1. Mise en œuvre du Cegid Web Access Server en https

Principe d'usage

La mise en œuvre du mode https sur un serveur Web Access implique :

- De disposer d'un certificat pour le nom d'hôte configuré sur le serveur
- Le mode https utilise le port standardisé TCP 443 (non réglable)
- Si usage de ferme de serveurs Web Access, chaque système doit disposer de ses éléments propres (adresse IP, certificat) dans le sens où chaque serveur est pleinement indépendant en terme d'usage vu des postes clients (la notion de ferme est un élément connu uniquement des serveurs Web Access entre eux)
- Dès lors que le serveur est en mode https, la modification de son nom d'hôte n'est plus possible (désactivation du mode https si besoin de modifier ce nom, **attention il faudra commander un nouveau certificat**)
- Une option permet de rediriger le flux http vers le flux https automatiquement pour faciliter l'installation ou la connexion de la partie cliente
- L'encryption https peut aller jusqu'à 256 bits

Il est important de noter que le serveur Web Access répond avec son nom d'hôte dès lors qu'il communique, et dans ce cadre (surtout sur Internet), la résolution de nom doit être opérationnelle vis-à-vis du client Web Access (il est conseillé d'avoir une résolution de nom DNS pleinement opérationnelle).

Fichiers de certificats

Le serveur Web Access s'appuie sur une gestion locale des fichiers nécessaires pour les certificats. 2 fichiers sont utiles, stockés à l'emplacement des exécutables du service, ils reprennent le nom d'hôte suivi d'une extension :

- Nom_du_cwas.cer : fichier de certificat, au format PEM
- Nom_du_cwas.pvk : fichier de clé privée

Autorité de certification Internet

Dans le cadre de l'usage le plus courant en mode https, soit par Internet, les certificats intermédiaires de l'autorité (et au besoin celui de l'autorité racine) devront être installés sur le système Windows du serveur Web Access, via les outils de gestion de certificats de Microsoft.

2. Usage d’une autorité de certification reconnue d’Internet

Autorité de certification reconnue d’Internet

Le serveur Web Access a pour vocation d’être connecté à Internet, et l’usage d’un certificat délivré par une autorité dument reconnue sur Internet est la solution recommandée vis-à-vis des aspects sécuritaires et confiance de la part des utilisateurs.

Demande de certificat

La demande se fait généralement directement via le site Internet de l’autorité émettrice, en lui communiquant soit le contenu du fichier de demande de certificat issu du serveur Web Access, soit en saisissant sur un formulaire tous les éléments nécessaires (URL, nom, pays, région, adresse ….).

Délivrance et usage du certificat

Une fois les opérations techniques vérifiées, et la partie facturation actée, un fichier de certificat sera délivré au demandeur.

Pour utiliser ensuite le certificat au niveau du serveur Web Access, il convient de recopier le fichier “cert.cer” en lui indiquant le bon nom, dans le dossier du serveur Web Access, et de renommer le fichier de clé privée .PVK.TMP en supprimant l’extension TMP.

De là, la mise en œuvre https du serveur Web Access est possible (la présence et la conformité des 2 fichiers autour du certificat va débloquer l'option d'activation du mode https).

Remarque : En complément, il convient de récupérer le certificat de l'autorité ayant validée celui du serveur Web Access, ainsi que les autorités intermédiaires et celle racine (elles sont disponibles et communiquées par l'autorité émettrice) et de l'installer localement dans les autorités intermédiaires de confiance du **compte de l'ordinateur** : ce point, important, va permettre, la délivrance de la chaîne complète des autorités de certifications utilisées à des systèmes dits statiques au niveau de la validation des autorités, comme les navigateurs Firefox 3.x et 4.x, iOS (sur iPhone et iPad), Android (contrairement à Internet Explorer qui peut suivant la version de Windows aller chercher sur Internet la validité des certificats intermédiaires). A défaut, si le service Web Access tourne avec un compte utilisateur, cette installation peut être limitée à l'installation dans le magasin de certificat de ce compte.

Attention : Il faut bien noter la date d'expiration du certificat afin de prévoir son renouvellement à échéance. C'est le demandeur « le client » qui devra réaliser ce renouvellement.

3. Gestion de l’expiration du certificat

Durée de vie du certificat

Un certificat est émis pour une durée précise, entre 1 et 3 ans généralement. Dès lors que la date d’expiration est arrivée à son terme, l’autorité de certification ne garantit plus l’intégrité du certificat. Il est donc recommandé de ne plus s’y connecter, les navigateurs Internet récents de même que les applications Cegid Web Access affichent un message d’alerte à ce sujet.

Renouvellement du certificat

Dans le cadre d’usage d’une autorité Internet pour la fourniture du certificat, cette dernière prévient par messagerie l’administrateur déclaré (le client) quelques mois avant la date d’expiration, afin de procéder aux opérations administratives et techniques pour son renouvellement.

Dès lors, la procédure de renouvellement se gère comme une demande initiale de mise en place d’un certificat sur le serveur Web Access.

4. Exemple de mise en œuvre (avec demande et validation de certificat via autorité Internet)

Partons du principe, comme exemple, que le nom du serveur sera **: srv-dt-vcwas.cegid.com**

Il va falloir dans l'ordre :

- Avoir une adresse IP fixe ainsi qu'un nom de domaine (dument déposé si usage via Internet)
- Créer un enregistrement de type CName par serveur Web Access, au niveau du détenteur de nom de domaine Internet et indiquer ce nom comme nom d'hôte au niveau du serveur Web Access
- Générer une demande de certificat avec ce nom d'hôte
- Enregistrer la demande auprès d'une autorité Internet
- Recevoir le certificat conforme et le copier sur le serveur Web Access
- Installer localement sur le système Windows, les certificats de l'autorité, les certificats intermédiaires, …
- Passer le serveur Web Access en mode https

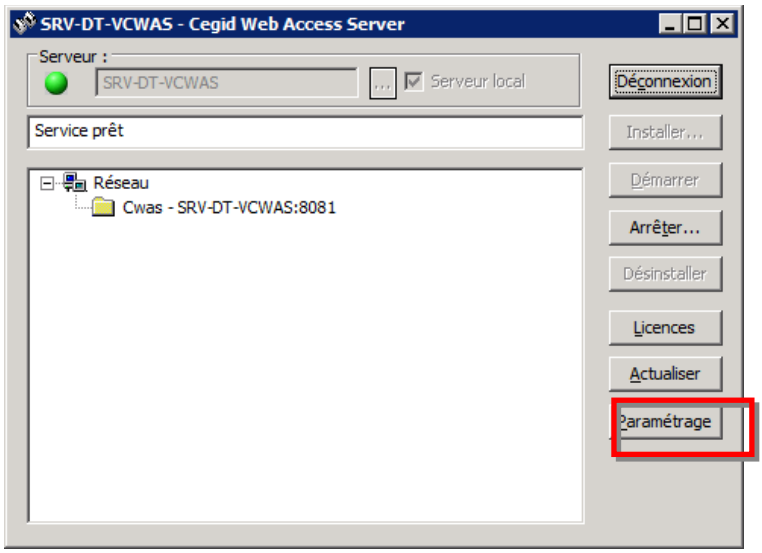
Optionnellement : rediriger automatiquement les connexions client arrivant sur le port TCP 80 vers le port 443 (sur solution de maquette, **ne pas utiliser cette option en production**)

Réglages du serveur Web Access

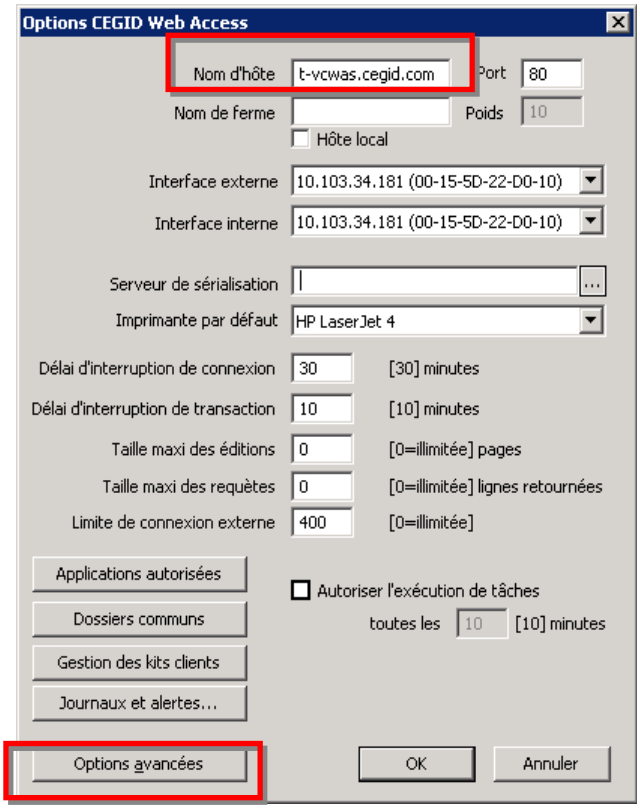
Configuration de nom :

Le nom d'hôte Windows du serveur peut être conservé en état, sous forme de connotation à usage interne, comme « srv-dt-vcwas », pas contre le nom du serveur Web Access devra être configuré précisément avec celui qui sera visible par les clients depuis Internet (le certificat étant émis pour cette URL). Ce nom doit être choisi et configuré avant toute demande de certificat !

Depuis la console du serveur Web Access, ouvrez le module PGIeMoniteur



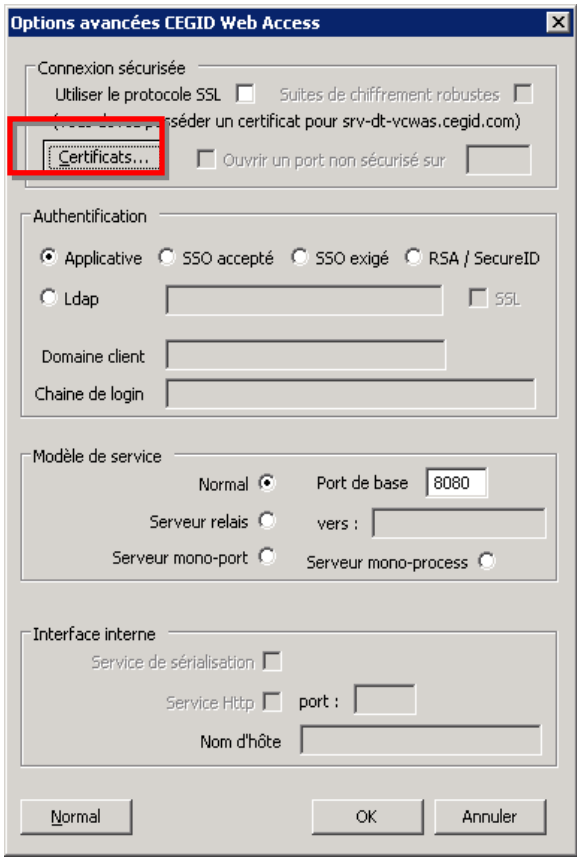
Allez sur **"Paramétrage"**



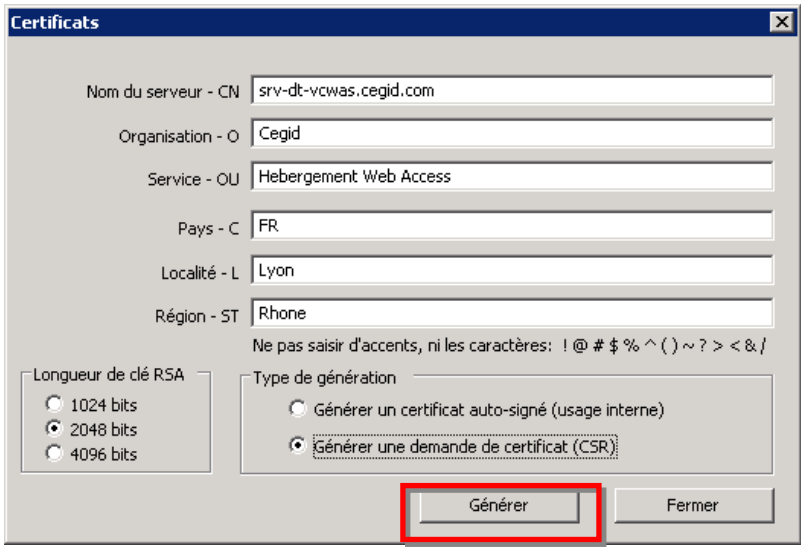
Indiquez au niveau du champ "Nom d'hôte", le nom complet DNS de votre serveur, soit dans notre exemple : **srv-dt-vcwas.cegid.com**

Validez votre choix par **"OK"**

Relancez l'appel du paramétrage et cliquez sur **"Options avancées"**



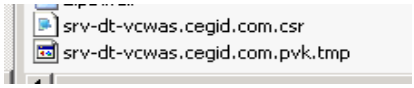
Appelez le bouton **"Certificats…"**



Renseignez bien tous les champs de description liés à votre demande,

Puis **"Générer une demande de certificat (CSR)"**, pour obtenir un fichier de demande

Appelez ensuite le bouton **"Fermer"**



Le fichier de demande de certificat est situé à l'emplacement des programmes du serveur Web Access, soit par défaut « c:\cws\nom_du_cwas.csr ». (le fichier de clé privée a dans un 1ier temps l'extension .tmp, **il ne doit surtout pas être perdu !**) Le contenu du fichier CSR peut être transmit par copier-coller lors de la demande sur la page web de l'autorité de certification

En retour, l'autorité va vous délivrer :

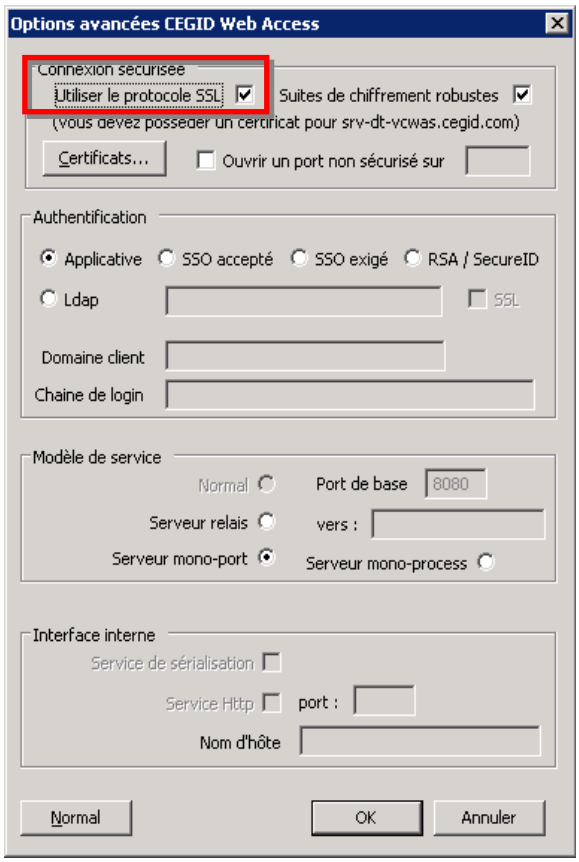
Votre certificat tel que demandé « votre_certificat.cer »

Les certificats des différentes autorités de la chaîne de validation

Le certificat de votre serveur Web Access, doit être copié à l'emplacement tel que décrit ci-dessus, et il doit s'appeler exactement « nom_url.cer ». Vous pouvez maintenant supprimer l'extension « .tmp » du fichier de clé privée lié à votre certificat.

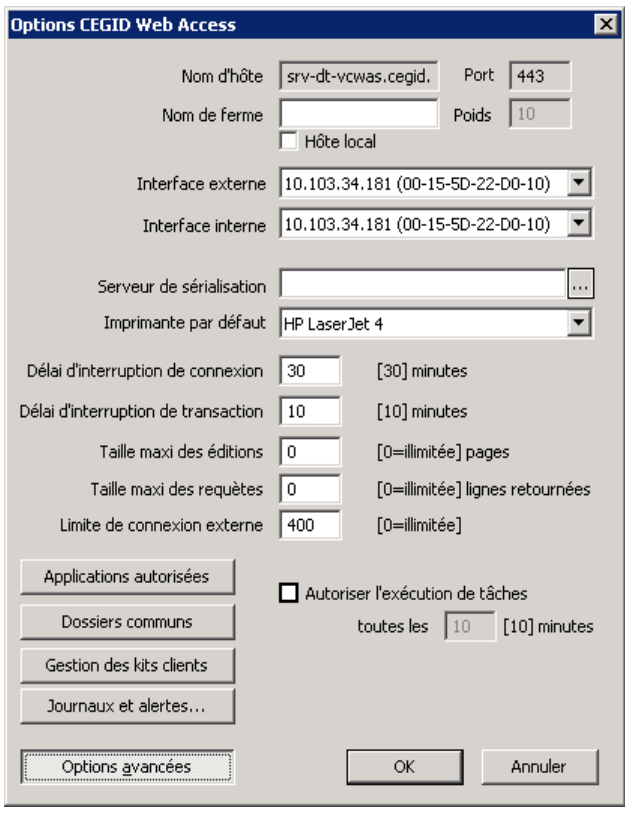
Les différents certificats des autorités transmises devront être installés dans le magasin Windows de ce système

Vous pouvez maintenant activez l'usage du mode https pour le serveur Web Access



Confirmez par **"OK"**

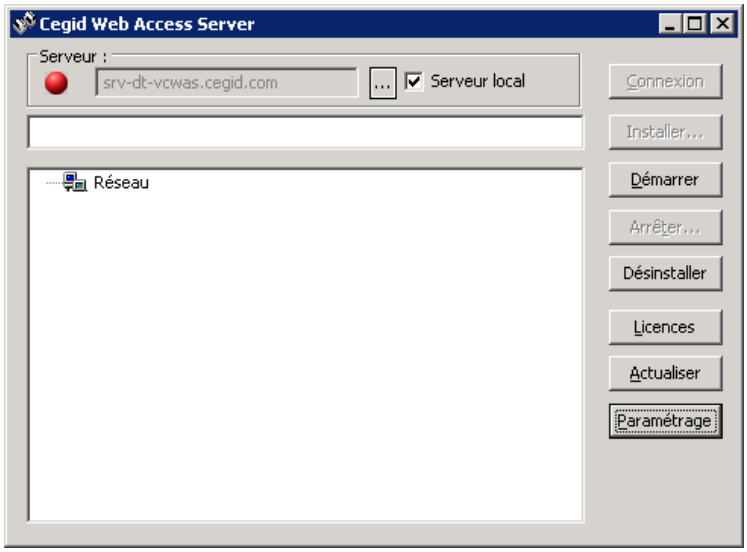
(Au besoin cochez « Ouvrir un port non sécurisé sur » « 80 », afin d'activer la redirection automatique des flux http vers https)



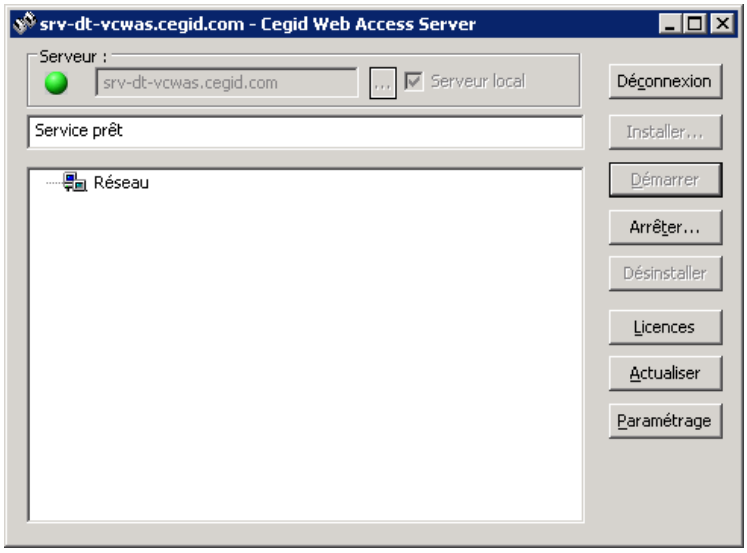
Le nom d'hôte ainsi que le port TCP 443 sont maintenant non modifiables

(Conséquence de l'usage du mode SSL)

Confirmez par **"OK"**



Arrêtez et redémarrez le serveur Web Access

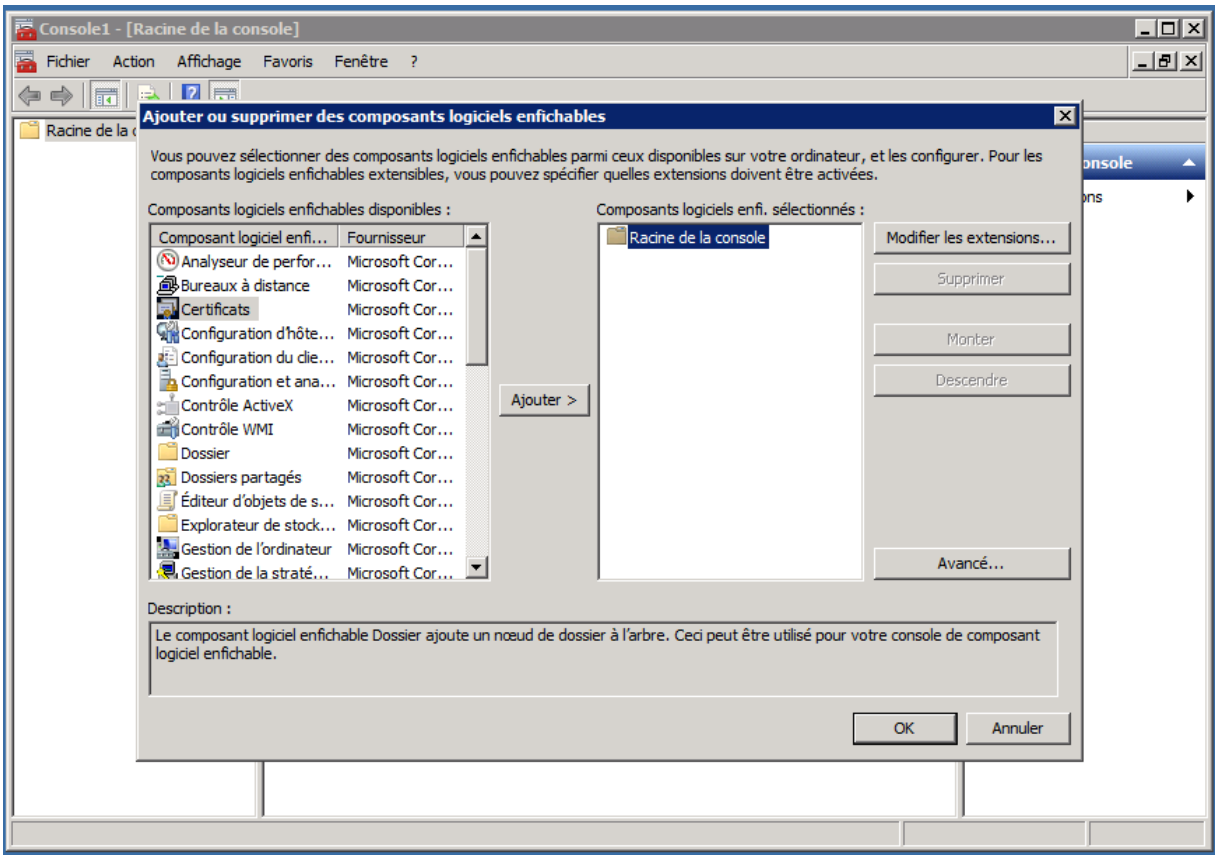


Au besoin, répétez cette opération pour chaque serveur Web Access d'une même ferme (avec indication d'un nom commun de ferme sur l'ensemble des serveurs).

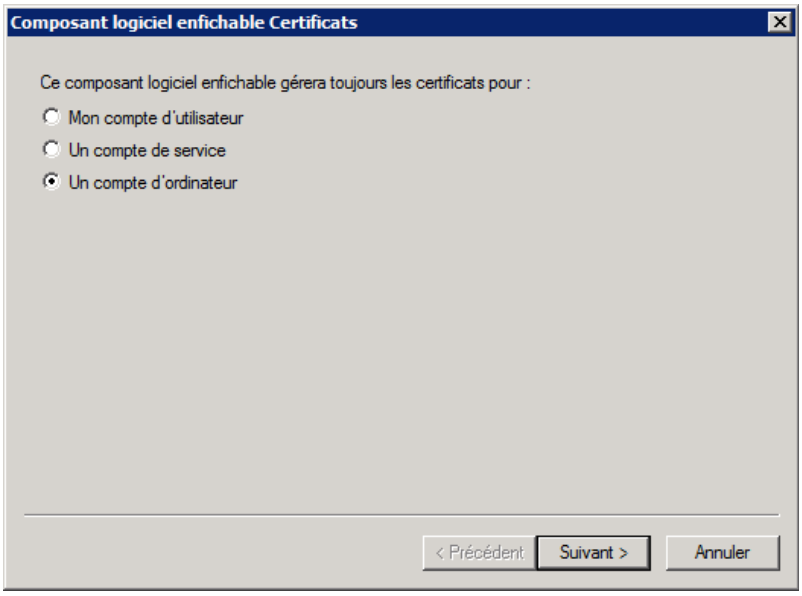
Installation des certificats intermédiaire et de l'autorité

L'ensemble des certificats de la chaine, soit ceux de l'autorité de certification ainsi que ceux intermédiaires, doivent être installés sur le compte de l'ordinateur qui gère le serveur Web Access. Ces certificats sont fournis par l'autorité utilisée pour la validation.

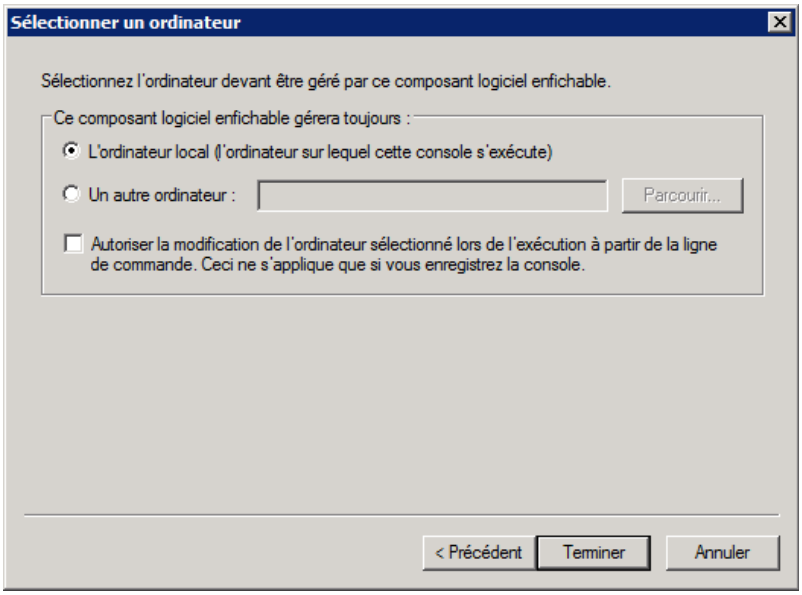
Pour cela, utilisez le module « MMC » de gestion de certificats



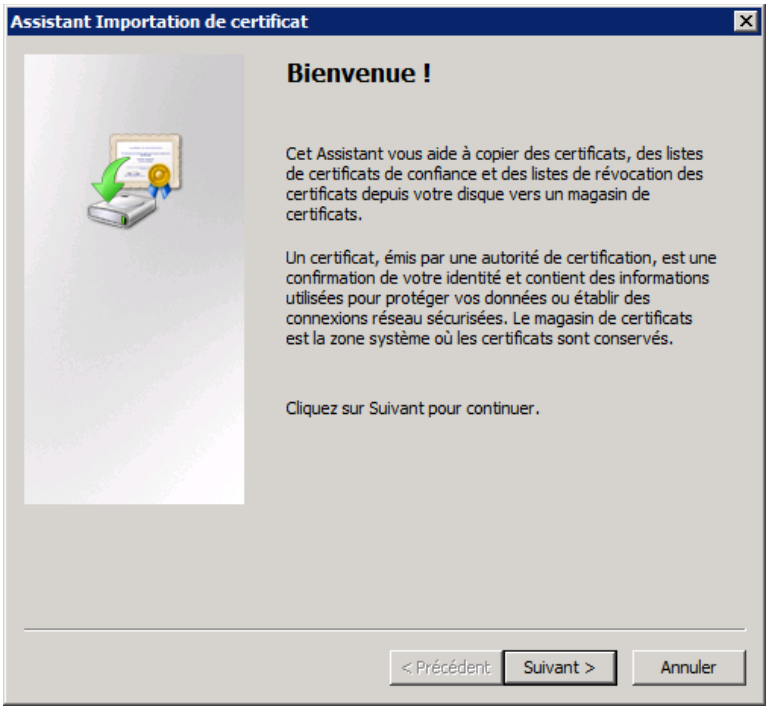
Choisir « Un compte d'ordinateur »



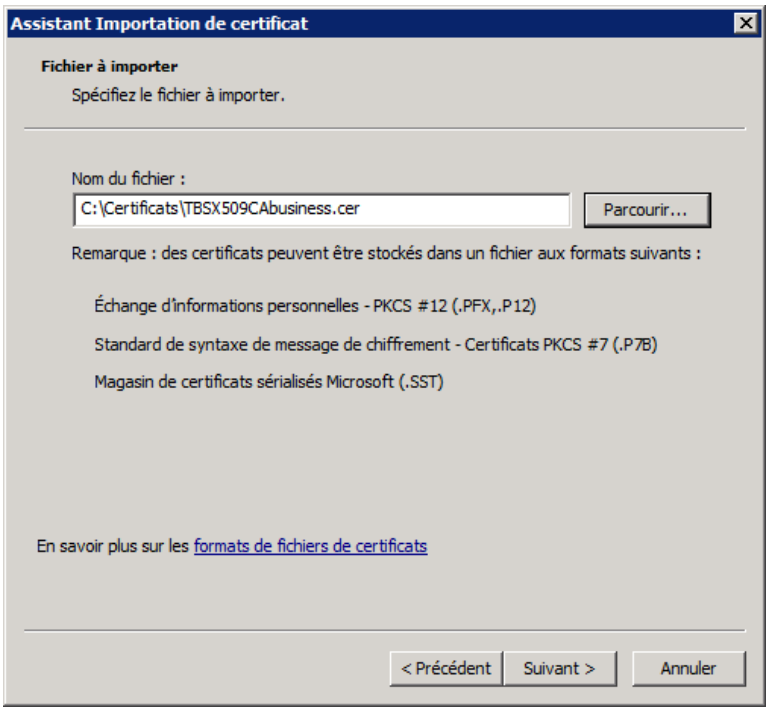
Et « l'ordinateur local »

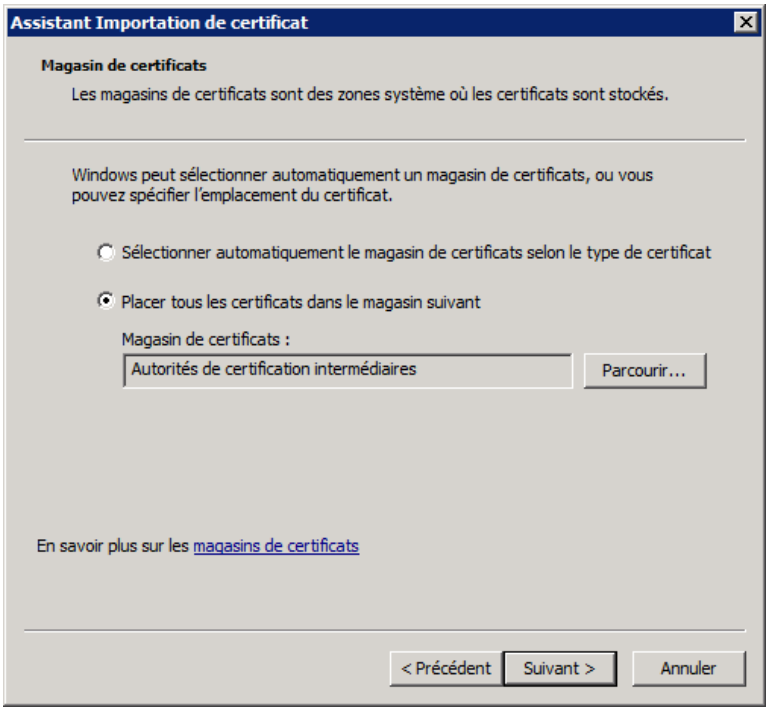


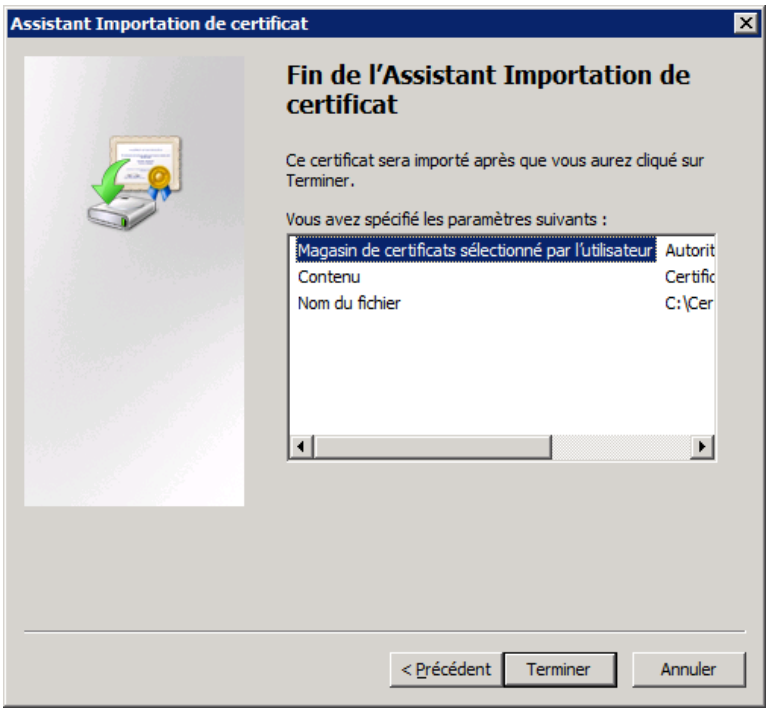
Au niveau des « autorités intermédiaires de confiance », choisir « Importer… »



Indiquer le fichier « .cer » communiqué par l'autorité







Répétez cette opération pour l'ensemble des certificats des autorités intermédiaires, ansi que pour celle de l'autorité racine, cette dernière étant à installer dans le magasin des « autorités de certification racines de confiance ».

De là, vous pouvez vérifier l'état du certificat affiché par le serveur Web Access, soit