

## Processus d'authentification

L'authentification est l'étape la plus importante mise en œuvre lors des connexions établies entre des clients ou des serveurs avec un serveur Domino.

La bonne compréhension des différentes étapes permet ainsi de corriger tous les problèmes d'interconnexion entre les différents participants d'un site Domino/Lotus-Notes.

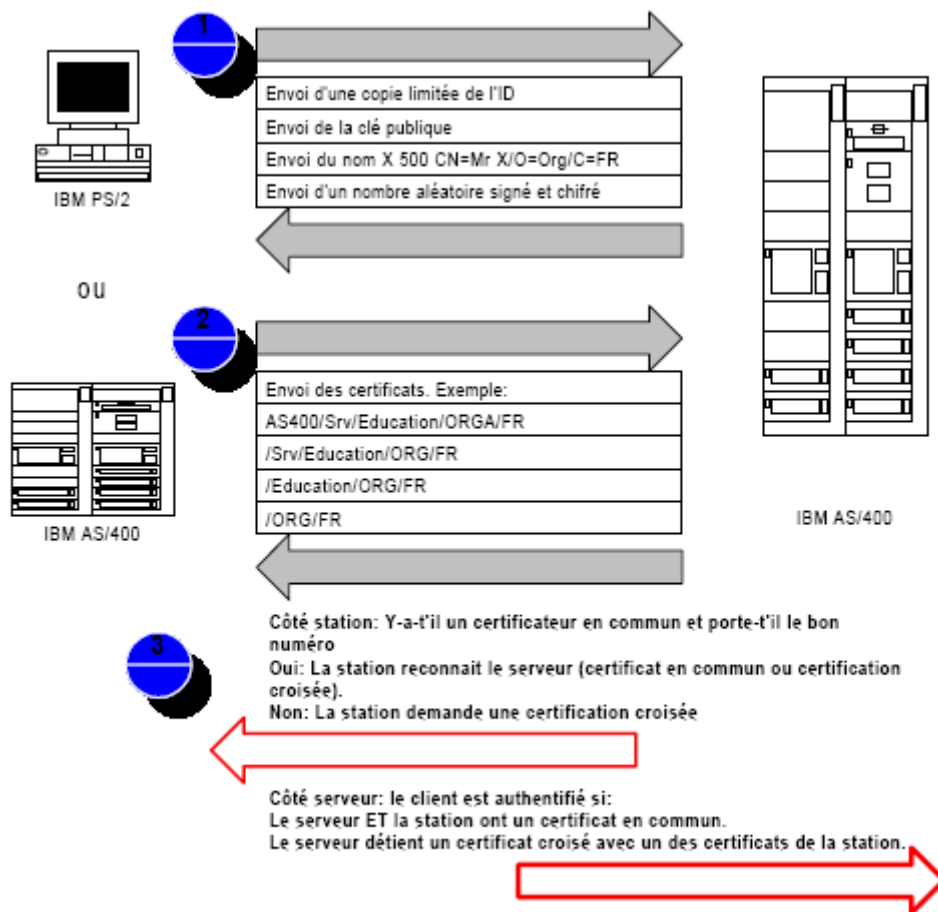
Les différentes étapes permettent ainsi d'éviter certaines erreurs lors de la création des certificats principaux. En effet, il n'est pas possible de se connecter entre clients et serveurs qui auraient un certificat de même nom mais différent. Le nom représente un contrôle pour Domino, il doit donc être unique.

Nous avons cette même contrainte avec les noms de domaine Internet.

Le mécanisme d'authentification est bi-directionnel, le serveur doit vous authentifier et le client doit pouvoir authentifier le serveur.

Lors de la connexion entre un client et un serveur, il est donc nécessaire au client de s'assurer de l'authenticité du serveur. Le chapitre sur les certifications croisées permettra de mieux assimiler cette notion fondamentale.

### Authentification - Etape 1: L'échange



Cette étape ne peut avoir lieu qu'après la saisie du mot de passe afin de pouvoir accéder aux certificats et clés publiques stockées dans le fichier ID de l'utilisateur ou du serveur.

La demande du mot de passe a lieu après connexion au serveur, dès que le client détecte le serveur sur le réseau, la station Lotus-Notes demande le mot de passe, ce qui permet ainsi de débiter l'étape d'authentification.

Les nombres sont chiffrés avec les clés publiques du destinataire, d'où l'échange des clés publiques.

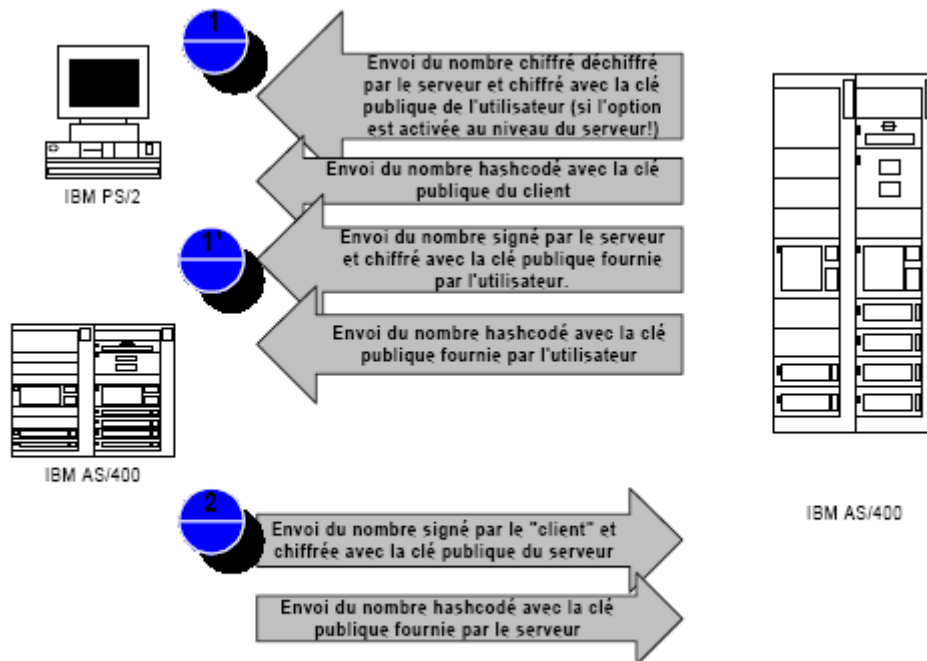
Seuls les détenteurs des clés privées peuvent déchiffrer les nombres aléatoires fournis. La clé publique est obligatoirement fournie pour permettre la vérification de la signature, en effet cette dernière est stockée dans le champ \$Signature, mais comme il y a un chiffrement, ce champ est inclus dans le champ \$SealData.

Le champ \$Seal contient la clé de chiffrement intermédiaire qui peut être déchiffrée par la clé privée du destinataire. La deuxième raison de l'échange de clé publique est que le poste client et le serveur ne détiennent pas forcément la clé publique du serveur de destination (cas de connexion Notes [port 1352] par Internet par exemple) L'échange des certificats (Nom et Identifiant) permet à Domino de vérifier s'il existe un certificat en commun ou non.

En présence de certificat différent (pas de père en commun), Domino recherche les certifications croisées dans les vues internes. Il est donc impossible de se connecter à un serveur avec un nom de certificat (Organisation en X500) identique mais contenant un numéro d'identifiant différent.

Le contrôle des certificats en commun est réalisé des deux côtés de la connexion, un client peut refuser une connexion en présence d'un certificat douteux.

### Authentification - Etape 2: Le défi



Si le client, ne possède pas de certificat en commun, le serveur Domino refuse la connexion. Ce phénomène se produit aussi si le client est renseigné dans le champ "Accès interdit" du document serveur ou si vous avez demandé de vérifier la présence du client dans le carnet d'adresses (attention cette fonction diminue les performances du serveur lors de connexions/déconnexions répétées).

L'analyseur de Windows NT sera d'un grand secours pour améliorer les performances de votre serveur. Vous avez les mêmes fonctionnalités sous AIX.

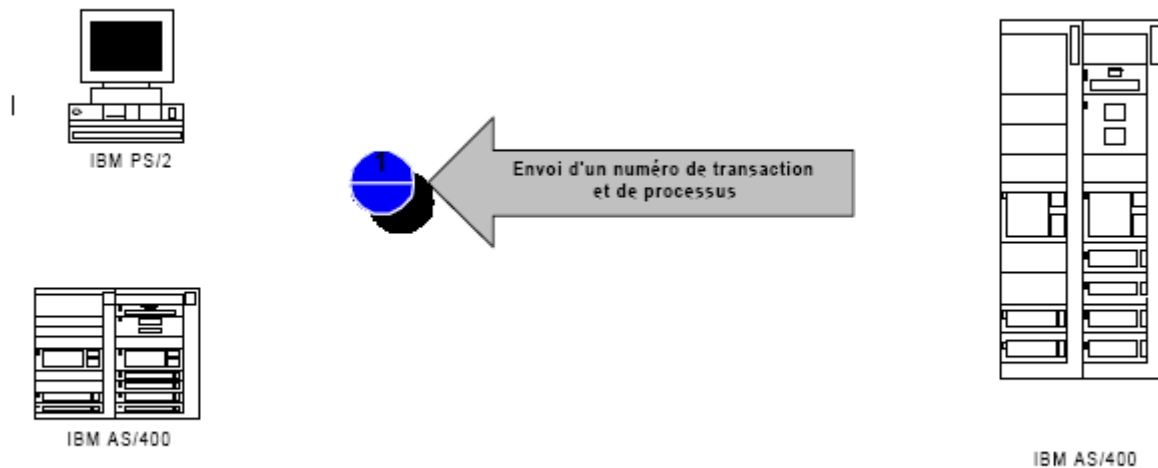
Le serveur peut s'assurer de l'authenticité du client. Pour ce faire, vous devez sélectionner l'option "Comparer les clé publiques", au niveau du document du serveur. Dans le cas inverse, seul le client (pour le point 1) vérifie l'authenticité du serveur. Cette option permet d'éliminer les clients "pirates" après une recertification par exemple.

En cas de non-conformité du nombre aléatoire envoyé par le serveur, le poste client annule la demande de connexion et prévient l'utilisateur de l'erreur de la connexion.

Lors de l'étape 2, le client fournit les informations au serveur, qui, à son tour peut annuler la connexion en cas de non conformité du nombre aléatoire.

Tout ce mécanisme permet ainsi de s'assurer que la connexion a bien été établie avec le bon serveur ou le bon client et évite toute intrusion non autorisée

### Authentification - Etape 3: Le ticket de session



Cette étape finale n'est pas actuellement exploitée par le client, toutefois en lançant la commande Show Tasks Debug sur la console du serveur, vous pouvez obtenir le numéro de session fournie au client par Domino. Ce numéro de session ne change qu'en cas de suppression de la session par Domino et lors d'une reconnexion au serveur par le client. Une autre méthode est de lancer une des commandes console suivantes:

- Show Users Debug
- Show db nombase.nsf
- Show File nombase.nsf

La commande Show Users Debug est intéressante lors de l'emploi du protocole TCP/IP puisqu'elle permet de connaître l'adresse IP du client actuellement connecté et de suivre ainsi qui utilise le même ID qu'un autre utilisateur.

Désormais le logiciel Administrator vous permet d'obtenir l'adresse TCPIP de l'utilisateur via l'onglet Serveur.