

Université IBM i 2018

16 et 17 mai

IBM Client Center Paris



S52 - Conformité GDPR avec le cryptage SSL/TLS

Dominique GAYTE

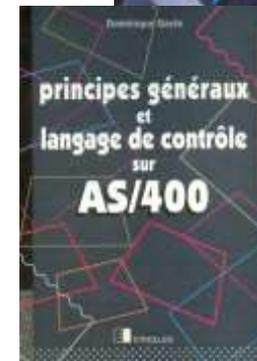
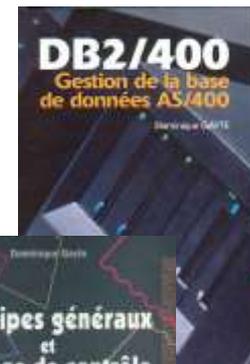
NoToS

dgayte@notos.fr – www.notos.fr



NoToS

- Expertise autour de l'IBM i
 - Regard moderne
 - Sécurité
 - Service
 - Formation, audit, développement...
- PHP sur IBM i avec Zend
 - Modernisation
 - Web Services...
- Développement de progiciels
 - Modernisation à valeur ajoutée des IBM i



Plan de la présentation

- Avant propos
 - Sécurité des connexions FTP et Telnet
 - Le GDPR et la sécurité des connexions
- SSL et IBM i
- Les certificats
 - Les Autorités de Certification (CA)
 - Digital Certificate Manager (DCM)
- Utilisation de SSL



Avant propos

- Connexions classiques aux IBM i sont non sécurisées
 - Emulation écran, FTP
 - ID et mot de passe circulent en clair
- Démonstration FTP

```
C:\Users\Imerys>ftp 192.168.1.3
Connecté à 192.168.1.3.
220-QTCP at SCORPION.NOTOS.BEAULIEU.
220 Connection will close if idle more than 5 minutes.
501 OPTS unsuccessful; specified subcommand not recognized.
Utilisateur (192.168.1.3:(none)) : QSECOFR
331 Enter password.
Mot de passe :
```



```
54 55981 → 21 [ACK] Seq=15 Ack=156 Win=8037 Len=0
68 Request: USER QSECOFR
75 Response: 331 Enter password.
54 55981 → 21 [ACK] Seq=29 Ack=177 Win=8016 Len=0
71 Request: PASS monpwd1234
```


Avant propos (2)

- Démonstration Telnet

```
Ouverture
Système . . . . . : SCORPION
Sous-système . . . : QBASE
Ecran . . . . . : QPADEV0003

Utilisateur . . . . . QSECOFR
Mot de passe . . . . .
Programme/procédure . . . . .
Menu . . . . .
Bibliothèque en cours . . . . .
```



```
40 f2 e9 5d 02 f9 00 15 5d 01 63 00 08 00 45 00 22).9.. ).....
00 4e 13 77 40 00 80 06 00 00 c0 a8 01 63 c0 a8 .+.. ... ..{y..{y
01 03 da 76 00 17 a0 c0 20 26 70 fe 58 ce 50 18 .....{ &....&.
00 fe 83 f7 00 00 00 24 12 a0 00 00 04 00 80 03 ..c7...$ .....
08 35 f1 11 06 35 d8 e2 c5 c3 d6 c6 d9 11 07 35 .51..QSECOFR..5
d4 d6 d5 d7 e6 c4 f1 f2 f3 f4 ff ef MONPWD12 34..
```

- Article 32 : sécurité des traitements

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, **le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque**, y compris entre autres, selon les besoins:

- a) la pseudonymisation **et le chiffrement des données à caractère personnel**;
- b) des moyens permettant de garantir la confidentialité**, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
- c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
- d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

GDPR (2)



- Nous devons assurer la confidentialité des mots de passe
 - Même en dehors du GDPR !
- Nous devons sécuriser les échanges de données à caractères personnels
- Toute connexion distante à votre IBM i (et autres serveurs !) doit être sécurisée
 - Telnet
 - FTP
 - Client Access, ACS
 - HTTP
 - Web
 - Web Services



SSL et IBM i

SSL : Secure Socket Layer



- C'est un protocole de sécurisation des échanges sur Internet
 - A utiliser à partir de V3.0
- TLS (Transport Layer Security) est la nouvelle version
 - TLS 1.0 équivalent de SSL 3.1
- Création d'un « tunnel » dans lequel les informations circulent cryptées
- Possibilité de s'assurer de l'identité du serveur et du client
- S'appuie sur des certificats émis par des autorités de certification (CA)
- Voir la présentation de S28 de 2013
- A télécharger
 - Sur le site d'IBM
 - [Sur le site de NoToS](#)

SSL dans l'IBM i

- Tous les outils en standard
 - DCM Digital Certificate Manager
 - Option 34 de SS1 (non facturable)
 - Serveur Web d'administration
 - Administration générale via le Web
 - IBM Web Administration for i
 - Administration des serveurs Web
- ACS, IBM i Access for Windows et System i Navigator
 - Toutes les fonctions supportent SSL
- IBM Portable Utilities for i
 - 5733SC1
 - SSH, SFTP

SSL dans l'IBM i et valeurs système

- Valeurs système qui permettent de spécifier les algorithmes et protocoles supportés
 - QSSLCSL, QSSLCSLCTL, QSSLPCL
- Les valeurs *OPSYS de QSSLCSLCTL et de QSSLPCL indiquent que se sont les valeurs associées à la version de l'IBM i qui sont prises en compte

Versions de SSL/TLS

- Depuis la V7R1 TR 6 : support de TLS 1.2 (SI48659))
- En V7R2, SSL V3 est désactivé par défaut
- Peut être réactivé avec la valeur système QSSLPCL

Etat de la connexion

🔒 La connexion est sécurisée.

Protocole de sécurité

Niveau de chiffrement de sécurité

Informations sur le certificat de serveur

```

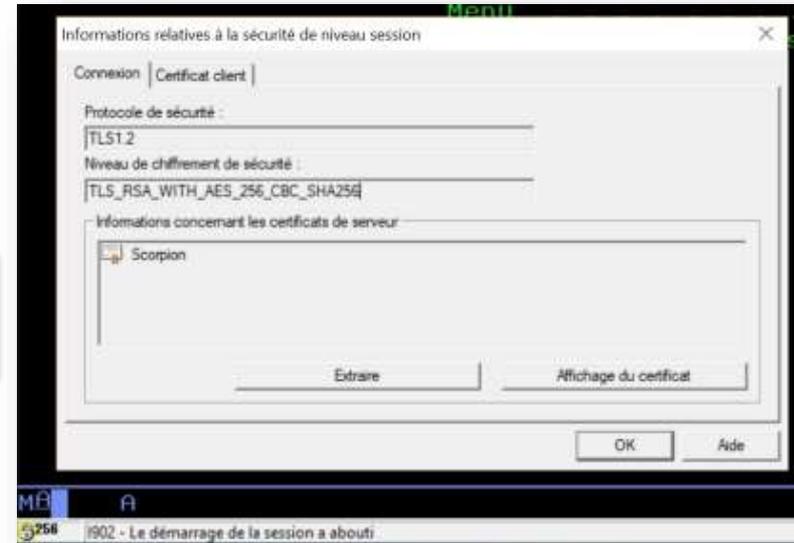
Nom = Scorpion
Société = NoToS
Pays = fr
Version = 3
Numéro de série = 55:71:BA:5F:0C:27:30
Algorithme de signature = SHA256withRSA
Emetteur = CN=Scorpion.notes.beaulieu,O=NoToS,ST=Beaulieu,C=FR
Valide depuis = jeudi 4 juin 2015 17 h 03 CEST
Valide jusqu'à = mercredi 25 novembre 2020 16 h 03 CET
Clé publique = RSA (2048 Bits)
Empreinte digitale MD5 = A7:0D:74:EA:D0:C9:A2:7A:83:A2:12:55:0D:E3:E7:38
Empreinte digitale SHA1 = 46:AE:2F:85:D7:43:D1:A0:58:54:2A:D2:E0:58:62:C8:29:BB:75:7D
    
```

OK Extraction... Affichage des AC dignes de la confiance du client... Affichage du certificat client... Affichage du certificat de l'émetteur... Aide

Niveau de chiffrement

- Algorithmes de chiffrement
 - Ordre de préférence dans la valeur système QSSLCSL
- Protocole utilisé (SSL ou TLS)
- Algorithme d'échange de clés (RSA, ECDHE)
- Algorithme de chiffrement (AES, DES)
- Hashage (SHA, MD5...)

TLS_RSA_WITH_AES_128_CBC_SHA256



Niveau de chiffrement

- Par défaut avec ACS et Client Access
 - *RSA_AES_128_CBC_SHA256



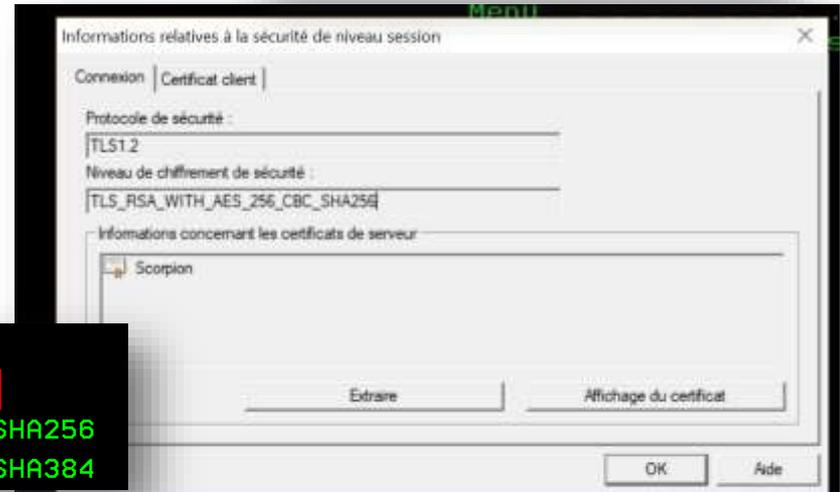
- On peut le forcer en AES 256
- Dépend du client !

```

10 *ECDHE_ECDSA_AES_128_CBC_SHA256
20 *ECDHE_ECDSA_AES_256_CBC_SHA384
30 *ECDHE_ECDSA_AES_128_GCM_SHA256
40 *ECDHE_ECDSA_AES_256_GCM_SHA384
50 *RSA_AES_128_CBC_SHA256
60 *RSA_AES_128_CBC_SHA
  
```

```

0
10 *RSA_AES_256_CBC_SHA256
20 *ECDHE_ECDSA_AES_128_CBC_SHA256
30 *ECDHE_ECDSA_AES_256_CBC_SHA384
  
```



The background of the slide features a complex network diagram. It consists of numerous small, light gray circular nodes scattered across the frame. These nodes are interconnected by a dense web of thin, light gray lines, creating a mesh-like structure that resembles a network or a molecular lattice. The overall aesthetic is clean and technical.

Les certificats

Les certificats

- Emis par une autorité de certification
 - CA : *Certificate Authority*
- L'IBM i peut être une CA et émettre tous les certificats dont nous auront besoin
 - Idéal dans le cas d'une utilisation interne
- Mais on peut aussi utiliser des certificats émis par d'autres CA
 - Windows
 - Ou achetés auprès de sociétés accréditées
 - Vendent les certificats et assurent leurs validités
 - CyberTrust, Verisign, Thawte ...
- Les certificats sont rangés dans un magasin de certificats
 - Quasiment chaque application a le sien !

Les CA dignes de confiance

- Chaque application vérifie si le certificat est valide
 - Est-ce que la CA qui a émis le certificat est « Digne de confiance » ?
- CA officielles
 - Les applications reconnaissent la CA comme digne de confiance en natif
- CA privées (locales)
 - Certificats émis sont gratuits
 - Mais non reconnus, il faudra définir la CA comme étant de confiance dans chaque application concernée

- Outil de gestion des certificats
- Interface Web
 - port 2001 de l'IBM i (@:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0)
 - Le serveur d'administration doit être démarré

Page des tâches IBM i

 [Gestionnaire de certificats numériques](#)

Permet de créer, de distribuer et de gérer les certificats numériques



Digital Certificate Manager



5769-NC1, 5769-NCE, 5769-SS1, 5722-SS1, 5761-SS1, 5770-SS1 (C) Copyright IBM Corporation 1997, 2014
All rights reserved.
US Government Users Restricted Rights -
Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Licensed Materials - Property of IBM

 Contains software from RSA Data Security, Inc.

[Get Started](#)

■ [Create Certificate](#)

■ [Create New Certificate Store](#)

■ [Install Local CA Certificate on Your PC](#)

▶ [Manage User Certificates](#)

▶ [Manage CRL Locations](#)

■ [Manage LDAP Location](#)

■ [Manage PKIX Request Location](#)

[Return to IBM i Tools](#)

Création d'une CA

Create a Certificate Authority (CA)

Certificate type: Certificate Authority (CA)

Certificate store: Local Certificate Authority (CA)

The system will create a certificate with a private key and store the certificate in the Local Certificate Authority (CA) certificate store.

Key algorithm: RSA ▼
Key size: 4096 ▼ (bits)
Hash algorithm: SHA-256 ▼

Certificate Information

Certificate Authority (CA) name: CA_NoToS_IBMi (required)
Organization unit: DSI
Organization name: NoToS (required)
Locality or city: BEAULIEU
State or province: Languedoc (required:minimum of 3 characters)
Country or region: FR (required)

Validity period of Certificate Authority (CA) (2-7300): 3650 (days)

Continue Cancel

Création d'un certificat

- De serveur

Create Certificate

Certificate type: Server or client

Certificate store: *SYSTEM

Use this form to create a certificate in the certificate store listed above.

Certificate Authority (CA) LOCAL_CERTIFICATE_AUTHORITY_218F5BV1(2) : RSA-4096 : SHA256 with RSA ▼

Key algorithm: RSA ▼

Key size: 2048 ▼ (bits)

Certificate label: Scorpion_Web

Certificate Information

Common name: www.cave.notos

Organization unit: DSI

Organization name: NoToS

Locality or city: BEAULIEU

State or province: Languedoc

Country or region: FR (required)

Association aux applications

- A la création du certificat ou ultérieurement
- Eventuellement arrêter/démarrer l'application serveur

<input type="checkbox"/>	Application	Type	Assigned certificate
<input type="checkbox"/>	Central Server	Server	Scorpion
<input type="checkbox"/>	Database Server	Server	Scorpion
<input type="checkbox"/>	Data Queue Server	Server	Scorpion
<input type="checkbox"/>	Network Print Server	Server	Scorpion
<input type="checkbox"/>	Remote Command Server	Server	Scorpion
<input type="checkbox"/>	Signon Server	Server	Scorpion
<input checked="" type="checkbox"/>	IBM i TCP/IP Telnet Server	Server	Scorpion
<input type="checkbox"/>	IBM i TCP/IP Telnet Client	Client	Scorpion
<input type="checkbox"/>	Serveur IBM i DDM/DRDA - TCP/IP	Server	Scorpion
<input type="checkbox"/>	Client IBM i DDM/DRDA - TCP/IP	Client	Scorpion

A background of a complex network graph with numerous nodes and connecting lines, rendered in a light gray color. The nodes are small circles, and the lines are thin, creating a dense web of connections across the entire page.

Utilisation de SSL

ACS et Client Access

- Toutes les fonctions sont éligibles à SSL
- Emulation écran
- Transfert de données
- System i Navigator
- Accès à l'IFS

Configuration au niveau de la connexion

Editer le système sélectionné

Général Connexion Console

Nom de système : xxx.notes.fr

Description :

Utilisation de SSL pour la connexion

Vérification de la connexion

Propriétés de Cave.notes.fr

Système d'administration Services d'annuaires Maintenance Modules d'extension

Général Connexion Utilisation de la fonction SSL Licences Redémarrage

Fonction SSL

Utiliser la fonction SSL pour la connexion

Vérification de la connexion SSL

Autorité d'accréditation i5/OS

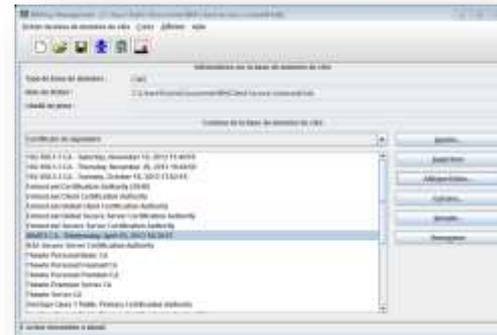
Pour que System i Access Express puisse se fier aux certificats de serveur signés ou créés par l'autorité d'accréditation i5/OS, cette dernière doit être téléchargée sur ce PC. Remarque : Il n'est pas nécessaire de télécharger les autres autorités d'accréditation fournies

Pour utiliser l'autorité d'accréditation i5/OS, cliquez sur

Téléchargement

Magasin de certificats

- Le certificat de la CA qui a émis le certificat de serveur doit être dans le magasin de certificats de l'application
- Client Access
 - Ce magasin est constitué de trois fichiers
 - **cwbsldf.kdb** c'est la base de données de clés
 - **cwbsljavaca.jck** c'est le fichier de clé utilisé par JDBC
 - **cwbsldf.sth** contient le mot de passe du magasin
 - Ils pourront être copiés sur les postes de travail lors d'un déploiement des postes clients
- Utilitaire de gestion des clés
 - IBM Key Management



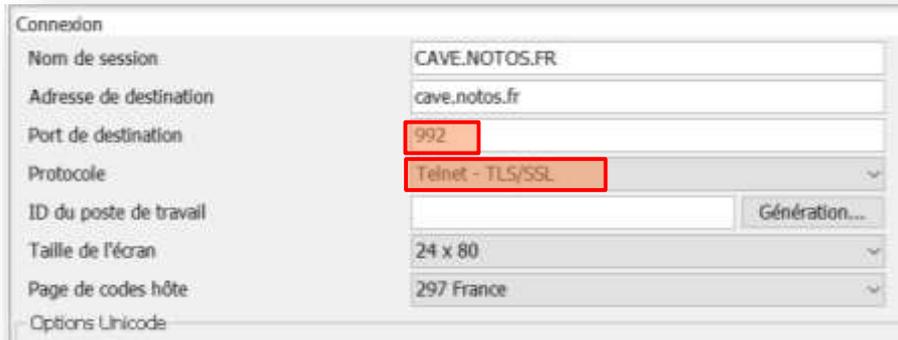
Magasin de certificats (2)

- ACS
 - Accessible à partir de l'interface (Outils/Gestion des clés)
 - Est propagé dans l'export/import de configuration

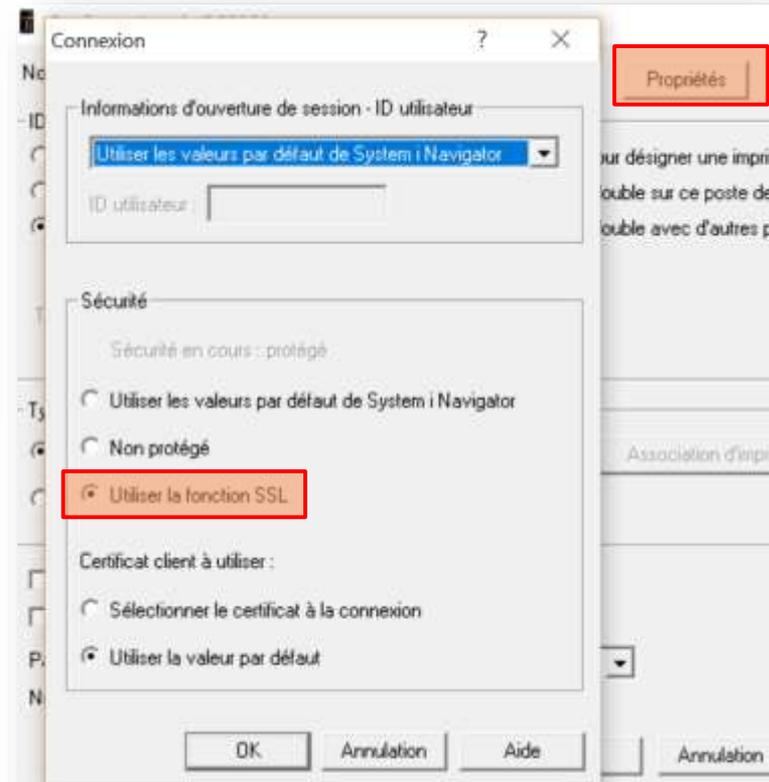


Emulation écran

- Pour configurer une session en particulier



Connexion	
Nom de session	CAVE.NOTOS.FR
Adresse de destination	cave.notos.fr
Port de destination	992
Protocole	Telnet - TLS/SSL
ID du poste de travail	<input type="text"/> Génération...
Taille de l'écran	24 x 80
Page de codes hôte	297 France
Options Unicode	



Connexion

Informations d'ouverture de session - ID utilisateur

Utiliser les valeurs par défaut de System i Navigator

ID utilisateur :

Sécurité

Sécurité en cours : protégé

Utiliser les valeurs par défaut de System i Navigator

Non protégé

Utiliser la fonction SSL

Certificat client à utiliser :

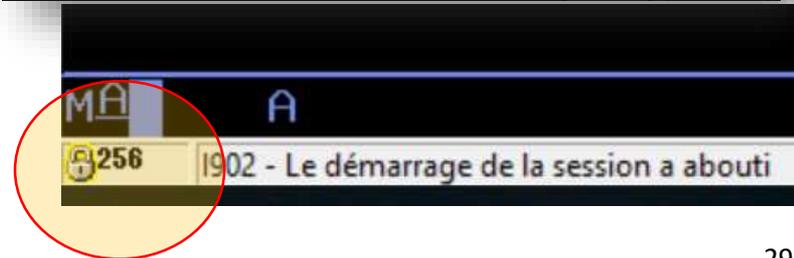
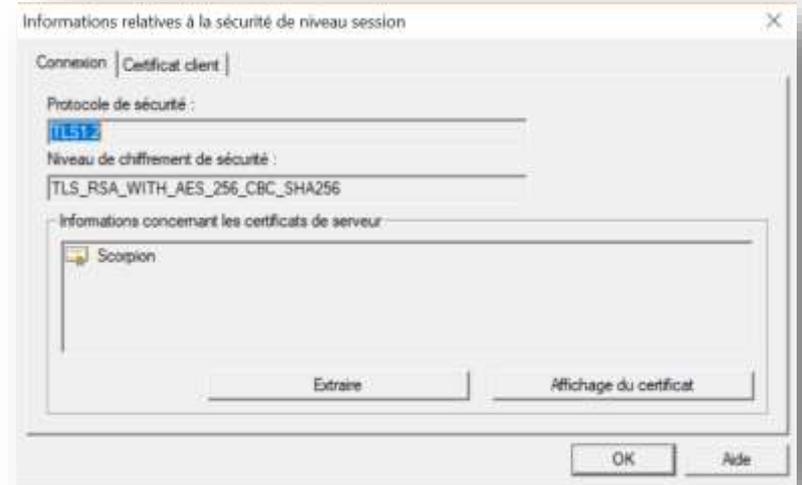
Sélectionner le certificat à la connexion

Utiliser la valeur par défaut

OK Annulation Aide Annulation

Informations de Sécurité

- Comparable entre ACS et Client access



Configuration du serveur TELNET

- CHGTELNA (Allow Secure Socket Layer . . . ALWSSL)
- SSL optionnel : *YES
- SSL obligatoire : *ONLY

```

Change TELNET Attributes (CHGTELNA)

Indiquez vos choix, puis appuyez sur ENTREE.

Autostart server . . . . . *YES          *YES, *NO, *SAME
Number servers . . . . . *CALC          1-200, *SAME, *CALC
Session keep alive timeout . . . *CALC    0-2147483647, *SAME, *CALC...
Default NVT type . . . . . *VT100      *SAME, *VT100, *NVT
Coded character set identifier . *MULTINAT 1-65533, *SAME, *MULTINAT...
ASCII fullscreen mapping:
  Outgoing EBCDIC/ASCII table . *CCSID     Nom, *SAME, *CCSID, *DFT
    Library . . . . .          _____ Nom, *LIBL, *CURLIB

  Incoming ASCII/EBCDIC table . *CCSID     Nom, *SAME, *CCSID, *DFT
    Library . . . . .          _____ Nom, *LIBL, *CURLIB
Allow Secure Socket Layer . . . *YES          *YES, *NO, *ONLY, *SAME

Fin
F3=Exit   F4=Invite   F5=Réafficher   F12=Annuler   F13=Mode d'emploi invite
F24=Autres touches
  
```

Rappel sur les ports utilisés

- Par ACS et Client Access

Nom	Non SSL	SSL
Server Mapper as-svrmap	449	449
License Management as-central	8470	9470
Database Access as-database	8471	9471
Data Queues as-dtaq	8472	9472
Network Drives as-file	8473	9473
Network Printers as-netprt	8474	9474
Remote Command as-rmtcmd	8475	9475
Signon Verification as-signon	8476	9476
Telnet (PC5250 Emulation) telnet	23	992
HTTP Administration as-admi >	2001	2010
Management Central as-mgtc >	5555	5566
Ultimedia Services as-usf	8480	9480
DDM DDM	447	448

En conclusions...

- Le GDPR n'est qu'une raison de plus pour mettre en place SSL
- Indispensable pour tous les échanges en dehors de votre réseau
 - Plus de FTP, mais du FTPS ou du SFTP (non SSL mais sécurisé) vers vos partenaires externes
- Fortement conseillé sur le réseau interne
 - Ressort souvent dans les audits
 - Pour les accès aux IBM i et les autres serveurs
- Pas (peu) couteux !

Merci de votre attention

Dominique GAYTE - NoToS
dgayte@notos.fr – www.notos.fr

