Connect:Express® OS/390

SSL Option

Version 4.2.0

Sterling Commerce
An IBM Company

Connect:Express OS/390 SSL Option
Version 4.2.0
First Edition

Contents

Activating the SSL Option

This document complements the Connect:Express OS/390 version 4.2.0 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.

```
TOM4200-------------- 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 file 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, certificate specification, and general SSL options. All parameters are defined in the SYSIN file.

General principles include the following :

- By default the SSL handler is inactive.
- SSL access by TCP/IP are characterized by specific ports.
- SSL access by X25 are characterized by X25 user data or by subaddresses.
- In this version, the monitor is associated with a unique key certificate.

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) becomes TCPORG=(SOE)

The table below describes the parameters that characterize the Connect :Express SSL service. Certain 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	N is the default value. Y requires at minimum the following SSL configuration parameters.	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 local certificate 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. [NOT SURE HOW TO TRANSLATE ‘APPELS’ IN THIS CONTEXT.] 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	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
SSLLEV	2 numeric chars	Minimum level of SSL protocol supported. The three possible values are 20, 30, and 31. The default value is 30: This signifies that the server will deal with SSL version 3 and TLS version 1 protocols. To limit support to TLS version 1, enter 31. To also support SSL version 2, enter 20.	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	Cipher suite. 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. The values provided are not controlled at the time of initialization; make sure they are valid.	Optional

(continued)

By default the list used by z/OS is as follows :
050435363738392F303132330A1613100D0915120F0C0306020100

The list below comprises the values supported by z/OS for SSL version 3 and TLS :

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

The list below comprises the values supported by z/OS, for SSL version 2 :

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)

New commands

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

```
TOM4200     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
```

ANM Configuration

Connect:Express receives the ANM SSL parameters via its SYSIN and transmits them to the ANM during initialization. The ANM configuration thus consists in adapting the procedure's JCL.

SSL Configuration

The ANM SYSLOG file shows the list of affected parameters.

JCL Procedure

You must add the LOADSSL library in STEPLIB of the JCL procedure.

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.

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=$$SSLTRC$$,DISP=SHR
```

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.”

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.

Return Codes and Message IDs

Specific Return Codes

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

New 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
```

New 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 a PeSIT SSL Transfer

Once monitor configuration is complete, the SSL handler initializes and the TCP/IP handler activates listeners according to the setup: one listener for PeSIT, one listener for PeSIT SLL, and in the same fashion one listener for Odette and a listener for Odette SSL.

In Server Mode

Incoming TCP/IP requests are processed by the listeners: if the request is accepted by an SSL server, it is processed under SSL. Partners should thus send requests to the port corresponding to the desired protocol.

Requests via X25 are handled by the X25 handler, which determines whether the session should be placed under SSL as a function of user data or of the subaddress, following monitor configuration.

In server mode, once the call request is processed, with or without SSL, the monitor controls the partner's SSL SECURITY TABLE field. The request may be rejected if this field does not conform to the type of request. It is possible to activate or deactivate the SSL session trace, as indicated below.

In Client Mode

In this version the monitor represents only a single entity, identified by the unique certificate declared in its SYSIN file (SSLCER). To trigger an SSL transfer to a partner, it is enough to declare a security table number in the partner definition (SSL SECURITY TABLE): As a function of this field's value and of the SSLTRC field value in the SYSIN file, the SSL session is either traced or not: 01 means that SSLTRC is used (the default); 02 means that the trace is active but limited to handshake data, regardless of SSLTRC; 03 means that the trace is active and includes all data, regardless of SSLTRC.
To establish an SSL connection with a Connect:Express server, you must indicate, in the corresponding partner definition, the TCP/IP port configured in the SYSIN file of this Connect:Express server (or, in case of an X25 session, the user data field).

```
TOM4200     PARTNER OF TOM8 TO  UPDATE     (2/4)
OPTION ===>                        -ENTER- : GO ON, -PF3- : CANCEL   X : EXIT
TYPE: TOM,PESIT-E
MOD: PSR0008  06/12/15 02:25:26       60
SYMBOLIC NAME         : GFIPSR8S           DPCSID ALIAS          -> GFIPSR4S
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 SECURITY TABLE    -> 02
AUTOMATIC RESTART    -> NO

LINK TYPES           => M   => IX          ADJACENT PARTNER      -> -
EFF. TOTAL/IN/OUT    => 256 -> 128 -> 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   -> MVSA.CSG.STERCOMM.COM                'S': - RIGHTS -> -
NOTE -> SSL TRANSFER
```

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, beginning of SSL session (handshake), and exchange of data.

The trace can be activated at monitor startup by the parameter SSLTRC=1 of SYSIN. By default, this parameter activates all levels.

A partner's SSL SECURITY TABLE parameter allows for deactivation of the data trace if SSLTRC=1, or to activate the trace for the partner if SSLTRC=0.

The partner's SSL SECURITY TABLE parameter is used in the following manner:

SSL SECURITY TABLE = 01	The trace is taken by default to be equal to the trace environment SSLTRC.
SSL SECURITY TABLE = 02	The data trace is inactive, but the session trace is active no matter how SSLTRC is set.
SSL SECURITY TABLE = 03	The handshake and data traces are active regardless of SSLTRC setting.

Environmental information is displayed only if SSLTRC=1. Session startup in server mode is displayed only if SSLTRC=1. You can limit trace size in client or server mode by specifying the parameter SSL SECURITY TABLE = 02.

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	Environmental
EnvHan	Control block address designated par SSL	Environmental
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)	Environmental
Tim	Sysin SSLTIM parameter (see TimV3)	Environmental
Trc	Sysin SSLTRC parameter	Environmental
Lev	Sysin SSLLEV parameter (see SslV2, SslV3 et TlsV1)	Environmental
Cip	Sysin SSLCIP parameter (see CipV3)	Environmental
Cer	Sysin SSLCER parameter (see Cerlabel)	Environmental
Krn	Sysin SSLKRN parameter	Environmental
Dbn	Sysin SSLDBN parameter	Environmental
Dpw	Sysin SSLDPW parameter	Environmental
Tra	Partner SSL SECURITY TABLE parameter	Environmental
InitializedValues	Initialized values including default values	Environmental
CerLabel	Local certificate label (provided in SSLCER or by default)	Environmental
SslV2	SslV2 support : ON / OFF (see SSLLEV)	Environmental
SslV3	SslV3 support : ON / OFF (see SSLLEV)	Environmental
TlsV1	TlsV1 support : ON / OFF (see SSLLEV)	Environmental
CipV2	Cipher suite for SSL V2	Environmental
CipV3	Cipher suite for SSL V3 and TLS V1 (see SSLCIP)	Environmental
TimV2	Session duration of SessionID forSSL V2	Environmental
TimV3	Session duration of SessionID for SSL V3 (see SSLTIM)	Environmental
AutCli	Client authentication: FULL/PASSTHRU (see SSLAUT)	Environmental
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
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.