC=0000 R
INCOMING REQUEST REJECTED 00000832 -SSL-I  SRC=0414 TRC=2154  PRC=0000 R
REQUEST  00000490 SESSION ERROR : SSLINI    NRC=S00008 000000
```

SSL Return Codes

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

Decimal	Hex	Description
1	1	GSK_INVALID_HANDLE
2	2	GSK_API_NOT_AVAILABLE
3	3	GSK_INTERNAL_ERROR
4	4	GSK_INSUFFICIENT_STORAGE
5	5	GSK_INVALID_STATE
6	6	GSK_KEY_LABEL_NOT_FOUND
7	7	GSK_CERTIFICATE_NOT_AVAILABLE
8	8	GSK_ERR_CERT_VALIDATION
9	9	GSK_ERR_CRYPTO
10	A	GSK_ERR_ASN
11	B	GSK_ERR_LDAP
12	C	GSK_ERR_UNKNOWN_ERROR
101	65	GSK_OPEN_CIPHER_ERROR
102	66	GSK_KEYFILE_IO_ERR
103	67	GSK_KEYFILE_INVALID_FORMAT
104	68	GSK_KEYFILE_DUPLICATE_KEY_ERR
105	69	GSK_KEYFILE_DUPLICATE_LABEL_ERR
106	6A	GSK_BAD_FORMAT_OR_INVALID_PASSWORD
107	6B	GSK_KEYFILE_CERTIFICATE_EXPIRED
108	6C	GSK_ERR_LOAD_GSKLIB
109	6D	GSK_KEYFILE_NO_CA_CERTIFICATES
201	C9	GSK_NO_KEYFILE_PASSWORD
202	CA	GSK_KEYRING_OPEN_ERROR
203	CB	GSK_RSA_TEMP_KEY_PAIR
204	CC	GSK_KEYFILE_PASSWORD_EXPIRED
301	12D	GSK_CLOSE_FAILED
302	12E	GSK_CONNECTION_ACTIVE
401	191	GSK_ERR_BAD_DATE
402	192	GSK_ERR_NO_CIPHERS
403	193	GSK_ERR_NO_CERTIFICATE
404	194	GSK_ERR_BAD_CERTIFICATE
405	195	GSK_ERR_UNSUPPORTED_CERTIFICATE_TYPE
406	196	GSK_ERR_IO
407	197	GSK_ERR_BAD_KEYFILE_LABEL
408	198	GSK_ERR_BAD_KEYFILE_PASSWORD
409	199	GSK_ERR_BAD_KEY_LEN_FOR_EXPORT
410	19A	GSK_ERR_BAD_MESSAGE
411	19B	GSK_ERR_BAD_MAC
412	19C	GSK_ERR_UNSUPPORTED
413	19D	GSK_ERR_BAD_CERT_SIG
414	19E	GSK_ERR_BAD_CERT
415	19F	GSK_ERR_BAD_PEER
416	1A0	GSK_ERR_PERMISSION_DENIED
417	1A1	GSK_ERR_SELF_SIGNED
418	1A2	GSK_ERR_NO_READ_FUNCTION

419	1A3	GSK_ERR_NO_WRITE_FUNCTION
420	1A4	GSK_ERR_SOCKET_CLOSED
421	1A5	GSK_ERR_BAD_V2_CIPHER
422	1A6	GSK_ERR_BAD_V3_CIPHER
423	1A7	GSK_ERR_BAD_SEC_TYPE
424	1A8	GSK_ERR_BAD_SEC_TYPE_COMBINATION
425	1A9	GSK_ERR_HANDLE_CREATION_FAILED
426	1AA	GSK_ERR_INITIALIZATION_FAILED
427	1AB	GSK_ERR_LDAP_NOT_AVAILABLE
428	1AC	GSK_ERR_NO_PRIVATE_KEY
429	1AD	GSK_ERR_INVALID_V2_HEADER
430	1AE	GSK_ERR_CERTIFICATE_EXPIRED
431	1AF	GSK_ERR_CERTIFICATE_REVOKED
432	1B0	GSK_ERR_NO_NEGOTIATION
433	1B1	GSK_ERR_NO_NEGOTIATION
434	1B2	GSK_ERR_EXPORT_RESTRICTION
435	1B3	GSK_ERR_INCOMPATIBLE_KEY
436	1B4	GSK_ERR_BAD_CRL
437	1B5	GSK_ERR_CONNECTION_CLOSED
438	1B6	GSK_ERR_INTERNAL_ERROR_ALERT
439	1B7	GSK_ERR_UNKNOWN_ALERT
501	1F5	GSK_INVALID_BUFFER_SIZE
502	1F6	GSK_WOULD_BLOCK
503	1F7	GSK_WOULD_BLOCK_READ
504	1F8	GSK_WOULD_BLOCK_WRITE
505	1F9	GSK_ERR_RECORD_OVERFLOW
601	259	GSK_ERR_NOT_SSLV3
602	25A	GSK_MISC_INVALID_ID
701	2BD	GSK_ATTRIBUTE_INVALID_ID
702	2BE	GSK_ATTRIBUTE_INVALID_LENGTH
703	2BF	GSK_ATTRIBUTE_INVALID_ENUMERATION
704	2C0	GSK_ATTRIBUTE_INVALID_SID_CACHE
705	2C1	GSK_ATTRIBUTE_INVALID_NUMERIC_VALUE
706	2C2	GSK_ATTRIBUTE_INVALID_PARAMETER

Performing Traces

This section summarizes the suite of available trace utilities, including the trace for the new SSL handler and the trace for the SSL and z/OS services.

Trace on Incoming Connection Checks

The command /F TOMJOB,TRACE=E allows for the display, in the monitor log, of detailed information related to an unrecognized request.

Once this trace is active, one can request its activation for a given partner : The trace displays related information in the monitor log in case a request from this partner is rejected.

In some cases, this trace is the sole means of obtaining the X25 address and data.

ATM Protocol Trace

The ATM produces complete protocol traces on demand. These traces are independent of the use or non-use of SSL, in that they are written before SSL processing when sending data and after SSL processing when receiving data.

SSL Trace

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 XML format, with each field defined by a tag. The details are timestamped, and each exchange is identified by a two-part number (number of request, Xrb internal block). The SSL handles are displayed, one for the environment and one for each session.

The following table lists the fields provided in the trace: In the initialization phase of the ANM, the configuration parameters provided are displayed in <SslConfig>, then the final values after taking into account by GSKSSL in <InitializedValues>. At initialization of each SSL session, the parameters provided are displayed in <SslConfig>, then the data following the handshake are displayed in <SessionValues>. During the exchanges, the network messages are defined by the tags <NetIn> and <NetOut>, and protocol exchanges are identified by the tags <ProtIn> and <ProtOut>. The data exchanged is displayed in hexadecimal format. The normal sequence is <NetIn> <ProtIn> or <ProtOut> <NetOut>.

Tag	**Description**	**Type of Trace**
Fun	1 = Initialization, 2 = Open client, 3 = Open server, 4 = Send, 5 = Receive, 6 = Close, 9 = Termination	Environment
EnvHan	Control block address designated par SSL	Environment
Req	Request number designated by the monitor	Session
Xrb	Control block address designated par the ANM	Session
Ssl	SSL extension address	Session
SocHan	Control block address designated by SSL	Session
SslConfig		Envir. and session
Aut	Sysin SSLAUT parameter (see AutCli)	Environment
Tim	Sysin SSLTIM parameter (see TimV3)	Environment
Trc	Sysin SSLTRC parameter	Environment
Lev	Supported Protocol(s) : 10 = TLS V1, 01 = SSL V2, 02 = SSL V3. Possible combination are : 11 = TLS V1 + SSL V2, 12 = TLS V1 + SSL V3, 13 = TLS V1 + SSL V3 + SSL V2, 03 = SSL V3 + SSL V2	Environment
Cip	Sysin SSLCIP parameter (see CipV3)	Environment
Cer	Sysin SSLCER parameter (see Cerlabel)	Environment
Krn	Sysin SSLKRN parameter	Environment
Dbn	Sysin SSLDBN parameter	Environment
Dpw	Sysin SSLDPW parameter	Environment
Tra	Profile SSLTRC parameter	Session
InitializedValues	Initialized values including default values	Environment
CerLabel	Local certificate label (provided in SSLCER or by default)	Environment
SslV2	SslV2 support : ON / OFF (see SSLLEV)	Environment
SslV3	SslV3 support : ON / OFF (see SSLLEV)	Environment
TlsV1	TlsV1 support : ON / OFF (see SSLLEV)	Environment
CipV2	Cipher suite for SSL V2	Environment
CipV3	Cipher suite for SSL V3 and TLS V1 (see SSLCIP)	Environment
TimV2	Session duration of SessionID forSSL V2	Environment
TimV3	Session duration of SessionID for SSL V3 (see SSLTIM)	Environment
AutCli	Client authentication: FULL/PASSTHRU (see SSLAUT)	Environment
SessionValues		Session
SessionID	Identifier designated by SSL and for which the duration is limited to TimV2 or TimV3 based on SSL version.	Session
SecType	Type of security : SSLV2 – SSLV3 – TLSV1	Session
SessType	Type of session : CLIENT, SERVER, SERVER+AUTCLI	Session
Cfg	Numéro de profil SSL. <Cfg>00</Cfg> = le profil défini en SYSIN.	Session
DnCtl	Nom du fichier de contrôle de DN.	Session
Cipher	Level of security, one of the values of the cipher suite	Session
CliCer	Client certificate	Session
SrvCer	Server certificate	Session
GskError	SSL error message	Session
Rc1	ANM return code – first NRC field	Session
Rc2	ANM return code – second NRC field	Session

SocSend	ANM service request send function.	Session and data
SocRecv	ANM service request receive function.	Session and data
Dad	Address of data exchanged between the ANM and SSL	Session and data
Dln	Length of data exchanged between ANM and SSL	Session and data
NetIn	Network message received (transmitted to SSL)	Session and data
NetOut	Network message sent (by SSL)	Session and data
ProtIn	Protocol message received (by SSL)	Data
ProtOut	Network message sent (transmitted to SSL)	Data

Trace gskssl

To obtain a trace of the SSL services of z/OS, you should activate the ENVIRON DD card in the JCL for the ANM. This card should point to a configuration file of the environment language, in which the parameters GSK_TRACE and GSK_TRACE_FILE indicate what level of trace is asked for and to which HFS file this trace should be written.

ANM JCL:

```
//*BPXTCAF     EXEC PGM=BPXTCAFF,PARM=TCPIP
//$SANM$       EXEC PGM=P1ANM000,REGION=4M,TIME=1440,DPRTY=(15,15),
//   PARM=('SSN=&SSN','MSN=&MSN','LHM=&LHM')
//STEPLIB  DD   DISP=SHR,DSN=$$LOADSSL$$
//                       DSN=$$LOADLIB$$
//ENVIRON DD DSN= TEST.ENVIRON.TRACE(SSL),DISP=SHR
```

CEE Environment Parameters:

```
ISREDDE2   TEST.ENVIRON.TRACE(SSL) - 01.10               Columns 00001 00072
 Command ===>                                              Scroll ===> CSR
 ****** ***************************** Top of Data ******************************
 000001 TZ=CST6CDT
 000002 LC_ALL=EN_US.IBM-037
 000003 LANG=EN_US.IBM-037
 000004 _CEE_DMPTARG=SYSOUT(X)
 000005 _BPXK_SETIBMOPT_TRANSPORT=LCTCPE2
 000006 GSK_SSL_HW_DETECT_MESSAGE=1
 000007 GSK_HW_DETECT_MESSAGE=1
 000008 GSK_SSL_ICSF_ERROR_MESSAGE=1
 000009 GSK_SSL_BSAFE_ERROR_MESSAGE=1
 000010 STEPLIB=CURRENT
 000011 GSK_TRACE=0xff
 000012 GSK_TRACE_FILE=/u/cexpress/gsktrc_%
****** **************************** Bottom of Data ****************************
```

The ANM procedure should be authorized to write to the HFS file indicated : **`/u/cexpress/gsktrc_%`** in the example below. For this, it is necessary to allocate an MVS segment and to give it write permission in a working directory. The syntax of the file name allows for identification of the trace file with a procedure number, which replaces the *%* character: In the example, the file name will be in the form **`/u/cexpress/gsktrc_33685540`**.

Once the file trace is obtained, after stopping the ANM should be formatted by the command oMVS gsktrace:

```
Gsktrace /u/cexpress/gsktrc_33685540 > /u/cexpress/gsktrc_33685540_formatted
```

This file can then be analyzed in an editor by the command ISPF oEDIT.