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

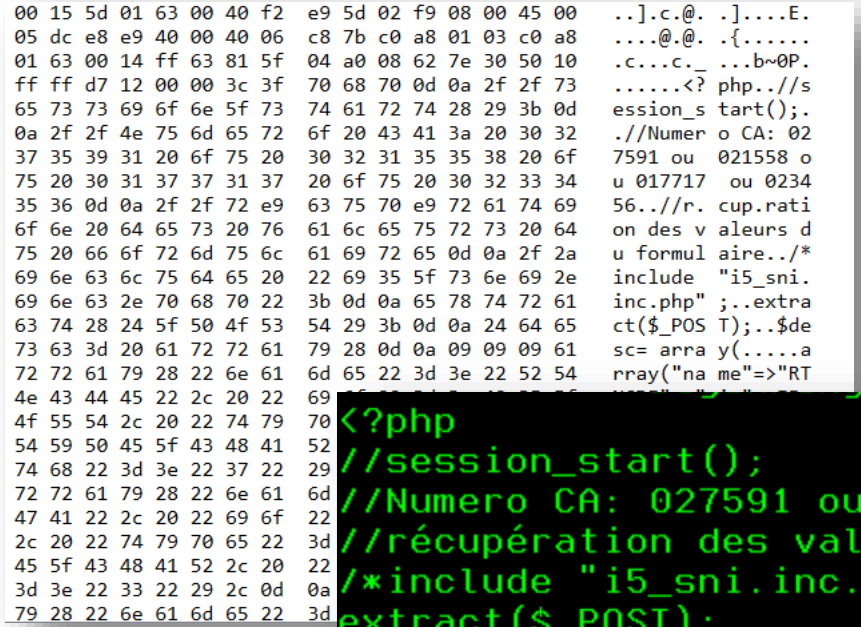
- Connexions classiques aux IBM i sont non sécurisées
  - Emulation écran, FTP
  - ID et mot de passe circulent en clair
- Démonstration FTP

```
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
```

Pour les données

- Il en est de même avec les données




```php
<?php
//session_start();
//Numero CA: 027591 ou 021558 ou 017717 ou 023456
//récupération des valeurs du formulaire
/*include "i5_sni.inc.php";
extract($_POST);
$desc= array(
   array("name"=>"RTNCDE", "io"=>I5_OUT, "type"=>I5_TYPE_CHAR,
```

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    2Z).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..5QS ECOFR.5
d4 d6 d5 d7 e6 c4 f1 f2  f3 f4 ff ef               MONPWD12 34..
```

GDPR

- 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

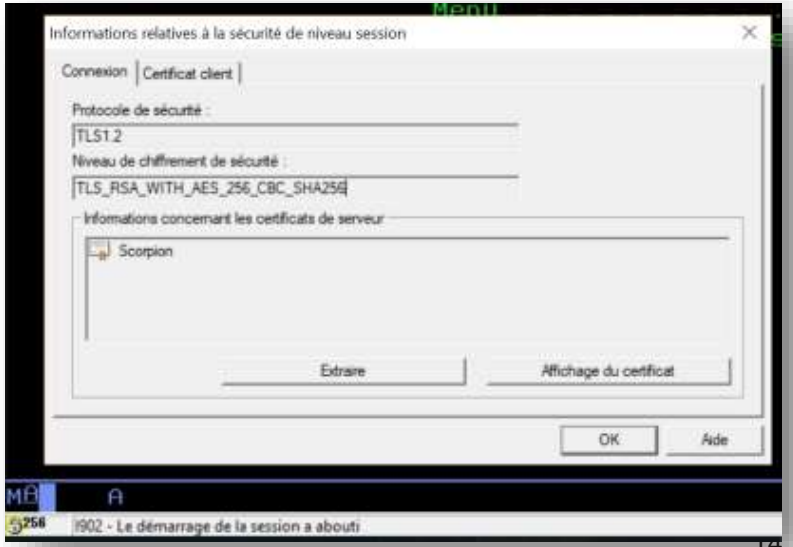
Versions de SSL/TLS

- 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

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…)

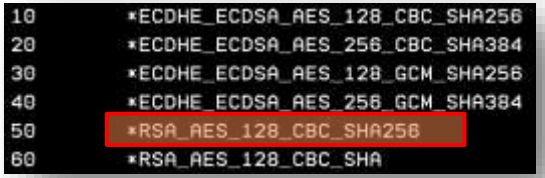
TLS_RSA_WITH_AES_128_CBC_SHA256

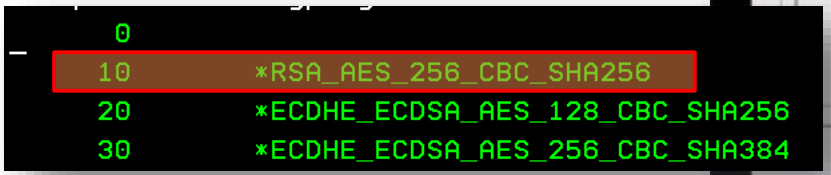


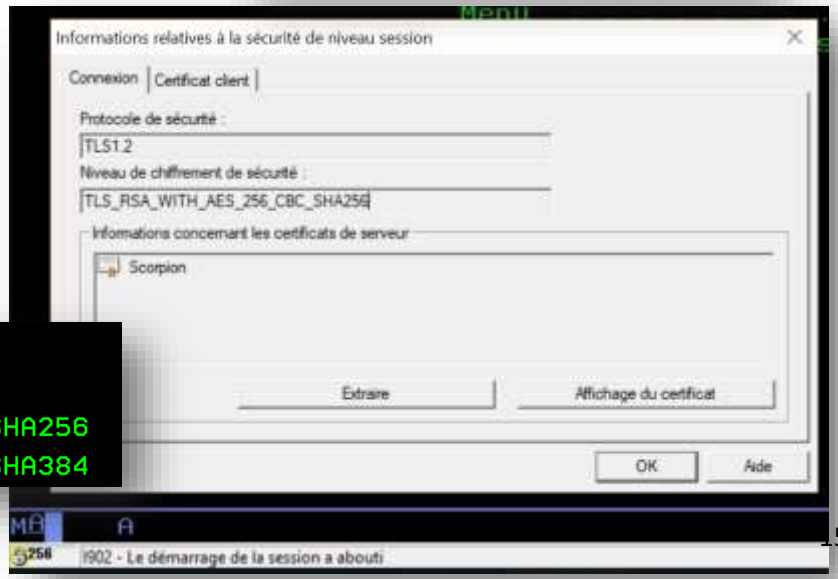
Niveau de chiffrement

- Par défaut avec ACS et Client Access
  - *RSA_AES_128_CBC_SHA256

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







Les certificats

Les certificats

- Emis par une autorité de certification
  - CA : *Certificate Autority*
- 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 !

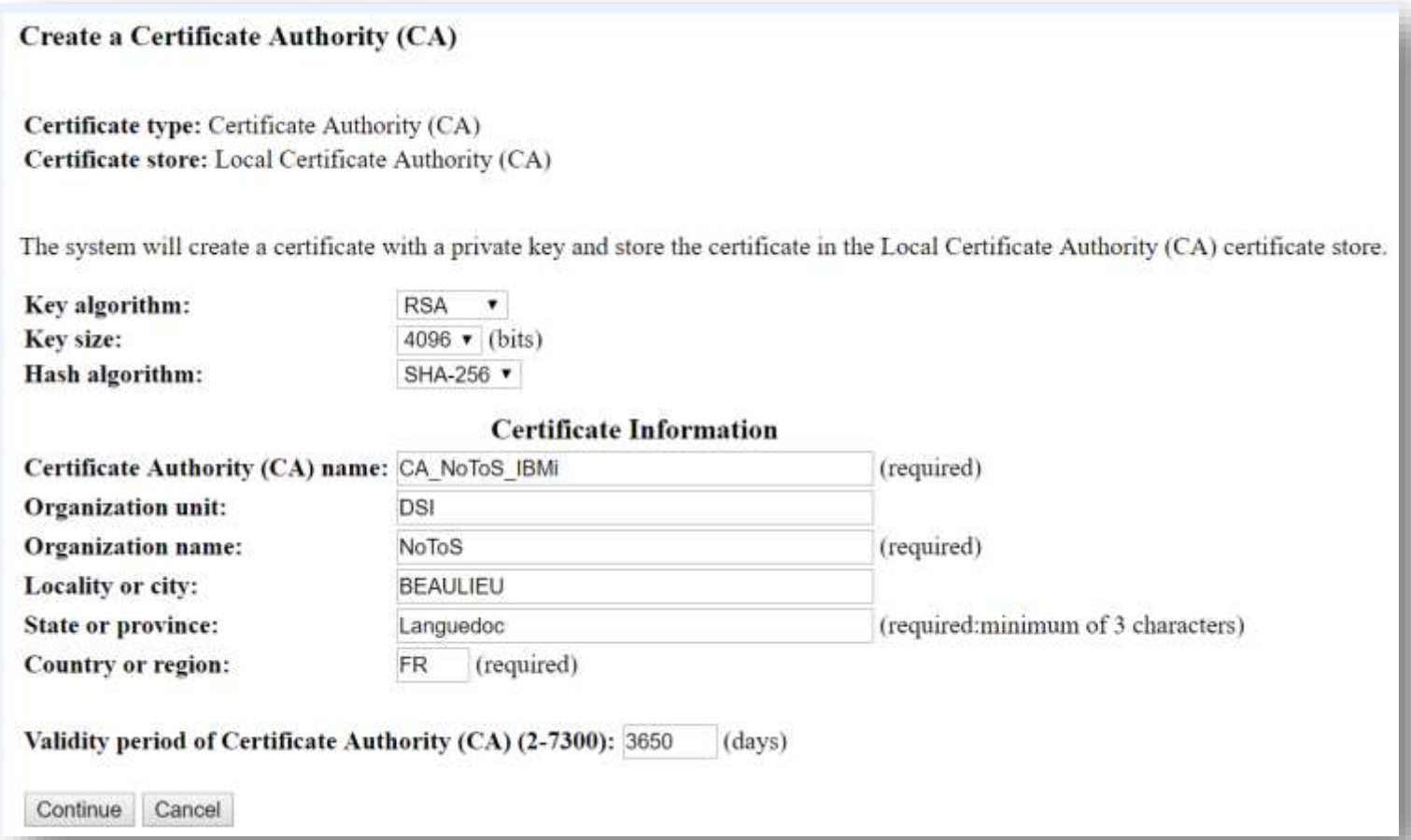
Les CA dignes de confiance

- 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

DCM

- 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

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

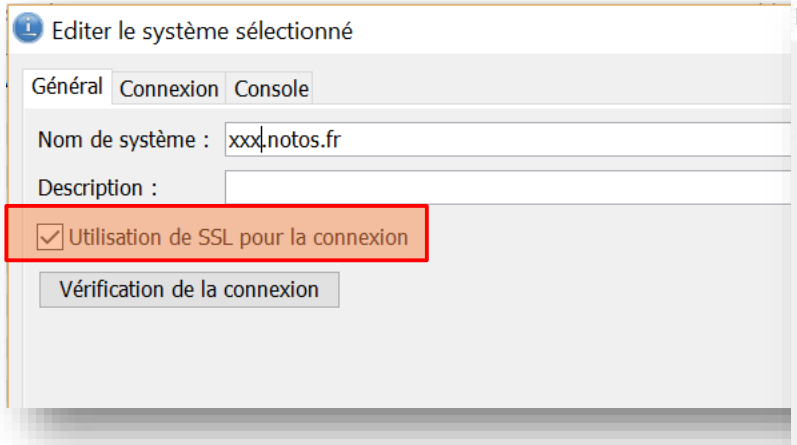
	Application	Type	Assigned certificate
☐	Central Server	Server	Scorpion
☐	Database Server	Server	Scorpion
☐	Data Queue Server	Server	Scorpion
☐	Network Print Server	Server	Scorpion
☐	Remote Command Server	Server	Scorpion
☐	Signon Server	Server	Scorpion
☑	IBM i TCP/IP Telnet Server	Server	Scorpion
☐	IBM i TCP/IP Telnet Client	Client	Scorpion
☐	Serveur IBM i DDM/DRDA - TCP/IP	Server	Scorpion
☐	Client IBM i DDM/DRDA - TCP/IP	Client	Scorpion

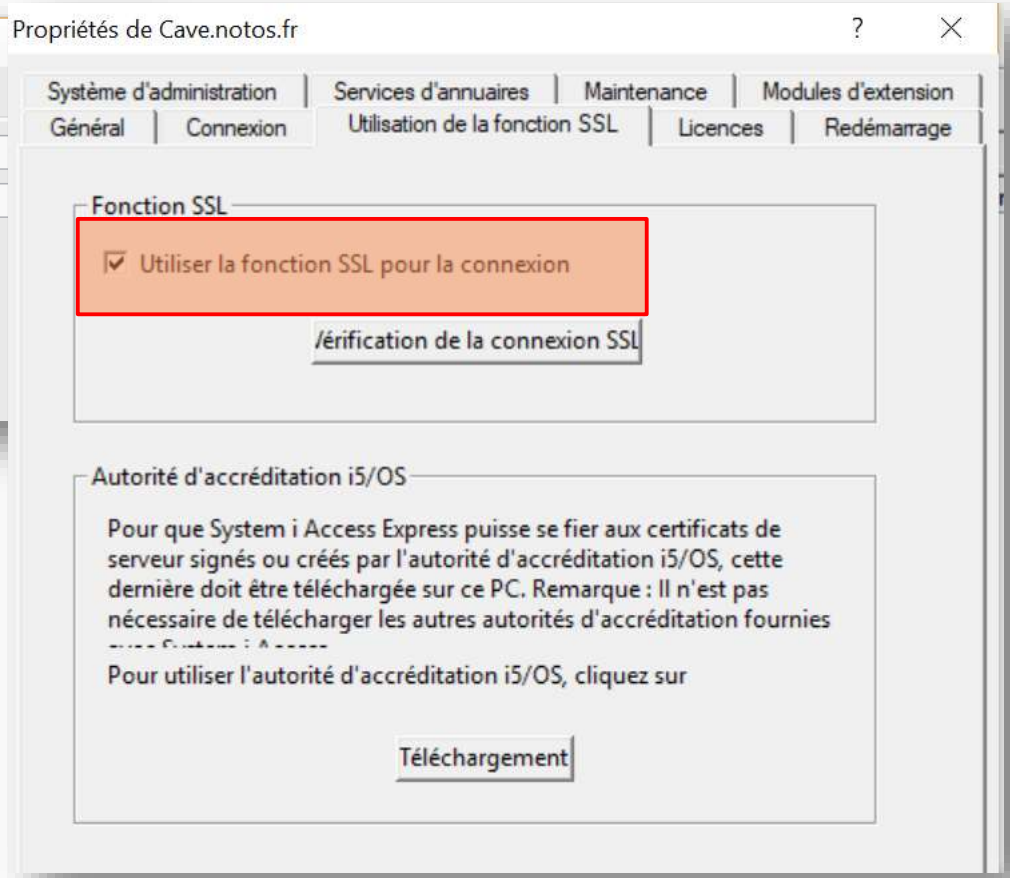
Utilisation de SSL

ACS et Client Access

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

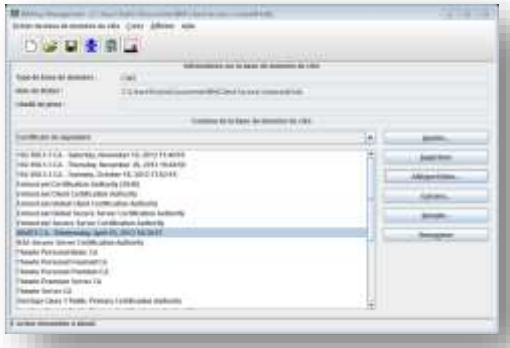
Configuration au niveau de la connexion





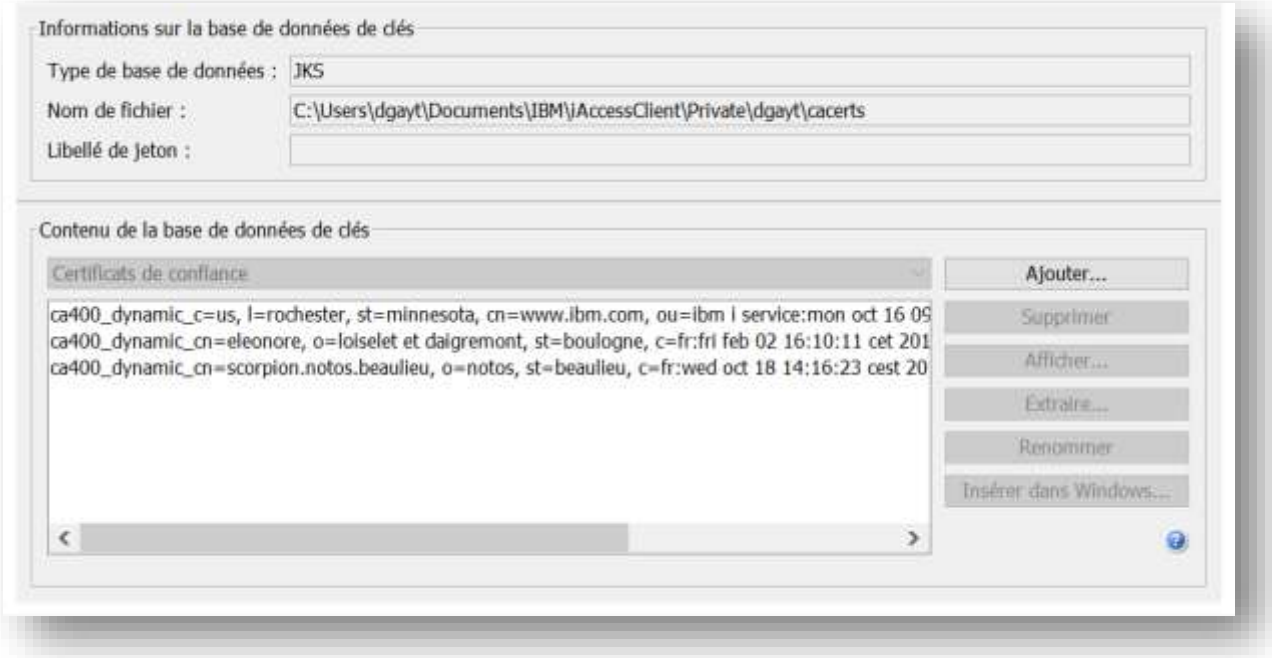
Magasin de certificats

- 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
    - **cwbssldf.kdb** c'est la base de données de clés
    - **cwbssljavaca.jck** c'est le fichier de clé utilisé par JDBC
    - **cwbssldf.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



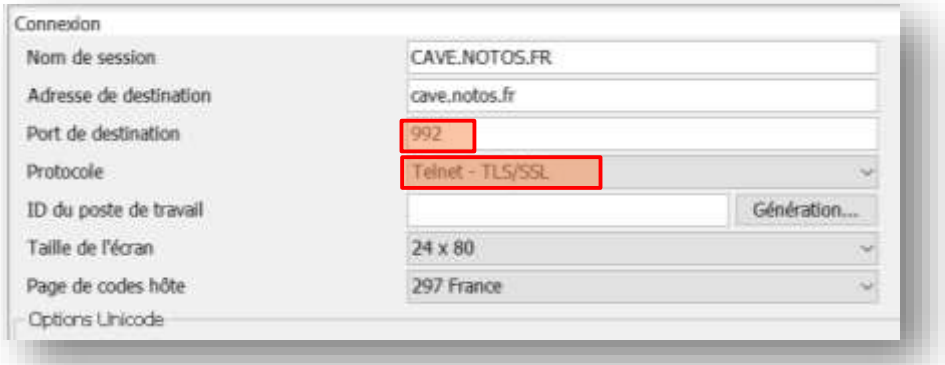
Magasin de certificats (2)

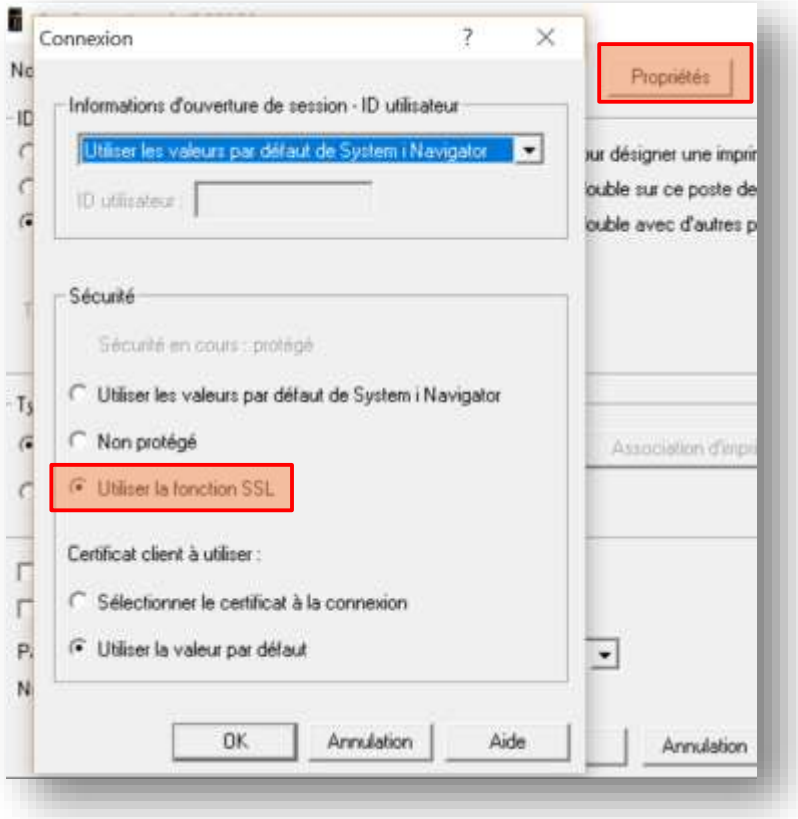
- ACS
  - Accessible à partir de l'interface (Outils/Gestion des clés)
  - Est propagé dans l'export/import de configuration



Emulation écran

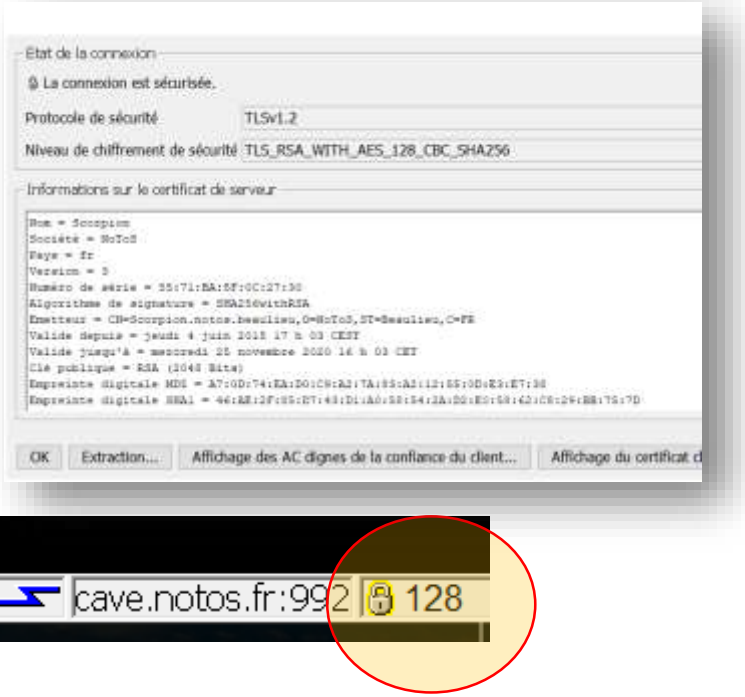
- Pour configurer une session en particulier

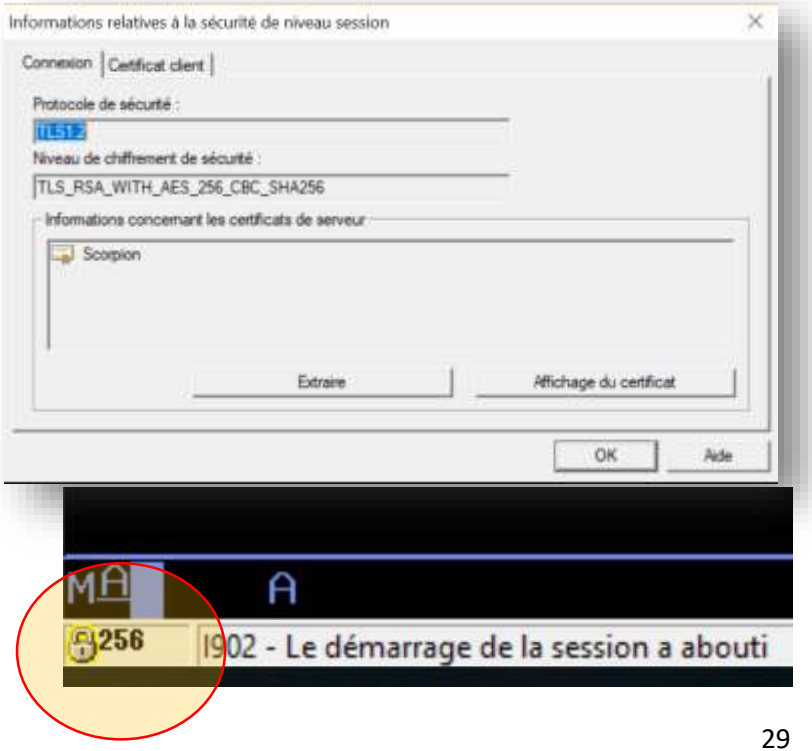




Informations de Sécurité

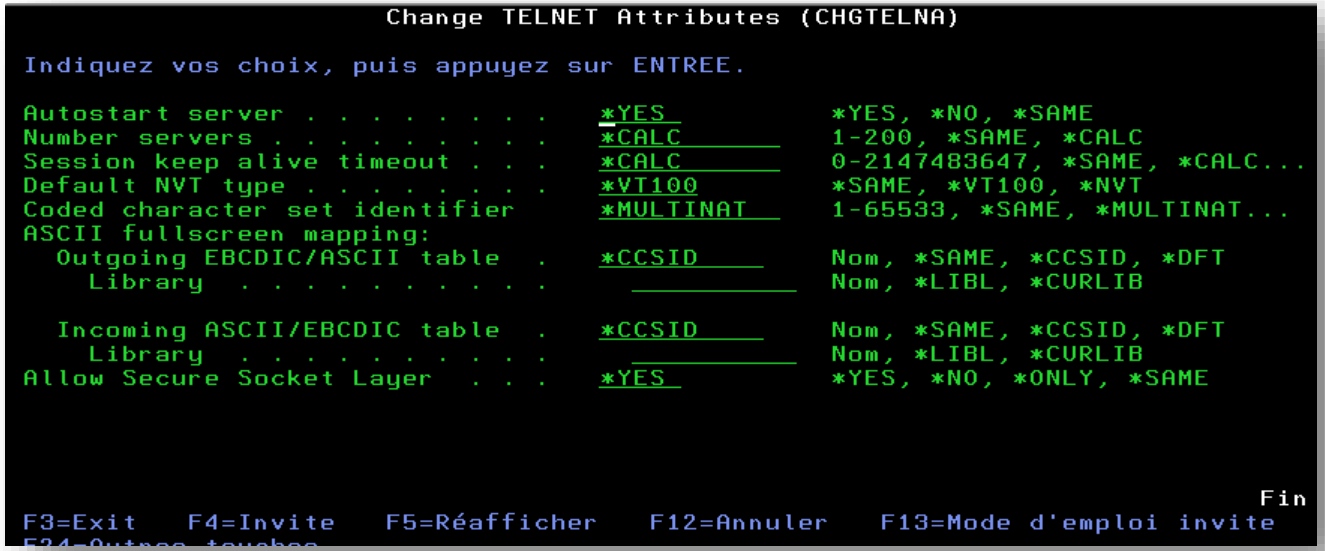
- Comparable entre ACS et Client access





Configuration du serveur TELNET

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



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