

S28 - La mise en œuvre de SSL afin de sécuriser les connexions avec un IBM i



Dominique GAYTE- dgayte@notos.fr

04 67 86 09 08 – 06 30 17 02 55

www.notos.fr

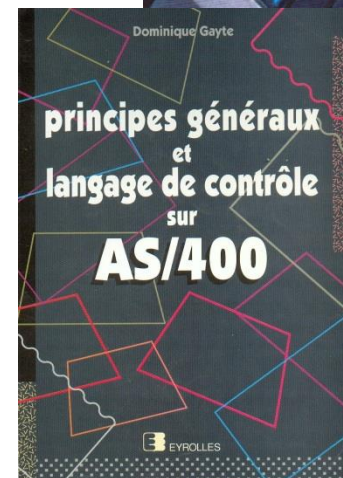
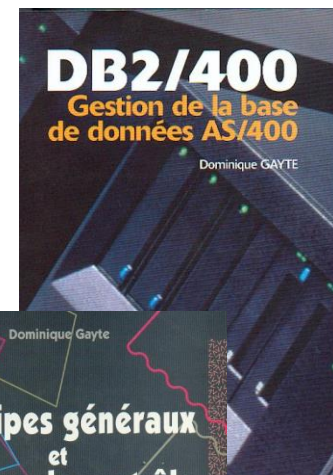
NoToS



- ❑ Expertise autour de l'IBM i
 - ❑ Plus de 20 ans d'expérience sur AS/400
 - ❑ Regard moderne
 - ❑ PHP sur IBM i
 - ❑ DB2 Web Query

- ❑ Développement de progiciels
 - ❑ PHP

- ❑ Fourni des solutions et des services autour de IBM i, PHP et de Zend



Le contexte

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

- Un simple test !
 - FTP vers un IBM i
 - Traces avec IP Tools (par exemple)
 - ID et PWD en clair
 - En TELNET (PC5250) à peine plus complexe
 - EBCDIC

FTP

IP Tools 1.99.3.0 By Erwan L. / RunAs : XPMUSER

File Edit View Capture Tools Help

192.168.1.36

Time	Source	Destination	Prot.	Len.	Src Port	Dest Port
11:46:05.016	192.168.1.36	192.168.1.3	TCP	48	3917	21
11:46:05.026	192.168.1.3	192.168.1.36	TCP	44	21	3917
11:46:05.026	192.168.1.36	192.168.1.3	TCP	40	3917	21
11:46:05.086	192.168.1.3	192.168.1.36	TCP	75	21	3917
11:46:05.226	192.168.1.36	192.168.1.3	TCP	40	3917	21
11:46:05.266	192.168.1.3	192.168.1.36	TCP	96	21	3917
11:46:05.426	192.168.1.36	192.168.1.3	TCP	40	3917	21
11:46:09.843	192.168.1.36	192.168.1.3	TCP	54	3917	21
11:46:09.843	192.168.1.3	192.168.1.36	TCP	61	21	3917
11:46:10.034	192.168.1.36	192.168.1.3	TCP	40	3917	21
11:46:12.798	192.168.1.36	192.168.1.3	TCP	51	3917	21
11:46:13.018	192.168.1.3	192.168.1.36	TCP	40	21	3917
11:46:17.886	192.168.1.3	192.168.1.36	TCP	86	21	3917
11:46:18.046	192.168.1.36	192.168.1.3	TCP	40	3917	21
11:46:21.351	192.168.1.36	192.168.1.3	TCP	46	3917	21
11:46:21.351	192.168.1.3	192.168.1.36	TCP	40	21	3917
11:46:21.361	192.168.1.3	192.168.1.36	TCP	71	21	3917
11:46:21.361	192.168.1.3	192.168.1.36	TCP	40	21	3917
11:46:21.361	192.168.1.36	192.168.1.3	TCP	40	3917	21
11:46:21.361	192.168.1.36	192.168.1.3	TCP	40	3917	21

0x00: 4500 0036 52C3 4000 8006 2487 C0A8 0124 . . 6R. @ . . \$ \$
 0x10: C0A8 0103 0F4D 0015 301C 8BF3 E68F EA0C *M. \$0.
 0x20: 5018 FFA4 8B2B 0000 5553 4552 2071 7365 P. USER qse
 0x30: 636F 6672 0D0A cof r

Frames : 20, Bytes : 1032, Bytes / sec. : 19, Frames / sec. : 0

ip proto 6 and port 21

IP
 - Version:4
 - Header len.:20
 - Total len.:54
 - ID:\$52C3
 + fragmentation
 - TTL:128
 - Protocol:\$06 (TCP)
 - Checksum:\$2487
 - Source IP:192.168.1.36
 - Dest. IP:192.168.1.3

TCP
 - src_port:3917
 - dest_port:21
 - seq_number:807177203
 - ack_number:3868191244
 - data_offset5
 + flags (PUSH)
 - window:65444
 - checksum:\$8B2B
 - urgent_pointer:\$00

FTP
 - USER qsecofr

IP Tools 1.99.3.0 By Erwan L. / RunAs : XPMUSER

File Edit View Capture Tools Help

192.168.1.36

Time	Source	Destination	Prot.	Len.	Src Port	Dest Port
11:46:13.018	192.168.1.3	192.168.1.36	TCP	40	21	3917
11:46:17.886	192.168.1.3	192.168.1.36	TCP	86	21	3917
11:46:18.046	192.168.1.36	192.168.1.3	TCP	40	3917	21
11:46:21.351	192.168.1.36	192.168.1.3	TCP	46	3917	21
11:46:21.351	192.168.1.3	192.168.1.36	TCP	40	21	3917
11:46:21.361	192.168.1.3	192.168.1.36	TCP	71	21	3917
11:46:21.361	192.168.1.3	192.168.1.36	TCP	40	21	3917
11:46:21.361	192.168.1.36	192.168.1.3	TCP	40	3917	21
11:46:21.361	192.168.1.36	192.168.1.3	TCP	40	3917	21
11:46:21.361	192.168.1.36	192.168.1.3	TCP	51	3917	21

0x00: 4500 0033 52E5 4000 8006 2468 C0A8 0124 . . 3R. @ . . \$ \$
 0x10: C0A8 0103 0F4D 0015 301C 8C01 E68F EA21 *M. \$0.
 0x20: 5018 FF8F E3FD 0000 5041 5353 2074 6F74 P. PASS t ot
 0x30: 6F0D 0A o

Frames : 20, Bytes : 1032, Bytes / sec. : 19, Frames / sec. : 0

ip proto 6 and port 21

IP
 - Version:4
 - Header len.:20
 - Total len.:51
 - ID:\$52E5
 + fragmentation
 - TTL:128
 - Protocol:\$06 (TCP)
 - Checksum:\$2468
 - Source IP:192.168.1.36
 - Dest. IP:192.168.1.3

TCP
 - src_port:3917
 - dest_port:21
 - seq_number:807177217
 - ack_number:3868191265
 - data_offset5
 + flags (PUSH)
 - window:65423
 - checksum:\$E3FD
 - urgent_pointer:\$00

FTP
 - PASS toto

Telnet

IP Tools 1.99.3.0 By Erwan L. / RunAs : XPMUSER

Time	Source	Destination	Prot.	Len.	Src Port	Dest Port
12:07:53.442	192.168.1.3	192.168.1.36	TCP	40	8476	3936
12:07:53.442	192.168.1.36	192.168.1.3	TCP	48	3937	23
12:07:53.442	192.168.1.3	192.168.1.36	TCP	44	23	3937
12:07:53.442	192.168.1.36	192.168.1.3	TCP	40	3937	23
12:07:53.442	192.168.1.3	192.168.1.36	TCP	46	23	3937
12:07:53.442	192.168.1.36	192.168.1.3	TCP	46	3937	23
12:07:53.442	192.168.1.3	192.168.1.36	TCP	71	23	3937
12:07:53.442	192.168.1.36	192.168.1.3	TCP	138	3937	23
12:07:53.442	192.168.1.3	192.168.1.36	TCP	52	23	3937
12:07:53.452	192.168.1.36	192.168.1.3	TCP	52	3937	23
12:07:53.452	192.168.1.3	192.168.1.36	TCP	115	23	3937
12:07:53.452	192.168.1.3	192.168.1.36	TCP	544	23	3937
12:07:53.452	192.168.1.36	192.168.1.3	TCP	40	3937	23
12:08:03.567	192.168.1.23	192.168.1.255	UDP	78	137	137
12:08:04.328	192.168.1.23	192.168.1.255	UDP	78	137	137
12:08:05.069	192.168.1.23	192.168.1.255	UDP	78	137	137
12:08:08.965	192.168.1.36	192.168.1.3	TCP	72	3937	23
12:08:08.965	192.168.1.3	192.168.1.36	TCP	583	23	3937
12:08:09.085	192.168.1.36	192.168.1.3	TCP	40	3937	23
12:08:10.708	192.168.1.1	255.255.255.255	UDP	328	67	68
12:08:13.011	192.168.1.1	255.255.255.255	UDP	328	67	68

```

0x00: 4500 0048 E8E3 4000 8006 8E54 C0A8 0124  E..H..@...T...$
0x10: C0A8 0103 DF61 0017 5C8E E504 F0BA A442  ....*a.\.....B
0x20: 5018 FD8B FEF5 0000 001E 12A0 0000 0400  P.....
0x30: 0003 073B F111 0635 E4E2 C5D9 F111 0735  .....5.....5
0x40: 4D6  D5D7 E6C4 FFEF  .....
    
```

USER1

MONPWD

Frames : 46, Bytes : 6133, Bytes / sec. : 180, Frames / sec. : 1

C1	A
C2	B
C3	C
C4	D
C5	E
C6	F
C7	G
C8	H
C9	I
CA	
CB	
CC	non-displayable
CD	
CE	non-displayable
CF	
D0	}
D1	J
D2	K
D3	L
D4	M
D5	N
D6	O
D7	P
D8	Q
D9	R
DA	
DB	
DC	
DD	
DE	
DF	
E0	\
E1	
E2	S
E3	T
E4	U
E5	V
E6	W
E7	X
E8	Y
E9	Z



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)

Les protocoles

- Généralement des protocoles spécifiques sont utilisés
 - HTTPS, FTPS...
 - SSH, SFTP (implémentation particulière sur IBM i)
 - Sur des ports spécifiques

modèle OSI	pile de protocoles
7 - couche application	HTTP, SMTP, FTP, SSH, IRC, SNMP, SIP ...
6 - couche de présentation	
5 - couche de session	TLS, SSL, SSH-user, NetBIOS
4 - couche de transport	TLS, SSL, TCP, UDP, SCTP, RTP, DCCP ...
3 - couche réseau	IPv4, IPv6, ARP, IPX ...
2 - couche de liaison	Ethernet, 802.11 WiFi, Token ring, FDDI, ...
1 - couche physique	Câble, fibre optique, ondes radio...

SSL dans l'IBM i

- V7R1 TR 6 : support de TLS 1.2
- Tous les outils en standard
 - DCM Digital Certificate Manager
 - 5770SS1 option 34 en V7R1
 - Serveur Web d'administration
 - Administration générale via le Web
 - IBM Web Administration for i
 - Administration des serveurs Web
- IBM i Access for Windows et System i Navigator
 - Toutes les fonctions supportent SSL
- IBM Portable Utilities for i
 - 5733SC1
 - SSH, SFTP

Les certificats

- Emis par une autorité de certification
 - *CA Certificate Authority*
 - *Soit officielles (accréditées)*
 - *CyberTrust, Verisign...*
 - *Vendent les certificats et assurent leurs validités*
 - *Soit privées (locales)*
 - *Certificats émis sont gratuits*
 - *Mais non reconnus comme surs, il faudra les définir comme étant de confiance sur les postes clients*

- *L'IBM i peut être une CA et émettre tous les certificats dont nous auront besoin*
 - *Idéal dans le cas d'une utilisation interne*

Les certificats (2)

- Caractéristiques
 - Longueur de clé
 - Common name
 - Numéro de série

- Contenus dans des magasins de certificats
 - Dans l'IFS de l'IBM i
 - /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB (System)
 - Dans Client Access
 - Dans Windows

Organisation avec une CA locale dans l'IBM i

1. Créer une CA locale sur l'IBM i
2. Créer les certificats et les associer aux applications
3. Configurer les applications
4. Eventuellement, configurer les clients afin de faire confiance à la CA locale de l'IBM i
 1. Web
 2. IBM i Client (Telnet, FTP...) SSL d'un autre IBM i

DCM

- Outil de gestion des certificats
- Interface Web
 - port 2001 de l'IBM i
 - 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 (dans Configurations Internet)

Digital Certificate Manager

Select a Certificate Store

Expand All Collapse All

- 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 Tasks](#)

Secure Connection

5769-NC1, 5769-NCE, 5769-SS1, 5722-SS1, 5761-SS1, 5770-SS1 (C) Copyright IBM Corporation 1997, 2009
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

Création de la CA locale

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 size:

4096 ▾ (bits)

Certificate store password:

•••••••• (required)

Confirm password:

•••••••• (required)

Certificate Information

Certificate Authority (CA) name: NoToS (required)

Organization unit:

DSI

Organization name:

NoToS (required)

Locality or city:

BEAULIEU

State or province:

34160 (required: minimum of 3 characters)

Country or region:

FR (required)

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

Continue

Cancel

Création de la CA locale (2)

- Eventuellement définir les applications acceptant la CA locale (trust)

Install Local CA Certificate

Certificate type: Certificate Authority (CA)

Certificate store: Local Certificate Authority (CA)

A certificate for your Certificate Authority (CA) was created.

You must install the Certificate Authority (CA) certificate in your browser. Your web browser will then trust the certificate in your browser. Your web browser will then trust the certificate in your browser.

[Install certificate](#)

After installing the certificate, select Continue so you can continue.

Continue

Cancel

Certificate Authority (CA) Policy Data

Your Certificate Authority (CA) was created with the default policy data shown below.

Allow creation of user certificates: Yes No

Validity period of certificates that are issued by this Certificate Authority (CA) (1-2000): (days)

Days until Certificate Authority (CA) expires: 3000

Continue

Cancel

Message The applications you selected will trust this Certificate Authority (CA).

Création de la CA locale (3)

View Certificate Authority (CA)

Certificate type: Certificate Authority (CA)

Certificate store: Local Certificate Authority (CA)

Certificate label: LOCAL_CERTIFICATE_AUTHORITY_1017A0R1(18)

Subject:

Common name	CA NoToS
Organization unit	DSI
Organization name	NoToS
Locality or city	BEAULIEU
State or province	34160
Zip or postal code	
Country or region	FR

Additional information:

Private key	Yes
Certificate Authority (CA) enabled	Yes
Signed certificate	Yes
Serial number	515C3032
Validity period	04/02/13 03:35:46 - 06/20/21 03:35:46

Private key information:

Key length	4096
Storage location	Stored in software

Issuer:

Common name	CA NoToS
Organization unit	DSI
Organization name	NoToS
Locality or city	BEAULIEU
State or province	34160
Zip or postal code	
Country or region	FR

Création de certificats

- Se connecter sur le magasin System

Certificate Store and Password

Enter the certificate store password.

Certificate type: Server or client
Certificate store: *SYSTEM
Certificate store path and filename: /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB
Certificate store password:

- Créer un certificat Server certifié par la CA locale

Création de certificats (2)

- Pour Client Access

Create Certificate

Certificate type: Server or client

Certificate store: *SYSTEM

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

Key size: (bits)

Certificate label: (required)

Certificate Information

Common name: (required)

Organization unit:

Organization name: (required)

Locality or city:

State or province: (required: minimum of 3 characters)

Country or region: (required)

Association à une application

- Associer le certificat aux applications (ici Client Access)

	Application	Type	Assigned certificate
<input checked="" type="checkbox"/>	Central Server	Server	<i>None assigned</i>
<input checked="" type="checkbox"/>	Database Server	Server	<i>None assigned</i>
<input checked="" type="checkbox"/>	Data Queue Server	Server	<i>None assigned</i>
<input type="checkbox"/>	Network Print Server	Server	<i>None assigned</i>
<input checked="" type="checkbox"/>	Remote Command Server	Server	<i>None assigned</i>
<input checked="" type="checkbox"/>	Signon Server	Server	<i>None assigned</i>
<input type="checkbox"/>	IBM i TCP/IP Telnet Server	Server	<i>None assigned</i>
<input type="checkbox"/>	IBM i TCP/IP Telnet Client	Client	<i>None assigned</i>
<input type="checkbox"/>	Serveur i5/OS DDM/DRDA - TCP/IP	Server	<i>None assigned</i>
<input type="checkbox"/>	Client i5/OS DDM/DRDA - TCP/IP	Client	<i>None assigned</i>
<input type="checkbox"/>	Cluster Security	Server	<i>None assigned</i>
<input checked="" type="checkbox"/>	Host Servers	Server	<i>None assigned</i>
<input checked="" type="checkbox"/>	File Server	Server	<i>None assigned</i>
<input checked="" type="checkbox"/>	Serv gestion centralisée	Server	<i>None assigned</i>
<input type="checkbox"/>	IBM Tivoli Directory Server	Server	<i>None assigned</i>

Pour les serveurs Web

- Le Common name doit être le constituant principal de l'URL
- Pour le site mante.notos.fr

Create Certificate

Certificate type: Server or client

Certificate store: *SYSTEM

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

Key size: (bits)

Certificate label: (required)

Certificate Information

Common name: (required)

Organization unit:

Organization name: (required)

Locality or city:

State or province: (required: minimum of 3 characters)

Country or region: (required)

Pour les serveurs Web (2)

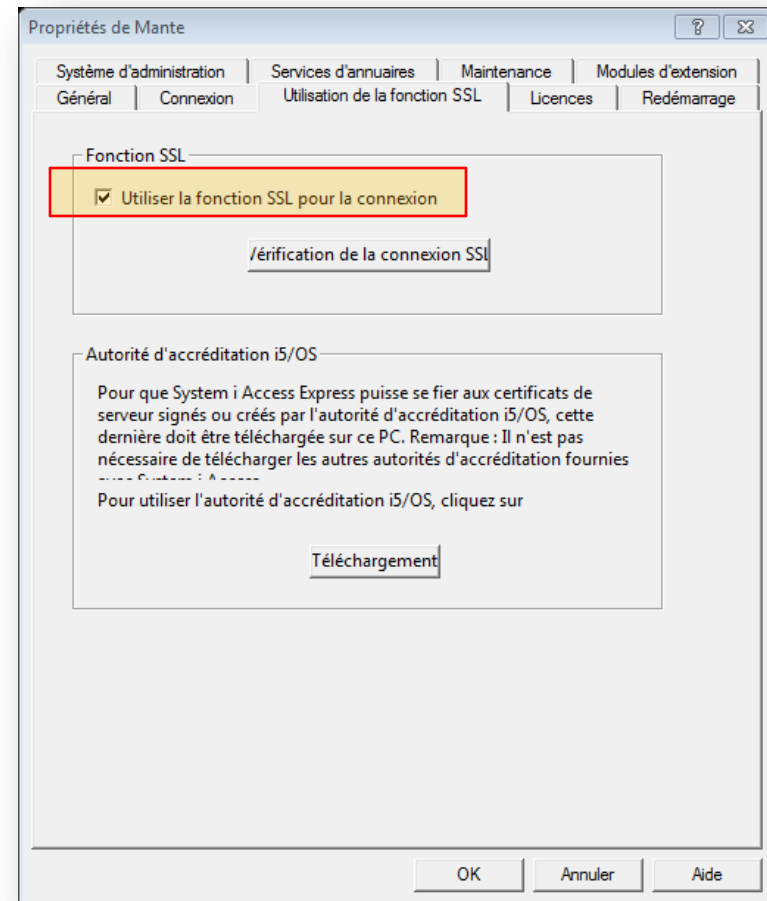
- Associer à l'application correspondant au site Web sélectionné

<input type="checkbox"/>	IBM i TCP/IP FTP Client	Client	<i>None assigned</i>
<input type="checkbox"/>	IBM i TCP/IP POP Server	Server	<i>None assigned</i>
<input checked="" type="checkbox"/>	QIBM_HTTP_SERVER_APACHEDFT	Server	<i>None assigned</i>
<input type="checkbox"/>	QIBM_HTTP_SERVER_ADMIN	Server	<i>None assigned</i>
<input type="checkbox"/>	QIBM_HTTP_SERVER_TESTSSL	Server	<i>None assigned</i>
<input type="checkbox"/>	QIBM_HTTP_SERVER_ADMIN1	Server	<i>None assigned</i>
<input type="checkbox"/>	QIBM_DIRECTORY_SERVER_QUSRDIR	Server	<i>None assigned</i>
<input type="checkbox"/>	QIBM_HTTP_SERVER_WQLWI77	Server	<i>None assigned</i>

Configuration de Client Access

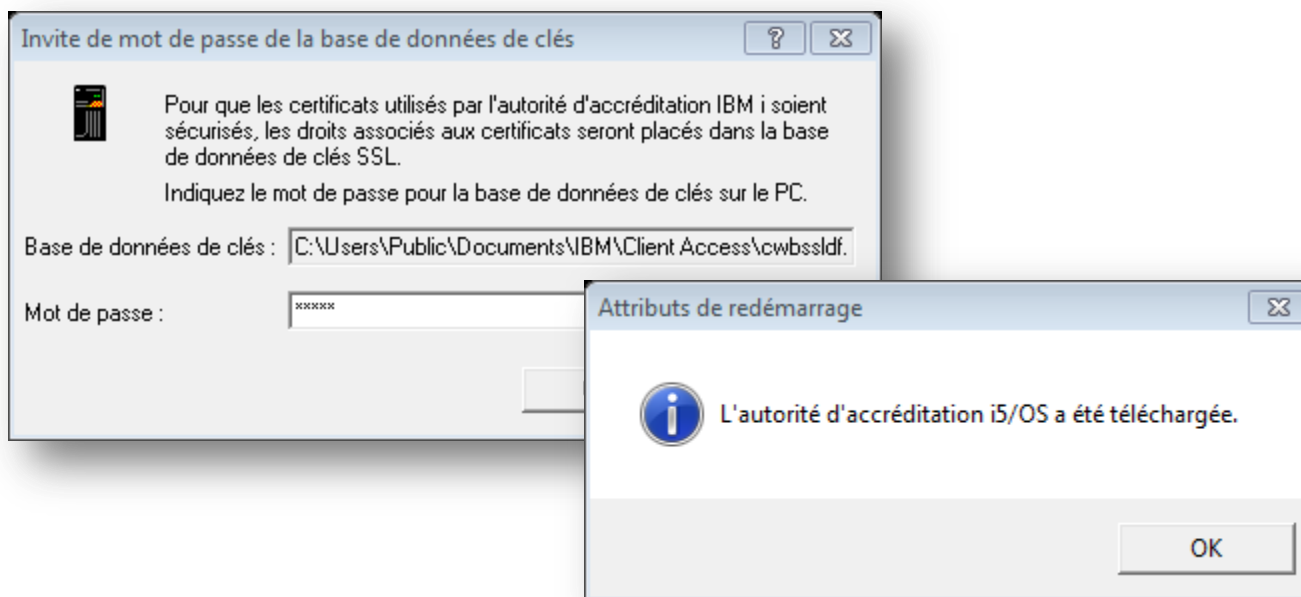
■ Dans System i Navigator

- Sur la connexion choisie, Propriétés, onglet Utilisation de la fonction SSL
- Si option installée !



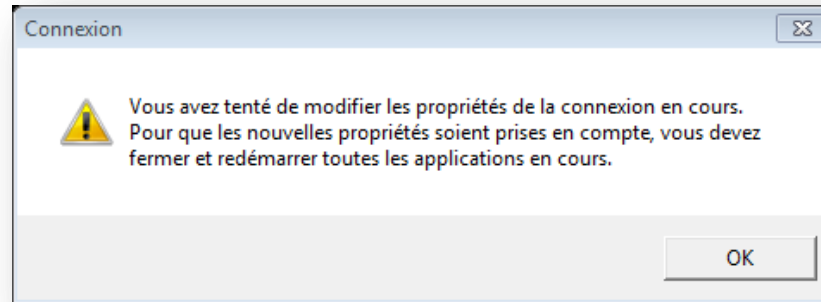
Magasin de certificat de CA/400

- Cliquer sur Téléchargement afin de redescendre le certificat de la CA locale dans le magasin de CA/400
- Le mot de passe par défaut du magasin est **ca400**

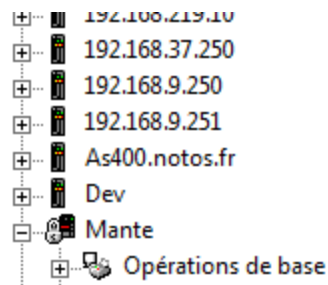


Magasin de certificat de CA/400 (2)

- Redémarrer IBM i Navigator



- Remarquer l'icone avec un cadenas

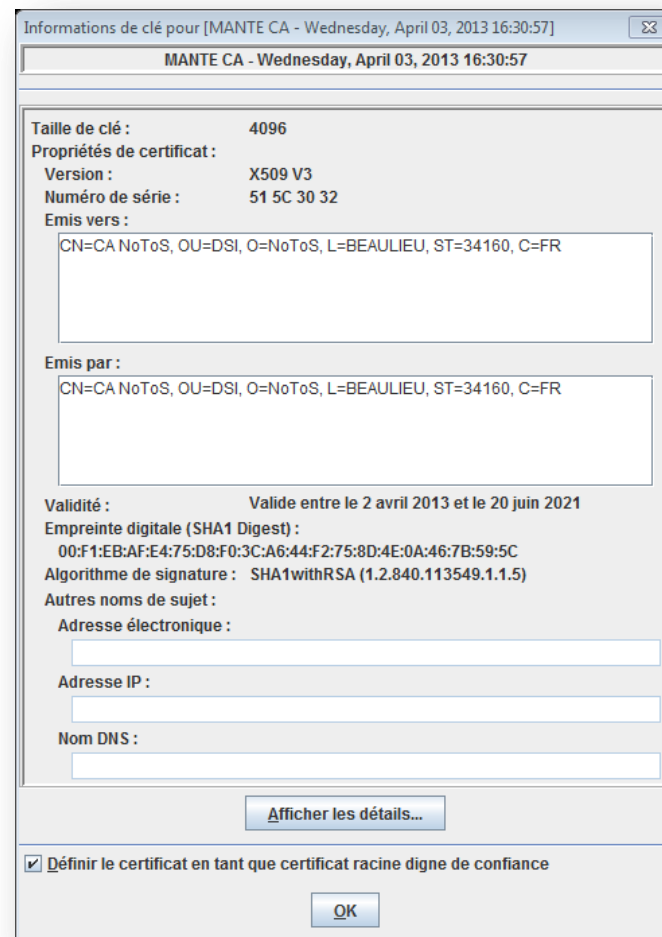
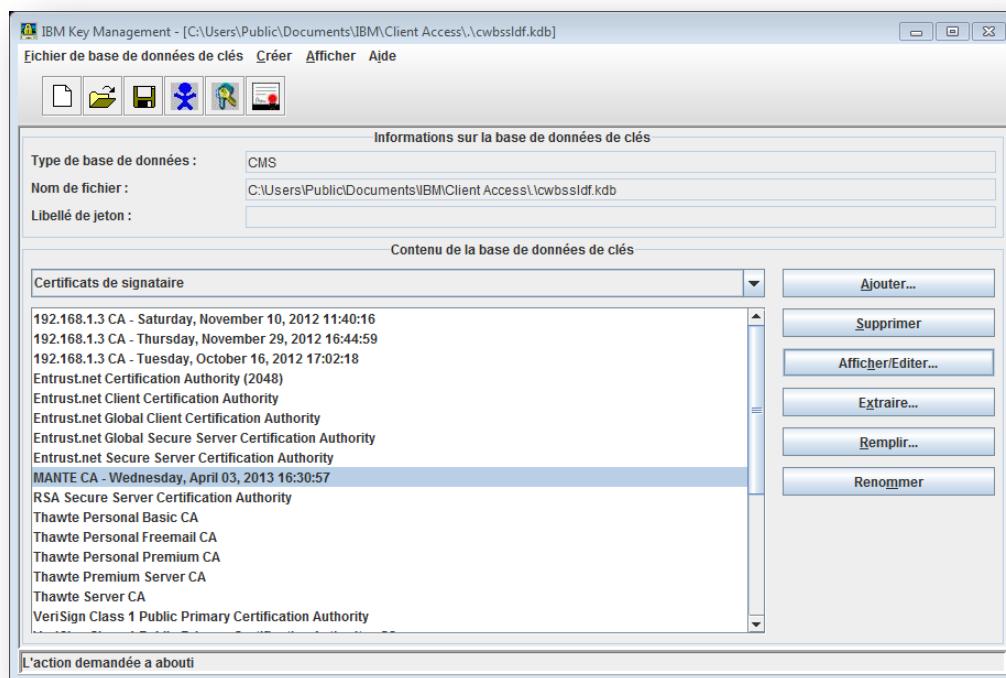


Magasin de certificat de CA/400 (4)

- 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

Magasin de certificat de CA/400 (5)

- Utilitaire de gestion des clés
 - IBM Key Management



TELNET

- Associer un certificat au serveur TELNET

- Celui de CA/400 ou un autre

<input type="radio"/>	IBM i TCP/IP Telnet Server	CA400
-----------------------	----------------------------	-------

- Faire reconnaître la CA Locale à l'application si ce n'est déjà fait (Define CA trust list)

Trusted	Certificate Authority (CA)		
<input checked="" type="checkbox"/>	LOCAL_CERTIFICATE_AUTHORITY_1017A0R1(18)	View	Validate

- Redémarrer le serveur Telnet (avec System i Navigator. **Attention à la perte de tous les écrans 5250 !**)
- Configurer les émulations écran et les démarrer

Session 5250

■ Configuration sur le port 992

Configuration de PC5250

Nom de système : MANTE

ID poste de travail

- Utiliser le nom de l'ordinateur
- Utiliser le nom utilisateur Windows
- Indiquer un ID poste de travail

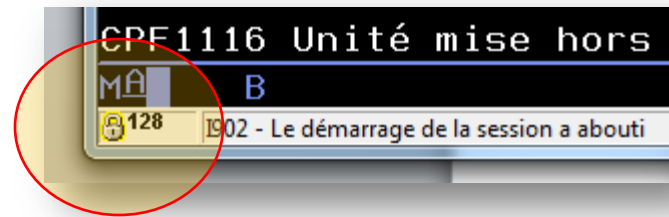
Tronquer : Caractères de début Caractères de fin

Type d'émulation

- Ecran
- Imprimante

Page de codes hôte : 1147 France (Euro)

Numéro de port : 992



Informations relatives à la sécurité de niveau session

Connexion Certificat client

Protocole de sécurité : TLS1.0

Niveau de chiffrement de sécurité : TLS_RSA_WITH_AES_128_CBC_SHA

Informations concernant les certificats de serveur

- CA400

Extraire Affichage du certificat

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

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

```

Netstat *CNN

```

Session B - [24 x 80]
Fichier  Edition  Vue  Communication  Actions  Fenêtre  Aide

Work with IPv4 Connection Status
Systeme:  S1017A0R

Type options, press Enter.
 3=Enable debug  4=End  5=Display details  6=Disable debug
 8=Display jobs

Opt  Remote      Remote      Local      Idle Time  State
   Address      Port      Port
--  -----      -
_   192.168.1.20  36819     as-data >  000:19:26  Established
_   192.168.1.20  36821     as-rmtc >  000:18:04  Established
_   192.168.1.20  36823     as-data >  000:19:25  Established
_   192.168.1.20  36825     as-rmtc >  000:19:17  Established
_   192.168.1.20  36831     telnet      000:07:58  Established
_   192.168.1.20  36832     telnet- >  000:00:00  Established
_   192.168.1.20  36926     cifs        000:05:37  Established

Fin

F4=Prompt      F10=Display connection totals  F14=Display port numbers
F15=Subset     F16=Repeat position to        F17=Position to  F24=More keys

Mâ  B          MW          09/003
128 | 1902 - Le démarrage de la session a abouti

```

FTP

- Idem Telnet
- Client FTPS

```
Statut : Déconnecté du serveur
Statut : Connexion à 192.168.1.3:990...
Statut : Connexion établie, initialisation TLS...
Statut : Vérification du certificat...
Statut : Connexion TLS/SSL établie, attente du message d'accueil...
Réponse : 220-QTCP at MANTE.NOTOS.BEAULIEU.
Réponse : 220 Connection will close if idle more than 5 minutes.
```

Certificat inconnu

Le certificat du serveur est inconnu. Examinez le certificat avec attention avant de faire confiance au serveur.

Chaîne de certificats : 0

Détails

Valable du : 02/04/2013
 Valable jusqu'à : 29/12/2015
 Numéro de série : 51:5c:37:7e:0b:4b:f8
 Algorithme de la clé publique : RSA avec 2048 bits
 Empreinte (MD5) : b3:90:56:d4:a5:9d:31:b7:2c:26:04:1b:56:5f:17
 Empreinte (SHA-1) : b5:19:08:20:a7:7e:95:99:de:39:f9:5f:18:3f:10

Objet du certificat	Émetteur du certificat
Nom commun : CA400	Nom commun : CA NoToS
Organisation : NoToS	Organisation : NoToS
Unité : DOI	Unité : DSI
Pays : FR	Pays : FR
État ou province : 34160	État ou province : 34160
Localité : BEAULIEU	Localité : BEAULIEU

Détails de session

Hôte : 192.168.1.3:990
 Chiffrement : AES-128-CBC
 MAC : SHA1

Approuver ce certificat et l'associer à la connexion ?

Toujours faire confiance à ce certificat lors des prochaines sessions.

OK Annuller

Gestionnaire de Sites

Sélectionnez une entrée :

- Mes Sites
 - 192.168.1.3
 - Mante
 - Nouveau site

Nouveau Site Nouveau Dossier

Nouveau Favori Renommer

Supprimer Copier

Général Avancé Paramètres de transfert Jeu de caractères

Hôte : 192.168.1.3 Port :

Protocole : FTP - Protocole de Transfert de Fichiers

Chiffrement : Connexion FTP implicite sur TLS

Type d'authentification : Demander le mot de passe

Identifiant : dgayte

Mot de passe :

Compte :

Commentaires :

Connexion OK Annuller

Serveur Web

- Configurer le serveur Web dans IBM Web Administration for i
 - HTTPxxx:2001/HTTPAdmin
- Attribuer un certificat à l'application dans DCM
- Intégrer le certificat de la CA locale dans le magasin Windows

Configuration du serveur Web

- Dans Security
 - Activer SSL
 - Associer une application

APACHEDEF > Security

Security ?

Authentication Control Access

SSL Proxy **SSL Proxy Advanced**

SSL with Certificate Authentication Control Certificate Access **SSL Advanced**

SSL: Enabled ?

Server certificate application name: QIBM_HTTP_SERVER_APACHEDF or... ?

Client certificates when establishing the connection: ?

Do not request client certificate for connection
 Accept client certificate if available before making connection
 Require client certificate for connection

- Dans General Server Configuration
 - Attribuer un port (443 ?)

Server IP addresses and ports to listen on: ?

	IP address	Port	Protocol
<i>Example</i>	<i>All IP addresses</i>	<i>80</i>	<i>http</i>
<input type="radio"/>	*	443	https

Add

Attribution du certificat à l'application

<input type="radio"/>	IBM i TCP/IP FTP Server	CA400
<input checked="" type="radio"/>	IBM i TCP/IP POP Server	<i>None assigned</i>
<input type="radio"/>	QIBM_HTTP_SERVER_APACHEDFT	WEB
<input type="radio"/>	QIBM_HTTP_SERVER_ADMIN	<i>None assigned</i>

Subject:

Common name	mante.notos.fr.
Organization unit	DOI
Organization name	NoToS
Locality or city	BEAULIEU
State or province	34160
Zip or postal code	
Country or region	FR

Additional information:

Private key	Yes
Signed certificate	Yes
Serial number	515C396E0AFF80
Validity period	04/02/13 04:15:10 - 12/29/15 03:15:10

Le magasin de certificat de Windows

■ Deux problèmes

1. Problème de sécurité



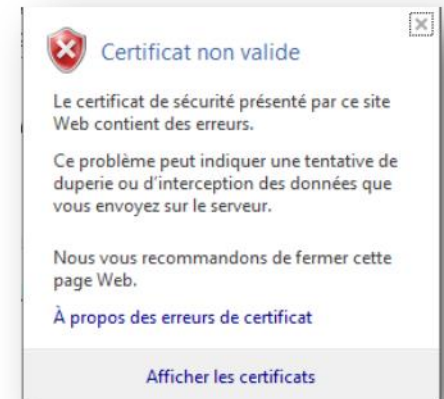
 Le certificat de sécurité de ce site Web présente un problème.


Le certificat de sécurité présenté par ce site Web a été émis pour une autre adresse de site Web.

Les problèmes de certificat de sécurité peuvent indiquer une tentative de duperie ou d'interception des données que vous envoyez sur le serveur.

Nous vous recommandons de fermer cette page Web et de quitter ce site.

-  Cliquez ici pour fermer cette page Web.
-  Poursuivre avec ce site Web (non recommandé).
-  Informations



 **Certificat non valide**

Le certificat de sécurité présenté par ce site Web contient des erreurs.

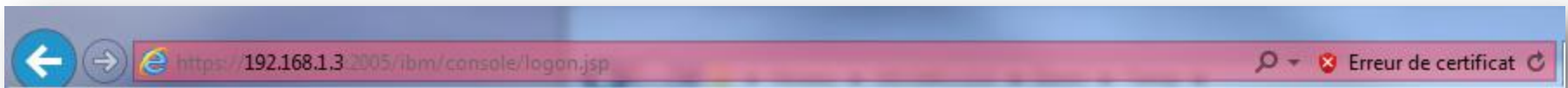
Ce problème peut indiquer une tentative de duperie ou d'interception des données que vous envoyez sur le serveur.


Nous vous recommandons de fermer cette page Web.

À propos des erreurs de certificat

[Afficher les certificats](#)

2. Erreur de certificat

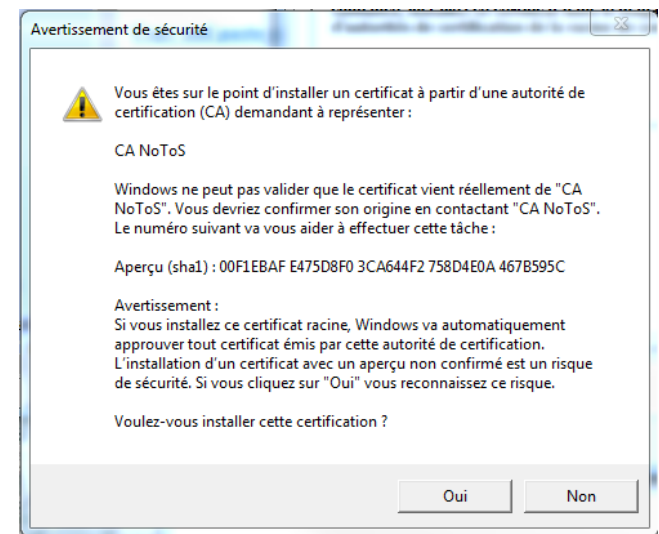
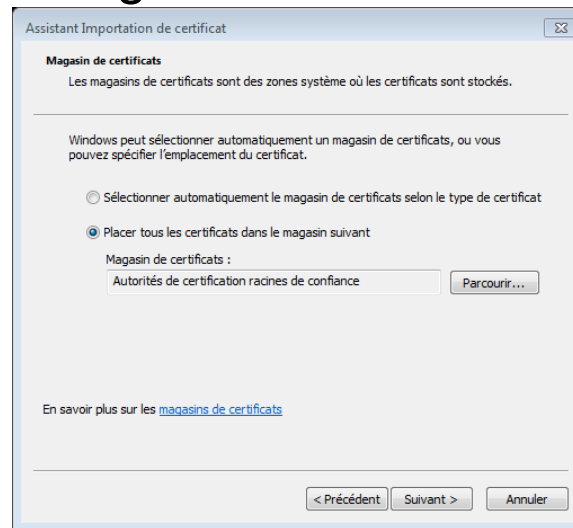
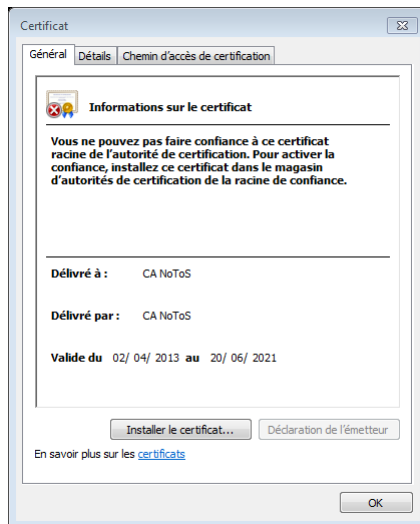


← →  <https://192.168.1.3:2005/ibm/console/login.jsp> 🔍  Erreur de certificat ↻

Problème de sécurité

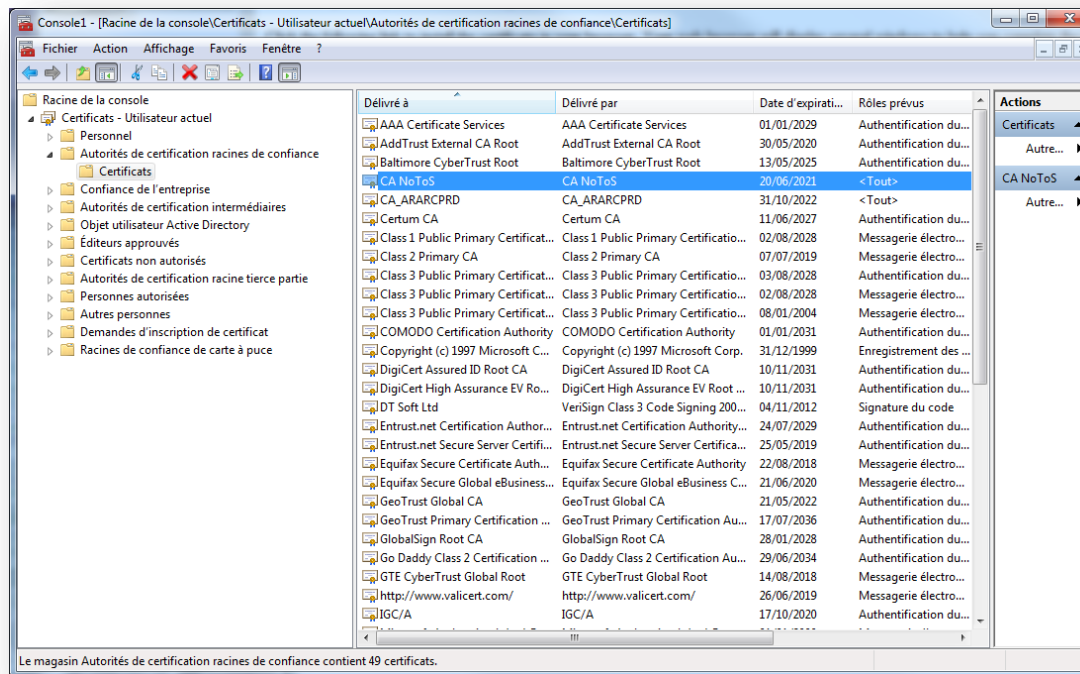
- Il faut que le certificat de la CA soit placé dans le magasin de certificat de Windows
- Dans « Autorité de certification racines de confiance »
- A partir de DCM
 - Copier le certificat en local
 - L'installer dans le magasin Windows

■ Install Local CA Certificate on Your PC



Le magasin de certificat de Windows

- À partir de MMC
- Installer le composant Certificats



- Les certificats de CA peuvent être déployés automatiquement avec les GPO de l'AD

Les serveurs utilisant SSL

- Interface d'administration
 - Peut être configurée pour ne fonctionner qu'en SSL
 - Administration (port 2001 => 2005)
 - DCM
 - IBM Web Administration for i

- POP, SMTP

- TIVOLI

- LDAP

- DRDA, DDM

- ...

S28 - La mise en œuvre de SSL afin de sécuriser les connexions avec un IBM i



Dominique GAYTE- dgayte@notos.fr

04 67 86 09 08 – 06 30 17 02 55

www.notos.fr