Livre Blanc

Mise en place d'un serveur HTTPS sous Windows 2000

Pierre LANSALOT-BASOU
M

Mise à jour : Mai 2003

Page 51 : Export/Import du certificat serveur vers un serveur IIS 5.

Les informations recueillies dans ce document sont tirées du MSDN, d'articles techniques, d'extrait de documents du TechNet et d'Internet et d'expériences personnelles. Le but de ce livre blanc est d'exposer les fonctionnalités de base de Microsoft Certificate server.

1) Architecture d'un serveur Web sécurisé par HTTPS

a. Présentation générale d'une architecture de site Web HTTPS

La mise en place d'une architecture de serveur HTTPS met en place plusieurs acteurs majeurs :

- L'autorité de certification privée (appelée aussi Root CA ou autorité d'accréditation)
- Le serveur Web (opérationnel sur HTTP que l'on souhaite sécuriser par la mlise en place du protocole sécurisé HTTPS)
- Les postes clients Internet Explorer (accédant depuis votre réseau Intranet ou depuis le réseau Internet)

i. Autorité de certification privée

Cette autorité est considéré comme une référence morale. Son rôle est de délivrer une accréditation (ou certificat serveur) suite à la demande émise dans un formulaire (via Internet ou par courrier). Cet organisme certifie la validité , assure la reconnaissance du certificat qui sera émis par ses soins et renvoie alors un certificat en bonne et dû forme à l'expéditeur du formulaire.

De nombreux organismes privés se sont spécialisés dans la délivrance (payante) de tels certificats comme aux Etats-Unis (Verisign, Thawte) et en France (Certplus), par exemple. Pour information, un certificat 128 bits complet demandé auprès de Verisign coûte environ 800$).

ii. Serveur Web sécurisé

Le serveur Web constitue la pierre angulaire du système sécurisé. C'est sur ce serveur que va être installé le certificats Serveur de l'autorité de certification qui l'a émis.

Internet Information Server possède en standard une liste des organisme de certification les plus courants. Certificat Server de Microsoft vous permet également de créer votre propre autorité de certification privée : cela vous permet de sécuriser votre serveur Web avec

un certificat émis par vos soins et présente l'avantage d'être gratuit

iii. Clients Internet Explorer

Une fois le serveur Web sécurisé par un certificat issu d'un organisme de certification, vous pouvez vous arrêter là. Mais la sécurisation ne sera pas alors complète. En effet, comme nous travaillons essentiellement dans une architecture client/serveur, la communication n'est pas sécurisée de bout en bout. Vous pouvez renforcer l'accès sécurisé en imposant aux postes client, accédant à votre serveur Web HTTPS, de présenter un certificat Client au serveur. Si ceux-ci ne le présentent pas, alors l'accès au site Web est refusé.

Nous pouvons comparer la sécurisation d'un site Web à l'analogie suivante :

Analogie : Accès à une Soirée privée

- L'autorité de certification peut être considéré à un organisme délivrant au compte goutte des badges pour accéder à une soirée. Ce badge (de couleur rouge, avec un texte unique et identifiant précisément cette soirée) vous a été délivré par l'organisme en retour de votre précédent courrier contenant un formulaire d'inscription et votre réglement.

- Le serveur Web peut être comparé à un vigile devant le portail de l'établissement dans lequel se déroule la soirée. Il a eu connaissance de ne laisser rentrer que les gens arborant le fameux badge rouge. En d'autres termes, le vigile a eu donc connaissance de l'existence d'un badge certifiant que l'organisme de certification (qui la embauché) autorise toute personne porteuse de ce badge d'accéder à cette soirée.

- Le client IE, c'est vous, personne physique qui souhaitez rentrer dans cette soirée. Pour y accéder, la présentation de ce badge est indispensable. Vous le portez donc sur vous à l'entrée de l'établissement.

b. Activer la sécurisation d'un site Web par SSL : Authentification par certificat côté serveur

Cette analogie met en valeur les précisions suivantes :

- le certificat doit absolument être connu du serveur pour que toute requête cliente soit examinée et acceptée ou refusée.
- Il est ensuite placé à la discrétion du serveur de demander au client le certificat pour rentrer sur le portail. En effet, des consignes peuvent avoir données au vigile soit :
  - de ne pas demander à tout le monde le badge
  - de demander à tout le monde de montrer le badge

Cette sécurisation est efficace pour rentrer sur le site car elle correspond à une authentification de la demande du client par le serveur via un mécanisme de sécurité (certificat). Cependant, nous verrons dans un prochain chapitre que cette sécurisation de site peut être renforcée, en particulier en ce qui concerne la cryptographie des données.

Voyons maintenant les différentes étapes nécessaires : Ces étapes seront intégralement reprises et détaillées dans le chapitre Travaux pratiques

i. Mise en place d'une autorité de certification privée (Certificat Root CA)

Cette partie n'est nécessaire d'effectuer que si vous désirez créer et installer votre propre organisme de certification privée, indépendamment de Verisign ou d'autres organismes payants.

1. **Création d'un serveur de certificat Root CA**

2. **Installation du certificat Root CA**

ii. Mise en place du certificat serveur de l'autorité de certification privée (Certificat Serveur)

Cette partie permet de créer la requête pour un certificat authentifié par un organisme de certification, de récupérer le certificat serveur et de l'installer sur le serveur Web. Après installation, le serveur Web sera configuré pour activer le canal SSL avec le certificat serveur.

1. **Création d'une demande de certificat**

2. **Soumission d'une requête de certificat**

3. **Traitement et téléchargement d'un certificat**

Cette étape se décompose en deux parties distinctes :

- Traitement de la demande, envoyée par le client à l'organisme de certification privé.
- Téléchargement

4. **Installation du certificat et paramétrage du site Web SSL**

Maintenant que nous possédons ce certificat CERTNEW.CER, il ne nous reste plus qu'à l'installer sur notre serveur Web HTTP. Il existe deux méthodes pour cela :

- soit copiez le certificat directement sur le serveur Web, puis double-cliquer dessus pour l'installer.
- Soit l'installer par l'assistant d'installation de certificat pour pré installer le certificat, puis le lier au site Web à sécuriser. Nous présenterons la deuxième méthode dans les travaux pratiques.

c. Activer la sécurisation d'un site Web par SSL : Authentification par certificat côté client

Il existe plusieurs manières d'installer le certificat Root CA dans la liste des Root CA de confiance dans Internet Explorer 5 :

- Par mail : envoyez le certificat à tous vos utilisateurs pour qu'ils puissent l'installer simplement.
- Par téléchargement : une page de téléchargement propose un lien vers le certificat Root CA.
- Par IEAK : dans le cadre de déploiement massif de nouvelles versions d'Internet Explorer, vous pouvez directement intégrer le certificat au sein des autorités de confiance dans le paquetage IEAK.

De toutes les manières, le certificat Root CA doit être installé sur les postes client pour indiquer à Internet Explorer de faire confiance au fait que le certificat de votre site n'est pas le certificat que vous venez juste de créer, mais plutôt le certificat Root CA, créé lorsque Certificate Serveur a été installé.

i. Installation du certificat Root CA

Pour ce faire, il nous faut télécharger le certificat depuis notre poste client :

ii. Installation du certificat client lié au CA

Jusqu'à présent, nous n'avions pas besoin de présenter sur nos postes client un certificat client. Cependant, dans le cas présenté ci-dessous où vous configurez votre serveur Web HTTPS pour exiger la présentation d'un certificat client, il est nécessaire d'installer un certificat client.

Lorsqu'on tente maintenant d'accéder au site HTTPS, le client IE présente une liste des certificat client correspondant à l'autorité de certification privé qui a configuré le serveur Web en HTTPS. C'est à l'utilisateur alors de choisir de présenter le certificat client au serveur et de valider son choix.

d. Renforcer la sécurisation d'un site Web par SSL : Cryptographie SSL

i. Différence entre authentification et cryptographie

Il est nécessaire de bien faire la distinction entre authentification SSL et cryptographie des données SSL.

Si nous revenons à notre exemple de vigile à l'entrée d'une soirée, l'authentification correspond à l'accord du vigile de nous laisser rentrer dans le lieu de la soirée après lui avoir montré notre badge rouge. Mais une fois entré, il nous faut encore pouvoir parler et se faire comprendre lorsque nous entamerons une discussion avec les autres invités. En effet, la langue utilisée (ou cryptage) dans cette soirée peut être une barrière pour communiquer et avoir les informations souhaitées. Il est donc nécessaire de pouvoir se mettre au même niveau de cryptographie côté serveur ET client afin de pouvoir échanger des informations. Il reste donc à se mettre d'accord sur le mode de cryptographie SSL à utiliser afin de se comprendre.

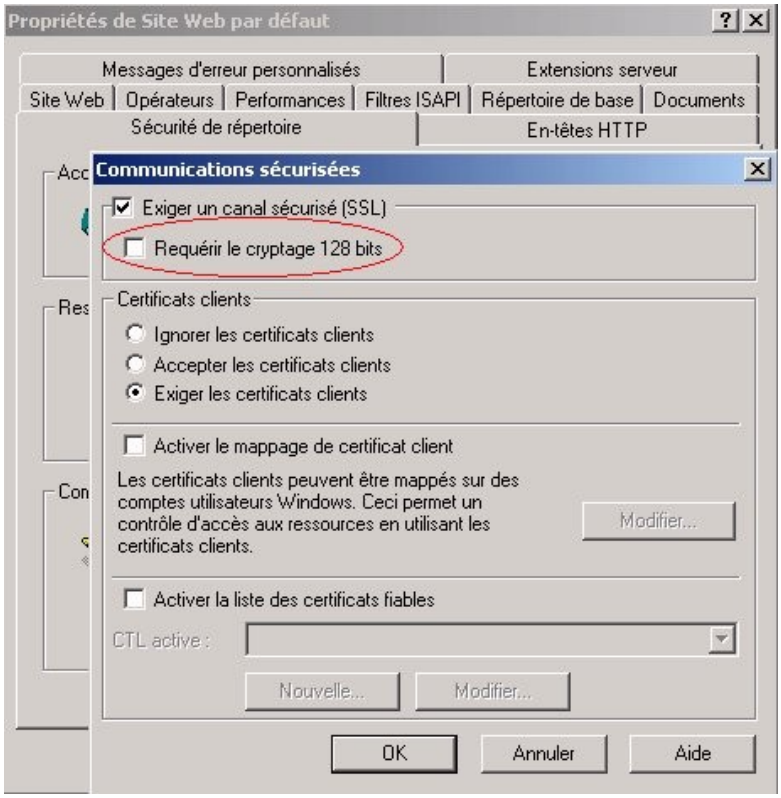
ii. Les différents modes de cryptographie SSL

1. **Encryptage SSL 40-56 bits**

   L'encryptage des données, circulant sur un canal SSL, sur 40 bits, est le mode communication standard SSL sous Windows NT4 Serveur et Windows 2000 Serveur.
   Côté client, tous les navigateurs, à partir de Internet Explorer 4.01 communiquent de base en mode 40 bits.

2. **Encryptage SSL 128 bits**

   L'encryptage des données, circulant sur un canal SSL, sur 128 bits, est le mode communication SSL offrant le plus de sécurité de bout en bout. Sous Windows NT4 Serveur et Windows 2000 Serveur, il vous suffit de l'activer comme le montre l'écran suivant :



Mais cela ne suffit pas : en effet, une DLL spéciale est utilisée sur le serveur et sur le client afin de crypter effectivement les données en 128bits. Cette DLL s'appelle SCHANNEL.DLL et peut être installée sur un serveur ou sur un client de deux manières différentes. Ces manières seront décrites dans le chapitre suivant.

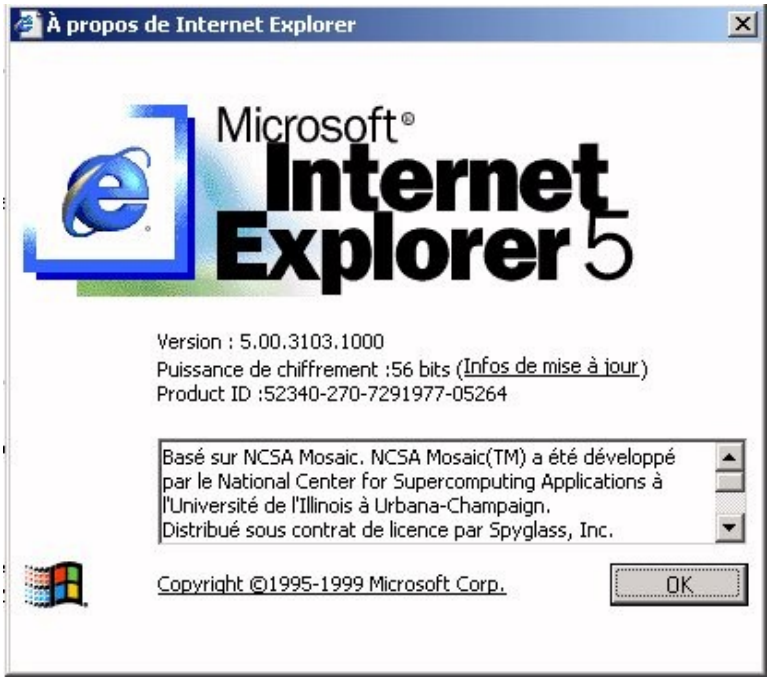
3. Activer un algorithme SSL sous IIS

Plusieurs algorithmes SSL sont inclus en standard dans Windows NT4 et Windows 2000. Il est possible de les activer ou non sure le serveur dans l'éditeur de registre. La procédure est décrite dans l'article technique Q245030.

iii. Encryption Pack 128 bits sur un serveur Web

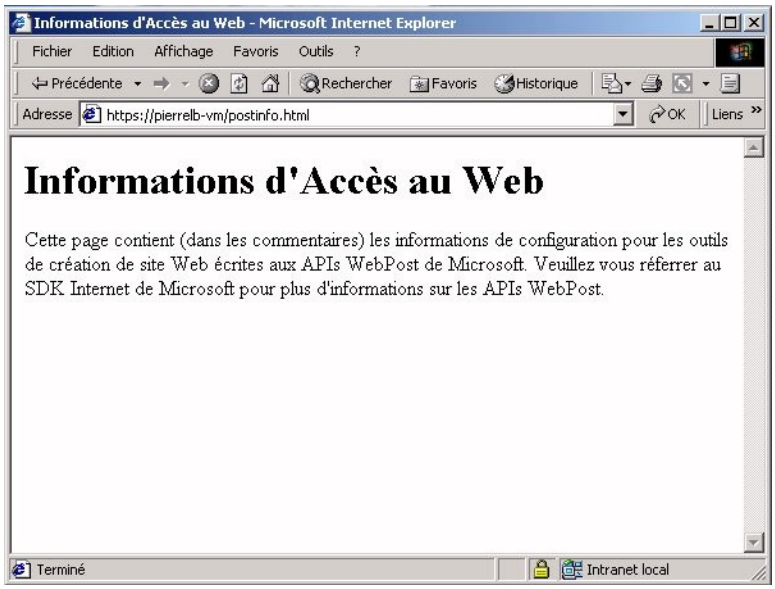
Pour vous assurer que votre serveur ou votre poste client a le mode 128bits installé, le meilleur moyen est de :

- Lancez Internet Explorer et allez dans le Menu ?; puis Option A propos de : Internet Explorer vous affichera alors une boite de dialogue dans laquelle sera affiché le mode d'encryption installé sur le système :



IMPORTANT :

Il est capital que la DLL système SCHANNELL.DLL soit installée côté client ET côté serveur, afin que l'encryption/désencryption soit effectuée des deux côtés. Une fois la communication sécurisée établie entre le poste client et le serveur, vous pouvez vérifier le mode d'encryption utilisé dans Internet Explorer par un petit symbole représentant un cadenas jaune affiché dans la barre d'état :



Si vous n'avez pas le mode 128 bits installé, alors nous vous présentons plusieurs moyens de l'installer sur vos serveurs et vos postes clients :

1. **sur NT4 : Encryption Service Pack**
    a. US
        i. Sur un serveur NT4 US, vous pouvez télécharger le Service Pack High-encryption. Disponible depuis le début sur le continent américain, son installation a été seulement légalement autorisée en France il y a seulement 2 ans. Auparavant, toute entreprise française devait demander une dérogation auprès du gouvernement afin de l'utiliser, ce qui n'est plus le cas seulement. Cette libéralisation a ainsi permis aux entreprises financières françaises de pouvoir implémenter l'encryptage 128 bits sur le territoire et de combler le retard technologique face aux autres pays, même européens.

b. Le cas Français
    i. Ce Service Pack High-encryption pour Windows NT4 est disponible dans sa version 6a en téléchargement sur le site Web de Microsoft, mais uniquement en version US (http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/allSP6.asp).
    ii. En effet, l'adoption tardive du SSL 128 bits par la France a en fait repoussé la sortie d'un tel Service Pack localisé en Français. Il faut donc avoir recours à une autre méthode qui est présentée ci-dessous.

c. Sites de téléchargement du IE High-encryption pack

    i. Nous avons vu que le fichier SCHANNEL.DLL était le point central dans l'activation de l'encryptage 128 bits. Nous avons également vu que l'installation du Service Pack High-encryption était une première solution, mais qui présente de nombreuses contraintes dans le cas du territoire Français, où de nombreux serveurs Web de production sont installées avec des versions françaises de Windows NT4 serveur. Que faire dans ce cas ?

    ii. La solution passe par Internet Explorer ! En effet, il existe en téléchargement un pack spécial pour toutes les versions d'Internet Explorer (4 et 5) afin d'activer le mode 128 bits SSL. Ce pack s'appelle le Internet Explorer High-encryption Pack.

Vous pouvez :

1. soit installer ce IE High-encryption Pack de manière autonome depuis le site Web de Microsoft. Le fichier s'appelle IE501DOM.EXE.
2. soit mettre à jour la version d'Internet Explorer sur votre serveur : en effet, à partir de la version Internet Explorer 5.01 SP1, ce High-encryption pack est présent et installé automatiquement lors de la mise à jour de la version d'Internet Explorer 5. Si vous utilisez IEAK pour déployer de nouvelles versions d'Internet Explorer sur vos postes, vous trouverez IE501DOM.EXE présent.

- La première méthode d'installation du High-encryption Pack présente l'avantage de laisser à l'utilisateur ou à l'administrateur système le choix d'installation d'un tel encryptage sur le poste.
- La deuxième méthode d'installation présente l'avantage évident d'installer l'encryptage 128 bits de manière automatique et transparente sur vos postes.

2. **sur Windows 2000**

    a. Sous Windows 2000, en effet, installer une nouvelle version d'Internet Explorer (IE5.5 par exemple) n'installera pas le IE Igh-encryption pack. Le seul moyen est alors d'installer le Windows 2000 Encryption Pack depuis le site Web de Microsoft (http://www.microsoft.com/windows2000/downloads/recommended/encryption/

3. **Internet Explorer : High-encryption Pack**

    a. Les interactions de certaines versions d'Internet Explorer sur l'encryption SSL 128 bits.

        i. Dans les deux cas présentés dans le chapitre précédent, vous devez être conscient d'une conséquence sur le système une fois le Internet Explorer High-encryption Pack installé sur votre serveur Windows NT4 (sans conséquence sous Windows 2000) : la DLL système SCHANNEL.DLL a été modifiée.

        ii. Supposons que maintenant vous souhaitiez installer un nouveau Service Pack Windows NT4 standard (par exemple NT4 SP6A alors que votre serveur est actuellement en Windows NT4 SP5), son installation vous sera refusée car il teste la DLL SCHANNEL.DLL : un message vous avertira alors que vous essayez d'installer une version Standard du Service Pack de NT4 sur une version 128bits de Service Pack de NT4, et arrêtera ici l'installation en vous conseillant d'installer à la

place le Service Pack high-encryption de NT4 à la place ! Problème que peut alors se révéler insoluble si votre serveur Windows NT4 est français : en effet, comme nous l'avons v u dans le chapitre précédent, il n'existe pas un tel Service Pack francisé ! Dans une telle situation, la solution consiste à appliquer la procédure décrite dans l'article technique TECHNET Q250867.

b. Sites de téléchargement du IE High-encryption pack

   i. Toutes les versions du Internet Explorer High-encryption Pack (Internationales, pour IE4, pour IE5) sont téléchargeables à l'adresse suivante : http://www.microsoft.com/windows/ie/downloads/recommended/128bit/default.asp

   ii. Sur cette page sont regroupées toutes les versions de IE501DOM.EXE qui existent selon le type de plate-forme: Windows NT4 SP4 ou moins, Windows NT4 SP5, Windows NT4 SP6, Internet Explorer 4.01, Internet Explorer 5.0 etc... Il est vivement recommandé de savoir exactement quelle plate-forme est concernée avant d'installer le Internet Explorer High-encryption pack correspondant.

2) Travaux pratiques :

a. Activer la sécurisation d'un site Web par SSL : Authentification par certificat côté serveur

i. Mise en place d'une autorité de certification privée (Certificat Root CA)

Cette partie n'est nécessaire d'effectuer que si vous désirez créer et installer votre propre organisme de certification privée, indépendamment de Verisign ou d'autres organismes payants.

1. **Création d'un serveur de certificat Root CA**

Pour créer un serveur Root CA, il vous suffit d'installer simplement les services Certificate Server depuis Ajout/suppression de programmes de Windows 2000. Par défaut, ces services ne sont pas installés sur Windows 2000 Server ou Windows 2000 Advanced Server.

Sous NT4, vous devez relancer l'installation d'Option Pack pour sélectionner l'installation de Certificate Services.

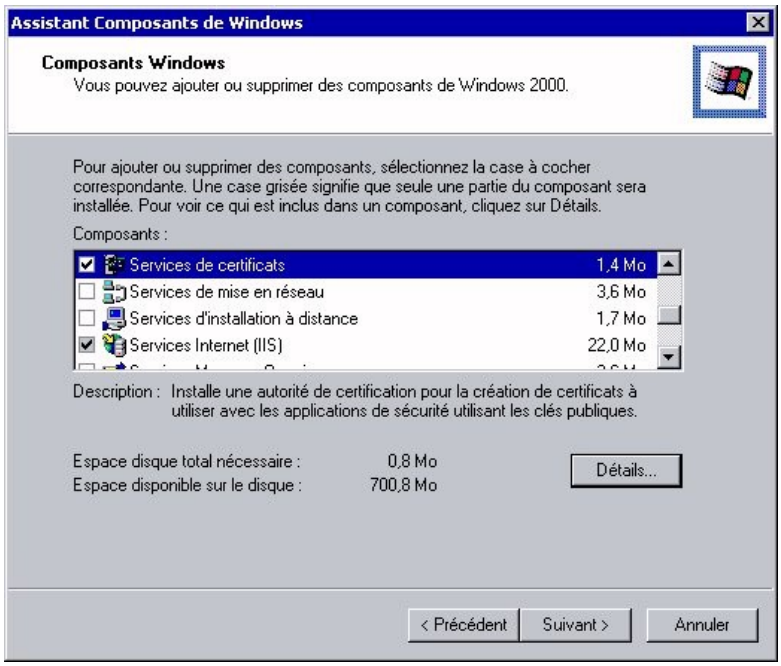


Figure1 : Installation des services de certificats sous Windows 2000

2. Installation du certificat Root CA

Sous Windows 2000, cette opération est effectuée automatiquement après l'installation des services Certificate Server 2.0. Un nouvel organisme de certification est alors rajouté : il s'agit par défaut du nom du serveur sur lequel a été installé Certificate Server.

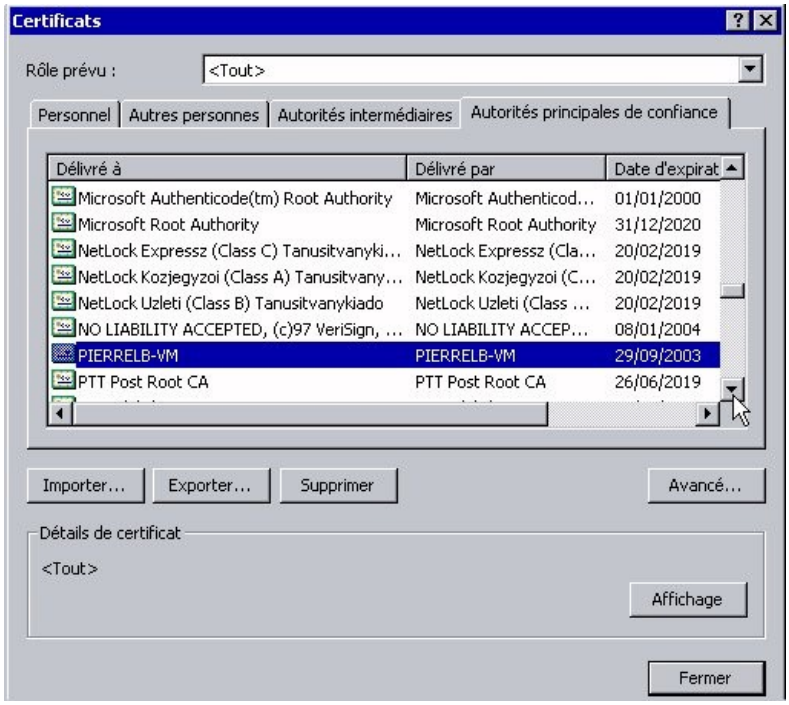


Figure2 : Installation automatique d'une nouvelle Autorité de confiance privée (ou Root CA) sous Windows 2000.

Sous NT4, une procédure doit être suivie pour installer le Certificat Root CA. Cette procédure est disponible dans l'article TECHNET Q218445 dans la partie «Install the Root CA certificate on the server»..

.

ii. Mise en place du certificat serveur de l'autorité de certification privée (Certificat Serveur)

Cette partie permet de créer la requête pour un certificat authentifié par un organisme de certification, de récupérer le certificat serveur et de l'installer sur le serveur Web. Après installation, le serveur Web sera configuré pour activer le canal SSL avec le certificat serveur.

1. Création d'une demande de certificat

Tout d'abord, nous devons soumettre notre demande d'obtenir un certificat serveur. L'organisme de certification à qui sera destinée cette demande renverra ensuite un certificat serveur. Dans les exemples ci-dessous, l'organisme de certification concerné est un organisme de certification privé créé sur un serveur de certificat Microsoft Root CA.

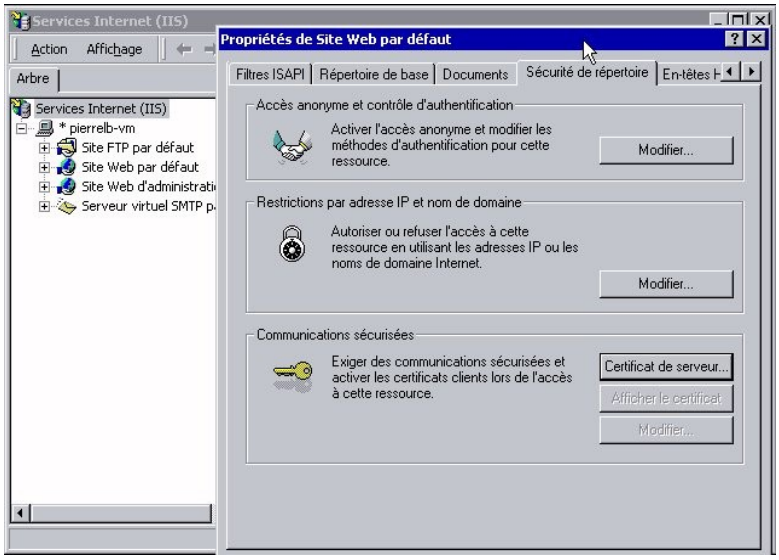


Figure3 : Création d'une demande de certificat serveur via le gestionnaire de services Internet sous Windows 2000.

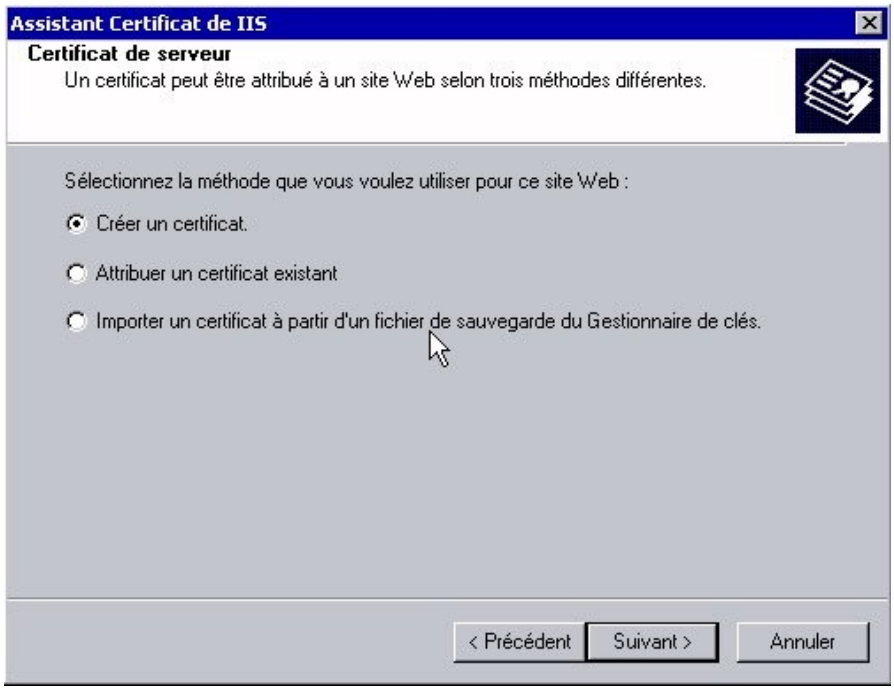


Figure4 : Une fois dans le wizard, l'administrateur est guidé pour créer un certificat sous Windows 2000.

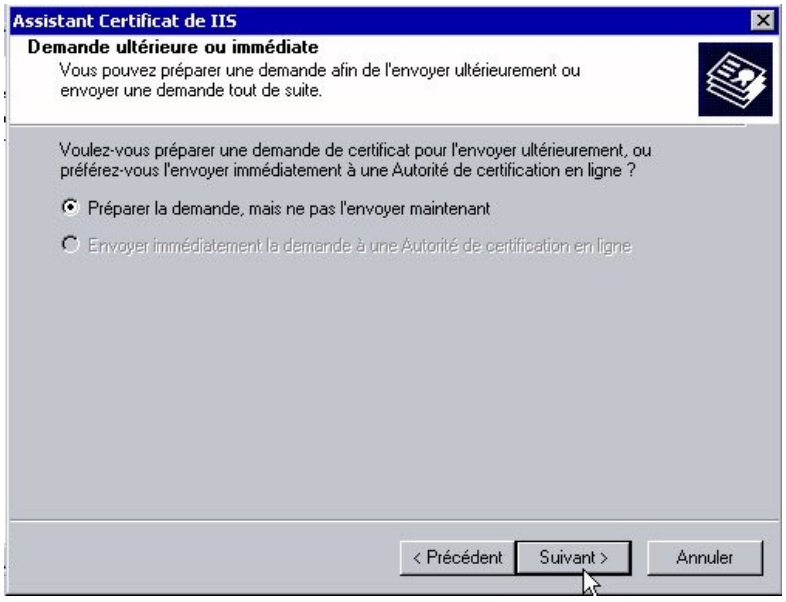


Figure5 : Préparation de la demande sous Windows 2000.

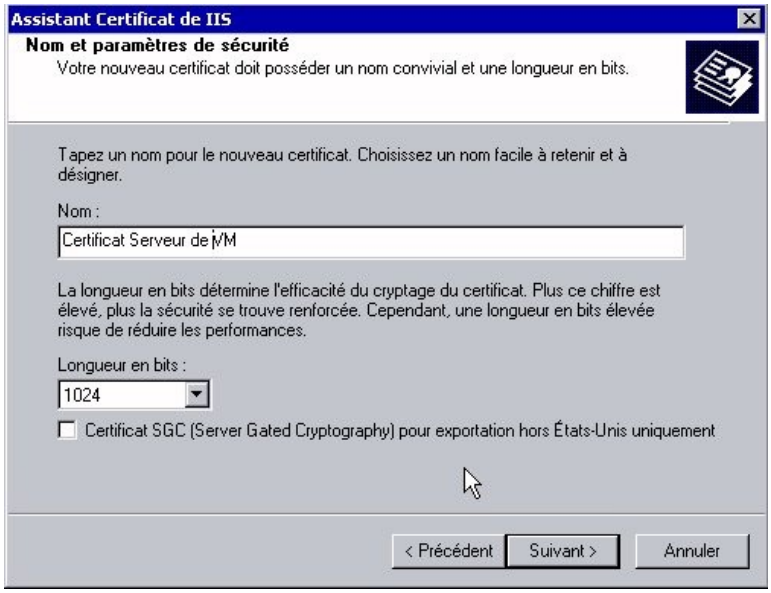


Figure6 : Saisie du nom du certificat serveur. Il est possible de préciser que ce certificat soit de type SGC.

Les certificats SGC sont les plus souvent utilisés par les organismes financiers qui nécessitent des connections de haute encryption (128 bits) même dans le cas où des utilisateurs ou navigateurs internationaux sont limités à l'encryption 40 bits. Lorsqu'un navigateur international (40 bits) se connecte sur un serveur où est installé un certificat SGC, ce dernier crée un canal 128 bits pour permettre l'encryption 128 bits. Le canal est aussitôt fermé dès que la connection sécurisée se termine ou que la session se termine.
D'autre part, dans le cas d'un domaine FQDN, si le nom du domaine d'un certificat ne correspond pas au nom de domaine du site Web, vous recevrez un avertissement avec le choix de continuer ou non. Avec un certificat SGC, la connexion échoue sans autre explication.

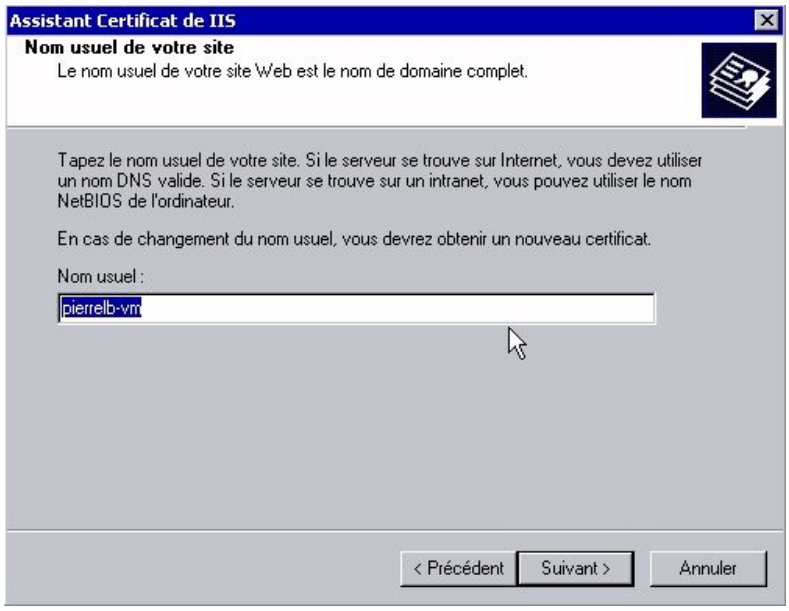


Figure7 : Un certificat serveur étant unique à chaque site Web, le nom usuel du site (common name) est important car il garantit l'unicité du certificat qui sera installé sur le site Web. Le nom usuel peut être soit le nom du serveur (comme dessus) ou bien le nom FQDN.

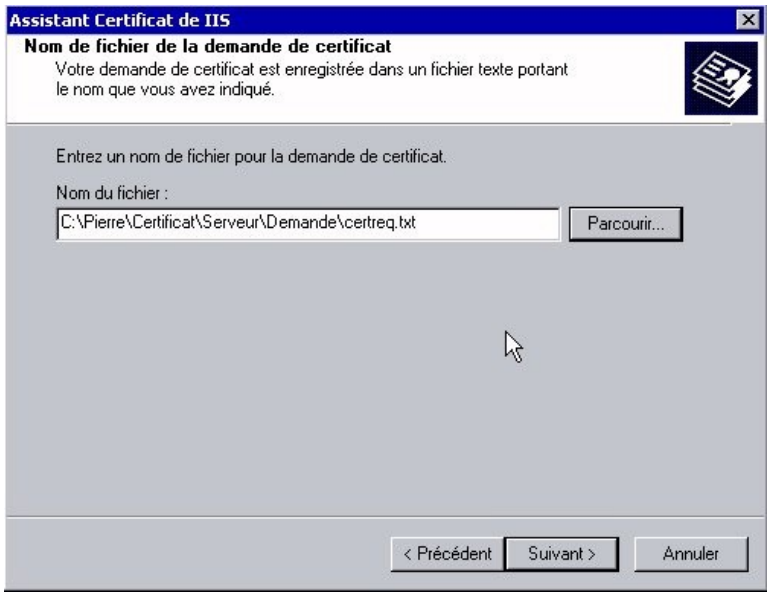


Figure 8 et 9 : Création d'un fichier contenant la demande de certificat serveur.

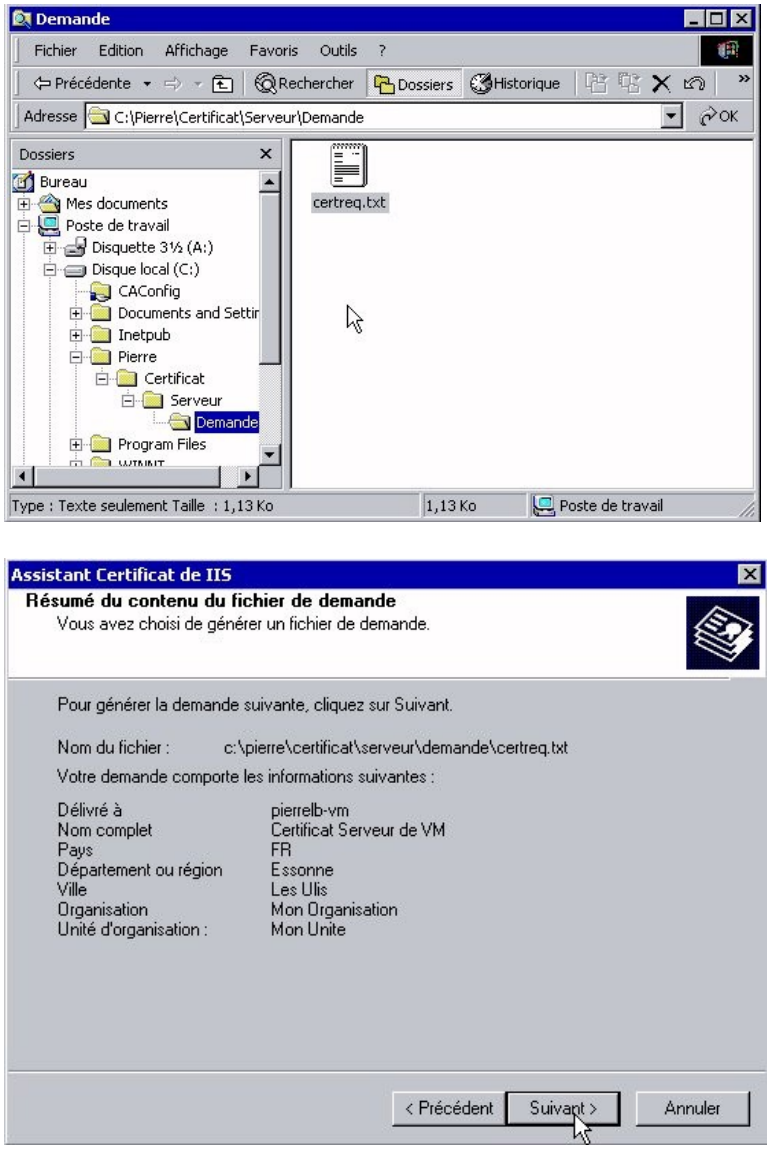


Figure 10 : Résumé des informations caractérisant la demande du certificat serveur.

Figure11 : Une fois la demande de certificat effectuée, Microsoft Certificate Server vous guide pour la suite des opérations à effectuer, à savoir la soumettre à un organisme de certification. A noter qu'une liste des autorités de certification disponibles pour authentifier votre demande est accessible sur le site Web de Microsoft.

2. Soumission d'une requête de certificat

Dans l'exemple que nous avons choisi de vous montrer, nous avons choisi de soumettre la demande de certification auprès de notre propre organisme de certification privé, créé à l'étape 1 « Installation d'un serveur de certificat Root CA ». C'est ce dernier qui va recevoir la demande, la valider et nous renvoyer alors un certificat authentifié par ses soins.

La procédure qui suit est spécifique à un serveur de certificat Root CA installé avec Microsoft Certificate Server, mais le principe de traitement, validation et renvoi du certificat authentifié est le même pour tous les autres organismes de certification (Verisign, Thawte, ...).

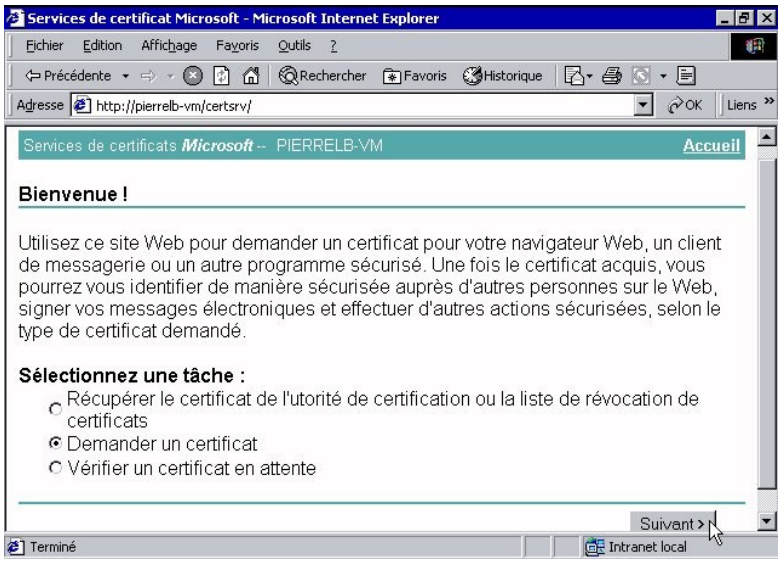


Figure12 : La demande de notre certificat est soumise à l'organisme de certification privé (PIERRELB-VM) qui propose un formulaire à remplir via l'assistant Microsoft Certificate Server 2.0.

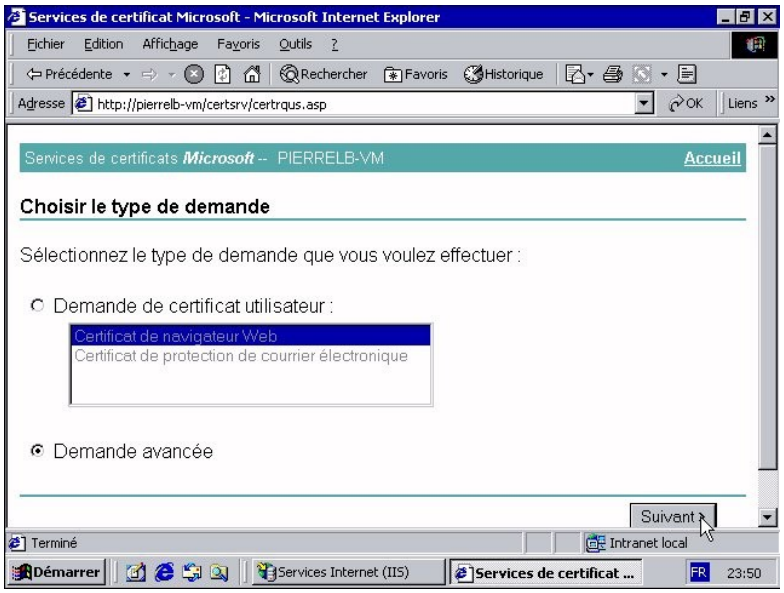


Figure13 : Microsoft Certificate Server propose plusieurs choix : soit de nous fournir un certificat client (cette étape sera vue ultérieurement), soit de fournir des options avancées puisqu'il s'agit ici

d’installer un certificat serveur. La deuxième option est choisie.

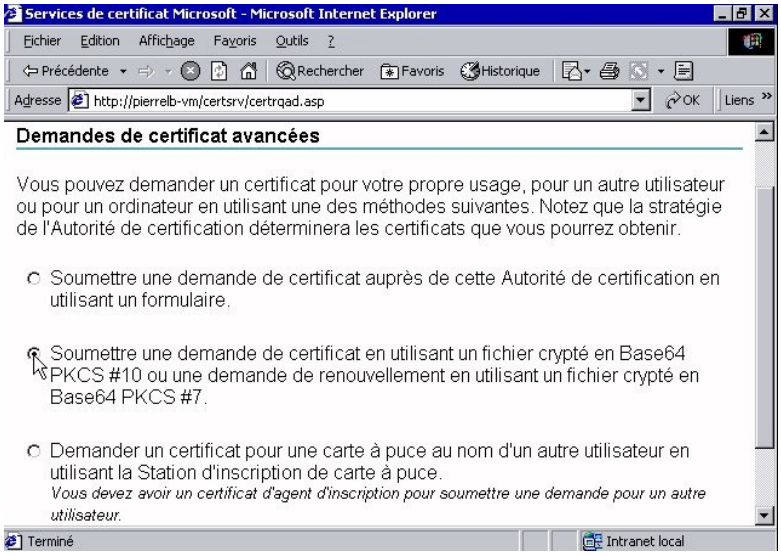


Figure14 : Microsoft Certificate Server propose plusieurs type de demandes : Il est recommandé de choisir l’option du milieu, car sécurisé pour l’envoi de notre demande.

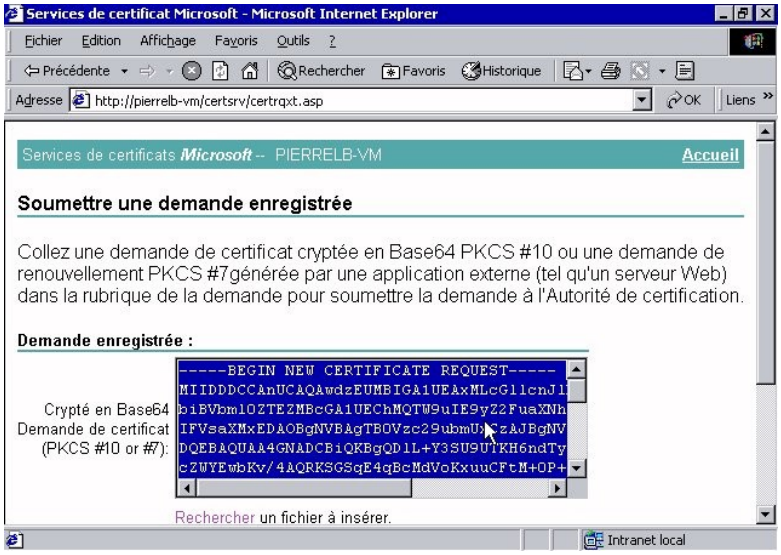


Figure15 : Le contenu du fichier certreq.txt, créé précédemment, est édité dans Notepad, copié et

collé à l'intérieur du formulaire ci-dessus proposé par Microsoft Certificate Server 2.0.
Attention : de bien inclure les champs ----- BEGIN NEW CERTIFICATE REQUEST et ----- END NEW CERTIFICATE REQUEST, sinon votre demande sera invalide.

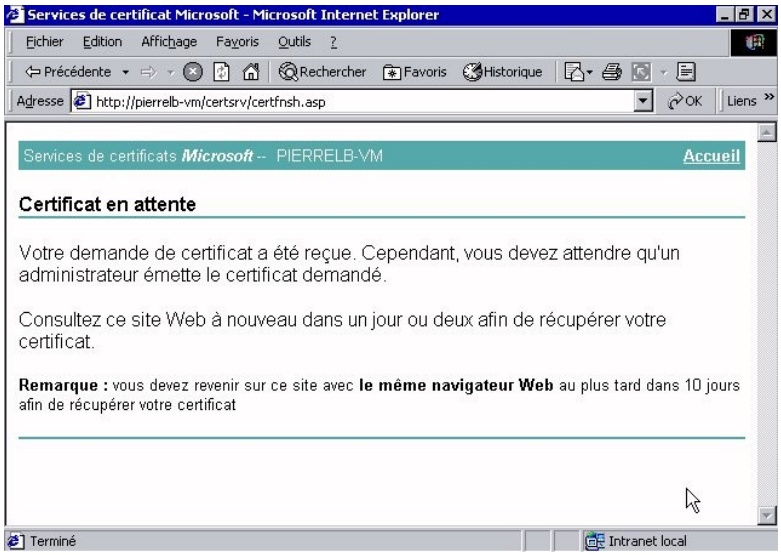


Figure16 : Une fois la demande soumise à l'organisme de certification, vous n'avez plus qu'à attendre qu'il vous retourne le certificat. Rappelons qu'avec organisme de certification « classique » (Verisign ou Thawte), ce service payant et le traitement peut prendre quelques jours. Avec notre propre autorité de certification créée avec Microsoft Certificate Server, notre demande va pouvoir être traité tout de suite dans la prochaine étape, et ce service est gratuit.

Dans notre exemple, le message donné par Certificate Server et présenté dans la figure 16 ci-dessus, le serveur PIERRELB-VM est configuré par défaut pour mettre en attente les demandes de certificat afin qu'un administrateur du serveur de certification puisse valider manuellement cette demande, ceci afin de garantir une validation manuelle et non automatique par le serveur de certification.

Cependant, il est possible de configurer le serveur de certification pour qu'il accepte par défaut toute demande (Dans Autorité de certification, propriétés du serveur, onglet Module de stratégie, bouton Configurer) : un autre écran sera alors montré, qui vous évitera d'attendre la validation de la demande et le téléchargement du certificat une fois validé. Dans ce cas, l'étape 3 est ignorée et l'étape 4 est effectuée directement.

3. Traitement et téléchargement d'un certificat

Cette étape se décompose en deux parties distinctes :

- Traitement de la demande, envoyée par le client à l'organisme de certification privé.

  Ce traitement est effectué par un administrateur au sein de l'organisme de certification privé. Il a simplement à approuver ou refuser la demande via la procédure suivante :

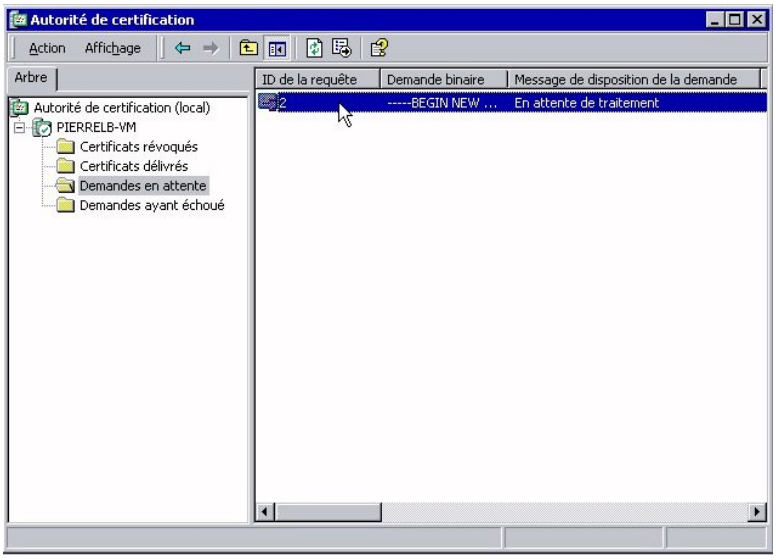


Figure17 : Sur le serveur de l'organisme de certification privé, l'administrateur lance l'application Autorité de certification dans

Menu Démarre-Programmes-Outils d'Administration. La liste des certificats en attente est affichée.

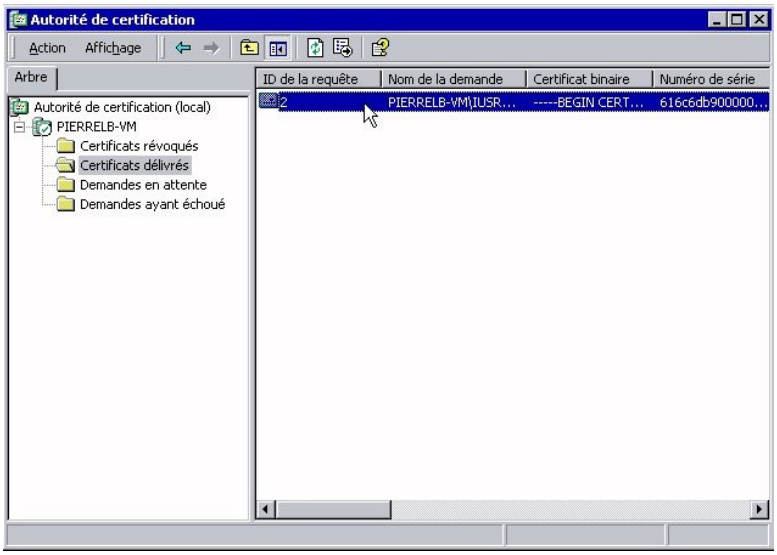


Figure18 : L'administrateur n'a plus ensuite qu'à sélectionner le bon certificat en attente, puis à le valider par un simple clic droit sur la demande : un menu contextuel est proposé pour refuser ou délivrer le certificat. Une fois délivré, le certificat apparaît maintenant dans la liste des certificats délivrés :

- Téléchargement

Une fois la tâche de l'administrateur de l'organisme de certification privé terminée, nous recevons par mail un avis comme quoi notre demande de certificat a été validée et qu'il ne nous reste plus qu'à télécharger le certificat serveur sur le site Web de l'organisme de certification privé.

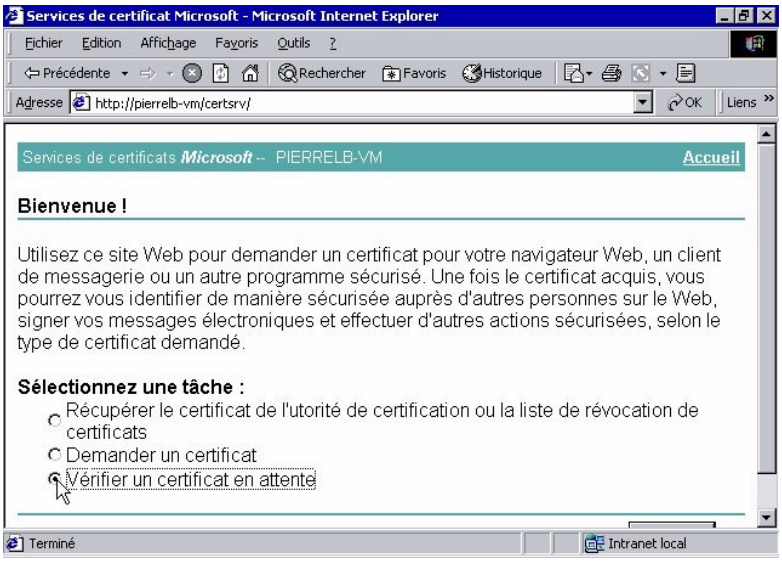


Figure19 : Pour télécharger le certificat serveur validé par l'organisme de certification, il faut se reconnecter sur le site de l'organisme, puis Vérifier les certificats en attente.

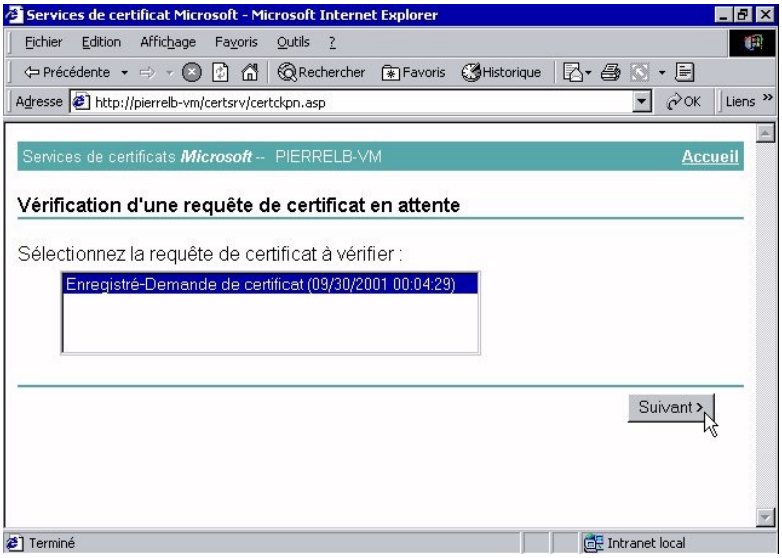


Figure20 : Le certificat délivré est bien disponible et visible. Il suffit de le sélectionner, puis de le télécharger localement sur son disque dur.

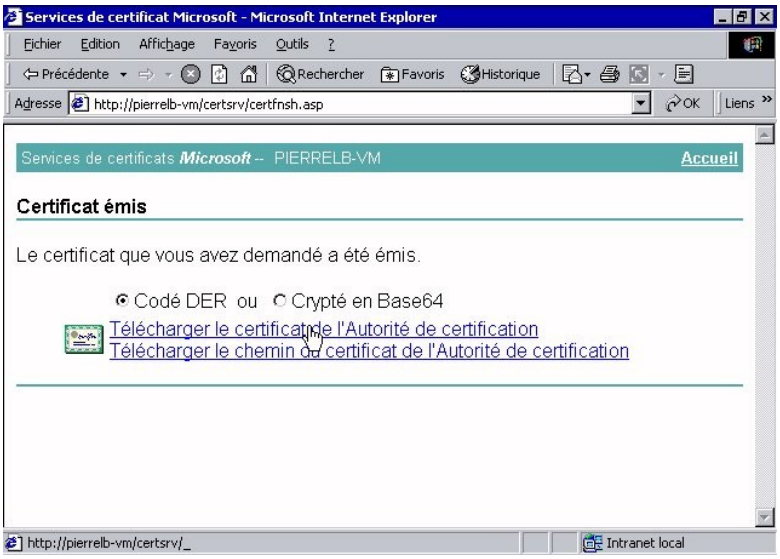


Figure21 : Le certificat est maintenant téléchargeable : choisissez de télécharger le certificat issu de l'autorité de certification, codé DER.

Figure 22 : le certificat de l'autorité de certification privé (CERTNEW.CER) vient d'être téléchargé sur notre poste de travail.

-

4. **Installation du certificat et paramétrage du site Web SSL**

Maintenant que nous possédons ce certificat CERTNEW.CER, il ne nous reste plus qu'à l'installer sur notre serveur Web HTTP. Il existe deux méthodes pour cela :

- soit copiez le certificat directement sur le serveur Web, puis double-cliquer dessus pour l'installer.
- Soit l'installer par l'assistant d'installation de certificat pour pré installer le certificat, puis le lier au site Web à sécuriser. Nous vous proposons la deuxième méthode ci-dessous :

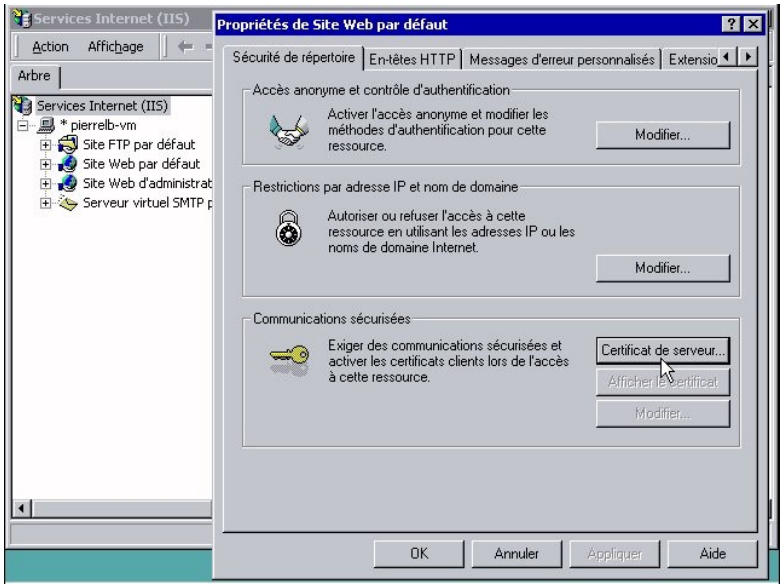


Figure 23 : Sur le serveur Web à sécuriser, Nous allons lancer l'assistant d'installation du certificat de l'autorité de certification privé (CERTNEW.CER) via le gestionnaire des services Internet. Après avoir sélectionné le site Web, et avoir choisi l'onglet « Sécurité de répertoire » dans les propriétés, nous cliquons sur le bouton Certificat de Serveur.

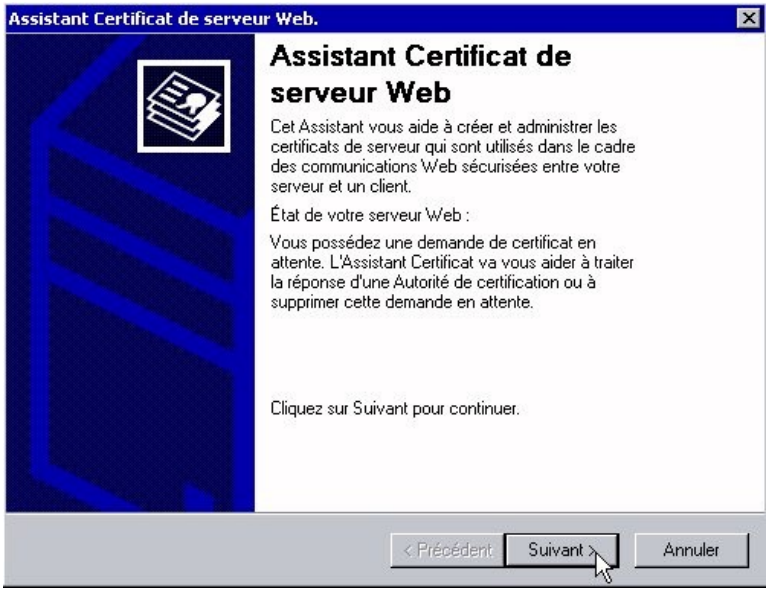


Figure 24 : L'assistant Certificat de serveur Web est alors exécuté, et le procédure d'installation de CERTNEW.CER sur votre site Web sélectionné peut commencer.

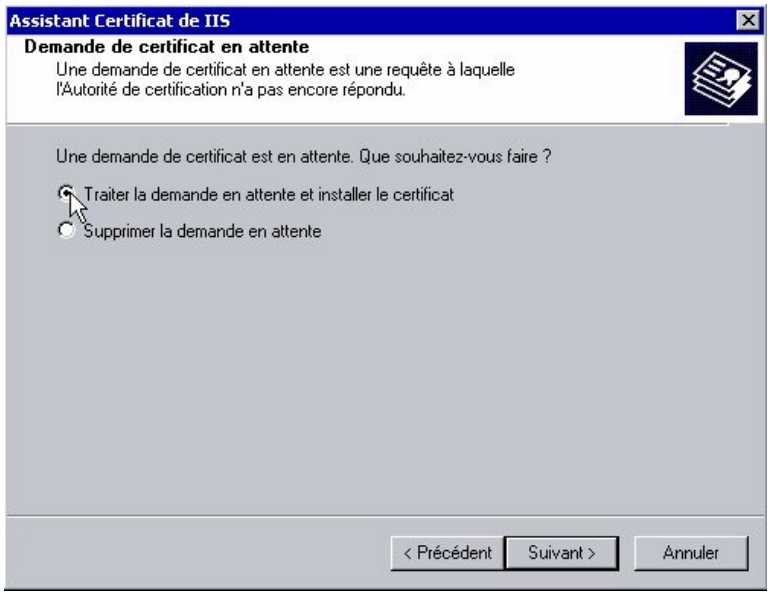


Figure 25 : L'assistant Certificat de serveur nous propose de traiter la demande en attente et d'installer le certificat.

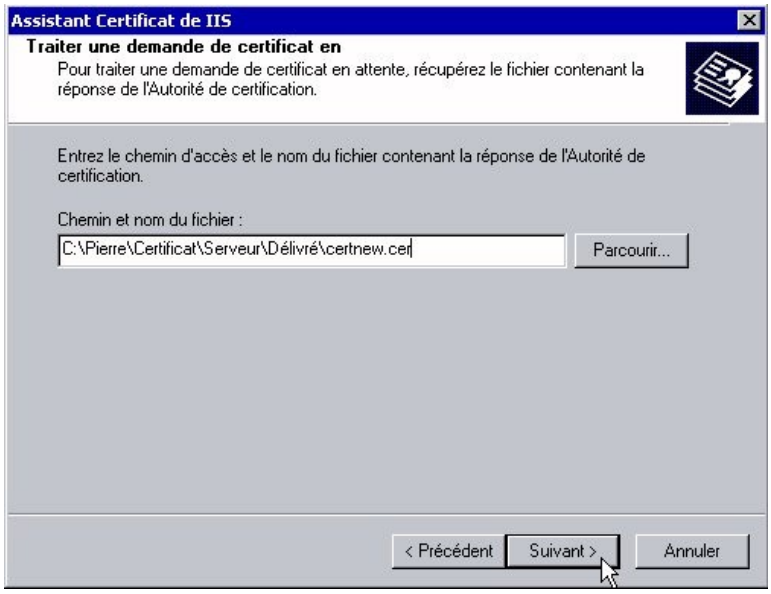


Figure 26 : L'assistant Certificat de serveur nous demande alors de lui fournir le certificat délivré sous forme de fichier CERTNEW.CER.

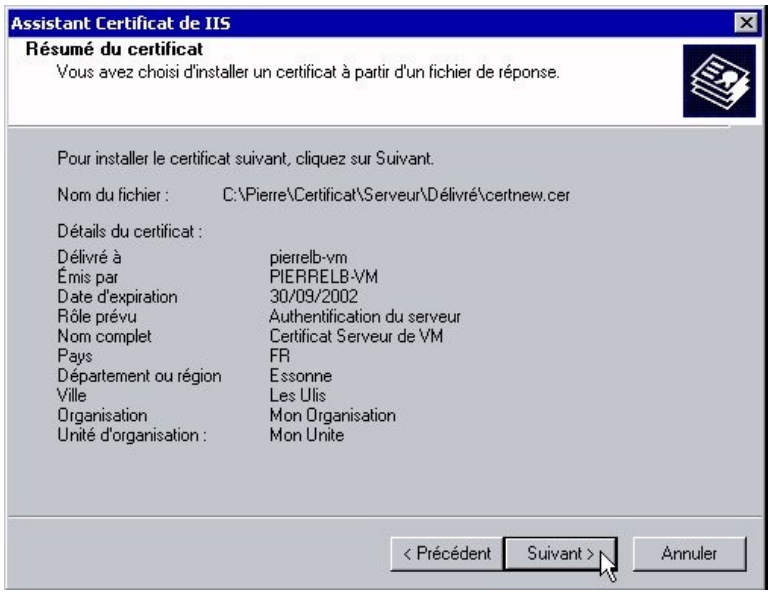


Figure 27 : L'assistant Certificat de serveur présente un résumé de toutes les caractéristiques avant d'installer le certificat pour le site Web.

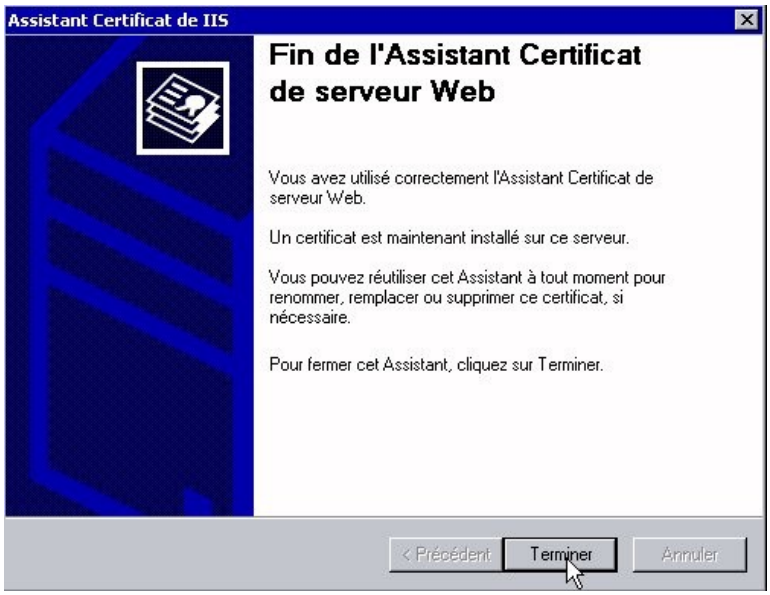


Figure 28 : L'assistant Certificat de serveur Web nous confirme que le certificat est correctement installé sur notre serveur.

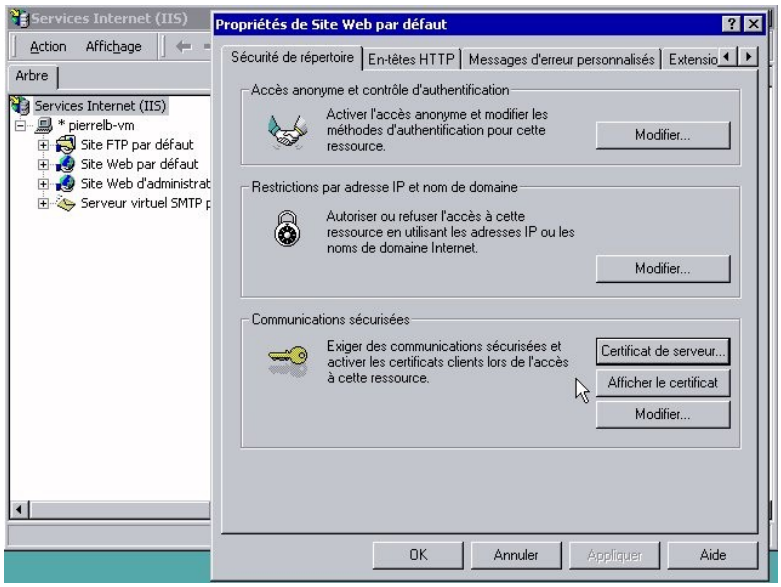


Figure 29 : Après avoir quitté l'assistant Certificat de serveur Web, nous constatons que deux nouveaux boutons apparaissent concernant les communications sécurisées : Afficher ou bien Modifier le certificat installé.

Il nous reste maintenant à configurer et à tester le certificat du côté du serveur en suivant les dernières étapes suivantes :

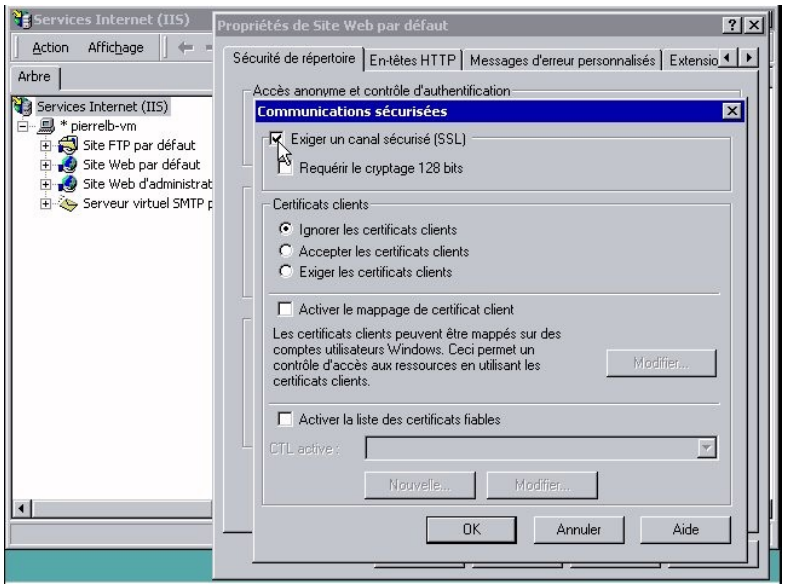


Figure 30 : Nous choisissons alors de modifier les communications sécurisées. Par défaut, le canal SSL n'est pas activé : un simple clic sur l'option Exiger un canal sécurisé SLL permet de l'activer. Par défaut les certificats clients sont ignorés et n'ont pas besoin d'être présentés au serveur Web pour accéder au site Web en HTTPS.

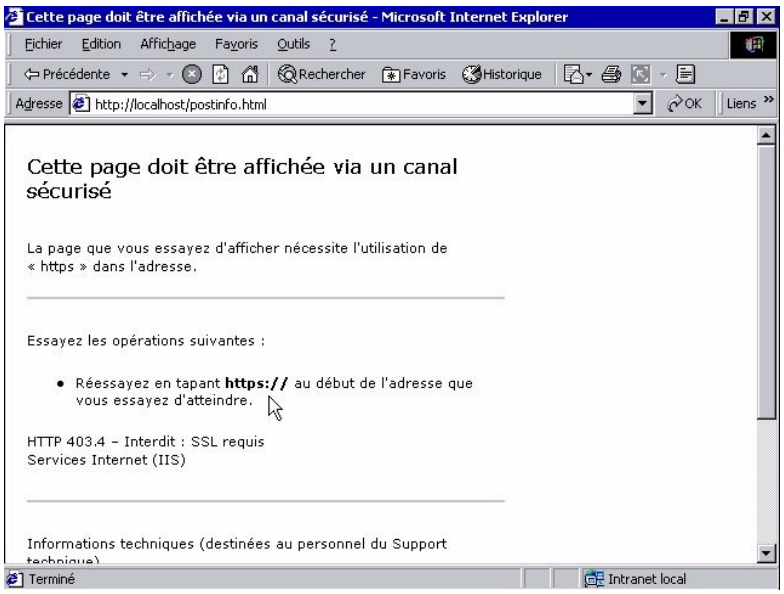


Figure 31 : Pour tester la mise en place du canal sécurisé SSL, essayons d'accéder à notre site Web sécurisé via une adresse URL HTTP : il n'est désormais possible d'accéder à notre site Web qu'uniquement via le protocole sécurisé HTTPS.

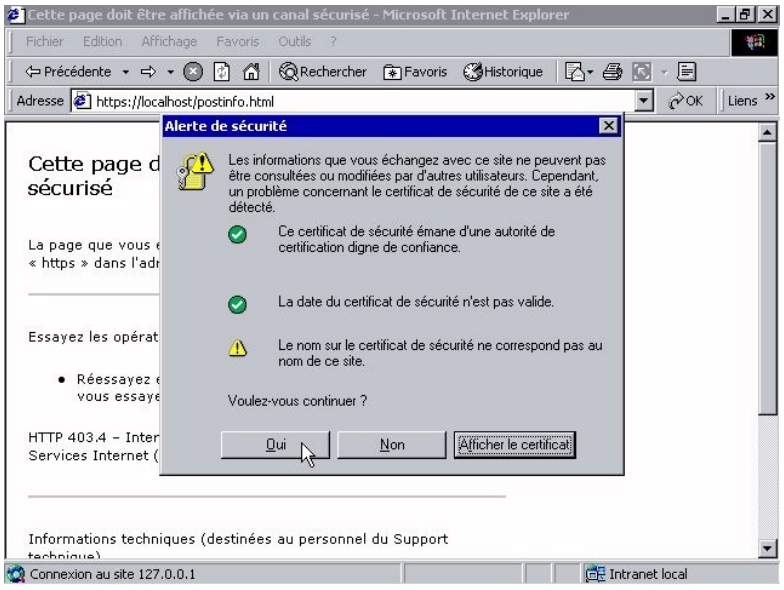


Figure 32 : L'accès au site HTTPS directement effectué depuis le serveur Web sécurisé nous montre plusieurs paramètres sur lequel le

certificat se base pour vérifier la validité de l'accès :

* L'autorité de certification privée : elle est bien connue du serveur Web.

* La date de validité du certificat émis par cet organisme : elle est bien valide et n'est pas périmée.

* Le nom du site sécurisé : il n'est pas correct. Pourquoi ?

Tout simplement parce que lorsque la demande du certificat é été émise à l'organisme de certification privé, nous avions spécifié le Common Name (Nom usuel) comme étant égale à la valeur « pierrelb-vm ». Comme nous tentons d'accéder à un site appelé localhost, il n'y a pas de correspondance entre les deux noms, d'où cet avertissement. Nous pouvons alors accepter quand même d'accéder à ce site : c'est à l'utilisateur final de décider de l'action à effectuer en toute connaissance de cause.

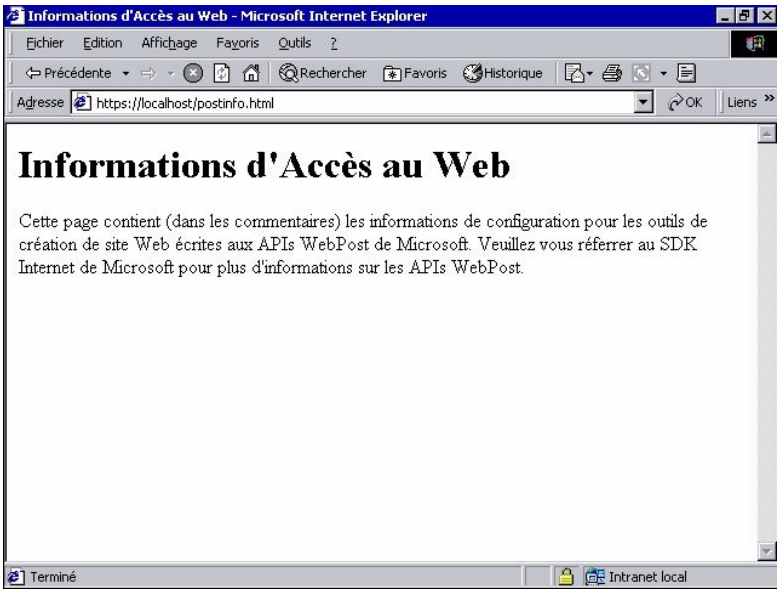


Figure 33 : L'accès à été autorisé : nous pouvons maintenant accéder au site Web en HTTPS.

-
- -

b. Activer la sécurisation d'un site Web par SSL : Authentification par certificat côté client

Il existe plusieurs manières d'installer le certificat Root CA dans la liste des Root CA de confiance dans Internet Explorer 5 :

- Par mail : envoyez le certificat à tous vos utilisateurs pour qu'ils puissent l'installer simplement.
- Par téléchargement : une page de téléchargement propose un lien vers le certificat Root CA.
- Par IEAK : dans le cadre de déploiement massif de nouvelles versions d'Internet Explorer, vous pouvez directement intégrer le certificat au sein des autorités de confiance dans le paquetage IEAK.

De toutes les manières, le certificat Root CA doit être installé sur les postes client pour indiquer à Internet Explorer de faire confiance au fait que le certificat de votre site n'est pas le certificat que vous venez juste de créer, mais plutôt le certificat Root CA, créé lorsque Certificate Serveur a été installé.

i. Installation du certificat Root CA

Pour ce faire, il nous faut télécharger le certificat depuis notre poste client :

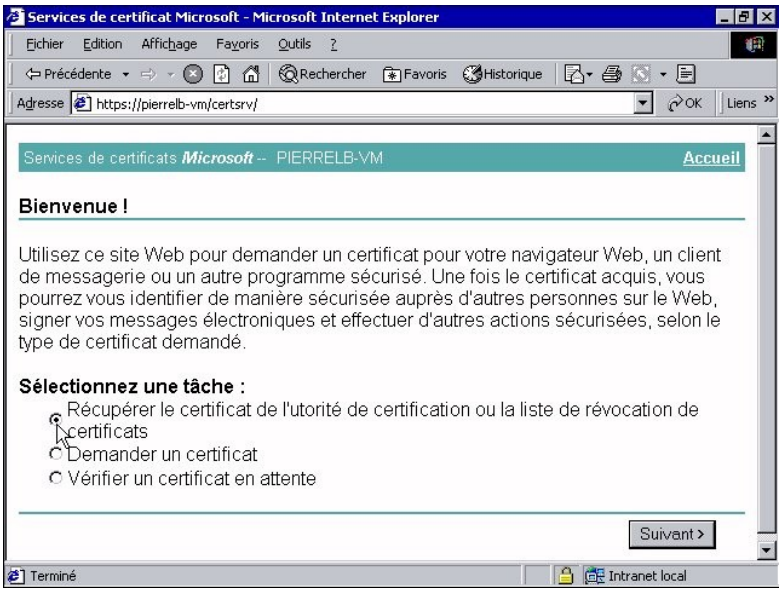


Figure 34 : Nous nous connectons (en HTTPS cette fois !) sur notre site Web où a été installé le certificat Serveur Root CA, afin de le récupérer en vue de l'installer sur le poste client.

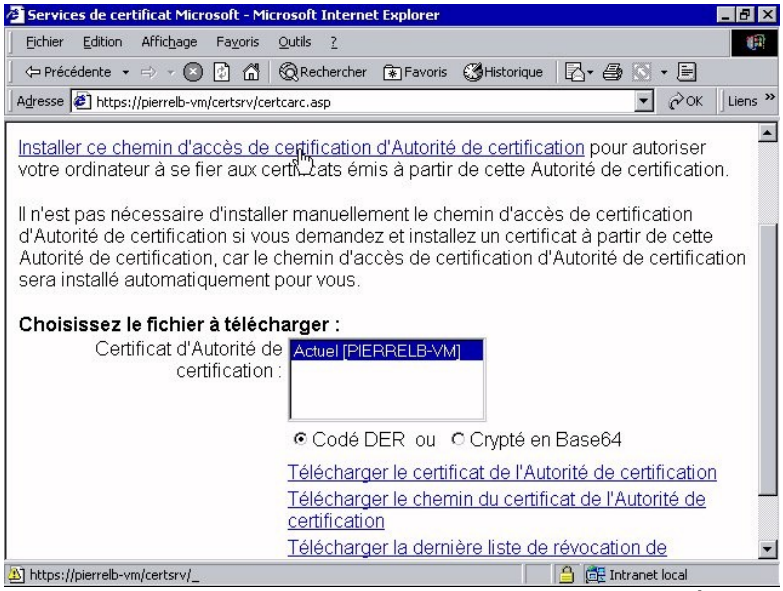


Figure 35 : Deux possibilités s'offrent alors à vous : Installer automatiquement ce certificat serveur depuis le chemin d'accès connu dans Internet Explorer.

Télécharger ce certificat serveur, le sauvegarder sur disque, puis double-cliquer sur le certificat pour démarre l'assistant d'installation du certificat serveur sur le poste client en choisissant l'emplacement physique (store) correspondant aux autorités de certification de confiance.

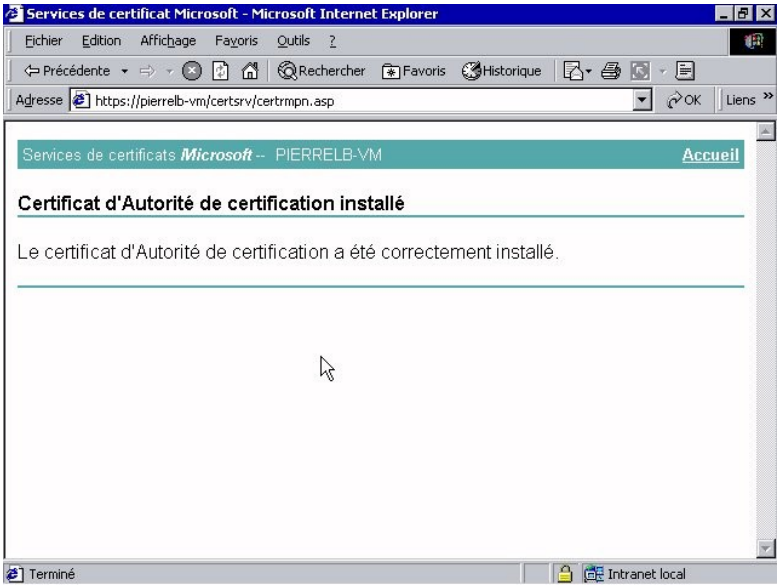


Figure 36 : En ayant choisi la première possibilité, voici alors ce que nous obtenons. La nouvelle autorité de certification vient d'être rajouté dans le store des autorités de certification dignes de confiance dans Internet Explorer de votre poste client.

ii. Installation du certificat client lié au CA

Jusqu'à présent, nous n'avions pas besoin de présenter sur nos postes client un certificat client. Cependant, dans le cas présenté ci-dessous où vous configurez votre serveur Web HTTPS pour exiger la présentation d'un certificat client, il est nécessaire d'installer un certificat client.

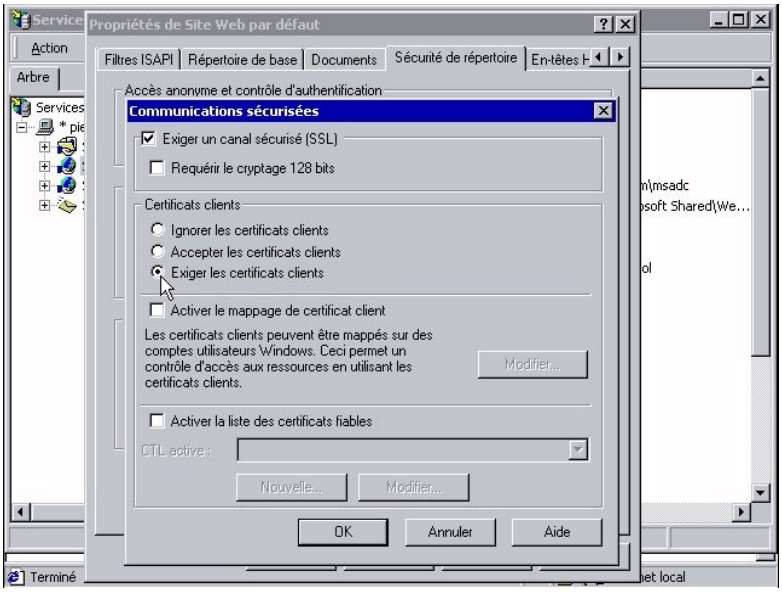


Figure 37 : Voici comment configurer votre site Web HTTPS afin d'exiger la présentation d'un certificat client installé sur le poste client.

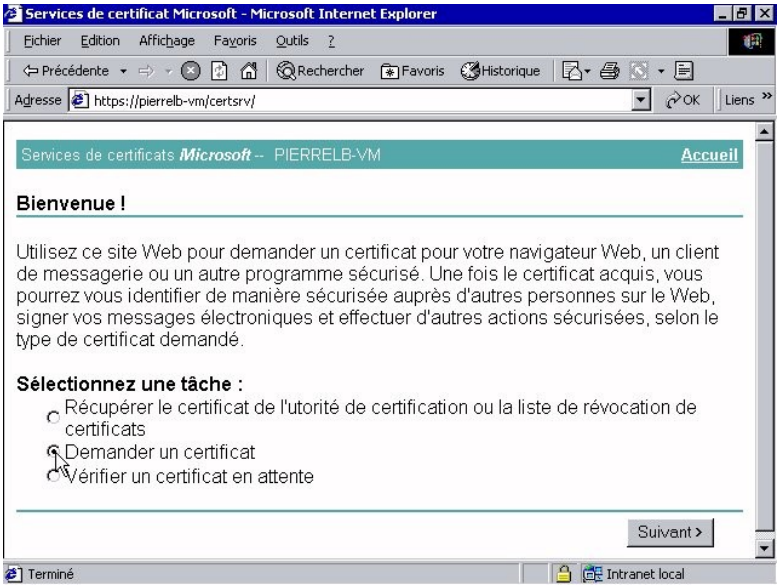


Figure 38 : Une fois configuré le site Web, il est nécessaire de créer un certificat client puis de l'installer dans Internet Explorer du poste client.

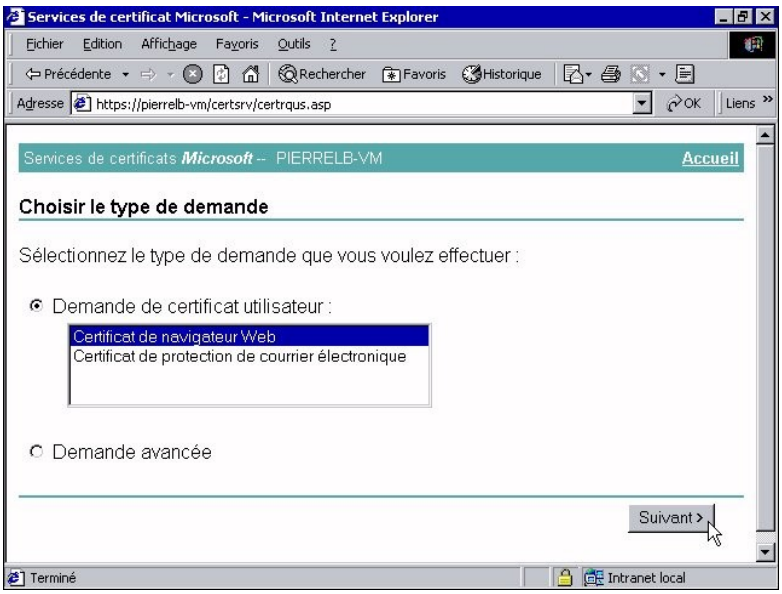


Figure 39 : Certificate server nous propose alors d'effectuer une demande de certificat client concernant la navigation sur le Web.

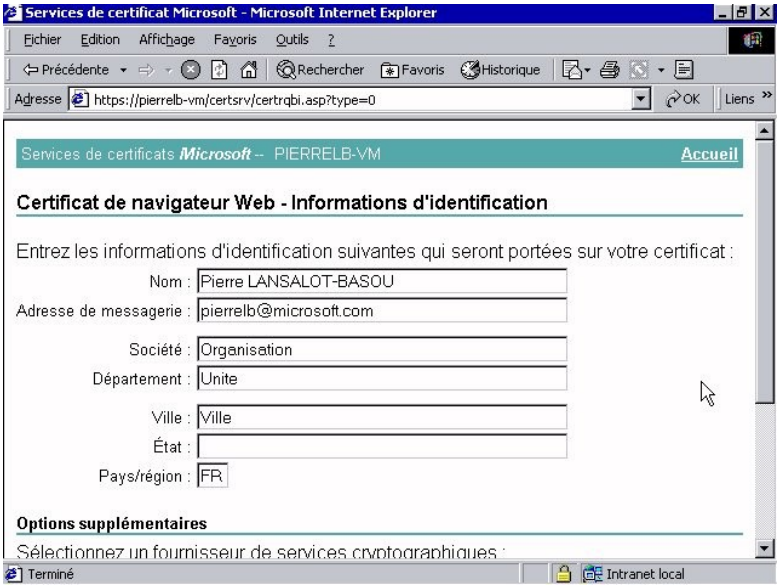


Figure 40 : Certificate server présente un formulaire demandant quelques informations concernant cet utilisateur. Notez que les informations concernant la société, le département et le pays sont affichés automatiquement, puisque cet utilisateur doit faire

partie de l'organisation .du serveur sur lequel il essaie d'accéder.

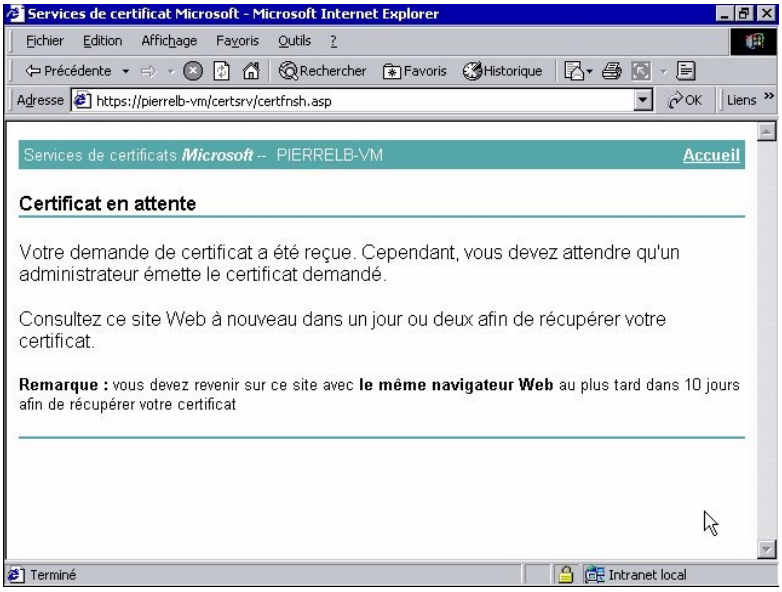


Figure 41 : Le certificat utilisateur est alors créé et est en attente de validation par l'autorité de certification.

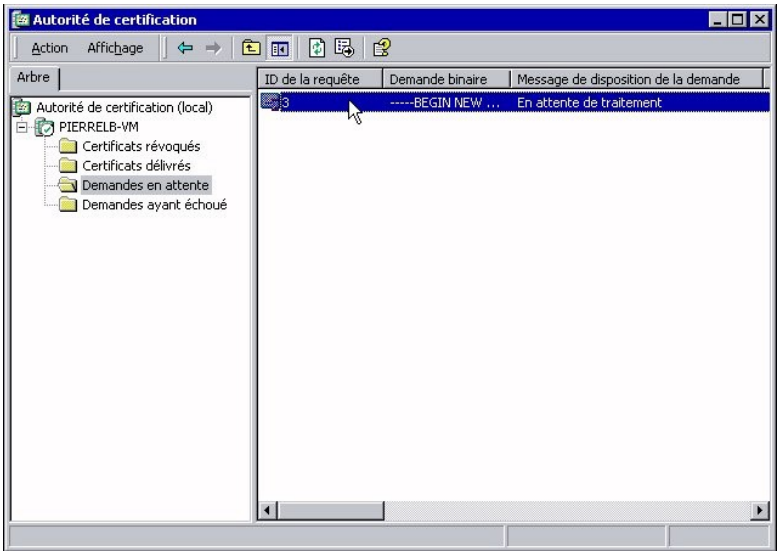


Figure 42 : Dans le programme Autorité de Certification, le certificat client est alors en attente de validation par un administrateur. Une fois qu'il est délivré, depuis le même poste utilisateur, nous allons

vérifier les certificats en attente : nous voyons alors notre certificat client délivré qui est en attente.

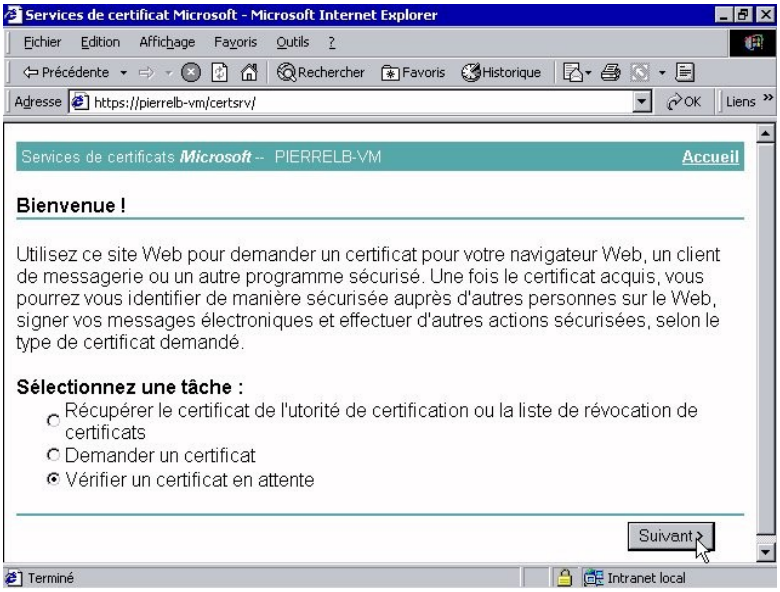


Figure 43 : Vérification des certificats en attente.

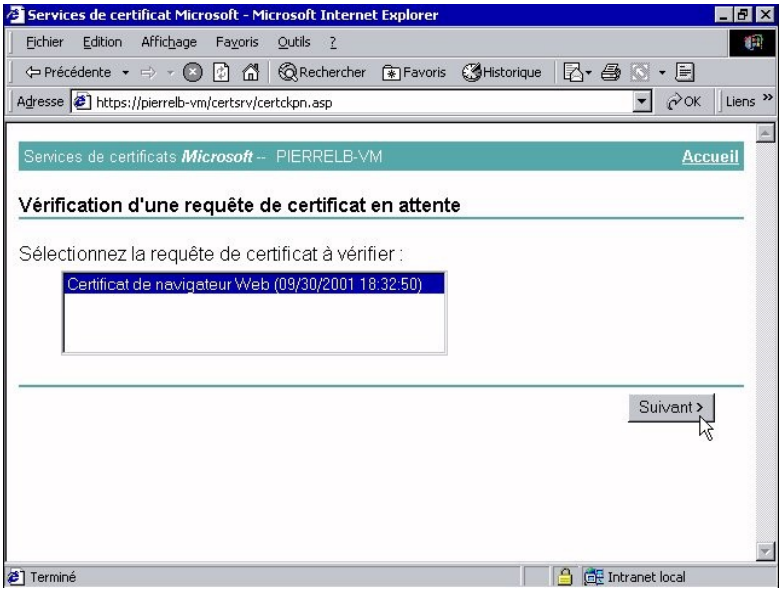


Figure 44 : Nous retrouvons notre certificat client qu'il nous maintenant télécharger et installer sur notre poste utilisateur.

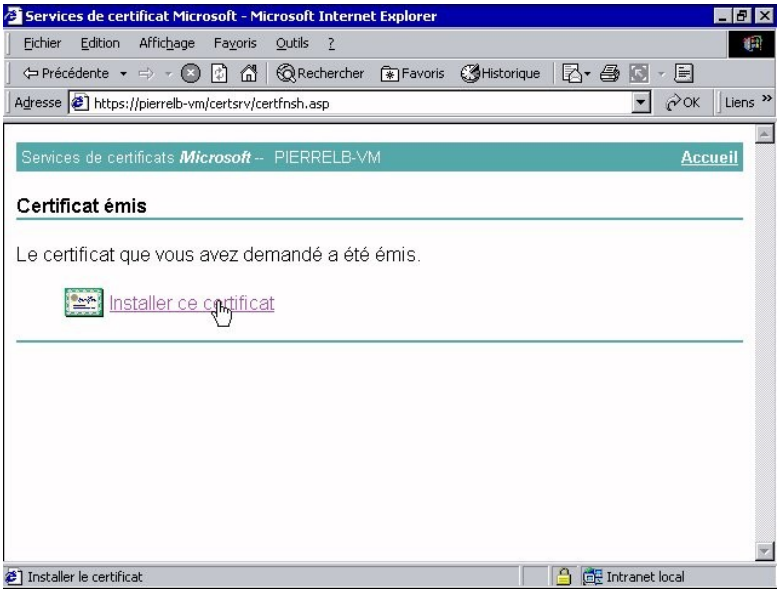


Figure 45 : Il nous est alors proposé d'installer directement sur notre poste utilisateur le certificat client.

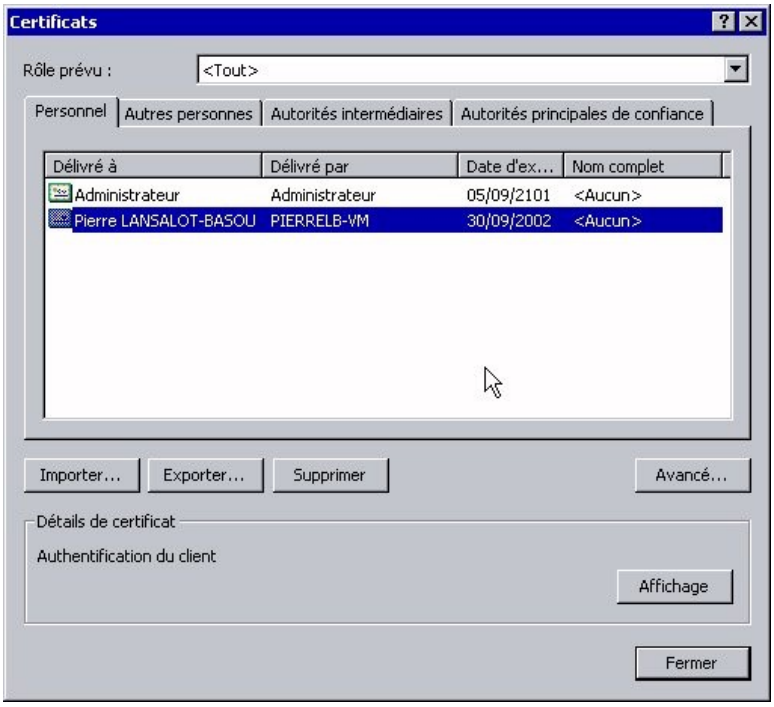


Figure 46 : Une fois installé ce certificat client, il nous suffit de vérifier qu'il apparaît bien dans Internet

Explorer du poste utilisateur : Options Internet – Onglet Contenu – Bouton Certificats – Onglet Personnel : Le certificat client pour l'utilisateur Pierre LANSALOT-BASOU apparaît dans la liste maintenant comme certificat personnel.

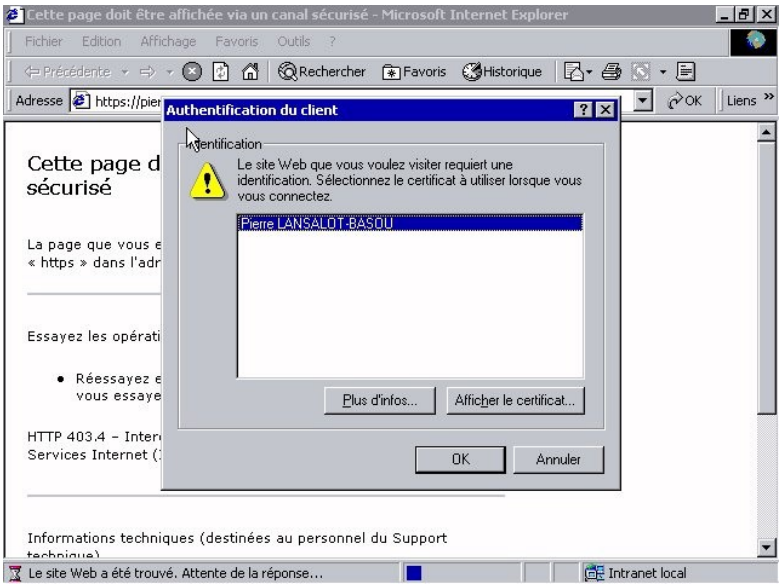


Figure 47 : Lorsqu'on tente maintenant d'accéder au site HTTPS, le client IE présente une liste des certificat client correspondant à l'autorité de certification privé qui a configuré le serveur Web en HTTPS. C'est à l'utilisateur alors de choisir de présenter le certificat client au serveur et de valider son choix.

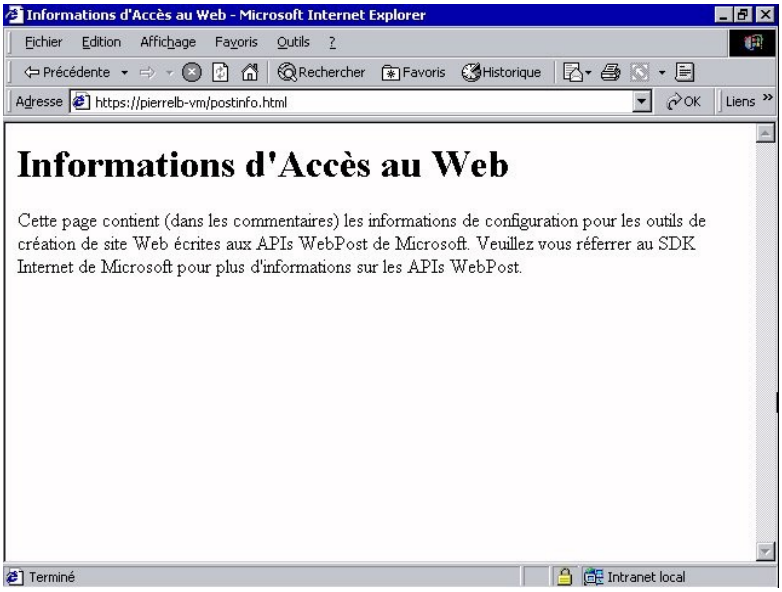


Figure 48 : Le site Web a accepté la présentation du certificat client : le client accède alors au site HTTPS sécurisé de bout en bout.

3) Présentation de la CRL

a. Validité d'un certificat :

Un certificat (client ou de l'autorité de certification privée) possède certaines caractéristiques qui indiquent sa validité.

Ces paramètres sont :

- l'autorité de certification Root CA.
- La date de validité.
- Le common name (ou nom usuel)

i. Root CA

Celle-ci doit être connue du serveur et du client dans une architecture client/serveur SSL.

ii. Date de validité du certificat serveur et client

Un certificat a une durée de vie limitée. Il est délivré par l'autorité de certification. Passée cette date, le certificat expire et il est nécessaire alors de demander un nouveau certificat dont la durée de validité sera prolongée pour une nouvelle période.

iii. Domaine

Un certificat est délivré par l'autorité de certification pour une adresse de domaine DNS unique. Ainsi, dans notre exemple en laboratoire, nous avons vu que notre certificat a été délivré pour un nom de serveur http://pierrelb-vm. Si je tente d'accéder à ce serveur avec un autre nom (par exemple http://localhost) , un message m'indiquera que le certificat n'est pas fait pour accéder à un tel site. Il est du ressort final de l'utilisateur de continuer ou non une fois qu'il est prévenu.

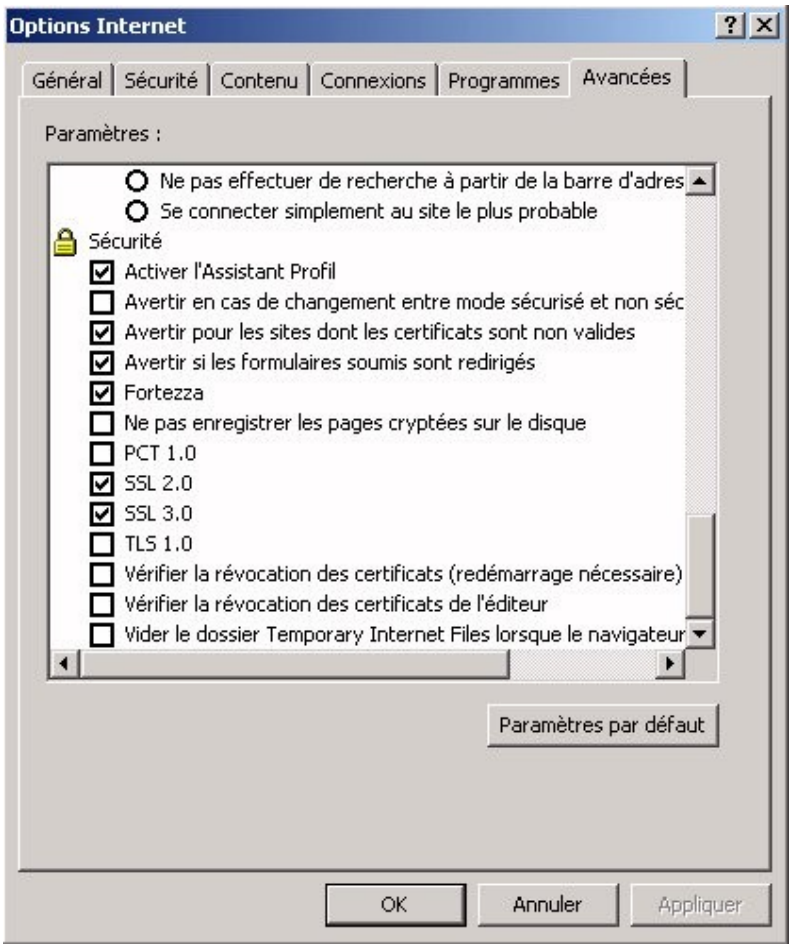
b. Vérification en ligne de la validité d'un certificat

i. Côté client IE5

Toute autorité de certification privée gère une CRL (Certification Revocation List). Cette liste contient l'ensembles des serveurs qui ne sont plus considérés comme ayant un certificat valide. Cette liste peut être

accessible en ligne directement par les postes clients Internet Explorer quand ils se connectent au serveur Web : ils vérifient ainsi auprès du CA qui a fournit ce certificat et si le serveur en question n'est pas dans la CRL en question en comparant le nom donné dans le certificat et les membres de cette liste.

Cette liste s'active sous Internet Explorer dans les Options avancées :



ii. Côté serveur IIS5

1. L'inverse est vrai également : Il est possible de demander à IIS de vérifier la validité d'un certificat client. Il suffit d'activer dans le registre la clé suivante :

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Inetinfo\Parameters\CheckForServerCertificateRevocation à 1 (0 par défaut).

4) Quelques points importants

a. Export / import du certificat serveur vers un autre serveur IIS 5

Envisageons le cas suivant : pour des raisons diverses dans votre entreprise, il a été décidé de réinstaller complètement votre serveur Windows 2000. Cette opération nécessite donc de réinstaller complètement le système d'exploitation et les applications. Votre entreprise a cependant indique deux éléments indispensables dans le cahier des charges :

- le serveur devra être réinstallé avec le même nom DNS.
- le serveur devra conserver le même certificat serveur SSL.

La question qui se pose est alors la suivante : comment sauvegarder et réinstaller le certificat serveur existant lors de la future réinstallation de notre serveur Windows 2000 ?

Un premier réflexe peut être de réémettre une demande de certificats auprès de l'autorité de certification avec les mêmes informations.

Cela fonctionnera certes, mais il existe une méthode plus adaptée à ce type de demande : **l'exportation et l'importation de certificats serveur**.

Nous vous présentons ici le guide détaillé des étapes à suivre pour exporter correctement un certificat web existant, avant de réimporter ce même certificat sur votre nouvelle installation du serveur.

Comment Exporter & Importer un certificat serveur Web existant ?

- Premièrement, constatons que notre certificat serveur est correctement installé et opérationnel sur notre serveur web : Vous pouvez alors afficher une information importante depuis la console MMC d'IIS :
    - Ce certificat serveur possède une clé privée. Elle devra être exportée par la suite, il est donc nécessaire de s'assurer que la clé privée est fonctionnelle.

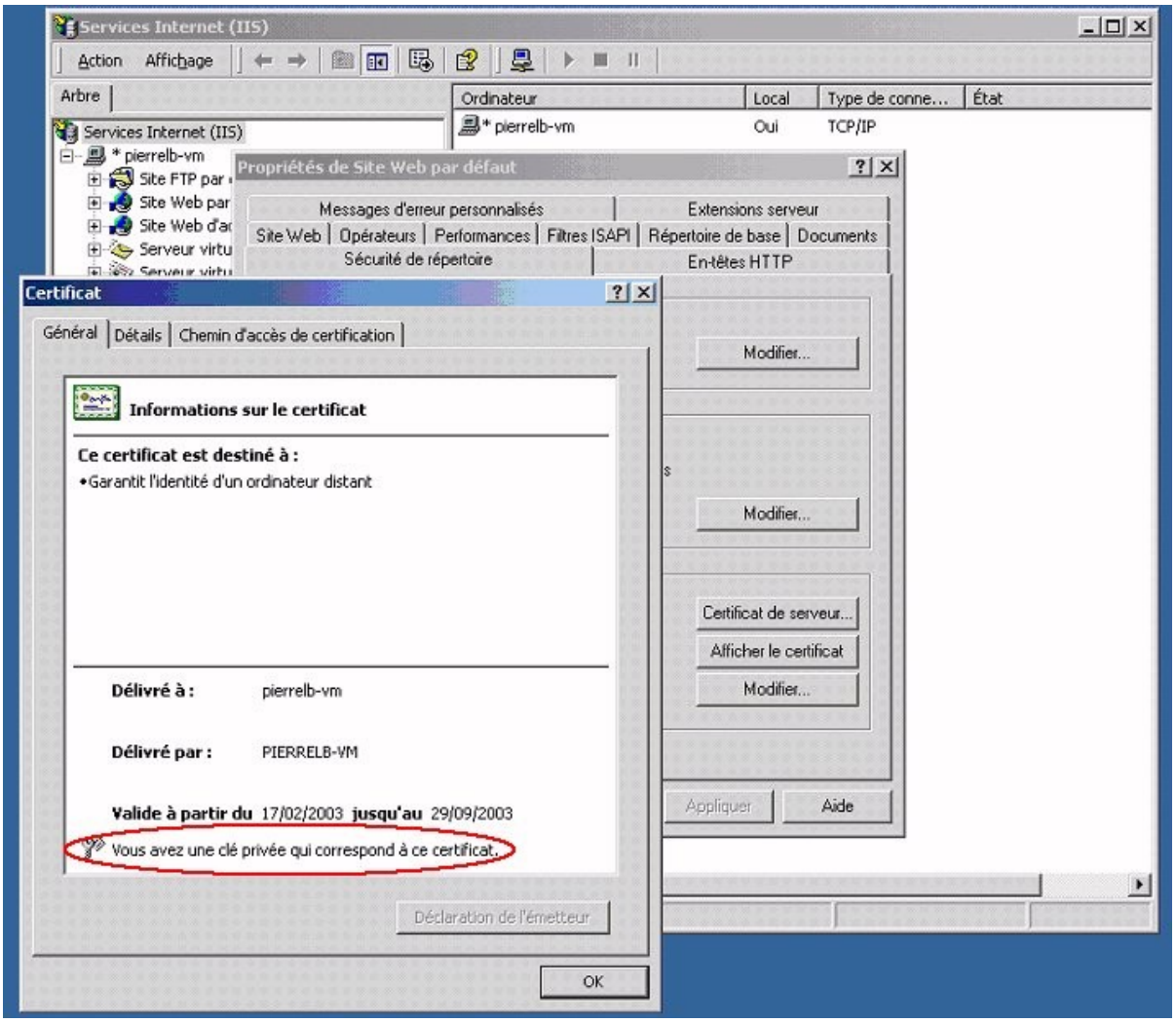


Figure 48 : Le certificat serveur possède bien une clé privée.

- Deuxièmement, nous allons exporter ce certificat serveur dans un fichier. Pour ce faire, la procédure est la suivante :
    - Depuis la console MMC d'IIS, cliquez sur le bouton "Copier dans un fichier".

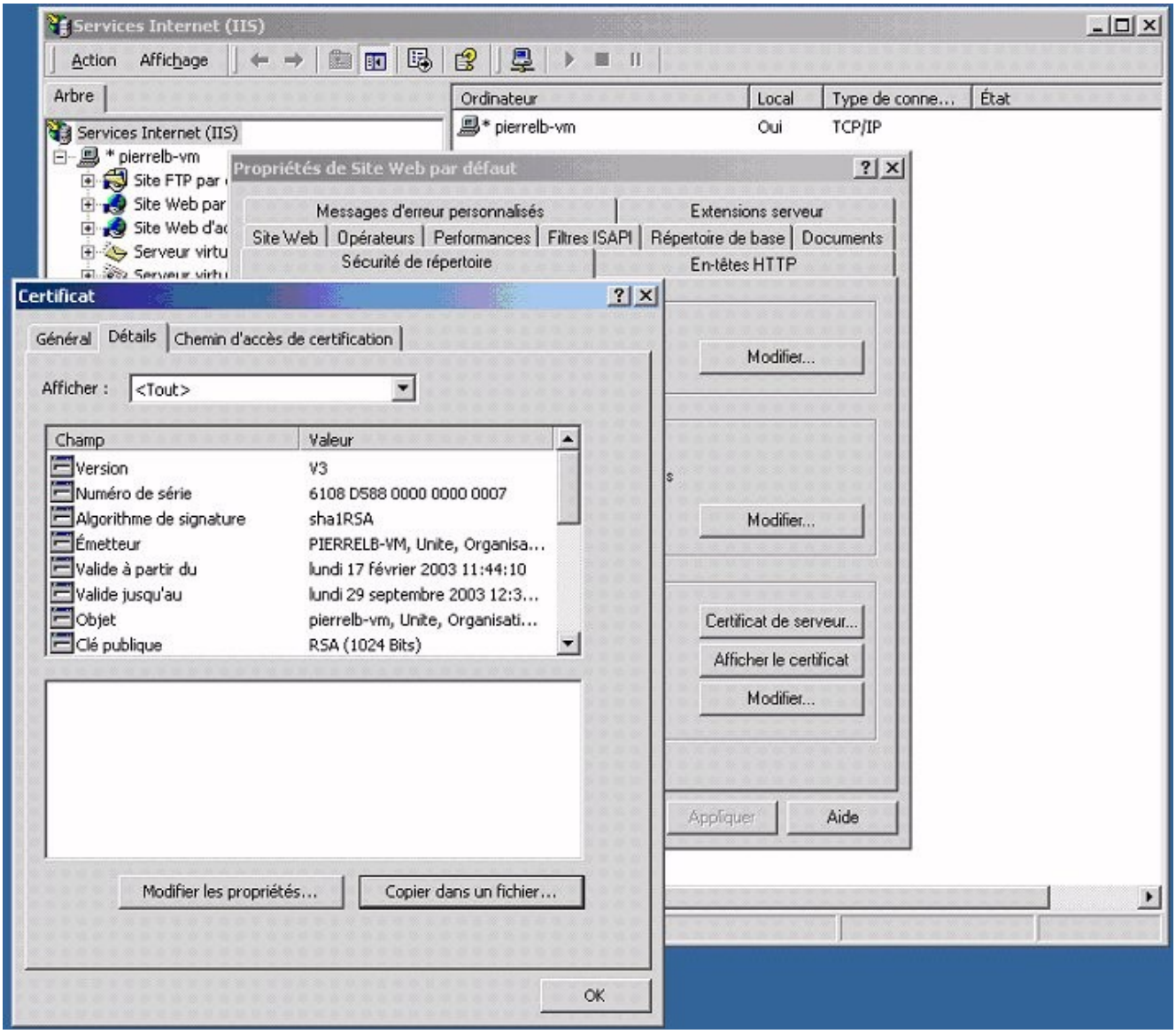


Figure 49 : Dans les détails du certificat, nous allons pouvoir copier le certificat dans un fichier d'un certain format.

- Un assistant est alors lancé pour nous aider lors de l'exportation du certificat serveur : il nous est d'abord demandé si nous désirons exporter ou non la clé privée de notre certificat serveur.

    - A noter que, lors de la demande initiale de votre certificat serveur existant, si vous n'aviez pas spécifié que la clé privée soit exportable, alors seule une option sera accessible).

- Nous vous conseillons de choisir l'option "Oui, exporter la clé privée". Si vous choisissez de ne pas l'exporter, cela peut engendrer des dysfonctionnements voire le non fonctionnement total du certificat une fois celui-ci importé.

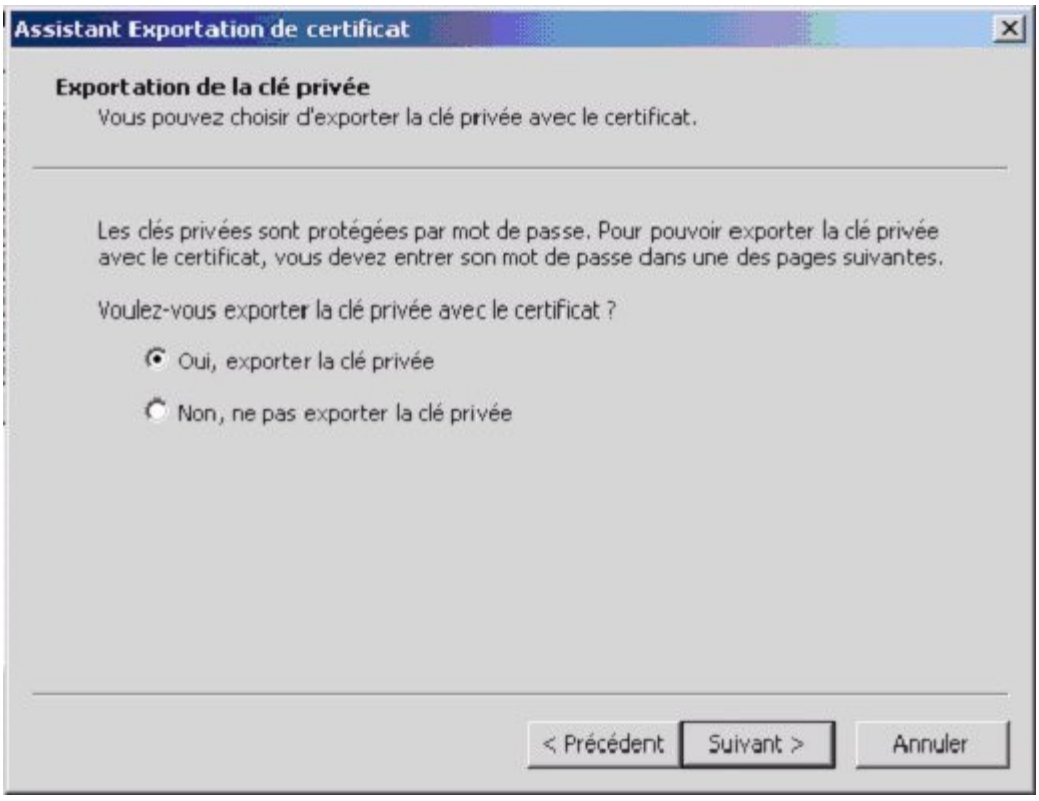


Figure 50 : Nous choisissons d'exporter également la clé privée du certificat serveur dans notre fichier d'export.

- Deux types de formats de fichiers export peuvent alors être utilisés et il est important de connaître la différence entre les deux formats :

  - Fichier export au format **PKCS #7** (extension **.P7B**)

    Ce type de format ne supporte pas l'export de la clé privée : si vous disposez d'un tel fichier dans vos archives, vous pouvez déjà en déduire que ce fichier d'export ne contient pas de clé privée, ce qui peut poser un problème de fonctionnement du certificat lors de son import ("La page ne peut pas être affichée").

  - Fichier export au format **PKCS #12** (extension **.PFX**)

    - Ce type de format supporte pas l'export de la clé privée : si vous disposez d'un tel fichier dans vos archives, vous pouvez déjà en déduire que ce fichier d'export contient pas une clé privée, ce qui est conseillé pour le futur import du certificat.

Comme vous avez pu le comprendre, nous recommandons que vous puissiez exporter votre certificate serveur dans un format PKCS#12, avec les options montrées dans la figure 51 :

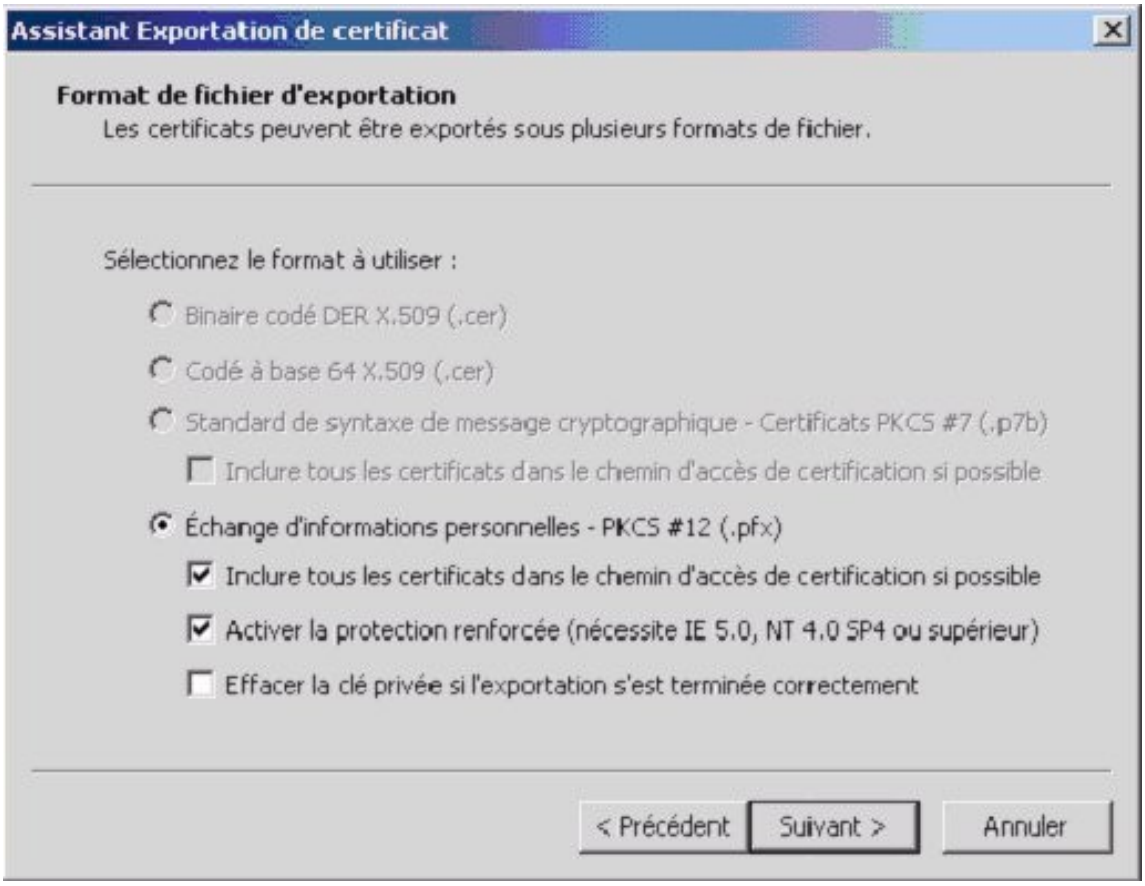


Figure 51 : Les options sélectionnées pour l'export du certificat serveur au format PKCS #12 sont nécessaires : Conservation de la chaine des serveurs CA et activation de la protection renforcée (mot de passe pour protéger la clé privée exportée).

Note : Pour votre information, si vous aviez choisi de ne pas exporter la clé privée de votre certificat serveur, la figure 52 montre l'écran que vous auriez obtenu :

Figure 52 : Vous avez choisi de ne pas exporter la clé privée et de sauvegarder le certificat serveur au format PKCS #7. Dans ce cas, conservez également toute la chaîne des certificats en cochant l'option ci-dessus.

- L'export du certificat serveur (et de sa clé privée) est une opération critique et sensible : elle peut être sécurisée par un mot de passe que vous pouvez spécifier. Entrez un mot de passe si vous le souhaitez (ne l'oubliez pas, vous en aurez besoin pour l'import !), ou laissez le champ à vide si vous ne souhaitez pas spécifier de mot de passe.

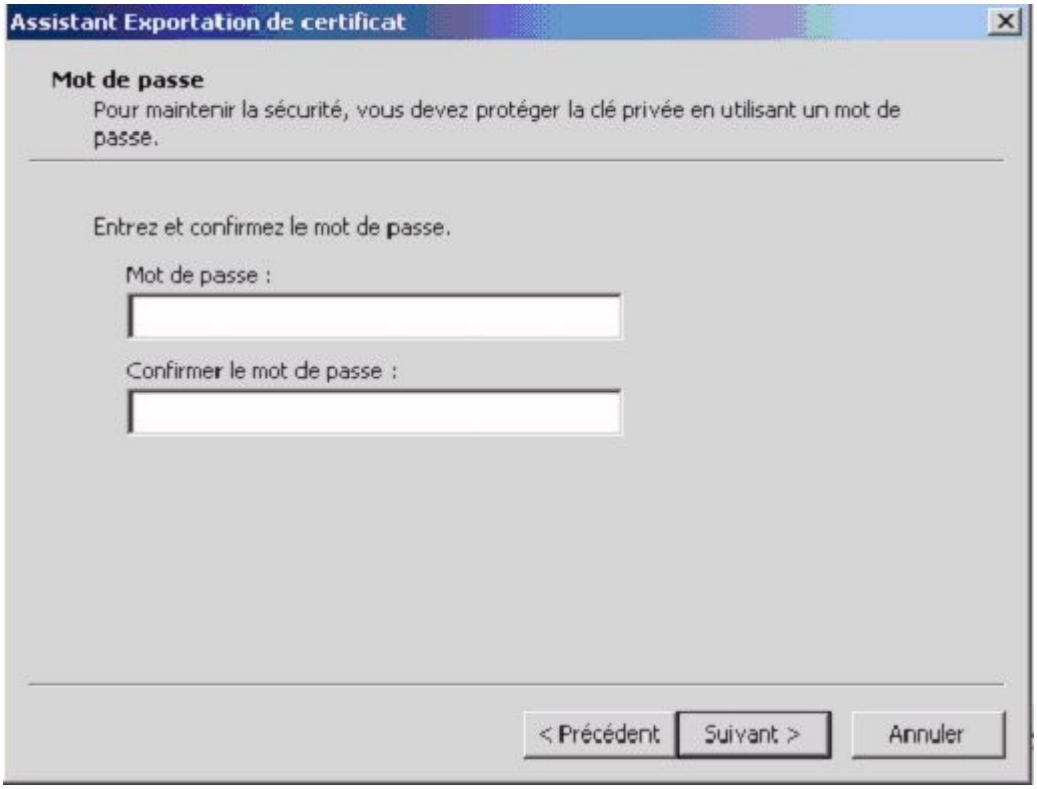


Figure 53 : Saisissez le mot de passe pour protéger la clé privée qui est exportée avec le certificat serveur au format PKCS #12.

- Sauvegardez alors le certificat serveur sous forme d'un fichier export à l'extension .PFX :

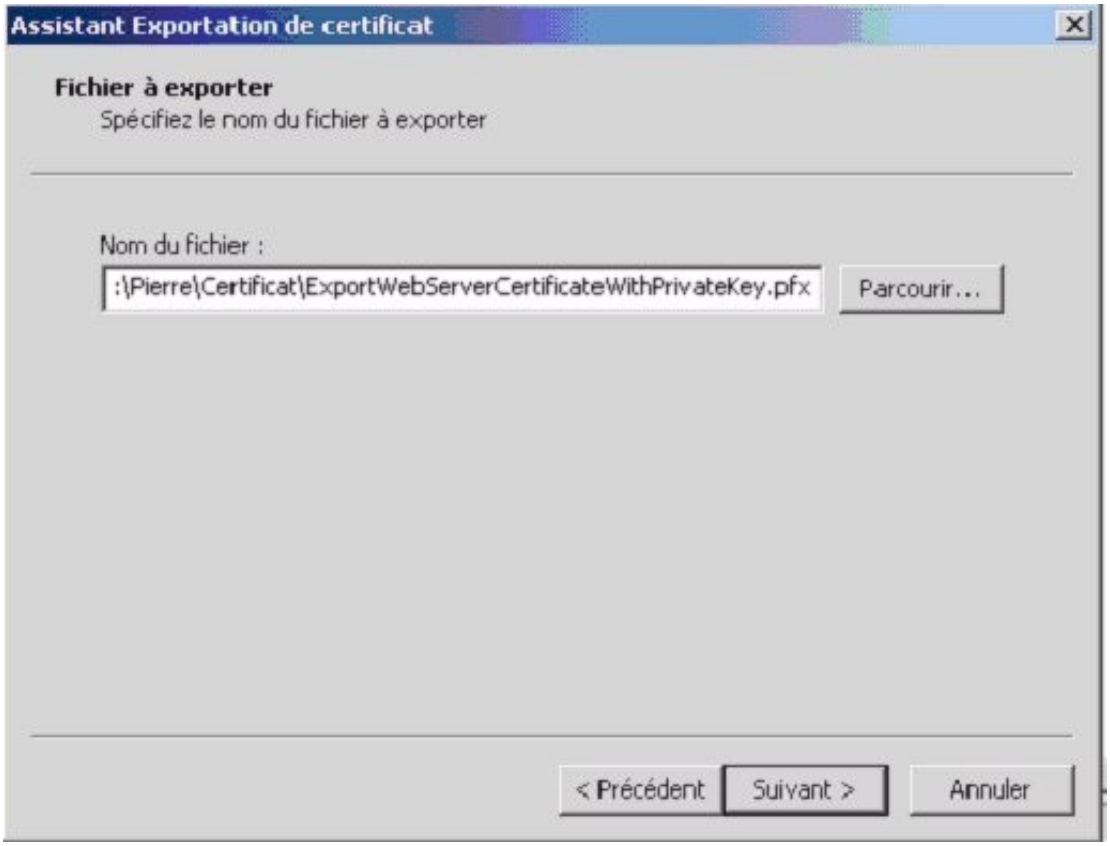


Figure 54 : Spécifiez un nom pour votre fichier export au format PKCS #12.

- Reconstruisez alors votre serveur Windows 2000 (Réinstallation complète ….).

- L'étape suivante consiste à maintenant lancer l'importation du certificat serveur. Cette étape doit être effectuée suivant ces étapes afin que le certificat soit correctement installé et opérationnel :

  - Ouvrez la console MMC des Certificats pour le **compte Ordinateur Local**, **Localement sur le serveur IIS 5.**
  - Puis sélectionnez le **Dossier Personnel**, faites un bouton droit sur le dossier, puis sélectionnez "**Toutes les tâches**"

dans le menu contextuel, puis sélectionnez l'option "**Importer**".

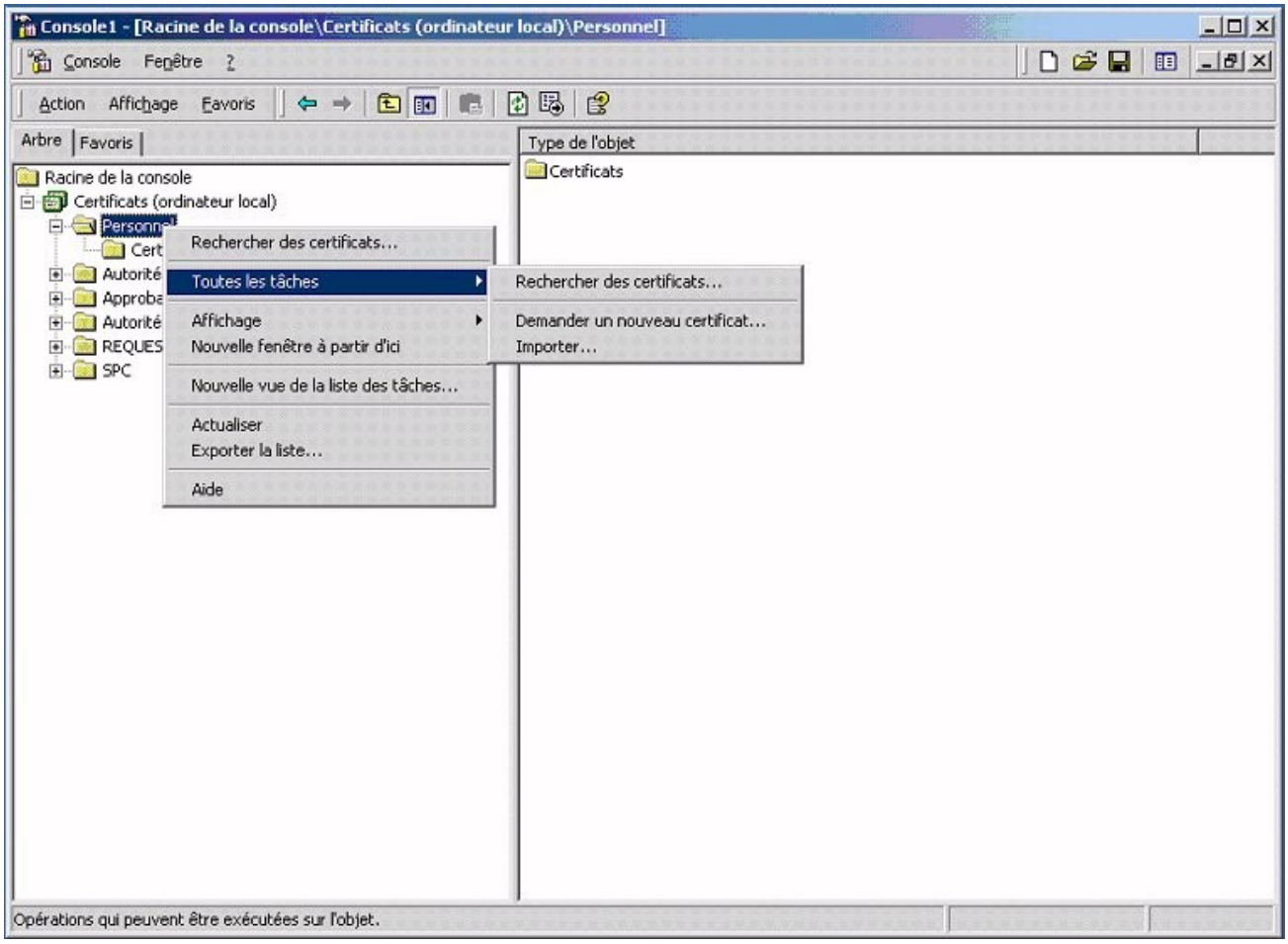


Figure 55 : Importer le fichier export du certificat serveur dans le store personnel du compte de l'ordinateur.

- Sélectionnez le fichier .**PFX** à importer :

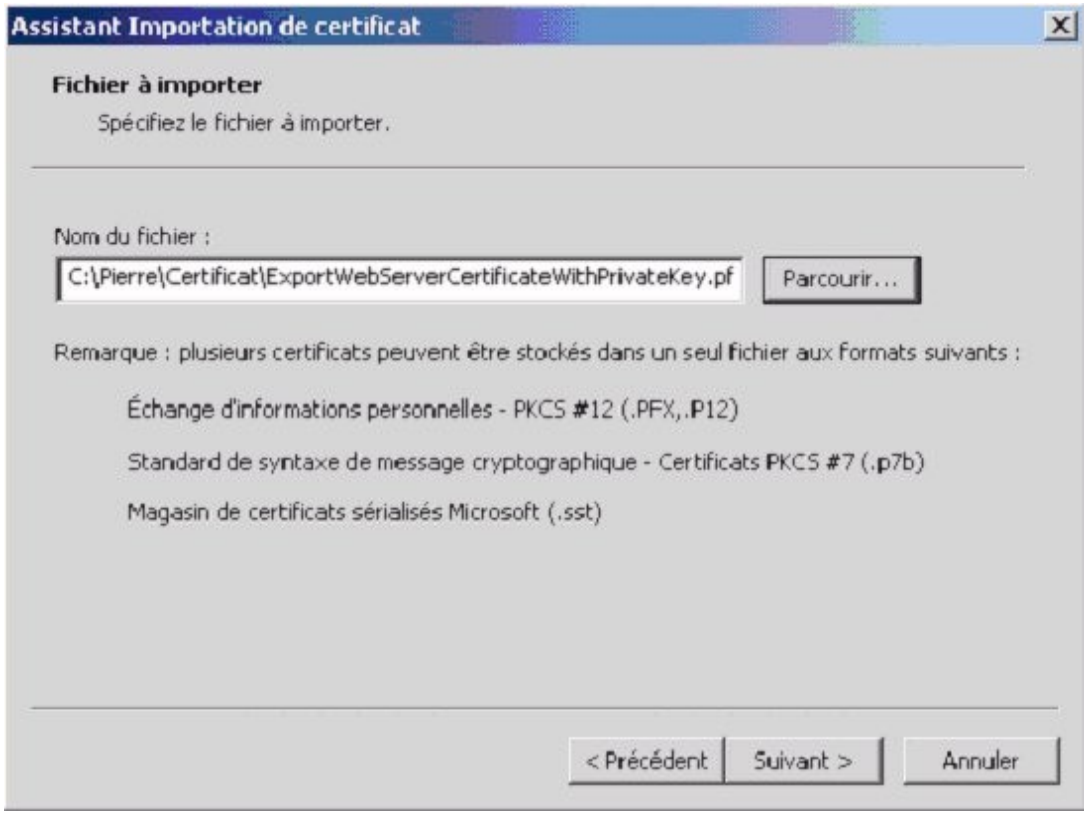


Figure 56 : Sélectionnez le fichier d'importation .PFX.

- Entrez le mot de passe qui protégé votre clé privée, puis cochez l'option "**Marquer la clé privée comme exportable**" : ceci vous permettra, dans une future réinstallation, de continuer à exporter la clé privée.

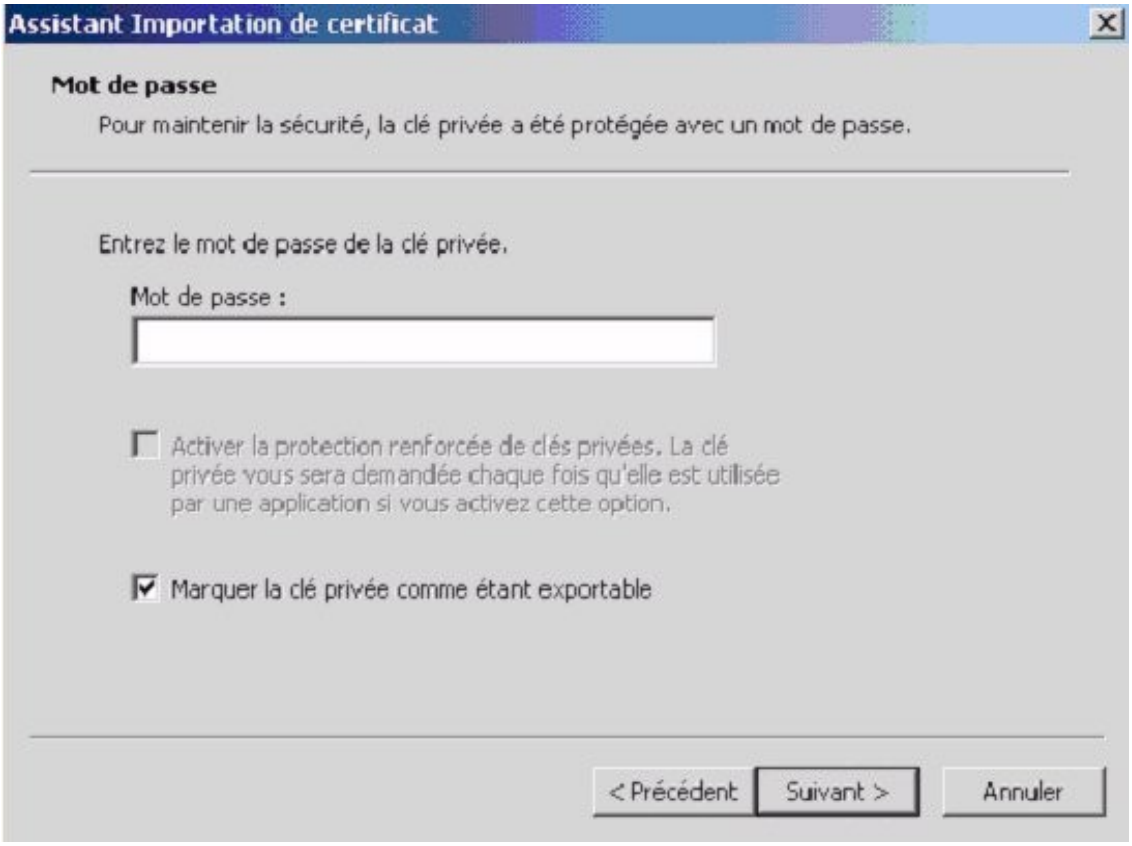


Figure 57 : Entrez le mot de passe pour l'importation (s'il y en a un), puis cochez l'option « marquez la clé privée comme exportable ».

- Sélectionnez ensuite le store où le certificat sera importé : choisissez le store **Personnel** comme montré dans la figure 58.

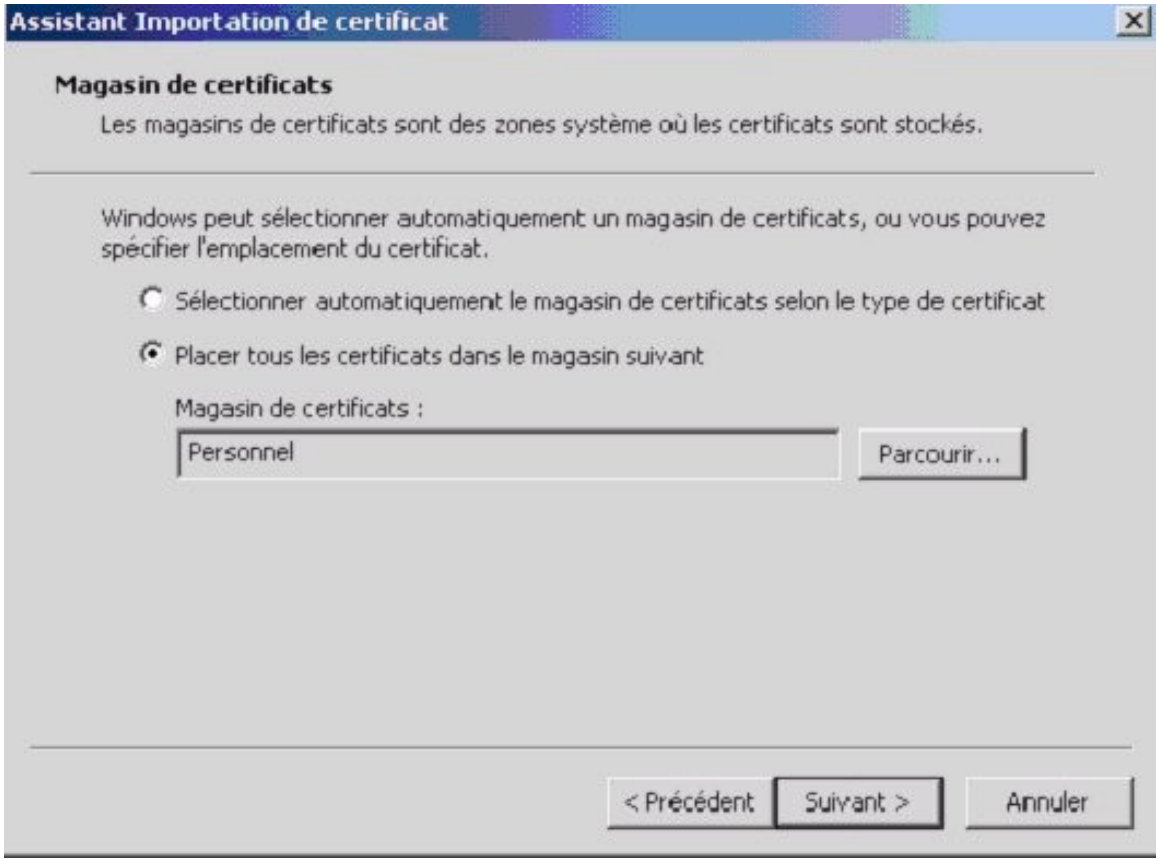


Figure 58 : Sélectionnez le store Personnel pour y copier le certificat serveur à importer.

- Retournez ensuite dans la console MMC Certificats et sélectionnez le dossier "Personnel"/ "Certificats" : vous verrez alors une nouvelle entrée dans la fenêtre droite, qui correspond au nouveau certificat que vous avez copié dans le store Personnel, comme le montre la figure 59 :

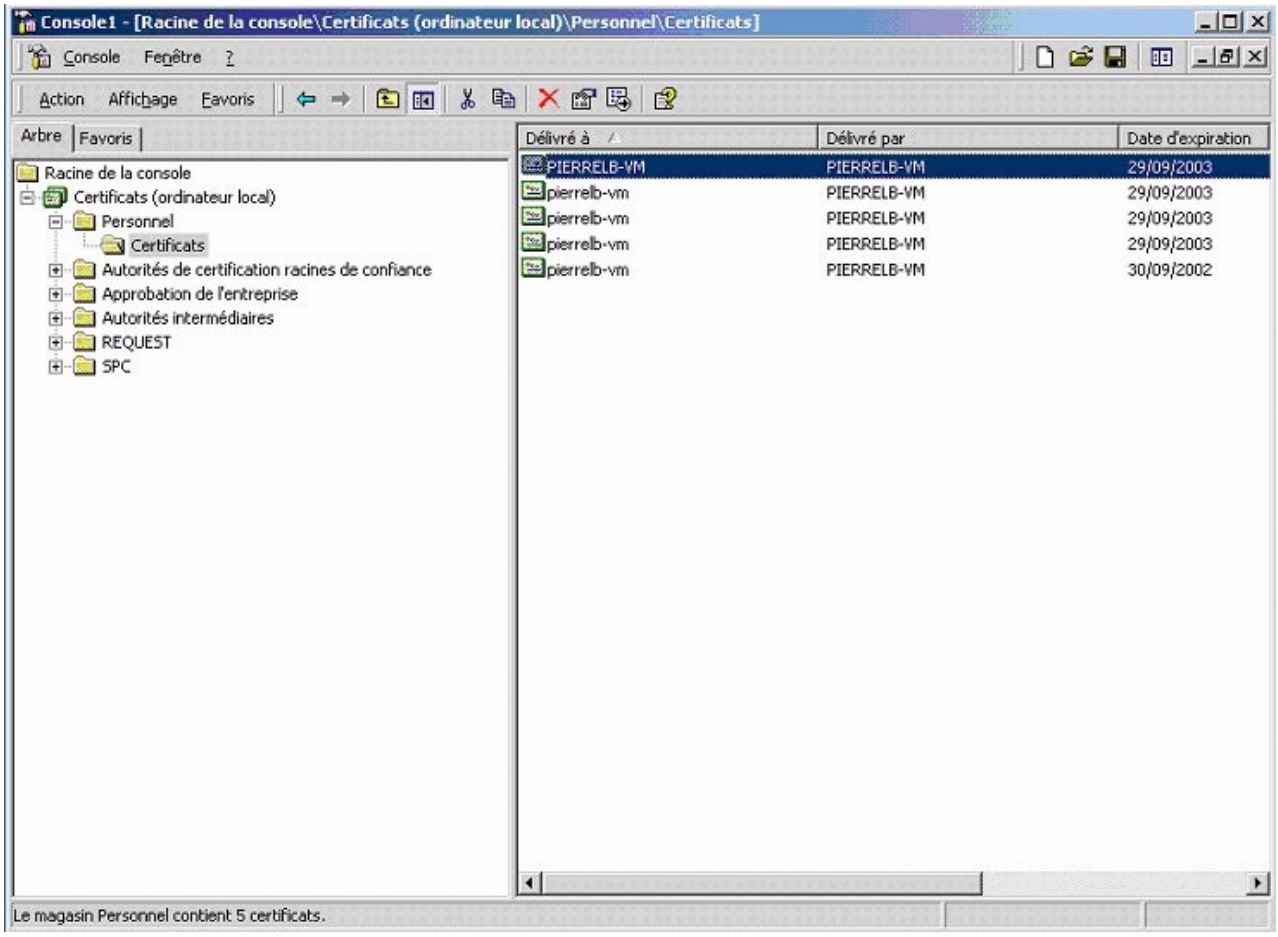


Figure 59 : Votre certificat vient d'être importé dans le store Personnel du compte de l'ordinateur local : il apparaît dans la liste de la fenêtre de droite.

- Dernière étape : il est nécessaire d'attribuer ce certificat serveur à votre site web :
    - Ouvrez la console MMC d'IIS, lancez l'assistant de Certificate Server, puis choisissez l'option "**Attribuer un certificat existant** ".

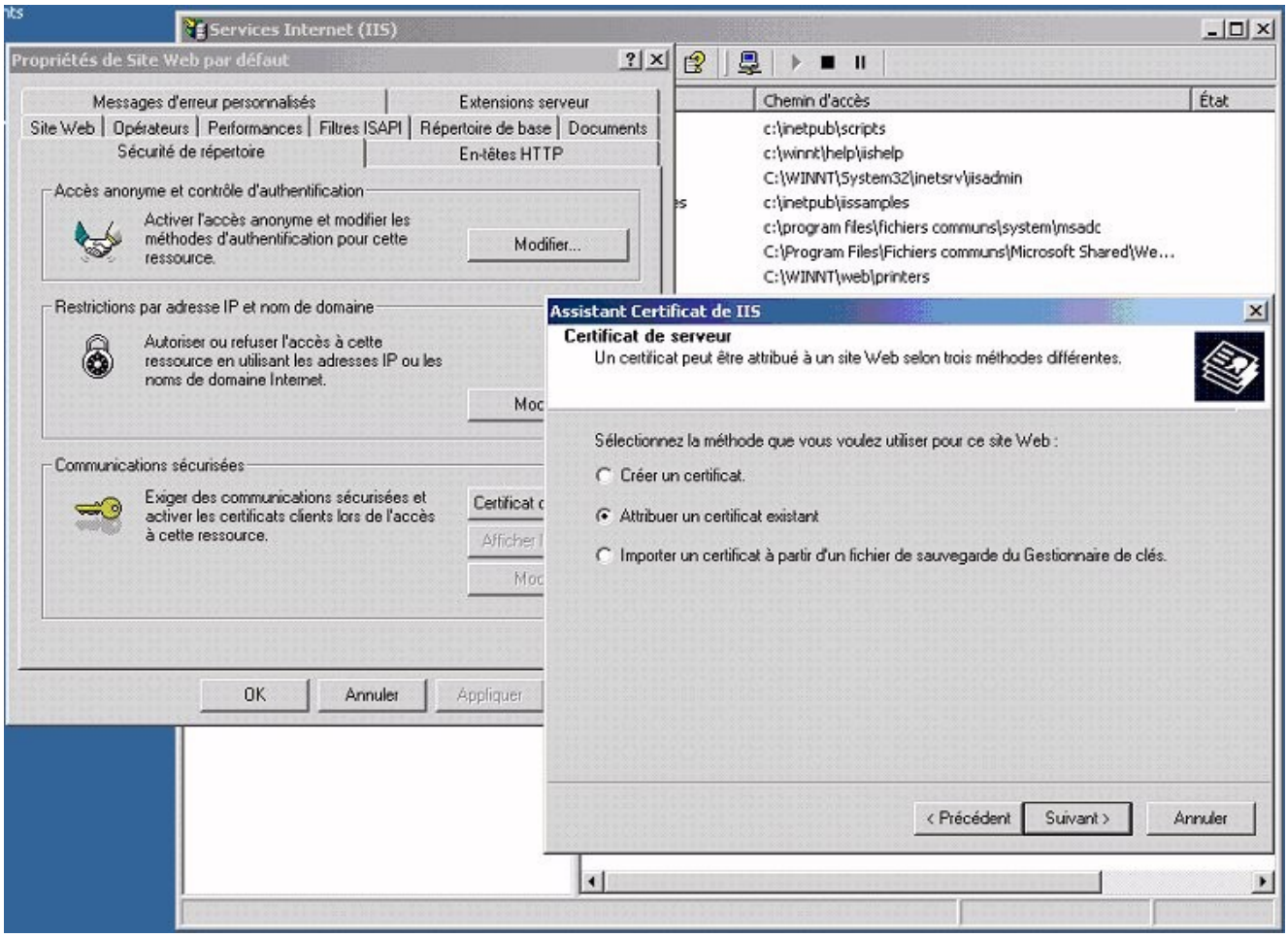


Figure 60 : Attribuez ensuite le certificat, copié dans le store Personnel, à votre site web.

- Le contenu du store Personnel sera alors affiché : sélectionnez dans la liste le certificat que vous venez d'importer précédemment.

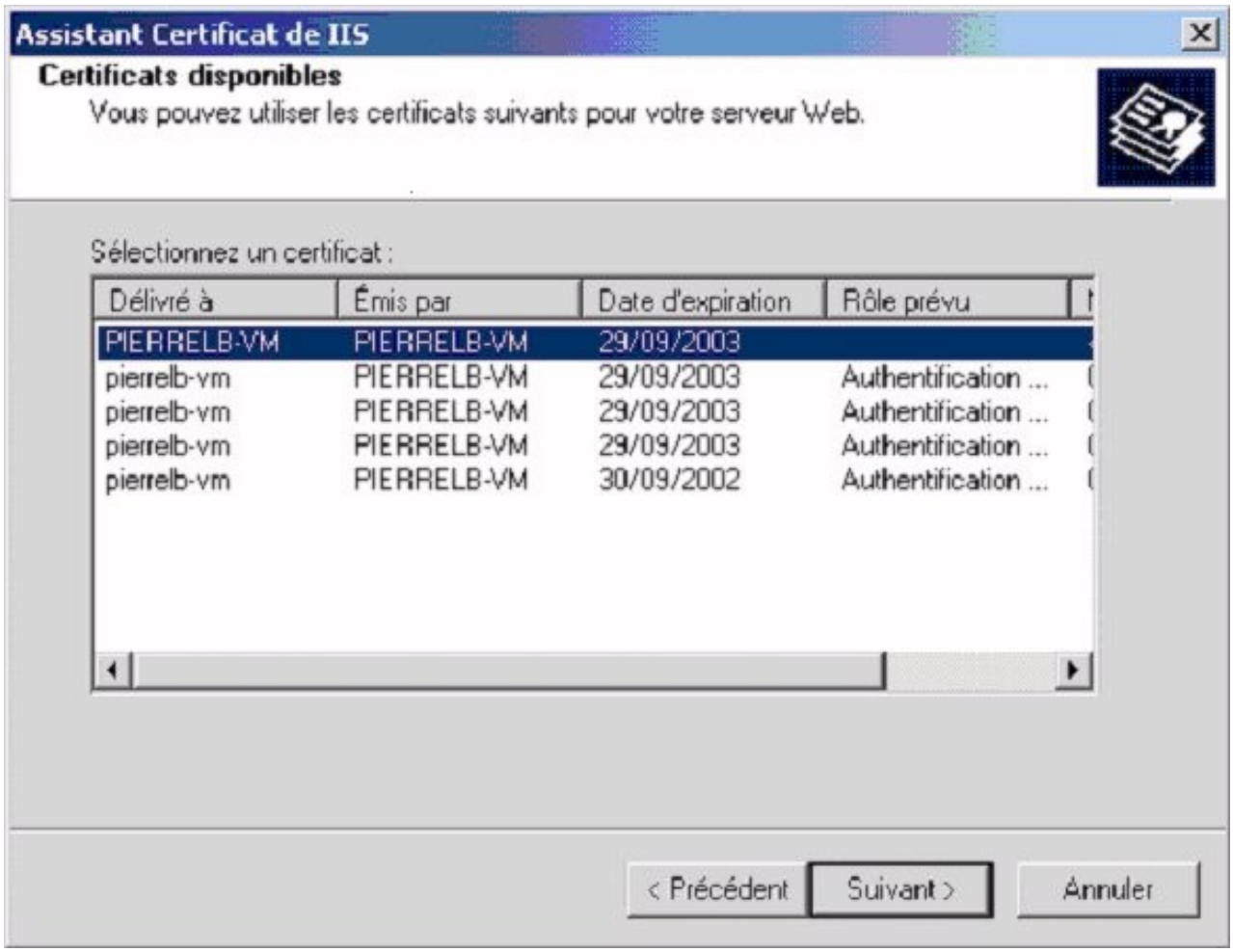


Figure 61 : Sélectionnez le certificat récemment importé dans la liste.

- Votre certificat a été correctement importé et attribué à un site web. L'opération d'export / import est maintenant terminée.

b. Assignation de certificats

i. par adresse IP

Vous ne pouvez assigner plusieurs certificats à une même adresse IP.

ii. par port SSL

Vous ne pouvez assigner plusieurs ports SSL à un site Web.

iii. par nom de domaine

Un seul certificat peut être assigné à un nom de domaine DNS.

iv. sur une ferme de serveurs Web (Web Farm)

Un certificat peut être partagée par plusieurs adresses IP d'un même nom de domaine (Fermes Web)

c. Mapping de certificats dans l'Active Directory

Il est possible de mapper les certificats clients dans un Active Directory de Windows 2000. Pour ce faire, voici les requisites pour mettre en place cette solution, la procédure à suivre ainsi qu'un conseil concernant la mise à jour des révocations de certificats client avec la CRL et AD :

- **Requisites :**
  - Un serveur Windows 2000 avec un Active Directory actif.
  - Un serveur de certification (privé ou déjà connu) Root CA (standalone ou subordonné) en mode « Entreprise ». .Ce mode permet d'utiliser l'Active Directory du serveur Windows 2000.
  - Un serveur Web sécurisé avec un certificat serveur unique, signé par l'organisme de certification Root CA ci-dessus. Ce certificat est installé sur le serveur Web à sécuriser.

- A noter que l'organisme Root CA ayant accordé ce certificat doit être connu dans la liste des organismes Root CA de confiance locale au serveur Web.

- Un ou plusieurs certificats client, signé(s) par l'organisme de certification Root CA ci-dessus. Ces certificats client sont installés sur les postes clients.

    - A noter que l'organisme Root CA ayant accordé ce certificat doit être connu dans la liste des organismes Root CA de confiance locale au poste client.

Procédure de mise en place d'un mapping de certificat dans Active Directory de Windows 2000 :

- Désactiver toutes les méthodes d'authentification du serveur IIS5 sécurisé (Anonyme, NTLM …) afin d'être sûr d'effectuer une authentification grâce à l'Active Directory.

- Suivre l'article technique Q272175 qui décrit complètement la procédure pour mettre en place le mapping de certificats dans l'Active Directory de Windows 2000.

    - Cette procédure est à suivre uniquement quand les requisites ci-dessus ont été correctement effectués.

Additif : Comment faire prendre en compte par Active Directory la révocation manuelle d'un certificat client ?

- Sur le serveur Root CA :
    - Sélectionner Revoked Certificates' - bouton droit - propriétés - Modifier l'intervalle de publication : 1h (au lieu de 7 jours).
    - Sélectionner 'Revoked Certificates' - All Tasks - Publish : ceci a pour effet de forcer la mise à jour, sur le Root CA, la liste des certificats révoqués.
    - Faire un IISRESET pour faire prendre en compte la révocation des certificats, par précaution.

- Sur le poste client :
    - Connection via IE avec un utilisateur : on obtient maintenant un message d'erreur - Impossible de se connecter avec son certificat client.

5) Forum Aux Questions

a. Base TECHNET

i. Q218445 : Comment configurer un serveur de certificat pour utiliser SSL sur IIS4 ?

- http://support.microsoft.com/support/kb/articles/Q218/4/45.ASP

ii. Q299525 : Comment paramétrer SSL en utilisant IIS5 et certificate Server 2.0 ?

- http://support.microsoft.com/support/kb/articles/Q299/5/25.ASP

iii. Q290625 : Comment configurer SSL sur Windows 2000 IIS5 ?

- http://support.microsoft.com/support/kb/articles/Q290/6/25.ASP

iv. Q232137 : Comment importer un certificat serveur à utiliser dans IIS5 ?

- http://support.microsoft.com/support/kb/articles/Q232/1/37.ASP

v. Q272175 : Comment configurer le mapping de certificats dans Active Directory ?

- http://support.microsoft.com/support/kb/articles/Q272/1/75.ASP

b. Articles techniques TECHNET annexes :

i. Q295329 : Comment renouveler un certificat SSL Verisign avec une nouvelle clé dans IIS5 ?

- http://support.microsoft.com/support/kb/articles/Q295/3/29.ASP

ii. Q228836 : Installer un nouveau certificat pour utiliser SSL/TLS sur IIS5

- http://support.microsoft.com/support/kb/articles/Q228/8/36.ASP

iii. Q247257 : Etapes pour signer un fichier .CAB.

- http://support.microsoft.com/support/kb/articles/Q247/2/57.ASP

iv. Q298559 : Comment mettre en place le Load-balancing sur des sites IIS sécurisés avec SSL

- http://support.microsoft.com/support/kb/articles/Q298/5/59.ASP

v. Q245030 : Comment restreindre le nombre des algorithmes SSL ?

http://support.microsoft.com/support/kb/articles/Q245/0/30.ASP

vi. Q250867 : Impossible d'installer le Service Pack 6a avec une version High-encryption d'Internet Explorer.

- http://support.microsoft.com/support/kb/articles/Q250/8/67.ASP