INTERNET PROFESSIONNEL
Avril 1999

Mise en œuvre: sécurité

Authentification par certificats X.509

Patrick CHAMBET
http://www.chambet.com

L'objectif de cet article:
Présenter la technique des certificats X509 et démontrer son efficacité en implémentant un mécanisme d'authentification sur IIS 4.0.

Les outils utilisés:
- Windows NT 4.0 SP4
- Internet Information Server 4.0
- Microsoft Certificate Server 1.0 (fait partie de l'option Pack pour Windows NT Server 4.0)
- La MMC (Microsoft Management Console) d'IIS 4.0
- Internet Explorer 4.01 SP1

Pour en savoir plus:
- http://premium.microsoft.com/msdn/library/backgrnd/html/secintro.htm Introduction aux crypto-systèmes sur Internet
- http://premium.microsoft.com/msdn/library/backgrnd/html/msdn_coretec.htm La cryptographie à clés publiques
- http://www.microsoft.com/workshop/security/client/certsvr.asp MS Certificate Server White Paper
- http://www.rsa.com/rsalabs/faq/index.html L'excellente FAQ de RSA à propos des certificats
- http://www.rsa.com/rsalabs/pubs/PKCS Les standards PKCS (Public-Key Cryptography Standards)
- ftp://ietf.org/internet-drafts/draft-ietf-pkix-ipki-part1-11.txt Le format X.509 (Internet Draft)

Qu’est-ce qu’un certificat X.509 ?

Une bonne analogie serait de comparer un certificat à un papier d’identité : il permet de vous identifier quand on vous demande de le présenter.

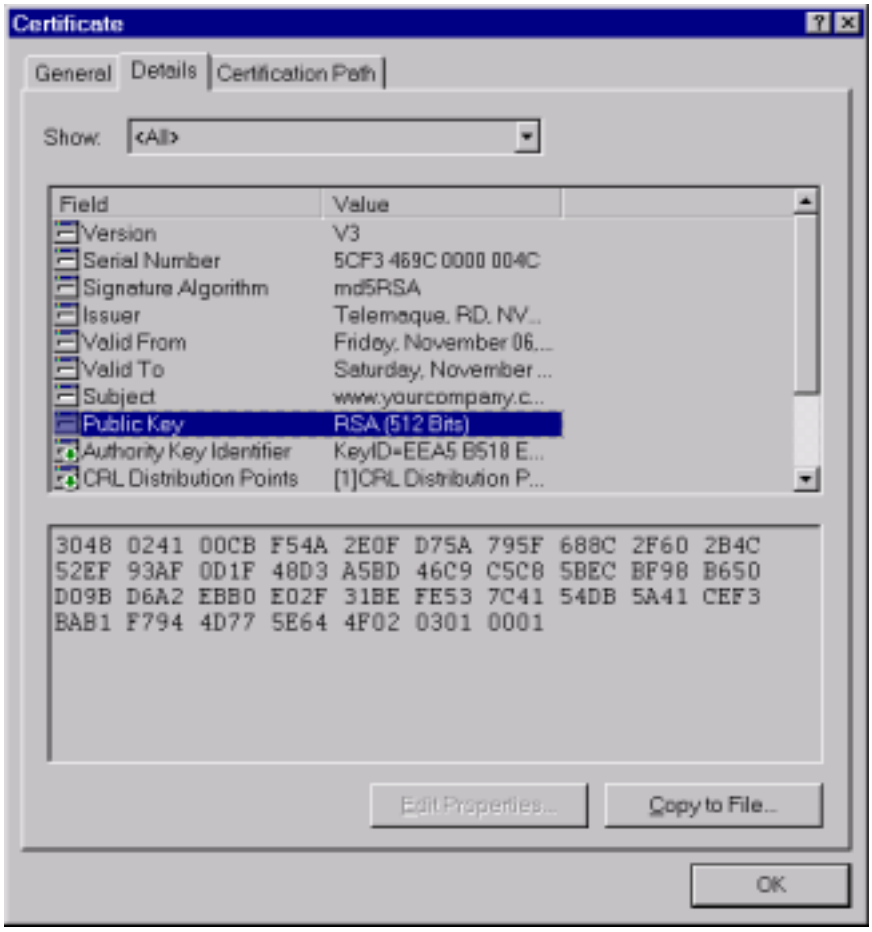
Plus précisément, un certificat est un document qui permet d’attester qu’une *clé publique* vous appartient bien. Pour cela, il renferme plusieurs informations : votre clé publique, bien sûr, mais aussi des renseignements vous identifiant (votre nom, votre société, votre e-mail, la date de validité du certificat, ou d’autres champs supplémentaires).

Ces informations sont certifiées être justes par une *authorité de certification* (Certification Authority ou CA) qui est censée avoir vérifié ces informations avant d’avoir validé votre certificat. La CA (Verisign par exemple) joue le rôle de la Préfecture qui vérifie votre identité avant de mettre le coup de tampon qui validera votre permis de conduire.

Pour cela, la CA hache et signe le certificat à l’aide de sa propre clé privée. Il suffit donc de connaître sa clé publique (largement distribuée et notamment intégrée aux navigateurs Web) pour vérifier la validité d’un certificat généré par elle.

Structure d’un certificat

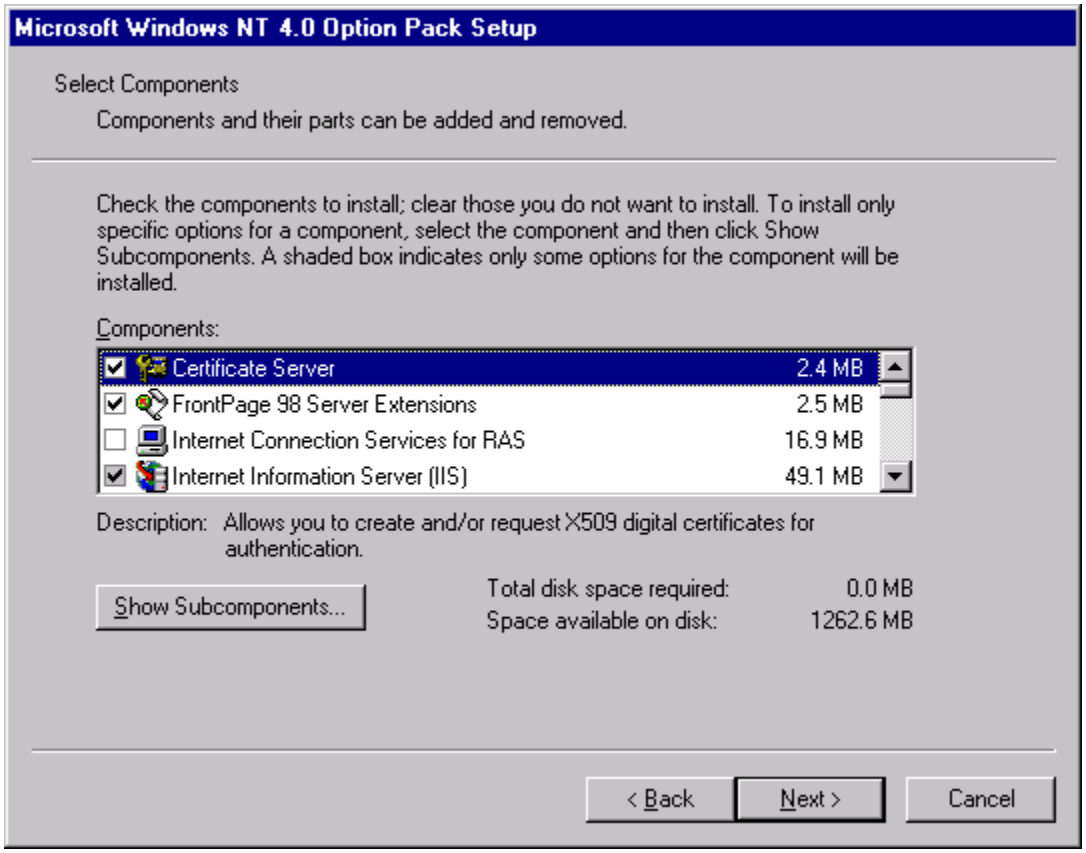
Sur NT, si vous avez installé le SP4, il vous suffit de double cliquer sur le fichier .cer ou .crt d’un certificat pour visualiser la valeur de ses champs. En effet, le SP4 comporte un Certificate Viewer qui vous affiche par exemple l’écran suivant :



Implémenter une authentification par certificats

1 – Installez IIS 4.0 et Certificate Server

Si ce n'est déjà fait, lancez l'installation de l'Option Pack pour Windows NT Server 4.0 et cochez les cases *Certificate Server* et *Internet Information Server* :



Des renseignements concernant votre autorité de certification vous seront demandés : nom de votre société, adresse, pays, etc… Indiquez-les avec soin, car ces renseignements feront partie intégrante du certificat de votre CA.

2 – Installez le certificat CA de votre Certificate Server dans IIS
Pour cela, double-cliquez sur le fichier *`NomDeMachine_NomDeCA`*`.crt` qui se trouve en général dans le répertoire `C:\WINNT\System32\CertSrv\CertEnroll`.

Cliquez sur “Install Certificate”: l’Import Wizard du SP4 se lance. Cliquez sur “Next”, puis sur le bouton radio “Place all the certificates in the following store” et sur “Browse”.

Cliquez ensuite sur “Show physical store”, déroulez “Trusted Root Certification Authorities” et cliquez sur “Registry”:

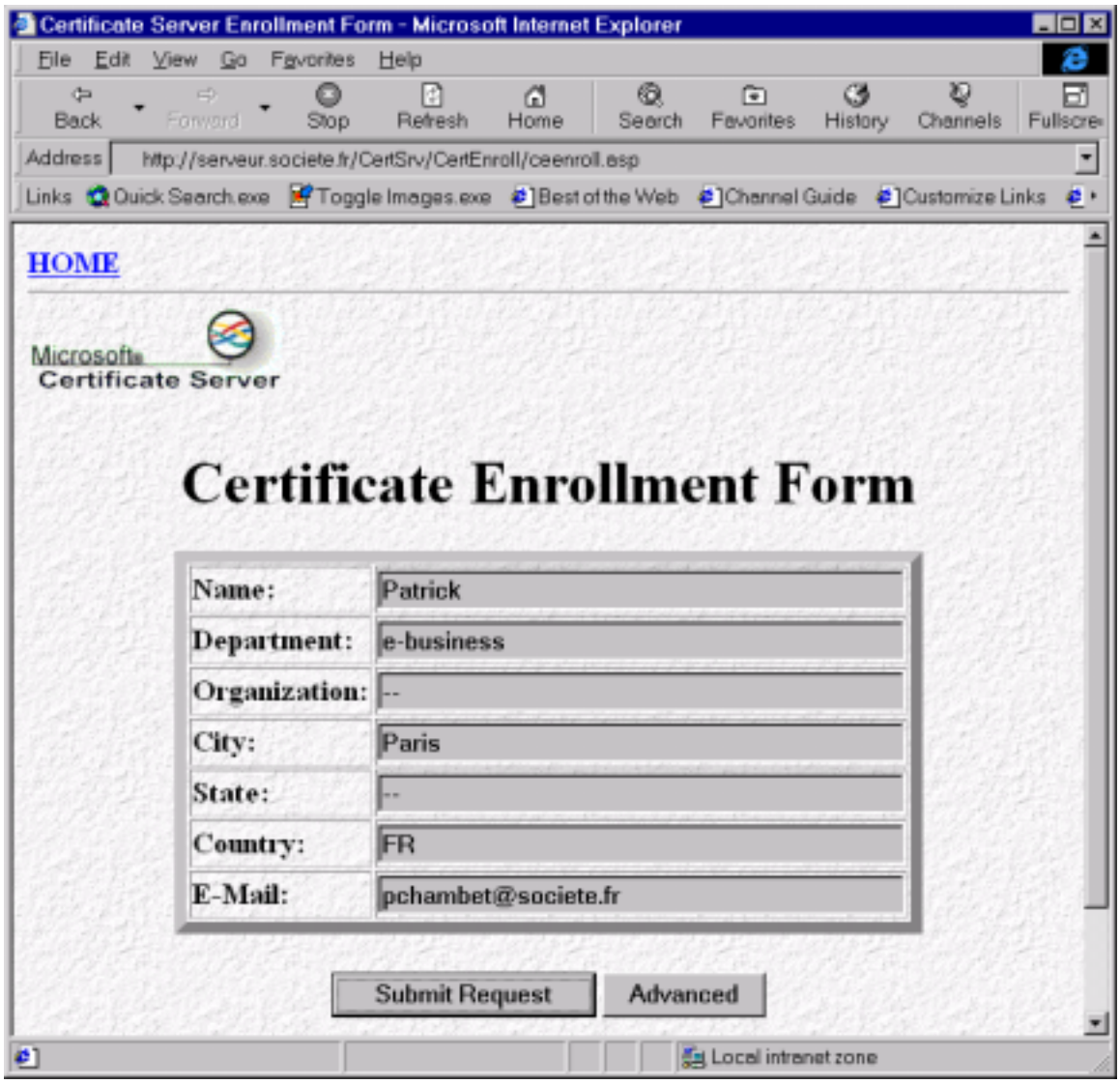
Cliquez enfin sur “OK”, “Next” et “Finish”. Votre CA est installée.

Remarque: avec le SP3 de NT, il fallait d’abord installer le certificat de votre CA dans IE 4.01 *sur le serveur*, puis uploader la liste des CA dans la métabase d’IIS 4.0 en exécutant l’utilitaire `iisca.exe`. Cette étape illogique n’est plus nécessaire avec le SP4, grâce à l’Import Wizard, comme nous venons de le voir.

3 – Générez les certificats clients

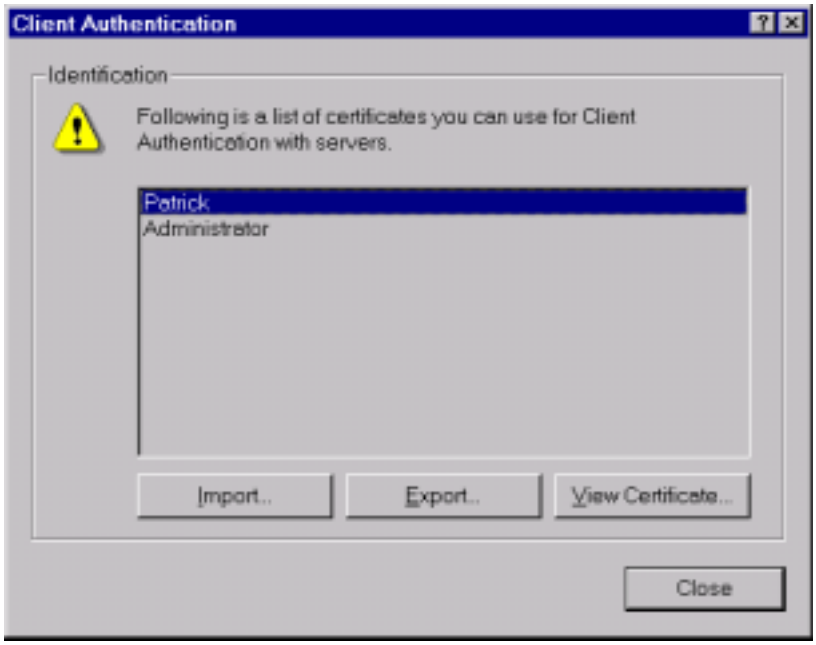
Pour cela, connectez-vous avec IE 4.01 SP1 au serveur Web hébergeant votre Certificate Server, depuis l’ordinateur sur lequel vous utiliserez le certificat client pour vous authentifier. L’URL est en général :
http://serveur.societe.fr/CertSrv/CertEnroll/ceenroll.asp

Remplissez les champs avec les données personnelles vous concernant :



Cliquez sur « Submit » puis sur « Download ».

Votre nouveau certificat client est maintenant installé dans votre navigateur, et est visible si vous choisissez l'onglet « Content » dans les options d'Internet Explorer et si vous cliquez sur « Personal » :



4 – Installez un certificat serveur dans IIS 4.0

Vous devez installer un certificat serveur pour pouvoir établir une connection sécurisée par SSL avec votre serveur IIS 4.0.

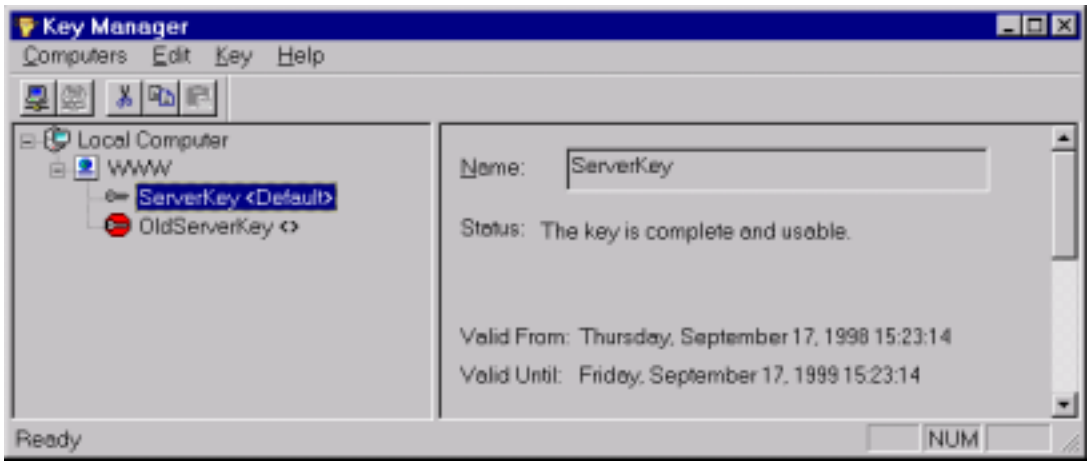
Ce certificat peut-être généré à l'aide de votre Certificate Server, mais il peut être préférable de demander à une CA reconnue par tous (Verisign par exemple) de le générer pour vous. Ainsi, tous les utilisateurs qui se connecteront à votre site Web auront confiance en la validité de votre certificat serveur.

Attention : veillez à bien indiquer le nom de domaine complet de votre serveur Web, par exemple `serveur.societe.fr`. Ce nom sera inscrit une fois pour toutes dans le certificat serveur, et une fenêtre d'alerte s'affichera si l'URL de votre site est différente.

Une fois que vous êtes en possession du fichier contenant votre certificat serveur, lancez la Management Console (MMC), cliquez sur un répertoire de votre serveur Web et cliquez sur l'icône du Key Manager dans la barre d'outils (elle représente une main tenant une clé).

Cliquez ensuite sur votre serveur Web, choisissez « Import Key », indiquez l'emplacement du fichier de votre certificat serveur, le mot de passe qui le protège et choisissez « Any unassigned » pour l'adresse IP et le port utilisés.

Vous avez maintenant un certificat serveur en état de fonctionner.



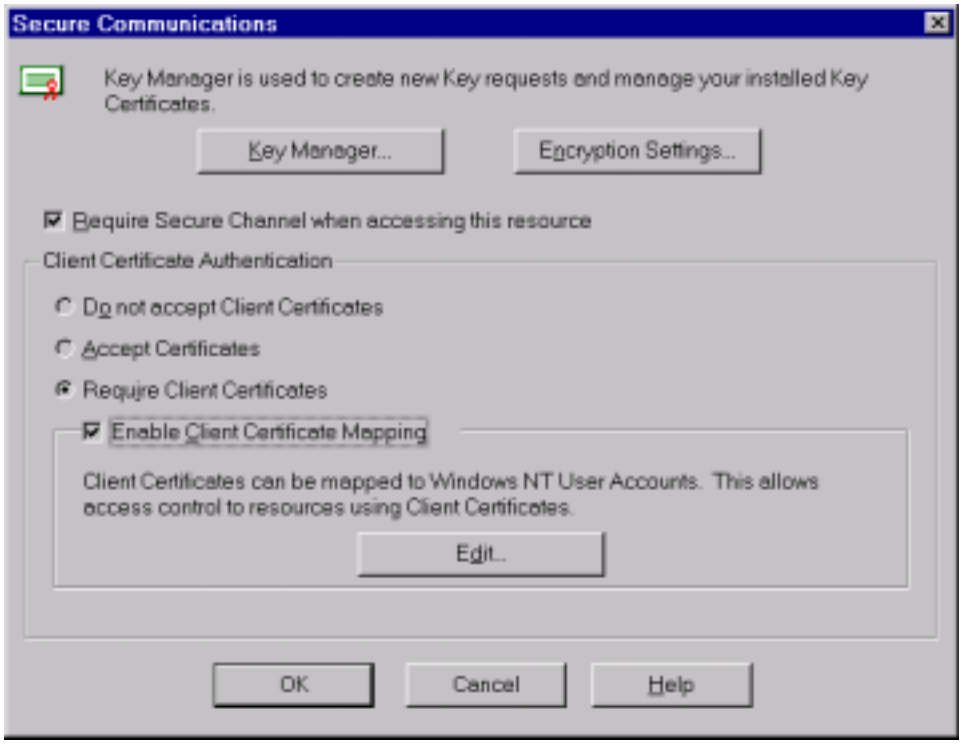
5 – Paramétrez les permissions d'accès de votre serveur IIS 4.0

A l'aide de la MMC, affichez les propriétés du répertoire dont vous voulez protéger l'accès dans l'arborescence de votre serveur Web et cliquez sur l'onglet « Security ».

Dans la section « Anonymous Access and Authentication Control », cochez « Allow Anonymous Access » uniquement. En effet, la sécurité ne reposera pas sur les protocoles d'authentification classiques (Basic Authentication et NTLM), mais sur l'utilisation des certificats.

Dans la section « Secure Communications », paramétrez les préférences comme ceci :

- Require Secure Channel when accessing this resource
- Require Client Certificates
- Enable Client Certificate Mapping



6 – Créez les règles d'accès à votre serveur IIS 4.0

Toujours dans la fenêtre ci-dessus, cliquez sur « Edit », puis sur l'onglet « Advanced » et sur le bouton « Add ». Nous allons créer une règle de mapping entre des certificats et un compte NT à l'aide d'un Wizard.

Dans la première fenêtre, indiquez le nom de votre règle et utilisez le bouton « Select » pour sélectionner votre CA (celle que nous avons installé au point 2) en double cliquant son nom dans la liste.

Dans la deuxième fenêtre, cliquez simplement sur « Next »

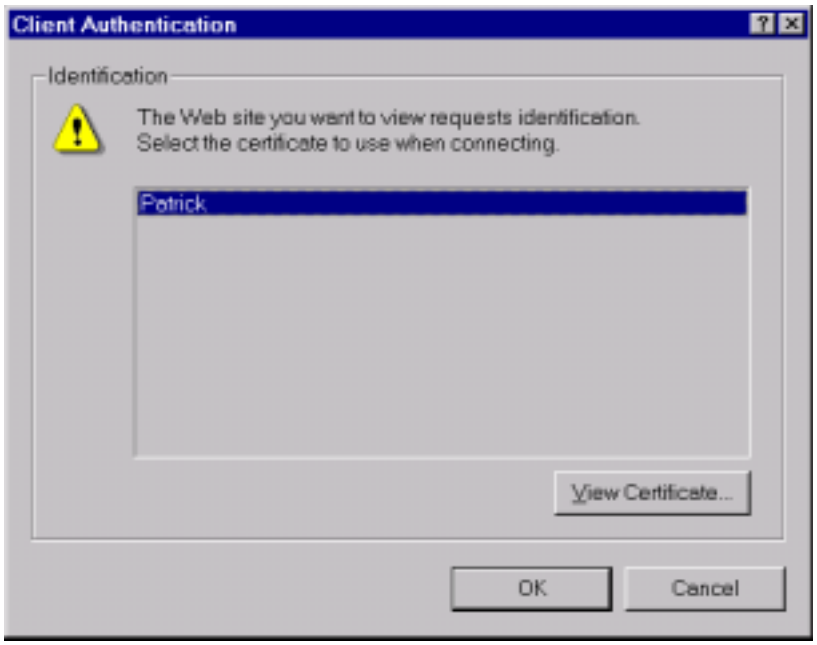
Enfin, dans la troisième fenêtre, indiquez le compte NT qui protègera l'accès à votre répertoire Web, ainsi que son mot de passe.

7 – Paramétrez les permissions d'accès au répertoire dont vous souhaitez protéger l'accès.

Dans l'onglet « Sécurité » des propriétés de votre répertoire (situé en général dans `C :\InetPub\wwwroot`), indiquez que seul le compte que vous avez spécifié dans le point précédent possède la permission « Read » (en plus des administrateurs, éventuellement).

8 – Connectez-vous sur votre site protégé

Si maintenant vous accédez par SSL au site protégé avec IE 4.01, par exemple (mais cela marche aussi avec Netscape si vous importez votre CA auparavant), le navigateur vous demande de présenter un certificat :



Si vous choisissez un certificat généré par votre certificate server, IIS va utiliser le compte que vous avez spécifié au point précédent pour vous loguer sur le serveur NT, et vous aurez donc accès au répertoire protégé.

Mais si vous n'avez pas de certificat ou si votre certificat a été émis par une autre CA (Verisign par exemple), votre accès sera interdit par une erreur HTTP 403.7 (Certificate required) ou 401.3 (Unauthorized due to ACL on resource**).**

Les certificats sont donc un moyen élégant de gérer la sécurité d'un ensemble de sites Web. En effet, cette technique règle le problème des mots de passe multiples nécessaires sur des serveurs différents. Un utilisateur peut être authentifié sur plusieurs serveurs en présentant toujours le même certificat.

Patrick Chambet