Installation d'un certificat de serveur

Rédacteur : Eric Drezet
Administrateur réseau
CNRS-CRHEA – 06/2004

But du papier : Installer un certificat de serveur en vue de sécuriser l'accès au Web Mail avec SSL

Préalable : Installer une autorité locale de certification (voir le papier « Installation autorité certification »)

Liens :

- Procédures pour publier des sites Web SSL en utilisant la publication sur serveur
- Comment utiliser des certificats avec les serveurs virtuels dans Exchange Server 2003

Conditions : le présent papier détaille la procédure dans le cas d'un serveur dont le système d'exploitation est Windows 2000 server.

L'accès à un serveur de courrier électronique Exchange via un navigateur est possible grâce à l'implémentation d'un serveur virtuel dont le protocole de base est http. Pour gérer ce serveur virtuel, il faut lancer IIS (version 5 pour une machine Windows 2000 server).

Il faut donc commencer par lancer le gestionnaire des services Internet (IIS) avec les droits appropriés. Sélectionnez ensuite le site web sur lequel vous souhaitez appliquer le certificat (Site web par défaut dans notre exemple) et ensuite implémenter l'accès SSL. Effectuez un click droit et sélectionnez « Propriétés » dans le menu contextuel (cf. figure 1).

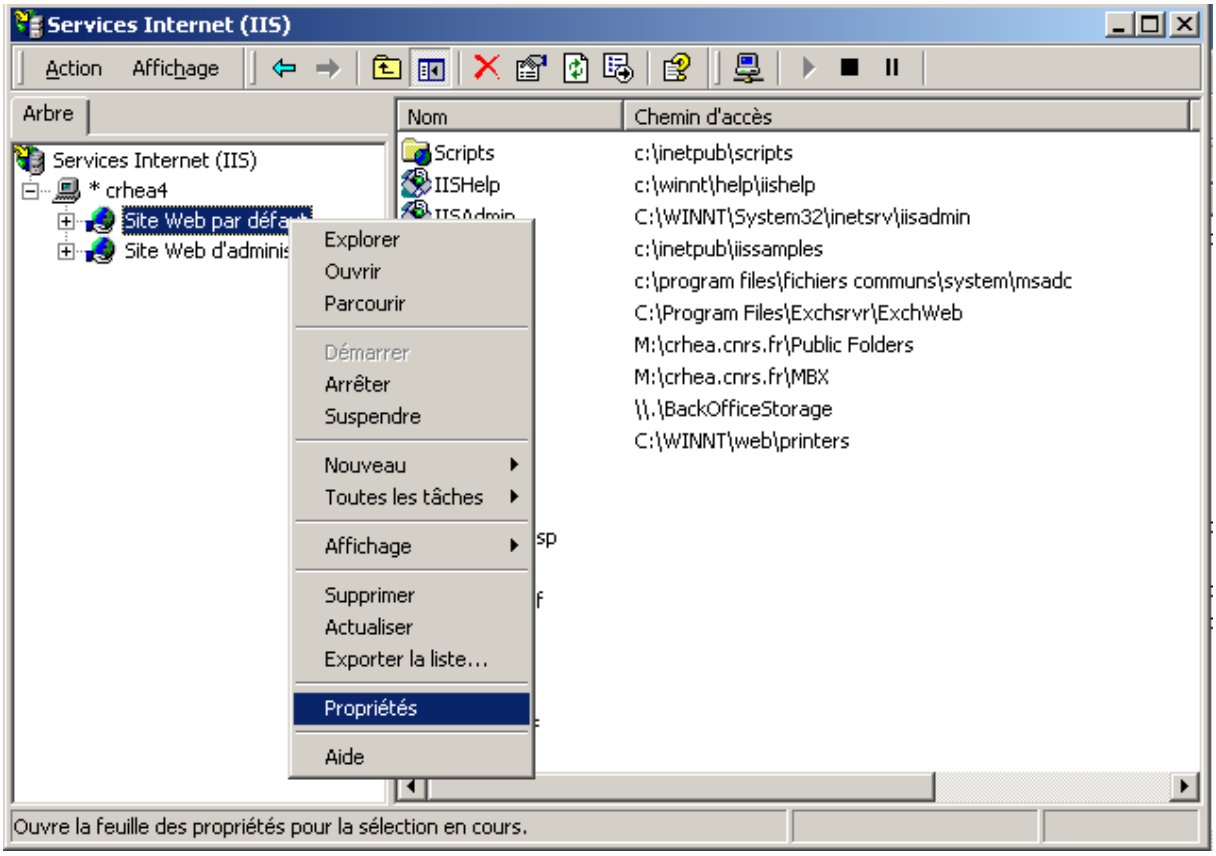

Figure 1 : affichage des propriétés du site web concerné

Dans la fenêtre des propriétés, sélectionnez l'onglet « Sécurité de répertoire ». Cliquez ensuite sur le bouton « Certificat de serveur… » situé dans la zone « Communications sécurisées » en bas de le fenêtre (cf. figure 2).

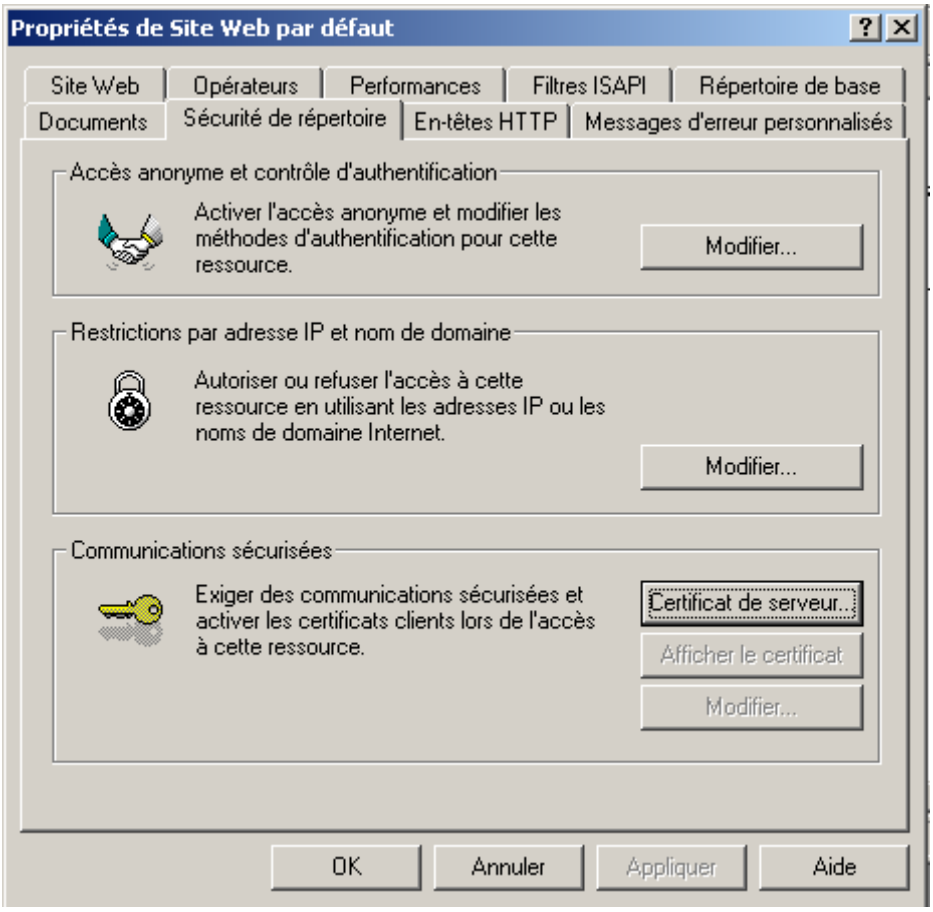

Figure 2 : installation du certificat de serveur

L'assistant « Certificat de serveur » démarre et va vous guider dans la procédure de création du certificat. Cliquez sur le bouton « Suivant > » pour démarrer la procédure (cf. figure 3).

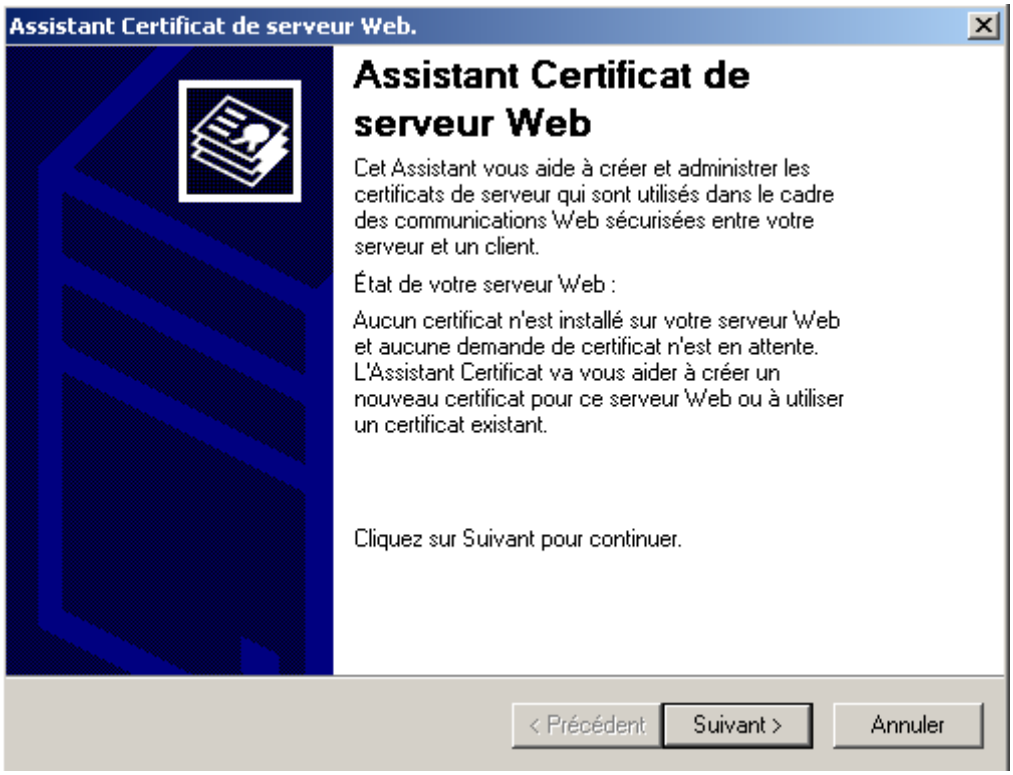

Figure 3 : début de la procédure à l'aide de l'assistant de certificat

Dans le premier écran, sélectionnez « Créer un certificat » si vous n'avez pas de certificat de serveur en votre possession. Dans le cas contraire, vous pouvez attribuer un certificat existant ou importer un certificat à partir d'une sauvegarde. Dans notre exemple, nous allons étudier le premier cas. Conservez donc la sélection par défaut et cliquez sur le bouton « Suivant > » (cf. figure 4).

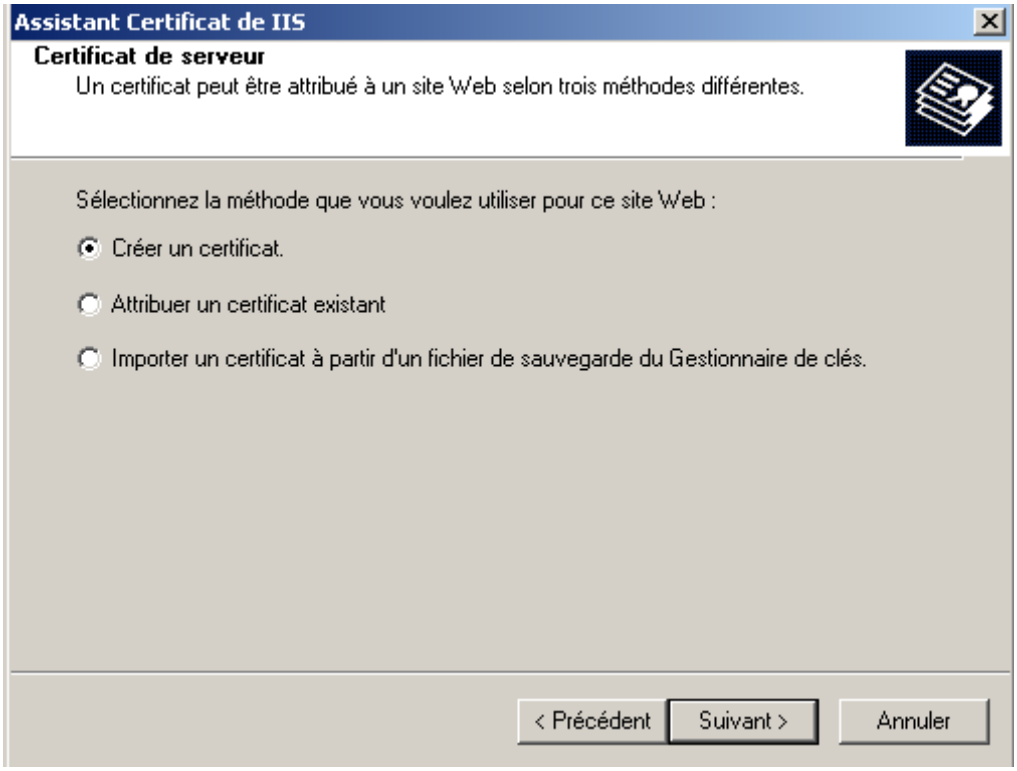

Figure 4 : création d'un certificat

Sélectionnez ensuite l'option « Envoyer immédiatement la demande à une Autorité de certification en ligne ». Cliquez sur le bouton « Suivant > » pour démarrer la procédure (cf. figure 5).

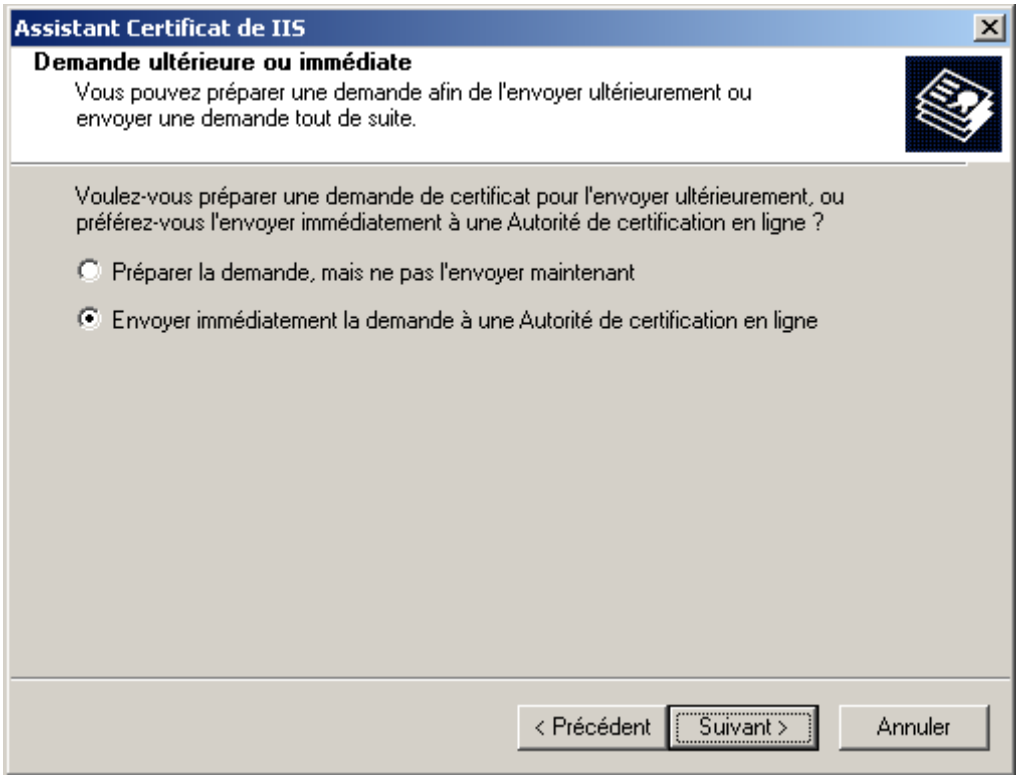

Figure 5 : envoi de la demande de certificat

Saisissez ensuite un nom et une longueur en bits pour votre certificat. Cliquez sur le bouton « Suivant > » (cf. figure 6).

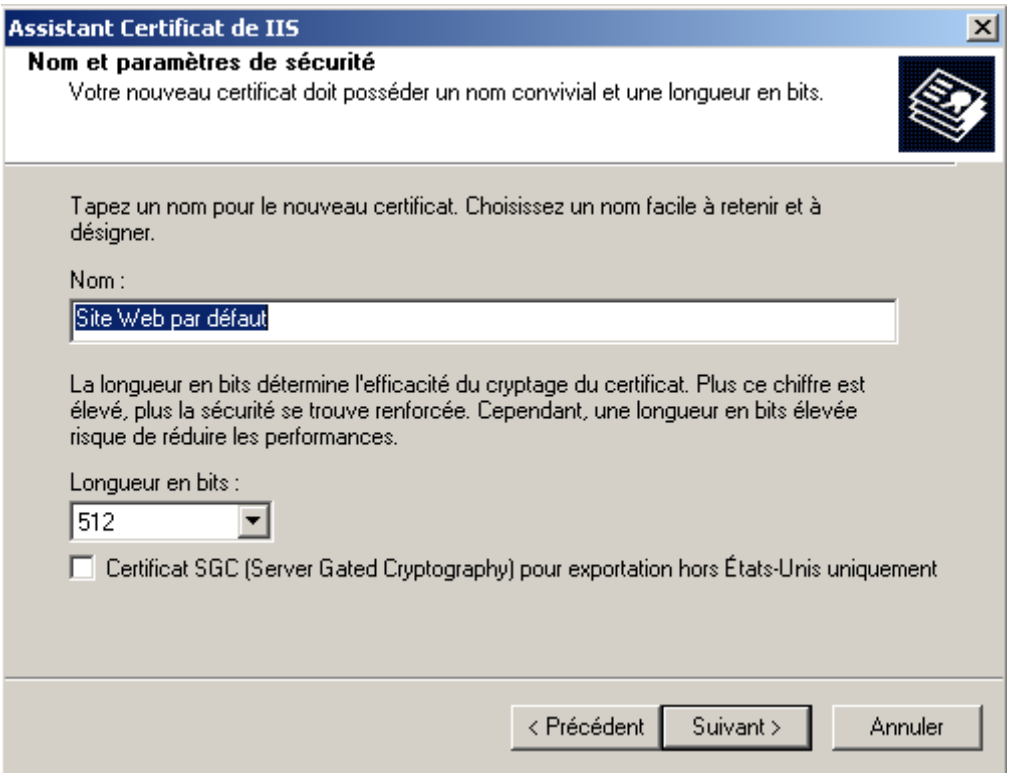

Figure 6 : nom et longueur du certificat

Saisissez ensuite les informations concernant l'organisation (nom de l'entreprise et du département. Cliquez sur le bouton « Suivant > » (cf. figure 7).

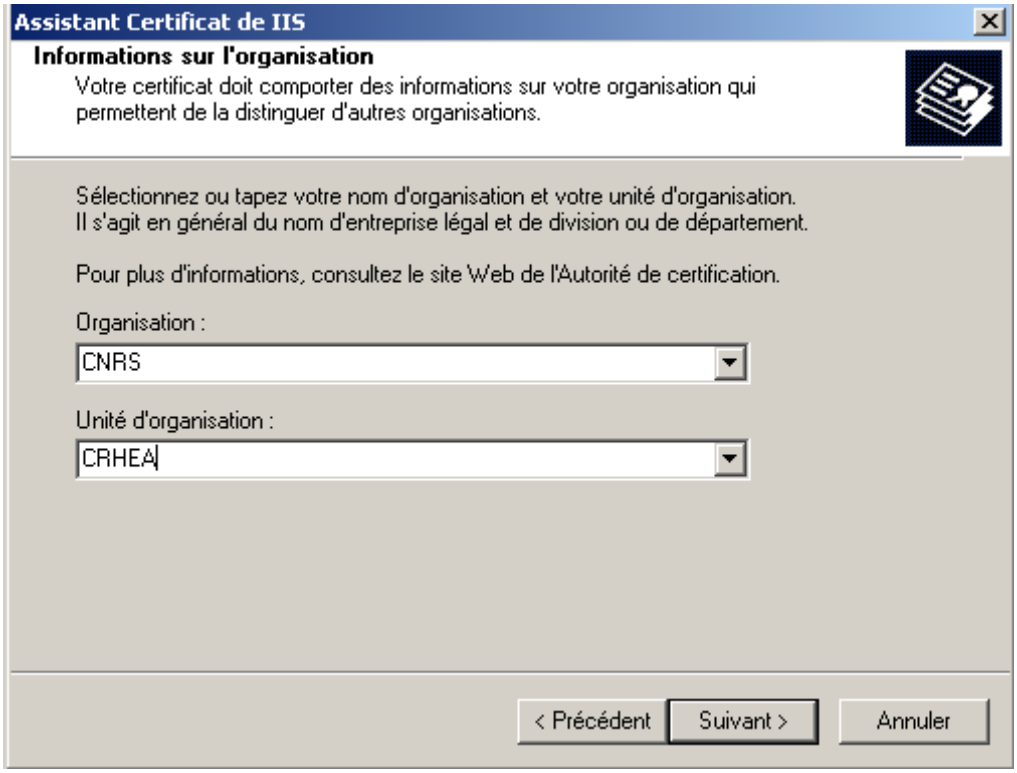

Figure 7 : nom et unité d'organisation

Il faut ensuite spécifier le nom de l'ordinateur qui recevra le certificat de serveur. Si l'ordinateur est situé dans le réseau local, le nom NetBios est suffisant. S'il est distant, il faut entrer le nom complet (FQDN) de l'ordinateur (cf. figure 8). Cliquez sur le bouton « Suivant > ».

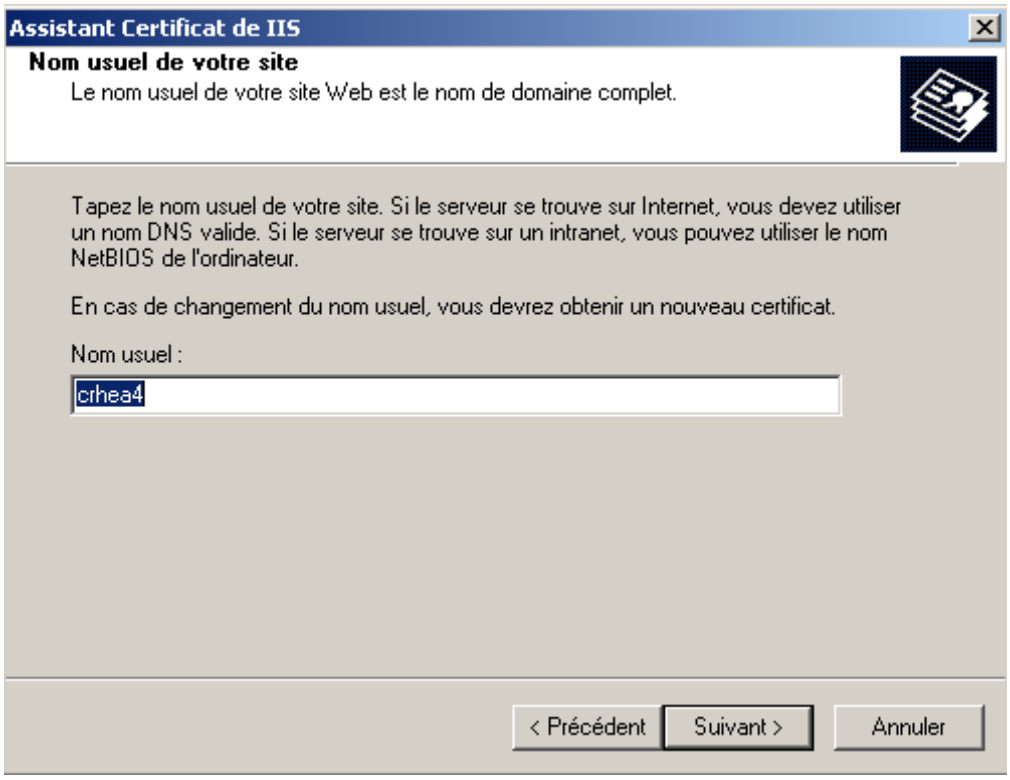

Figure 8 : nom de l'ordinateur pour lequel un certificat de serveur est demandé

Dans la fenêtre suivante (cf. figure 9), il vous est demandé de fournir des renseignements d'ordre géographique. Cliquez sur le bouton « Suivant > ».

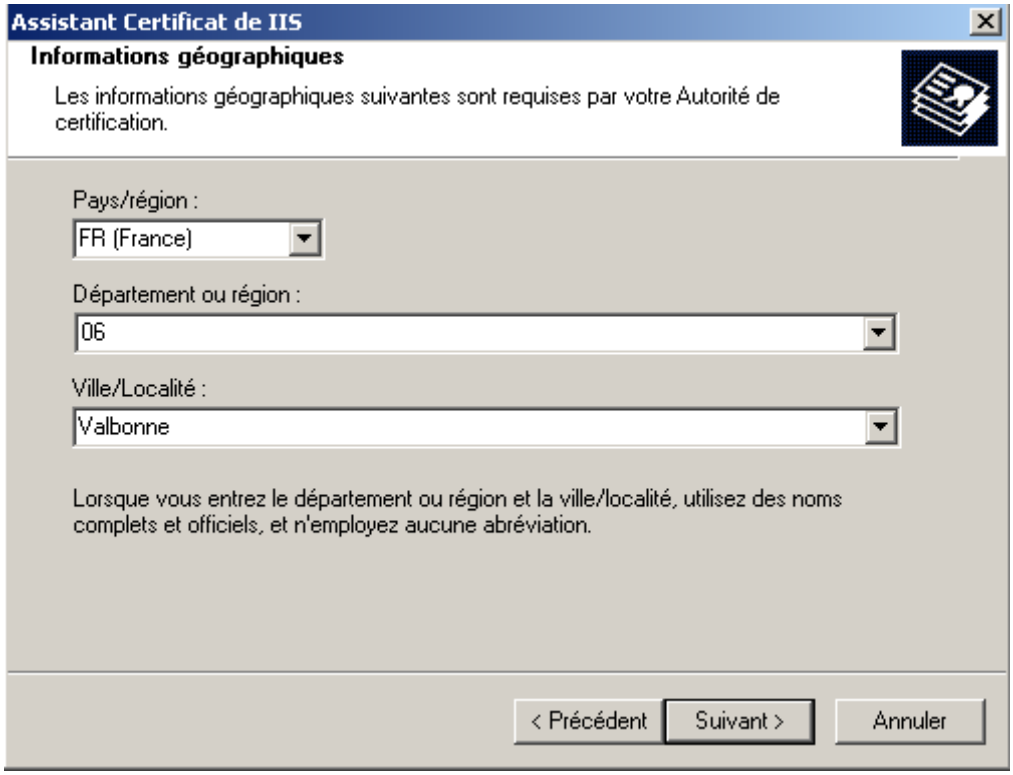

Figure 9 : renseignements géographiques

Il faut ensuite indiquer le nom de l'ordinateur détenteur de l'autorité locale de certification. La liste déroulante doit afficher le(s) nom(s) de (des) autorité(s) de certification créée(s) dans votre organisation (cf. figure 10). Cliquez sur le bouton « Suivant > ».

> *Note : au même titre que tout les autre services proposés dans le cadre d'un domaine, l'autorité de certification est référencée dans l'annuaire Active Directory à sa création. C'est pourquoi on la retrouve proposée dans cette liste déroulante de l'assistant de certificat IIS.*

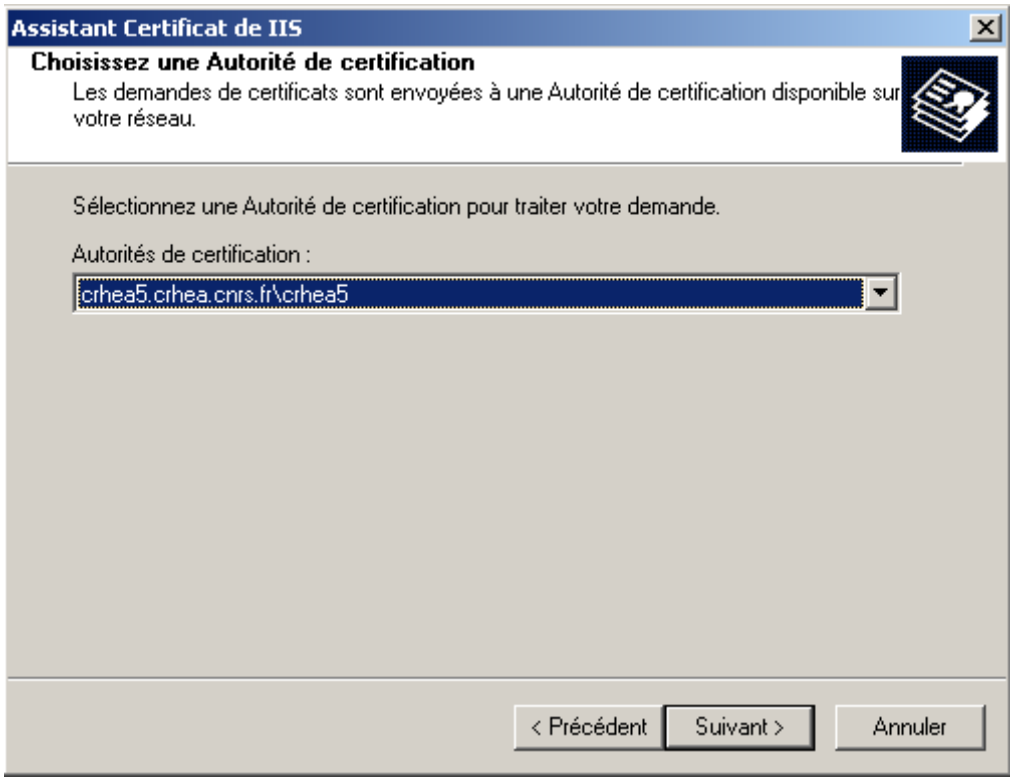

Figure 10 : choix de l'autorité de certification

La fenêtre suivante récapitule les choix effectués depuis le lancement de l'assistant de certificat IIS. A ce stade, il est encore possible de revenir en arrière pour effectuer des modifications à n'importe quelle étape du processus. Si les choix sont corrects, cliquez sur le bouton « Suivant > » (cf. figure 11).

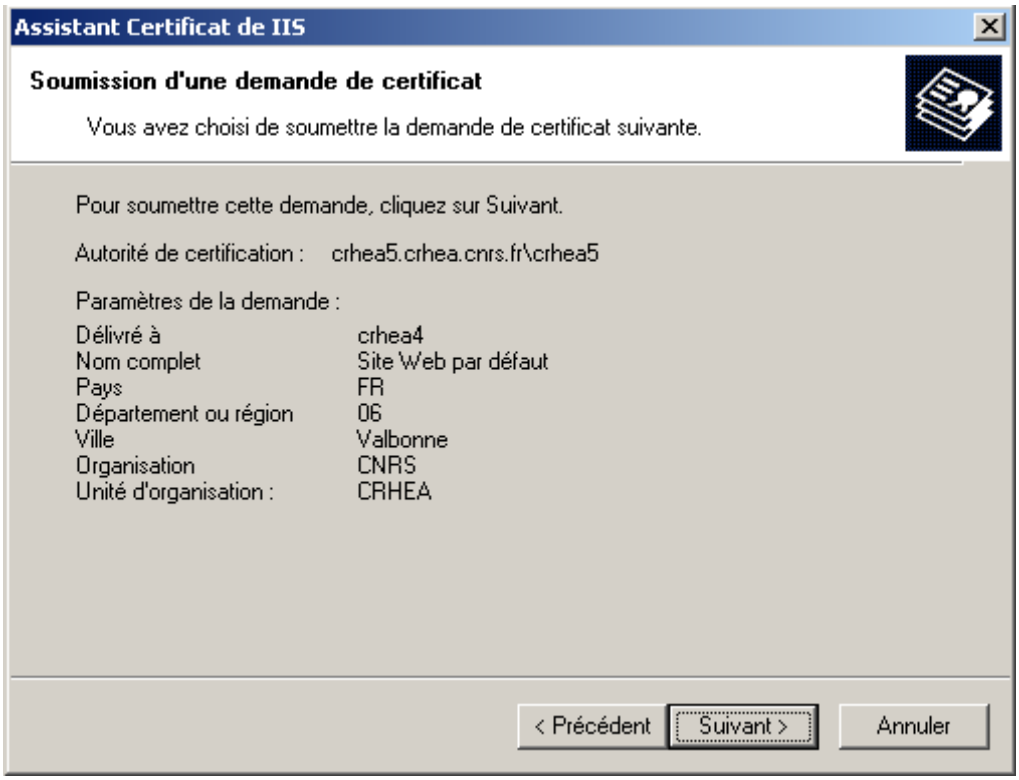

Figure 11 : récapitulatif des choix avant soumission

Cliquez ensuite sur le bouton « Terminer » pour soumettre la demande de certificat à l'autorité de certification et installer automatiquement le certificat sur le serveur désigné (cf. figure 12).

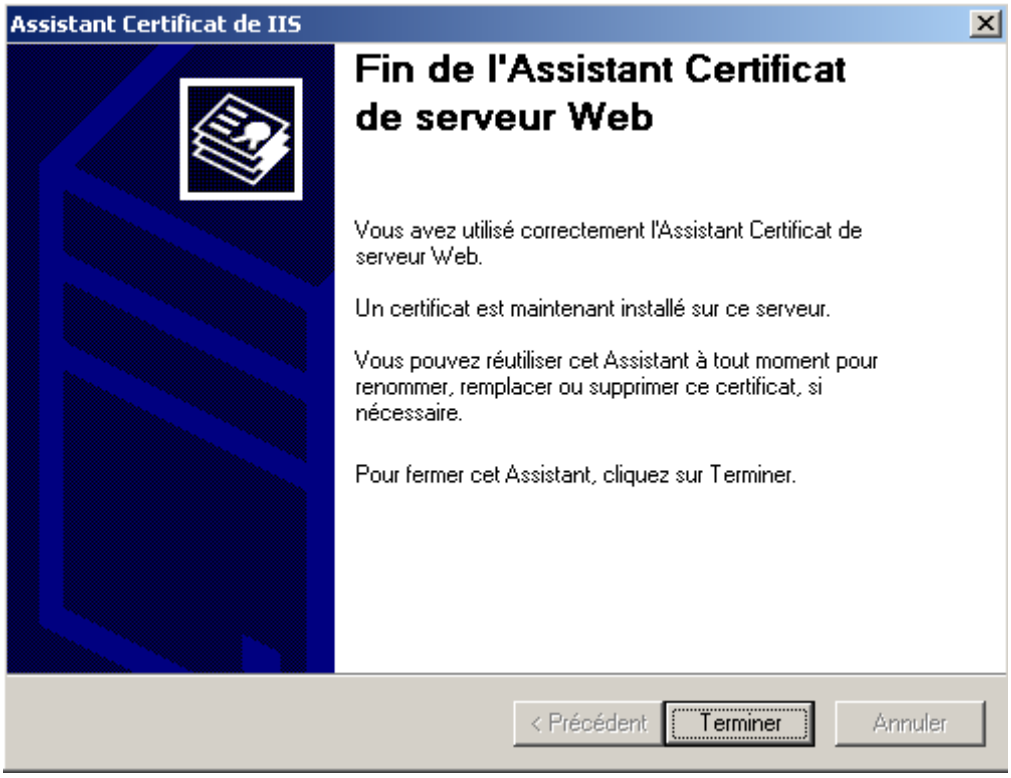

Figure 12 : fin de la demande de certificat de serveur

Pour visualiser le certificat de serveur installé, lancez le gestionnaire des services Internet (IIS) avec les droits appropriés. Sélectionnez ensuite le site web sur lequel le certificat a été appliqué (Site web par défaut dans notre exemple). Effectuez un click droit et sélectionnez « Propriétés » dans le menu contextuel (cf. figure 1). Dans la fenêtre des propriétés, sélectionnez l'onglet « Sécurité de répertoire ». Cliquez ensuite sur le bouton « Afficher le certificat… » situé dans la zone « Communications sécurisées » en bas de le fenêtre. Les informations relatives au certificat de serveur installé sont alors affichées (cf. figure 13). L'onglet « Général » décrit le certificat et sa durée de validité. L'onglet « Détails » liste toutes les caractéristiques du certificat et enfin l'onglet « Chemin d'accès de certification » donne l'arborescence de l'autorité de certification aux certificats délivrés par elle.

> *Note : par défaut, la durée de validité du certificat de l'autorité de certification est de 5 ans, alors que celle pour un certificat de serveur est fixée à 2 ans. Ces valeurs par défaut peuvent être modifiées au niveau de l'autorité de certification.*

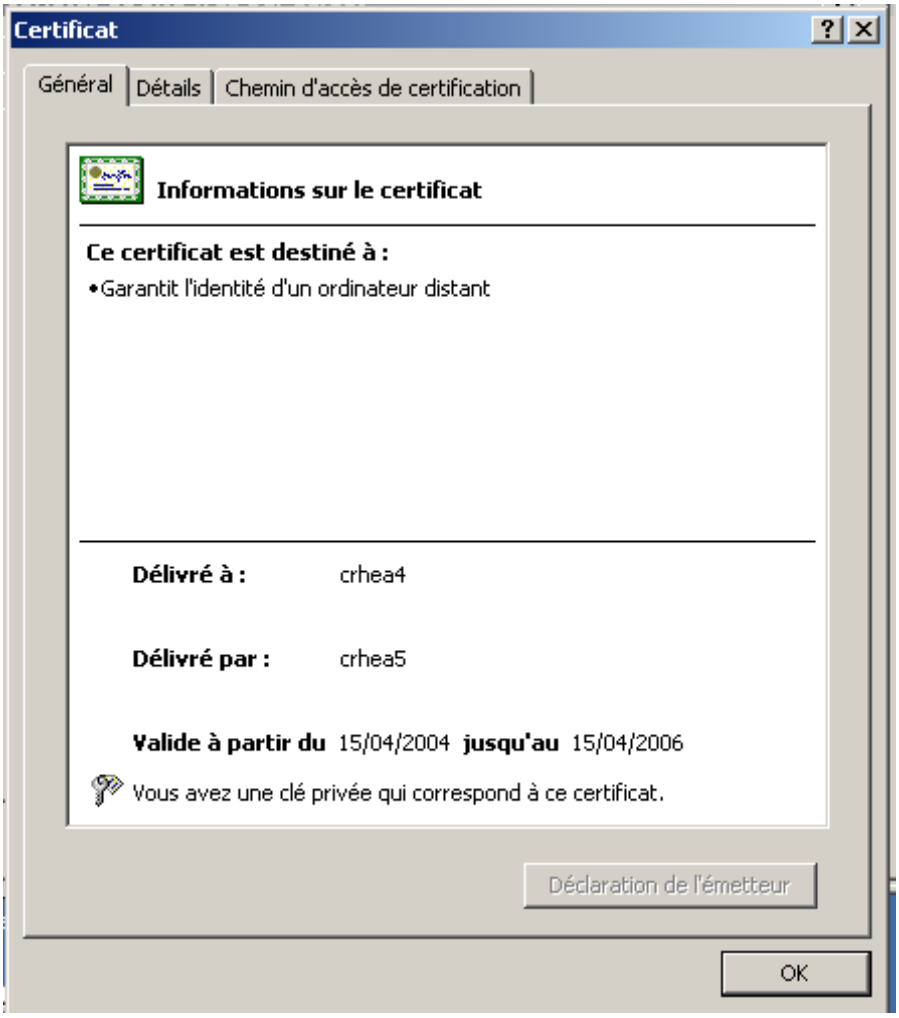

Figure 13 : Détails du certificat de serveur installé

La dernière étape consiste à imposer l'emploi de SSL (Secure Socket Layer) pour la protection de certaines pages, du site web entier. Dans notre exemple de sécurisation de l'accès au WebMail d'Exchange via OWA (Outlook Web Access), nous allons imposer l'emploi de SSL au niveau de l'ensemble du serveur virtuel http. Pour valider l'emploi de SSL au niveau de ce serveur virtuel, lancez le gestionnaire des services Internet (IIS) avec les droits appropriés. Sélectionnez ensuite le site web sur lequel le certificat a été appliqué (Site web par défaut dans notre exemple). Effectuez un click droit et sélectionnez « Propriétés » dans le menu contextuel (cf. figure 1). Dans la fenêtre des propriétés, sélectionnez l'onglet « Sécurité de répertoire ». Cliquez ensuite sur le bouton « Modifier » (cf. figure 14).

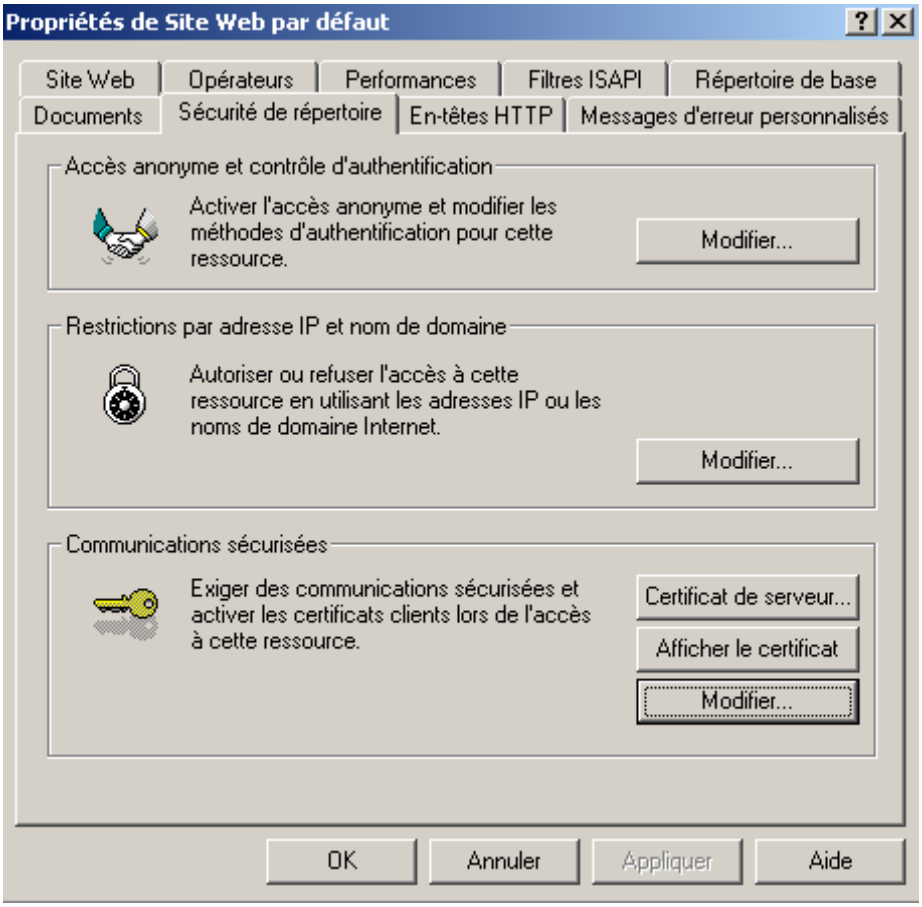

Figure 14 : Modifier la sécurisation des communications

Dans la fenêtre suivante, cochez la case « Exiger un canal sécurisé (SSL) » (cf. figure 15). A partir de cet instant, l'accès au WebMail via OWA se fera via une adresse http sécurisée. Exemple d'accès sécurisé via OWA :

https ://server_exchg.corp.net/exchange/

Note : SSL en deux mots créée un canal chiffré entre le client et le serveur le temps que dure la communication. Sans l'emploi de SSL, toute la communication est « en clair » sur l'Internet ce qui veut dire que, outre le contenu des messages, le login de l'utilisateur peut être intercepté (nom d'utilisateur et mot de passe).

D'autre options peuvent être activées à ce stade pour renforcer l'autorisation d'accès au WebMail en sélectionnant l'emploi de certificats clients par exemple.

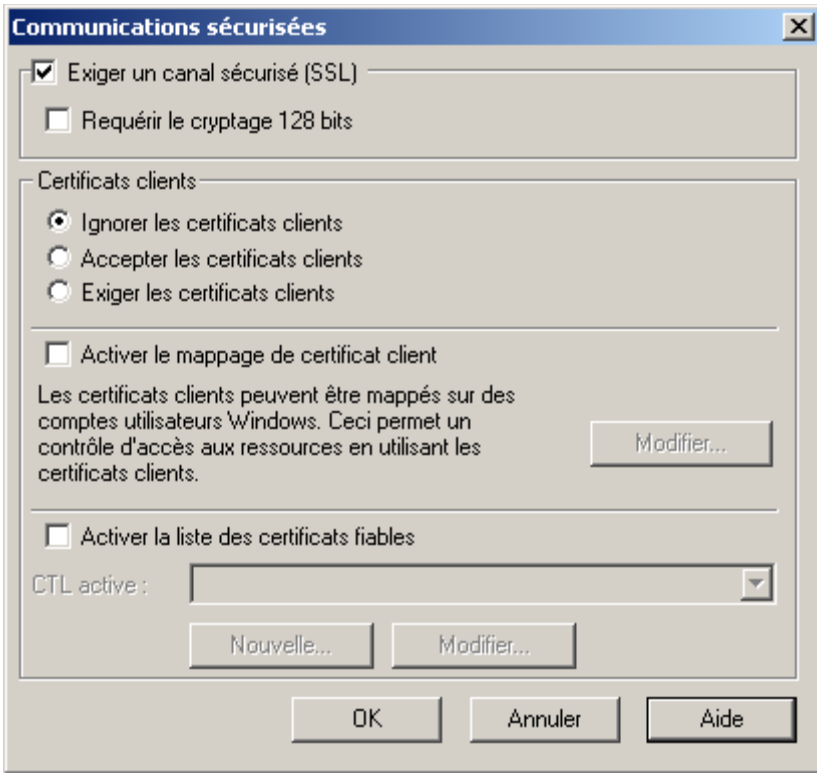

Figure 15 : Activation de SSL pour l'accès OWA