Connect:Express® OS/390

Option SSL

Sterling Commerce
An IBM Company

Connect:Express OS/390 Option SSL
Version 4.2.0
Deuxième 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.

TABLE DES MATIERES

Activation de l’option SSL

Ce document vient en complément de la documentation de Connect:Express OS/390 version 4.2.0. 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.

```
TOM4200-------------- 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
```

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, il est nécessaire de 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.

L’ANM doit êre associé à un keyring RACF, auquel seront connectés le certificat de Connect :Express et ceux des autorités de certification (CA) reconnues.

Configuration du moniteur

Le paramétrage du moniteur 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 générales. 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.
- ✓ Dans cette version le moniteur est associé à un certificat unique : il représente une seule entité.

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	'N' est la valeur par défaut. 'Y' doit être associé avec les paramètres de configuration SSL de type 'obligatoire' et au moins un paramètre de type 'attendu' .	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 local 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	'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
SSLLEV	2 c. Num.	Niveau de protocole SSL minimum supporté. Les trois valeurs possibles sont 20, 30 et 31. Par défaut la valeur est 30 : ceci signifie que le serveur traitera les protocoles SSL V3 et TLS V1. Pour se limiter à TLS V1 on peut indiquer 31. Pour supporter aussi SSL V2 on peut indiquer 20.	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 : 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

La liste ci-dessous résume les valeurs supportées par z/OS, pour SSL V3 et 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

Pour SSL V2, la liste est toujours prise égale à la liste par défaut de z/OS, soit : 713642

La liste ci-dessous résume les valeurs supportées par z/OS, pour SSL V2 :

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)

Nouvelles commandes

Le handler SSL peut être activé et désactivé : 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

```
TOM4200     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 de l'ANM sont reçus par TOM dans sa SYSIN et transmis à L'ANM pendant la phase d'initialisation. La configuration de l'ANM consiste donc à adapter le JCL de la procédure.

Configuration SSL

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

Procédure JCL

Il faut ajouter la bibliothèque LOADSSL en STEPLIB du JCL de la procédure.

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.

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

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*.

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. 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). Les certificats des partenaires n'ont pas à être connectés 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.

Un certificat peut être créé localement ou intégré 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
- ✓ Certificat autosigné
- ✓ Certificat de type autorité
- ✓ 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.

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.

Nouveaux 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
```

Nouveaux messages

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 oeuvre d'un transfert PeSIT SSL

Une fois que la configuration du moniteur est effectuée, le handler SSL s'initialise, le handler TCP/IP active les listeners suivant le paramétrage : 1 listener pour PeSIT, 1 listener pour PeSIT SSL et de la même façon 1 listener pour Odette et un listener pour Odette SSL.

En mode serveur

Les appels entrants TCP/IP sont traités par les listeners: si l'appel est accepté par un serveur SSL il sera traité sous SSL. Les partenaires doivent donc appeler le port correspondant au protocole souhaité.
Les appels par X25 sont pris en charge par le handler X25 qui détermine si la session doit être placée sous SSL, en fonction des données utilisateur ou de la sous adresse, suivant la configuration du moniteur.

En mode serveur, une fois l'appel traité, avec ou sans SSL, le moniteur contrôle le champ T-SECURITE SSL du partenaire. L'appel peut être rejeté si ce champ n'est pas conforme au type d'appel. Il est possible d'activer/désactiver la trace SSL session, comme c'est indiqué plus bas.

En mode client

Dans cette version, le moniteur ne représente qu'une seule entité, représentée par le certificat unique déclaré dans sa SYSIN. Pour déclencher un transfert SSL vers un partenaire, il suffit de déclarer un numéro de table de sécurité dans la définition du partenaire : en fonction de la valeur de ce champ la session SSL sera tracée ou non : 01 = SSLTRC par défaut, 02 = Trace inactive quelque soit SSLTRC, 03 = Trace active quelque soit SSLTRC.

Pour appeler un Connect:Express il faut indiquer le port TC/IP prévu dans la configuration de l'autre Connect:Express ou les données utilisateur dans le cas d'une session X25.

```
TOM4200     PARTENAIRE DE TOM8 A MODIFIER   (2/4)
OPTION ===>                          -ENTREE- : SUITE, -PF3- : ANNULER  X : EXIT
TYPE: COMPAT.,PESIT-E
MOD: PSR0008  06/03/24 01:19:35        8
NOM SYMBOLIQUE        : GFIPSR8S           DPCSID ALIAS         -> GFIPSR4S
MOT DE PASSE TOM     => PSR                DPCPSW ALIAS         -> -
ETAT INITIALISATION  -> E                  CLASSE APM RECEPTION -> A
UTILISATEUR RACF     -> TOMPSR             GROUPE RACF          -> -

NATURE PARTENAIRE    => O
PROT.SESSION NUM.-T. => 5   => 2           T-SECURITE SSL       -> 01
REESSAI AUTOMATIQUE  -> OUI

TYPES DE LIAISON     => M   => IX          PARTENAIRE ADJACENT   -> -
EFF. TOT.-ENT.-SOR.  => 256 -> 128 -> 128  T-REGULATION FLUX SLD -> -

SNA: LUNAME => -          LOGMODE   -> -        LOGDATA  -> -          DISC -> N
X25: MCHMSC -> A     ADR.DIST. => 1932674506054    ADR.LOC. -> -
     GFA    -> -     UDF        -> ABCD            TAXATION -> 1
     SERVICES COMPLEMENTAIRES  -> -
IP : ADRES. => -                PORT => 20009 FTP PASV => - PROFIL -> -
     HOTE   -> CSG.STERCOMM.COM                 'S': - DROITS -> -
NOTE -> TRANSFERTS SSL
```

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. Par défaut, ce paramètre active tous les niveaux.
Le paramètre T-SECURITE SSL d'un partenaire permet de désactiver la trace des données si SSLTRC=1, ou d'activer la race pour le partenaire si SSLTRC=0.

Le paramètre au niveau du partenaire est utilisé de la façon suivante :

T-SECURITE SSL = 01	La trace est prise égale par défaut à la trace environnement SSLTRC.
T-SECURITE SSL = 02	La trace données est inactive, mais la trace session est active quelle que soit l'option SSLTRC.
T-SECURITE SSL = 03	Les traces session et données sont actives quelle que soit l'option SSLTRC.

Les informations d'environnement ne sont affichées que si SSLTRC=1.
Les mises en session en mode serveur ne sont affichées que si SSLTRC=1.
On peut limiter la taille de la trace, en mode client et serveur, par le paramètre T-SECURITE SSL = 02.

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	Paramètre SSLLEV de la Sysin (voir SslV2, SslV3 et TlsV1)	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 T-SECURITE-SSL du partenaire	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
Cipher	Niveau de sécurité, une des valeurs de la cipher suite	Session
CliCer	Certificat du client	Session
SrvCer	Certificat du serveur	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.