Connect:Express® Windows

Guide de paramétrage SSL

Version 3.0.6.002

Sterling Commerce
An IBM Company

Connect:Express
Guide de paramétrage SSL

Version 3.0.6.002
Première édition

Préface

Ce document décrit la mise en œuvre de transferts de fichiers sécurisés par SSL sur TCP/IP.

Le Chapitre 1 présente l'installation des certificats et clés utilisés par Connect:Express.
Le Chapitre 2 décrit le paramétrage de Connect:Express pour effectuer des transferts SSL.

Introduction

Pour effectuer des transferts de fichiers sur SSL et TCP/IP, Connect:Express Windows s'appuie sur les api SSPI (Security service provider interface), SChannel (Secure channel) et CryptoApi[1] de Microsoft Windows.

Ce document ne décrit ni les protocoles SSL et TLS, ni les différentes spécifications PKI ni les différents standards cryptographiques.
Le lecteur pourra consulter entre autre :

- RFC2246. The TLS protocol version 1.0
- SSL2 Protocol Specification (http://home.netscape.com)

La fonctionnalité suivante est implémentée dans cette version :

- Contrôle de l'autorisation des partenaires PeSIT distants en fonction du DN du certificat qu'ils présentent.

Installation

L'installation de cette version de Connect:Express est décrite dans « *Guide d'installation et des utilitaires* ».

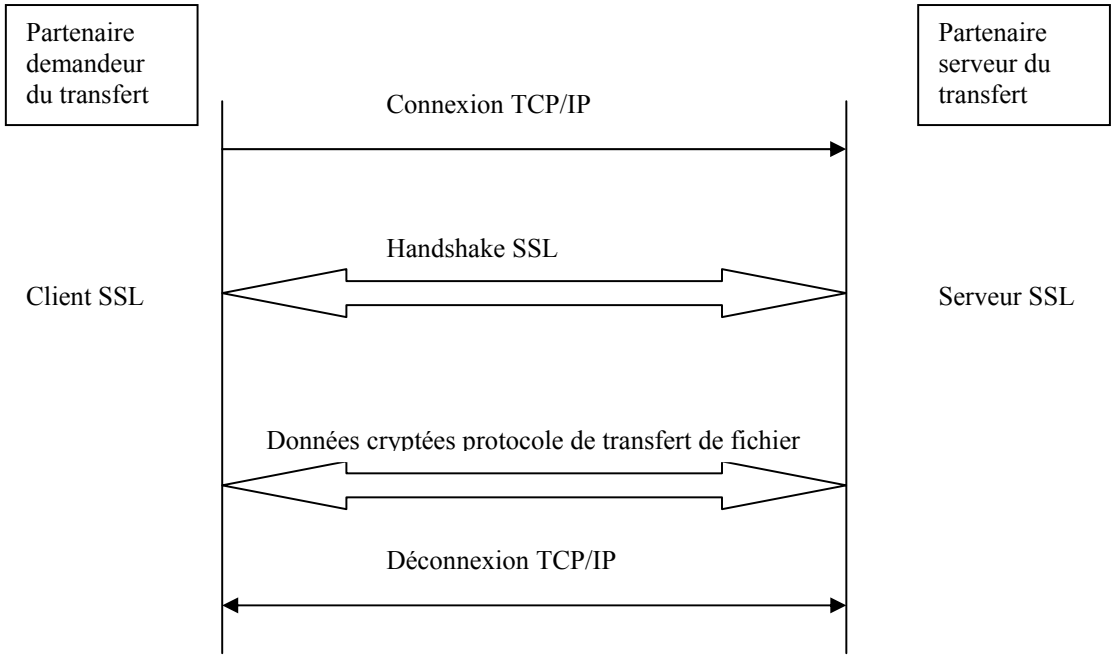
Le programme d'installation permet de mettre à jour une version antérieure sans pré-requis particuliers.
Il est néanmoins nécessaire d'obtenir de Sterling Commerce une clé d'autorisation logicielle spécifique afin de pouvoir disposer de l'option SSL de Connect:Express. Il est nécessaire dans ce cas de remplacer l'ancienne clé dans le fichier tomnt.ini de configuration de Connect:Express[2].

[1] DLLs: secur32.dll et crypt32.dll dans le répertoire c:\WINDOWS\system32

[2] Mettre à jour avec notepad les propriétés ALIAS et NUMERO du fichier tomnt.ini

Transfert de fichier sur SSL

La figure suivante illustre le déroulement d'un transfert de fichier sur SSL entre 2 partenaires :



Chapitre1

Ce chapitre décrit l'importation des certificats dans les magasins de certificats de Windows.
Les certificats importés seront utilisés par Connect:Express pour effectuer les transferts SSL.

En mode client ou serveur avec authentification du client, Connect:Express doit disposer des éléments suivants :

- Un certificat personnel et la clé privée associée.
- Le(s) certificat(s) de l'autorité de certification (CA) ayant signé le certificat personnel.
- Le certificat racine de l'autorité de certification ayant signé le certificat du partenaire distant.

En mode serveur sans authentification du client, Connect:Express doit disposer des éléments suivants :

- Un certificat personnel et la clé privée.
- Les certificats de l'autorité de certification ayant signé le certificat personnel

En mode client sans authentification du client, Connect:Express doit disposer des éléments suivants :

- Le certificat racine de l'autorité de certification ayant signé le certificat du partenaire distant.

Connect:Express permet de gérer les transferts SSL en utilisant plusieurs certificats personnels distincts suivant les partenaires auxquels on s'adresse.

Importation des certificats et des clés

Obtention d'un certificat personnel

L'obtention d'un certificat personnel se déroule de la manière suivante :

- Création d'une demande de certificat (CSR : Certificate Signing Request) associée à une clé privée.
- Envoi de la CSR à une autorité de certification (CA).
- Réception en retour du certificat.

Consultez la documentation de votre autorité de certification, afin d'avoir une description plus détaillée de ces différentes étapes.
Divers outils permettent la génération d'une CSR et de la clé privée associée (keytool, openssl). Certains sont plus spécifiquement associés à des serveurs Web (iKeyman de IBM Websphere MQ, Internet services Manager de IIS, …).
Ces utilitaires permettent également l'exportation et la mise sous différents formats des certificats et des clés.

Format des certificats personnels à importer

Un certificat personnel à importer doit être disponible sous forme d'un fichier au format PKCS#12, qui contient :

- Le certificat de l'utilisateur
- Sa clé privée,

- Eventuellement, le ou les certificats du CA

Le fichier pkcs#12 est protégé par un mot de passe.

Note :
Dans le cas où le CA est hiérarchisé, le certificat de l'utilisateur peut avoir été signé par un CA secondaire, et le fichier PKCS#12 peut inclure tous les certificats de CA en remontant la chaîne de certification jusqu'au certificat CA racine. Si ce n'est le cas, il sera nécessaire d'importer par ailleurs manuellement tous les certificats manquants de la chaîne de certification.

Magasins de certificats de Windows

Les certificats sont importés dans un des magasins système logiques de certificats de Windows à l'aide de la console de gestion Microsoft (Microsoft management console).
Les magasins systèmes de certificats sont organisés suivant une hiérarchie de répertoires dans lesquels sont placés par importation les différents certificats :

Les répertoires suivants concernent Connect:Express :

- Certificats de l'ordinateur local : Contient des certificats disponibles pour tous les utilisateurs et tous les services de l'ordinateur local.
- Certificats du service Connect:Express : Contient les certificats du service Connect:Express lorsque Connect:Express a été enregistré en tant que service.
- Certificats de l'utilisateur actuel : Contient les certificats de l'utilisateur actuellement connecté.

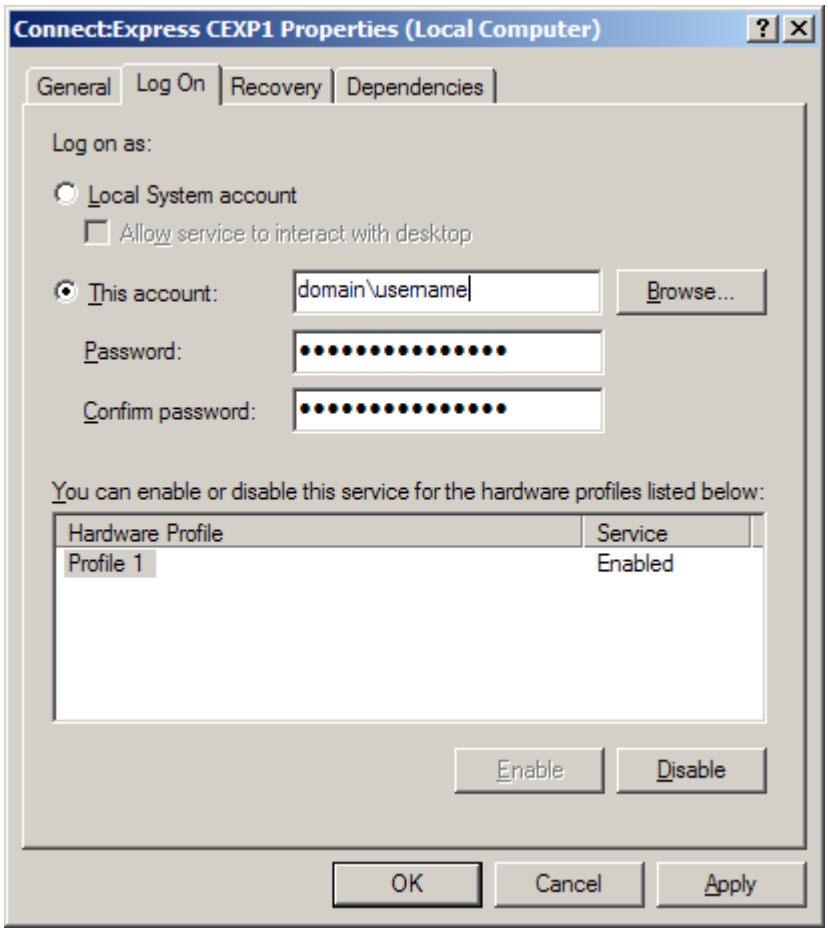
Chaque répertoire principal contient notamment les répertoires suivants :

- Personnels : Contient les certificats personnels. Si elle est présente lors de l'importation, la clé privée associée au certificat est également stockée.
- Autorités de certification racines de confiance : Contient les certificats des CA

Suivant l'emplacement des certificats dans les différents répertoires, Connect:Express peut être utilisé ou pas s'il est démarré depuis le bureau ou comme service Windows.

Il y a deux possibilités d'installation de Connect:Express en service Windows :
- Avec le *Log On* « compte système local », qui n'est pas associé à un utilisateur particulier.
- Avec le *Log On* d'un utilisateur donné.

Seule l'installation du service pour le compte d'un utilisateur particulier permet à Connect:Express d'accéder par leur UNC a des fichiers situés sur disques réseau. Dans ce cas les droits d'accès sont ceux de l'utilisateur concerné.
Le programme d'installation du service Connect:Express (tom_srv) installe par défaut celui-ci avec le *Log On* « compte système local ». Pour assigner le service Connect:Express à un utilisateur particulier, il suffit de modifier les propriétés du service à l'aide du panneau de configuration :



Si les certificats personnels sont enregistrés dans le répertoire d'un utilisateur donné, ils pourront être accédés par Connect:Express lorsqu'il est lancé depuis le bureau de l'utilisateur ou en tant que service de l'utilisateur mais pas lorsqu'il est lancé en tant que service « compte système local ».

Le tableau suivant indique les différents répertoires possibles d'importation des certificats. Il indique également les emplacements dans le magasin de certificats correspondant à renseigner dans les définitions de paramètres SSL clients et serveur de Connect:Express (*Voir paramètres des serveurs et des clients SSL pages 24 et 28*).

Certificats personnels	Certificats de CA	Bureau	Service
Ordinateur local / Personnel Emplacement magasin de certificats : SYSTEM_STORE_LOCAL_MACHINE	Ordinateur local / Autorités de certification racines de confiance	Oui	Oui
Service (Connect:Express *Nom-Moniteur*) / Personnel Emplacement magasin de certificats : SYSTEM_STORE_SERVICES	Ordinateur local / Autorités de certification racines de confiance	Oui	Oui
Utilisateur actuel / Personnel Emplacement magasin de certificats : SYSTEM_STORE_LOCAL_USER	Utilisateur actuel / Autorités de certification racines de confiance	Oui	Non[1] / Oui[2]

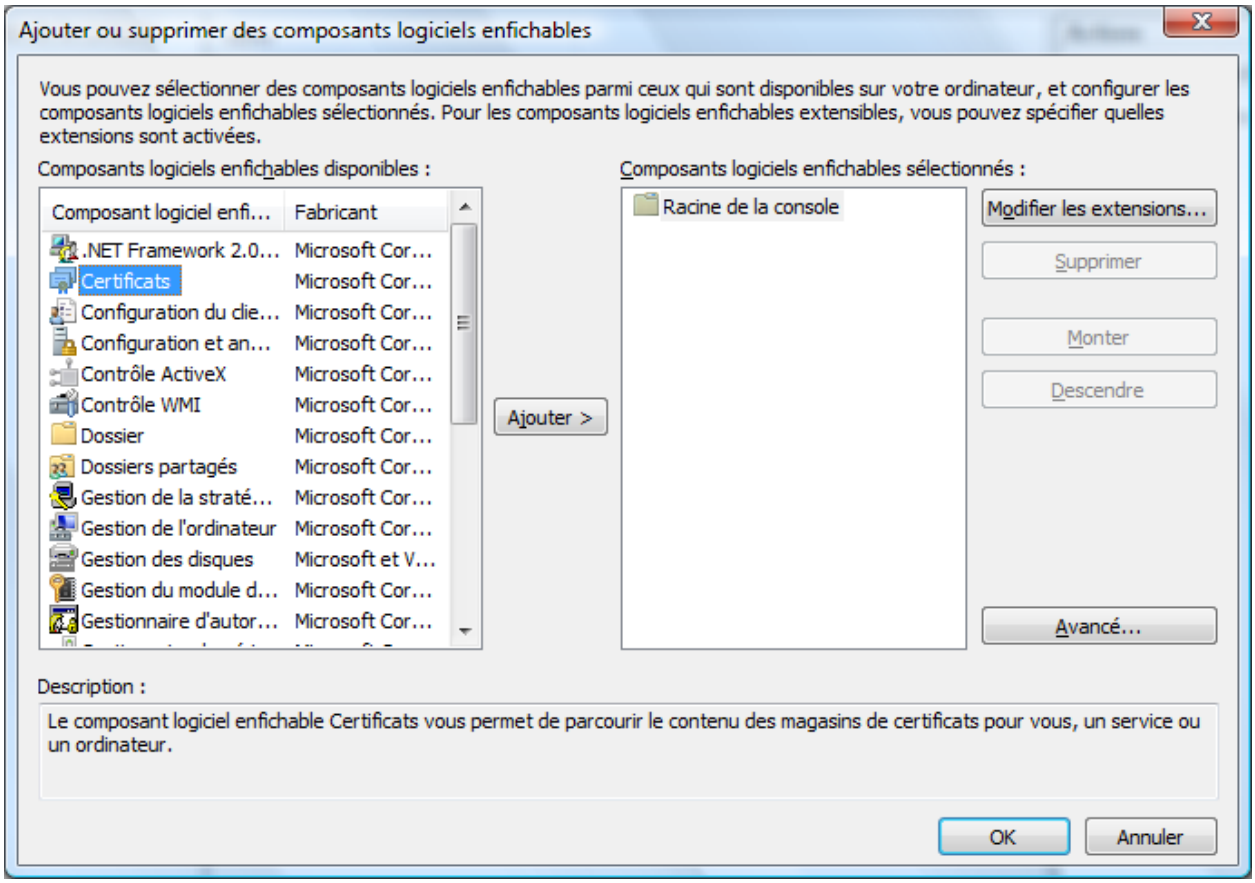
[1] Si le log on du service est « compte système local »

[2] Si le log on du service est « compte de l'utilisateur »

Importation des certificats personnels par la console de gestion.

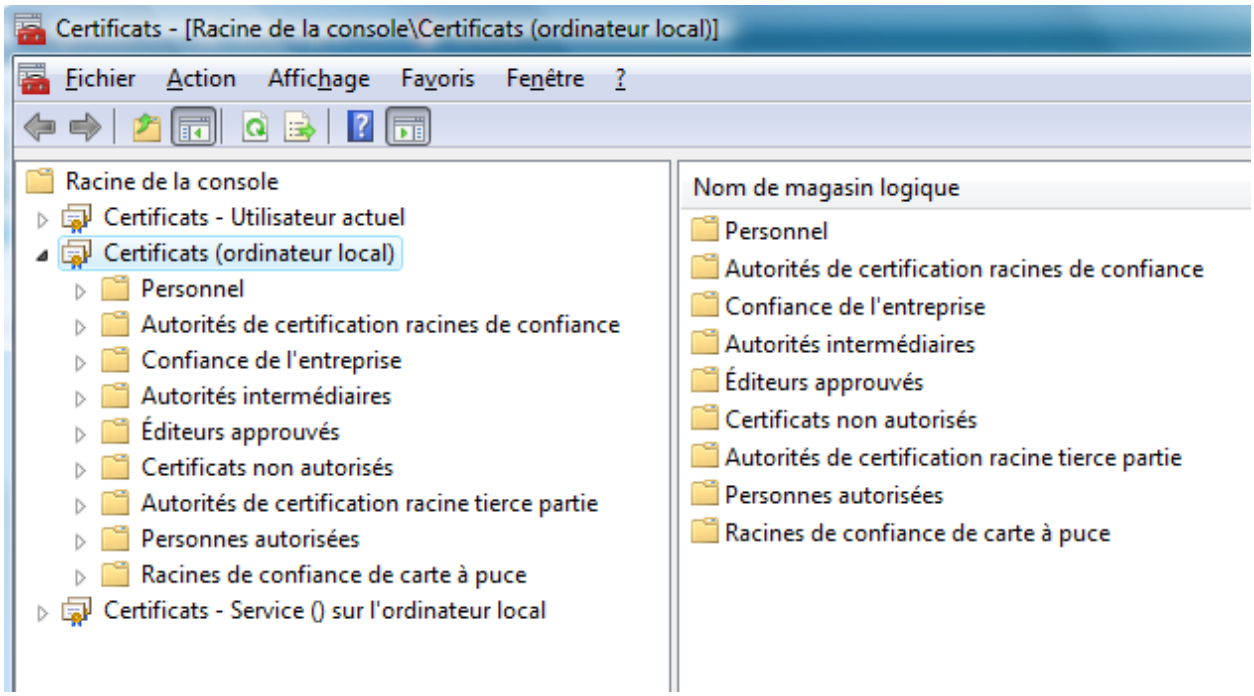
Dans les paragraphes suivants on suppose qu'on importe les certificats dans le magasin de l'ordinateur local.

- ✓ Lancer la console de gestion avec la commande *mmc*.
- ✓ Sélectionner : *Fichier – Ajouter un composant logiciel enfichable …*
- ✓ Dans la boîte de dialogue obtenue, cliquer sur *Ajouter*, et sélectionner *Certificats*.



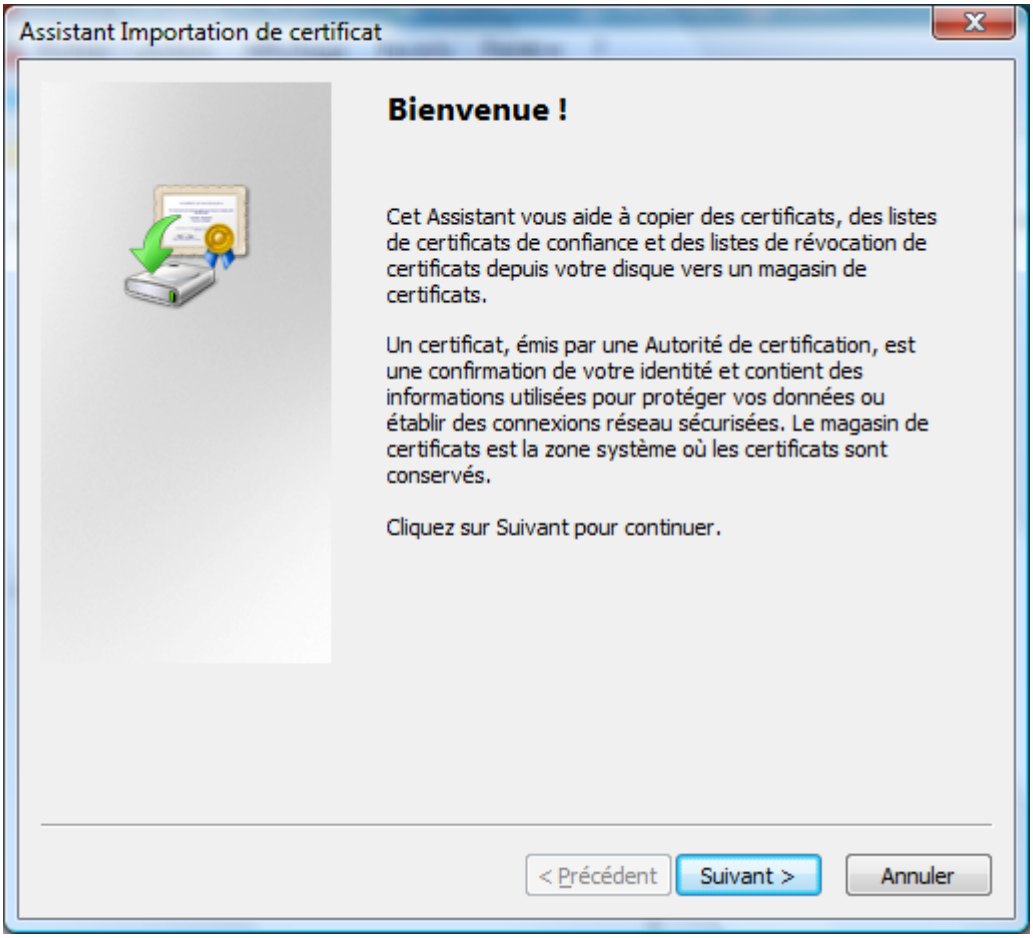
- ✓ Sélectionner : *Certificats*, puis choisir *Le compte de l'ordinateur*.

On obtient la console de gestion des certificats pour l'ordinateur local :

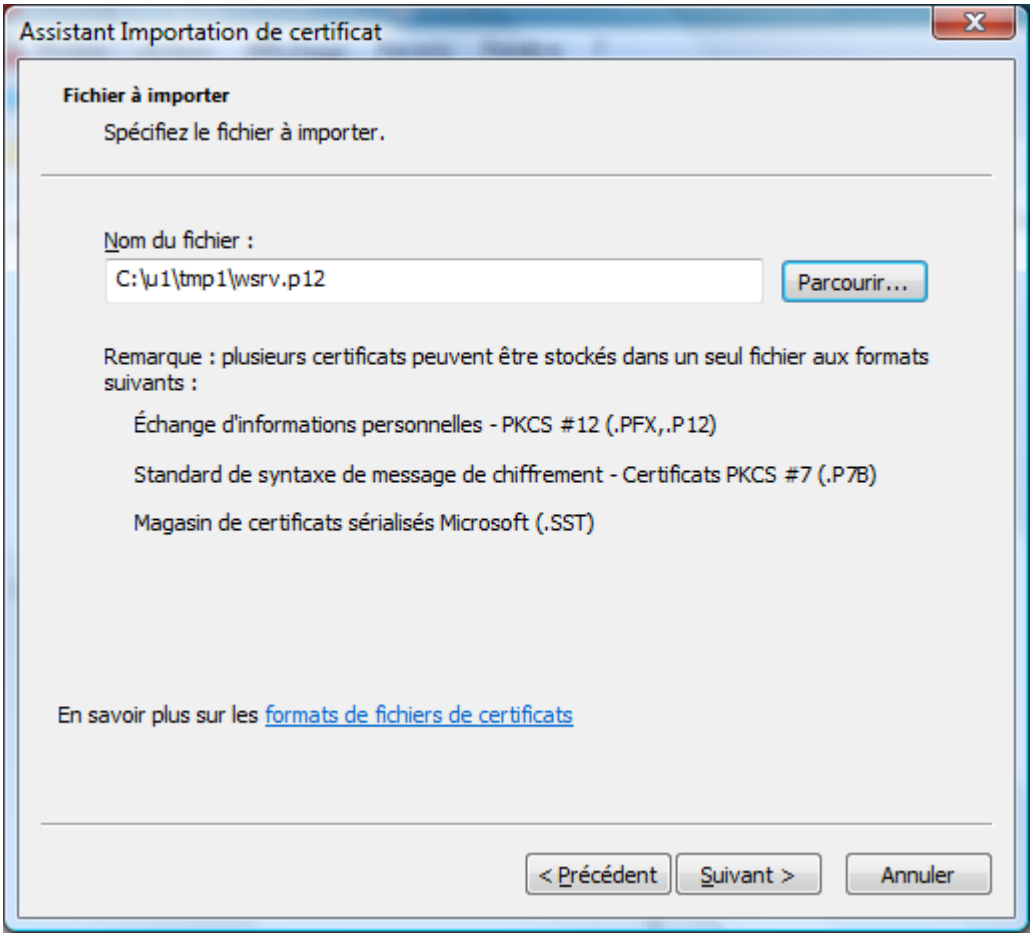


- ✓ Se placer dans le répertoire *Certificats – Ordinateur local \ Personnel \ Certificats*
- ✓ Sélectionner, à partir du menu de la console : *Actions – Toutes les tâches – Importer …*

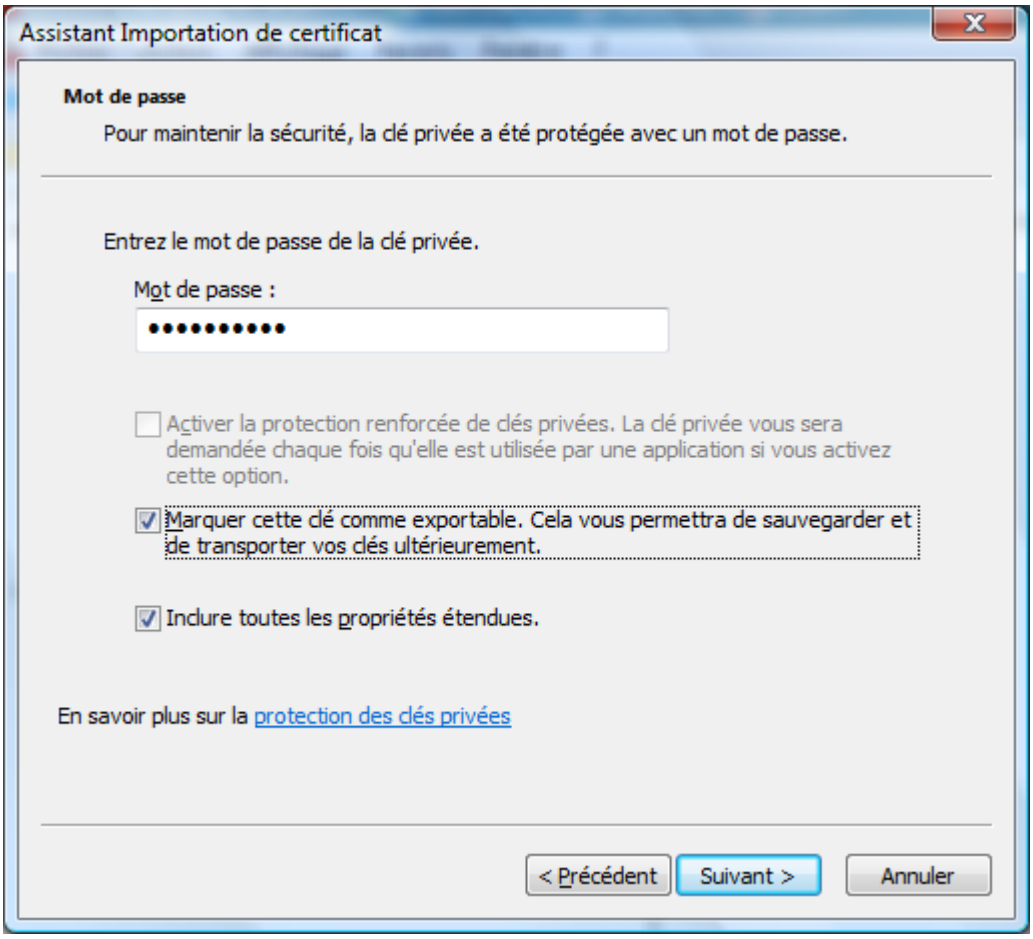
L'assistant d'importation de certificats est lancé :



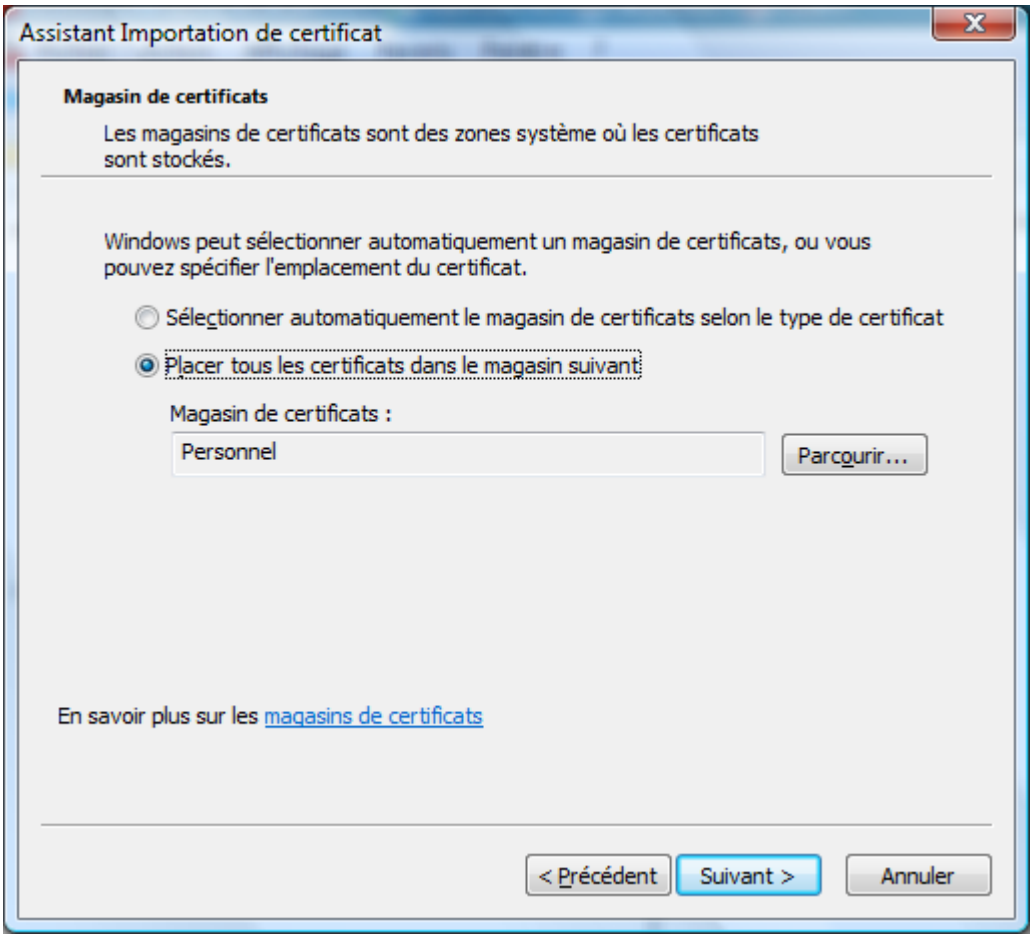
✓ Entrer le nom du fichier pkcs#12 à importer :



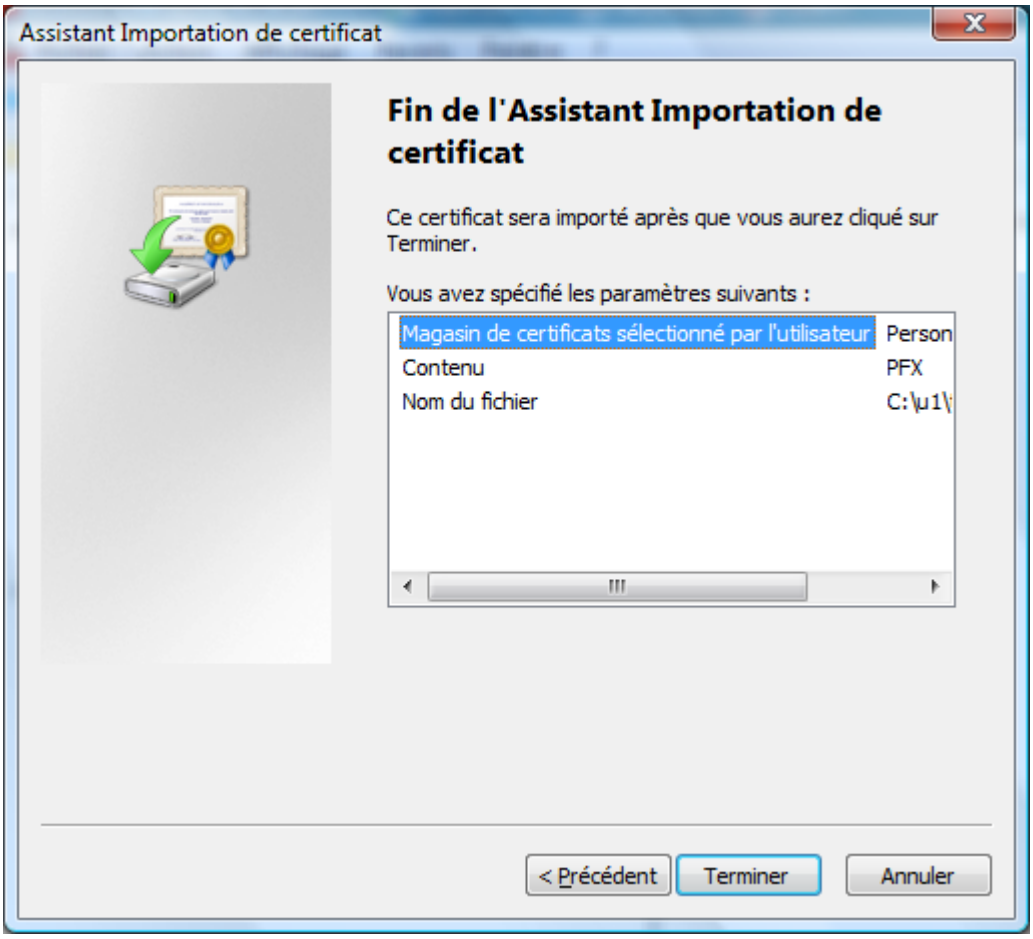
✓ Entrer le mot de passe du fichier et laisser désactivée la protection renforcée des clés privées :



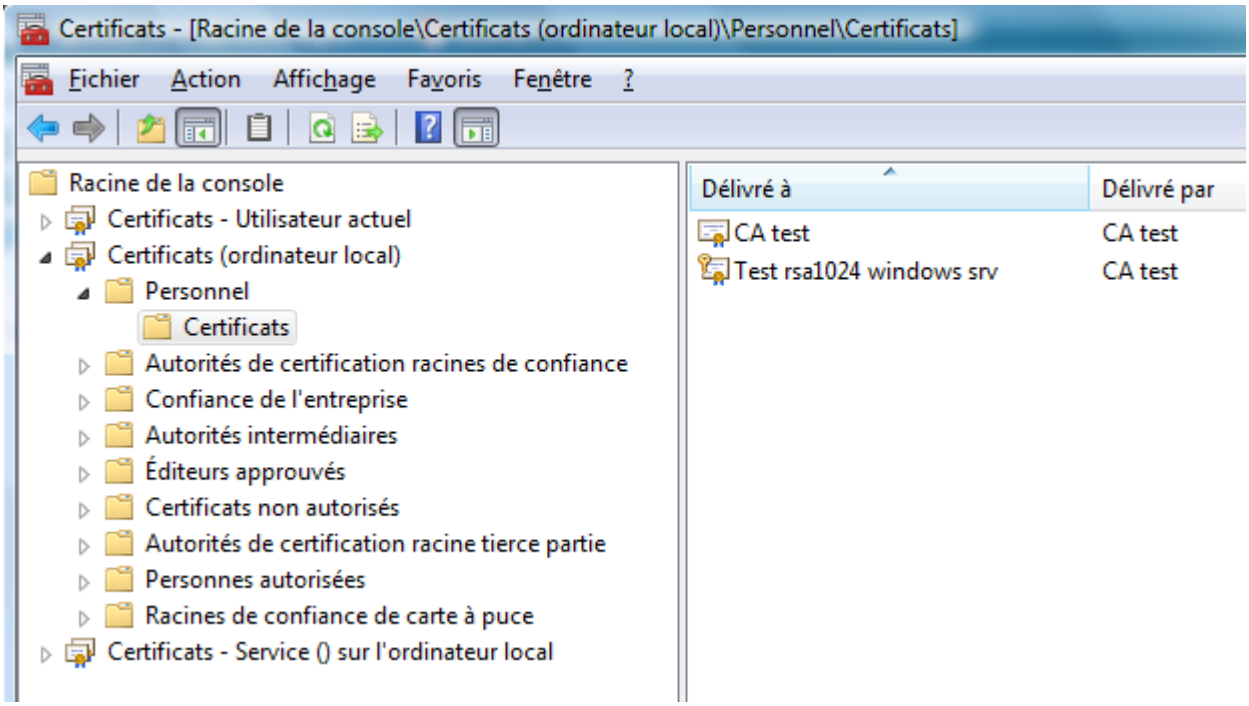
✓ Sélectionner le placement des certificats dans le magasin personnel :



✓ Cliquer *terminer* :



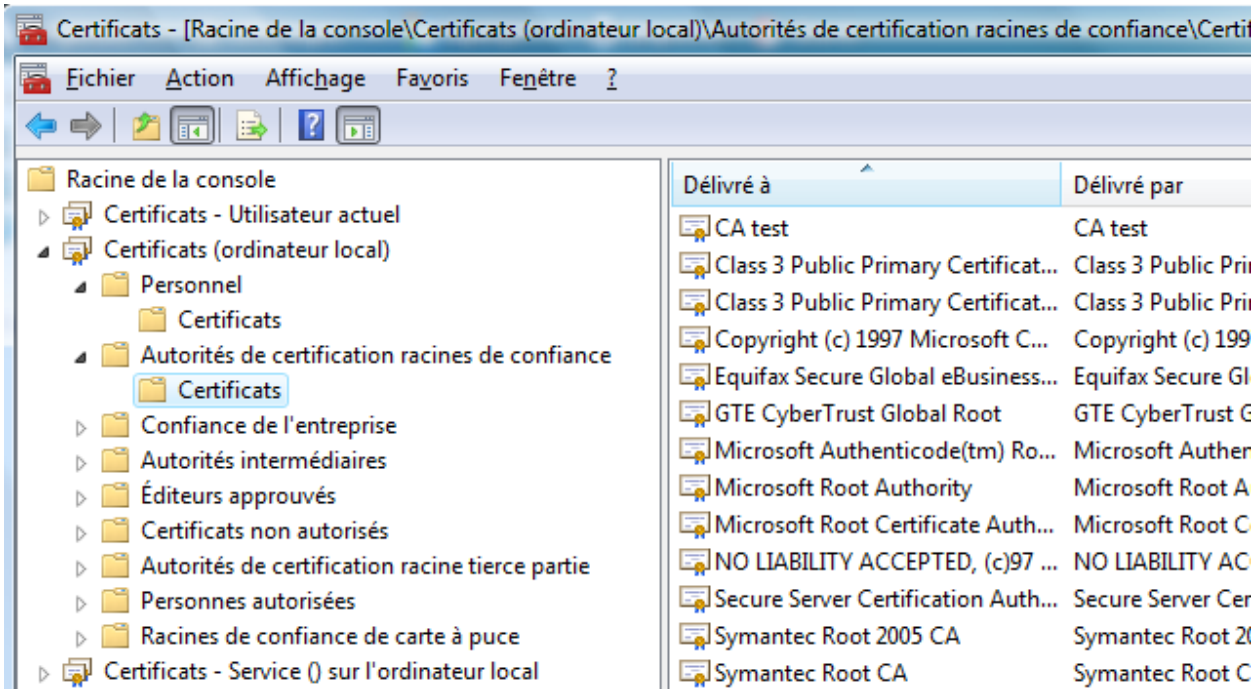
Les certificats apparaissent dans la fenêtre de la console :



Si le certificat de l'autorité de certification n'est pas déjà dans le répertoire « *Autorités de certification racines de confiance* \ *Certificats* », le déplacer de la manière suivante :

- ✓ Sélectionner le certificat, puis *Action – Couper*.
- ✓ Sélectionner le répertoire *Autorités de certification racines de confiance* \ *Certificats*, puis *Action - Coller*.
- ✓ Confirmer l'installation.

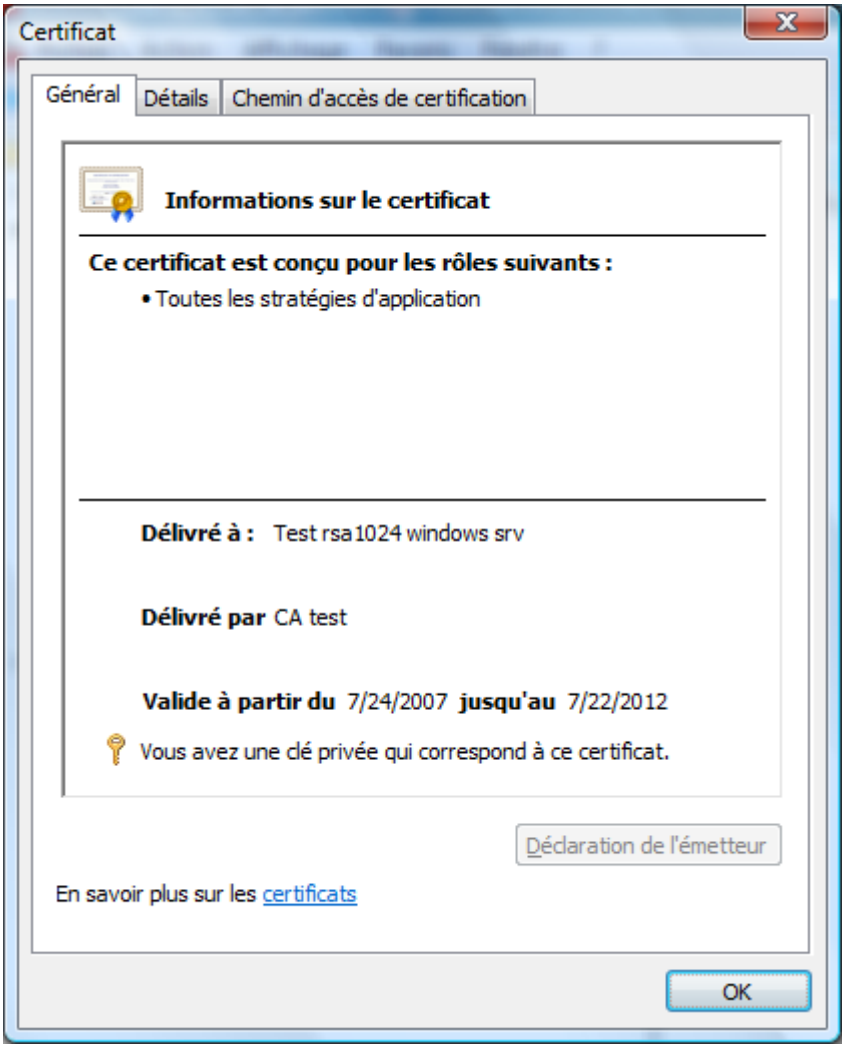
On obtient :



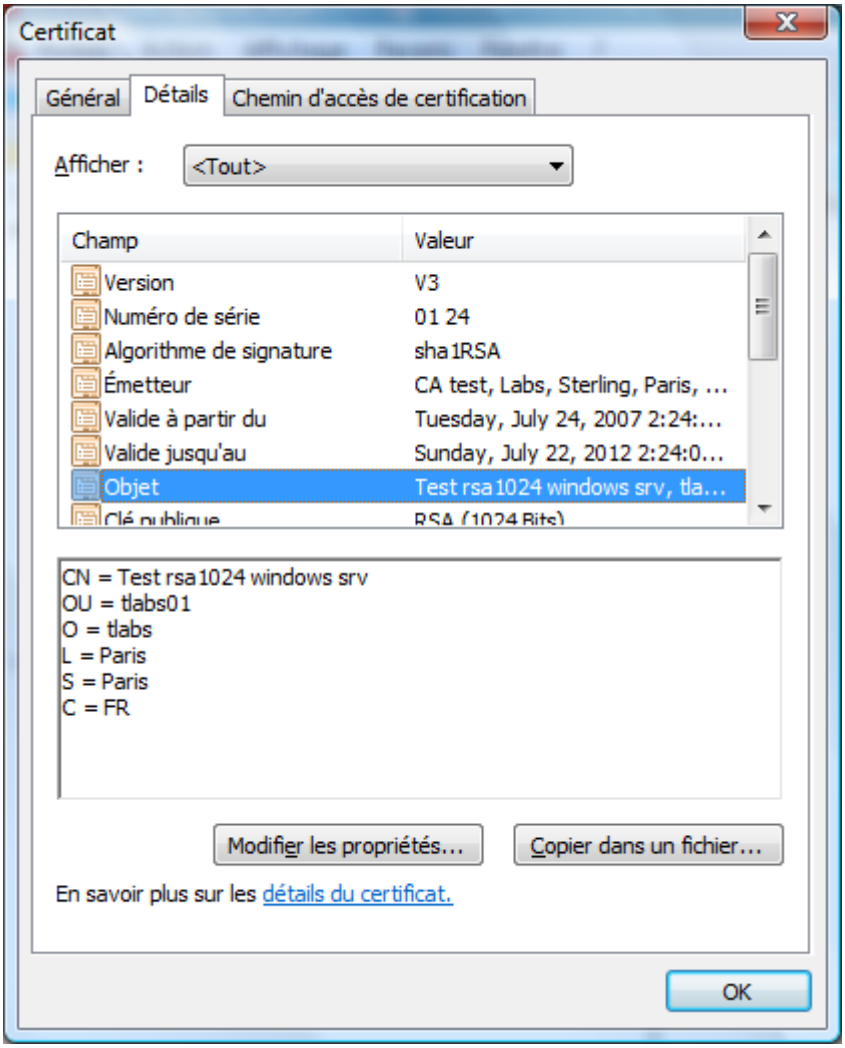
Si le certificat de l'autorité de certification est déjà dans le répertoire *Autorités de certification racines de confiance* \ *Certificats*

- ✓ Le supprimer du répertoire personnel.

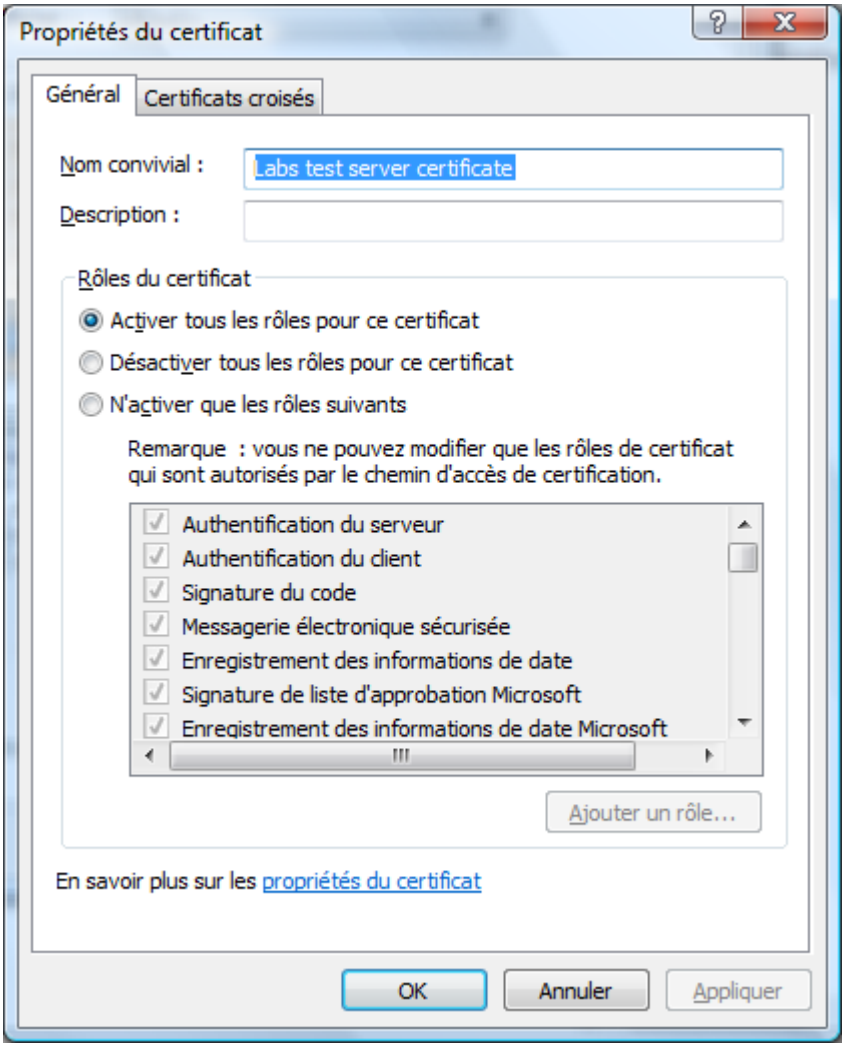
Le détail des certificats importés peut être consulté :



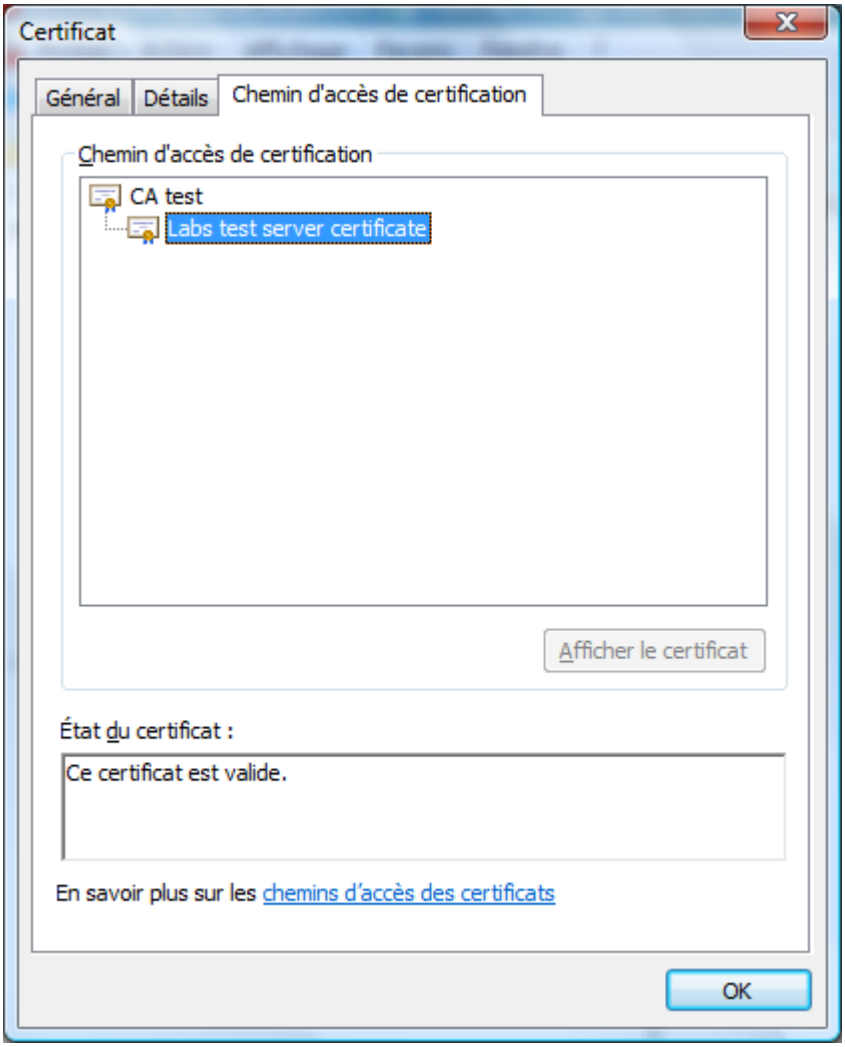
Les éléments *DN objet* et *DN émetteur* seront repris dans la configuration des paramètres SSL de Connect:Express.



Les rôles du certificat ne sont pas contrôlés par Connect:Express :



✓ Vérifier que la chaîne de certification est correcte.



Importation de certificats de CA.

Afin que Connect:Express puisse authentifier un partenaire distant qui présente un certificat au cours du handshake protocolaire SSL, il est nécessaire d'avoir préalablement importé dans le magasin de certificats utilisé, le certificat racine du CA ayant signé directement ou indirectement le certificat du partenaire (Certificat racine de la chaîne de certification du certificat du partenaire).
Les certificats des différents CA du commerce sont présentés sur leurs sites Internet.

Pour importer un certificat de CA :

- ✓ Récupérer dans un fichier texte le certificat du CA (Par exemple par copier-coller à partir du site Web du CA) et effectuer l'importation du certificat à l'aide de **mmc** dans le répertoire *Autorités de certification racines de confiance*.

Chapitre 2

Ce chapitre décrit les divers éléments de paramétrage de Connect:Express afin de pouvoir effectuer des transferts sur SSL.

Paramétrage SSL de Connect:Express.

Connect:Express permet de définir différents ensembles de paramètres indiquant les caractéristiques protocolaires des connexions SSL. Les différents profils recouvrent deux catégories de connexions : Les profils du mode serveur et les profils du mode client.
Plusieurs profils différents peuvent être créés pour chaque catégorie.

Paramétrage des serveurs.

Connect:Express démarre un serveur en écoute sur un port TCP spécifique pour chaque ensemble de connexions entrantes SSL ayant des caractéristiques différentes. Des ensembles de caractéristiques distincts peuvent être rendus nécessaires par l'utilisation de certificats différents ou de suites de chiffrement différentes pour dialoguer avec tel ou tel partenaire.

Chaque serveur peut gérer simultanément plusieurs transferts avec des partenaires différents. Les ports des serveurs SSL sont distincts du port d'écoute du serveur TCP standard de Connect:Express (sans SSL).

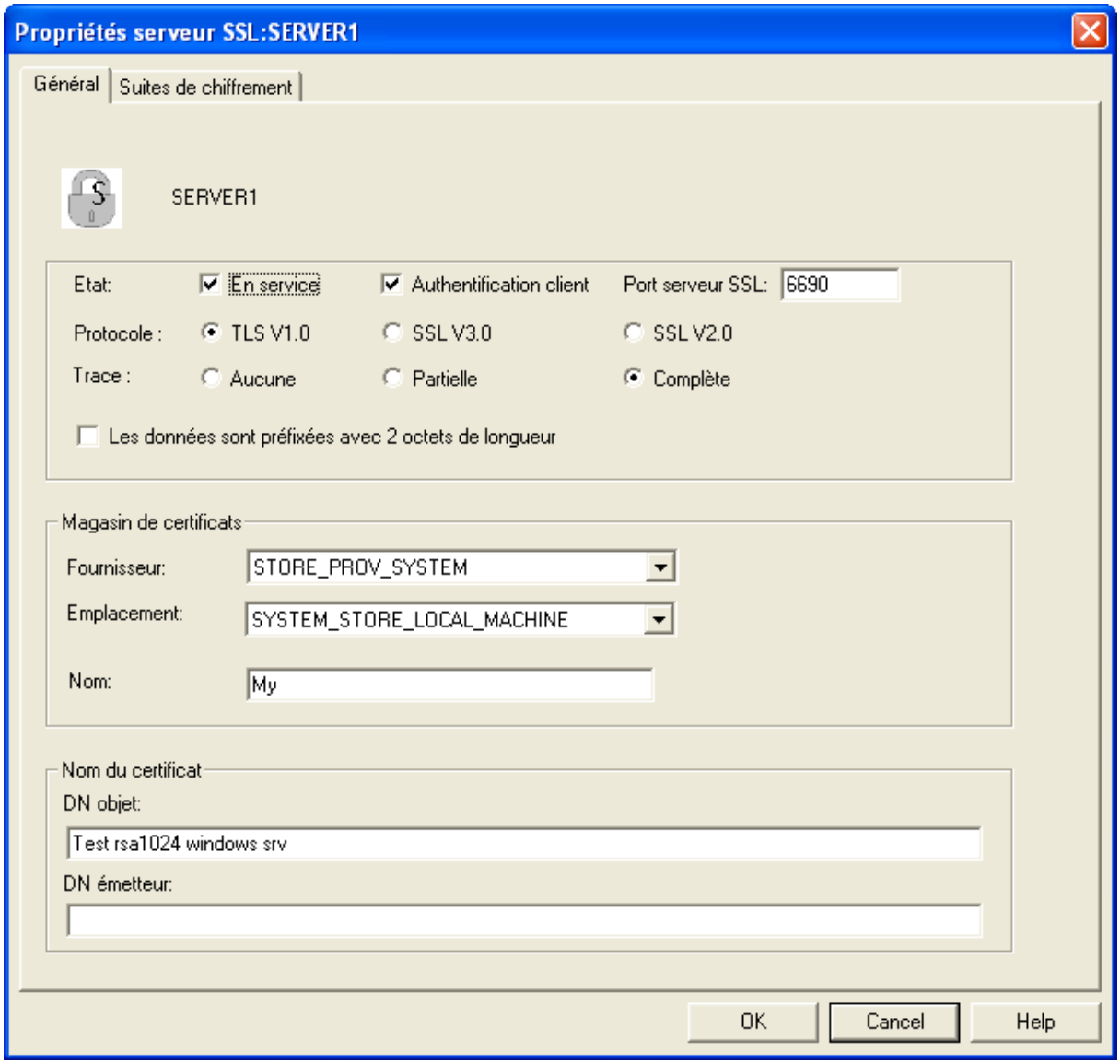
Chaque serveur SSL est identifié par un nom symbolique et est configuré dans le répertoire « **Paramétrage \ Serveurs SSL** » de l'interface graphique de Connect:Express.

Un arrêt - redémarrage du moniteur est nécessaire pour prendre en compte la configuration d'un nouveau serveur.

Un paramètre dans la définition locale de chaque partenaire indique si, pour les connexions entrantes, le partenaire distant doit se connecter via un des serveurs SSL ou via le serveur standard TCP/IP de Connect:Express.

Paramètres d'un serveur SSL.

Les boîtes de dialogue de définition des paramètres se présentent comme suit :



Nom symbolique

Ce champ est formé au maximum de 8 caractères majuscules (A-Z, 0-9).
Il est utilisé pour identifier une définition de serveur SSL.

Etat

Indique l'état du serveur SSL pour le moniteur.
S'il est coché, un serveur SSL est démarré avec ces paramètres; s'il n'est pas coché, le serveur SSL n'est pas démarré.

Authentification client

Indique si le serveur demande aux clients distants de s'authentifier.
Si cette option est cochée et si le client distant ne s'authentifie pas, la connexion échoue.

Port du serveur SSL

Port TCP/IP d'écoute des connexions entrantes pour des transferts utilisant cet ensemble de paramètres SSL.
Un thread serveur SSL est démarré pour chaque définition de serveur SSL.
Un arrêt/redémarrage de Connect:Express est nécessaire pour la prise en compte de nouvelles définitions de serveurs SSL.

Protocole

Indique la version de protocole SSL à utiliser (TLS V1, SSL V3, SSL V3).
Connect:Express ne permettra pas la négociation d'une autre version de protocole que celle fixée ici.

Trace

Indique le niveau de trace pour les transferts.
Les traces sont enregistrées dans le sous répertoire **trace** de Connect:Express.

- **Complète:** Trace complète du handshake, trace complète des échanges de données applicatives.
- **Partielle:** Trace complète du handshake, trace partielle des échanges de données applicatives.

Les données sont préfixées avec 2 octets de longueur

Indique que 2 octets de longueur sont placés avant les données non cryptées.
Ceci peut être nécessaire avec certaines passerelles effectuant des conversions PeSIT sur SSL ↔ PeSIT sans SSL.

Fournisseur du magasin de certificats

Définit le type de fournisseur du magasin de certificats qui fournit les certificats à utiliser.
Actuellement, il y a un seul type de fournisseur disponible: « **STORE_PROV_SYSTEM** » indiquant le magasin logique standard accessible à l'aide de la console de gestion Microsoft **mmc**.

Emplacement dans le magasin

Définit l'emplacement dans le magasin. Trois emplacements sont possibles

- **SYSTEM_STORE_LOCAL_MACHINE** indique que les certificats sont situés dans le répertoire « *Certificat (Ordinateur local)* » du magasin système.
- **SYSTEM_STORE_SERVICES** indique que les certificats sont situés dans le répertoire « *Certificats – Service (Connect:Express Nom-du-moniteur) de l'ordinateur local* » du magasin système.
- **SYSTEM_STORE_CURRENT_USER** indique que les certificats sont situés dans le répertoire « *Certificats – Utilisateur actuel* » du magasin système.

Notes :
Si l'emplacement est SYSTEM_STORE_CURRENT_USER, Connect:Express ne peut être utilisé en service Windows que si le service a pour Log On l'utilisateur concerné (Voir Tableau page 10).
Lorsque l'option SYSTEM_STORE_SERVICES est choisie, les certificats d'autorité racine doivent être placés dans le répertoire « *Certificats (Ordinateur local) / Autorités de certification racines de confiance* ».

Nom dans le magasin

Ce champ indique le sous répertoire où le certificat personnel sera trouvé.
Utiliser « **My** », pour indiquer le répertoire des certificats personnels. mmc doit afficher le certificat dans « *Certificats (Ordinateur local) / Personnel/Certificats* », « *Certificats - Service(Connect:Express Nom-du-*

Moniteur) de l'ordinateur local) / Personnel/Certificats » ou « *Certificats - Utilisateur actuel / Personnel/Certificats* » suivant l'emplacement choisi.

.

DN Objet

Ce champ indique le « Distinguished Name » objet du certificat personnel.
Vous pouvez entrer :

- Soit le DN complet (par exemple « **CN=Test rsa1024 windows srv,OU=tlabs01,O=tlabs, L=Paris,S=Paris,C=FR »**).
- Soit simplement le nom commun (« Common Name » du DN), si cette valeur est unique dans votre répertoire des certificats personnels (par exemple « **Test rsa1024 windows srv** »).

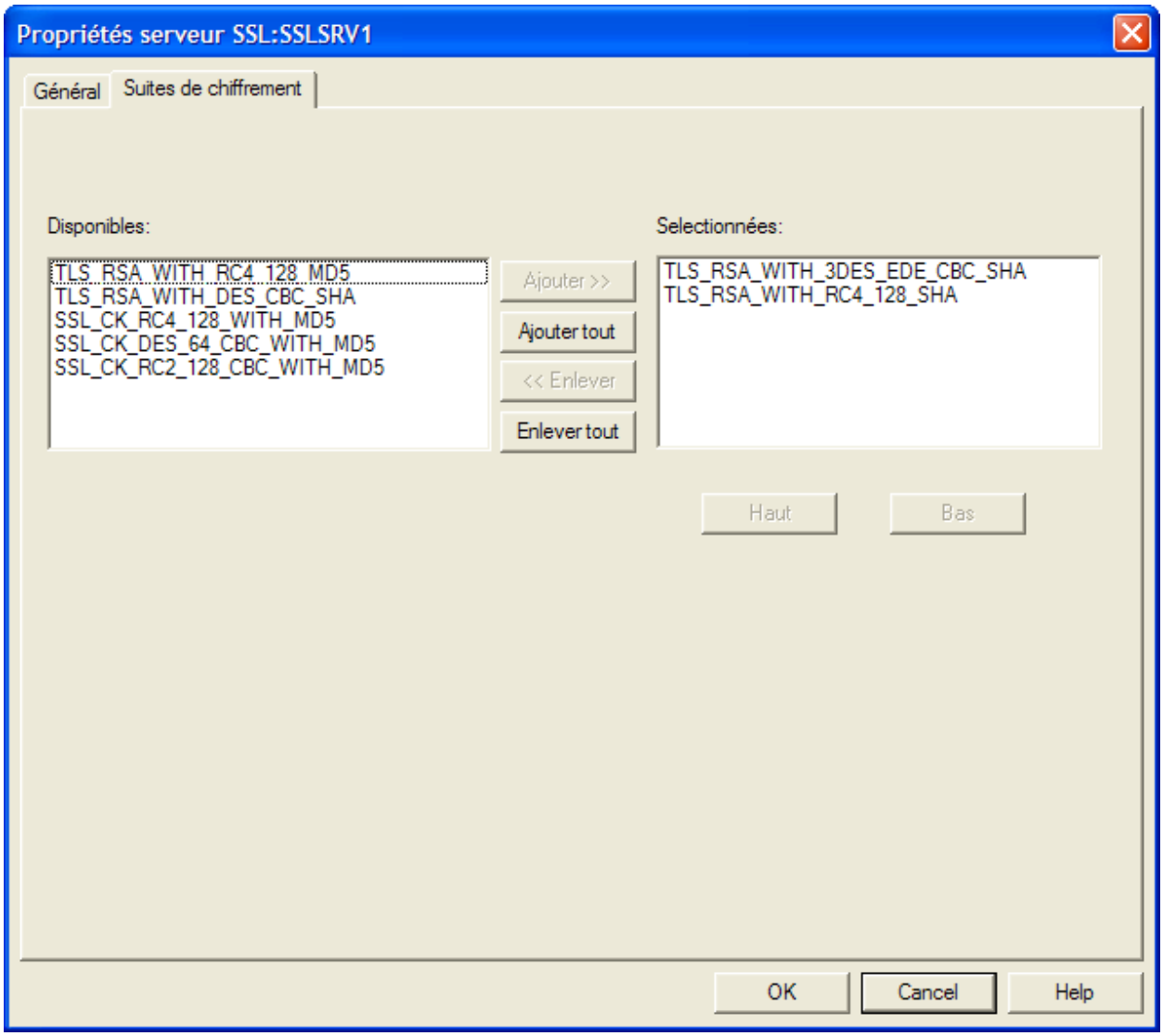
Le DN objet de votre certificat peut être visualisé en consultant les détails du certificat avec mmc.

DN émetteur

Ce champ indique le « Distinguished Name » de l'émetteur de votre certificat (Autorité de certification ayant signé votre certificat).
Ce champ peut en général être laissé non renseigné, sauf si vous avez deux certificats ayant le même DN objet, mais signés par deux autorités de certification différentes.
Vous pouvez entrer :

- Soit le DN complet (par exemple « **CN=CA test,OU=tlabs01,O=tlabs,L=Paris,S=Paris,C=FR** »).
- Soit simplement le nom commun (« common name » du DN), si cette valeur est unique parmi la liste des autorités émettrices de vos certificats (par exemple « **CA test** »).

Le DN émetteur de votre certificat peut être visualisé en consultant les détails du certificat avec mmc.



Suites de chiffrement

Ces boîtes de sélection vous permettent de sélectionner un ensemble de suites de chiffrements pouvant être utilisées pour la connexion SSL.
Si aucune suite de chiffrement n'est sélectionnée dans la liste de droite, le système choisira une suite de chiffrement pour vous, en fonction des possibilités du client distant.
Il est préférable de fixer les suites de chiffrement dont vous autorisez l'utilisation.
Dans les boîtes de sélection, les suites commençant par **TLS_** s'appliquent aux protocoles TLS V1 et SSL V3, les suites commençant par **SSL_CK_** s'appliquent au protocole SSL V2.
Les suites sélectionnées dans la boîte de droite peuvent être ordonnées par ordre de préférence.

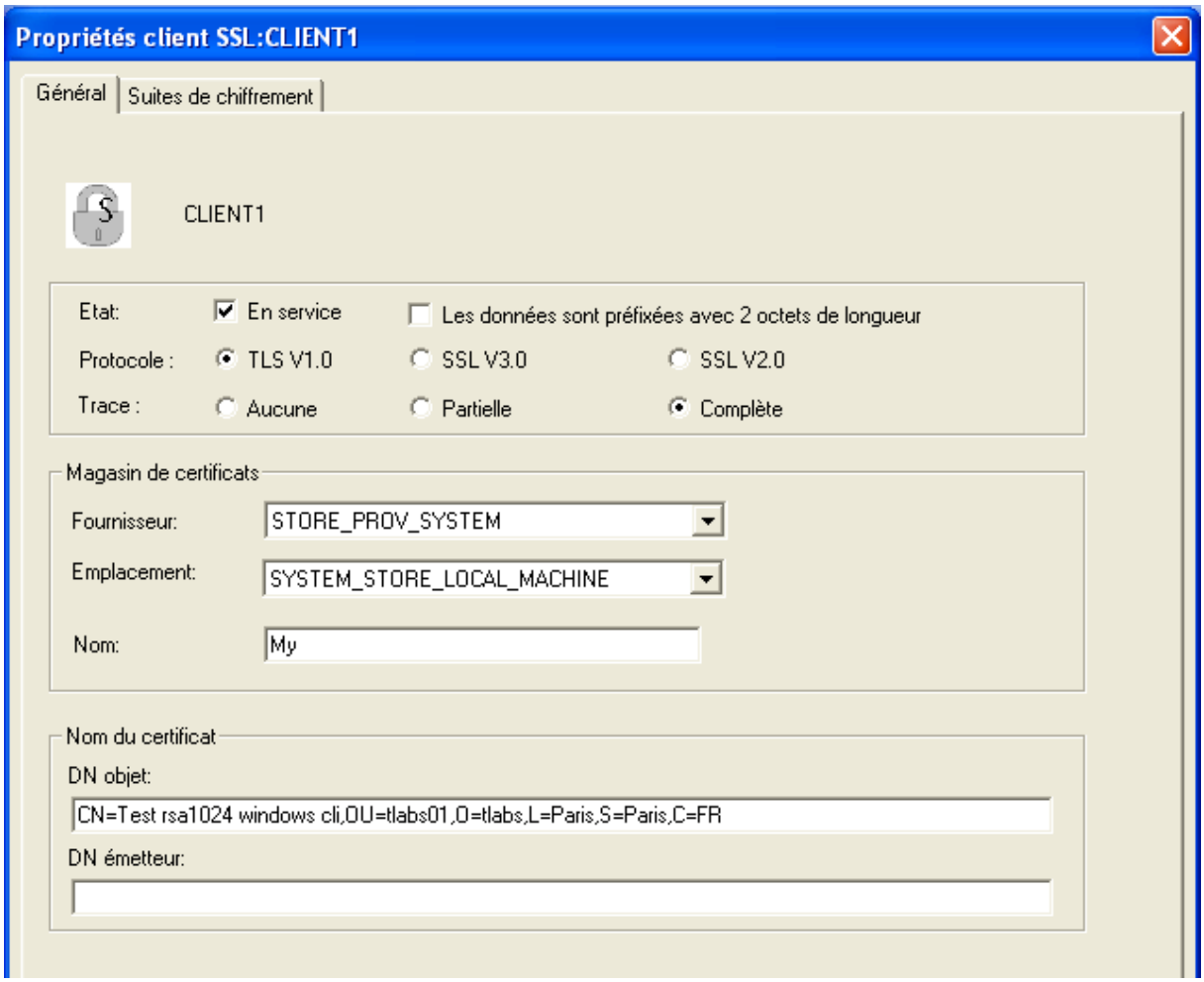
Paramétrage des clients

Contrairement aux paramètres du mode serveur, les paramètres du mode client sont choisis dynamiquement pour chaque partenaire au moment de l'établissement d'une connexion sortante vers ce partenaire.
De même que pour les paramètres du mode serveur, les paramètres clients sont identifiés par un nom symbolique. La définition d'un partenaire, pour fonctionnement en mode SSL client, indique le nom symbolique des paramètres clients à utiliser.
La définition de nouveaux paramètres SSL client, ne nécessite pas d'arrêt – redémarrage du moniteur.

Paramètres d'un client SSL

Chaque client SSL, identifié par son nom symbolique, est configuré dans le répertoire « **Administration \ Répertoires \ Clients SSL** » de l'interface graphique de Connect:Express.

Les boîtes de dialogue de définition des paramètres du mode client sont très semblables à celles du serveur et se présentent comme suit :



Nom symbolique

Ce champ est formé au maximum de 8 caractères majuscules (A-Z, 0-9).
Il est utilisé pour identifier une définition de paramètres client SSL.

Etat

Indique l'état des paramètres client SSL pour le moniteur.
S'il est coché, les paramètres client SSL peuvent être utilisés pour des transferts SSL; s'il n'est pas coché, les communications utilisant cet ensemble de paramètres échoueront.

Les données sont préfixées avec 2 octets de longueur

Indique que 2 octets de longueur sont placés avant les données non cryptées.
Ceci peut être nécessaire avec certaines passerelles effectuant des conversions PeSIT sur SSL ↔ PeSIT sans SSL.

Protocole

Indique la version de protocole SSL à utiliser (TLS V1, SSL V3, SSL V3).
Connect:Express ne permettra pas la négociation d'une autre version de protocole que celle fixée ici.

Trace

Indique le niveau de trace pour les transferts.
Les traces sont enregistrées dans le sous répertoire **trace** de Connect:Express.

- **Complète:** Trace complète du handshake, trace complète des échanges de données applicatives.
- **Partielle:** Trace complète du handshake, trace partielle des échanges de données applicatives

Fournisseur du magasin de certificats

Définit le type de fournisseur du magasin de certificats qui fournit les certificats à utiliser.
Actuellement, il y a un seul type de fournisseur disponible: « **STORE_PROV_SYSTEM** » indiquant le magasin logique standard accessible à l'aide de la console de gestion Microsoft **mmc**.

Emplacement dans le magasin

Définit l'emplacement dans le magasin. Trois emplacements sont possibles

- **SYSTEM_STORE_LOCAL_MACHINE** indique que les certificats sont situés dans le répertoire « *Certificat (Ordinateur local)* » du magasin système.
- **SYSTEM_STORE_SERVICES** indique que les certificats sont situés dans le répertoire « *Certificats – Service (Connect:Express Nom-du-moniteur) de l'ordinateur local* » du magasin système.
- **SYSTEM_STORE_CURRENT_USER** indique que les certificats sont situés dans le répertoire « *Certificats – Utilisateur actuel* » du magasin système.

Notes :
Si l'emplacement est SYSTEM_STORE_CURRENT_USER, Connect:Express ne peut être utilisé en service Windows que si le service a pour Log On l'utilisateur concerné (Voir Tableau page 10).
Lorsque l'option SYSTEM_STORE_SERVICES est choisie, les certificats d'autorité racine doivent être placés dans le répertoire « *Certificats (Ordinateur local) / Autorités de certification racines de confiance* ».

Nom dans le magasin

Ce champ indique le sous répertoire où le certificat personnel sera trouvé.
Utiliser « **My** », pour indiquer le répertoire des certificats personnels. mmc doit afficher le certificat dans « *Certificats (Ordinateur local)/Personnel / Certificats* », « *Certificats - Service(Connect:Express Nom-du-moniteur) de l'ordinateur local) / Personnel/Certificats* » ou « *Certificats - Utilisateur actuel / Personnel/Certificats* » suivant l'emplacement choisi.

DN Objet

Ce champ indique le « Distinguished Name » objet de votre certificat.
Vous pouvez entrer :

- soit le DN complet (par exemple « **CN=Test rsa1024 windows cli,OU=tlabs01,O=tlabs, L=Paris,S=Paris,C=FR** »)
- soit simplement le nom commun (« Common Name » du DN), si cette valeur est unique dans votre répertoire des certificats personnels (par exemple « **Test rsa1024 windows cli** »).

Le DN objet de votre certificat peut être visualisé en consultant les détails du certificat avec mmc.

DN émetteur

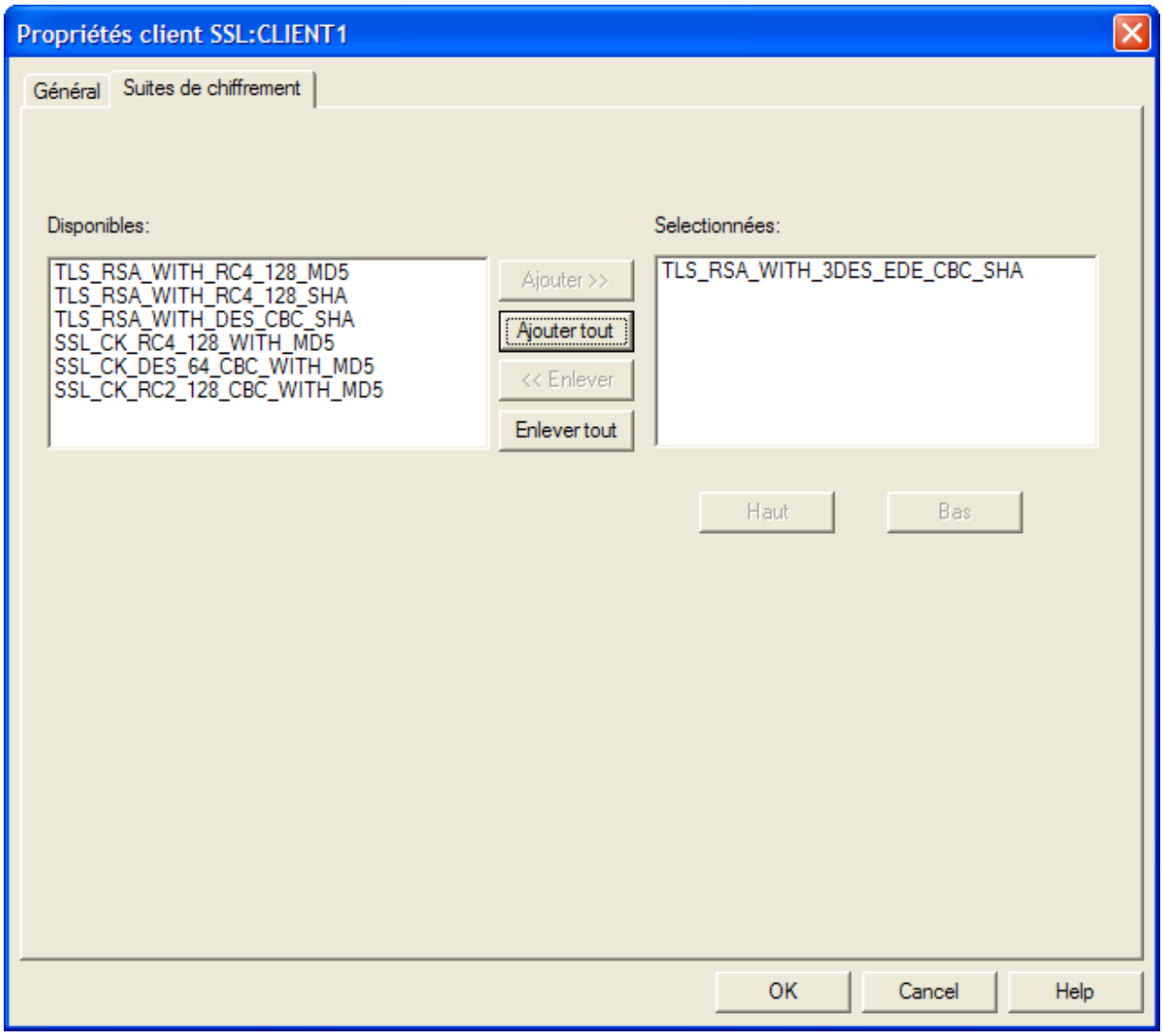
Ce champ indique le « Distinguished Name » de l'émetteur de votre certificat (Autorité de certification ayant signé votre certificat).

Ce champ peut en général être laissé non renseigné, sauf si vous avez deux certificats ayant le même DN objet, mais signés par deux autorités de certification différentes.
Vous pouvez entrer :

- Soit le DN complet (par exemple « **CN=CA test,OU=tlabs01,O=tlabs,L=Paris,S=Paris,C=FR** »).

- Soit simplement le nom commun (« Common Name » du DN), si cette valeur est unique parmi la liste des autorités émettrices de vos certificats (par exemple « **CA test** »).

Le DN émetteur de votre certificat peut être visualisé en consultant les détails du certificat avec mmc.



Suites de chiffrement

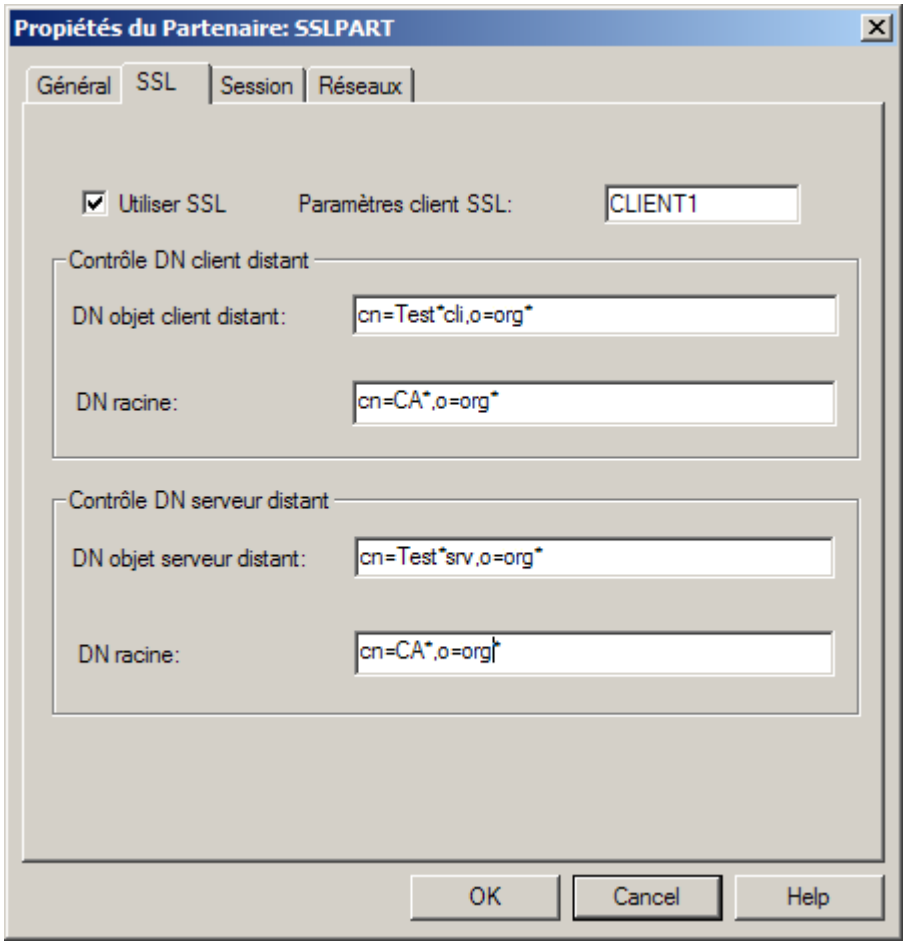
Ces boîtes de sélection vous permettent de sélectionner un ensemble de suites de chiffrements pouvant être utilisées pour la connexion SSL.
Si aucune suite de chiffrement n'est sélectionnée dans la liste de droite, le système choisira une suite de chiffrement pour vous, en fonction des possibilités du serveur distant.
Il est préférable de fixer les suites de chiffrement dont vous autorisez l'utilisation.
Dans les boîtes de sélection, les suites commençant par **TLS_** s'appliquent aux protocoles TLS V1 et SSL V3, les suites commençant par **SSL_CK_** s'appliquent au protocole SSL V2.

L'ordre des suites dans la boîte de droite est sans effet.
Le système choisit selon son ordre de préférence personnel parmi les suites sélectionnées.
Donc, si vous voulez utiliser une suite spécifique dans tous les cas, ne sélectionnez que cette suite uniquement.

Définition d'un partenaire

Ecran de définition

L'écran de définition SSL d'un partenaire se présente comme suit :



Dans l'exemple ci-dessus, le nom symbolique CLIENT1 est le nom symbolique d'un ensemble de paramètres clients SSL, qui seront utilisés pour les transferts en mode demandeur.

Note :
Cette définition de partenaire peut être simultanément utilisée pour des connexions entrantes (transferts en mode serveur). Mais dans ce cas, CLIENT1 n'est pas utilisé puisque les caractéristiques de la connexion sont déterminées par le serveur SSL qui est à l'écoute des connexions entrantes venant du partenaire distant.
Dans le cas d'une connexion entrante, l'option *Utiliser SSL* permet de forcer l'utilisation de SSL pour ce partenaire.

Contrôle du DN du partenaire distant

Les champs facultatifs de définition de contrôle du « distinguished name » distant permettent d'autoriser au niveau de la définition du partenaire (PeSIT ou Etebac3) un ensemble restreint de partenaires SSL.
Le partenaire SSL distant présente un certificat lors de l'établissement du handshake SSL. Si ce certificat ne satisfait pas aux critères d'autorisation définis pour le partenaire, le transfert est refusé.

Pour les connexions en mode SSL client, utiliser les champs « Contrôle du DN du serveur distant ».

Pour les connexions en mode SSL serveur, utiliser les champs « Contrôle du DN du client distant ».

Les critères « DN objet distant » indiquent des critères devant être satisfaits par le DN objet du certificat présenté par le partenaire.
Les critères « DN racine distant » indiquent des critères devant être satisfaits par le DN de l'autorité de certification racine du certificat présenté par le partenaire.

Chaque critère est constitué d'une suite de « relative distinguished names » (RDNs) séparés par des virgules.
Les critères supportent les wildcards simples * et ?.
Chaque RDN doit trouver sa correspondance dans le DN présenté par le partenaire.

Par exemple :
Si Dn objet distant = « cn=Test01*srv,o=org* », un partenaire présentant un certificat ayant pour DN objet « CN=Test01 rsa1024 srv,ou=unit1,o=org1 » sera accepté, alors qu'un partenaire présentant un certificat ayant pour DN objet « CN=Test**02** rsa1024 srv,ou=unit1,o=org1 » sera refusé.

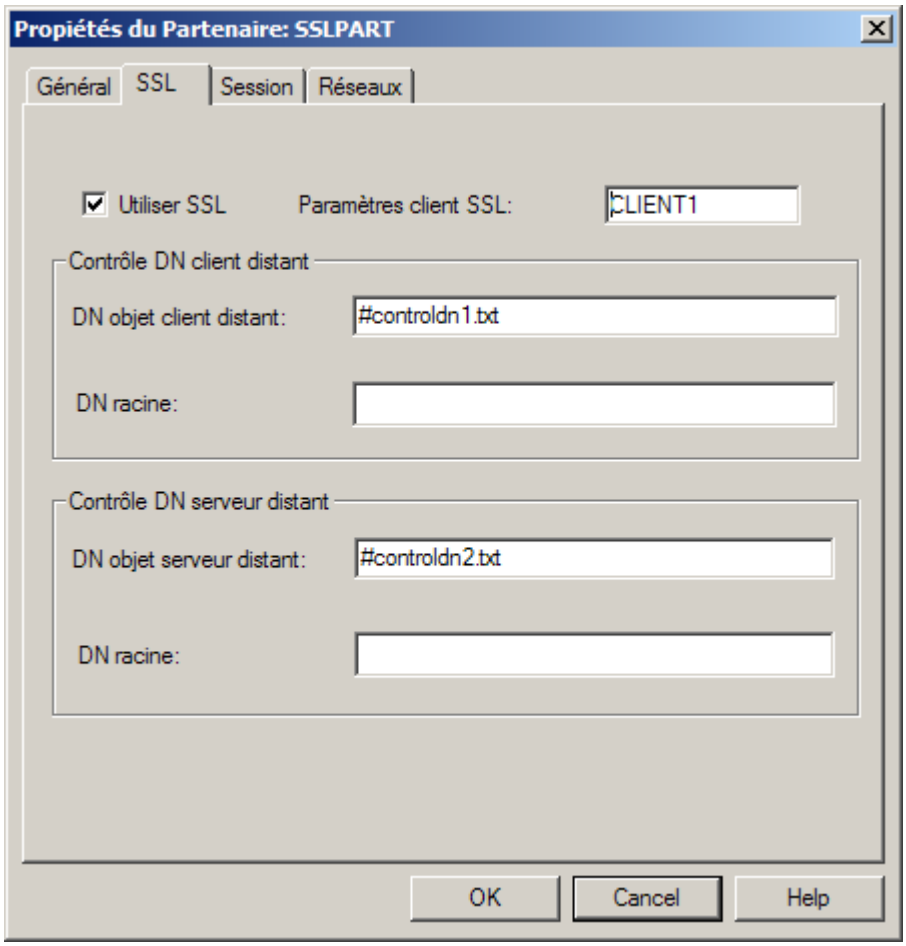
Les clés suivantes sont acceptées pour les RDNs :

C	Contains a two-letter ISO 3166 country or region code
CN	Contains a common name
E,EMAIL	Contains an e-mail address
DC	Contains one component of a Domain Name System (DNS) name
G,GivenName	Contains the part of a person's name that is not a surname
I	Contains a person's initials
L	Contains the locality name that identifies a city, country, or other geographic region
O	Contains the name of an organization
OU	Contains the name of a unit subdivision within an organization
S,ST	Contains the full name of a state or province
STREET	Contains the physical address
SN	Contains the family name of a person
T,TITLE	Contains the title of a person in the organization

Note : Les clés sont insensibles à la casse, par contre les valeurs associées sont sensibles à la casse. Par exemple, « ou=unit » a le même effet que « OU=unit », mais est différent de « ou=Unit ».

Fichier de contrôle du DN

Si le nombre de DN différents à contrôler pour le partenaire est trop grand (ce qui peut être le cas notamment en mode serveur), il est également possible de mentionner dans les champs « DN objet distant » un nom de fichier contenant une liste de DNs.
Chaque nom de fichier doit être préfixé par '#' et faire référence à un fichier situé dans un sous -répertoire « config » du répertoire d'installation du moniteur.
Si une liste de contrôle est mentionnée dans un champ DN objet distant, le champ « DN racine » correspondant doit être laissé non renseigné.



Une liste de contrôle est similaire à celle présentée dans l'exemple suivant :

```
# Remote DN control
S CN=Test*cli,OU=tlabs01,O=tlabs
R cn=CA*
S CN=name*,O=org
R
S CN=Test*srv,OU=tlabs01,O=tlabs
R cn=CA*
```

Chaque ligne doit commencer par :

- # : Commentaire
- S : Critère DN objet
- R : Critère DN racine

Une ligne S doit être suivie d'une ligne R. Le certificat du distant est examiné pour chaque couple (S,R), jusqu'à ce qu'il satisfasse aux critères d'autorisation d'un de ceux-ci.
Pour chaque ligne S ou R, le critère DN peut être laissé à espaces indiquant qu'il n'y a pas de contrôle dans le couple pour cette ligne.

Messages d'erreurs des transferts SSL

Les messages d'erreur des transferts SSL sont accessibles dans la rubrique *Messages* de l'interface graphique.
Les codes d'erreur NRC décrivent la cause d'erreur rencontrée par le composant réseau de Connect:Express.
Les codes d'erreur des appels aux composants SSPI, Schannel ou CryptoApi sont indiqués dans le champ TCP/IP RC des messages de Connect:Express.
L'aide en ligne de l'interface graphique détaille la signification des codes NRC et des codes retour SSL tels que décrits dans la documentation Microsoft.

Ci-dessous un extrait de messages de Connect:Express correspondant à un transfert en boucle en erreur :

```
2007/10/31 - 11:24:51 : 200730400002 - APPEL ENTRANT (SSL/TCP) ACCEPTE
2007/10/31 - 11:24:51 : 200730400001 - ERREUR OUVERTURE COMMUNICATION AVEC SSLPART
2007/10/31 - 11:24:51 : 200730400002 - COMMUNICATION REJETEE - PARTENAIRE INCONNU
2007/10/31 - 11:24:51 : 200730400002 - TRC= A000 PRC= 0000 SRC= 0000 NRC= A526
2007/10/31 - 11:24:51 : 200730400002 - TCP/IP RC= 80090304
2007/10/31 - 11:24:51 : 200730400002 - MISE HORS SERVICE
2007/10/31 - 11:24:51 : 200730400002 - PURGEE
2007/10/31 - 11:24:51 : 200730400001 - TRC= A000 PRC= 0000 SRC= 0000 ERC= 0000 NRC= A525
2007/10/31 - 11:24:51 : 200730400001 - TCP/IP RC= 8009030E
```

L'aide en ligne fournit les éléments suivants :

Client (requête n° 200730400001)
NRC : A525: Error Client handshake
TCP/IP RC : 8009030E SEC_E_NO_CREDENTIALS No credentials are available in the security package

Serveur (requête n° 200730400002)
NRC : A526: Error Server handshake
TCP/IP RC : 80090304 SEC_E_INTERNAL_ERROR The Local Security Authority cannot be contacted

L'erreur côté client indique que le certificat du client n'a pu être trouvé dans le magasin des certificats (No credentials).

Trace

En cas de problèmes lors de la mise en place de transferts SSL avec un partenaire distant, il est conseillé d'activer la trace. Les traces peuvent être activées sélectivement à l'aide de l'interface graphique au niveau du paramétrage d'un client ou d'un serveur SSL. L'activation de la trace pour un serveur nécessite un arrêt – redémarrage du moniteur.
Les fichiers de trace se trouvent dans le sous-répertoire trace du répertoire d'installation de Connect:Express.
Les fichiers de trace correspondant à des transferts ont un nom de la forme <n° de requête>.txt.