Demande et installation d'un certificat

Table des matières

Introduction

Pour obtenir un certificat, il faut dans un premier temps générer une demande de certificat (CSR, Certificate Signing Request). Lors de la demande de certificat vous allez générer une clé privée. Dès que cette clé est générée, faites-en une copie de sauvegarde et protégez-la très sérieusement (voir la partie **« Récupérer la clé privée »**).
Le CSR contient la clé publique et des informations d'identification du demandeur que l'on spécifiera dans la documentation ci-dessous.

Linux

Demander un certificat

- Pour commencer, vérifier si **« openssl »** est bien installé sur votre système qui héberge le service
- Ensuite ouvrez un terminal, allez dans le répertoire **« certificats »** du service (ex : service Apache) que vous désirez mettre en place et tapez la commande suivante :

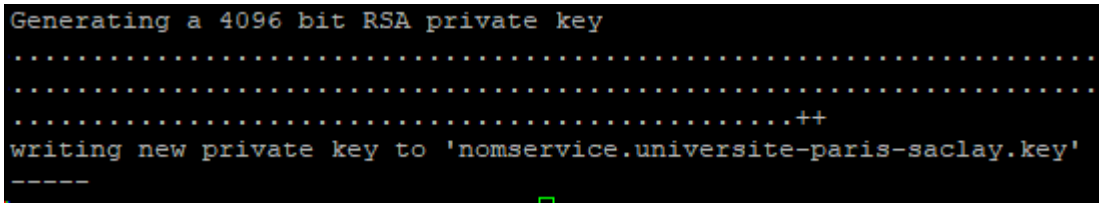
  - **Cas d'un certificat avec un seul domaine**

openssl req -newkey rsa:4096 ***-keyout*** nomservice.universite-paris-saclay.fr.key ***-nodes -subj*** "/C=FR/O=UNIVERSITE PARIS-SACLAY/CN=nomservice.universite-paris-saclay.fr/" ***-out*** nomservice.universite-paris-saclay.fr.csr

Attention, nomservice**.universite-paris-saclay.fr** devra correspondre au nom DNS du service

Exemple : pour le service d'annuaire Adonis (https://adonis.universite-paris-saclay.fr), le nom DNS a renseigné est adonis.universite-paris-saclay.fr

- La demande de certificat est alors générée voir ci-dessous



  - **Cas d'un certificat avec des multi-domaines**

- ***En ligne de commande :***

Vous devez vous assurer que le fichier de configuration openssl par défaut existe.
Pour cela, tapez la commande :

ls `openssl version -d | awk -F"" '{print $2}'`/openssl.cnf

Si le fichier openssl.cnf est /etc/pki/tls/openssl.cnf et le nom des services sont nomservice.universite-paris-saclay.fr et nomservice.u-psud.fr, tapez la commande :

openssl req -newkey rsa:4096 ***-keyout*** nomservice.universite-paris-saclay.fr.key ***-nodes -subj*** "/C=FR/O=UNIVERSITE PARIS-SACLAY/CN=nomservice.universite-paris-saclay.fr/" **-reqexts SAN -config** <(cat /etc/pki/tls/openssl.cnf <(printf "\n[SAN]\nsubjectAltName=DNS:nomservice.universite-paris-saclay.fr,DNS: nomservice.u-psud.fr")) ***-out*** nomservice.universite-paris-saclay.fr.csr

- ***En utilisant un script dont il faudra modifier les variables :***

Vous pouvez télécharger le script à l'adresse : .https://securite-informatique.dsi.universite-paris-saclay.fr/docs/download/CreationCSR.sh

```
#!/bin/sh

# Initialisation des variables
hostname="monservice.universite-paris-saclay.fr"
alternative_name="monservice.universite-paris-saclay.fr monservice.u-psud.fr"
organisation="UNIVERSITE PARIS-SACLAY"

# On cherche le fichier par défaut pour openSSL
def=`openssl version -d | awk -F'"' '{print $2}'`

#On le copie en local en activant l'extension v3_req.
cat $def/openssl.cnf | sed 's/^#[ ]*req_extensions = v3_req/req_extensions = v3_req/' | sed 's/\[ v3_req \]/\[ v3_req \]\'$'\nsubjectAltName = @alt_names/' > ./openssl.cnf

#On ajoute la section [ alt_names ]
echo "[ alt_names ]" >> ./openssl.cnf

#On ajoute tous les noms de $alternative_name
count=0
```

```
for i in $alternative_name; do
    let count="$count +1"
            echo "DNS.$count=$i" >> ./openssl.cnf
done

#On génère les fichiers .key et .csr
openssl req -config ./openssl.cnf -newkey rsa:4096 -out $hostname.csr -keyout
$hostname.key -nodes -subj "/C=FR/O=$organisation/CN=$hostname/"

#On peut controler les noms inclus avec la commande ci-dessous
#openssl req -text -noout -in $hostname.csr
```

Copiez et collez le contenu du script dans un fichier.sh.
Rendre ce script exécutable (chmod a+x script.sh)
Exécutez le script : ./script.sh

- La clé privée ***« nomservice.universite-paris-saclay.fr.key »*** et la demande de certification ***« nomservice.universite-paris-saclay.fr.csr »*** sont maintenant créés dans le répertoire **« certificats »**

- **Envoyer** la demande de certificat (CSR) au pôle « sécurité » de la Direction des Systèmes d'Information via la plateforme https://sos.di.u-psud.fr Catégorie **« Sécurité »** afin qu'il puisse générer un certificat.
  Attention, il faut envoyer la demande avec les lignes « Begin New Certificate Request » et « End New Certificate Request ».

- De plus, **indiquez** avec l'envoi du CSR, le service utilisé qui se rapproche le plus de la liste ci-dessous

Apache
Microsoft IIS 5 or 6
Microsoft IIS 7
Microsoft IIS 8
Microsoft Exchange Server 2007
Microsoft Exchange Server 2010
Microsoft Exchange Server 2013
Tomcat
Microsoft Lync Server 2010
Microsoft Lync Server 2013
Microsoft Office Communications Server 2007
Microsoft Live Communications Server 2005
IBM HTTP Server
Netscape iPlanet
Java Web Server (Javasoft / Sun)
Lotus Domino
Microsoft IIS 1.x to 4.x

Netscape Enterprise Server
Novell NetWare
Oracle
SunOne
Qmail
Juniper
F5 FirePass
F5 Big-IP
Cisco
WebStar
Bea Weblogic 7 and older
Zeus Web Server
Citrix (Other)
Barracuda
BEA Weblogic 8 & 9
cPanel
Lighttpd

nginx
Citrix Access Essentials
Microsoft Exchange Server 2003
Mac OS X Server
Citrix Access Gateway 4.x
Citrix Access Gateway 5.x and higher
Microsoft OCS R2
Microsoft Small Business Server 2008 & 2011
Novell iChain
Microsoft Forefront Unified Access Gateway
OTHER

- La Direction des Systèmes d'Information vous enverra ensuite un **fichier zip** qui contiendra le certificat (nomservice_universite-paris-saclay_fr.cer) ainsi qu'un fichier donnant des instructions pour l'installation si besoin.

Installer un certificat

- Pour l'installation du certificat sous Linux, rechercher sur Internet comment installer un certificat pour le service que vous désirez mettre en place.
  Vous pouvez également vous aider des instructions envoyées dans le fichier zip.

Récupérer la clé privée

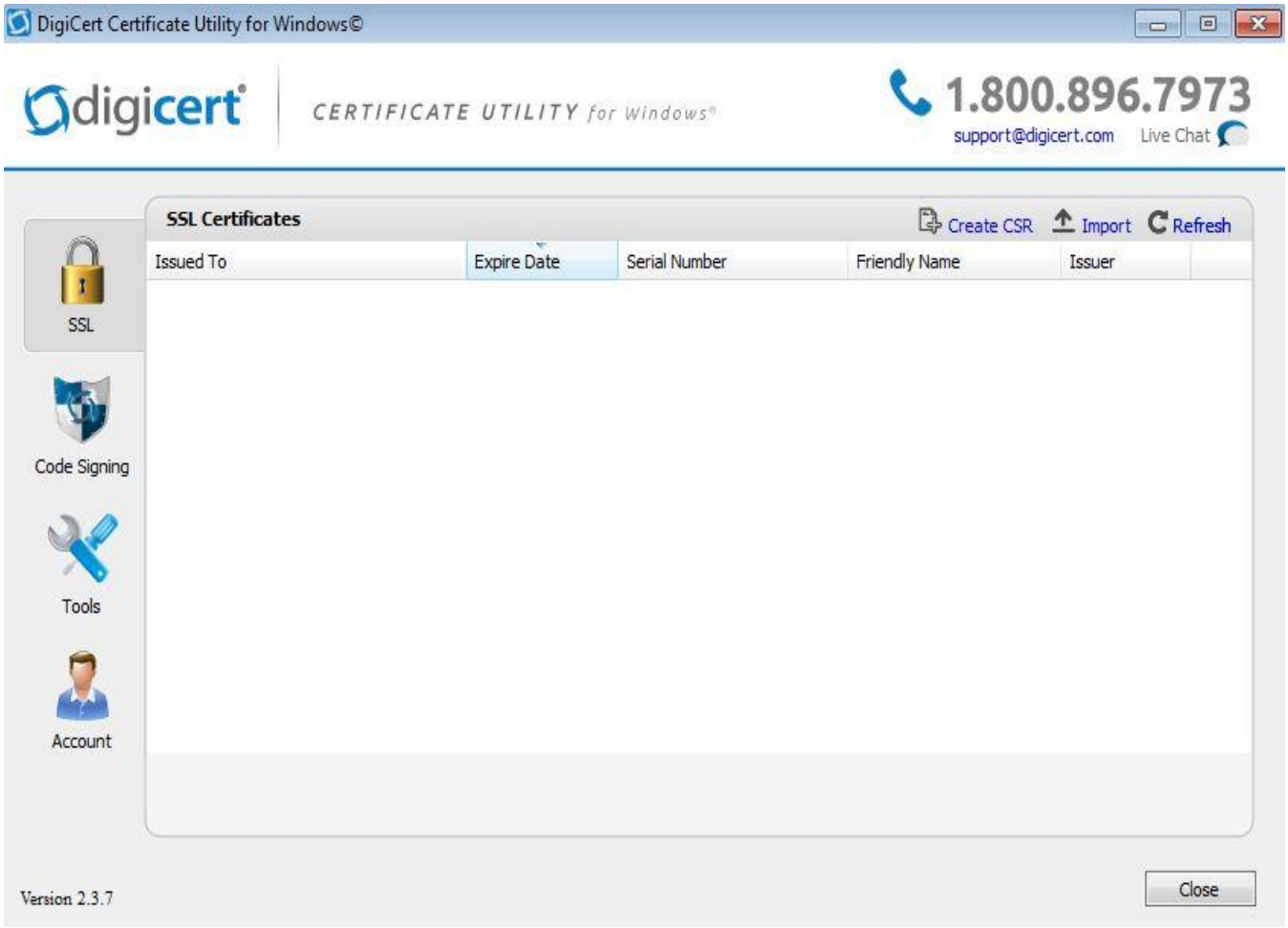
- Pour récupérer la clé privée, il suffit de récupérer le fichier ***«*** *nomservice****.universite-paris-saclay.fr.key »***, le crypter et le copier dans un endroit sécurisé.

Windows

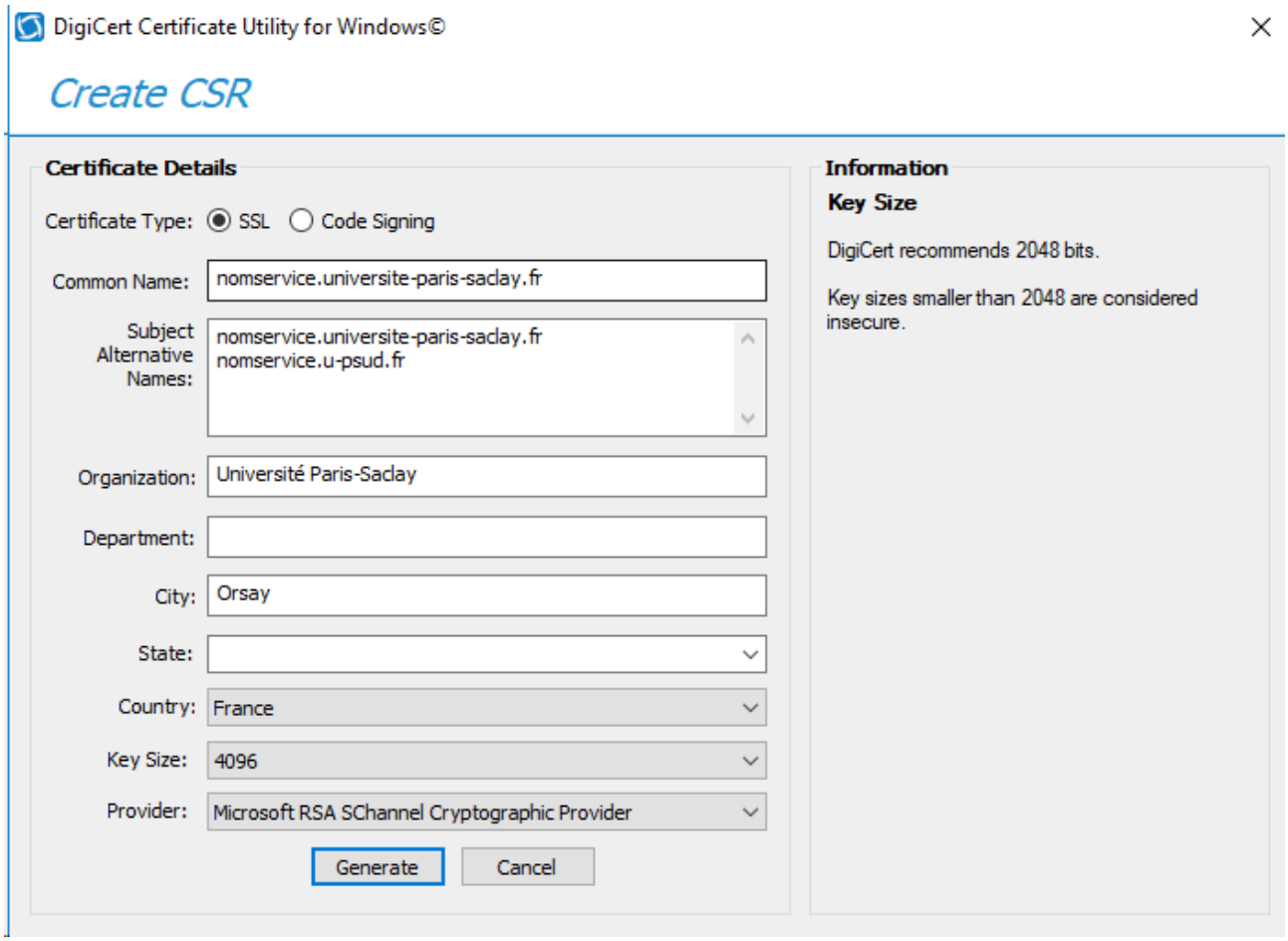
Demander un certificat

Pour créer cette demande il faut télécharger l'outil suivant via ce lien https://securite-informatique.dsi.universite-paris-saclay.fr/docs/download/DigiCertUtil.exe.
Une fois l'exécutable lancé sur le serveur, suivre les étapes suivantes :

- Cliquer sur **« SSL »** à gauche de la fenêtre et sur **« Create CSR »**



- Sélectionner **« SSL »** et renseigner les champs suivants



« Common Name » : Saisir le nom DNS du service (exemple : service d'annuaire Adonis https://adonis.universite-paris-saclay.fr, le nom sera adonis.universite-paris-saclay.fr)

« Subject Alternative » : Saisir les autres domaines si vous en avez

« Organization » : Saisir le nom de l'établissement **« Université Paris-Saclay »**

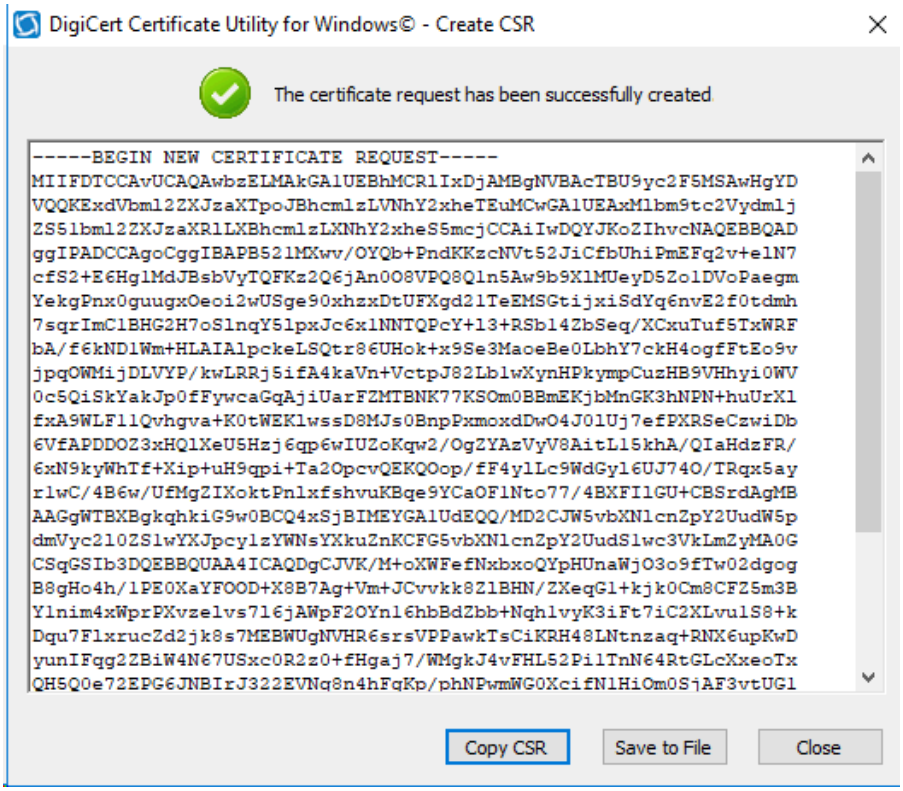
« City » : Entrer la ville où se situe l'établissement

« Country » : Entrer le pays

« Key Size » : Définir la taille de la clé à **4096**

« Provider » : Sélectionner l'algorithme de cryptage **« Microsoft RSA SChannel Crytographic Provider »**

- Cliquer sur **« Generate »,** la fenêtre ci-dessous apparait



- **Copiez** la demande de certificat (CSR) et l'**envoyer** au pôle « sécurité » de la Direction des Systèmes d'Information via la plateforme https://sos.di.u-psud.fr Catégorie **« Sécurité »** afin qu'il puisse générer un certificat.

  Attention, il faut envoyer la demande avec les lignes « Begin New Certificate Request » et « End New Certificate Request ».

- De plus, **indiquez** avec l'envoi du CSR, le service utilisé qui se rapproche le plus de la liste ci-dessous et précisez dans votre demande qu'il s'agit d'un certificat de type **multi-domaines**.

Apache
Microsoft IIS 5 or 6
Microsoft IIS 7
Microsoft IIS 8
Microsoft Exchange Server 2007
Microsoft Exchange Server 2010
Microsoft Exchange Server 2013
Tomcat
Microsoft Lync Server 2010
Microsoft Lync Server 2013
Microsoft Office Communications Server 2007
Microsoft Live Communications Server 2005
IBM HTTP Server
Netscape iPlanet
Java Web Server (Javasoft / Sun)
Lotus Domino
Microsoft IIS 1.x to 4.x

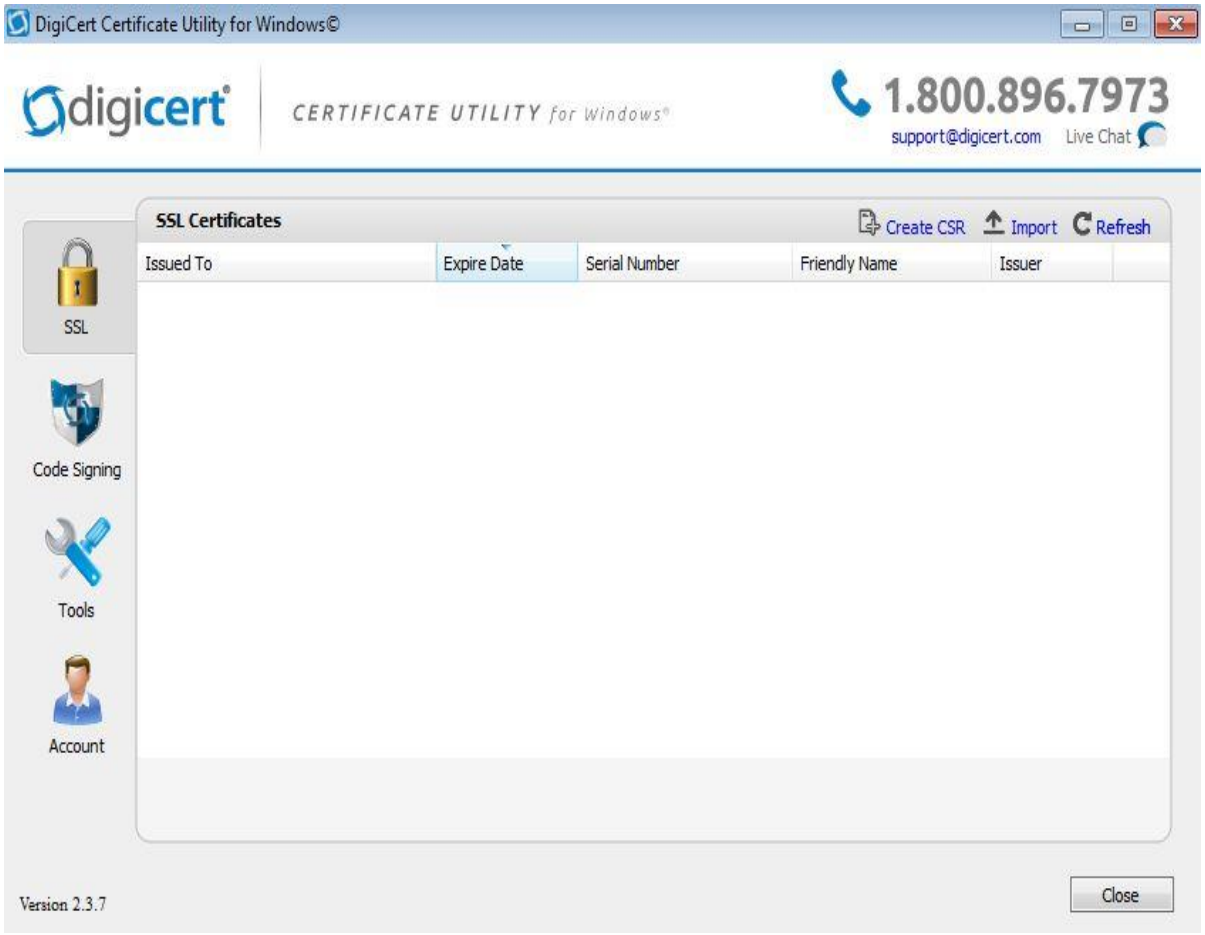
Netscape Enterprise Server
Novell NetWare
Oracle
SunOne
Qmail
Juniper
F5 FirePass
F5 Big-IP
Cisco
WebStar
Bea Weblogic 7 and older
Zeus Web Server
Citrix (Other)
Barracuda
BEA Weblogic 8 & 9
cPanel
Lighttpd

nginx
Citrix Access Essentials
Microsoft Exchange Server 2003
Mac OS X Server
Citrix Access Gateway 4.x
Citrix Access Gateway 5.x and higher
Microsoft OCS R2
Microsoft Small Business Server 2008 & 2011
Novell iChain
Microsoft Forefront Unified Access Gateway
OTHER

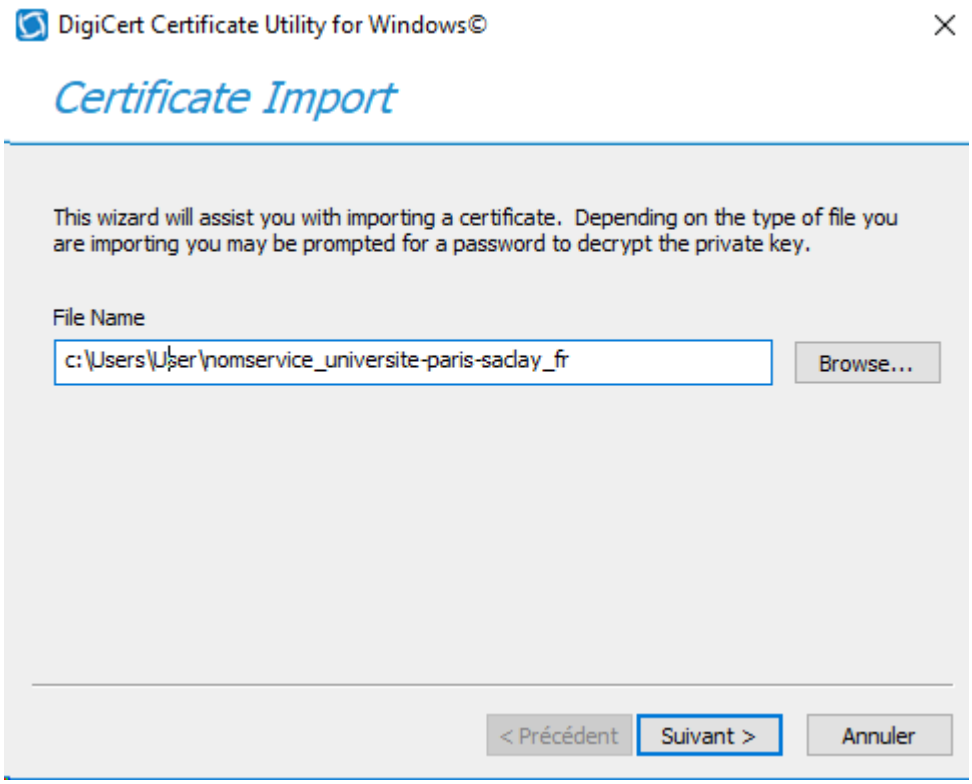
- La Direction des Systèmes d'Information vous enverra ensuite un **fichier zip** qui contiendra le certificat (nomservice_universite-paris-saclay_fr.cer) ainsi qu'un fichier donnant des instructions pour l'installation si besoin.

Installer un certificat

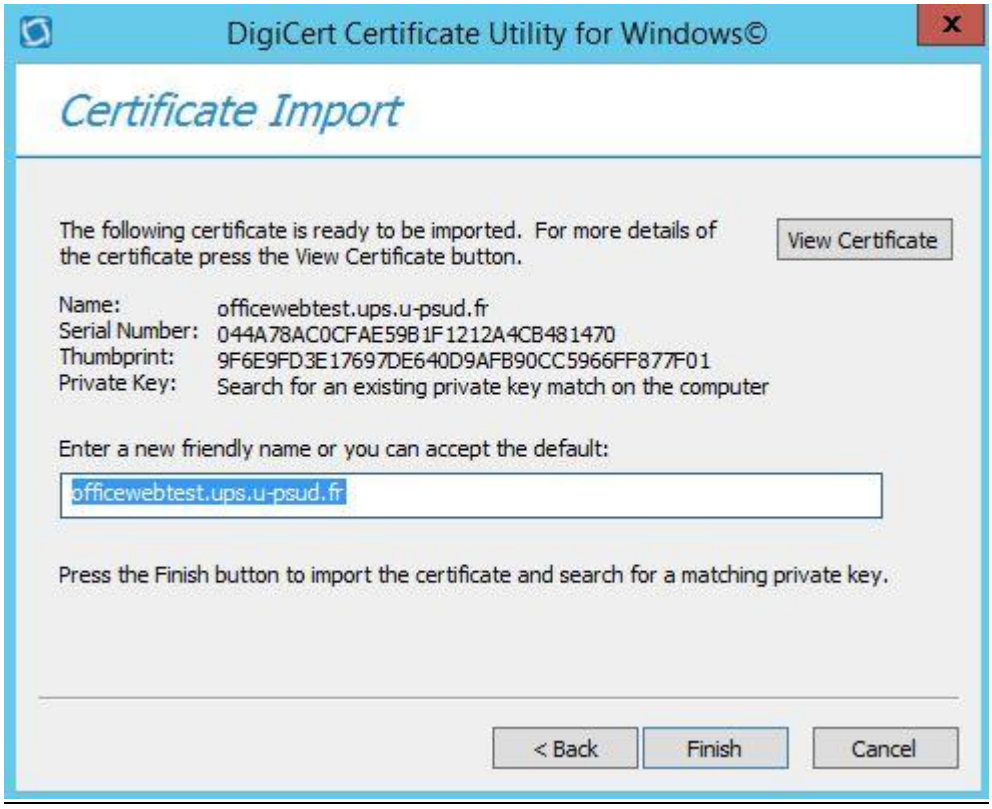
- Lorsque vous avez récupéré le certificat, vous pouvez l'installer sur le serveur à l'aide de l'outil **« DigiCertUtil.exe »**.
- Cliquez sur **« SSL »** à gauche de la fenêtre puis sur **« Import »** en haut à droite

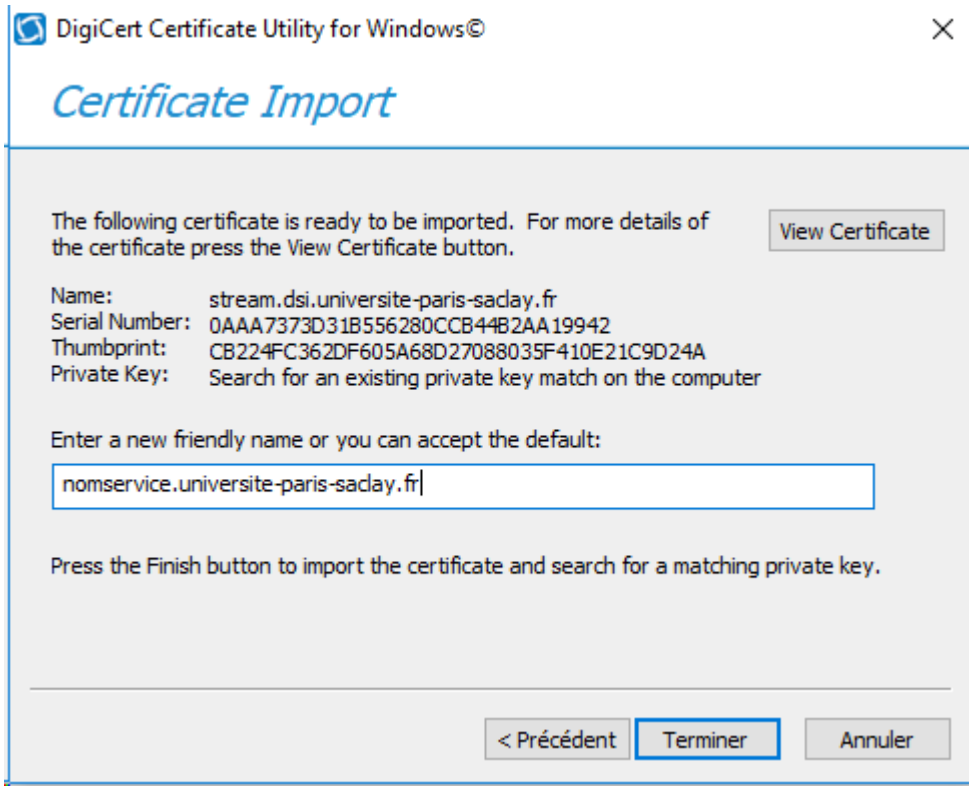


- Cliquez sur **« Browse »** pour allez chercher le certificat et cliquez sur **« Suivant »** comme ci-dessous



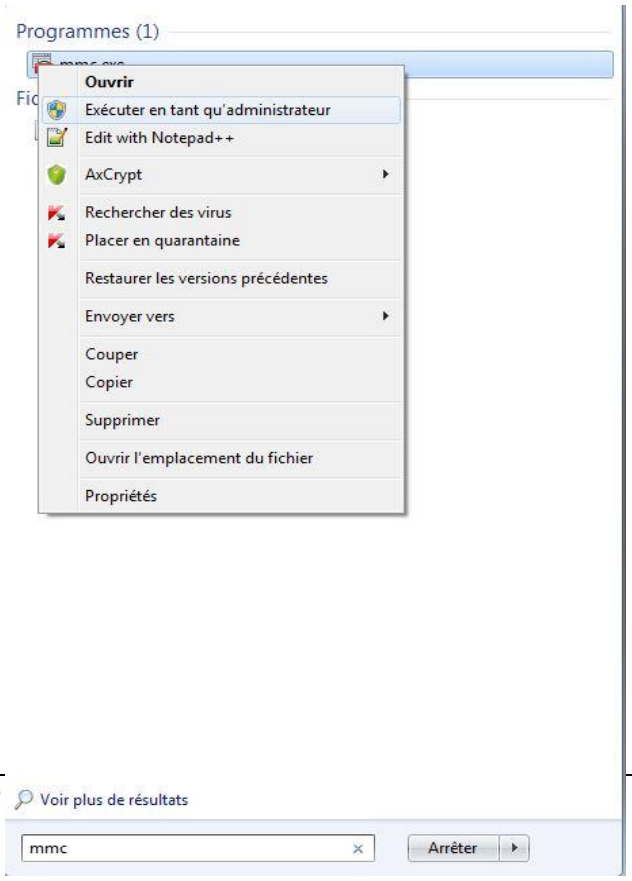
- Ensuite entrer la valeur de **« Name : »** dans le champ **« Enter a new friendly name.. »** si ce champ est vide puis cliquer sur **« Terminer »**



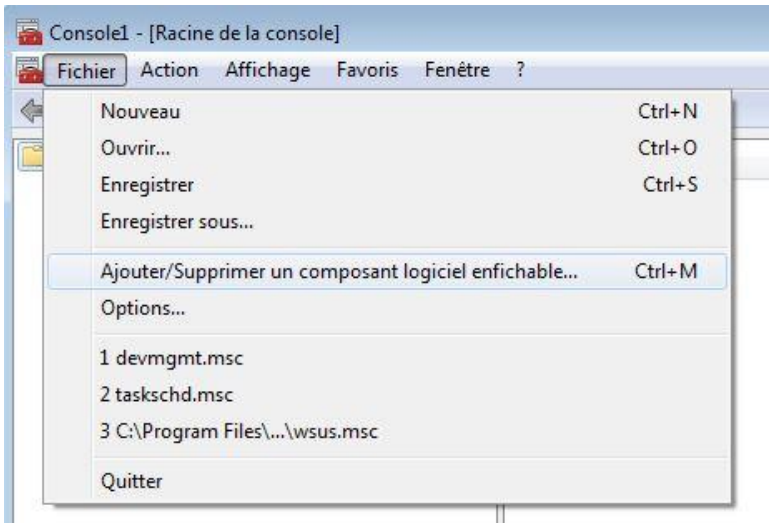


Récupérer la clé privée

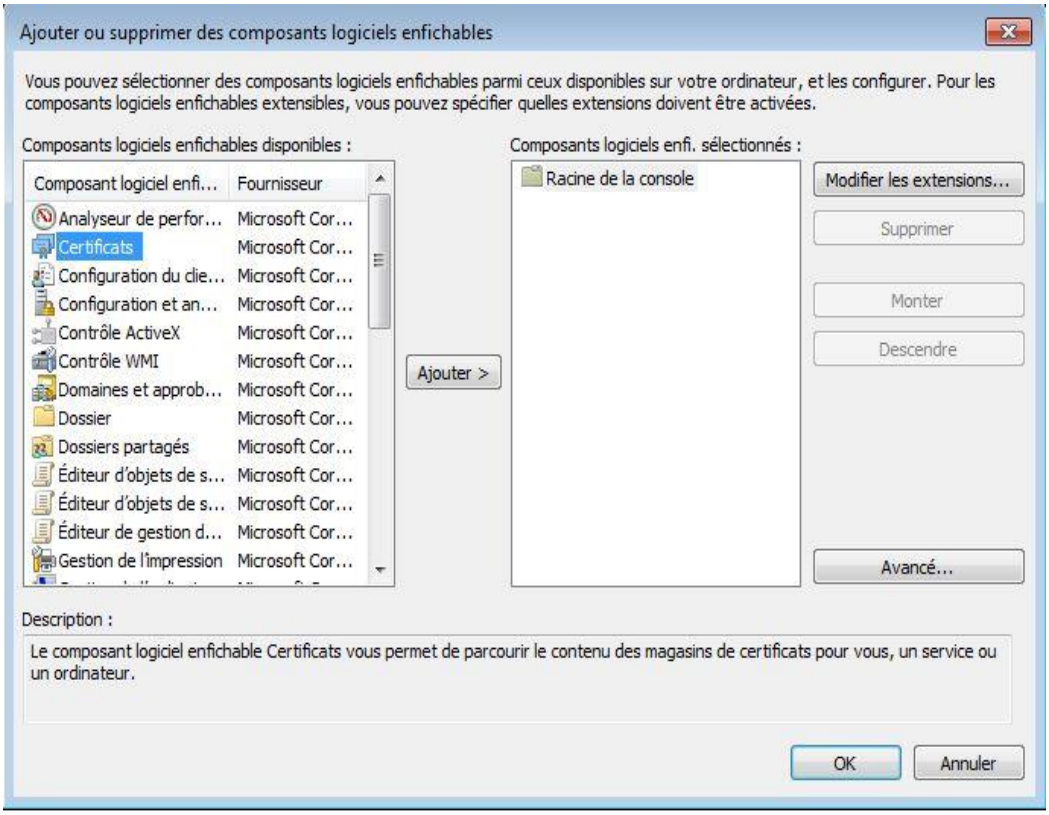
- Cliquer sur **« Démarrer »** et lancer la commande **« mmc.msc »** dans la zone de recherche. Il faut exécuter « mmc.msc » en **mode administrateur**.



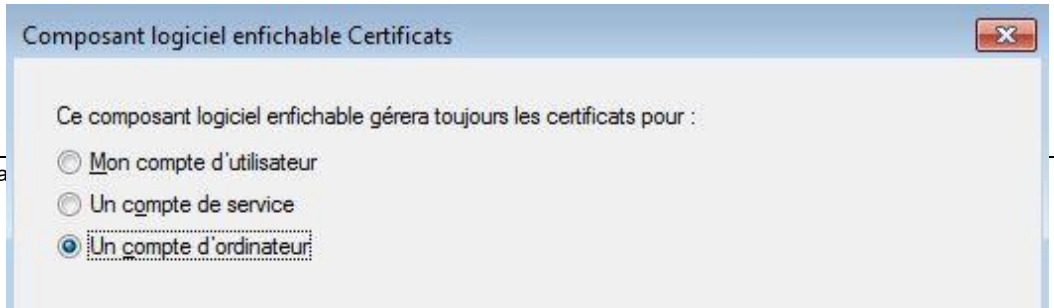
- Ajouter un composant logiciel enfichable



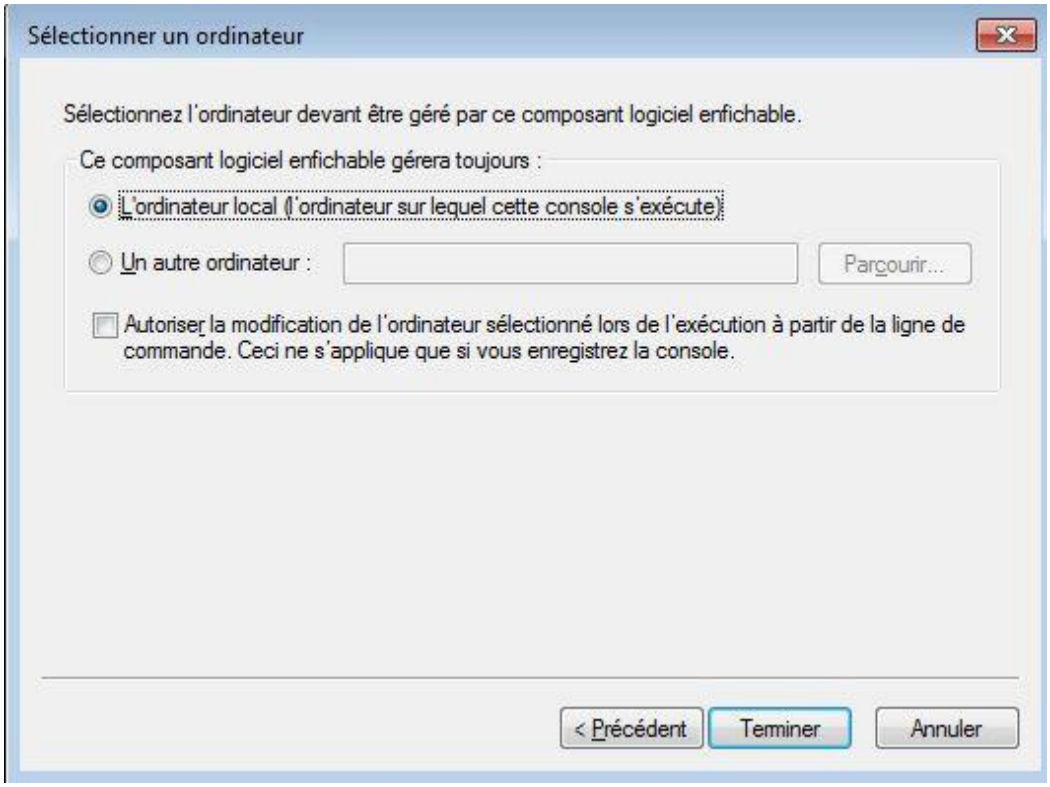
- Sélectionner **« Certificats »** et cliquer sur **« Ajouter »**



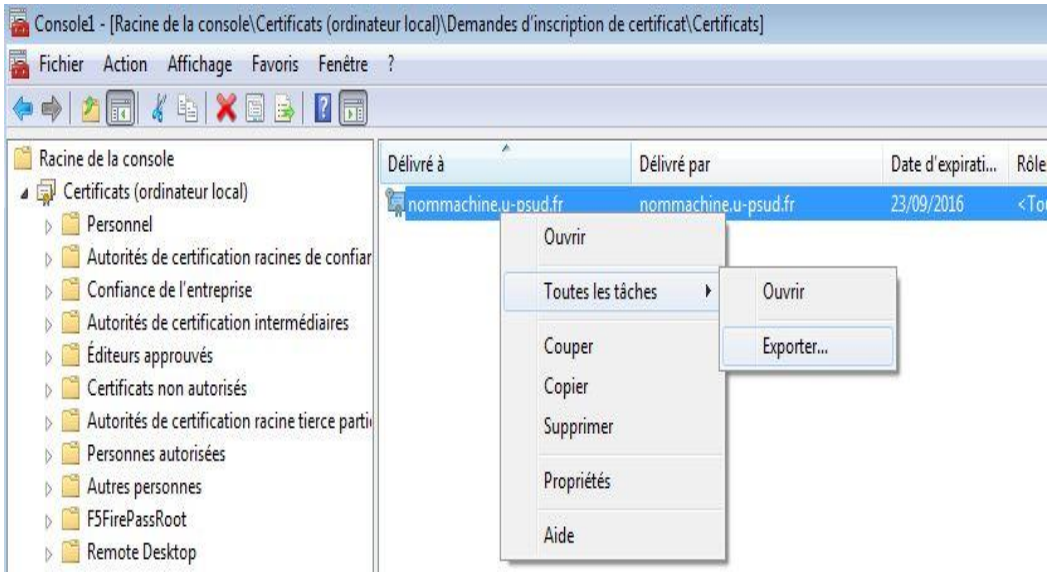
- Sélectionner **« Compte ordinateur »**



- Sélectionner ensuite **« ordinateur local »**

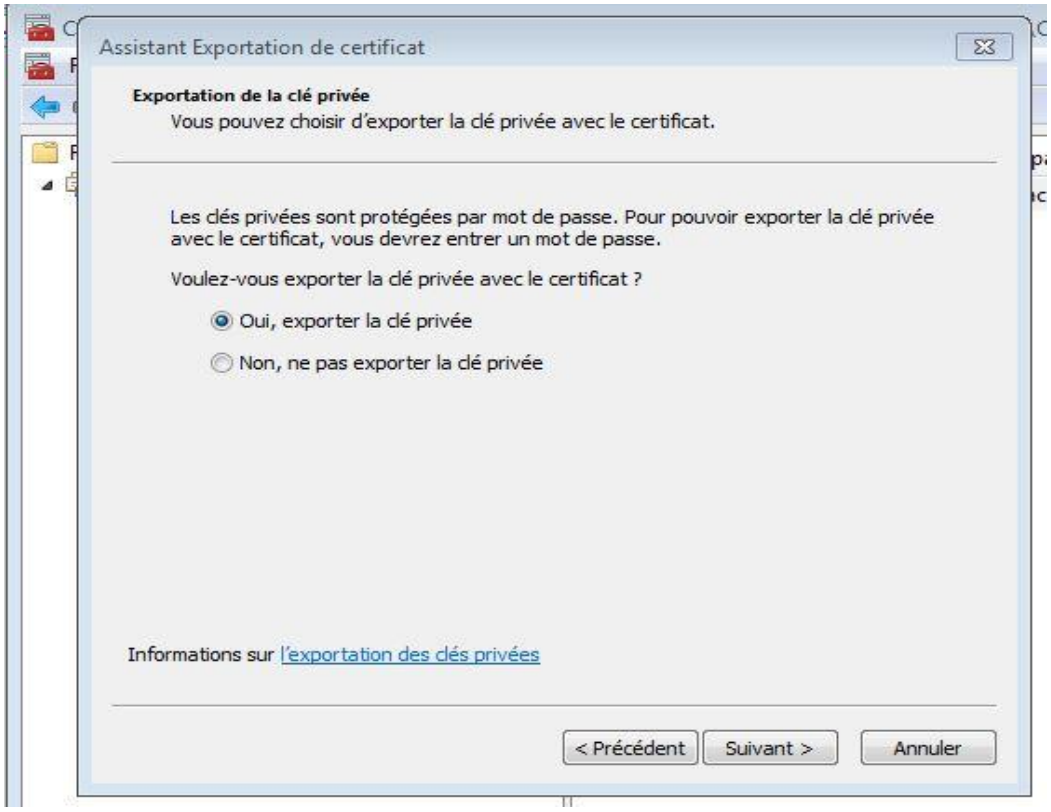


- Chercher votre certificat installé et cliquer sur **« exporter »**

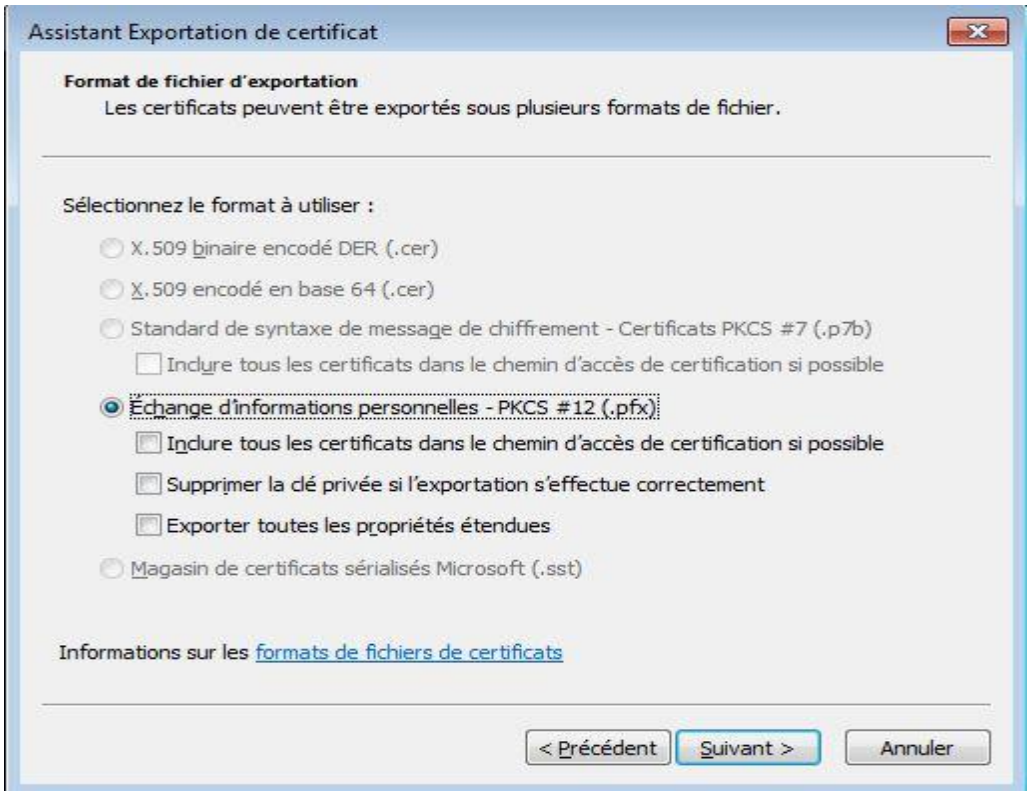


- La fenêtre **« Assistant d'exportation de certificat »** s'ouvre, cliquer sur **« suivant »**.

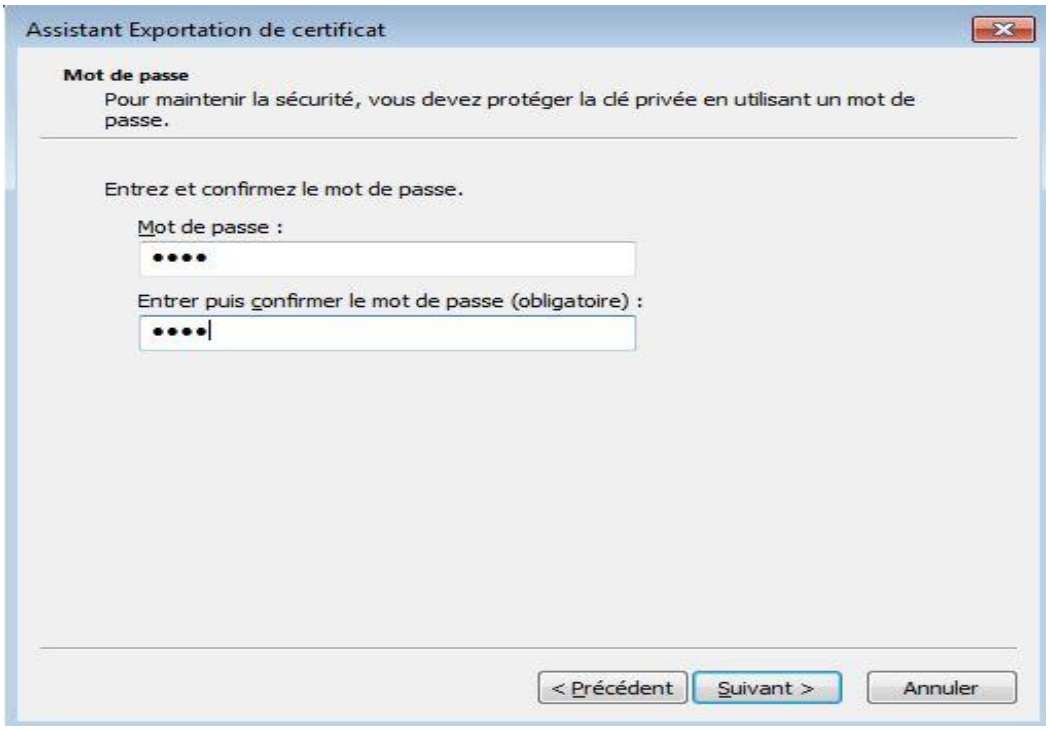
- Si la clé privée est exportable, sélectionner **« oui, exporter la clé privée »**



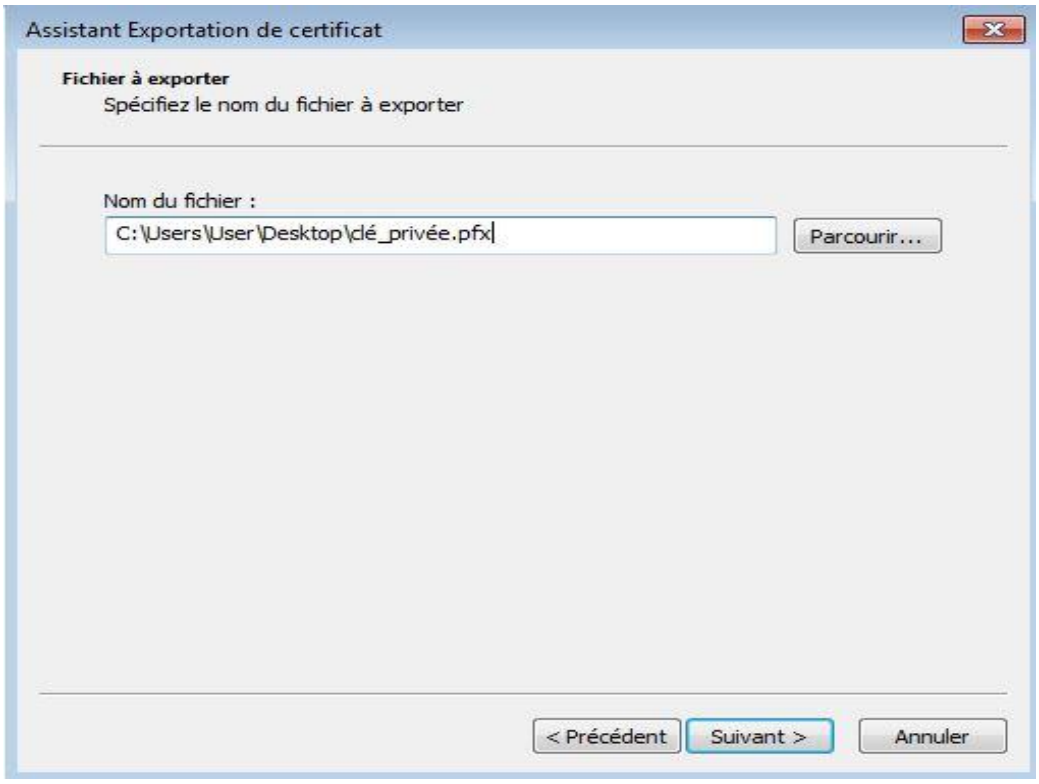
- Sélectionner **« Echange d'informations personnelles »**



- Définir un **« mot de passe »** pour protéger la clé privée



- Cliquer sur **« Parcourir »** afin de sauvegarder cette clé privée



- Puis cliquer sur **« Terminer »**