



---

# Annexe – WebService consultation - certificats



## Table des matières

<b>1</b>	<b>But du document</b>	<b>3</b>
<b>2</b>	<b>Création du fichier .pks</b>	<b>3</b>
<b>3</b>	<b>Paramètre VM à ajouter</b>	<b>8</b>



# 1 But du document

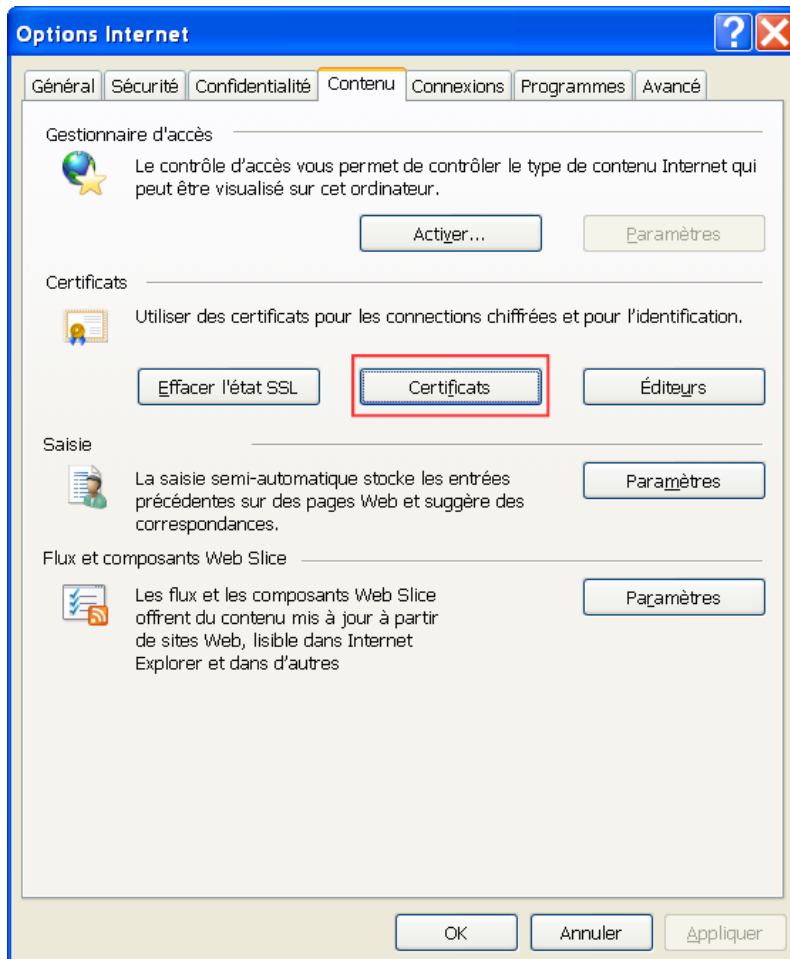
Fournir des informations complémentaires sur la configuration du client webservice RAFam Consultation, dans le cadre d'appels sécurisés (SSL).

Cette configuration est optionnelle, et uniquement nécessaire sur certains environnements, dès lors que des erreurs liées à la sécurité surviennent lors des appels SSL au webservice RAFam consultation.

# 2 Création du fichier .pks

Le fichier avec extension pks, permet de fournir des informations liées à l'utilisation de certificats à la machine virtuelle Java. Voici la procédure complète pour le créer :

Exclusivement depuis internet explorer, aller dans les options internet, onglet Contenu :



Importer le certificat (.p12) qui vous a été fourni dans IE :



**Certificats**

Rôle prévu : <Tout>

Personnel | Autres personnes | Autorités intermédiaires | Autorités principales de confiance

Délivré à	Délivré par	Date d'...	Nom convivial
-----------	-------------	------------	---------------

Importer... Exporter... Supprimer Avancé...

Détails de certificat

Affichage

Fermer

Saisir le mot de passe du certificat et marquer la clé comme exportable :

**Assistant Importation de certificat**

**Mot de passe**

Pour maintenir la sécurité, la clé privée a été protégée avec un mot de passe.

Entrez le mot de passe de la clé privée.

Mot de passe :

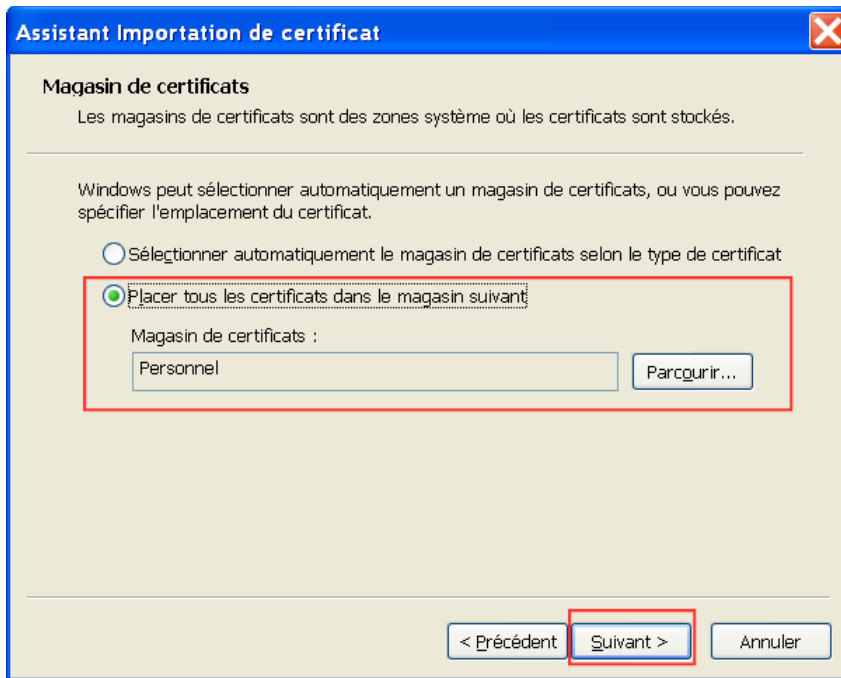
Activer la protection renforcée de clés privées. La clé privée vous sera demandée chaque fois qu'elle est utilisée par une application si vous activez cette option.

Marquer cette clé comme exportable. Cela vous permettra de sauvegarder et de transporter vos clés ultérieurement.

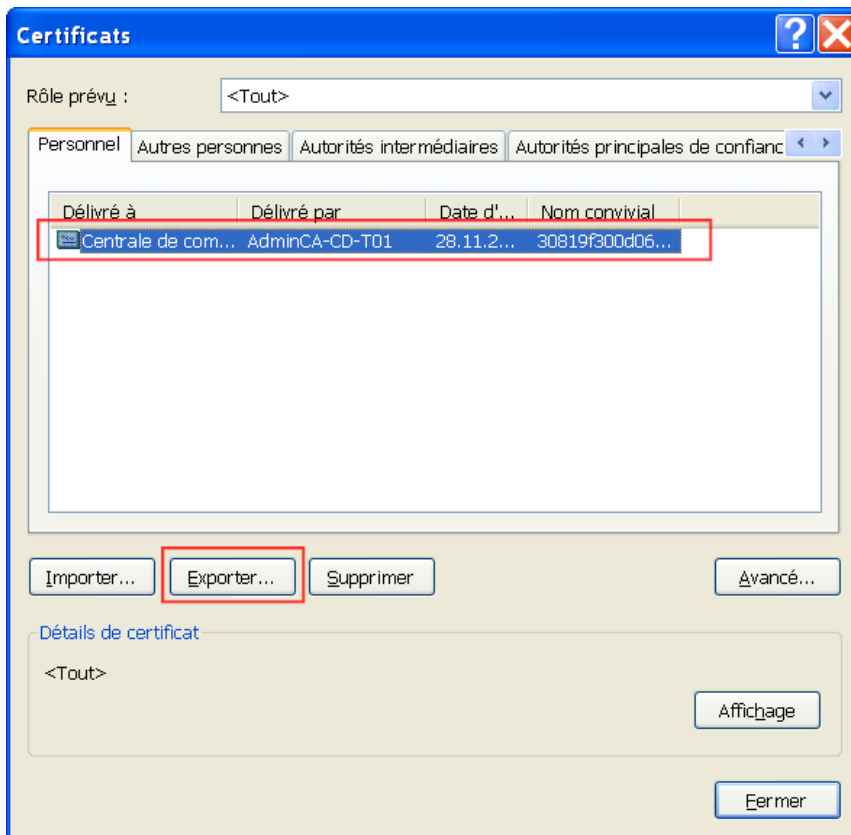
< Précédent Suivant > Annuler



Placer le certificat dans le magasin « Personnel »



Terminer l'importation, sélectionner le certificat que vous venez d'importer puis exportez-le:



Ne pas exporter la clé privée :



**Assistant Exportation de certificat**

**Exportation de la clé privée**  
Vous pouvez choisir d'exporter la clé privée avec le certificat.

Les clés privées sont protégées par mot de passe. Pour pouvoir exporter la clé privée avec le certificat, vous devez entrer son mot de passe dans une des pages suivantes.

Voulez-vous exporter la clé privée avec le certificat ?

Oui, exporter la clé privée

Non, ne pas exporter la clé privée

< Précédent   Suivant >   Annuler

Sélectionnez le format à utiliser (à base 64 X.509) :

**Assistant Exportation de certificat**

**Format de fichier d'exportation**  
Les certificats peuvent être exportés sous plusieurs formats de fichier.

Sélectionnez le format à utiliser :

Binaire codé DER X.509 (.cer)

Codé à base 64 X.509 (.cer)

Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.p7b)

Inclure tous les certificats dans le chemin d'accès de certification si possible

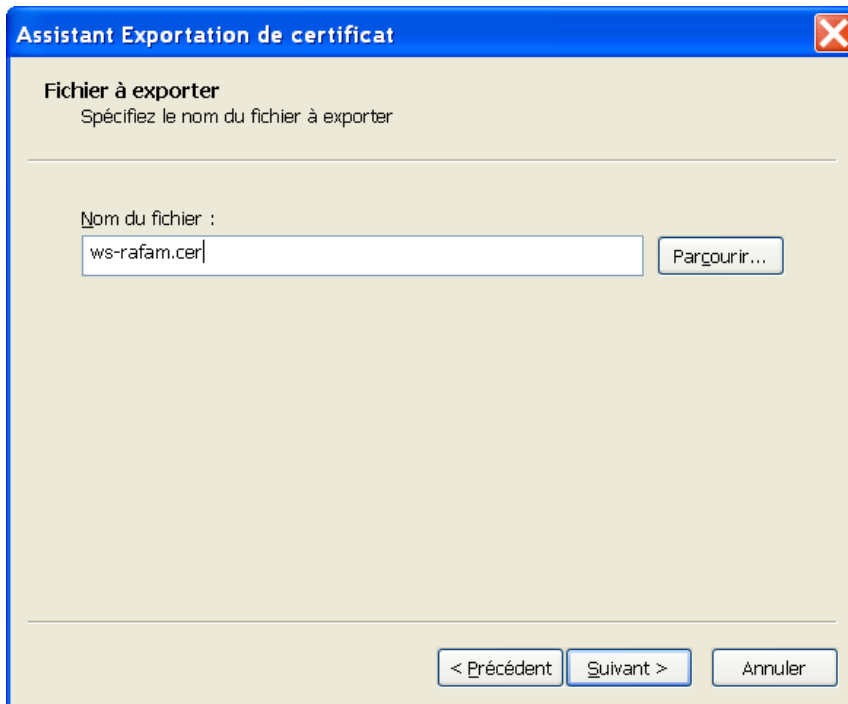
Échange d'informations personnelles - PKCS #12 (.pfx)

Inclure tous les certificats dans le chemin d'accès de certification si possible

Activer la protection renforcée (nécessite IE 5.0, NT 4.0 SP4 ou supérieur)

Supprimer la clé privée si l'exportation s'est terminée correctement

< Précédent   Suivant >   Annuler



Convertir le certificat que vous venez d'exporter au format pks, en lançant la commande suivante depuis le répertoire bin de votre JAVA\_HOME :

```
keytool -importcert -file {Chemin utilisé pour exporter le certificat}/ws-rafam.cer -keystore {Chemin des ressources de votre projet client WS}/ws-rafam.keystore.jks -storepass wsrafamprodcert -noprompt
```



### 3 Paramètre VM à ajouter

Pour finaliser la configuration, il faut ajouter le paramètre VM suivant à votre client WS RAFam dans votre Eclipse :

