



**ACTES - Dématérialisation du contrôle de légalité**

**Certificats & navigateurs**



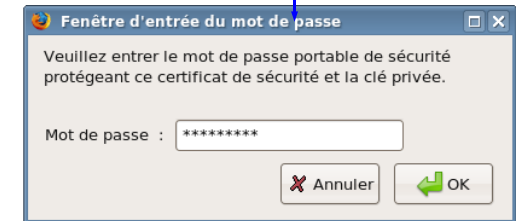
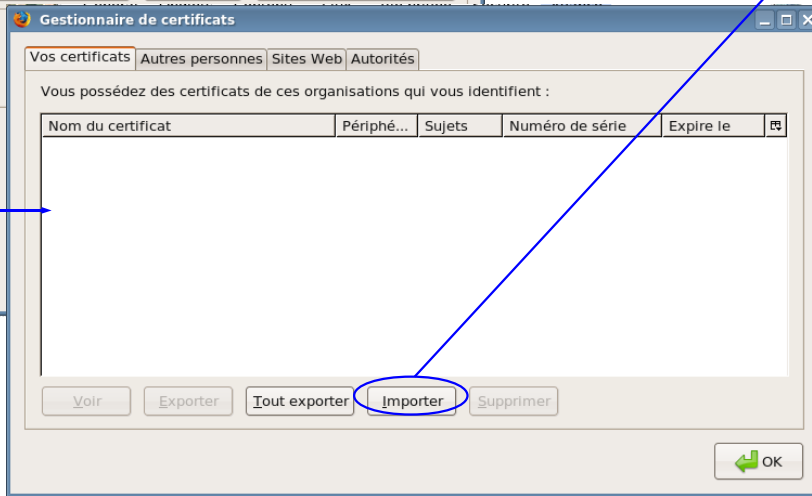
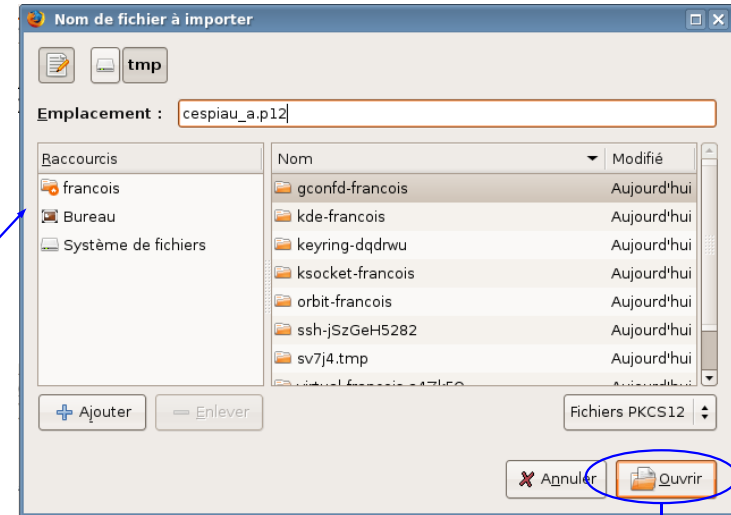
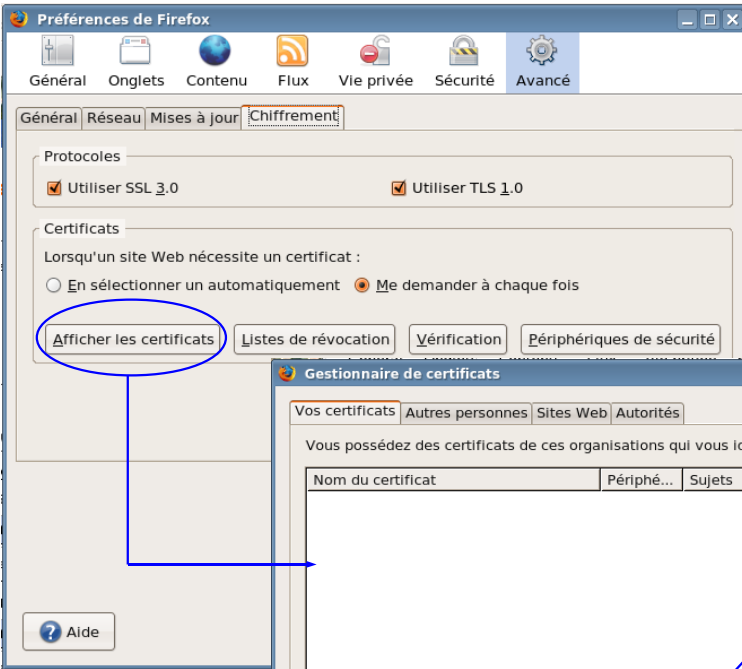


## Gestion des certificats / navigateurs

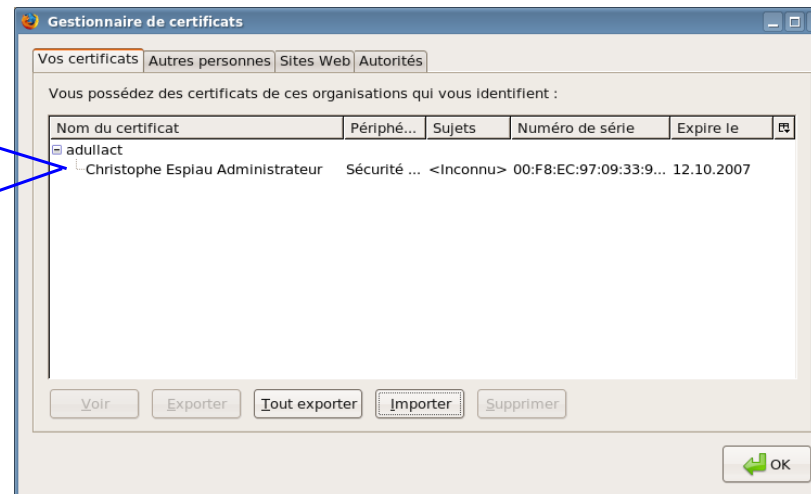
---



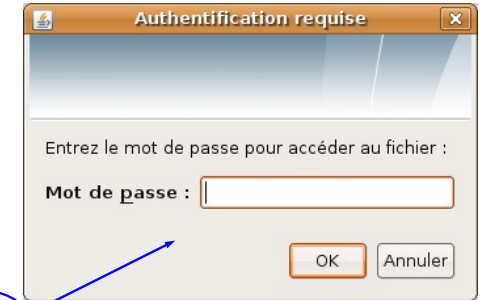
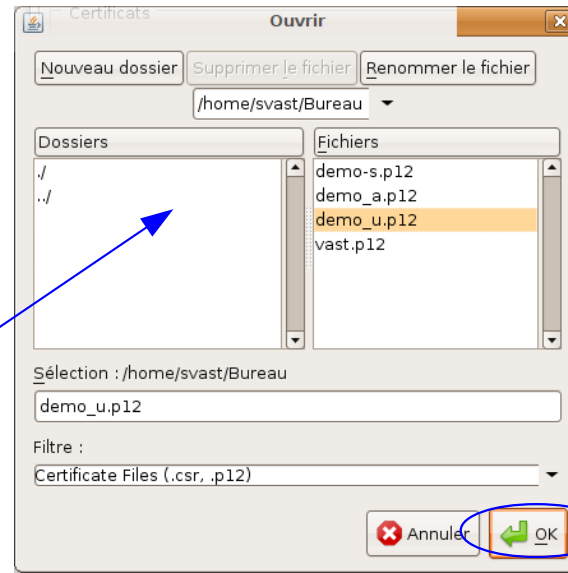
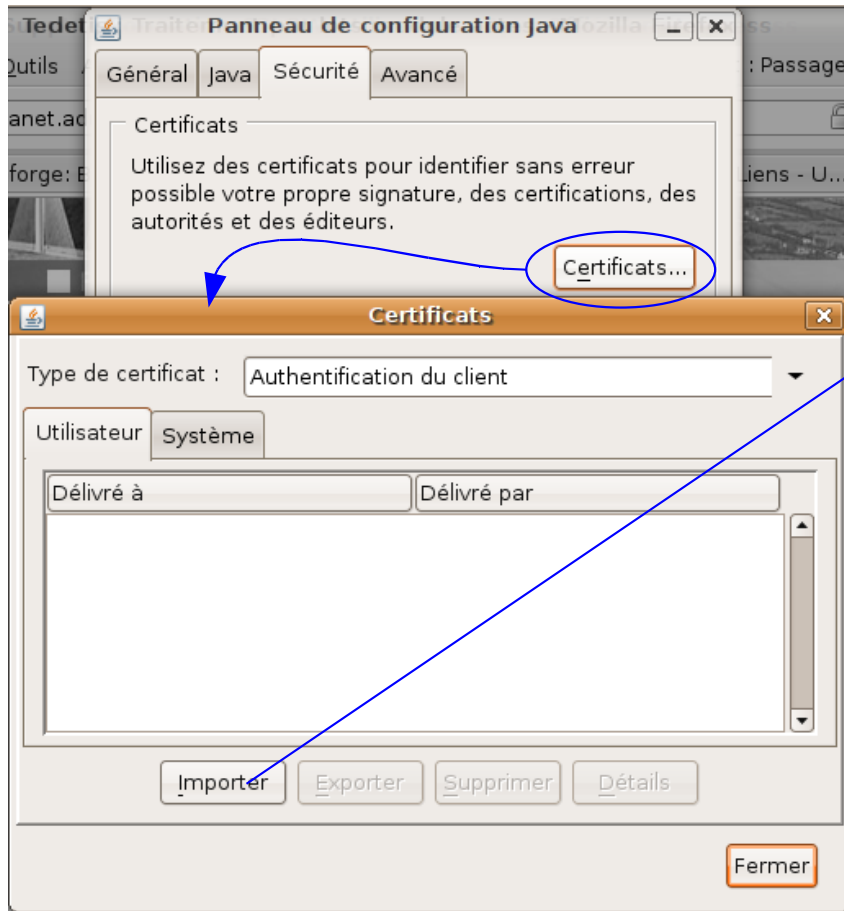
# Installation d'un certificat \*.p12 dans Firefox



Résultat



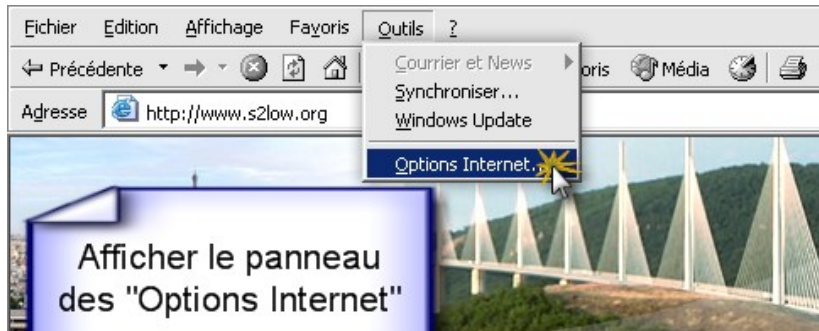
# Installation d'un certificat \*.p12 dans JAVA



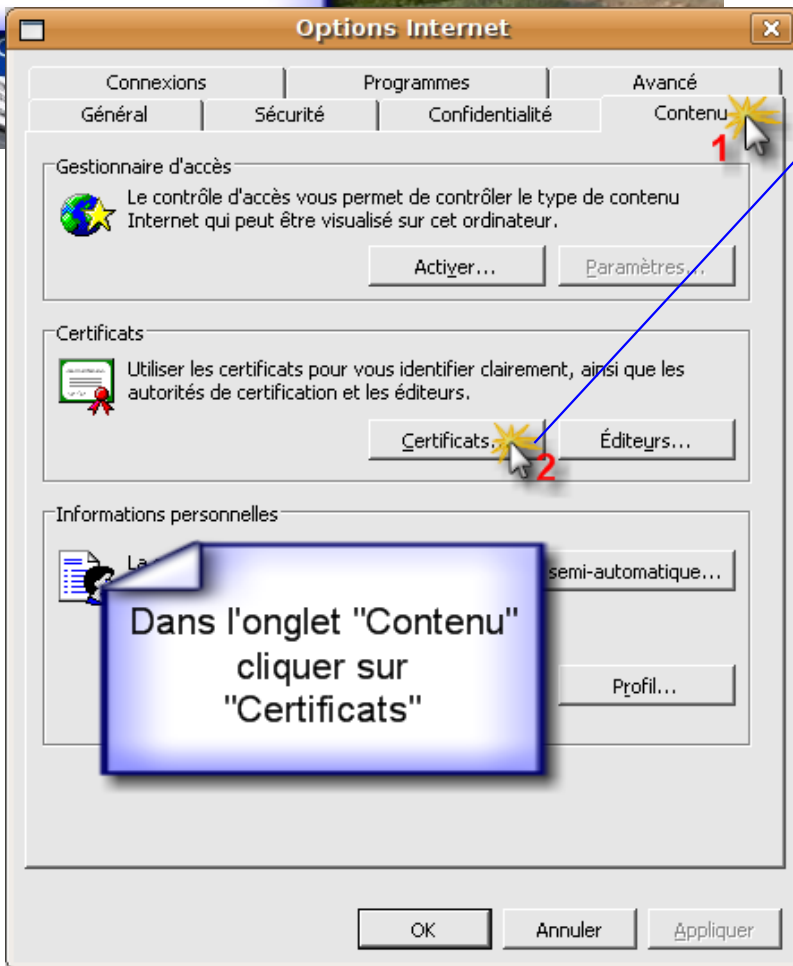
Résultat

**NB:** Cette opération est requise pour la gestion par lots sous Firefox

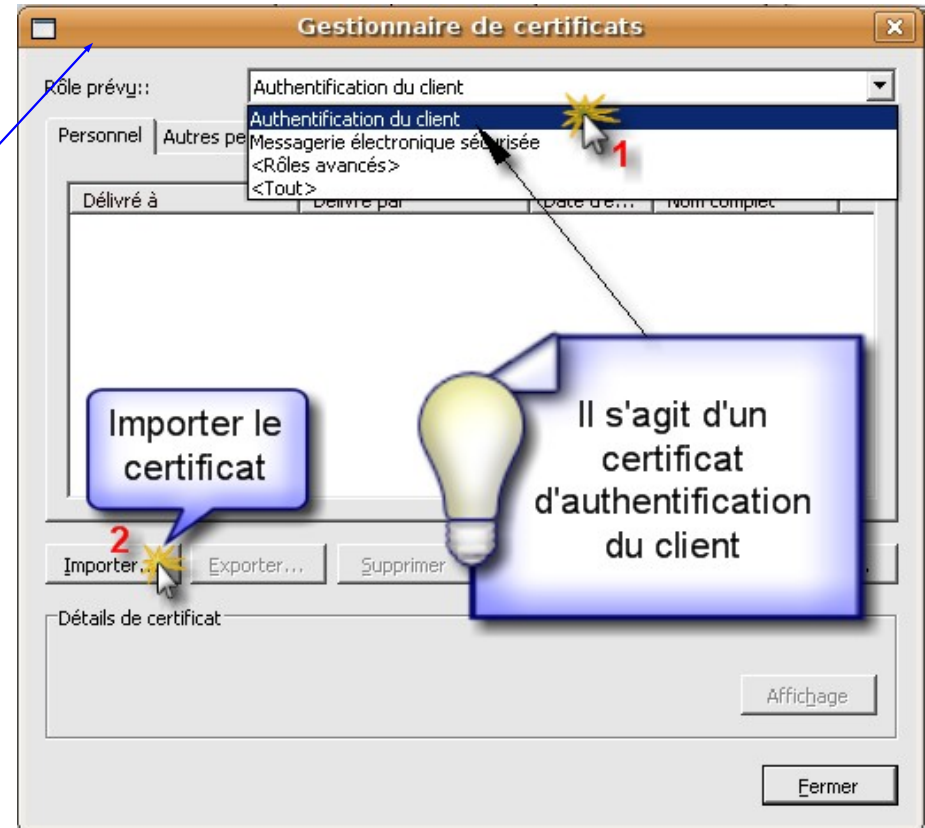
# Installation d'un certificat \*.p12 dans Internet Explorer 6 (1/3)



Afficher le panneau des "Options Internet"



Dans l'onglet "Contenu" cliquer sur "Certificats"

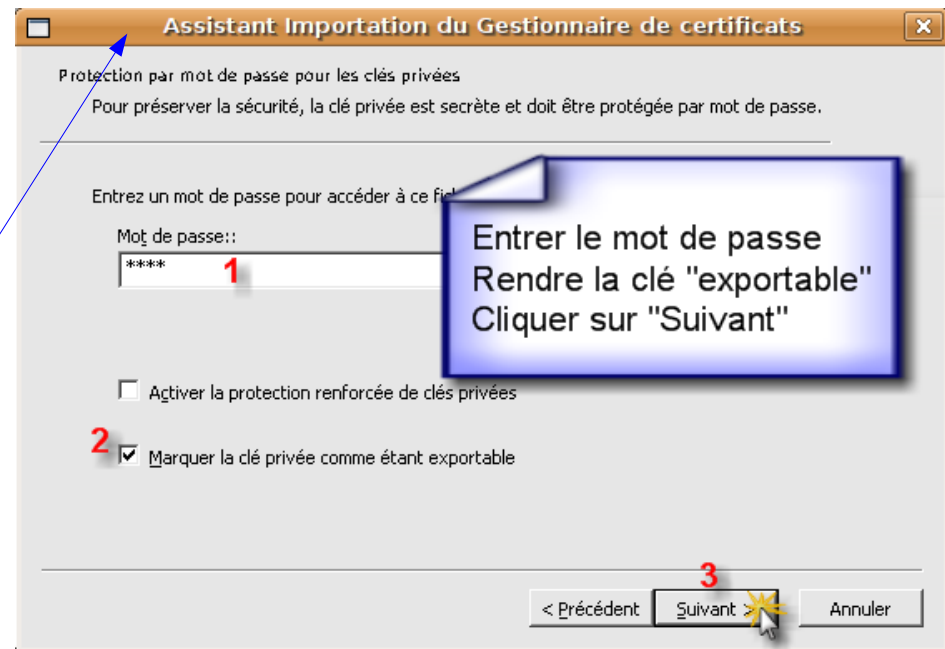
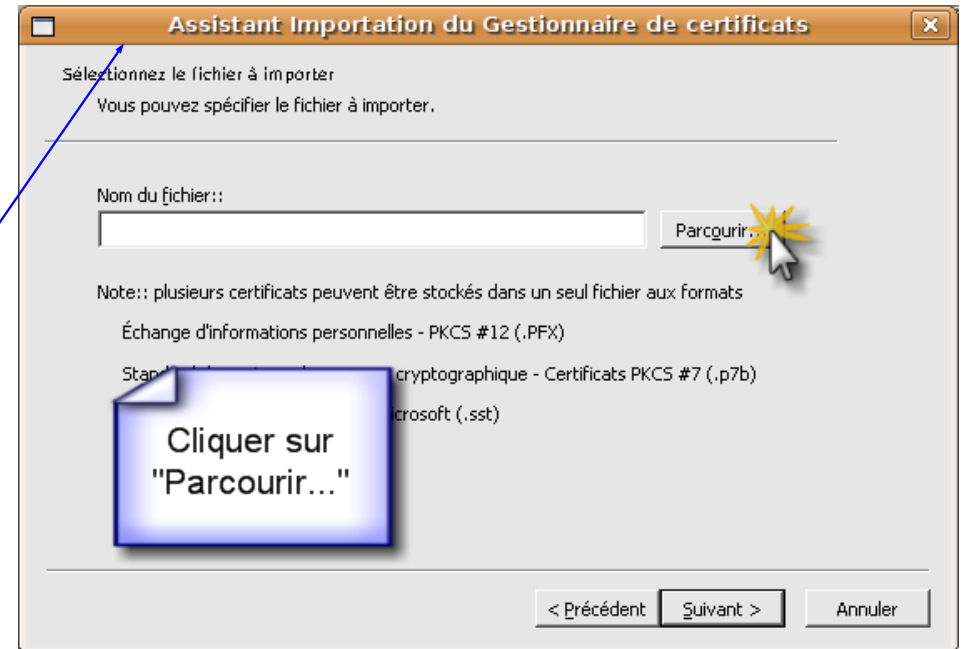
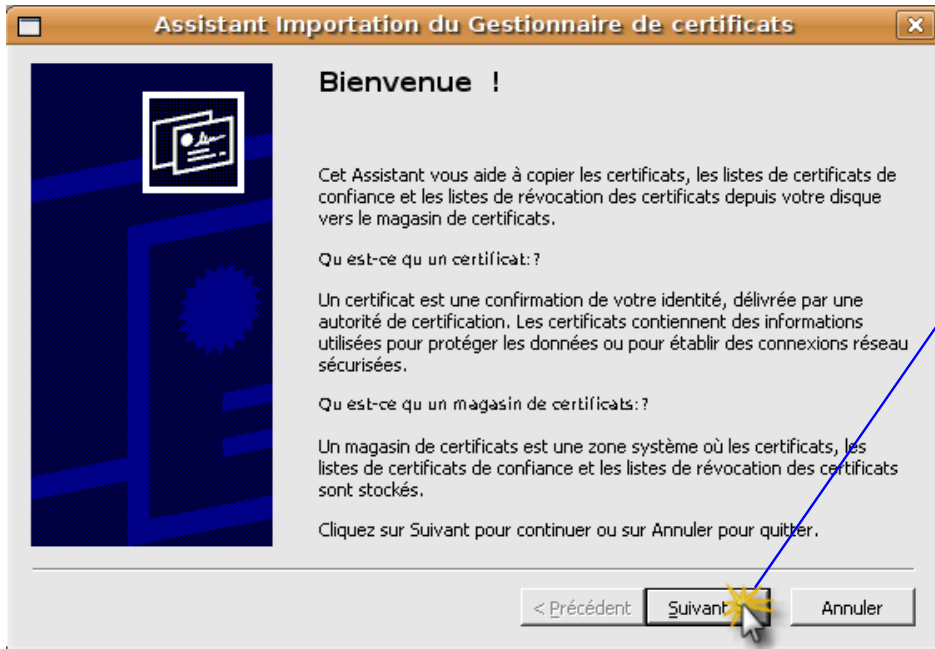


Importer le certificat

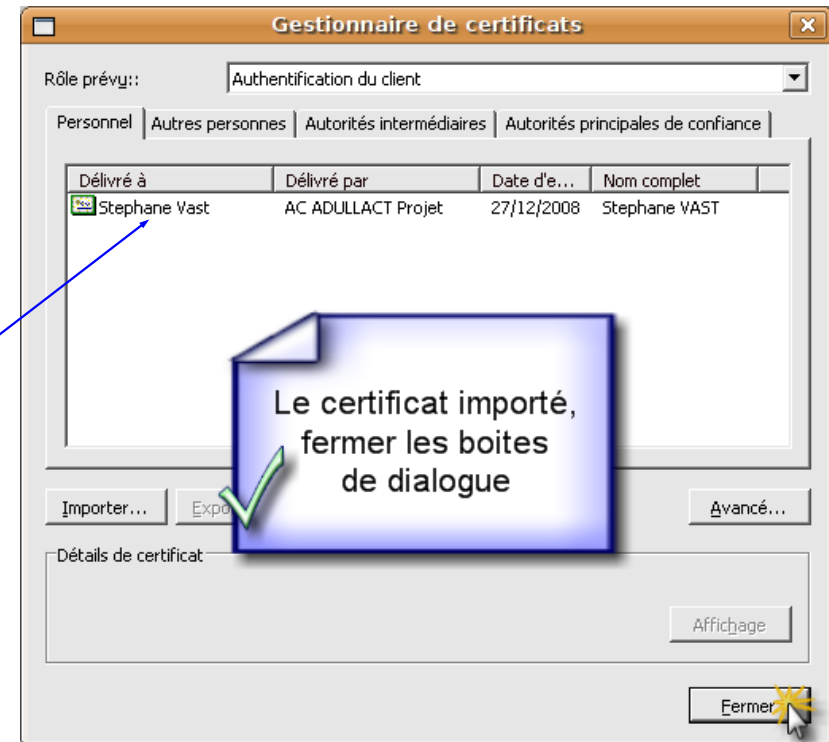
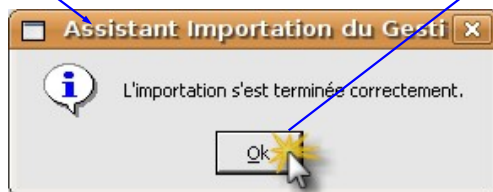
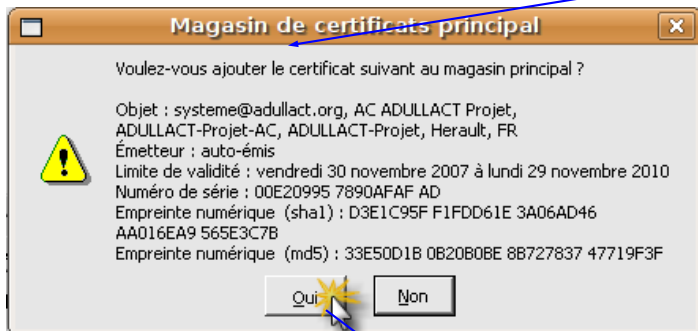
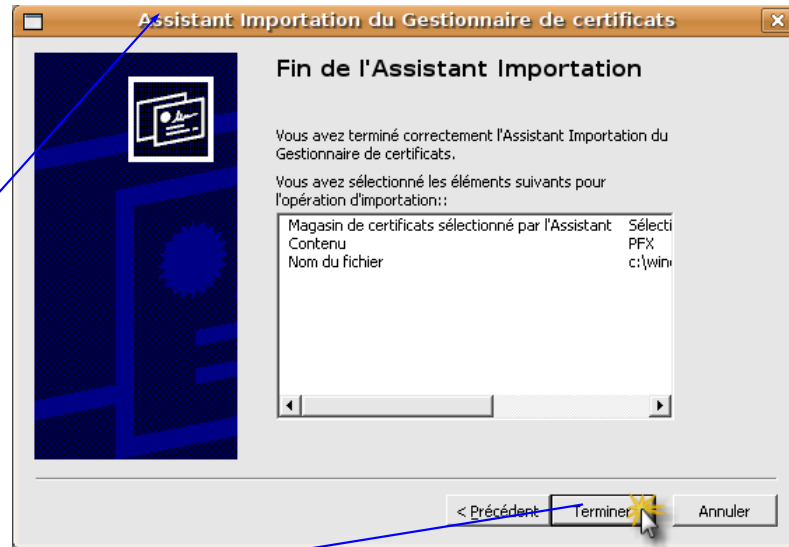
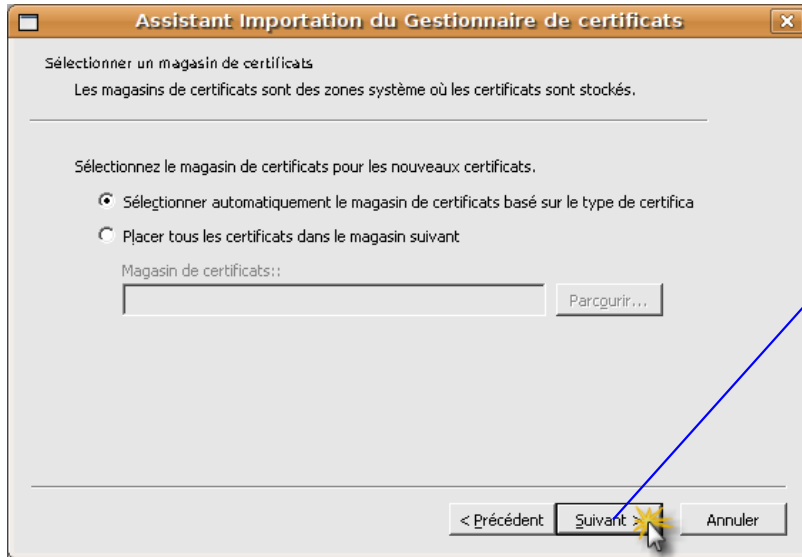
Il s'agit d'un certificat d'authentification du client



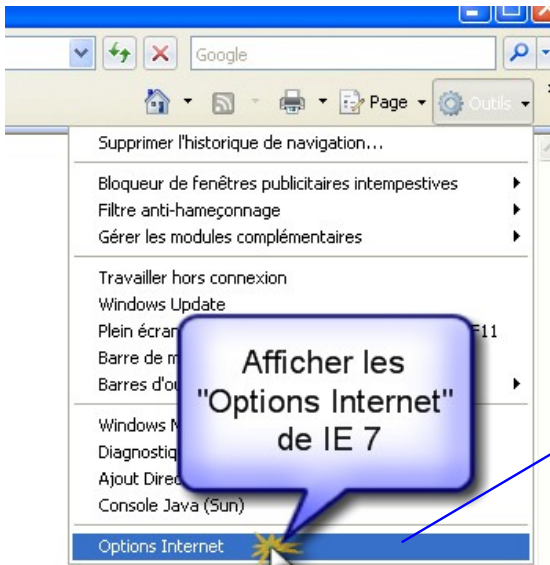
# Installation d'un certificat \*.p12 dans Internet Explorer 6 (2/3)



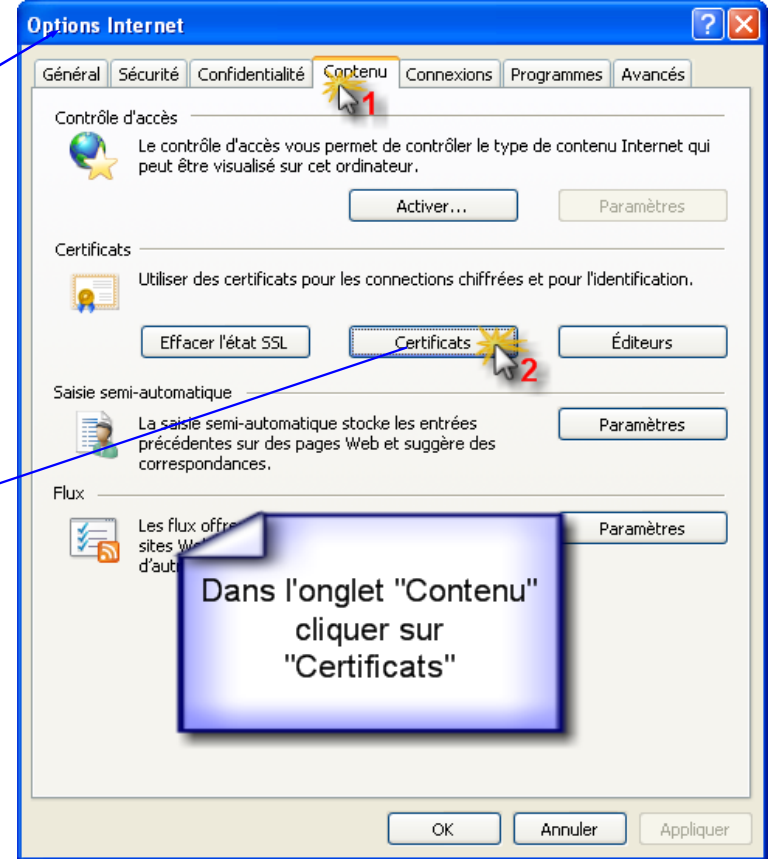
# Installation d'un certificat \*.p12 dans Internet Explorer 6 (3/3)



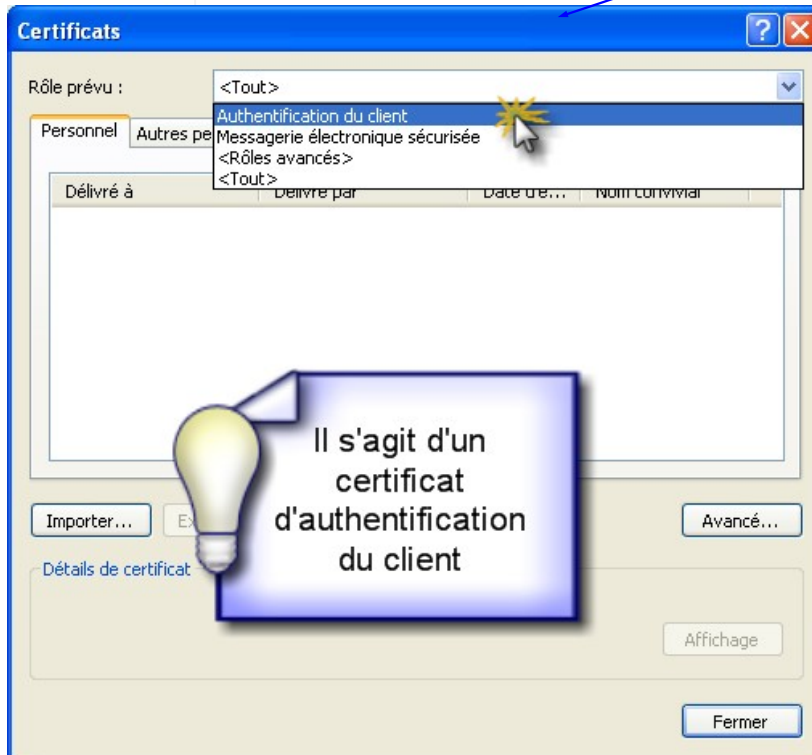
# Installation d'un certificat \*.p12 dans Internet Explorer 7 (1/3)



Afficher les "Options Internet" de IE 7



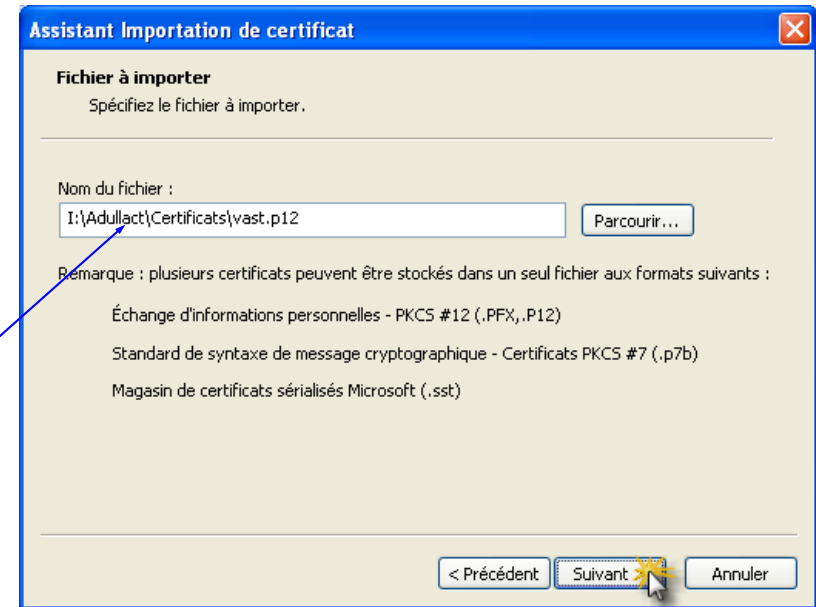
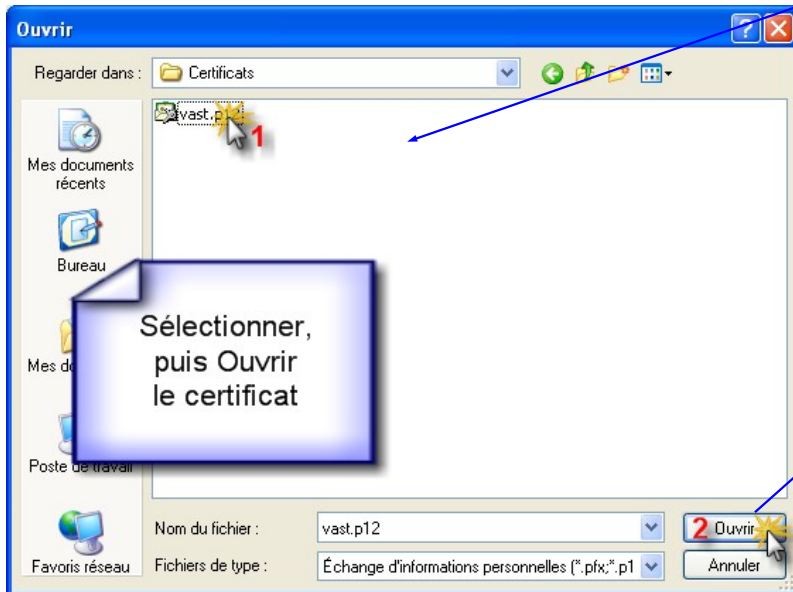
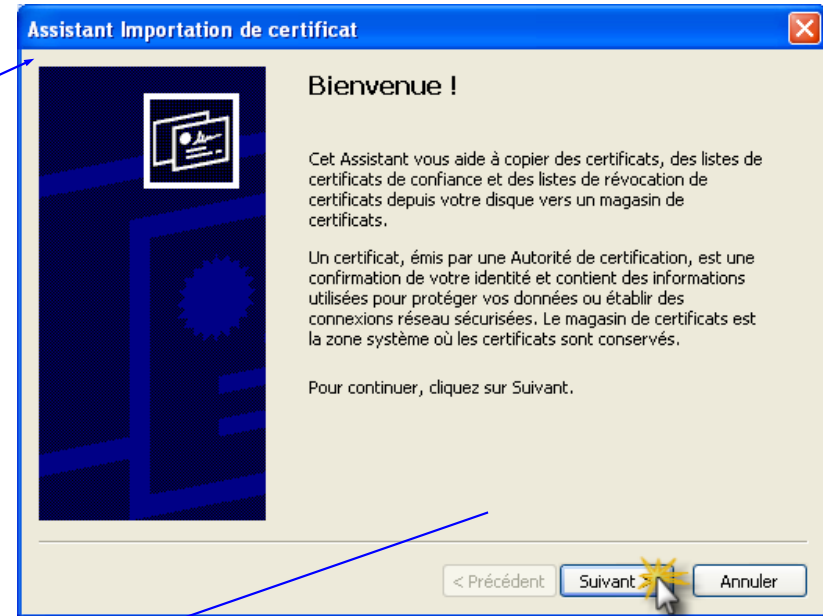
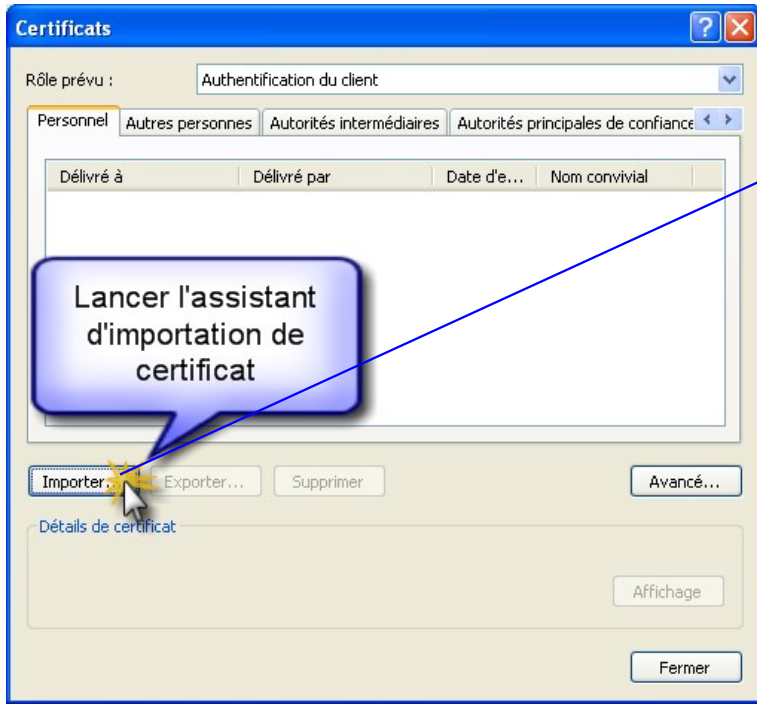
Dans l'onglet "Contenu" cliquer sur "Certificats"



Il s'agit d'un certificat d'authentification du client



# Installation d'un certificat \*.p12 dans Internet Explorer 7 (2/3)



# Installation d'un certificat \*.p12 dans Internet Explorer 7 (3/3)

**Assistant Importation de certificat**

**Mot de passe**  
Pour maintenir la sécurité, la clé privée a...

Entrez le mot de passe de la clé privée

Mot de passe :  
\*\*\*\* 1

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.

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

< Précédent 3 Suivant > Annuler

Entrer le mot de passe  
Rendre la clé "exportable"  
Cliquer sur "Suivant"

**Assistant Importation de certificat**

**Magasin de certificats**  
Les magasins de certificats sont des zones système où les certificats sont stockés.

Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier l'emplacement du certificat.

Sélectionner automatiquement le magasin de certificats selon le type de certificat

Placer tous les certificats dans le magasin suivant

Magasin de certificats :  
Personnel Parcourir...

< Précédent Suivant > Annuler

**Assistant Importation de certificat**

**Fin de l'Assistant Importation de certificat**

Vous avez terminé correctement l'Assistant Importation de certificat.

Vous avez spécifié les paramètres suivants :

Magasin de certificats sélectionné par l'utilisateur	Personnel
Contenu	PFX
Nom du fichier	I:\Adu

< Précédent Terminer > Annuler

**Assistant Importation de certificat**

L'importation s'est terminée correctement.

OK

**Certificats**

Rôle prévu : Authentification du client

Personnel Autres personnes Autorités intermédiaires Autorités principales de confiance

Délivré à	Délivré par	Date d'e...	Nom convivial
Stephane Vast	AC ADULLACT Projet	27/12/2008	Stephane VAST

Importer... E Avancé...

Détails de certificat  
<Tout> Affichage

Fermer

Le certificat importé,  
fermer les boîtes  
de dialogue.



# Insertion du certificat (partie publique) pour un utilisateur

[Page d'accueil](#) > [Gestion des utilisateurs](#)

On passera par le formulaire d'ajout des utilisateurs pour définir les caractéristiques des utilisateurs de la plate-forme et en particulier pour insérer le certificat (partie publique) de l'utilisateur sur le serveur S2LOW. Il comporte une série de champs, certains sont obligatoires :

- Nom, Prénom (Obligatoires) ;
- Adresse électronique (Obligatoire) ;
- Téléphone (Facultatif) ;
- **Certificat X509 au format PEM (Obligatoire lors de la création, facultatif lors de la modification) ;**
- État (Obligatoire) ;
- Rôle (Obligatoire) ;
- Permissions sur les modules (Obligatoire).

*Concernant le certificat utilisateur, celui-ci doit avoir été émis par une autorité de certification reconnues par la plate-forme. Dans le cas contraire, l'authentification de l'utilisateur ne fonctionnera pas.*

## Gestion des utilisateurs de la collectivité « ADULLACT »

[Retour liste utilisateurs](#)

### Ajout d'un utilisateur

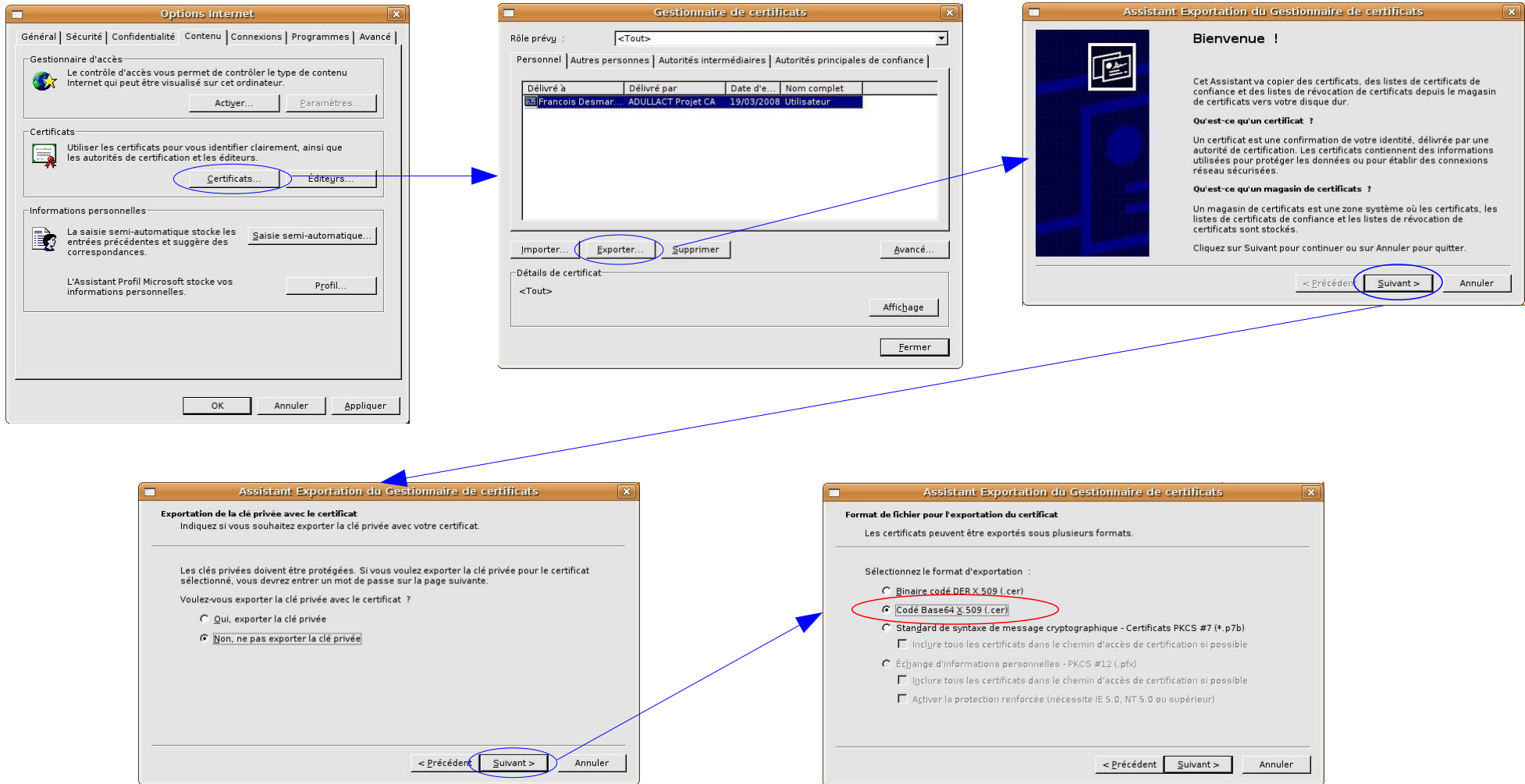
Nom :	<input type="text"/>
Prénom :	<input type="text"/>
Adresse électronique :	<input type="text"/>
Téléphone :	<input type="text"/>
Importer le certificat utilisateur (format PEM) :	<input type="text"/> <a href="#">Parcourir...</a>
État :	Choisissez ▼
Rôle :	Choisissez ▼
Permissions modules :	Module Actes : Choisissez ▼

[Ajouter l'utilisateur](#)

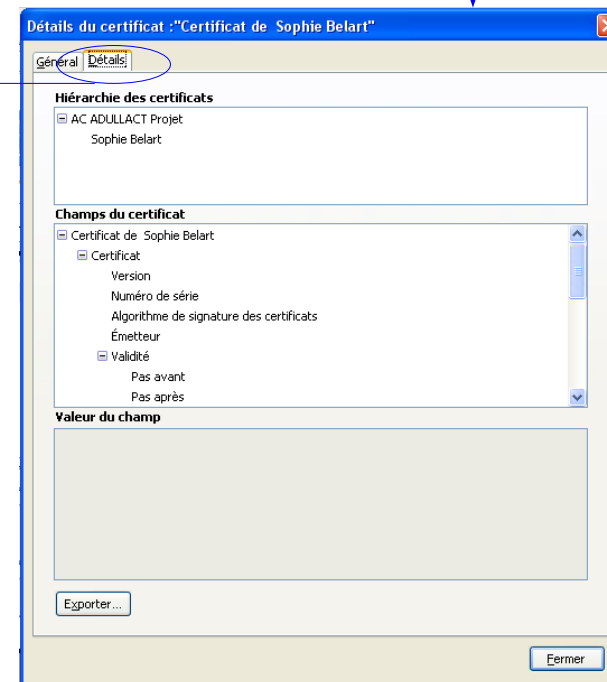
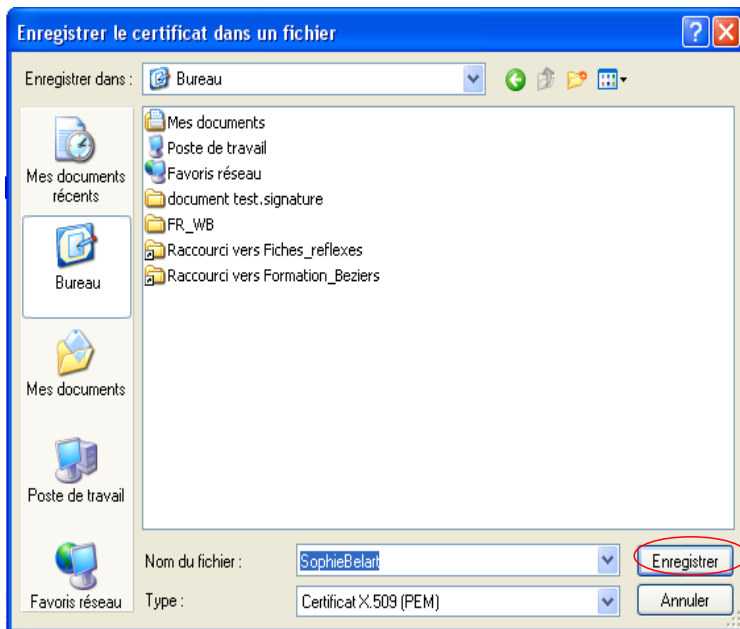
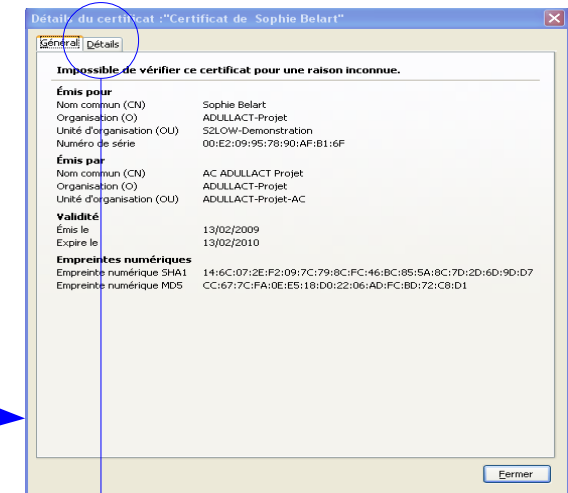
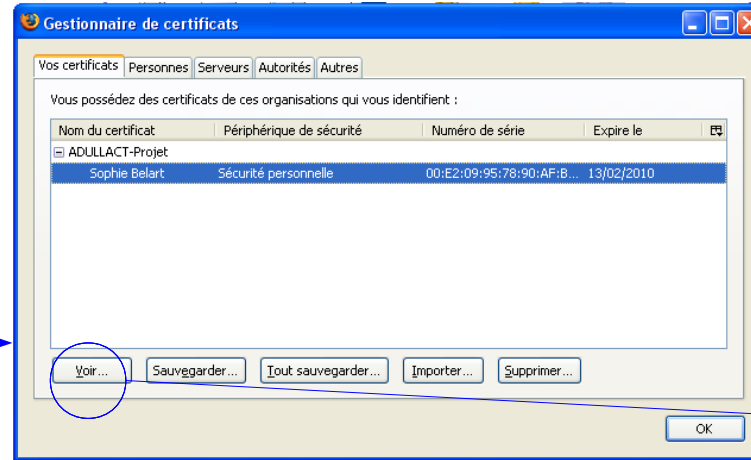
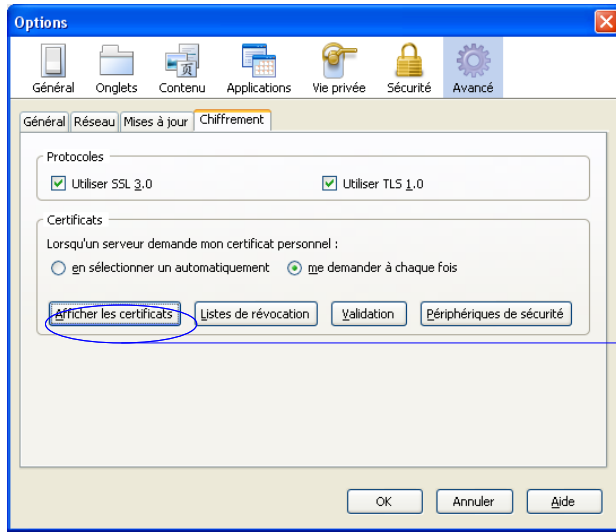
On importe ici la partie publique du certificat X509; selon les éditeurs, ce fichier peut avoir pour extension: **.pem, .cer (MS-Windows), .der**



# Extraction de la partie publique d'un certificat logiciel avec Internet Explorer 6 (sous MS-Windows)



# Extraction de la partie publique d'un certificat logiciel avec Mozilla- Firefox 3.0.5 (sous Windows)





## Extraction de la partie publique d'un certificat logiciel avec OpenSSL (tous systèmes & navigateurs)

Afin d'extraire la partie X509 (partie publique) d'un certificat logiciel (format p12 ou PKCS#12), il suffit de disposer du logiciel OpenSSL (sous GNU/Linux, MS-Windows, MacOS-X,...), et d'exécuter la commande suivante dans un terminal :

```
openssl pkcs12 -clcerts -nokeys -in fichier_cert.p12 -out fichier_cert.pem
```

C'est cette partie publique du certificat (*fichier\_cert.pem*) qu'il faudra insérer dans le formulaire lors de la création d'un nouvel utilisateur.



Pour MS-Windows, OpenSSL est librement téléchargeable ici:  
<http://gnuwin32.sourceforge.net/packages/openssl.htm>



# Liste des autorités retenues

## Autorités de certification reconnues

---

Le TdT reconnaît les autorités de certification ci-dessous pour l'authentification des collectivités et la signature des fichiers :

- ADULLACT Projet CA
- AC Racine - Root CA
- TelePro Entreprise
- Azzarius Classe 3
- Azzarius Root CA
- BNP PARIBAS - AUTHORITY ENTERPRISE
- BNP PARIBAS ROOT CERTIFICATION AUTHORITY
- AC Certeurope Classe 3Plus
- Certeurope Root CA
- AC Certigrefe Classe 3Plus
- Class 2 Primary CA
- AC CERTINOMIS SSL
- CertiNomis Classe 2
- CertiNomis Classe 3
- CertiNomis
- BANQUE POPULAIRE - CLICK AND TRUST - TVA
- BANQUE POPULAIRE - CLICK AND TRUST - PAIEMENTS SECURISES
- BANQUE POPULAIRE - AUTORITE DE CERTIFICATION
- CA Certificat
- CA root Credit Agricole
- CSF - Classe III - Sign et Crypt ← Chambersign
- CSF
- /C=FR/O=GIP-CPS/OU=AC-CLASSE-1
- /C=FR/O=GIP-CPS
- Greffe-TC-Paris-Or-S
- DigiGrefe
- CCF Elys CERTIFICATION
- CCF Certification
- NATEXIS BANQUES POPULAIRES - NXBP CESAM Relations Fiscales - AC
- S2LOW CA
- SG TRUST SERVICES AUTHENTIFICATION ET CHIFFREMENT DE CLEF
- SG TRUST SERVICES RACINE
- AC ADULLACT Projet