Mettre en place un certificat SSL

Cette page a été écrite pour Windows 7, et doit être considérée avec prudence. Si vous avez l'occasion de dérouler cette procédure pour Windows11, faites nous un retour !

Pour mettre en place un certificat, il faut d'abord l'acheter auprès d'une des autorités de certification, organismes qui ont vendu ces prestations à des prix éhontés pendant fort longtemps, avant que la concurrence ne finisse par permettre à de nouveaux acteurs de proposer des certificats low-cost, ou même gratuits.

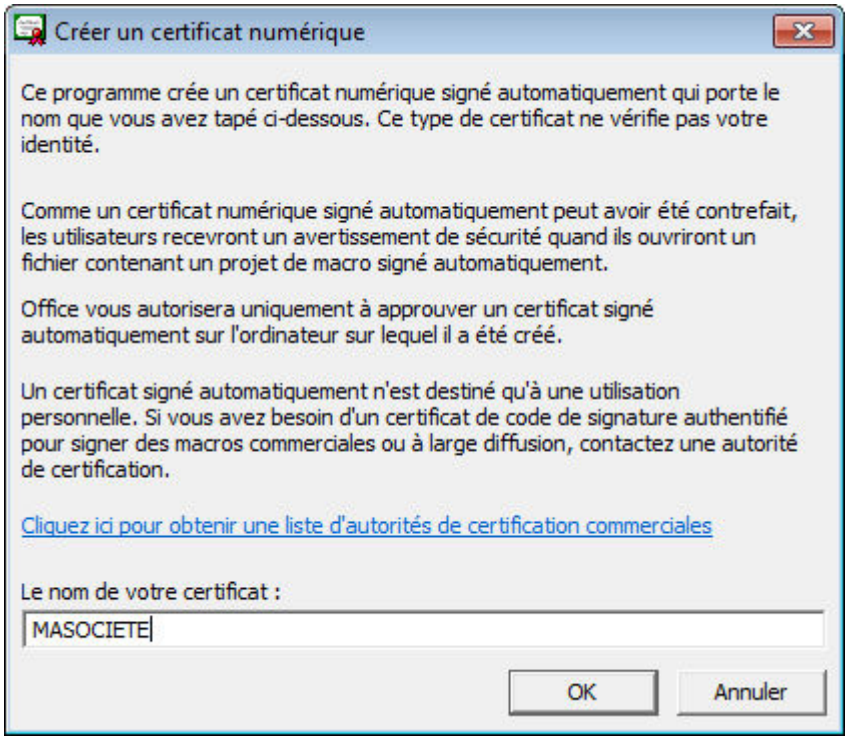
Cependant, il existe deux autres méthodes qui permettent de générer vous-même, et immédiatement, des certificats auto-signés, et donc gratuits.

- La première est d'utiliser l'assistant de génération de certificat numérique pour les projets VBA. Mais il faut pour cela avoir installé la suite Office sur sa machine.
- La seconde méthode est d'utiliser le programme WinXXOpenSSL, qui permet d'utiliser de manière pratique les bibliothèques OpenSSL, un outil open-source destiné à cela.

La limitation d'un certificat auto-signé est que si vous signez numériquement un document à l'aide d'un certificat numérique que vous avez créé et si vous partagez ensuite le fichier signé numériquement, les autres personnes ne pourront pas vérifier l'authenticité de votre signature numérique sans décider d'approuver manuellement votre certificat auto-signé. L'autre limitation est que la loi précise que le certificat doit être "qualifié", notion sujette à interprétation.

Utilisation de l'assistant pour les projets VBA

Dans Windows, cliquez sur le bouton Démarrer. Sélectionnez Tous les programmes. Cliquez sur le dossier Microsoft Office, puis sur le dossier Outils Microsoft Office 2010. Cliquez sur Certificat numérique pour les projets VBA (vous pouvez aussi utiliser le menu démarrer, et taper "certificat" dans la zone de recherche)



Dans la boîte de dialogue Créer un certificat numérique, tapez un nom pour votre certificat et cliquez sur OK.

Utilisation de WinXXOpenSSL

Installation de WinXXOpenSSL

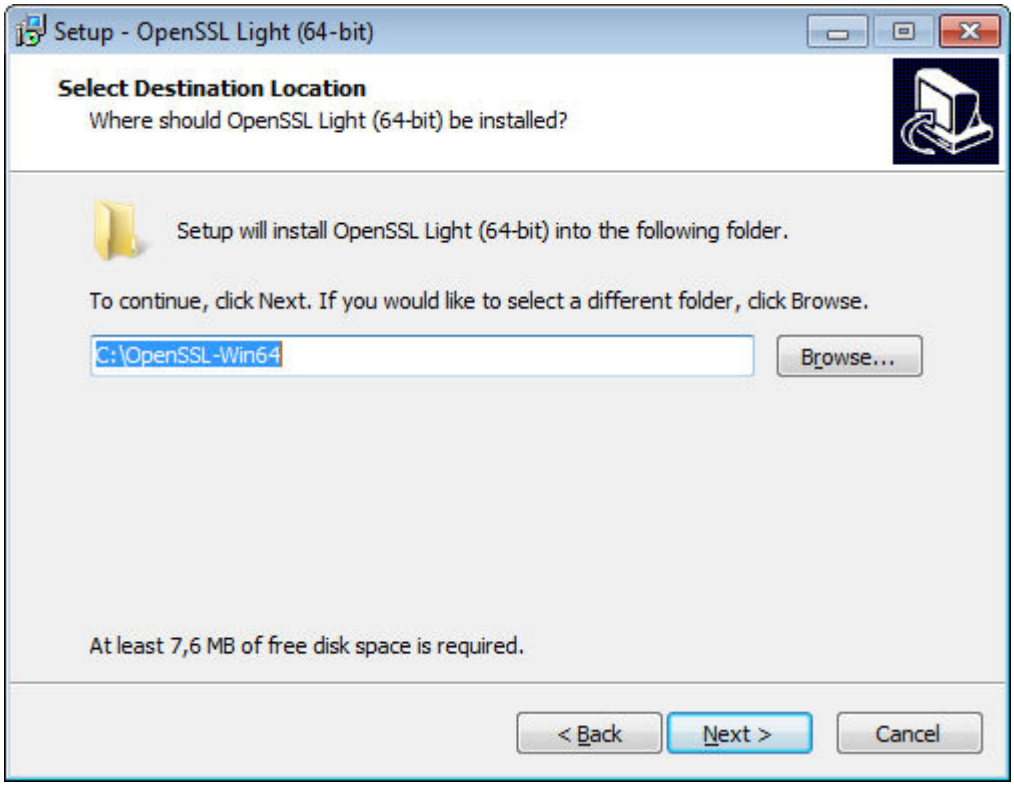
Pour créer votre certificat auto-signé, nous allons utiliser un programme développé par Shining Light Productions, utilisant la bibliothèque open-source OpenSSL.

Ce programme est disponible sur cette page. Visiblement, le développeur a un caractère assez direct !, mais vous pouvez lui faire un don car son programme fait vraiment gagner du temps.

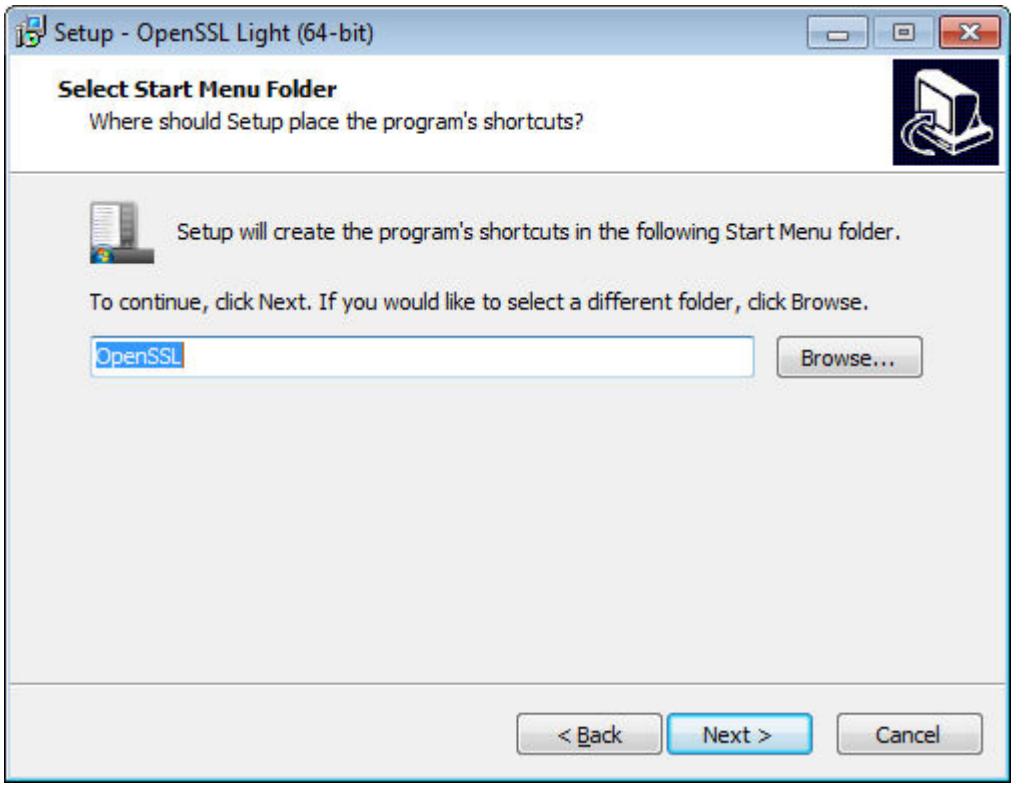
Plusieurs versions sont diponibles :

- la version 32 bits et la version 64 bits. Choisissez la version 64 bits si votre système est en 64 bits (pour le vérifiez, si vous ne le savez pas, cliquez sur le menu “démarrer”, faites un clic droit sur le menu “ordinateur”, et choisissez “propriétés”). Pour ce tuto, nous avons sélectionné la version 64 bits.
- la version light ou la version standard. Téléchargez la version light, elle est plus simple.

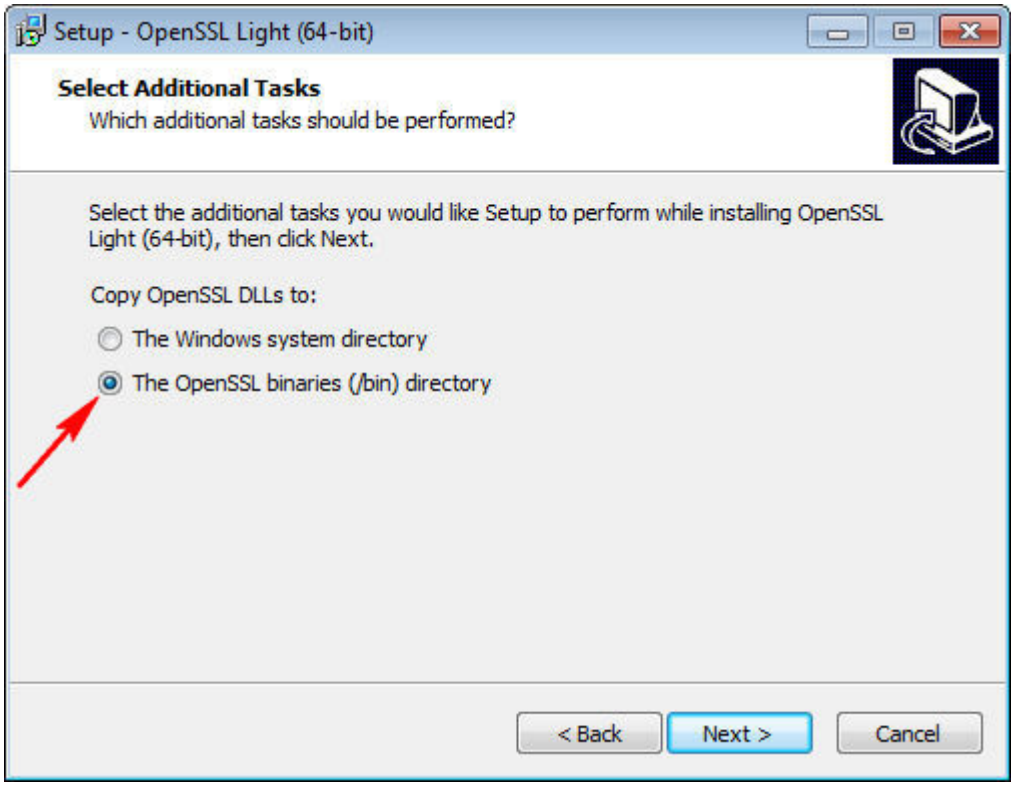
Exécutez ensuite le programme.



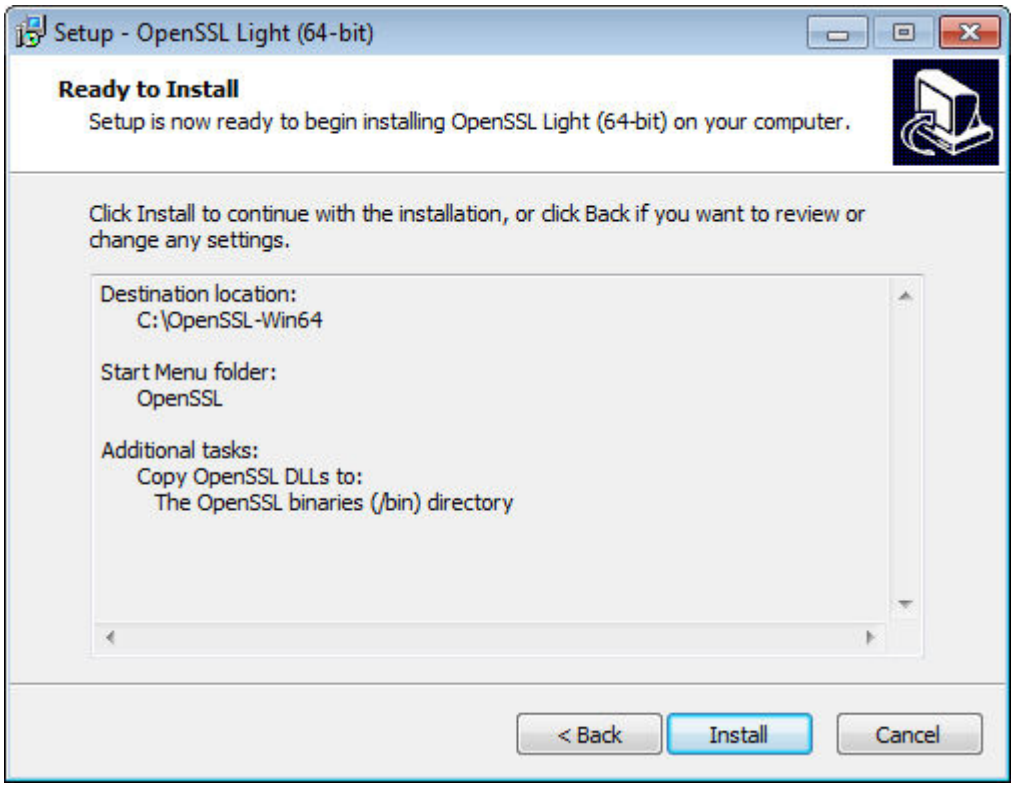
Sur l'écran de sélection du répertoire d'installation, vous pouvez laisser la valeur par défaut, "*C:\OpenSSL-Win64*" (ou "*C:\OpenSSL-Win32*" si votre système est en 32 bits.)



Là aussi, vous pouvez laisser le raccourci par défaut.



Sélectionnez la destination des DLL servant à utiliser OpenSSL : choisissez "*The OpenSSL binaries (/bin) directory*"



Et voilà la fenêtre récapitulative de l'installation. Cliquez sur "Install" pour terminer l'installation.

Ajout de la variable d'environnement

Maintenant, ajoutons dans les variables d'environnement de votre ordinateur le répertoire "bin"

d'OpenSSL : “*C:\OpenSSL-Win64\bin*” (ou “*C:\OpenSSL-Win32\bin*”).

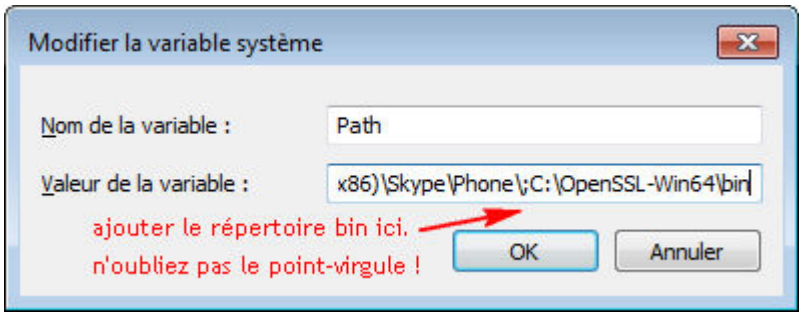
Pour cela, aller dans le menu démarrer de Windows, et cliquez droit sur ordinateur, puis “*Propriétés*”.

Dans cette fenêtre cliquez sur “*Paramètres système avancés*”.

Cliquez ensuite sur “*Variables d'environnement...*”

Puis sélectionnez la ligne “PATH” et cliquez sur le bouton “Modifier”

Sur cet écran, ajoutez le répertoire bin d'OpenSSL au “path” de windows, c'est à dire soit “*;C:\OpenSSL-Win64\bin*” si vous avez choisi la version 64 bits, soit “*;C:\OpenSSL-Win32\bin*” si vous avez choisi la version 32 bits.



Création du certificat SSL

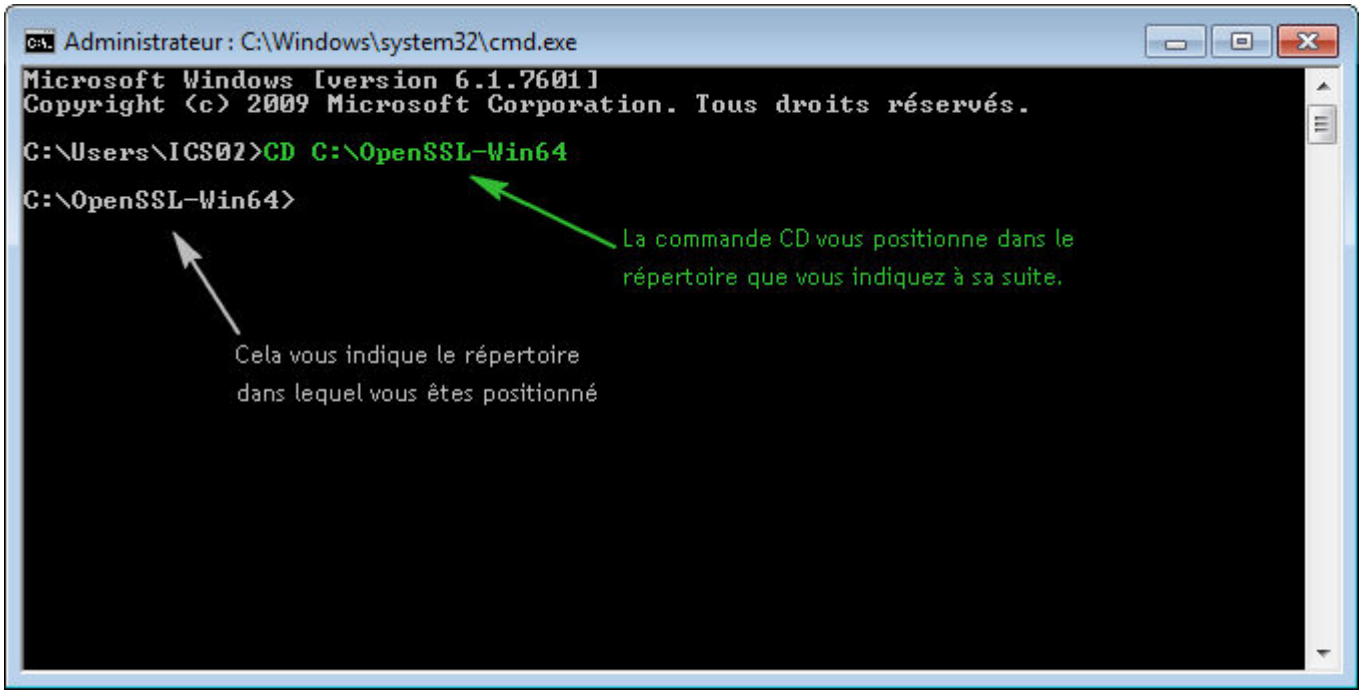
A présent, nous allons nous lancer dans la création du certificat SSL. Cela peut paraître un tout petit peu compliqué aux gens normaux, pas geeks, mais nous avons tellement détaillé le tuto que même si vous n'avez qu'un seul bras gauche, vous devriez y arriver facilement. Suivez le guide.

Commençons par ouvrir une fenêtre d'invite de commande. Non, restez assis, allez simplement dans le menu démarrer de Windows, tapez “cmd” dans la barre de recherche, et exécutez le programme cmd.exe.

Cela va ouvrir une fenêtre que l'on appelle la console.

Tapez la ligne de commande suivante afin de vous placer dans le dossier contenant OpenSSL :

```
cd C:\OpenSSL-Win64
```



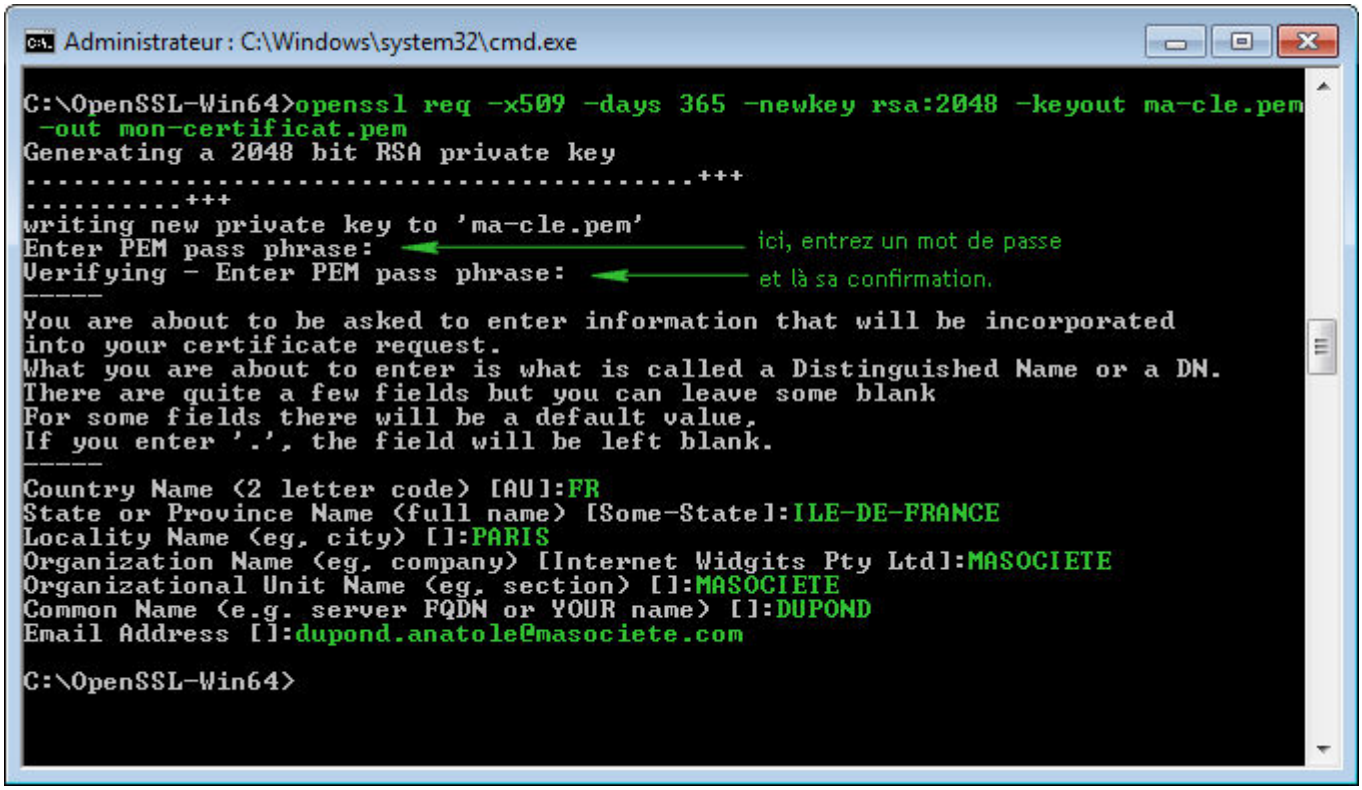
Nous allons ensuite créer deux fichiers important pour la création du certificat, pour ce faire tapez la commande suivante :

```
   openssl req -x509 -days 365 -newkey rsa:2048 -keyout ma-cle.pem -out mon-certificat.pem
```

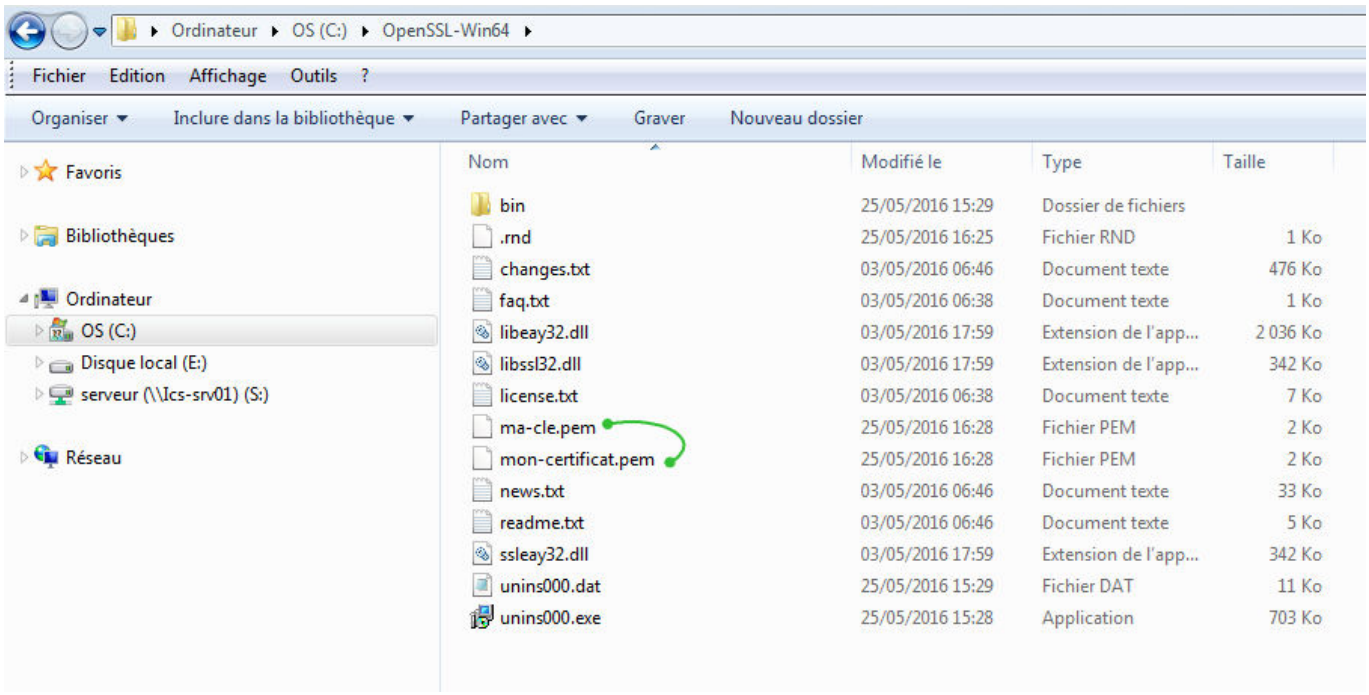
Dans cette ligne, le premier fichier important se nomme “ma-cle” et l'autre se nomme “mon-certificat”. L'option “*-days 365*” permet de générer un certificat valable un an.

Cette commande va ensuite vous demander un mot de passe (évitez azerty, comme mot de passe !), puis va vous demander les caractéristiques du certificat.

Voici par exemple, ce que nous avons rentré :



Désormais si vous regardez dans votre dossier "*C:\OpenSSL-Win64*", vous verrez deux nouveaux fichiers : ma-clem.pem et mon-certificat.pem comme ici :



Il faut maintenant initialiser la variable RANDFILE. Pour ce faire tapez dans la console :

```
set RANDFILE=.rnd
```

Nous allons maintenant créer le certificat au format p12.

Pour cela, tapez la ligne suivante :

```
openssl pkcs12 -export -in mon-certificat.pem -inkey ma-cle.pem -out
```

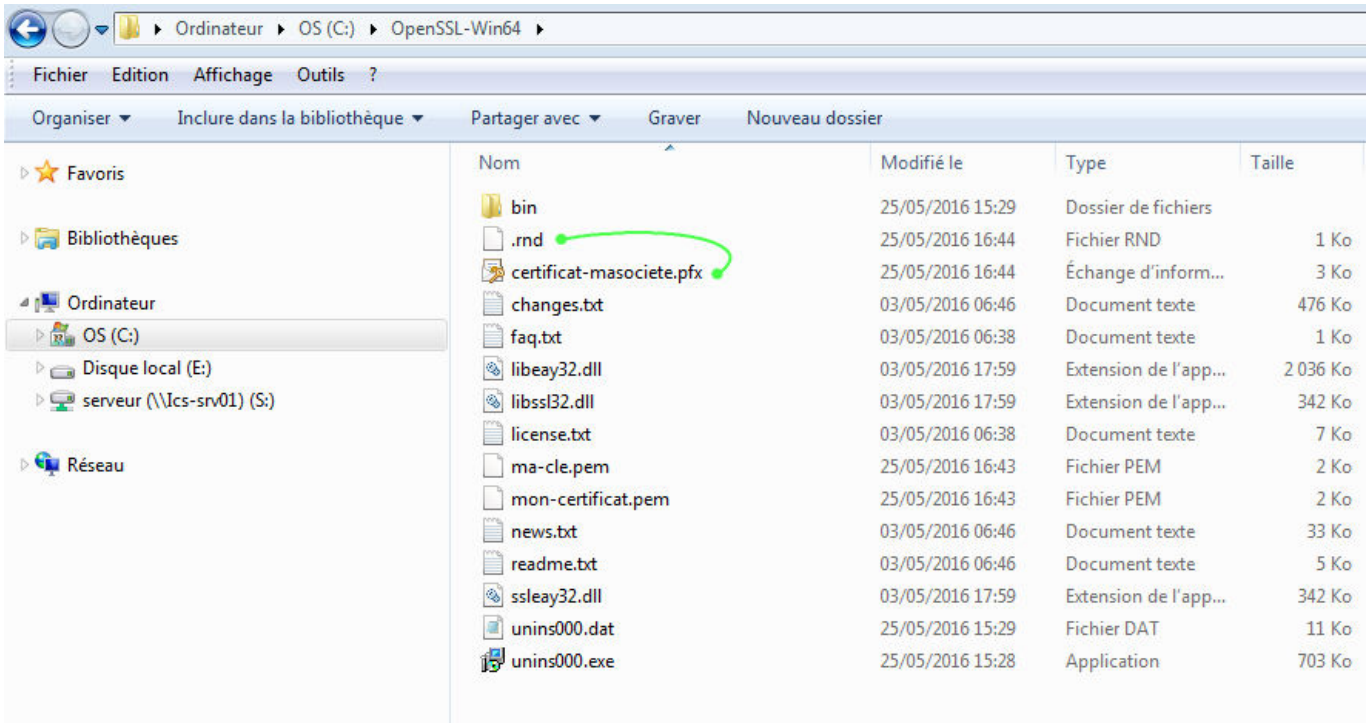
```
certificat-masociete.pfx
```

Dans cette ligne, le nom de mon certificat sera "*certificat-masociete*". Ne pas oublier l'extension du fichier qui est "*pfx*".

Cette commande va ensuite vous demander le mot de passe que vous avez donné plus haut, puis va vous demander créer un mot de passe pour l'export/import du fichier dans la bande de certificat.

Voici ce que vous aurez :

Désormais si vous regardez dans votre dossier "*C:\OpenSSL-Win64*", vous verrez deux nouveaux fichiers : .rnd et certificat-masociete.pfx comme ici :

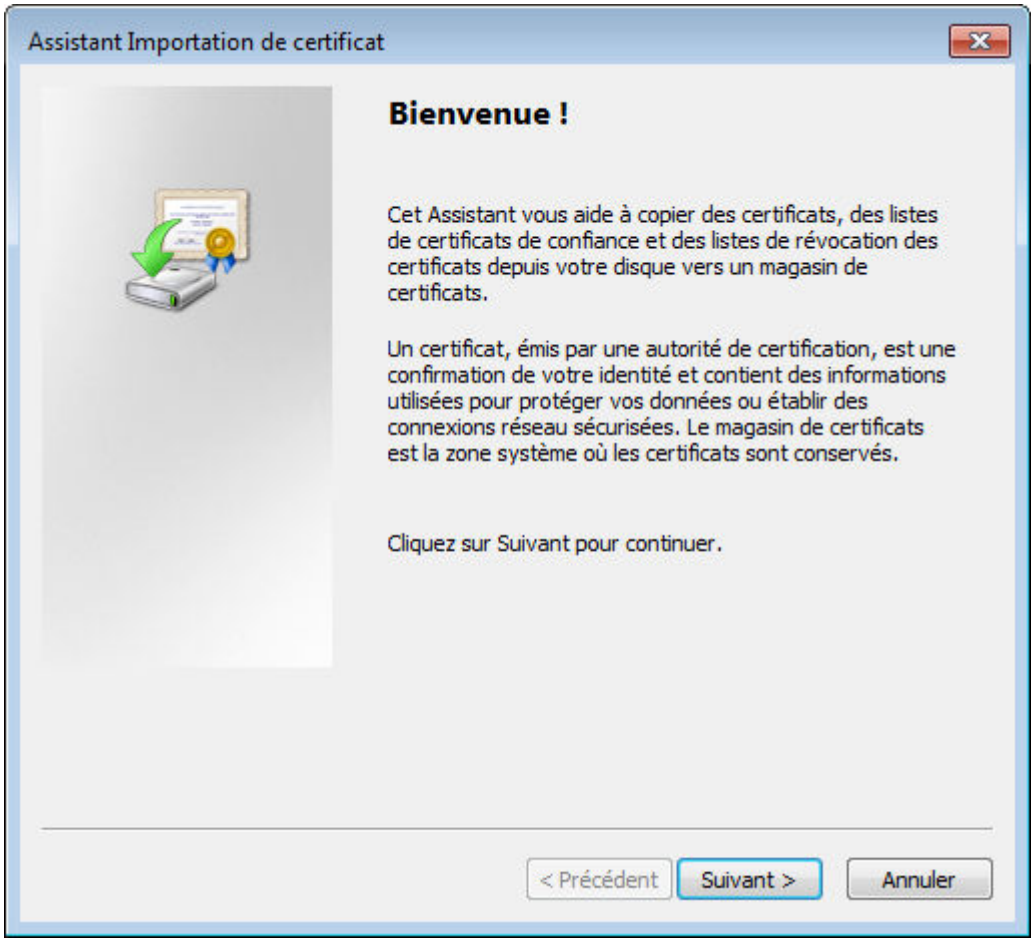


Installation du certificat dans la banque de certificat

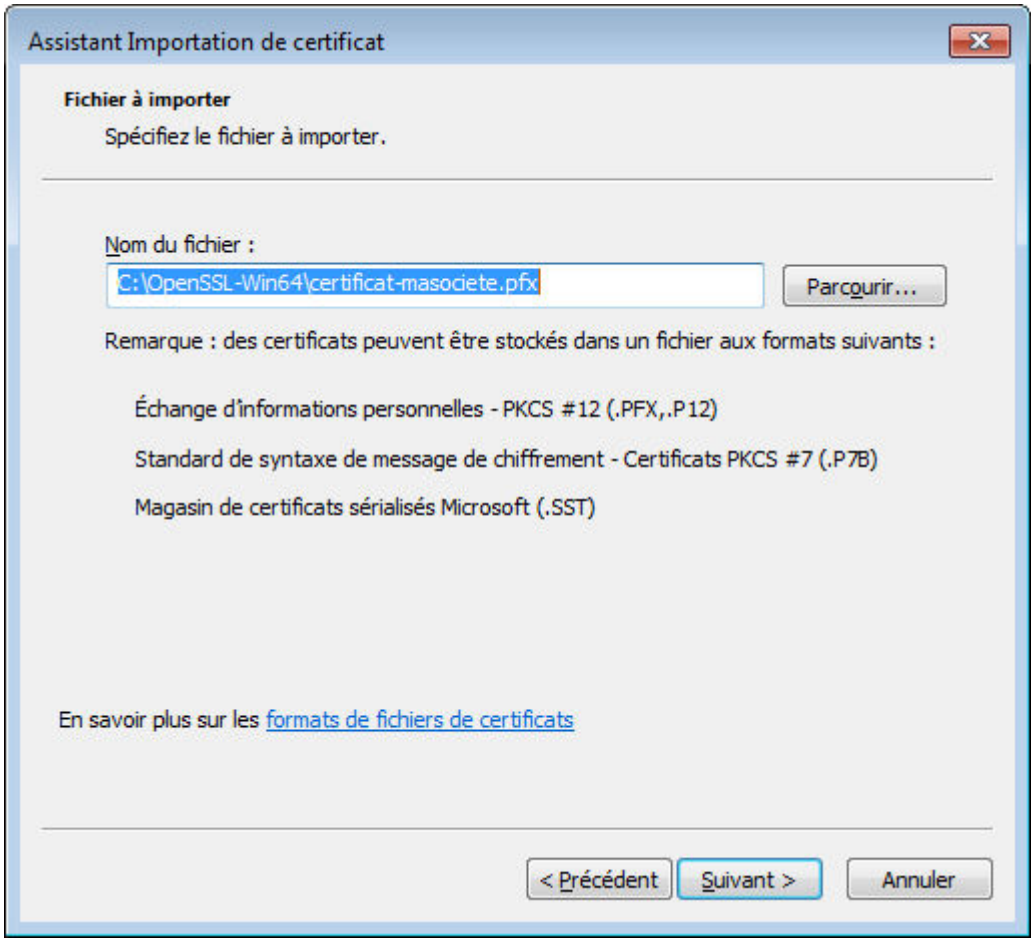
Allez dans votre dossier "*C:\OpenSSL-Win64*", puis double-cliquez sur le fichier "*certificat-gestan.pfx*".

Voilà les écrans qui apparaissent.

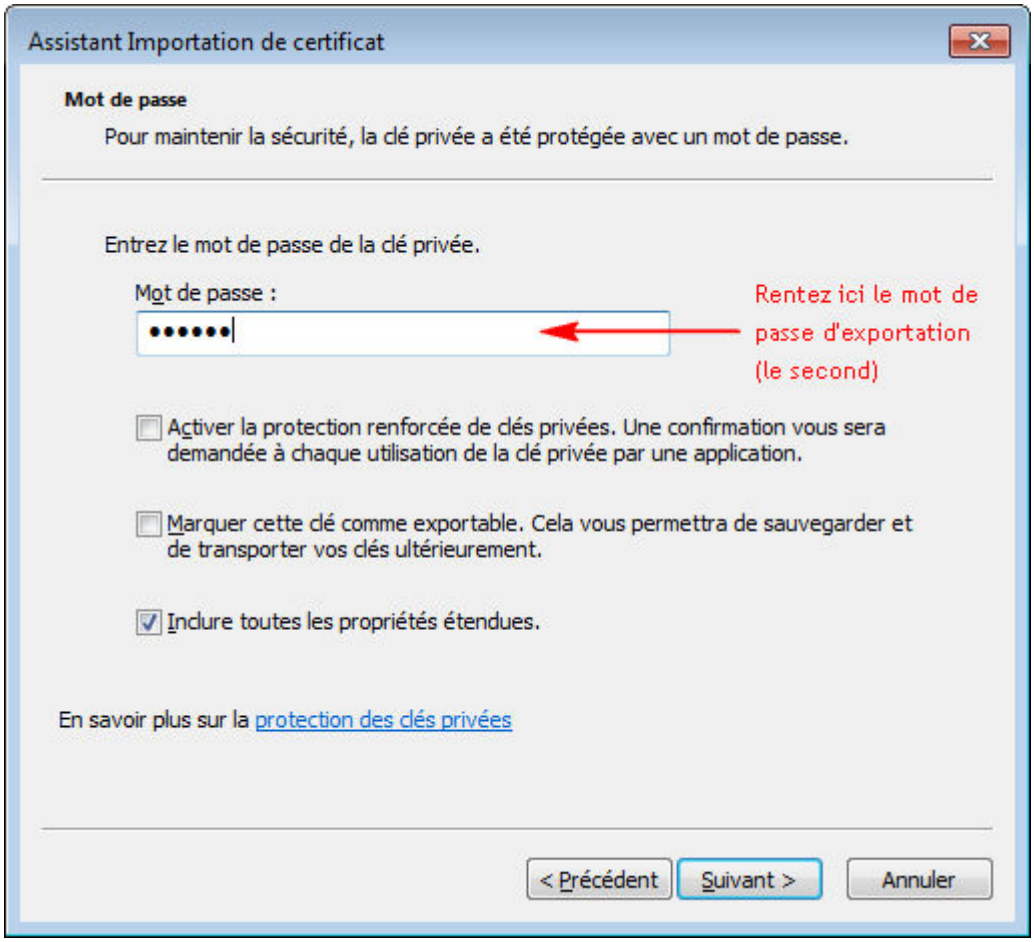
Tout d'abord un écran de bienvenue. Cool !



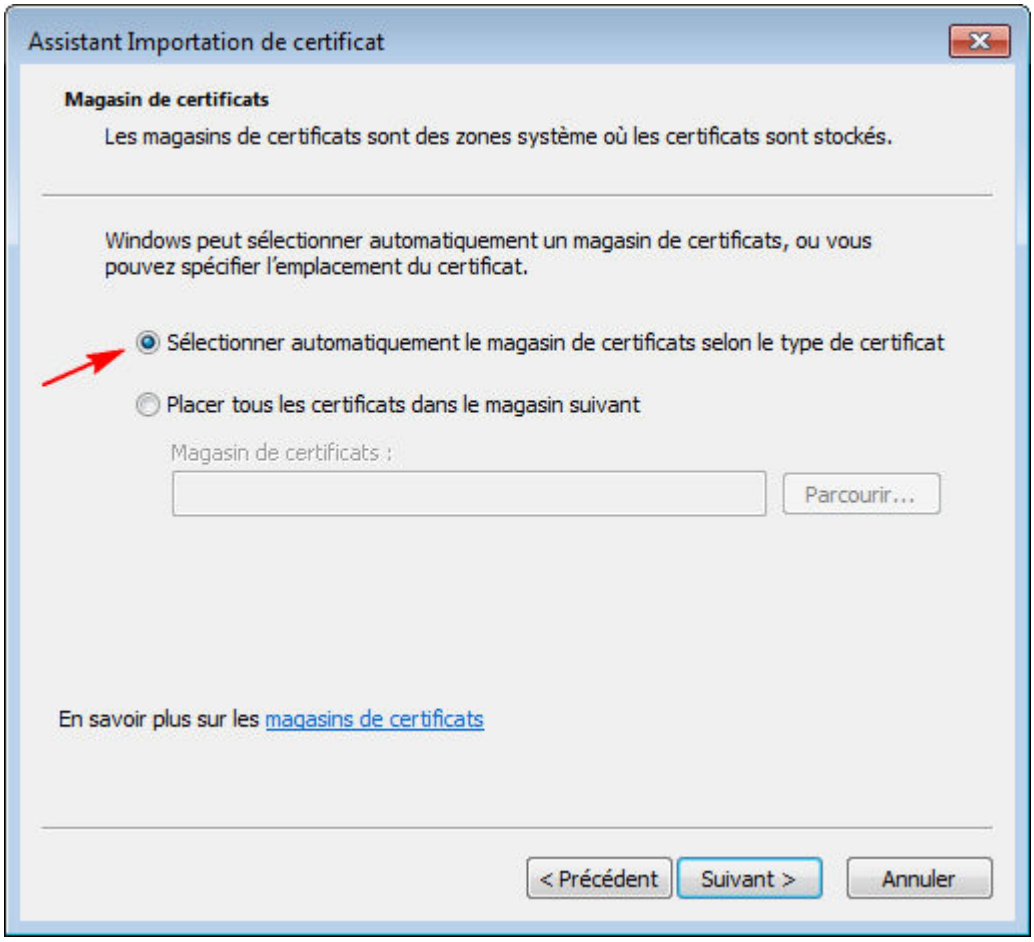
La sélection du fichier à importer. Laissez la valeur affichée.



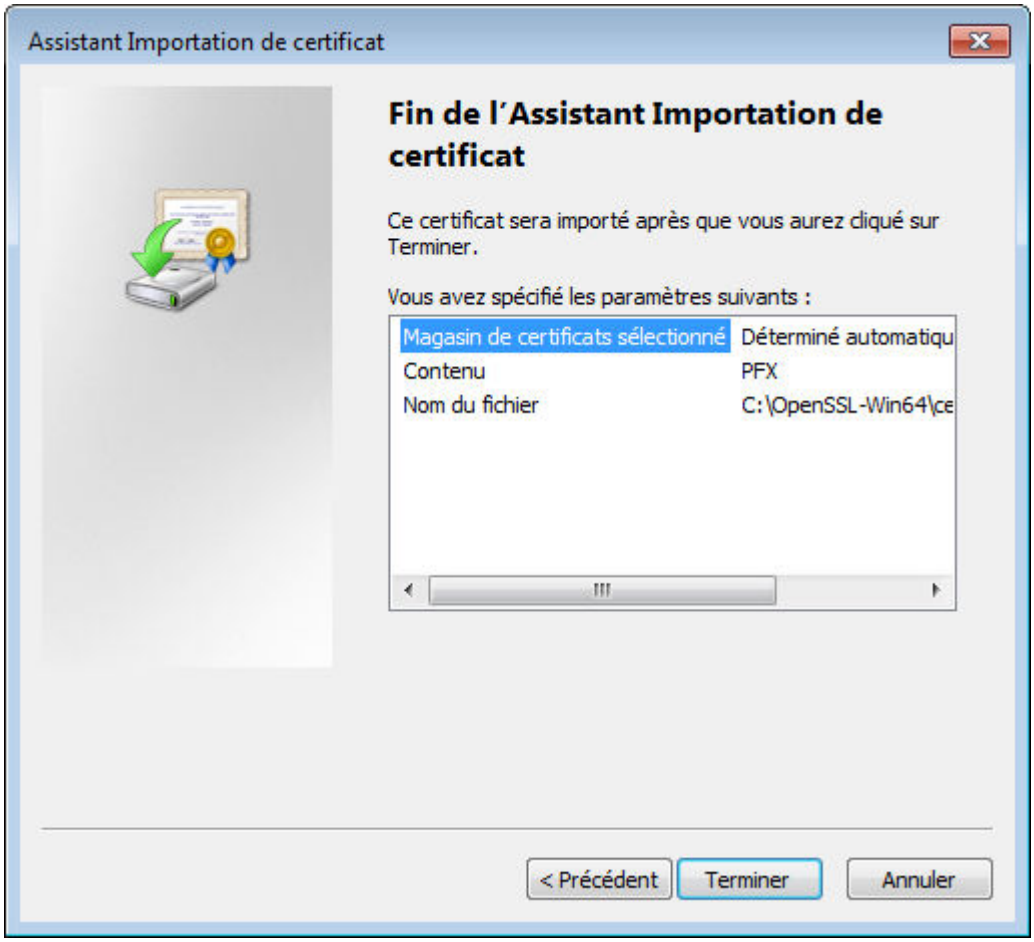
L'écran de saisie du mot de passe (saisir le mot de passe d'exportation, c'est à dire le second de vos mots de passe)



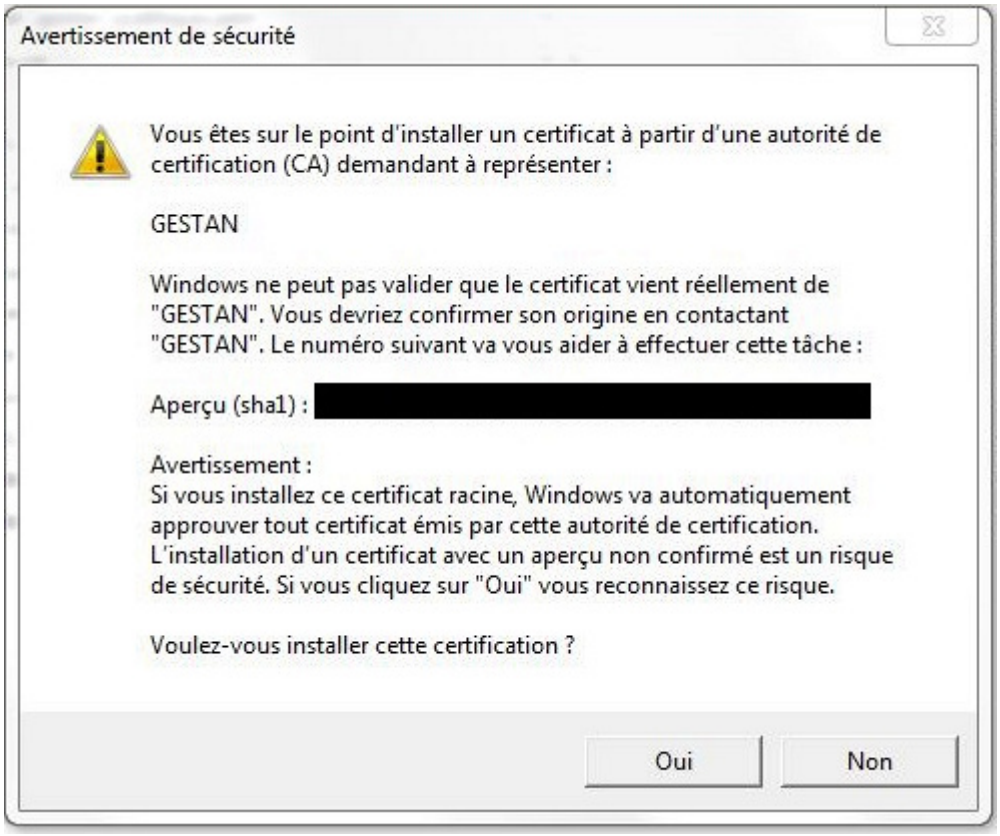
L'écran de sélection du magasin de certificats. Vous pouvez laisser la détermination automatique.



Et enfin l'écran de récapitulation.



A la fin de l'installation, si vous êtes administrateur, une pop-up vous indiquera la bonne installation du certificat. Dans le cas contraire, une fenêtre d'avertissement va s'ouvrir dans laquelle la clé de hachage du fichier va être indiquée. Vous pouvez la conserver au chaud (par exemple, avec un Ctrl+C sur cette pop-up, puis un Crtl+V dans le gestionnaire de notes de Gestan 😉)



Voilà, vous avez installé votre certificat. Bravo !

Autres articles “Technique”

Temps de réponse
Tester la communication
Tester votre connexion Internet
Transférer Gestan d'ordinateur
Tuto détaillé SuperPDP
Téléphonie SIP-TAPI *
Utiliser Linux