



**Faculté des Sciences de Bizerte (FSB)**  
**Université de Carthage**



# **Pratiques Cryptographiques**

## **TP – PKI et Certificats Electroniques**

**CI 2**

Semestre 2

**Dr. Ing. Nizar Ben Neji**  
**nizar.benneji@fsb.ucar.tn**

**2024 / 2025**

# Plan

- Génération des paires de clés **RSA**
- Génération d'un certificat **auto-signé**
- Génération de **requêtes PKCS#10**
- Usage de OpenSSL et comprendre les divers sections du fichier de configuration **openssl.cnf**
- **Révocation** des certificats électroniques
- Génération des **LCR** (Liste de Certificats Révoqués)
- **Changement de l'encodage** des certificats et des LCRs du texte (**PEM**) vers le binaire (**DER**) et vis versa
- Création d'enveloppes **PKCS#12** englobant des clés et des certificats
- **Installation** du certificat au niveau des **magasins des certificats** du système d'exploitation et des autres outils (Mozilla Firefox, JAVA Keystore,...):
  - ✓ **MS Key Store**
  - ✓ **Firefox Store (Mozilla et Thunderbird)**
  - ✓ **Java Keystore**
  - ✓ ...

# Prérequis

- **Distribution Linux** (Fedora, Centos, Ubuntu,...) pour la partie création du certificat
- **SE Windows** pour la partie installation et exploitation des certificats électroniques
- **OpenSSL** est la boîte à outils cryptographiques disposant d'une interface en ligne de commande ayant plusieurs options qui offrent plusieurs types de chiffrement symétrique (Blowfish, DES, Triple DES, RC4, RC5, ...), chiffrement asymétrique (RSA, DSA, ...), hachage cryptographique (MD5, SHA1, SHA2, ...) et encodage de données (Base 64, DER, PEM, ...)
- **Java Keytool** est un utilitaire en ligne de commande JAVA de gestion des clés et des certificats électroniques
- **pki/** répertoire joint à ce TP contenant tous les fichiers nécessaires à la réalisation de ce TP. Placez ce répertoire au niveau du **/home** de votre machine linux.

# OpenSSL

**OpenSSL** est une boîte à outils cryptographiques disposant d'une interface en ligne de commande ayant plusieurs options qui offrent plusieurs types de chiffrement (Blowfish, DES, Triple DES, RC4, RC5, ...), hachage (MD5, SHA1, SHA2, ...) et encodage de données (Base 64, DER, PEM, ...).

OpenSSL supporte les protocoles de sécurité réseau Secure Sockets Layer v2/v3 (SSLv2/SSLv3), et Transport Layer Security v1 (TLSv1) et peut être utilisée comme bibliothèque de chiffrement pour la mise en place d'application intégrant des modules cryptographiques.

Une des utilisations les plus courantes d'OpenSSL est de fournir des certificats électroniques utilisables avec des applications logicielles. Ces certificats assurent que les identités des sociétés ou des individus sont valides et non frauduleuses. Si le certificat en question n'a pas été issu par une autorité de confiance, une alerte est généralement produite pour prévenir l'utilisateur.



<http://www.openssl.org/>

# Mise en place d'une PKI

## Mise en place d'une PKI OpenSSL (1/6)

### Contenu du répertoire « pki » :

```
ca/
  fsb.key          # Clé de l'AC FSB
  fsb.crt          # Certificat de l'AC FSB
config/            # Fichiers de configuration d'OpenSSL
  openssl_ca.cnf
  openssl_mail.cnf
  openssl_ssl.cnf
  openssl_signature_code.cnf
certs/             # Répertoire va contenir les certificats
  utilisateur1/    # des utilisateurs finaux
    utilisateur1.key
    utilisateur1.req
    utilisateur1.crt
    utilisateur1.p12
```

# Mise en place d'une PKI

## Mise en place d'une PKI OpenSSL (2/6)

### Contenu du répertoire « pki » (suite):

crls/  
liste.crl

# Répertoire contenant la liste  
# des certificats révoqués

index/  
index  
serial/  
serial

# Fichier base de données de la PKI  
  
# Fichier contenant le numéro de série  
# du certificat courant qui va s'incrémenter  
# après la génération de chaque certificat

# Mise en place d'une PKI

## Mise en place d'une PKI OpenSSL (3/6)

### 1. Génération d'un certificat auto-signé

```
openssl genrsa -out ca/uc_ca.key -des3 4096
```

Editez le fichier « **config/openssl\_ca.cnf** » et changez le nom de l'autorité de certification et nommez la « **AC FSB** » et modifiez tous les chemins et noms des fichiers si nécessaire.

```
openssl req -new -x509 -key          ca/fsb.key
                        -out          ca/fsb.crt
                        -config       config/openssl_ca.cnf
                        -days        3650
                        -set_serial   0xABCD
```

### 2. Affichage du certificat

```
openssl x509 -in ca/fsb.crt
            -text
            -noout
```

### 3. Conversion du certificat du format PEM (ASCII) au format DER (Binaire)

```
openssl x509 -inform PEM
            -outform DER
            -in      ca/fsb.crt
            -out      ca/fsb.der
```

# Mise en place d'une PKI

## Mise en place d'une PKI OpenSSL (4/6)

### 4. Génération d'un certificat utilisateur

#### (a) Génération de la paire des clés

```
openssl genrsa -out certs/utilisateur1/utilisateur1.key -des3 2048
```

Editez le fichier « **config/openssl\_mail.cnf** » et changez les informations concernant le propriétaire du certificat et modifiez tous les chemins et noms des fichiers. Créer un repertoire utilisateur1 sous le repertoire « **../pki/certs/utilisateur1/** »

#### (b) Génération de la requête

```
openssl req -new  
-key      certs/utilisateur1/utilisateur1.key  
-out      certs/utilisateur1/utilisateur1.req  
-config   config/openssl_mail.cnf
```

(affichage requête)

#### (c) Génération du certificat (Signature de la requête par l'uc AC)

```
openssl ca -config config/openssl_mail.cnf  
-in       certs/utilisateur1/utilisateur1.req  
-out      certs/utilisateur1/utilisateur1.crt
```

### 5. Affichage du certificat utilisateur et vérification des données

### 6. Conversion PEM vers DER



# Mise en place d'une PKI

## Mise en place d'une PKI OpenSSL (5/6)

### 7. Génération de l'enveloppe PKCS#12

#### (a) Génération du fichier PKCS#12

```
openssl pkcs12 -export  
              -inkey      certs/utilisateur1/utilisateur1.key  
              -in          certs/utilisateur1/utilisateur1.crt  
              -out         certs/utilisateur1/utilisateur1.p12  
              -certfile    ca/fsb.crt  
              -name        "Nom Prenom Utilisateur 1"
```

**(b) Vérifier le contenu de l'enveloppe PKCS#12 généré.**

**(c) Installer le certificat PKCS#12 « utilisateur1.p12 » au niveau des magasins des certificats du système et des applications à utiliser**

# Mise en place d'une PKI

## Mise en place d'une PKI OpenSSL (6/6)

### 8. Révocation du certificat

Refaire l'étape (4) et générer un certificat pour un utilisateur2

```
openssl ca -config config/openssl_ca.cnf  
           -revoke certs/utilisateur2/utilisateur2.crt
```

### 9. Mise à jour de la LRC (Liste des certificats révoqués)

```
openssl ca -gencrl  
           -config config/openssl_ca.cnf  
           -out crls/rev_list.crl
```

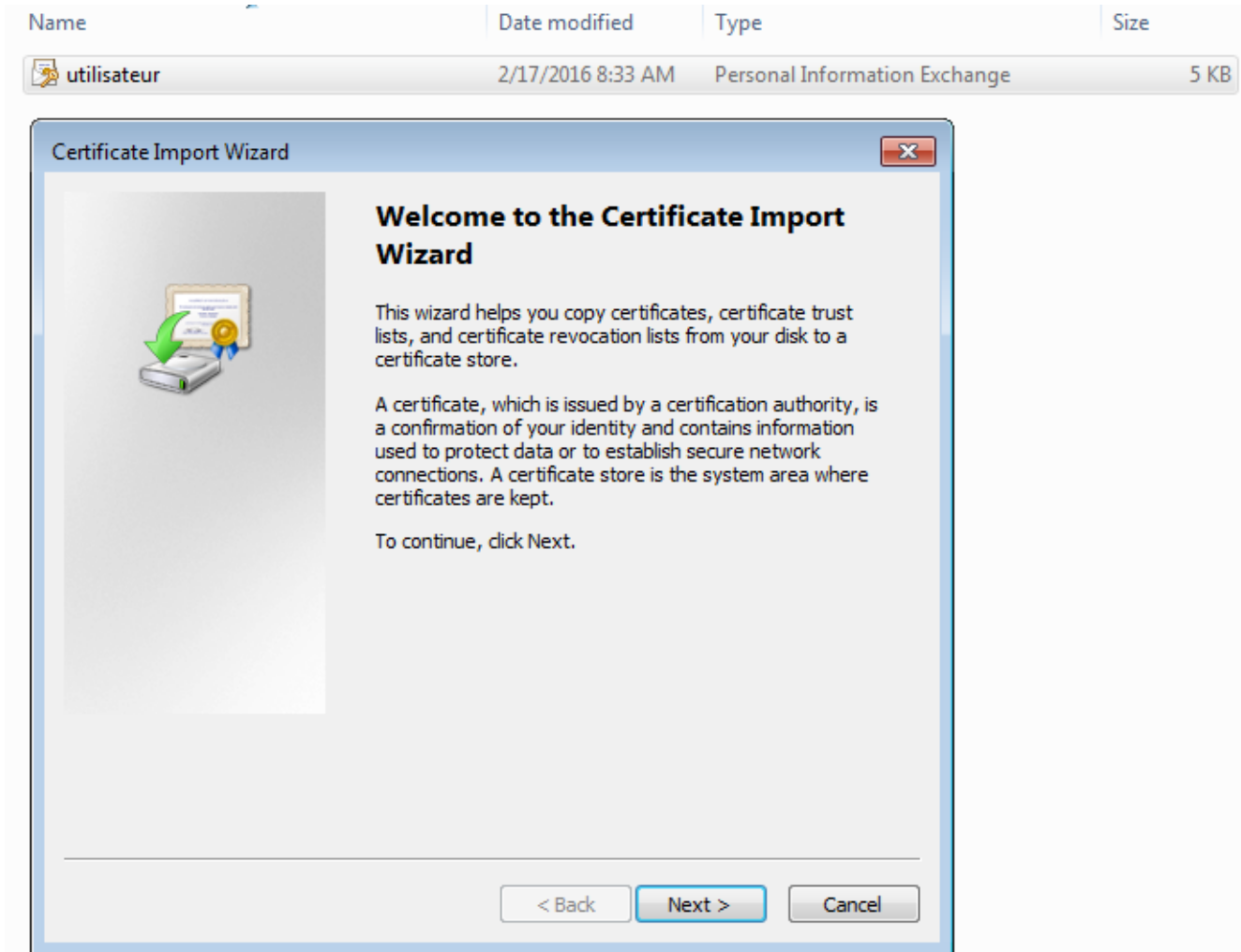
### 10. Affichage de la LRC

```
openssl crl -in crls/rev_list.crl -text
```

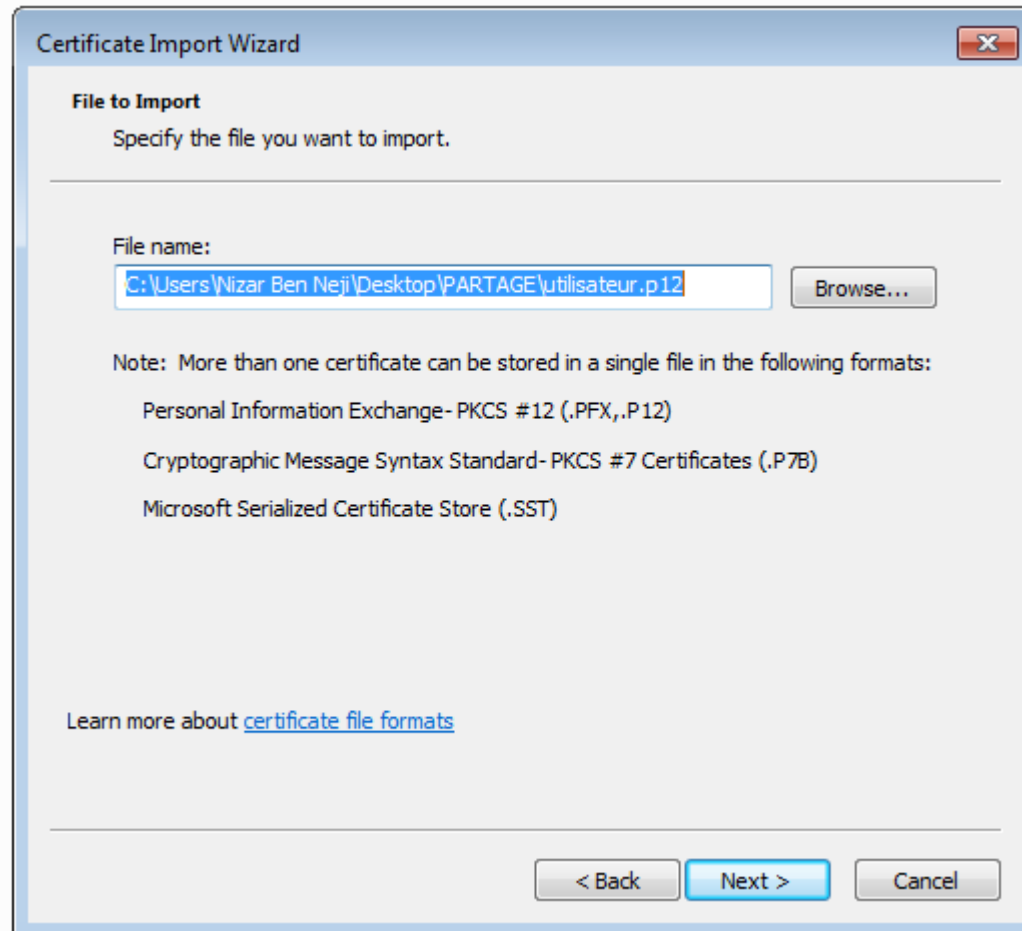
### 11. Conversion LRC du format PEM au format DER (Binaire)

```
openssl crl -in crls/rev_list.crl  
           -out crls/rev_list.der  
           -inform PEM  
           -outform DER
```

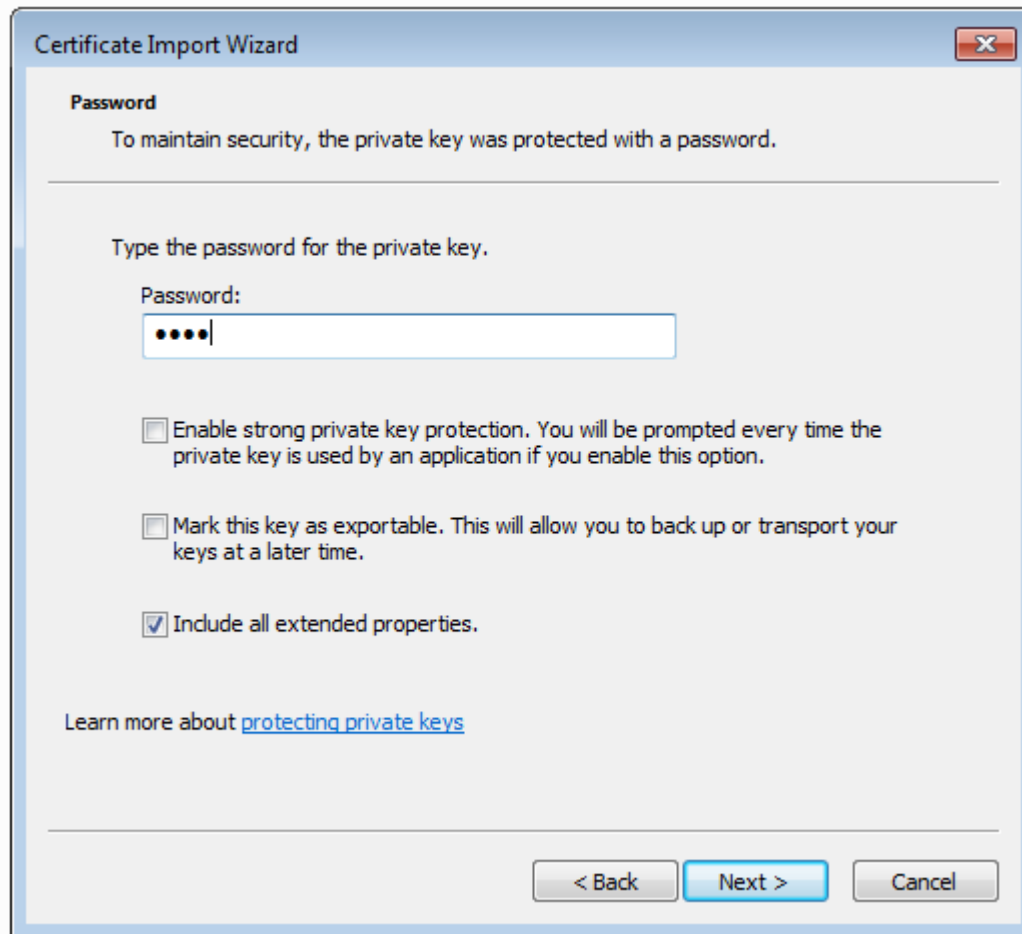
# Installation du certificat au niveau du magasin de Windows



# Installation du certificat au niveau du magasin de Windows

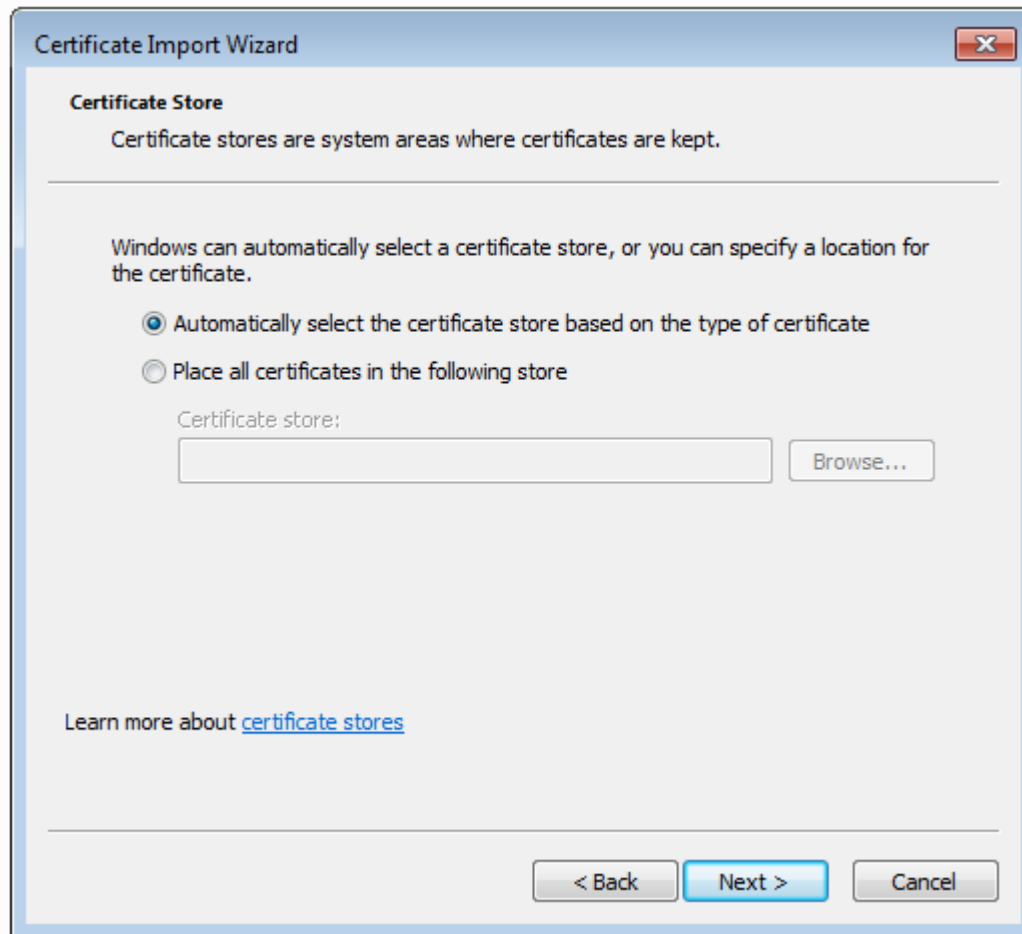


# Installation du certificat au niveau du magasin de Windows

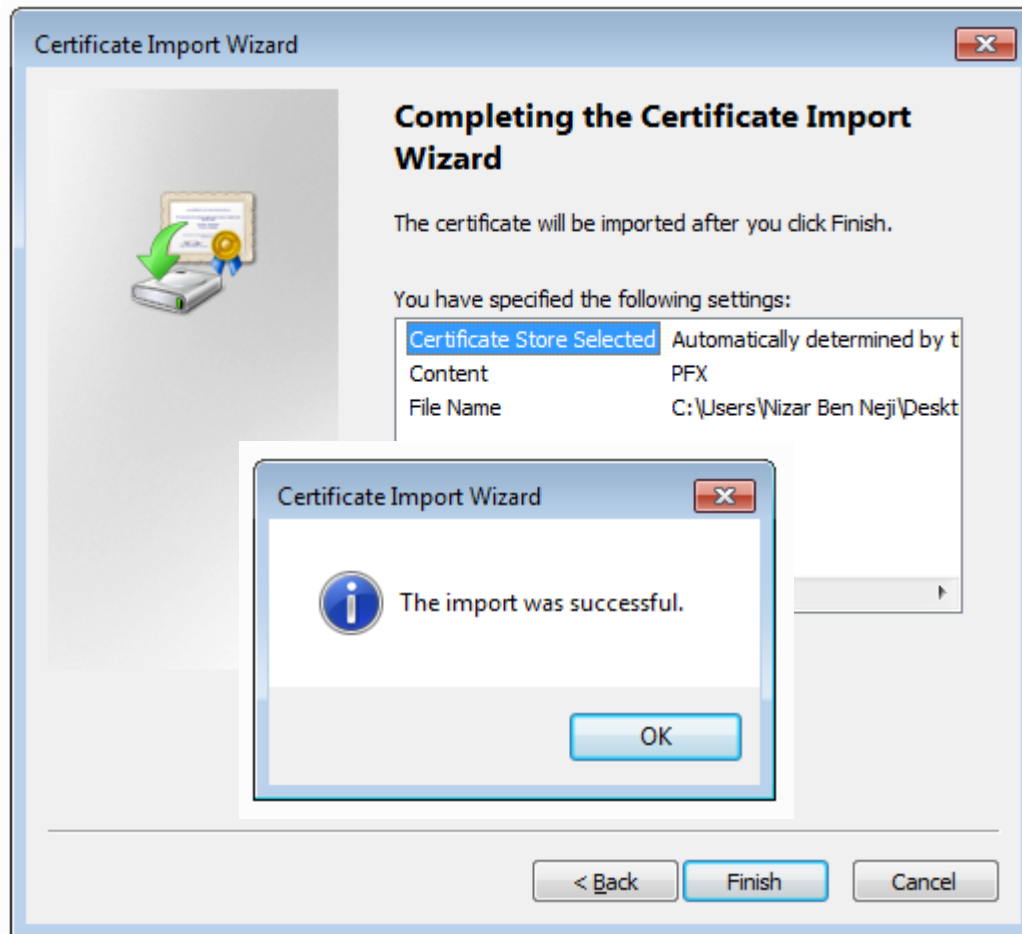


The image shows a Windows 'Certificate Import Wizard' dialog box. The title bar reads 'Certificate Import Wizard' with a close button. The main content area is titled 'Password' and contains the following text: 'To maintain security, the private key was protected with a password.' Below this is a prompt 'Type the password for the private key.' followed by a 'Password:' label and a text input field containing five dots. There are three checkboxes: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.' (unchecked), 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.' (unchecked), and 'Include all extended properties.' (checked). At the bottom, there is a link 'Learn more about [protecting private keys](#)'. The bottom of the dialog features three buttons: '< Back' (disabled), 'Next >' (active/highlighted), and 'Cancel' (disabled).

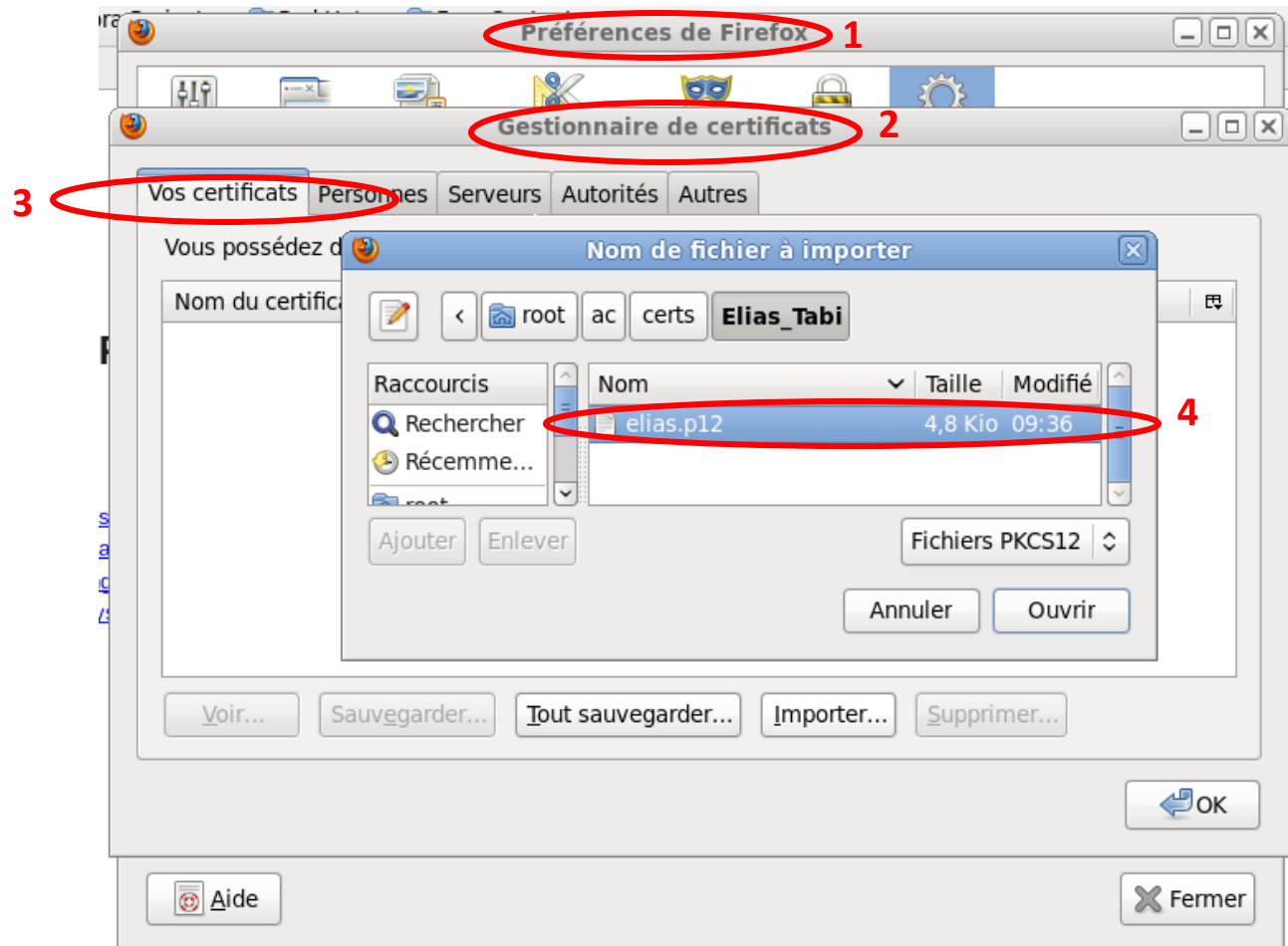
# Installation du certificat au niveau du magasin de Windows



# Installation du certificat au niveau du magasin de Windows

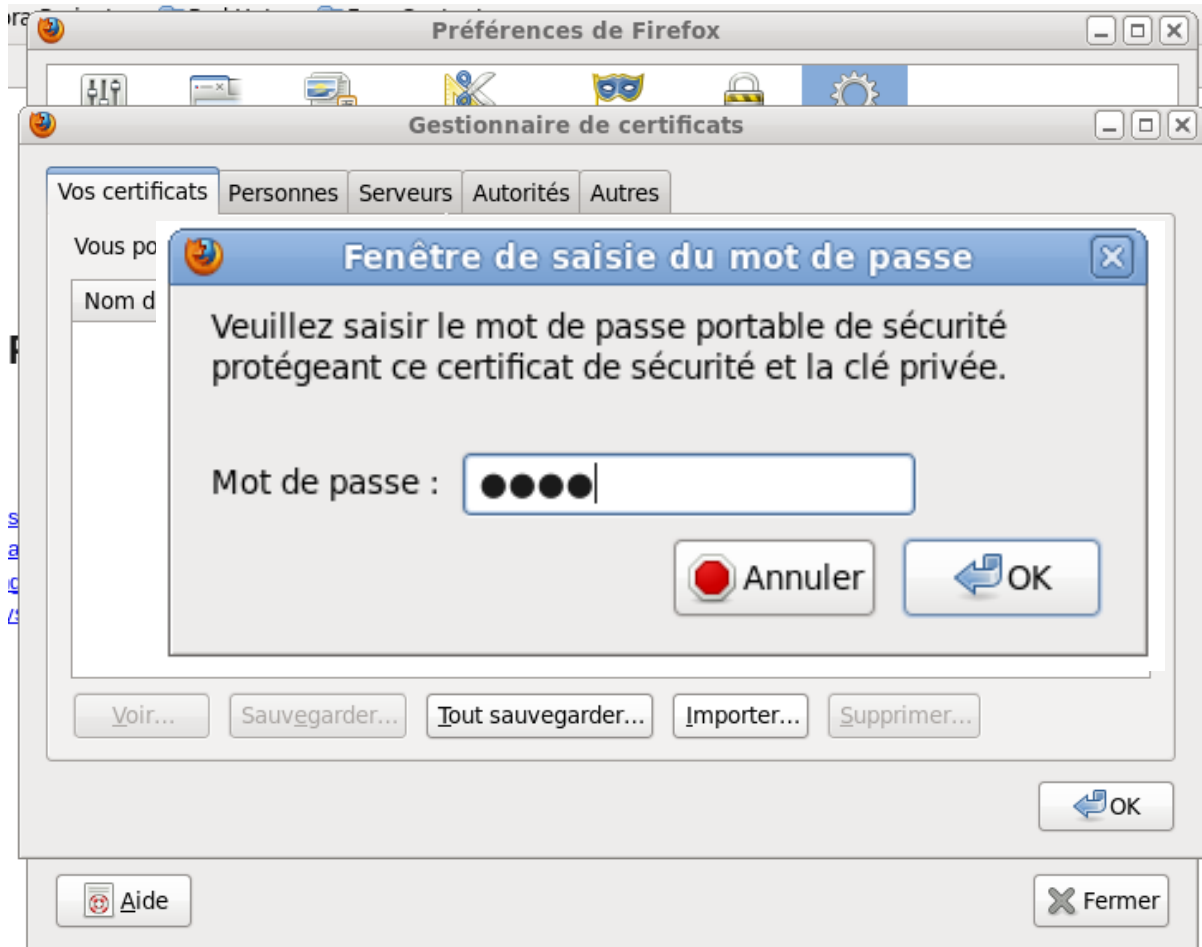


# Installation du certificat au niveau du magasin de Mozilla Firefox (1/6)

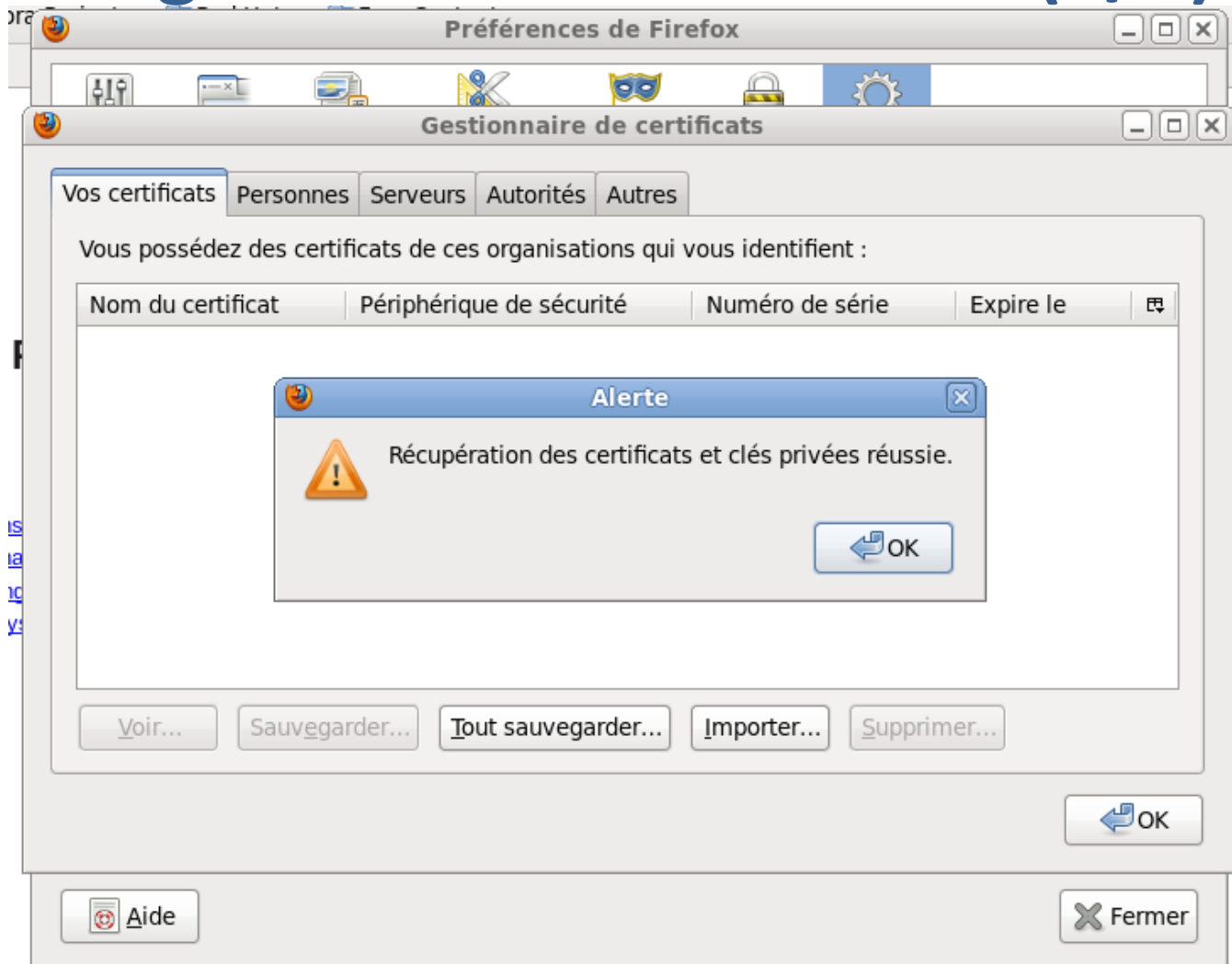




# Installation du certificat au niveau du magasin de Mozilla Firefox (2/6)



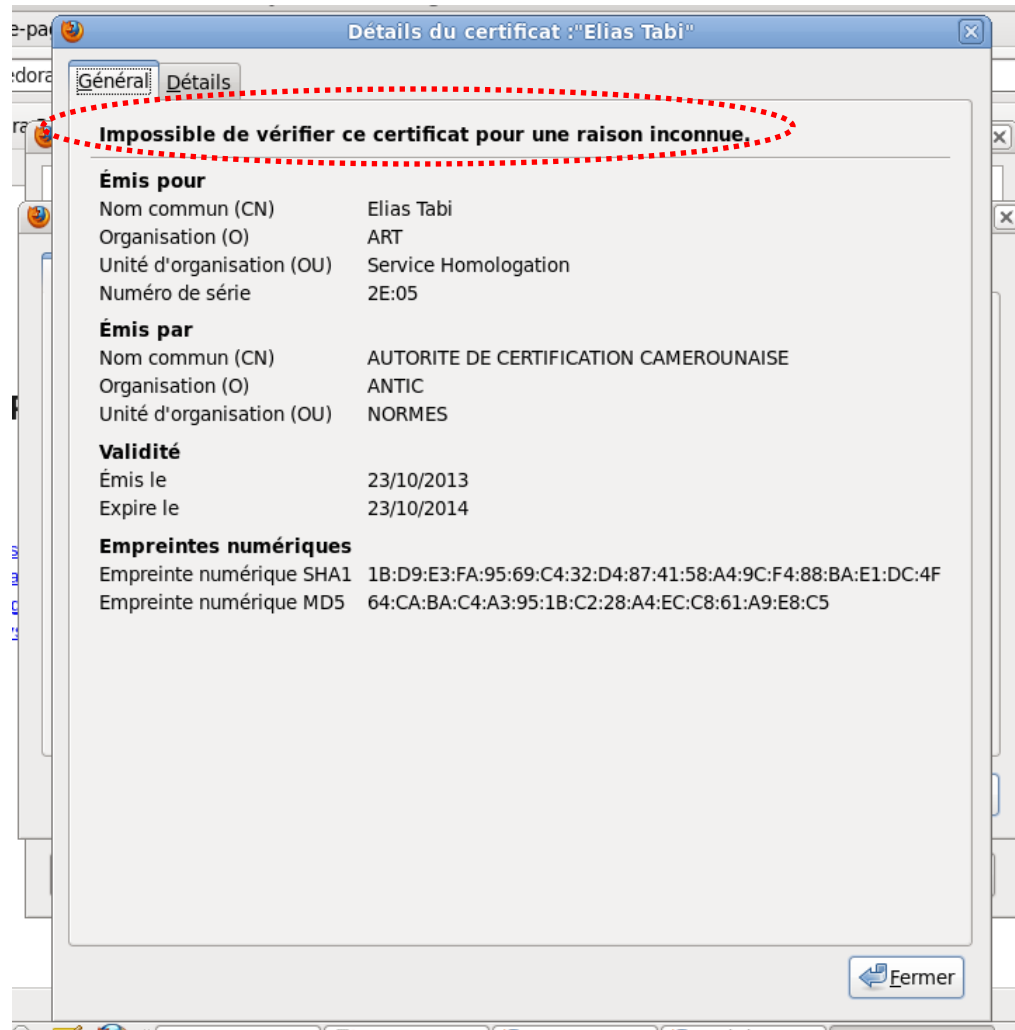
# Installation du certificat au niveau du magasin de Mozilla Firefox (3/6)



# Installation du certificat au niveau du magasin de Mozilla Firefox (4/6)



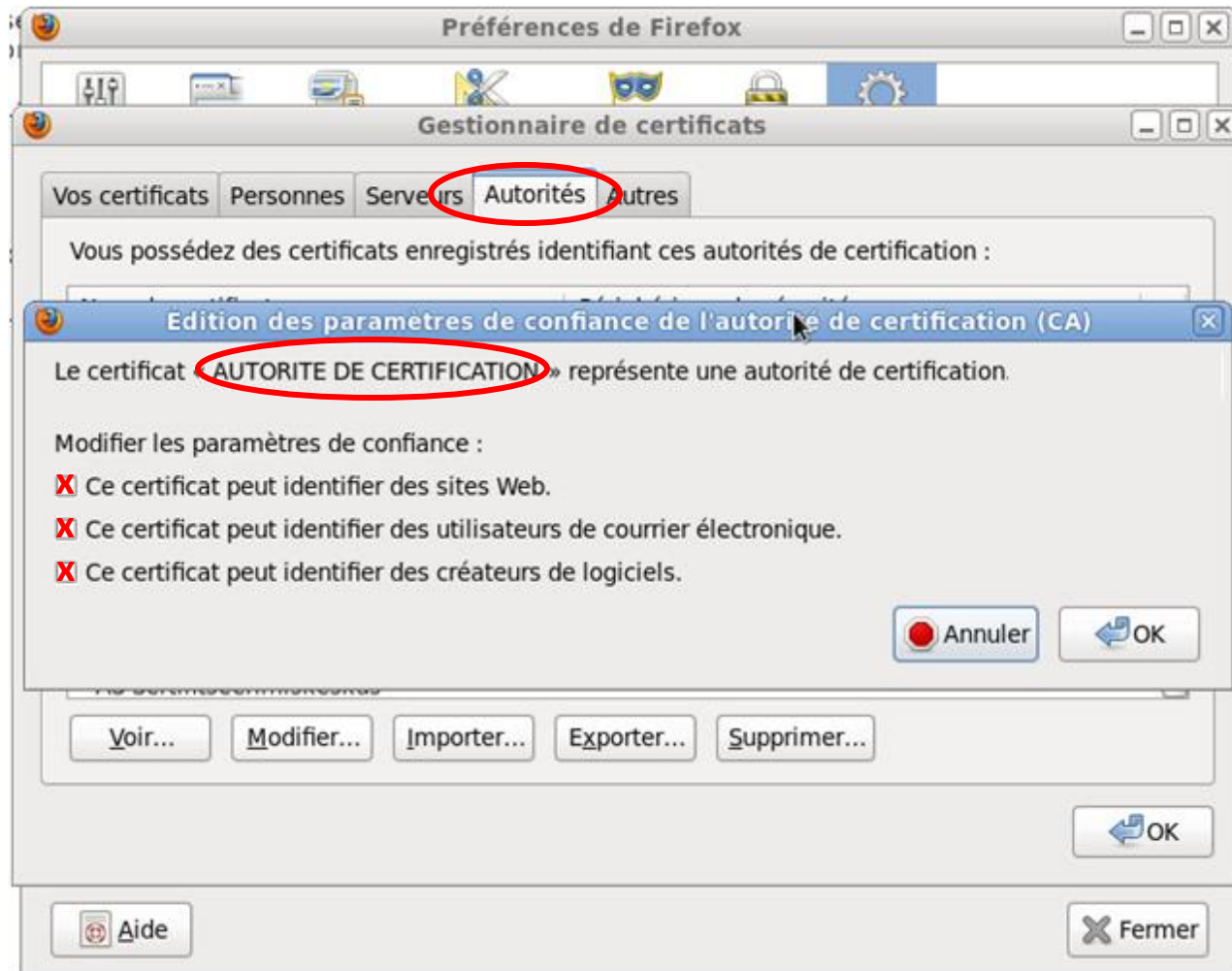
Certificat est refusé par Mozilla Firefox car l'autorité n'est pas reconnue (n'est pas présente dans son Magasin des autorités de confiance)



# Installation du certificat au niveau du magasin de Mozilla Firefox (5/6)



Modifiez les paramètres de confiance de l'autorité émettrice



# Installation du certificat au niveau du magasin de Mozilla Firefox (6/6)



Certificat est bien accepté  
par Mozilla Firefox

