S²LO

ACTES - Dématérialisation du contrôle de légalité

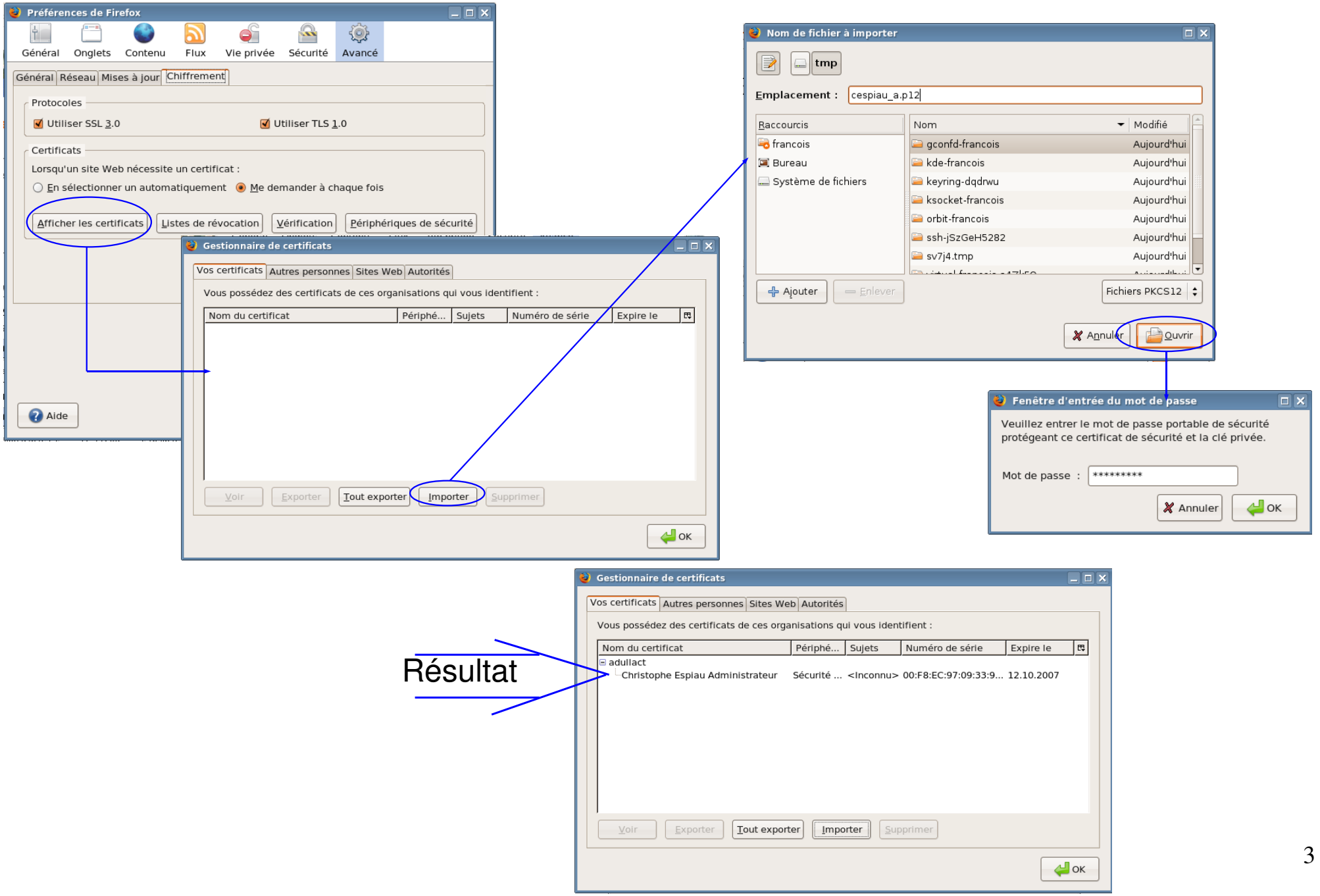
Certificats & navigateurs

ADULLACT Projet

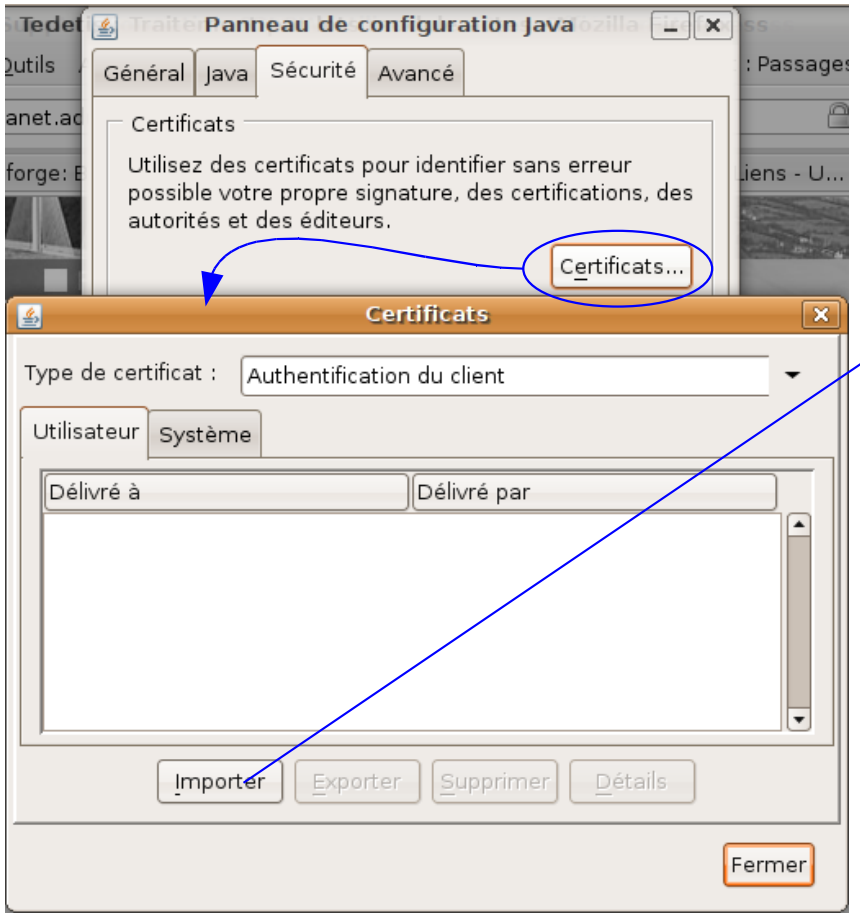
Alternance Soft

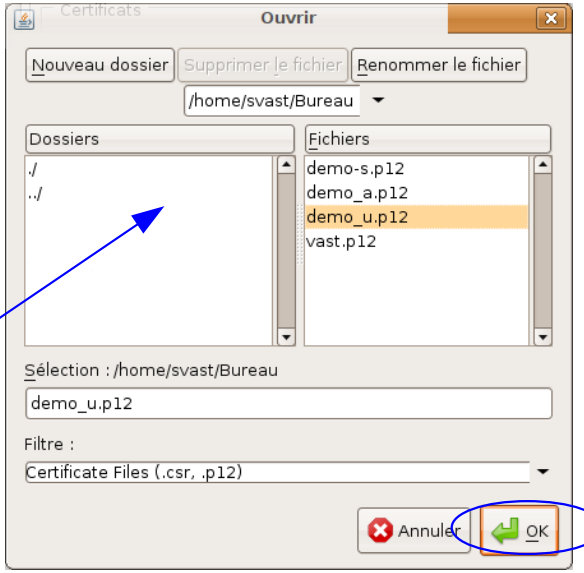
Gestion des certificats / navigateurs

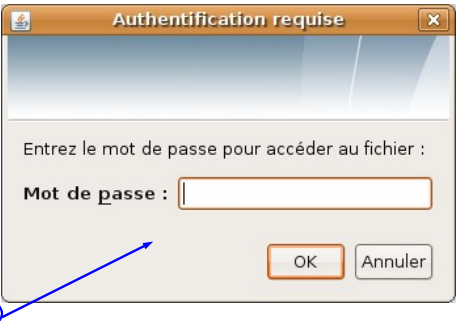
Installation d'un certificat *.p12 dans Firefox

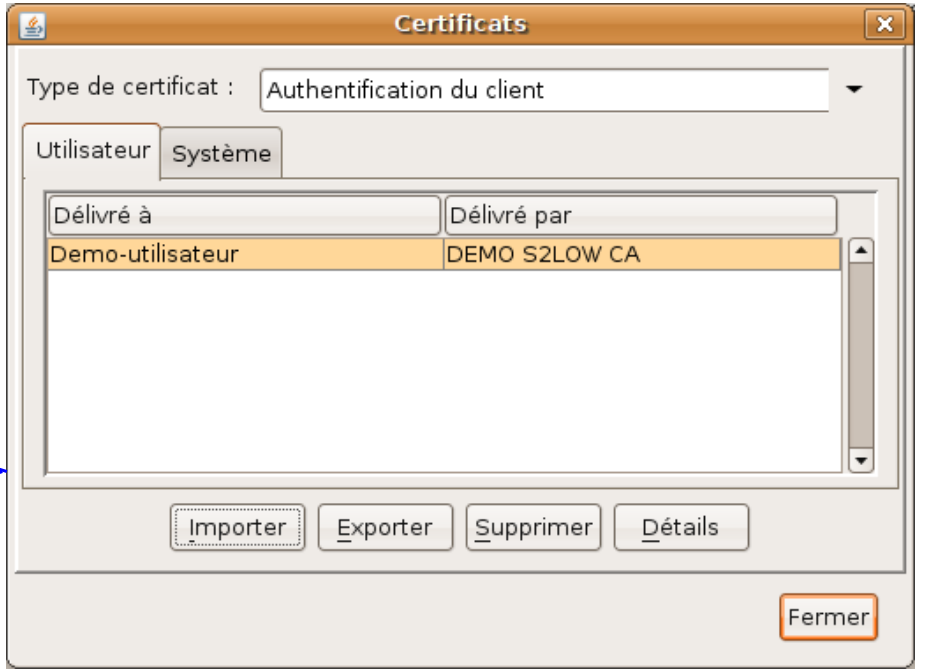


Installation d'un certificat *.p12 dans JAVA





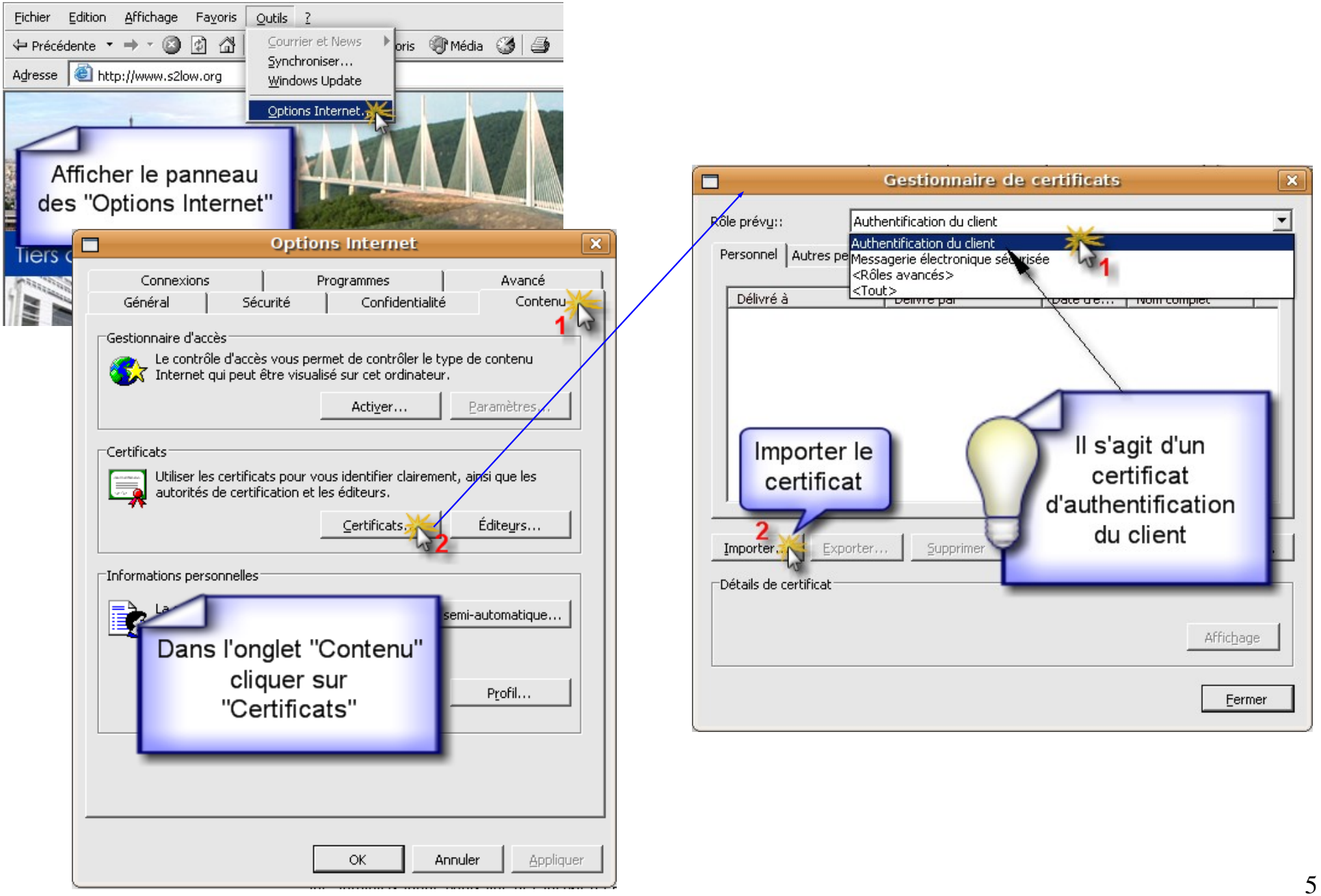




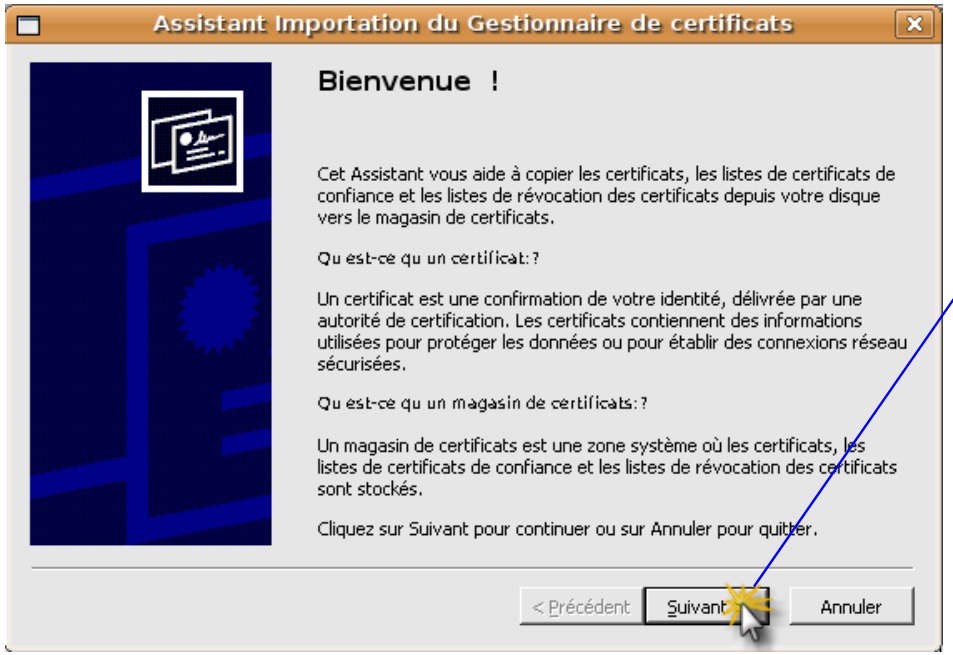
Résultat

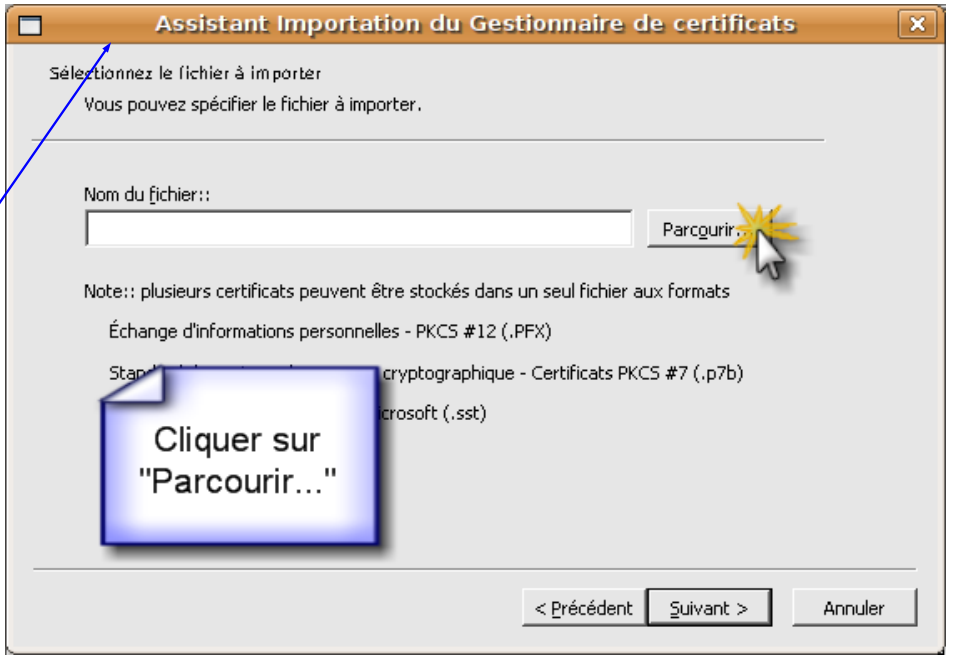
NB: Cette opération est requise pour la gestion par lots sous Firefox

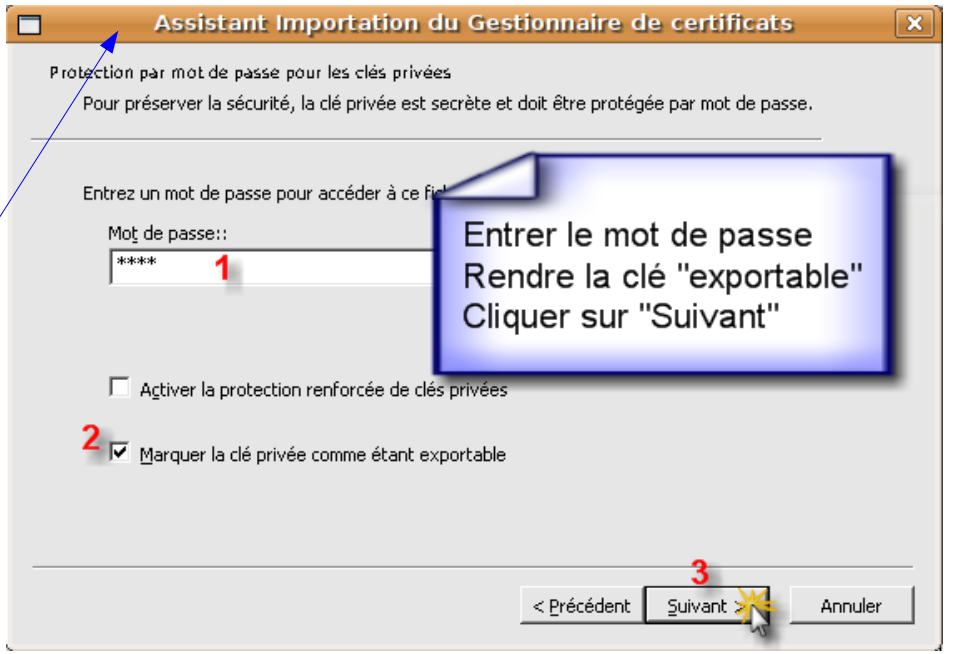
Installation d'un certificat *.p12 dans Internet Explorer 6 (1/3)



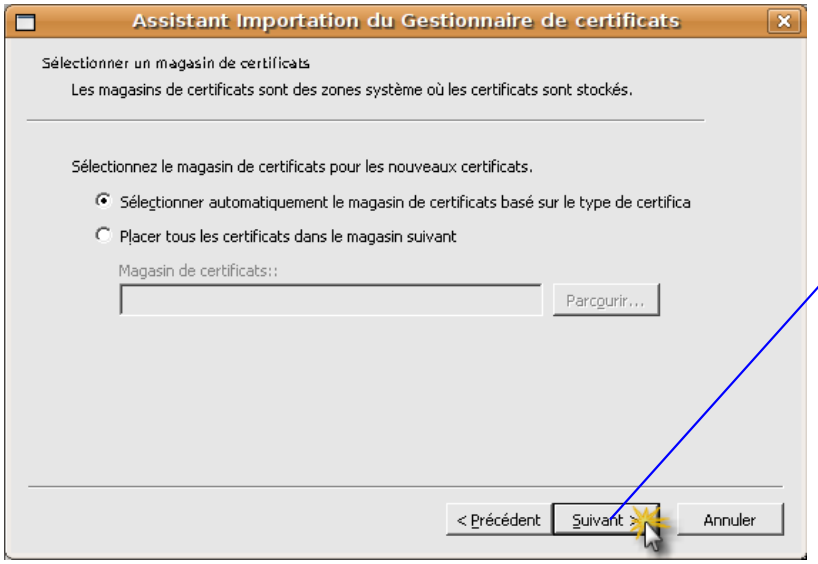
Installation d'un certificat *.p12 dans Internet Explorer 6 (2/3)

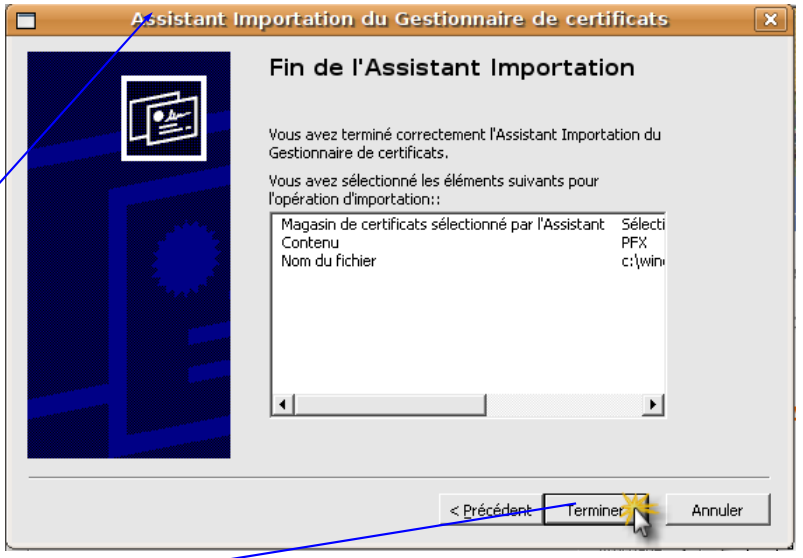


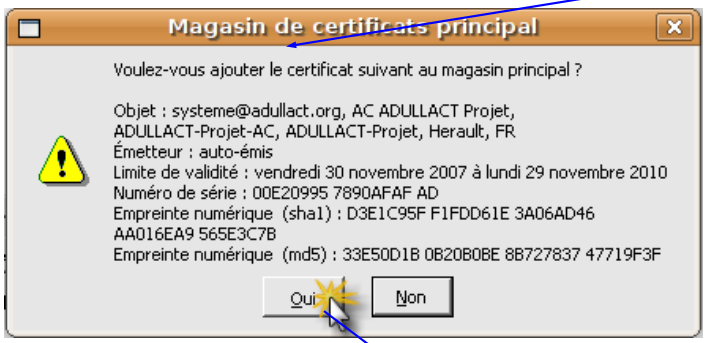


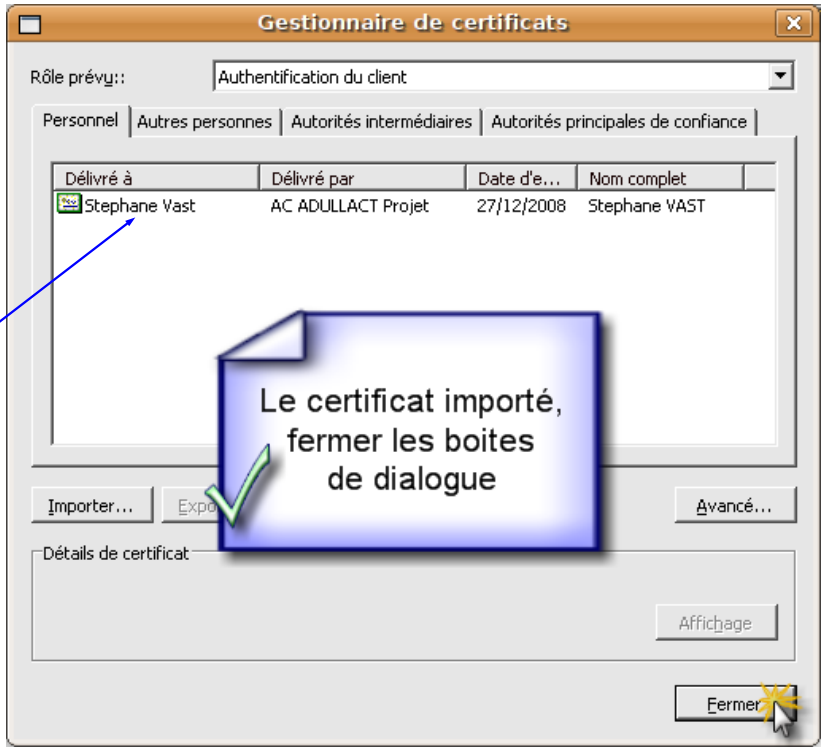


Installation d'un certificat *.p12 dans Internet Explorer 6 (3/3)

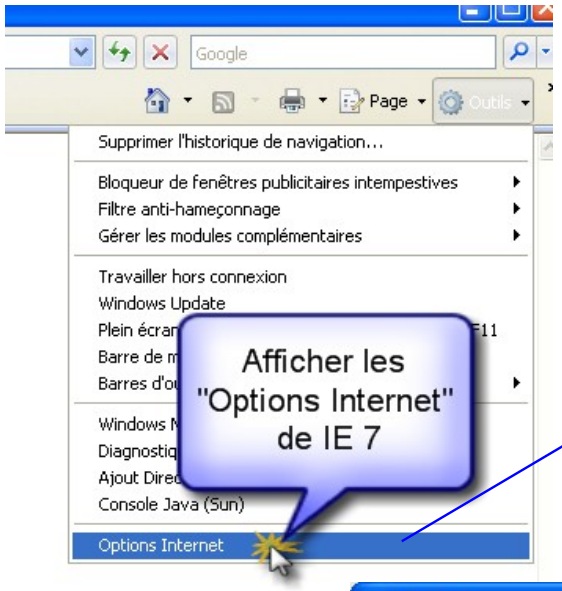


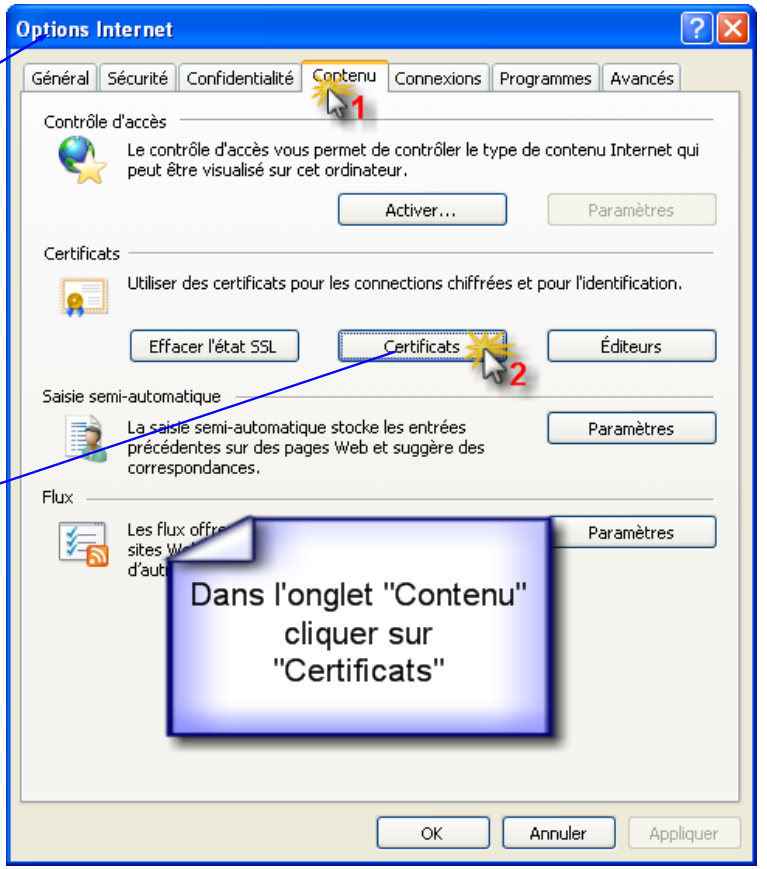


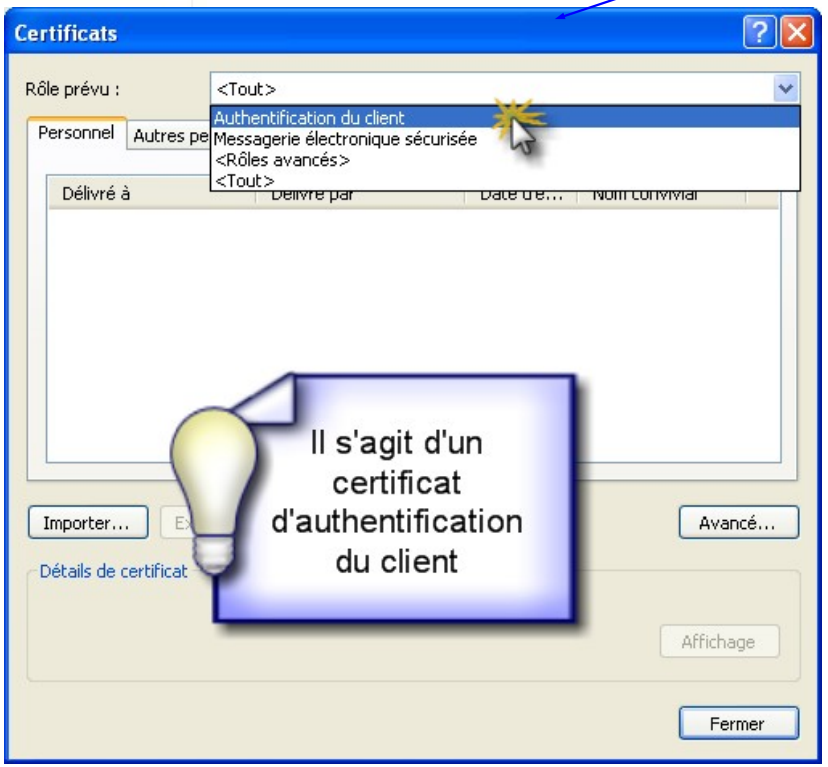




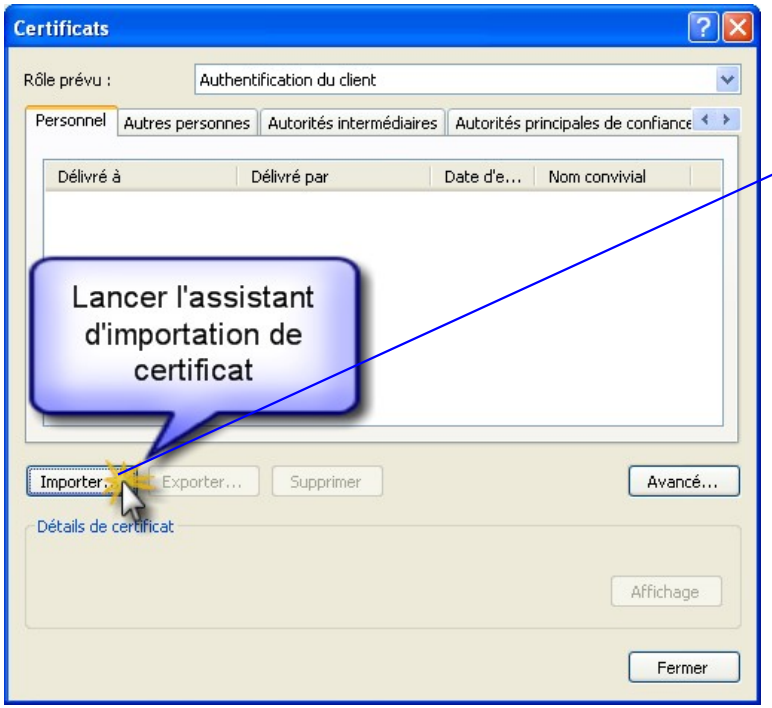
Installation d'un certificat *.p12 dans Internet Explorer 7 (1/3)

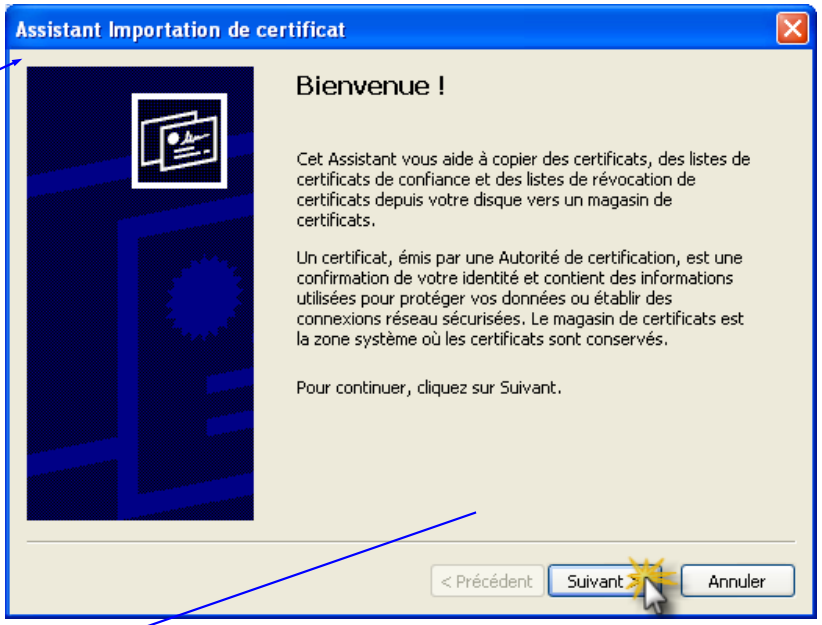


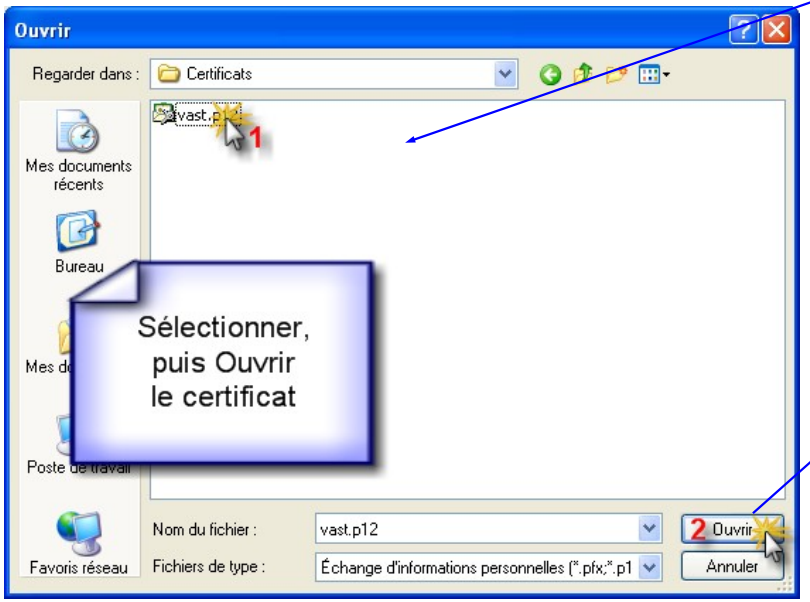


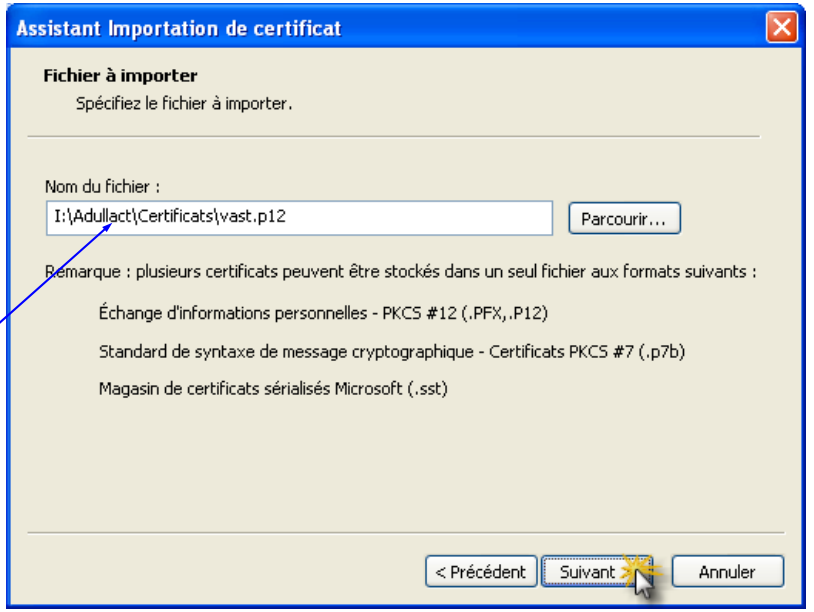


Installation d'un certificat *.p12 dans Internet Explorer 7 (2/3)

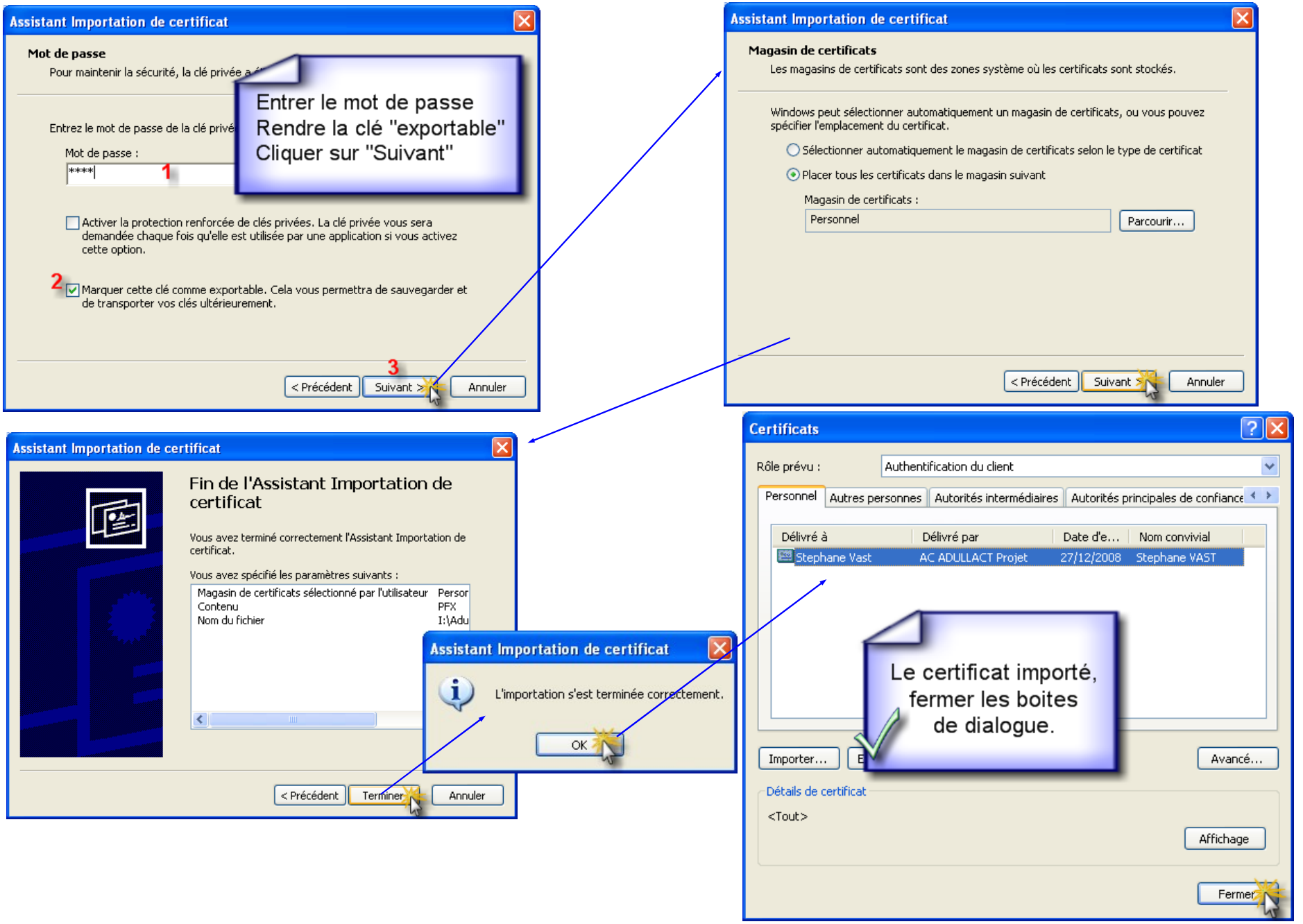








Installation d'un certificat *.p12 dans Internet Explorer 7 (3/3)



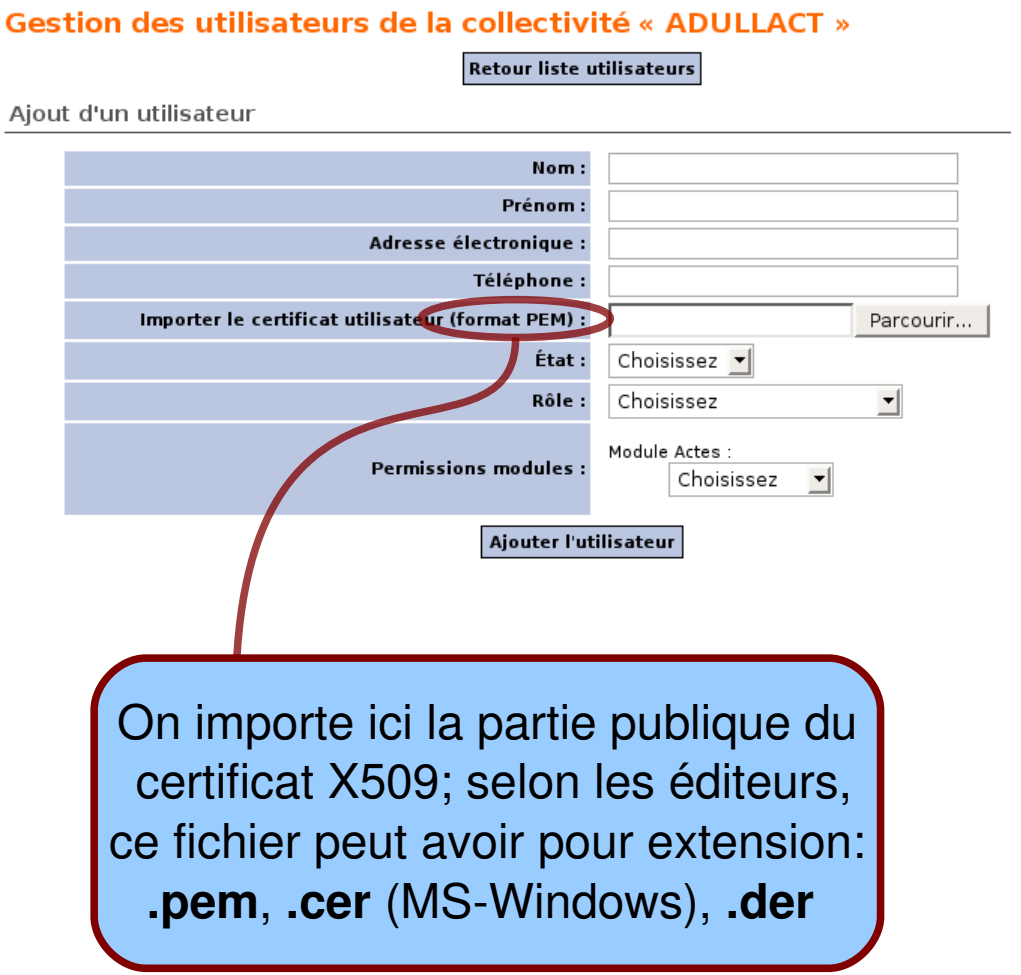
Insertion du certificat (partie publique) pour un utilisateur

Page d'accueil > Gestion des utilisateurs

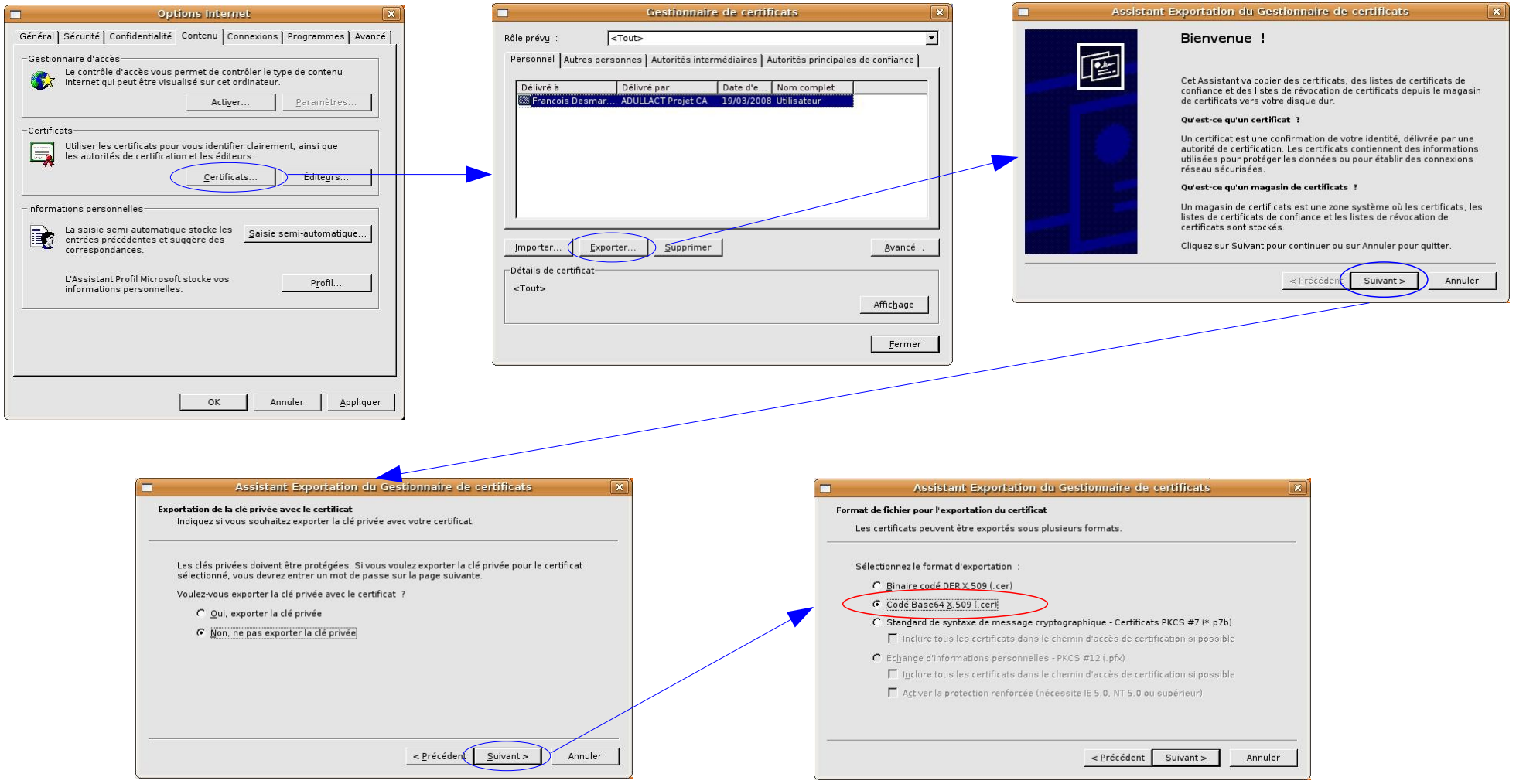
On passera par le formulaire d'ajout des utilisateurs pour définir les caractéristiques des utilisateurs de la plate-forme et en particulier pour insérer le certificat (partie publique) de l'utilisateur sur le serveur S2LOW. Il comporte une série de champs, certains sont obligatoires :

- 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).

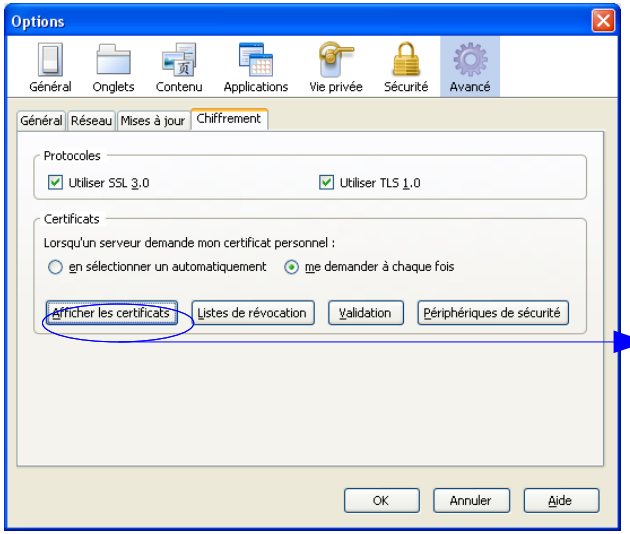
Concernant le certificat utilisateur, celui-ci doit avoir été émis par une autorité de certification reconnues par la plate-forme. Dans le cas contraire, l'authentification de l'utilisateur ne fonctionnera pas.

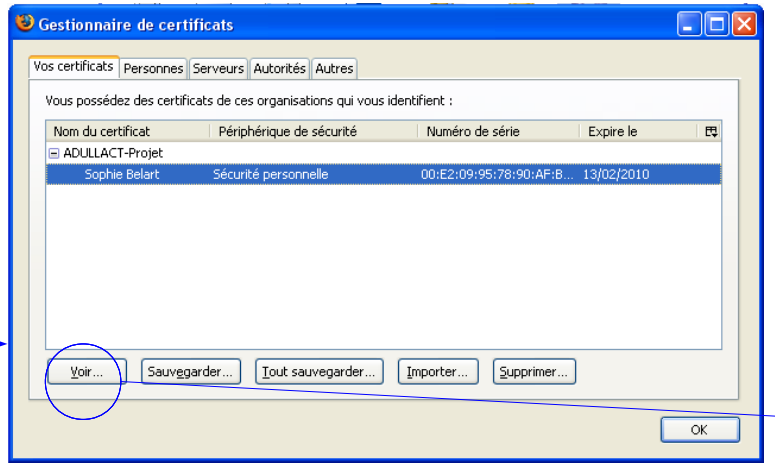


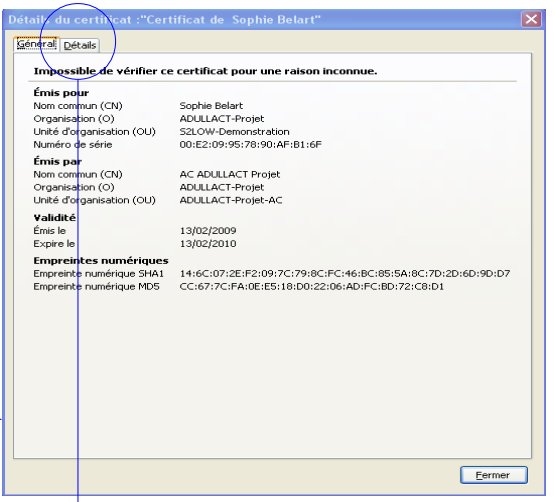
Extraction de la partie publique d'un certificat logiciel avec Internet Explorer 6 (sous MS-Windows)

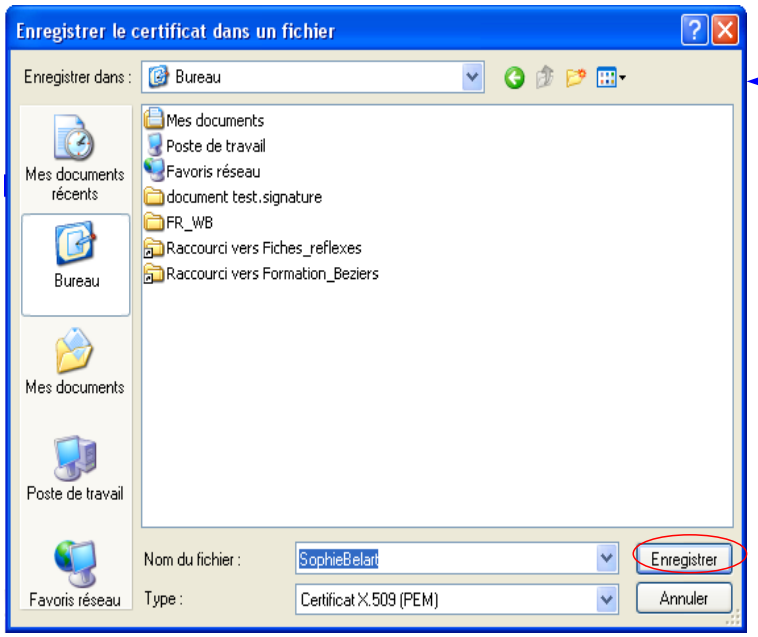


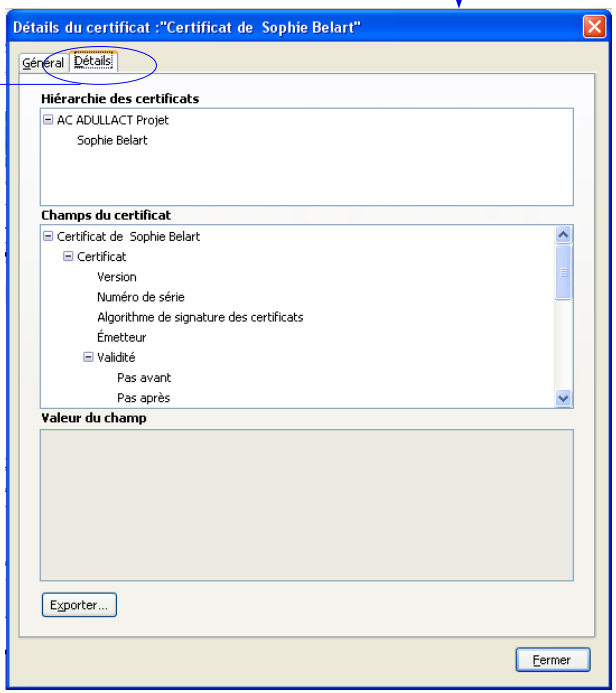
Extraction de la partie publique d'un certificat logiciel avec Mozilla- Firefox 3.0.5 (sous Windows)











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 Certigreffe 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
- CSF
- /C=FR/O=GIP-CPS/OU=AC-CLASSE-1
- /C=FR/O=GIP-CPS
- Greffe-TC-Paris-Or-S
- DigiGreffe
- 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