Connect:Express® z/OS

Option SSL

Version 4.2.3

Sterling Commerce
An IBM Company

Connect:Express z/OS Option SSL
Version 4.2.3
Première édition

La présente documentation a pour objet d'aider les utilisateurs autorisés du système Connect:Express (ci-après le « Logiciel de Sterling Commerce »). Le Logiciel de Sterling Commerce, la documentation correspondante ainsi que les informations et le savoir-faire qu'il contient, sont la propriété de Sterling Commerce Inc. et sont confidentiels. Ils constituent des secrets commerciaux de cette dernière, de ses sociétés affiliées ou de ses/leurs concédants (ci-après dénommés collectivement « Sterling Commerce »). Ils ne peuvent pas être utilisés à des fins non autorisées ni divulgués à des tiers sans l'accord écrit préalable de Sterling Commerce. Le Logiciel de Sterling Commerce ainsi que les informations et le savoir-faire qu'il contient ont été fournis conformément à un contrat de licence qui inclut des interdictions et/ou des limitations quant à la copie, la modification et l'utilisation. La reproduction, en tout ou partie, si et lorsqu'elle est autorisée, devra inclure la présente notice d'information et la légende de copyright de Sterling Commerce Inc. Lorsqu'un Logiciel de Sterling Commerce ou un Logiciel Tiers est utilisé, reproduit ou divulgué par ou à une administration des Etats-Unis ou un cocontractant ou sous-traitant d'une telle administration, le Logiciel est assorti de DROITS LIMITES tels que définis au Titre 48 CFR 52.227-19 et est régi par les dispositions suivantes : Titre 48 CFR 2.101, 12.212, 52.227-19, 227-7201 à 227.7202-4, FAR 52.227-14 (g) (2) (6/87) et FAR 52.227-19 (c) (2) et (6/87), et le cas échéant, la licence habituelle de Sterling Commerce, tel que cela est décrit au Titre 48 CFR 227-7202-3 concernant les logiciels commerciaux et la documentation des logiciels commerciaux, y compris le DFAR 252-227-7013 (c) (1), 252.227-7015 (b) et (2), DFAR 252.227-7015 (b) (6/95), DFAR 227.7202-3 (a), selon le cas.
Le Logiciel de Sterling Commerce et la documentation correspondante sont concédés « EN L'ETAT » ou assortis d'une garantie limitée, telle que décrite dans le contrat de licence de Sterling Commerce. A l'exception des garanties limitées accordées, aucune autre garantie expresse ou implicite n'est concédée, y compris les garanties de qualité marchande et de convenance à un usage particulier. La société Sterling Commerce concernée se réserve le droit de revoir cette publication périodiquement et d'effectuer des modifications quant à son contenu, sans obligation d'en informer qui que ce soit, personne physique ou personne morale.
Les références faites dans le présent manuel aux produits, logiciels ou services Sterling Commerce ne signifient pas que Sterling Commerce a l'intention de les commercialiser dans tous les pays dans lesquels elle a des activités.

Imprimé aux Etats-Unis.
Copyright © 2006-2009. Sterling Commerce, Inc. Tous droits réservés.
Connect:Express est une marque déposée de Sterling Commerce. Les noms des Logiciels Tiers sont des marques ou des marques déposées de leurs sociétés respectives. Tous (toutes) autres marques ou noms de produit sont des marques ou des marques déposées de leurs sociétés respectives.

TABLE DES MATIERES

Activation de l’option SSL

Ce document vient en complément de la documentation de Connect:Express z/OS version 4.2.3. Il décrit la mise en œuvre de l’option SSL.

Pré-requis

Les fonctions SSL s’appuient sur les services SSL de z/OS qui doivent être installés. Elles mettent en œuvre les UNIX System Services de z/OS (POSIX) qui doivent donc être installés et configurés.

Il est nécessaire de configurer deux moniteurs pour effectuer des tests en interne.

Clé de protection

L’option SSL fait l’objet d’une license : la clé d’autorisation doit contenir l’option SSL.
Vous pouvez vérifier ce paramètre par l’option 0.O de l’interface ISPF.

```
TOM4230-------------- OPTIONS ------------------------ NOMS INITIALISES     !
 OPTION ===> ?                                          X EXIT, -PF3- FIN

 MONITEUR => TOM8 / PSRTOM8   CSGA ACTIF GLOBAL
             AP BROWSE ASSET-PROTECTION.      RACFCN= S ADHOCN= Y UPRFCT= Y
                0=OPTION NON AUTORISEE, CPUID=000194BA2064
 ACT       04 : 0       HABILITATIONS FTP-HTML.
 BSC       02 : 1       PROTOCOLE BSC (ETEBAC1/2).
 CICS      10 : 1       INTERFACE CICS.
 ETEBAC3   05 : 1       PROTOCOLE ETEBAC3.
 FTP       03 : 1       PROTOCOLE FTP.
 IMS       16 : 1       INTERFACE IMS.
 LU6.2     06 : 1       PROTOCOLE LU6.2.
 MBO       12 : 0       OPTION MAILBOX.
 ODETTE    11 : 1       PROTOCOLE ODETTE.
 LOCAL     09 : 1       MONITEUR LOCAL.
 PAC       08 : 1       AIDE A L'EXPLOITATION.
 PESIT     01 : 1       PROTOCOLE PESIT.
 SYSPLEX   19 : 0       INTERFACE SYSPLEX
 TCP-IP    15 : 1       PROTOCOLE TCP-IP.
           14 : 0
 SSL       20 : 1       INTERFACE SSL
```

Par l'option « AP » Vous pouvez afficher le fichier « Asset Protection » :

```
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
```

Présentation de l'option SSL

L'option SSL s'appuie sur les services SSL de z/OS, qui peuvent être associés au dispositif hardware de cryptographie « *Integrated Cryptographic Service Facility* » (*ICSF*). La gestion des certificats est assurée soit par l'utilitaire SSL *gskkyman*, soit par les fonctions RACF spécifiques (méthode conseillée et décrite dans ce document).

La fonctionnalité s'intègre dans l'architecture de Connect:Express au travers d'un « handler SSL » qui assure l'interface entre les services réseau du moniteur (l'ANM) et les services SSL de z/OS.

L'activation de SSL est indépendante du protocole de transfert utilisé (PeSIT, Etebac ou Odette), et du réseau utilisé (TCP/IP, X25), aux paramètres de configuration près.
La fonctionnalité est disponible en mode client et en mode serveur.

NOTE IMPORTANTE : L'option SSL ne s'applique pas aux transferts FTP qui sont traités dans l'AFM.

Généralités sur la cryptographie

La cryptographie est l'ensemble des techniques qui permettent de chiffrer des messages. Un système cryptographique utilise des clés de chiffrement échangées entre partenaires. Seuls les partenaires en possesion de ces clés peuvent partager une information en la chiffrant et la déchiffrant avec les clés .

Il y a deux types de systèmes : l'un dit "à clé symétrique", l'autre dit "à clé asymétrique". Le système à clé symétrique (ou clé secrète) utilise la même clé pour chiffrer et déchiffrer un message. Le système à clé asymétrique (ou clé publique) utilise deux clés différentes, l'une publique et l'autre privée, pour chiffrer et déchiffrer un message : la clé publique permet de déchiffrer un message chiffré par la clé privée, et réciproquement. Les systèmes à clé symétrique sont plus simples et plus rapides, mais les deux parties doivent échanger la clé par un moyen quelconque mais sécurisé, car si la clé secrète est découverte par une tierce partie, la sécurité est compromise. Les sytèmes à clé asymétrique n'ont pas ce problème car la clé publique peut être échangée librement sans compromettre la sécurité. Le clé privée, elle, n'est jamais transmise.

La cryptographie permet de mettre en oeuvre les fonctions de sécurités suivantes:

- ✓ L'authentification permet de vérifier que l'entité présente à l'autre bout de la connexion est le bon interlocuteur.
- ✓ La non-répudiation fournit la preuve de l'origine des informations transmises.
- ✓ L'intégrité des données assure que l'information n'a pas été altérée pendant la transmission.
- ✓ La confidentialité des données assure que l'information reste privée pendant la transmission.

L'option SSL vous permet de choisir entre deux protocoles de sécurité : le protocole TLS (Transport Layer Security), ou le protocole SSL (Secure Sockets Layer) .

Les protocoles SSL (Secure Sockets Layer) et TLS (Transport Layer Security)

Les protocoles SSL et TLS utilisent des certificats pour échanger des clés de session entre l'initiateur de la transmission des données et le récepteur des données. Un certificat est un document électronique qui associe une clé publique avec un individu ou une entité quelconque. Il vous permet de vérifier qu'une clé publique appartient bien à l'entité qui la revendique. Une autorité de certification (CA) est une entité responsable de la création et de la révocation de ces certificats. Le CA vérifie l'identité du demandeur, crée un certificat pour cette entité et signe ce certificat afin de se porter garant de sa validité.

Les protocoles SSL et TLS fournissent trois niveaux de sécurité:

- ✓ Le premier niveau de sécurité est activé lorsqu'un partenaire se connecte à un serveur Connect:Express. Après un premier contact, le 'handshake', le serveur Connect:Express envoie son certificat électronique au partenaire . Celui ci vérifie que ce certificat n'est pas expiré et qu'il a été créé par une autorité (CA) en qui il a confiance. Ce contrôle nécessite que le partenaire ait enregisté le fichier certificat de l'autorité et que le serveur Connect:Express ait accès à son propre certificat. Si les contrôles échouent pendant cette phase, le partenaire est prévenu que la session n'est pas sécurisée, et la connexion échoue.
- ✓ Le second niveau de sécurité, appelé authentification client, nécessite que le partenaire envoie à son tour son certificat. Si cette option est active, le serveur Connect:Express, après avoir envoyé son propre certificat, demande au partenaire de lui envoyer son certificat. Si le certificat du partenaire est signé par une autorité reconnue, la connexion s'établit. Ce contrôle nécessite que le partenaire ait enregisté son certificat et sa clé et que le serveur Connect:Express ait enregistré le fichier certificat de l'autorité.
- ✓ Le troisième niveau de sécurité s'applique à l'authentification client et ajoute le contrôle du champ 'common name' (CN) du certificat du partenaire par le serveur Connect:Express. Si Connect:Express ne trouve pas ce nom, la connexion échoue.

Pour communiquer avec les protocoles SSL et TLS, vous devez posséder un couple certificat X509 et clé privée.
Les protocoles SSL et TLS assurent la sécurité des données de la façon suivante:

- ✓ Authentification — Du fait que le CA a validé l'identité du demandeur selon une procédure établie, les utilisateurs qui font confiance à ce CA peuvent être sûrs qu'une clé publique appartient bien à celui qui le prétend. Le CA protège contre l'usurpation d'identité, et fournit une structure de confiance en associant chaque entité avec sa clé publique et sa clé privée.
- ✓ Preuve de l'origine et de l'intégrité des données — Le certificat apporte la preuve de l'origine de la transmission, le chiffrement valide l'intégrité des données. Le chiffrement avec la clé privée assure que les données ne sont pas altérées.
- ✓ Confidentialité des données — Le chiffrement des données assure la confidentialité. L'information sensible est convertie en un format illisible par l'émetteur avant d'être envoyée au récepteur qui la convertit en format lisible par le déchiffrement.

Les deux protocoles gèrent les communications de la même façon, TLS apportant plus de sécurité dans le processus:

- ✓ Authentification des messages: TLS utilise une méthode plus sûre — le HMAC (Key-Hashing for Message Authentication Code) — que SSL pour assurer l'intégrité et valider l'origine des données échangées.
- ✓ TLS définit une fonction pseudo aléatoire (PRF), qui utilise deux algorithmes de hashage pour générer le HMAC.
- ✓ TLS combine PRF and HMAC dans l'authentification des messages.
- ✓ TLS précise le type de certificat à utiliser.
- ✓ TLS ajoute des alertes

Configuration de l'option SSL

Avant de mettre en œuvre l'option SSL, vous devez configurer les composants impliqués dans les transferts sécurisés : le moniteur TOM, l'ANM et la base de donnée dans laquelle sont stockés les certificats SSL. Il est conseillé d'utiliser les fonctions RACF de gestion des certificats.

Vous devez associer L'ANM à un keyring RACF, auquel vous connecterez le ou les certificats attribués à Connect:Express et ceux des autorités de certification (CA) reconnues.

Configuration du moniteur

Le paramétrage du moniteur vous permet de définir ses caractéristiques locales en tant que moniteur SSL: activation du handler, définition des accès par les clients et indication du certificat et des options SSL par défaut. Tous les paramètres sont définis dans le fichier SYSIN.

Les principes généraux sont les suivants :

- ✓ Par défaut, le handler SSL est inactif.
- ✓ Les accès SSL par TCP/IP sont caractérisés par des ports spécifiques.
- ✓ Les accès SSL par X25 sont caractérisés par des données utilisateur X25 ou des sous adresses.
- ✓ Les valeurs par défaut sont celles des services SSL de z/OS.
- ✓ Les valeurs définies en SYSIN représentent les valeurs par défaut des fichiers de configuration de l'ANM.
- ✓ Le profil SSL défini par la SYSIN est par définition le profil zéro (SSLCFG00)

D'autre part, l'interface HPNS ne permet pas d'intégrer le handler SSL: il faut donc modifier le paramétrage pour utiliser l'interface Open Edition de z/OS.

TCPORG=(HPNS, jobtcpip) devient TCPORG=(SOE)

Le tableau ci-dessous récapitule les paramètres caractérisant le service SSL de Connect:Express. Certains paramètres admettent les minuscules : il faut donc être prudent dans la saisie car la plupart des paramètres de la SYSIN sont exclusivement en majuscule, les mots clés en particulier.

Fichier SYSIN

Pour pouvoir utiliser le service SSL il faut au minimum l'ensemble des paramètres suivants :

SSLOPT=Y
SSLKRG=Nom de keyring racf (ou couple SSLDTTB + SSLPSW)
SSLPRT=Numéro de port TCP/IP à l'écoute des clients SSL
et / ou
SSLUDF=Données utilisateur X25 attendues des clients SSL

Champ	Lg/Val	Description	Type
TCPORG	(SOE)	Cette valeur détermine l'utilisation de l'interface Open Edition de z/OS. Elle est obligatoire pour pouvoir faire cohabiter les handlers TCP/IP et SSL.	Obligatoire
SSLOPT	N/Y	Activation du handler SSL. 'N' est la valeur par défaut. 'Y' doit être associé avec un minimum de paramètres de configuration SSL de type 'obligatoire' .	Optionnel
SSLCFG	N/Y	Utilisation de profils multiples. 'N' est la valeur par défaut. 'Y' suppose que le fichier ANMSSL est défini et alloué à l'ANM.	Optionnel
SSLKRG	1 à 44 car. M+m	Nom du « Keyring » racf associé à l'ANM. Ce paramètre exclut les paramètres SSLDTB et SSLPSW. Exemple : SSLKRG=TOM4.KEYRING	Obligatoire (1)
SSLDTB	1 à 44 car. M+m	Nom de la base de données HFS dans laquelle sont stockés les certificats. Ce paramètre est associé au paramètre SSLPSW et exclut le paramètre SSLKRG.	Obligatoire (1)
SSLPSW	1 à 16 car. M+m	Mot de passe d'accès à la base de données HFS dans laquelle sont stockés les certificats.	Obligatoire (1)
SSLCER	1 à 34 car. M+m	Label du certificat par défaut (profil SSLCFG00) référencé dans la base de données des certificats ou dans le Keyring Racf : il peut inclure des blancs. S'il est absent, le certificat défini par défaut dans la base est pris en compte. Exemple : SSLCER=Label du serveur Paris 2	Optionnel
SSLPRT	1 à 5 c. num.	Numéro de port TCP/IP à l'écoute des appels entrants sous SSL. De 1 à 65535.	Obligatoire (2)
SSLUDF	1 à 16 c. hex.	Données utilisateur X25 attendues des clients SSL. Le nombre de caractères doit être pair, soit 8 fois 2 caractères au maximum. Exemple : SSLUDF=AB02	Obligatoire (2)
SSLSAD	1 à 4 c. num.	Sous adresse X25 attendue des clients SSL.	Obligatoire (2)
SSLPRO	1 à 5 c. num.	Numéro de port TCP/IP à l'écoute des appels entrants Odette sous SSL. De 1 à 65535.	Obligatoire (2)
SSLUDO	1 à 16 c. hex.	Données utilisateur X25 attendues des clients SSL Odette. Le nombre de caractères doit être pair, soit 8 fois 2 caractères au maximum. Exemple : SSLUDF=AB04	Obligatoire (2)
SSLSAO	1 à 4 c. num.	Sous adresse X25 attendue des clients SSL odette.	Obligatoire (2)
SSLTRC	0/1	Option de trace par défaut (profil SSLCFG00). '0' est la valeur par défaut. '1' active la trace environnement du handler SSL. Cette trace est écrite dans un fichier SYSPRINT de l'ANM.	Optionnel
SSLTIM	1 à 6 c. Num.	Durée de rétention de l'identifiant de session SSL, en nombre de secondes. Par défaut elle est égale à 86400 secondes.	Optionnel
SSLTL1	N/Y	Support du protocole TLS V1 par défaut (profil SSLCFG00). La valeur par défaut est 'Y'.	Optionnel
SSLVE3	N/Y	Support du protocole SSL V3 par défaut (profil SSLCFG00). La valeur par défaut est 'Y'.	Optionnel
SSLVE2	N/Y	Support du protocole SSL V2 par défaut (profil SSLCFG00). La valeur par défaut est 'N'.	Optionnel
SSLAUT	N/Y	'N' est la valeur par défaut. 'Y' indique que, en mode serveur, l'autentification du client sera demandée.	Optionnel
SSLCIP	1 à 32 c. hex.	Cipher suite par défaut(profil SSLCFG00) : indique l'ordre de préférence des options de chiffrement, parmi les options supportées par les services SSL de z/OS. Le nombre de caractères doit être pair, soit 16 fois 2 caractères au maximum. Exemple SSLCIP=09060504.	Optionnel

(1) SSLKRG ou SSLDTB+SSLPSW

(2) L'un au moins des paramètres SSLPRT,SSLUDF,SSLSADR, SSLPRO,SSLUDO,SSLSADO

		Les valeurs données ne sont pas contrôlées au moment de l'initialisation: s'assurer de leur validité. Par défaut, la liste utilisée par z/OS est la suivante : **050435363738392F303132330A1613100D0915120F0C0306020100** <u>La liste ci-dessous résume les valeurs supportées par z/OS, pour SSL V3 et 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 **Pour SSL V2, la liste est toujours prise égale à la liste par défaut de z/OS, soit : 713642** <u>La liste ci-dessous résume les valeurs supportées par z/OS, pour SSL V2 :</u> **1** 128-bit RC4 encryption with MD5 message authentication (128-bit secret key) **2** 128-bit RC4 export encryption with MD5 message 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 message 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 message authentication (168-bit secret key)	

Commandes MVS au moniteur

Le handler SSL peut être en service ou hors service : le status est affiché dans l'écran général du suivi, option TSO/ISPF 2.1.

```
/F TOMJOB,SSL=ON active le handler
/F TOMJOB,SSL=OFF désactive le handler
```

```
TOM4230     Suivi du moniteur     ID=          mode= *
 OPTION ===> !

             ^                                                    PSR0008
             F (ID)       - FICHIERS.         B   - BYPASS.       06/03/24
             P (ID)       - PARTENAIRES.      C   - COUPLAGE.     06:45
             R (ID)       - REQUETES.         G   - GLOBAL.       CSGA
             N            - RESEAU.           Z   - ACTIVITE.     CSGPLEX
             T            - TRANSFERTS.
             */-/A/H/I/U  - 'mode'.

             MONITEUR  ===> TOM4 / CSGA  ACTIF     GLOBAL
             EXIT UEXJNL  : L1B2PDIX     EN-SERVICE

 ----------- S DETAIL, E EN-SERVICE, H HORS-SERVICE
 V
 _   1074    FICHIERS     - RESSOURCE  : EN-SERVICE
 _   586     PARTENAIRES  - RESSOURCE  : EN-SERVICE
 _   -       REQUETES     - RESSOURCE  : EN-SERVICE   UTILISEE A -   %
 _           RESEAU       - VOIR DETAIL: EN-SERVICE
 _           TRANSFERTS   - VOIR DETAIL, SERVEURS UTIL./ALLOUES: -   /  16
             SSL          - RESSOURCE  : EN-SERVICE

             X EXIT, -PF3- FIN, -ENTREE- SUIVI, -PF10/11- DEFILEMENT
```

Configuration de l'ANM

Les paramètres SSL par défaut sont reçus par TOM dans sa SYSIN et transmis à L'ANM pendant la phase d'initialisation. Si le paramètre SSLCFG est égal à 'N', ou absent, l'ANM charge en mémoire la configuration par défaut.

```
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
```

Si le paramètre SSLCFG est égal à 'Y', l'ANM charge en mémoire les fichiers de configuration définis dans le fichier ANMSSL.

```
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
```

Le fichier ANMSSL

Le fichier des profils SSL est déclaré dans le JCL de l'ANM, par la carte DD ANMSSL. C'est un fichier PDS, de format fixe, dont la taille d'enregistrement ne doit pas dépasser 300 octets.

L'exemple ci-dessous illustre le contenu du fichier ANMSSL.

```
   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**
```

Les membres préfixés par les lettres 'DN' sont utilisés pour le contrôle des certificats, décrit au chapitre '*Contrôle des DN*'. Les membres préfixés par 'SSLCFG' définissent les profils SSL, numérotés de 01 à 99, décrits au chapitre '*Utilisation des profils SSL*'. Le fichier SYSSSL est utilisé pour la sélection d'un profil en appel entrant, décrit au paragraphe '*Mode serveur – Fichier SYSSSL*'.

Tout membre dont le nom ne respecte pas les conditions ci-dessus, 'README' par exemple, est ignoré.

Configuration SSL par défaut

Le fichier SYSLOG de l'ANM montre la liste des paramètres traités.

Procédure JCL de l'ANM

Les fichiers spécifiques de l'option SSL sont indiqués ci-dessous :

- La bibliothèque LOADSSL est concaténée en STEPLIB
- La bibliothèque ANMSSL allouée par la carte DD ANMSSL
- Le fichier SYSOUT SYSPRINT contient les traces SSL
- Le fichier SYSOUT SYSCFG contient le résultat du chargement de la configuration SSL
- Le fichier SYSOUT SYSDNCTL contient la trace des contrôles de certificats

L'utilisation de l'interface TC/IP Opend Edition peut rendre nécessaire l'ajout d'une carte pour préciser le stack IP à utiliser. Si elle est absente les statck IP de la machine sont utilisés indifféremment ce qui peut perturber le traitement des contrôles d'adresses et de noms de hosts.

```
//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)
//*
//* 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.TOMV423.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
//SYSDNCTL DD SYSOUT=&OUT
```

La carte « ENVIRON DD » peut être activée pour obtenir une trace sur les services SSL de z/OS. Le fichier de configuration du langage environment $$SSLTRC$$ est décrit au paragraphe *Trace gskssl*.

Le fichier ANMSSL est accessible à l'opérateur par l'option 0 de l'interface TSO/ISPF : l'option 'S' permet de prendre le fichier ANMSSL sous éditeur. Les mises à jour sont prises en compte après arrêt-relance du handler SSL, par les commandes suivantes passées successivement au moniteur:

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

```
TOM4230-------------- INITIALISATION 2/2 -------------------------------------
 OPTION ===>


             ? MONITEUR ===> TOM3  INITIALISATION AUTOMATIQUE ---> OUI
               UNITE TEMPORAIRE ===> SYSDA    , INTERFACE JES2 ---> ISF
             L LOGON-PROCEDURE, O OPTIONS, V VERIFICATION D'INSTALLATION.
 ---------- S : VERIFICATION DES FICHIERS JOBTOM3 CSGB ACTIF 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- FIN, -PF10/11- DEFILEMENT
```

Utilisation des profils SSL

Les profils SSL sont gérés par l'ANM au cours des mises en session SSL. Ils permettent d'appliquer des règles différentes selon les partenaires.

Définition

Un profil SSL est défini dans un membre du fichier ANMSSL dont le nom respecte la syntaxe suivante :

SSLCFGnn	'nn' différent de '00'

Les deux caractères numériques 'nn', non nuls, serviront à identifier le profil. Le membre SSLCFG00 serait ignoré, comme tout membre dont le nom ne respecte pas les conditions définies au paragraphe précédent.

Un profil SSL peut être défini pour préciser un ou plusieurs paramètres de configuration, le profil défini dans le fichier SYSIN du moniteur constituant la configuration numéro 00. Un profil SSL est constitué par les paramètres définis, dans l'ordre suivant :

1. Dans le profil SSLCFG
2. Dans la SYSIN du moniteur
3. Les valeurs par défaut de z/OS

Le tableau suivant indique la liste des paramètres de configuration SSL et où il peuvent être définis :

Paramètre	**z/OS**	**Sysin**	**SSLCFG**
Activation du handler SSL		SSLOPT (Y/N)	
Nom du keyring RACF associé à l'ANM		SSLKRG	
Nom de la base de donnée HFS Mot de passe d'accès		SSLDTB SSLPSW	
Port d'écoute, sous addresse ….. Pour TCP/IP ou X25 Pour PeSIT ou odette		SSLPRT, SSLPRO SSLSAD, SSLSAO SSLUDF, SSLUDO	
Authentification réciproque	No	SSLAUT (Y/N)	
Durée de rétention de l'identifiant de session SSL	86400 secondes	SSLTIM	
Label du certificat local	Certificat par défaut	SSLCER	SSLCER
Niveaux SSL supportés (pour compatibilité)	30	SSLLEV (31,30,20)	
Support de SSL V2	No	SSLVE2 (Y/N)	SSLVE2 (Y/N)
Support de SSL V3	Yes	SSLVE3 (Y/N)	SSLVE3 (Y/N)
Support de TLS V1	Yes	SSLTL1 (Y/N)	SSLTL1 (Y/N)
Liste de chiffrement	**050435363738392F30313 2330A1613100D0915120F 0C0306020100**	SSLCIP	SSLCIP
Activation de la trace dans le handler SSL		SSLTRC (0/1)	SSLTRC (0/1/2)
Contrôle du DN			SSLDNC
Description du profil			SSLCFG
Etat du profil			STATUS

Règles de syntaxe

Une ligne commençant par le caractère '*' est un commentaire , une ligne vide est ignorée.
Une ligne commençant par les deux caractères '/*' provoque la fin du traitement sur le profil en cours.
Un profil doit fournir au moins un paramètre actif, le paramètre SSLCFG étant descriptif, sauf s'il prend la valeur $DUMMY$ qui a été introduite pour assurer la compatibilité avec la version 4.2.0.
Les mots clés sont uniques et en caractères majuscules.

Le handler SSL ne s'initialise que si aucune erreur de syntaxe n'a été détectée.

Exemple de profil :

```
   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=*** CONFIGURATION DE PRODUCTION ***
 000002
 000003 STATUS=E               E/H
 000004 SSLCER=Certificat 05                     END OF FIELD
 000005 * Pas de trace en 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 ****************************
```

Les paramètres suivants peuvent être définis dans le profil, dans n'importe quel ordre. Les valeurs par défaut sont celles définies dans la SYSIN du moniteur.

Champ	Lg/Val	Description	Type
SSLCFG	Selon LRECL	Description du profil. Exemple : SSLCFG=*** Configuration spéciale *** Valeur particulière $DUMMY$: ce profil est équivalent au profil 00 (la SYSIN) et le paramètre SSLCFG doit être unique.	Descriptif ou Actif
STATUS	E/H	Décrit l'état de ce profil. La valeur par défaut est 'E'=Enabled. Ce paramètre permet de désactiver le profil, par la valeur 'H'.	Actif
SSLCER	1 à 34 car. M+m	Label du certificat local référencé dans la base de données des certificats ou dans le Keyring Racf : il peut inclure des blancs, des majuscules et des minuscules. Exemple : SSLCER=Label du certificat spécial	Actif
SSLTRC	0/1 /2	'0' désactive la trace. '1' active la trace limitée au handshake. '2' active la trace complète, handshake et transfert des données. Cette trace est écrite dans le fichier SYSPRINT de l'ANM.	Actif
SSLCIP	1 à 32 c. hex.	Cipher suite : indique l'ordre de préférence des options de chiffrement, parmi les options supportées par les services SSL de z/OS. Le nombre de caractères doit être pair, soit 16 fois 2 caractères au maximum. Exemple SSLCIP=09060504.	Actif
SSLTL1	Y/N.	Support de TLS V1	Actif
SSLVE2	Y/N.	Support de SSL V2	Actif
SSLVE3	Y/N.	Support de SSL V3	Actif
SSLDNC	DN….	Nom d'un membre de contrôle de DN. Voir le chapitre '*Contrôle des DN*'	Actif

Chargement des profils SSL

Les profils sont chargés durant l'initialisation du handler SSL. Toute modification de profil doit être suivie d'un rechargement par arrêt relance du handler.

Lorsque qu'une erreur est détectée dans un profil, un message WTO est envoyé pour signaler l'erreur. Le handler ne s'initialise que si aucune erreur n'a été détectée. Le message SSL0011E indique que une ou plusieurs erreurs ont été détectées : un ou plusieurs messages SSL0012E précèdent ce message.

```
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
```

Le fichier SYSCFG récapitule quels profils ont été chargés : il signale les erreurs de syntaxe par un point d'exclamation en colonne 2, et signale qu'un profil a été rejeté par la ligne ======REJECTED===== comme dans le profil SSLCFG08 de l'exemple ci dessous.

```
      ======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======
```

Les erreurs sont identifiées par les mots clés suivants:

Code	Explication	Action
DUPK	Mot clé en double	Modifier le profil
INVK	Mot clé invalide	Modifier le profil
KVAL	La valeur associée à un mot clé est invalide	Modifier le profil
LREC	La taille d'enregistrement du fichier ANMSSL est invalide	Allouer le fichier ANMSSL avec une taille d'enregistrement de 300 caractères maximum.
NLEV	La combinaison des paramètres SSLTL1, SSLVE3 et SSLVE2, après fusion avec la définition par défaut en SYSIN, résulte en une valeur nulle	Modifier le profil
NULL	Un profil ne contient aucun paramètre	Modifier le profil
LINK	Erreur d'allocation	Contacter le support
OPEN	Erreur à l'ouverture du fichier	Contacter le support
STOR	Erreur à l'acquisition de mémoire virtuelle	Contacter le support

La séquence normale des messages d'initialisation est la suivante :

```
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
```

Mode demandeur

Le déclenchement d'un transfert sécurisé par SSL peut se faire à différents niveaux :

- Attribution d'un numéro de profil au partenaire, par le champ CONFIGURATION SSL.

```
TOM4230     PARTENAIRE DE TOM3 A MODIFIER   (2/4)
 OPTION ===>                        -ENTREE- : SUITE, -PF3- : ANNULER  X : EXIT
 TYPE: TOM,PESIT-E

 NOM SYMBOLIQUE        : PARTNER3            DPCSID ALIAS          -> -
 MOT DE PASSE TOM     => PSR                DPCPSW ALIAS          -> -
 ETAT INITIALISATION  -> E                  CLASSE APM RECEPTION  -> B
 UTILISATEUR RACF     -> TOMPSR             GROUPE RACF           -> -

 NATURE PARTENAIRE    => T
 PROT.SESSION NUM.-T. => 5   => 2           CONFIGURATION SSL     -> 06
 REESSAI AUTOMATIQUE  -> N                  CONTROLE DU DN        -> -

 TYPES DE LIAISON     => M   => IXS
 EFF. TOT.-ENT.-SOR.  => 256 -> 000 -> 000  T-REGULATION FLUX SLD -> -

 SNA: LUNAME => TOM3AP01  LOGMODE   -> -        LOGDATA  -> -         DISC -> N
 X25: MCHMSC -> B     ADR.DIST. => 3110214404824    ADR.LOC. -> -
      GFA    -> -     UDF       -> -                TAXATION -> 1
      SERVICES COMPLEMENTAIRES  -> -
 IP : ADRES. => -              PORT => 20740 FTP PASV => - PROFIL -> -
      HOTE   -> MVS.<HOST>                          'S': - DROITS -> -
 NOTE ->
```

- Attribution d'un numéro de profil au fichier, par le champ CONFIGURATION SSL.

```
TOM4230---- REPERTOIRE DES FICHIERS (2/5) -----------------------------------
 OPTION ===>

 NOM SYMBOLIQUE             : FICTST     MODE: NORMAL

 ETAT INITIALISATION ...    : E          E: EN-SERVICE H: HORS-SERVICE

 DIRECTION .............    : *          T:TRANSMETTRE R:RECEVOIR *:TRANS./REC.
 PARTENAIRE RECEPTEUR ..    : *          'NOM', £LISTE, */$$ALL$$ OU $$API$$
 PARTENAIRE EMETTEUR ...    : *          'NOM', £LISTE, */$$ALL$$ OU $$API$$

 PRIORITE ..............    : 1          0:URGENT 1:RAPIDE 2:NORMAL 3:LENT
 TYPE DEFINITION DU DSN     : D          D:DYNAMIQUE F:FIXE
 REGLE ALLOCATION ......    : 2          0:CREER/REMPLACER 1:PREALL. 2:A CREER
                                         3:EXIT A:SERVEUR APPLICATIF
 TYPE FICHIER ..........    : S          S/H/M/P/PU/V/VU/UU/SU/TU/HU
 PRESENTATION ..........    : 04         COMPRESS.,T.DONNEES (01-24)
 MEMBRE CHARG./DECHARG..    : -          OPTIONNEL
 CONFIGURATION SSL .....    : 02         OPTIONNEL

 OPTION   : VISUALISER                   MAJ   : 09/02/03 07:57 PSR0003
 -ENTREE- : ECRAN SUIVANT                -PF3- : ANNULATION
```

- Attribution d'un numéro de profil à la requête, par le champ :
  - CONFIG. SSL de l'interface opérateur (Extension de requête)

```
TOM4230     EXTENSION DE TRANSFERT                        NOMS INITIALISES     !
 OPTION ===>                                                                CSGB

 4XX/TEST

 SOUS-SYSTEME  :   TOM3
 FICHIER ....  :   FICTST                                        EN-SERVICE
 DIRECTION ..  :   T          (T/R)     <- *
 PARTENAIRE .  :   PARTNER3             <- $$ALL$$  30           EN-SERVICE
 DSN LOCAL ..  :   PSR$REC.PS.F080.SHORT                         DYNAMIQUE
                <- PSR$TST.& PARTNID.&REQNUMB                 -   SEQUENTIEL
 Rdsn/Pi99 .. --->                                             <  *1
                <-
 FTP T/S/M .. ---> '' ---> '  ---> '   <- -   -  -     STOU   ---> '    <- N
 GROUPE RACF. ---> ''''''''                           ('VALEUR'/'BLANC')
 Org/Dest ... --->          < --->          <         *1
 ET SEULEMENT SI TOM EST ACTIF :
 CONFG. SSL . ---> 05                                 ('VALEUR'/'BLANC')
 Alias id/psw --->          < --->          <         *1
 V----- S : DETAIL
 '' Api ....  --->
                    <                           *1:('VALEUR'/'valeur'/'BLANC')
             X EXIT, -ENTREE- CONFIRMATION, -PF1- AIDE TRC, -PF3- RETOUR
```

  - SEC de l'utilitaire 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
```

  - EX1SSECN du programme L0B2Z20

Ce paramètre est traité par le handler SSL, qui retrouvera le profil correspondant dans la table chargée durant son initialisation. Si le profil n'existe pas, le transfert tombe en erreur de session avec un code NRC de la forme NRC=SCF0xx , xx étant le profil demandé, et non trouvé. Le message SSL0015W est envoyé.

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

Jesmsglg de l'ANM
02.30.34 STC99845  SSL0015W CONFIGURATION FILE 99 NOT FOUND
```

Mode serveur – Fichier SYSSSL

Un appel entrant est traité sous SSL si il arrive sur un des point d'accès décrits par les paramètres de la SYSIN du moniteur SSLPRT ou SSLPRO pour TCP/IP, SSLSAD, SSLUDF, SSLSAO ou SSLUDO pour X25. Par défaut la configuration SSL utilisée est celle définie par la SYSIN, soit la configuration 00.

Le membre SYSSSL du fichier ANMSSL permet de choisir un profil particulier, sur critère.

Règles de syntaxe

Une ligne commençant par le caractère '*' est un commentaire , une ligne vide est ignorée.
Une ligne commençant par les deux caractères '/*' définit la fin du fichier et l'arrêt du traitement.
Les mots clés sont uniques et en caractères majuscules.

```
'CRITERE',CF='Numéro de profil'

 CRITERE : 'LT='Adresse à contrôler'
```

Chaque ligne définit un critère et le numéro de profil associé, séparés par une virgule, dans un ordre indifférent. Le critère indique le type de lien *L* (X=X25, I=TCP/IP) , le type d'adresse *T* (A=Adresse, H=Nom de host) - les combinaisons possibles sont XA, IA et IH - et la valeur d'adresse à contrôler. La valeur peut représenter une adresse spécifique ou une adresse générique sous la forme '*generic**'. Le paramètre CF= indique le numéro de profil à prendre en compte, deux caractères numériques de 00 à 99.

Traitement des adresses TCP/IP

Pour les adresses TCP/IP, toujours considérer la représentation complète de l'adresse 'xxx.xxx.xxx.xxx'.

Par exemple :

'12.24', qui est équivallent à '12.24.*', est traité comme '012.024.*'
'12.24*' est traité comme '012.24*'.

L'adresse '12.241.20.1' satisfait le critère '12.24*', mais pas le critère '12.24' .

L'exemple ci-dessous illustre la syntaxe du fichier SYSSSL. Les noms de host TCP/IP doivent être en lettres majuscules.

```
  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             SOCIETE 1
000018 XA=012345678*,CF=03              GROUPE 1
000019 *
000020 * IP
000021 *
000022 IH=XBF.OFF*,CF=02                GROUPE 2
000023 IH=MVS*,CF=10                    GROUPE 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 *
```

Algorithme de sélection

La table chargée en mémoire est l'image exacte du fichier SYSSSL.

La sélection d'un profil se fait au moment de la connexion réseau. Pour X25, le handler compare l'adresse de l'appelant avec les critères de type XA définis dans la table. Pour TCP/IP, il y a deux modes de recherche, le mode nom de host et le mode adresse. Le handler commence par traiter le nom de host en le comparant avec les critères de type IH. Dès qu'un critère de type IA est trouvé, le traitement bascule sur le mode adresse IP.
La table est balayée entièrement pour chaque traitement, tant qu'aucune égalité exacte n'est trouvée : le critère le plus précis est pris. La précision du critère est déterminée par la longueur sur laquelle l'égalité est trouvée.

Si aucun critère n'est satisfait, le profil par défaut de la SYSIN, est pris.
Si le profil indiqué n'existe pas, la connexion est rejetée, avec les messages et codes suivants :

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

Jesmsglg de l'ANM
07.55.48 STC00065  SSL0015W CONFIGURATION FILE 99 NOT FOUND
```

Exemple en TCP/IP

En TCP/IP, la recherche commence sur le nom de host, mais peut basculer sur le mode adresse au premier critère IA trouvé. Trois scénarios sont à envisager :

1. Tous les critères TCP/IP sont de type H : le traitement s'arrête à la première égalité trouvée sur le nom de host. Si aucune égalité n'est trouvée, le plus précis des critères satisfaits est pris en compte.
2. Tous les critères TCP/IP sont de type A : le traitement bascule tout de suite en mode adresse et s'arrête à la première égalité trouvée sur l'adresse. Si aucune égalité n'est trouvée, le plus précis des critères satisfaits est pris en compte.
3. Les critères TCP/IP sont mélangés de type A ou H: le traitement commence en mode nom de host jusqu'à égalité sur le nom de host ou passage en mode adresse. Une fois en mode adresse, le traitement s'arrête à la première égalité trouvée sur le nom de host, ou à la première égalité trouvée sur l'adresse. Si aucune égalité n'est trouvée, le plus précis des critères satisfaits en mode adresse est pris en compte.

Dans l'exemple de fichier SYSSSL ci-dessus, le partenaire de nom de host `MVSB.XBF.COMPANY.COM, d'adresse 12.24.55.3,` sera traité avec le profil SSL CF=05, du fait de l'égalité trouvée sur le nom de host, alors que la recherche avait basculé sur le mode adresse, et que le critère IA=12.24 était satisfait.

Chargement du fichier SYSSSL

Le fichier SYSSSL est chargé durant l'initialisation du handler SSL. Toute modification de ce fichier doit être suivie d'un rechargement par arrêt relance du handler.
Lorsque qu'une erreur est détectée dans une définition, un message WTO est envoyé pour signaler l'erreur. Le handler ne s'initialise que si aucune erreur n'a été détectée. Le message SSL0011E indique que une ou plusieurs erreurs ont été détectées : un ou plusieurs messages SSL0012E précèdent ce message.

```
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
```

Le fichier SYSCFG récapitule le contenu du fichier SYSSSL : il signale les erreurs de syntaxe par un point d'exclamation en colonne 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           DEVELOPPEMENT
IH=XBF.OFF*,CF=02               GROUPE 2
IH=MVS*,CF=10                   GROUPE 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
```

Les erreurs sont identifiées par les mots clés suivants:

Code	Explication	Action
DUPK	Mot clé en double – le numéro de ligne est précisé	Modifier la ligne
INVK	Mot clé invalide – le numéro de ligne est précisé	Modifier la ligne
KVAL	La valeur associée à un mot clé est invalide	Modifier la ligne
NOCF	Aucun profil n'est défini – le numéro de ligne est précisé	Modifier la ligne
INVR	Enregistrement invalide, suite à une des erreurs précédentes	Corriger les erreurs correspondantes
MAXR	Le maximum de définitions a été atteint - le numéro de ligne indique le point où le traitement est arrété, la première ligne non prise en compte	Supprimer les lignes inutiles
LREC	La taille d'enregistrement du fichier ANMSSL est invalide	Allouer le fichier ANMSSL avec une taille d'enregistrement de 300 caractères maximum.
NULL	Le fichier SYSSSL ne contient aucune spécification valide	Corriger les erreurs
LINK	Erreur d'allocation	Contacter le support
OPEN	Erreur à l'ouverture du fichier	Contacter le support
STOR	Erreur à l'acquisition de mémoire virtuelle	Contacter le support

Contrôle des DN

Ce chapitre décrit la mise en oeuvre du contrôle des certificats.

Définition

Le contrôle des DN apporte un niveau supplémentaire d'authentification. Une fois le handshake SSL terminé, les certificats échangés, qui ont été authentifiés par les services SSl de z/OS, peuvent être contrôlés au niveau de leur contenu. Le traitement est basé sur des fichiers de contrôles, placés dans le fichier PDS ANMSSL, et qui peuvent être référencés par leur nom de différentes façons, selon que la communication est d'initiative locale ou distante.
Les noms de ces membres de PDS sont préfixés par 'DN' , par convention. L'utilisation d'un fichier de contrôle n'est effective que lorsque c'est nécessaire. La mise à jour de ces fichiers et de leur contenu peut donc être considérée comme dynamique.

L'écran d'initialisation de l'interface opérateur permet d'accéder au fichier ANMSSL en ligne.

```
TOM4230-------------- INITIALISATION 2/2 -------------------------------------
 OPTION ===>


             ? MONITEUR ===> TOM3  INITIALISATION AUTOMATIQUE ---> OUI
               UNITE TEMPORAIRE ===> SYSDA    , INTERFACE JES2 ---> ISF
             L LOGON-PROCEDURE, O OPTIONS, V VERIFICATION D'INSTALLATION.
 ---------- S : VERIFICATION DES FICHIERS .         . . .
 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- FIN, -PF10/11- DEFILEMENT
```

```
   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**
```

Paramétrage du contrôle de DN

Le contrôle est effectué à l'issue du handshake SSL : en mode demandeur le partenaire symbolique est connu, alors qu'en mode serveur seule l'adresse du distant est connue. Les mécanismes diffèrent dans les deux cas.

Mode demandeur

En mode demandeur le contrôle peut être paramétré au niveau de la définition du partenaire, ou dans le profil SSL. Dans l'exemple ci-dessous, le partenaire PARTNER3 est appelé sous la configuration SSL SSLCFG05. Ce profil est rattaché au fichier de contrôle DNCFG05 mais, pour ce partenaire, le contrôle de DN est effectué par le fichier DN00001.

```
TOM4230     PARTENAIRE DE TOM3 A MODIFIER   (2/4)
 OPTION ===>                        -ENTREE- : SUITE, -PF3- : ANNULER  X : EXIT
 TYPE: TOM,PESIT-E

 NOM SYMBOLIQUE        : PARTNER3            DPCSID ALIAS          -> -
 MOT DE PASSE TOM     => PSR                DPCPSW ALIAS          -> -
 ETAT INITIALISATION  -> E                  CLASSE APM RECEPTION  -> B
 UTILISATEUR RACF     -> TOMPSR             GROUPE RACF           -> -

 NATURE PARTENAIRE    => T
 PROT.SESSION NUM.-T. => 5   => 2           CONFIGURATION SSL     -> 05
 REESSAI AUTOMATIQUE  -> N                  CONTROLE DU DN        -> DN00001

 TYPES DE LIAISON     => M   => IXS
 EFF. TOT.-ENT.-SOR.  => 256 -> 000 -> 000  T-REGULATION FLUX SLD -> -

 SNA: LUNAME => TOM3AP01  LOGMODE   -> -        LOGDATA  -> -         DISC -> N
 X25: MCHMSC -> B     ADR.DIST. => 3110214404824    ADR.LOC. -> -
      GFA    -> -     UDF       -> -                TAXATION -> 1
      SERVICES COMPLEMENTAIRES  -> -
 IP : ADRES. => -                PORT => 20740 FTP PASV => - PROFIL -> -
      HOTE   -> MVS.<HOST>                          'S': - DROITS -> -
 NOTE ->
```

```
      ======SSLCFG05======
SSLCFG=*** CONFIGURATION DE PRODUCTION ***
SSLCER=Certificat de production
SSLCIP=0A                        168-bit Triple DES -SHA-1 -RSA
SSLTL1=Y
SSLVE3=N
SSLDNC=DNCFG05
```

Mode serveur

En mode serveur, le contrôle de DN est toujours défini par le profil, sélectionné à partir du fichier SYSSSL. Dans l'exemple ci-dessous, le partenaire de nom de host MVSB.XBF.COMPANY.COM est pris sous le profil SSLCFG05, et donc le fichier de contrôle est DNCFG05.

```
====== SYSSSL ======
XA=0193562,CF=01             BNP,SG,CEDI
XA=012345678*,CF=03          SOFINCO
CF=03,XA=012345678*
IH=XBF.OFF*,CF=02                GROUPE 2
IH=MVS*,CF=10                    GROUPE 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
```

Traitement du contrôle de DN

Le contrôle de DN est effectué par le handler SSL à l'issue d'un handshake réussi.

Syntaxe

Une ligne commençant par le caractère '*' est un commentaire.
Une ligne commençant par les deux caractères '/*' définit la fin du fichier.
Une ligne vide est rejetée.
Les blancs en tête de ligne sont ignorés.

La syntaxe est de type XML. L'exemple ci-dessous illustre la structure d'un fichier DN.

Quatres certificats peuvent être contrôlés :

- Le certificat local : LDN
- Le certificat de l'émetteur du certificat local : LISSDN
- Le certificat distant : DN
- Le certificat de l'émetteur du certificat distant : ISSDN

```
   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>
------------------------------------------------------------------------------
```

Quatre tags sont acceptés : <LDN>, <LISSDN>, <DN> et <ISSDN>, de façon unique.
La présence d'un des tags rend obligatoire la présence du tag de fermeture correspondant.
Chaque champ du certificat peut être contrôlé indépendamment, les mots clés des champs peuvent être quelconques, mais seulement sur 1 ou 2 caractères.
Les caractères ' ?' et '*' sont traités de la façon suivante :

- ' ?' signifie n'importe quel caractère à cette place.
- '*' doit être placé en fin de chaine, et signifie n'importe quelle chaine de caractère à la suite.

Réalisation du contrôle

A l'issue du handshake SSL, le contrôle est effectué si il est demandé au niveau du partenaire ou du profil. En cas d'erreur un message WTO SSLDN03E est envoyé par l'ANM : il indique le numéro de requête et le fichier de contrôle concernés, ainsi que la nature de l'erreur. Dans la log du moniteur, le code retour précise que l'erreur provient du contrôle de DN, par exemple NRC=SDC008 en appel sortant, SRC=SD08 en appel entrant. Le code 8 des exemples correspond à l'une des valeurs du tableau des codes ci dessous.

```
Log du moniteur
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 de l'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
```

Les erreurs sont identifiées par les mots clés et les codes suivants:

Code	Mot clé	Explication	Action
1	OPANMSSL	Erreur d'ouverture sur le fichier ANMSSL	Analyser le code erreur - Contacter le support
2	NOMEMBER	Le membre n'existe pas	Vérifier la configuration
3	LDYALINK	Erreur système	Contacter le support
4	ALLODNCT	Erreur d'allocation du fichier DN	Ajouter le paramètre SSLCFG=Y dans la SYSIN du moniteur, et la carte DD ANMSSL dans le JCL de l'ANM
5	OPENDNCT	Erreur d'ouverture sur le fichier DN	Analyser le code erreur - Contacter le support
6	LRECDNCT	La taille d'enregistrement du fichier ANMSSL est invalide	Allouer le fichier ANMSSL avec une taille d'enregistrement de 300 maximum.
7	SYNTDNCT	Erreur de syntax	Corriger le fichier DN
8	REJECTED	Le contrôle a détecté une différence	Vérifier le certificat concerné
9	DNINVKEY	Un tag invalide a été trouvé	Corriger le fichier DN
10	DNKEYACT	Le fichier DN se termine alors qu'un tag n'a pas été fermé	Corriger le fichier DN

L'analyse des problèmes peut être facilitée par l'utilisation des traces.

Analyse des erreurs

Les outils de trace à disposition sont :

- Le fichier SYSPRINT utilisé pour tracer les opérations SSL, sous contrôle du paramètre SSLTRC.
- Le fichier SYSDNCTL utilisé pour tracer les traitements du contrôle de DN, sous contrôle du paramètre SSLTRC aussi.

Ces deux fichiers doivent être déclarés dans le JCL de l'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)
//*
//* 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
//SYSIN DD DISP=SHR,DSN=index1.TOMV423.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
```

Informations du fichier SYSPRINT

Le fichier SYSPRINT contient les informations relatives au contexte, au profil et aux résultats du handshake SSL. Le contexte indique le numéro de requête, le profil indique quel fichier de contrôle et quel certificat local sont utilisés, et les résultats du handshake affichent les certificats traités. Rechercher les tags suivants, pour le numéro de requête '*nnnnnnnn*' :

Tag	Description
<Req>nnnnnnn</Req>	Les éléments de trace sont reliés à la requête concernée
<Cfg>06</Cfg>	Numéro du profil SSLCFG06
<DnCtl>DNCFG06 </DnCtl>	Fichier de contrôle DN, à blanc si le contrôle n'est pas demandé
<Cer>CERTZOS</Cer>	Label du certificat local
<SrvCer> <DN> <IssDN>	Certificat du serveur SSL DN en clair du serveur, tel qu'il est contrôlé DN en clair de l'émetteur du certificat du serveur, tel qu'il est contrôlé
<CliCer> <DN> <IssDN>	Certificat du client SSL DN en clair du client, tel qu'il est contrôlé DN en clair de l'émetteur du certificat du client, tel qu'il est contrôlé

Informations du fichier SYSDNCTL

Le fichier SYSDNCTL fournit une trace du traitement appliqué à partir du fichier DN sur les certificats traités durant le handshake.

L'exemple ci-dessous montre le contrôle du DN et de l'ISSDN du partenaire distant, à partir du fichier DNCFG06 suivant :

```
   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>
-------------------------------------------------------------------------------
```

Le DN est : CN=AN8CERT,OU=TEST,C=SSL
L'ISSDN est : CN=IssCERT,OU=UNIT,C=SSL

Dans la trace, les enregistrements lus sont précédés du nom du fichier de contrôle, DNCFG06 dans l'exemple.

```
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
```

Le certificat est rejeté parceque la chaine 'UNIT' diffère de la chaine 'Tes' attendue.
En modifiant la ligne 18 du fichier DNCFG06, '*OU=Tes*' changé en '*OU=UNIT*', l'exemple montre un cas de contrôle satisfait :

```
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
```

Gestion des certificats avec RACF

La gestion des certificats est assurée de façon externe à Connect:Express. Si le certificat à utiliser n'est pas le certificat défini par défaut pour l'ANM dans la base des certificats, il peut être indiqué par le paramètre « label de certificat » indiqué dans la configuration du moniteur (SSLCER). Ce label peut être en majuscules et minuscules et faire au maximum 34 caractères.

Le certificat local (celui défini par défaut ou tout autre) et les certificats des autorités impliquées dans les échanges prévus doivent être connectés au keyring de l'ANM. Ils ne sont pas eux mêmes nécessairement associés à l'ANM (paramètre ID de la commande RACDCERT). Il n'est pas nécessiare de connecter les certificats des partenaires au keyring .

Remarque : dans le cas de certificats autosignés, les certificats local et distant doivent être présents dans le keyring.

Dans cette version béta, un seul certificat est associé au moniteur : il peut être précisé dans le fichier SYSIN.

SSLCER=Label du serveur Paris 2 < taille maximum = 34 caractères

Pour les premiers tests, on peut utiliser des certificats « auto signés » ou créer sa propre autorité et créer des certificats authentifiés par cette autorité. Dans les conditions normales, pour être signé, un certificat doit faire l'objet d'une requête de certificat, soumise à une autorité. L'autorité renvoie le certificat authentifié qu'il faut alors intégrer dans la base.

Vous pouvez créer un certificat localement ou intégrer un certificat dans la base à partir d'un fichier reçu .
La commande TSO RACDCERT et l'interface ISPF de RACF permettent d'effectuer l'ensemble des opérations.

- ✓ Création d'un Keyring
- ✓ Création d'un certificat
  - o Certificat autosigné
  - o Certificat de type autorité
  - o Certificat de type utilisateur
- ✓ Requête de certificat

- ✓ Extraction d'un certificat dans un fichier
- ✓ Intégration d'un certificat dans la base, à partir d'un fichier
- ✓ Connexion d'un certificat à un Keyring

Commande RACDCERT

Les exemples ci-dessous illustrent la gestion des certificats: le paramètre '*withlabel'* est l'information utilisée dans la configuration de connect:Express (SSLCER).

Certificat auto signé

Un certificat autosigné se suffit à lui-même, mais certains systèmes ne permettent pas de l'utiliser. Ce certificat doit être connecté au keyring de l'ANM.

Cette opération peut être faite par l'interface ISPF.

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

Certificat de type autorité

Un certificat de type autorité permet de signer des certificats de type utiilisateur. Ce certificat doit être connecté au keyring de l'ANM si les certificats utilisés au cours des tests sont signés par lui.

```
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))
```

Connexion d'un certificat au keyring

Cette opération peut être faite par l'interface ISPF.

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

Exportation d'un certificat dans un fichier

Cette opération permet de transmettre le certificat à un partenaire.
Cette opération peut être faite par l'interface ISPF.

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

Menus ISPF

Mis part la création d'un certificat de type autorité, toutes les opérations peuvent se faire par l'interface SPF.

```
           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.
```

Voici un enchainement type d'opérations :

1. Création d'un keyring : option 6.
2. Création d'un certificat autosigné : option 1.
3. Création d'un certificat signé par une autorité existante :
4. Identification du certificat : option 1.
5. Création de la requête de certificat : option 2.
6. Signature du certificat par l'autorité : option 1. à nouveau.
7. Connexion du certificat au keyring : option 6.
8. Exportation du certificat : option 3.
9. Importation d'un certificat : option 4.

Codes retour et messages spécifiques

Codes retour spécifiques

Des nouveaux codes TRC ont été ajoutés, et les codes d'erreur SSL sont affichés dans les champs SRC ou NRC selon le contexte.

Codes TRC

TRC=2163 : le handler SSL est inactif.
TRC=2164 : SSL interdit pour ce partenaire
TRC=2165 : SSL obligatoire pour ce partenaire
TRC=A7AS : le handler SSL a fait un abend.
TRC=A7ES : le handler SSL s'est arrêté suite à une erreur détectée par System SSL: analyser le code SRC associé.

Codes retour SSL

Les codes retour SSL sont conformes à la liste donnée plus bas. Ils s'affichent en décimal dans le champ NRC, sous la forme NRC=Sxxxxx, ou dans le champ SRC sous la forme SRC=Sxxx.

L'affichage dans le champ SRC est utilisé pour les rejets d'appels entrants, exclusivement.

Exemples :

Appel entrant rejeté : le client appelle sur le port TCP/IP SSL, mais fait du PeSIT sans SSL :

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

Appel entrant rejeté : le client appelle en X25 avec des donnnées utilisateur attendues pour SSL, mais fait du PeSIT sans SSL :

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

Appel sortant rejeté : erreur pendant le handshake SSL :

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

Messages spécifiques

L'intégration de la fonctionnalité SSL apparaît dans les fichiers SYSMSG et SYSLOG de TOM et le fichier JESMSGLG de l'ANM.

Messages du handler SSL

Les messages du handler SSL, visibles dans le fichier JESMSGLG de l'ANM, signalent des erreurs d'environnement et doivent être signalés au support pour analyse.

```
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
```

Messages de l'ANM

Deux nouveaux messages apparaissent à l'activation et à l'arrêt du handler SSL.

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

Messages de TOM

Les messages du moniteur précisent l'utilisation de SSL : 'PESIT SSL' remplace alors 'PESIT' dans les messages de connexion.

```
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
```

Les messages courants sont utilisés avec des informations spécifiques :

Abend du handler SSL : TRC=A7AS

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

Erreurs et rejets en phase de connexion :

```
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
```

Codes retour SSL

Les codes retour SSL sont associés à des messages en clair affichés dans le fichier SYSPRINT de l'ANM par le tag <GskError>.

Décimal	Hexadéc.	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

Mise en œuvre des traces

Ce paragraphe récapitule l'ensemble des outils de trace à disposition, complété par la trace interne du nouveau handler SSL et la trace des services SSL de z/OS.

Trace sur les échecs de connexions entrantes

La commande /F TOMJOB,TRACE=E permet l'affichage, dans la log du moniteur, d'informations complémentaires dans le cas d'un appel non reconnu.

On peut, une fois que cette trace est active, demander son activation pour un partenaire donné : la trace affiche dans la log du moniteur, des informations complémentaires en cas de rejet d'un appel de ce partenaire.

Dans certains cas, cette trace est le seul moyen d'obtenir l'adresse et les données X25.

Trace protocolaire ATM

L'ATM produit à la demande des traces protocolaires complètes. Ces traces sont indépendantes de l'utilisation ou non de SSL car elles sont écrites en amont des traitement SSL en émission et en aval des traitements SSL en réception.

Trace SSL

Le handler SSL possède une trace interne, lisible dans le fichier SYSPRINT de l'ANM. Cette trace affiche les données telles qu'elles circulent sur le réseau et telles qu'elles sont traitées par le protocole, ainsi que certaines informations caractéristiques .

Il existe trois niveaux d'informations: environnement, mise en session SSL (handshake) et échange des données. La trace peut être activée au démarrage du moniteur par le paramètre SSLTRC=1 de la SYSIN. Ce paramètre active, par défaut, les niveaux environnement et session.

Le paramètre SSLTRC peut être déiifni dans un profil SSL, de la façon suivante :

SSLTRC = 0	Pas de trace
SSLTRC = 1	Trace session uniquement
SSLTRC = 2	Toutes les dnnées échangées sont incluses dans la trace

Les informations d'environnement ne sont affichées que si SSLTRC=1.

Lecture de la trace ssl

La trace est affichée dans une syntaxe de type XML, chaque champ est défini par un tag. Les informations sont horo datées, et chaque échange est identifié par un couple (numéro de requête, bloc Xrb interne). Les handles SSL sont affichés, un pour l'environnement et un par session.
Dans la phase d'initialisation de l'ANM, les paramètres de configuration fournis sont affichés dans <SslConfig>, puis les valeurs finales après prise en compte par GSKSSL dans < InitializedValues>. A l' initialisation de chaque session SSL, les paramètres fournis sont affichés dans <SslConfig>, puis les informations courantes après le handshake sont affichées dans < SessionValues>. Pendant les échanges, les messages réseau sont définis par les tag <NetIn> et <NetOut>, les échanges protocolaires sont identifiés par les tags <ProtIn> et <ProtOut>. Les données échangées sont affichées en hexadécimal. La séquence normale est <NetIn> <ProtIn> ou <ProtOut> <NetOut>. Le tableau suivant donne la liste des champs fournis dans la trace.

Tag	Description	Type de trace
Fun	1 = Initialisation, 2 = Open client, 3 = Open serveur, 4 = Send, 5 = Receive, 6 = Close, 9 = Terminaison	Environnement
EnvHan	Adresse du bloc de contrôle attribué par SSL	Environnement
Req	Numéro de requête attribué par le moniteur	Session
Xrb	Adresse du bloc de contrôle attribué par l'ANM	Session
Ssl	Adresse de l'extension SSL	Session
SocHan	Adresse du bloc de contrôle attribué par SSL	Session
SslConfig		Environ. et session
Aut	Paramètre SSLAUT de la Sysin (voir AutCli)	Environnement
Tim	Paramètre SSLTIM de la Sysin (voir TimV3)	Environnement
Trc	Paramètre SSLTRC de la Sysin	Environnement
Lev	Protocole(s) SSL/TLS supportés : 10 = TLS V1, 01 = SSL V2, 02 = SSL V3. Les combinaisons possibles de ces trois valeurs sont : 11 = TLS V1 + SSL V2, 12 = TLS V1 + SSL V3, 13 = TLS V1 + SSL V3 + SSL V2, 03 = SSL V3 + SSL V2	Environnement
Cip	Paramètre SSLCIP de la Sysin (voir CipV3)	Environnement
Cer	Paramètre SSLCER de la Sysin (voir Cerlabel)	Environnement
Krn	Paramètre SSLKRN de la Sysin	Environnement
Dbn	Paramètre SSLDBN de la Sysin	Environnement
Dpw	Paramètre SSLDPW de la Sysin	Environnement
Tra	Paramètre SSLTRC du profil	Session
InitializedValues	Valeurs prises en compte incluant les valeurs par défaut	Environnement
CerLabel	Label de certificat local (fourni dans SSLCER ou par défaut)	Environnement
SslV2	Support de SslV2 : ON / OFF (voir SSLLEV)	Environnement
SslV3	Support de SslV3 : ON / OFF (voir SSLLEV)	Environnement
TlsV1	Support de TlsV1 : ON / OFF (voir SSLLEV)	Environnement
CipV2	Cipher suite pour SSL V2	Environnement
CipV3	Cipher suite pour SSL V3 et TLS V1 (voir SSLCIP)	Environnement
TimV2	Durée de vie de SessionID pour SSL V2	Environnement
TimV3	Durée de vie de SessionID pour SSL V3 (voir SSLTIM)	Environnement
AutCli	Authentification client : FULL/PASSTHRU (voir SSLAUT)	Environnement
SessionValues		Session
SessionID	Identifiant attribué par SSL et dont la durée de vie est limitée à TimV2 ou TimV3 suivant la version Ssl.	Session
SecType	Type de sécurité : SSLV2 – SSLV3 – TLSV1	Session
SessType	Type de session : CLIENT, SERVER, SERVER+AUTCLI	Session
Cfg	Numéro de profil SSL. <Cfg>00</Cfg> = le profil défini en SYSIN.	Session
Cipher	Niveau de sécurité, une des valeurs de la cipher suite	Session
CliCer	Certificat du client	Session
Cfg	Numéro de profil SSL. <Cfg>00</Cfg> = le profil défini en SYSIN.	Session
DnCtl	Nom du fichier de contrôle de DN.	Session

GskError	Message en clair associé à une erreur SSL	Session
Rc1	Code retour de l'ANM – premier champ du NRC	Session
Rc2	Code retour de l'ANM – deuxième champ du NRC	Session
SocSend	Fonction d'appel aux services de l'ANM, en émission.	Session et données
SocRecv	Fonction d'appel aux services de l'ANM, en réception.	Session et données
Dad	Adresse des données échangées entre l'ANM et SSL	Session et données
Dln	Longueur des données échangées entre l'ANM et SSL	Session et données
NetIn	Message réseau reçu (transmis à SSL)	Session et données
NetOut	Message réseau émis (par SSL)	Session et données
ProtIn	Message Protocolaire reçu (par SSL)	Données
ProtOut	Message réseau émis (transmis à SSL)	Données

Trace gskssl

Pour obtenir une trace des services SSL de z/OS, vous devez activer la carte ENVIRON DD dans le JCL de l'ANM. Cette carte doit pointer sur un fichier de configuration du langage environment, dans lequel les paramètres GSK_TRACE et GSK_TRACE_FILE indiquent quel niveau de trace est demandé et dans quel fichier HFS cette trace doit être écrite.

JCL de l'ANM:

```
//*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
```

Paramètres d'environnement CEE :

```
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 ****************************
```

La procédure ANM doit être autorisée à écrire dans le fichier HFS indiqué, **`/u/cexpress/gsktrc_%`** dans l' exemple ci dessus. Pour celà il est nécessaire de lui attribuer un segment oMVS et de lui donner les droits d'écriture dans un répertoire. La syntaxe du nom de fichier permet d'identifier le fichier trace avec un numéro de procédure qui remplace le caractère « % » : dans l'exemple le fichier sera de la forme /u/cexpress/gsktrc_33685540.

Le fichier trace obtenu, après arrêt de l'ANM, doit être formatté par la commande oMVS gsktrace :

```
Gsktrace /u/cexpress/gsktrc_33685540 > /u/cexpress/gsktrc_33685540_formattée
```

Ce fichier peut ensuite être analysé sous éditeur par la commande ISPF oEDIT.