

## Manuel d'installation

MAC OS X 10.5.5 à 10.5.9 et Mac OS X 10.6 - MOZILLA FIREFOX  
MAC OS X 10.6.5 et 10.6.6 - APPLE SAFARI



Pour assurer la sécurité de votre entreprise tout en profitant  
des avantages et des évolutions d'Internet

**AGIR  
POUR  
REUSSIR**  
[www.artisanat.fr](http://www.artisanat.fr)



# Sommaire

<b>NOTIONS SUR LE CERTIFICAT .....</b>	<b>4</b>
<b>UN DOUBLE CERTIFICAT SUR VOTRE CLE CERTIMETIERSARTISANAT .....</b>	<b>5</b>
<b>UTILISATION D'UN CERTIFICAT ELECTRONIQUE CLASSE 3+ OU RGS** .....</b>	<b>6</b>
<b>POINTS IMPORTANTS.....</b>	<b>8</b>
<b>INSTALLATION DES PILOTES SYSTEMES .....</b>	<b>10</b>
<b>INSTALLATION POUR APPLE SAFARI.....</b>	<b>16</b>
<b>INSTALLATION POUR MOZILLA FIREFOX.....</b>	<b>17</b>
<b>PARAMETRAGE MOZILLA FIREFOX .....</b>	<b>25</b>
<b>TEST DE BON FONCTIONNEMENT.....</b>	<b>28</b>
<b>REVOCACTION D'URGENCE .....</b>	<b>30</b>
<b>CHANGEMENT DU CODE PIN .....</b>	<b>32</b>

# Notions sur le certificat

Problème : il est facile, aujourd'hui, de s'octroyer une adresse e-mail sous une fausse identité ou pire encore de détourner une adresse e-mail existante. Le certificat électronique permet de s'identifier sur Internet, de protéger et de garantir les données transmises.

## ▪ Identifier

Le **certificat électronique** est une carte d'identité électronique, matérialisée sous forme de carte à puce ou de clé USB. Le **certificat électronique** permet de **s'identifier sur Internet**. Sa légitimité est liée à l'Autorité de Certification qui le génère et à l'Autorité d'Enregistrement qui le délivre.

## ▪ Protéger

Outre l'authentification de l'émetteur, le certificat permet d'assurer l'intégrité des documents échangés, avec l'assurance que le document reçu est identique au document initial (document Word, Excel...). Avec un logiciel de signature, ou une application intégrée à un portail, le certificat permet également de signer des documents d'un simple clic de souris.

## ▪ Garantir

Les documents signés par un certificat RGS \*\* ou 3+ (remis en face à face par une autorité légitime et sur un support cryptographique clé USB ou carte à puce) sont opposables au tiers, en vertu des lois et décrets sur la signature électronique.

# Un double certificat sur votre clé CertimétiersArtisanat

L'Etat impose un nouveau système de référencement des certificats électroniques. L'ensemble des acteurs se basant sur ce système de référencement effectuent donc actuellement les modifications nécessaires pour répondre aux nouvelles directives de l'Etat.

CertimétiersArtisanat utilise déjà ce système afin d'être à la pointe tant en termes technologiques que législatifs. Nous sommes donc d'ores et déjà en mesure de distribuer des clés ou cartes à puce munies de certificats conformes au RGS (Référentiel Général de Sécurité), le nouveau référentiel édicté par l'Etat.

Nous avons mis en place un double certificat dans votre support cryptographique afin de vous en faciliter l'utilisation quotidienne et de vous accompagner au mieux durant cette période de transition.

Le fonctionnement est très simple.

Votre certificat principal est un certificat **CERTIMETIERSARTISANT**. Il s'agit d'un certificat conforme au RGS.

Cependant, les applications nécessitant l'utilisation d'un certificat électronique (plateformes de réponse aux appels d'offre, SIV etc....) ne sont pas encore toutes en mesure d'accepter les certificats dits RGS\*\*.

Ainsi, votre support cryptographique contient également un certificat « Certeurope Classe 3+ » conforme à l'ancien référentiel : PRIS v1. Vous utiliserez ce certificat à chaque fois que l'utilisation de CERTIMETIERSARTISANAT n'est pas autorisée.

Pendant toute la période de transition, CertimétiersArtisanat vous offre donc la possibilité de vous connecter à la fois sur les plateformes à jour et les plateformes en cours de migration grâce à l'ajout d'un certificat PRIS v1 dans votre clé.

# Utilisation d'un certificat électronique classe 3+ ou rgs\*\*

## ▪ Dans l'entreprise

Sécuriser, Authentifier, Formaliser les échanges est essentiel pour toute entreprise qui utilise les outils Internet (Extranet, Intranet, messagerie...).

Le certificat électronique facilite la gestion du service commercial (catalogues en ligne, bons de commande, factures), des ressources humaines (dates de congés, notes de frais), et du juridique (contrats, convocations aux assemblées générales...).

En signant vos courriers (lettres, contrats, bons de commande, factures, propositions commerciales...) vous leur conférez une valeur probante, ils sont ainsi opposables au tiers.

## ▪ Dans les administrations

Les certificats CertimétiersArtisanat sont référencés par l'Administration et permettent l'accès aux télé-procédures administratives telles que :

- **Télé-TVA** : déclaration de TVA par Internet.
- **Impots.gouv.fr** : consultation du compte fiscal professionnel, paiement de l'IS et de la TS.
- **Déclarations sociales** : DUCS sur le site des URSSAF.
- **Net-entreprises.fr** : service officiel permettant aux entreprises d'effectuer en ligne leurs déclarations sociales : Urssaf, Assedic, retraite et retraites complémentaires.
- **SIV : Immatriculations** en ligne des véhicules automobiles et des deux roues et déclarations d'achat et de cession d'automobiles d'occasion.
- Candidatures aux **Appels d'offres des marchés publics**: dépôt électronique des candidatures.
- **Déclaration des Produits Biocides** par Internet.

- **Formalités en ligne des greffes des Tribunaux de Commerce :** déclarations en ligne des modifications du Registre du Commerce, requêtes en Injonctions de payer.

Vous trouverez la liste des plateformes et services certifiés compatibles avec votre certificat Certeurope sur le site [www.artisanat.fr](http://www.artisanat.fr) dans la rubrique service / signature électronique.

Avant de pouvoir effectuer vos télédéclarations, vous devez retirer un dossier d'inscription auprès de l'administration concernée.

**Pour toute information :**

le site web : [www.artisanat.fr](http://www.artisanat.fr),

la hotline : 0 899 700 046 (1,349 € TTC + 0,337 € TTC/min) ou par mail : [certimetiersartisanat@apcma.fr](mailto:certimetiersartisanat@apcma.fr)

# Points importants

## **Vous possédez bien les éléments suivants :**

- La (ou les) clé(s) USB CertimétiersArtisanat qui vous a (ont) été délivrée(s) par l’Autorité d’Enregistrement.
- Le (ou les) code(s) PIN, que vous avez reçu(s) par courrier postal, et qui vous permet d’activer votre (vos) clé(s)

Veillez-vous référer au tableau ci-dessous pour vérifier la compatibilité de votre système d’exploitation, votre navigateur et le certificat.

Version de Mac OS X	10.5.5 à 10.5.9 Leopard	10.6.0 à 10.6.2 et 10.6.4 Snow Leopard	10.6.5 à 10.6.6 Snow Leopard
Apple Safari			✓
Mozilla Firefox	✓	✓	✓

Pour un plus grand confort d’installation, nous recommandons Apple Safari pour les versions 10.6.5 et 10.6.6 de Mac OS X.

**NB :** Il est nécessaire de se connecter sous un compte avec les privilèges « administrateur » avant de commencer l’installation.

Si un administrateur procède à l’installation du pilote sur le poste, il est nécessaire qu’il l’effectue sur la cession de l’utilisateur et non sur sa cession administrateur.

Certains anti-virus empêchent le lancement du pilote d’installation. Dans le cas où une fenêtre vous alerte, veuillez désactiver votre anti-virus le temps de l’installation.



**Mise en garde**

Pour utiliser un service qui requiert un certificat sur Mac OS, il faut :

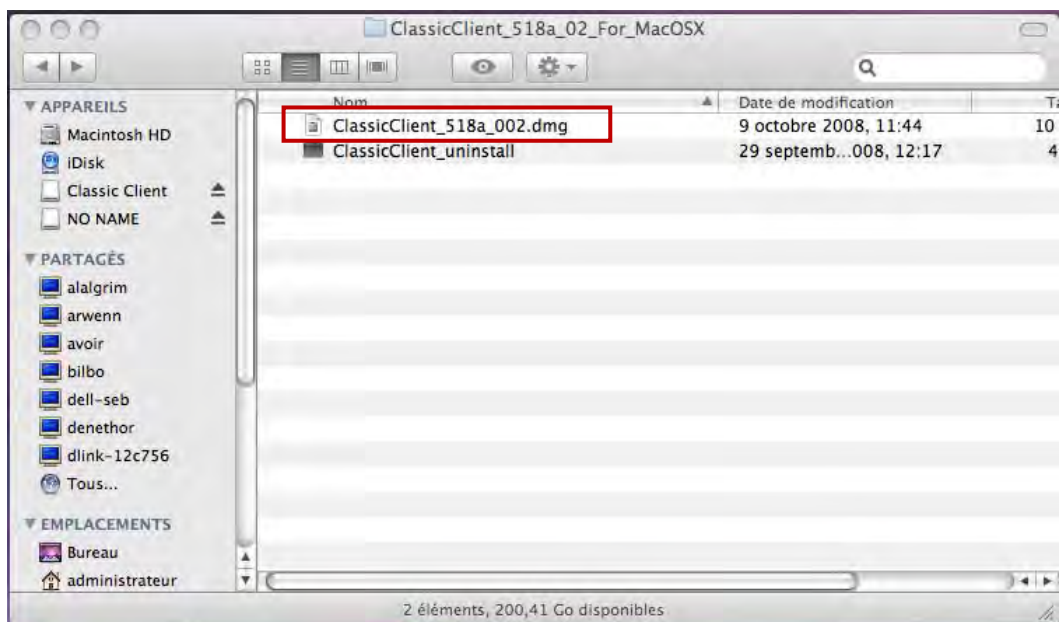
- Disposer des pilotes et les installer (cf. la présente documentation)
- Que le service soit compatible avec Mac OS.

# Installation des pilotes systèmes

- **Mac OS X 10.5.5 à 10.5.9 :**

Après avoir téléchargé le pilote sur votre ordinateur, double cliquez sur le pilote., puis double-cliquez sur le dossier **ClassicClient\_518a\_002.dmg** un dossier meta-installer se crée.

Double-cliquez sur ce dossier pour l'ouvrir



Double-cliquez sur **ClassicClient\_518a\_002.dmg**

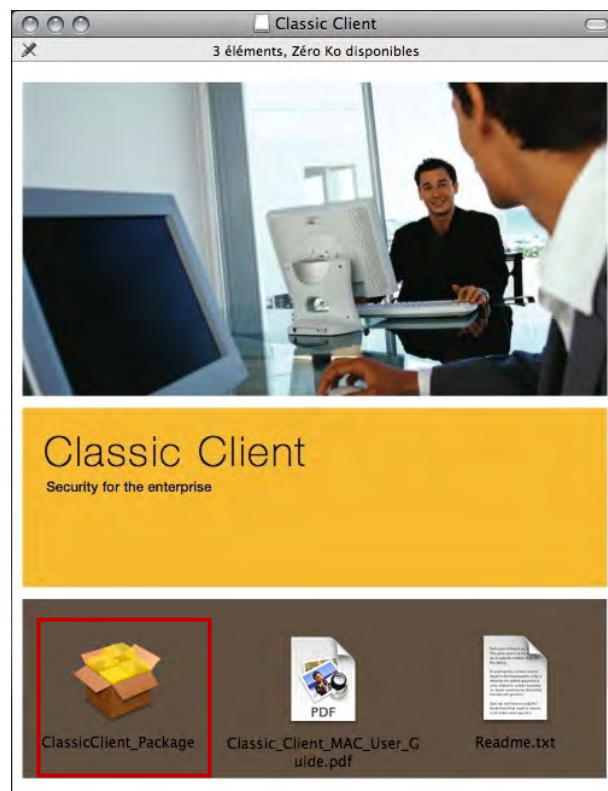
▪ **Mac OS X 10.6**

Après avoir téléchargé le pilote sur votre ordinateur, cliquez sur téléchargement et sélectionnez :

**Classic Client\_60\_SnowLeopard\_V2\_V3\_IAS.dmg**



**Pour les 2 versions :**



Cliquez sur **ClassicClient.pkg** ou **ClassicClient\_Package**

La fenêtre suivante n'apparaît que pour la version Mac OS X 10.5.5 à 10.5.9

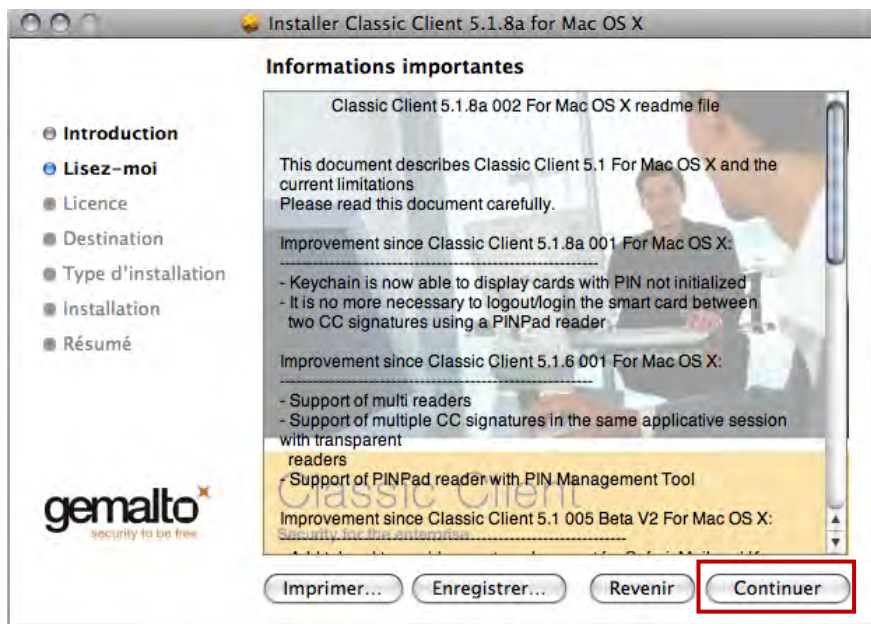


Cliquez sur **Continuer**

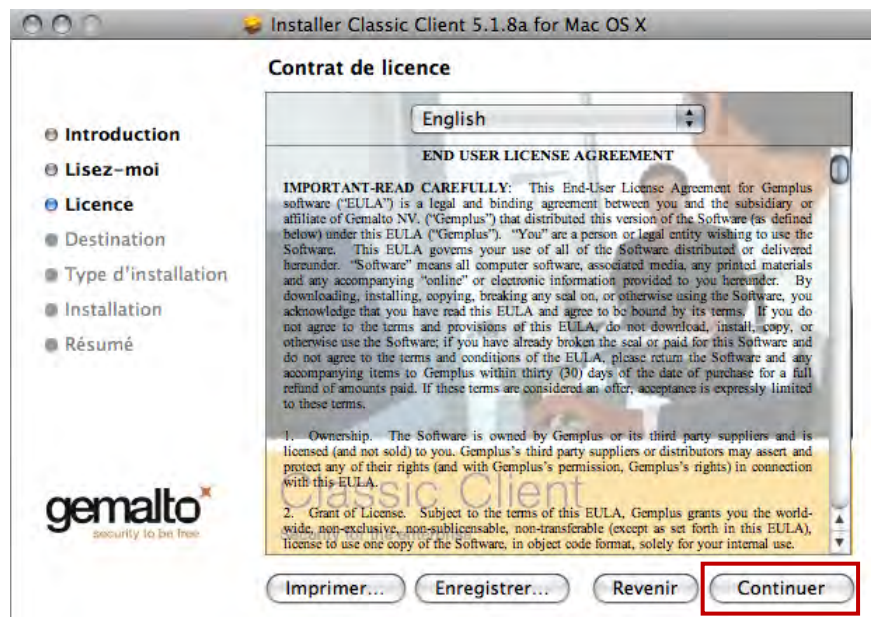


Cliquez sur **Continuer**

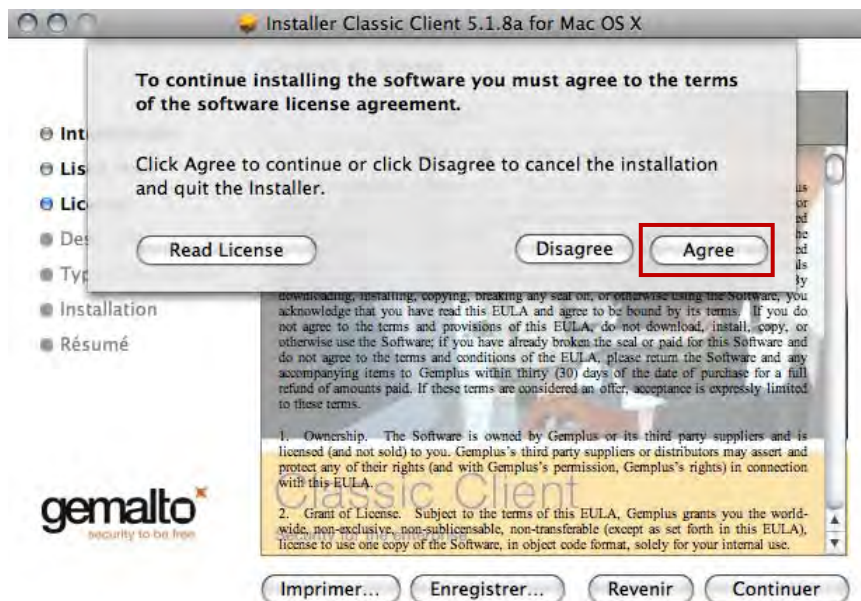
La fenêtre suivante n'apparaît que pour la version Mac OS X 10.5.5 à 10.5.9



Cliquez sur **Continuer**



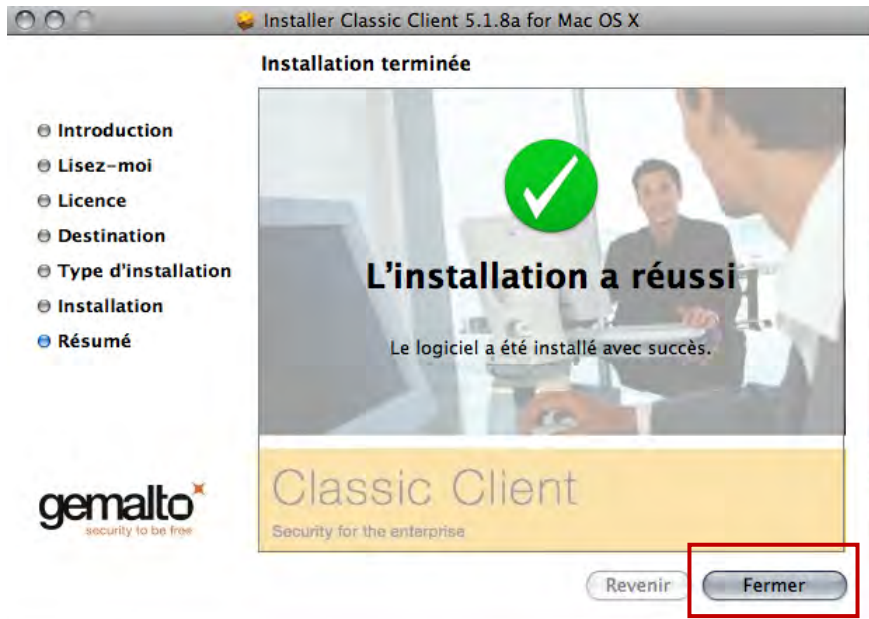
Cliquez sur **Continuer**



Cliquez sur **Agree** ou **Accepter**



Cliquez sur **Installer**



Cliquez sur **Fermer**

# Installation pour Apple Safari

Après l'installation du **ClassicClient\_Package** sur votre ordinateur, le certificat ne requiert pas d'installation supplémentaire.

Pour utiliser le certificat, il vous suffit d'insérez la clé cryptographique dans votre ordinateur et exécutez Safari.

# Installation pour Mozilla Firefox

Vous devez maintenant installer les Autorités de Confiance. Pour ce faire, vous devez d'abord **télécharger les certificats d'Autorité**, puis **les importer dans Firefox**.

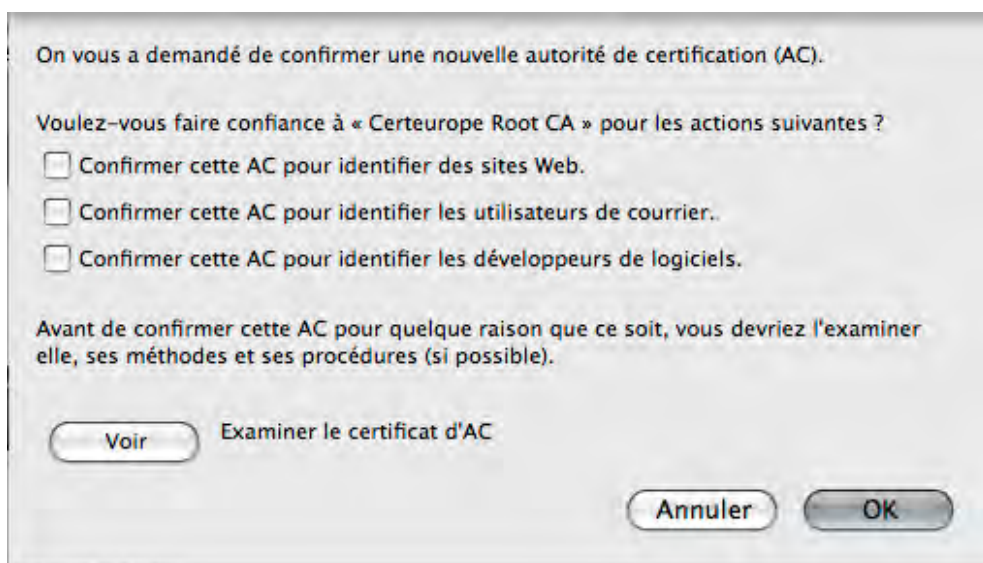
**Attention : n'insérez pas la clé avant cette étape !**

## ▪ 1 Installation de l'Autorité de Confiance AC Certeurope root CA

Pour installer le certificat de l'Autorité Racine, entrez dans la barre d'adresse de *Mozilla Firefox* l'url suivante :

[www.certeurope.fr/fichiers/certificats/certeurope\\_root\\_ca.crt](http://www.certeurope.fr/fichiers/certificats/certeurope_root_ca.crt) et cliquez sur Entrée

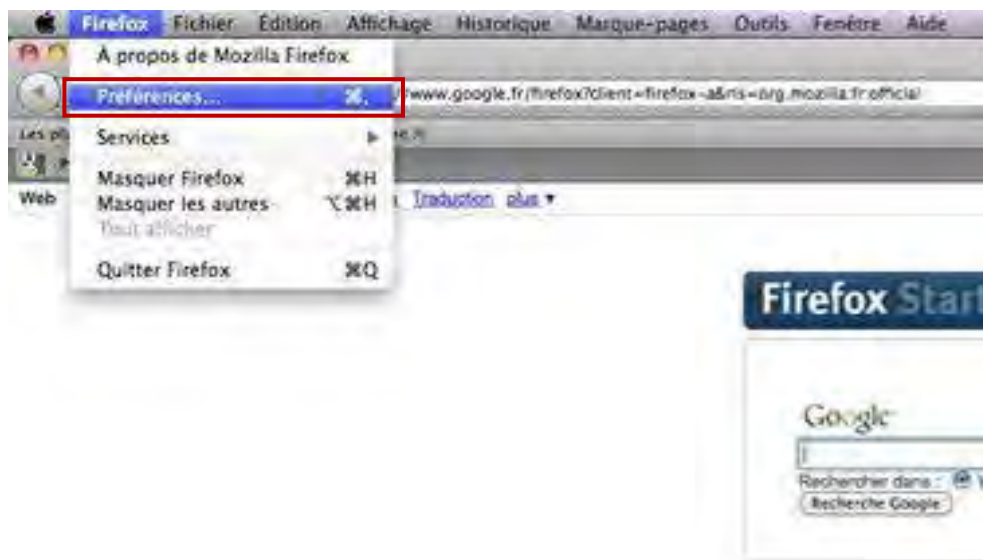
- Si la fenêtre suivante apparaît, cliquez sur **OK**



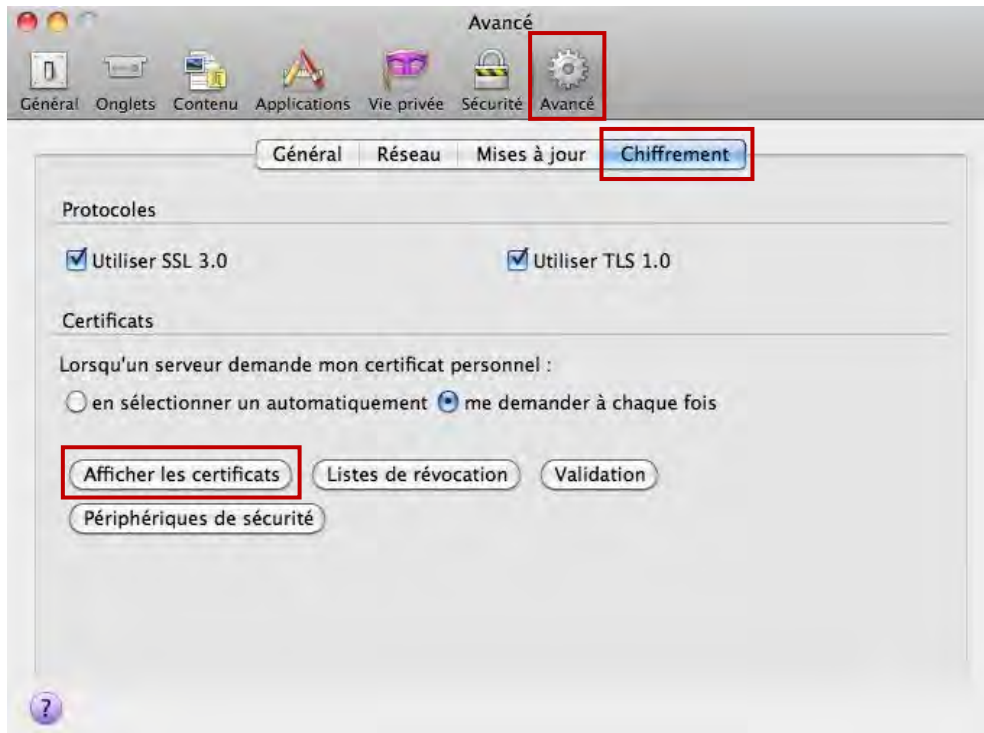
- Si la fenêtre suivante apparaît, suivez les étapes ci-dessous :



Cliquez sur **Enregistrer le fichier** (ou sélectionnez **Enregistrer le fichier** puis cliquez sur **OK**).

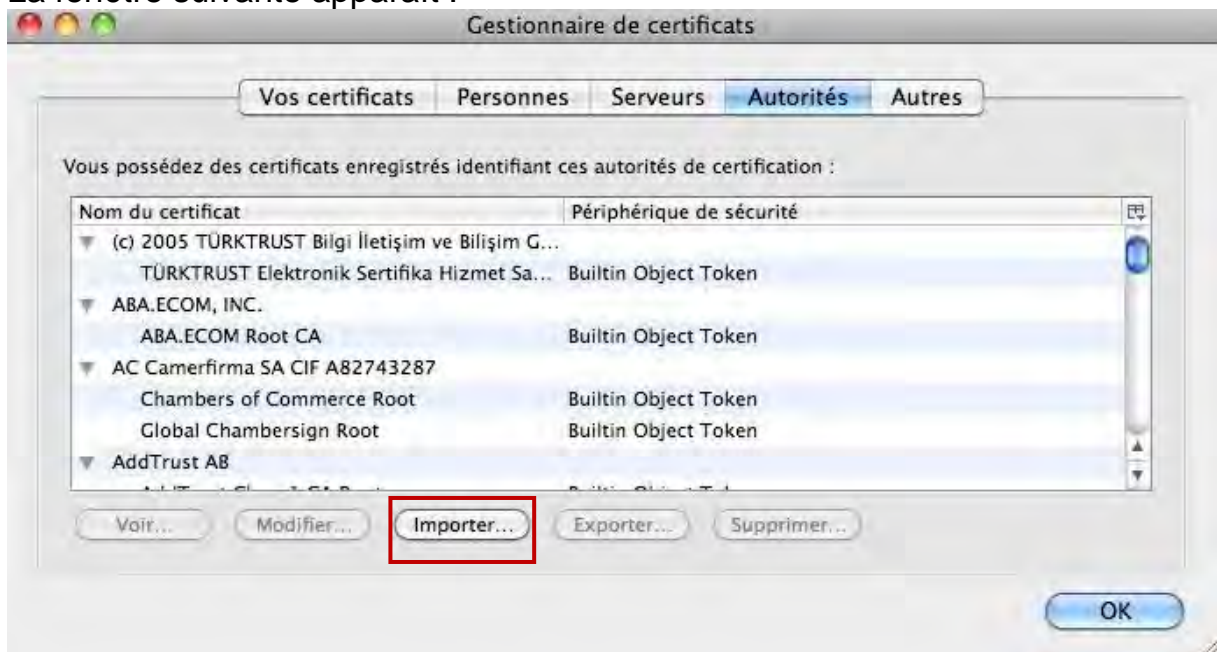


Une fois le téléchargement terminé, cliquez sur **Préférences** du menu **Firefox**

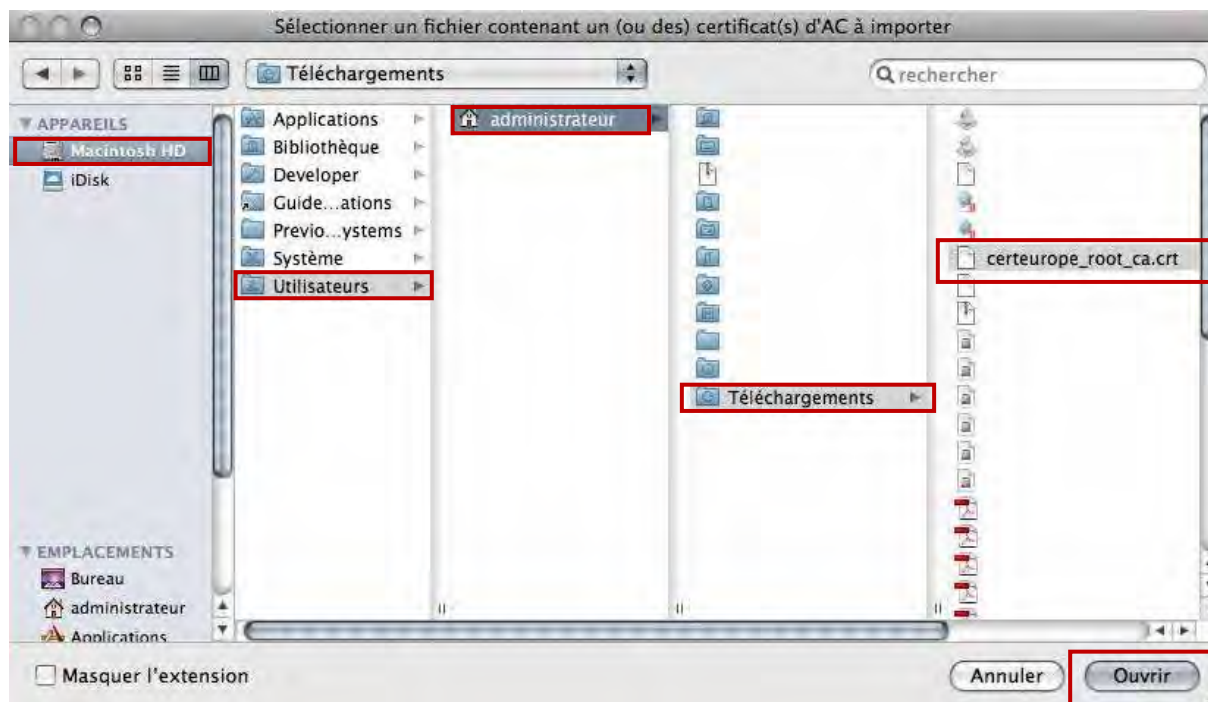


Dans l'onglet **Avancé**, cliquez sur l'onglet **Chiffrement** puis sur **Afficher les certificats**.

La fenêtre suivante apparaît :

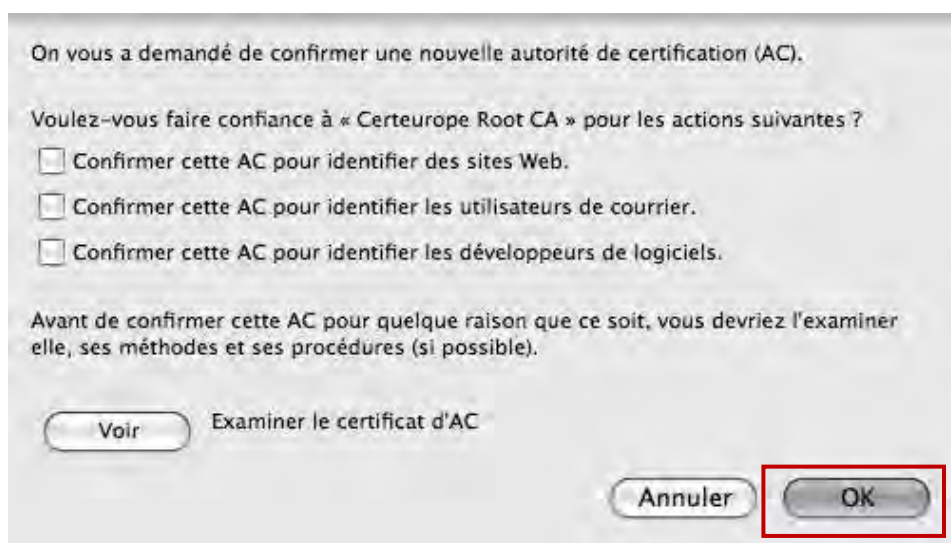


Cliquez sur **Importer**



Allez dans votre session : Macintosh HD → utilisateurs → nom de la session (ici Administrateur).

Dans téléchargement, sélectionnez le fichier **certeurope\_root\_ca**.  
Puis cliquez sur **Ouvrir**.



Cliquez sur **OK**.

### **Le Certificat de l'Autorité Racine est Importé dans Firefox.**

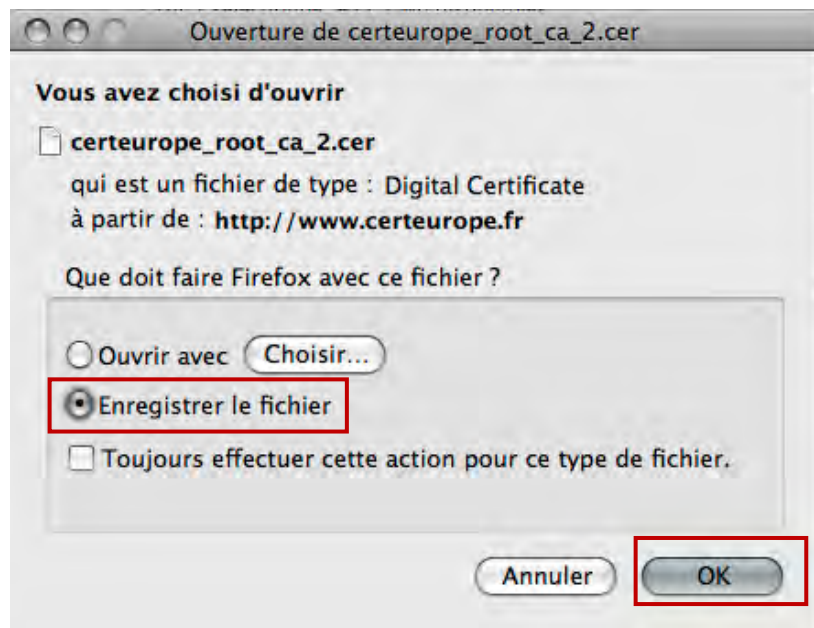
Veillez maintenant procéder à la même manipulation pour les certificats des Autorités ROOT CA V2, CERTEUROPE ADVANCED CA V3 et Certeurope Classe 3Plus v2.

## 2 Installation de l'Autorité de Confiance Racine ROOT CA V2

Pour installer le certificat de l'Autorité Certeurope ROOT CA V2, entrez dans la barre adresse de Mozilla Firefox l'url suivante :

[http://www.certeurope.fr/reference/certeurope\\_root\\_ca\\_2.cer](http://www.certeurope.fr/reference/certeurope_root_ca_2.cer) et cliquez sur Entrée

La fenêtre suivante apparaît :



Sélectionnez **Enregistrer le fichier** puis cliquez sur **OK**).

Téléchargez le certificat **certeurope\_root\_ca\_2** puis importez-le dans Firefox de la même manière que précédemment :

- enregistrez le fichier
- cliquez sur **Préférences** du menu **Firefox**
- dans l'onglet **Avancé**, cliquez sur l'onglet **Chiffrement** puis sur **Afficher les certificats**
- cliquez sur **Importer**
- allez dans votre session : Macintosh HD → utilisateurs → nom de la session. Dans téléchargement, sélectionnez le fichier **certeurope\_root\_ca\_2**
- cliquez sur **Ouvrir**.
- puis cliquez sur **OK**.

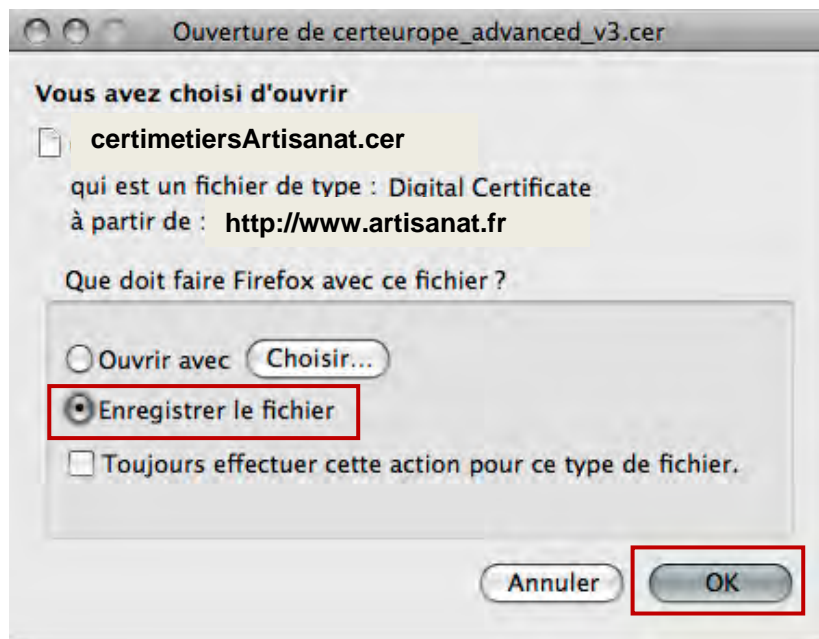
**Le Certificat de l'Autorité Racine ROOY CA V2 est Importé dans Firefox.**

### 3 Installation de l'Autorité de Confiance CERTIMETIERSARTISANAT

Pour installer le certificat de l'Autorité CertimétiersArtisanat, entrez dans la barre adresse de Mozilla Firefox l'url suivante :

<http://pc.certimetiersartisanat.fr/reference/certimetiersartisanat.crt>

Téléchargez le certificat certimetiersArtisanat puis importez-le dans Firefox de la même manière que précédemment.



Sélectionnez **Enregistrer le fichier** puis cliquez sur **OK**).

Téléchargez le certificat **certimetiersartisanat** puis importez-le dans Firefox de la même manière que précédemment :

- enregistrez le fichier
- cliquez sur **Préférences** du menu **Firefox**
- dans l'onglet **Avancé**, cliquez sur l'onglet **Chiffrement** puis sur **Afficher les certificats**
- cliquez sur **Importer**
- allez dans votre session : Macintosh HD → utilisateurs → nom de la session. Dans téléchargement, sélectionnez le fichier **certimetiersartisanat**
- cliquez sur **Ouvrir**.
- puis cliquez sur **OK**.

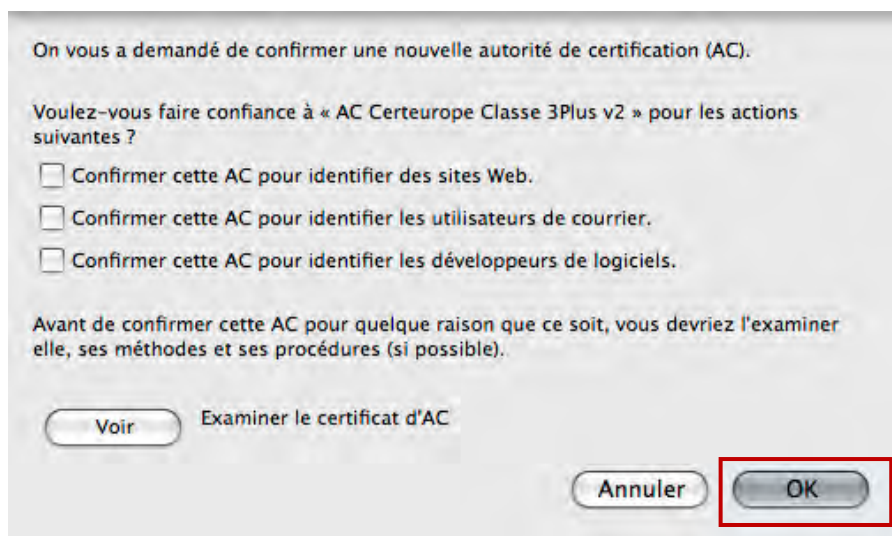
**Le Certificat de l'Autorité CERTIMETIERSARTISANAT est importé dans Firefox.**

#### ▪ 4 Installation de l'Autorité de Confiance AC Certeurope Classe 3Plus v2

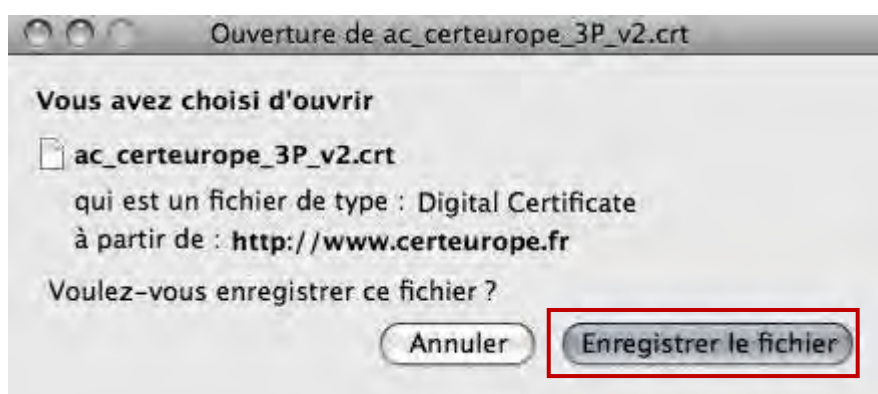
Pour installer le certificat de l'Autorité Certeurope Classe 3Plus v2, entrez dans la barre d'adresse de *Mozilla Firefox* l'url suivante :

[http://www.certeurope.fr/certificats2009/ac\\_certeurope\\_3P\\_v2.crt](http://www.certeurope.fr/certificats2009/ac_certeurope_3P_v2.crt) et cliquez sur Entrée

- Si la fenêtre suivante apparaît, cliquez sur **OK**



- Si la fenêtre suivante apparaît, suivez les étapes ci-dessous :



Cliquez sur **Enregistrer le fichier** (ou sélectionnez **Enregistrer le fichier** puis cliquez sur **OK**).

Téléchargez le certificat **ac\_certeurope\_classe\_3P\_v2** puis importez-le dans Firefox de la même manière que précédemment :

- enregistrez le fichier
- cliquez sur **Préférences** du menu **Firefox**
- dans l'onglet **Avancé**, cliquez sur l'onglet **Chiffrement** puis sur **Afficher les certificats**
- cliquez sur **Importer**
- allez dans votre session : Macintosh HD → utilisateurs → nom de la session. Dans téléchargement, sélectionnez le fichier **ac\_certeurope\_classe3P\_v2**.
- cliquez sur **Ouvrir**
- puis cliquez sur **OK**

**Le Certificat de l'Autorité Certeurope Classe 3Plus v2 est Importé dans Firefox.**

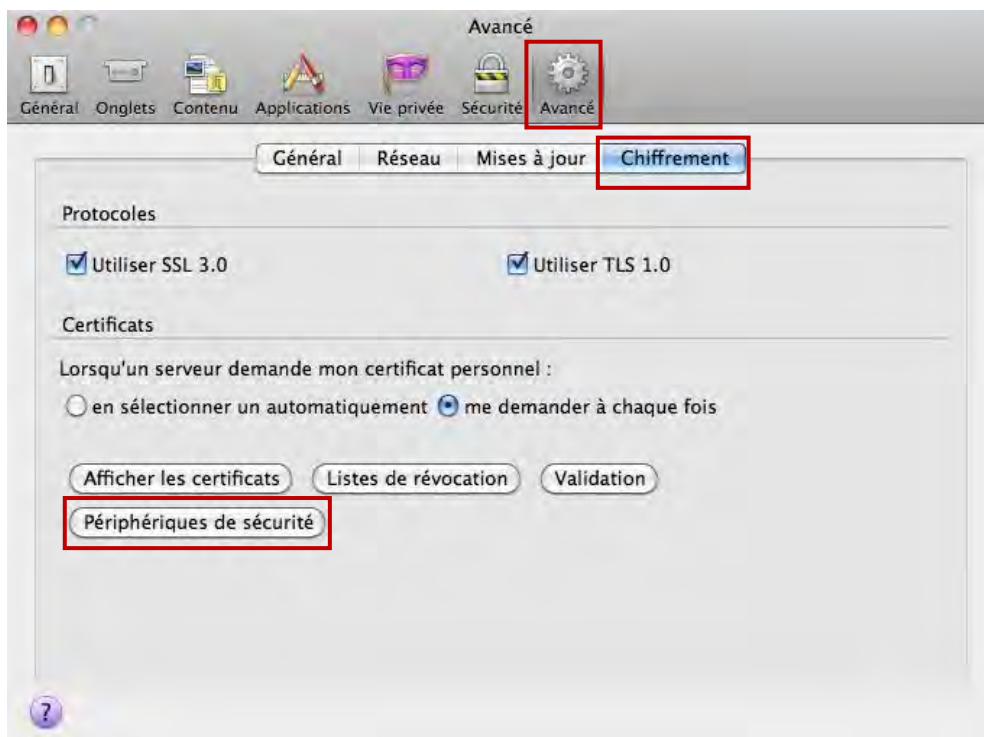
Quittez Firefox avant de le relancer dans l'étape suivante.

# Paramétrage Mozilla Firefox

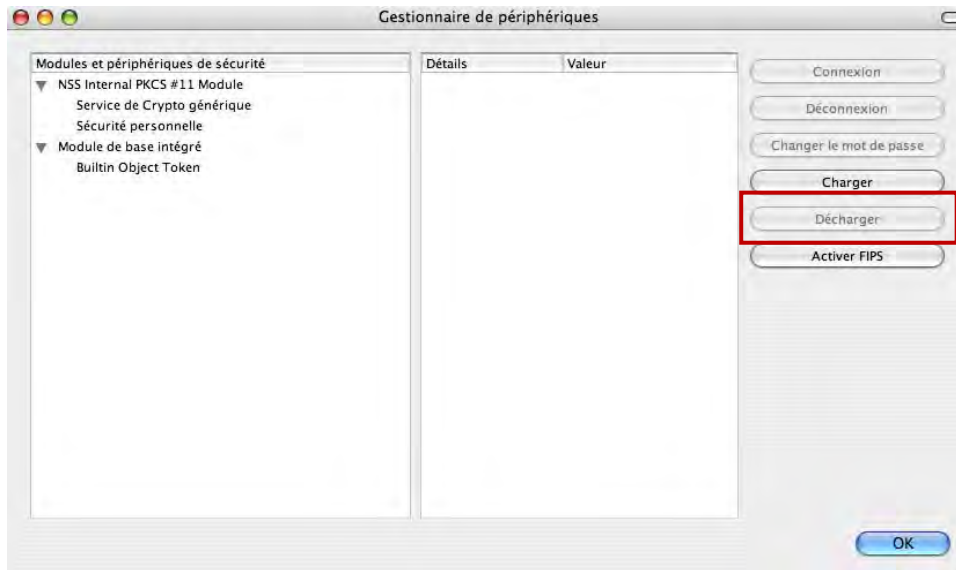
Il faut maintenant préciser à Firefox qu'il y a une clé cryptographique et quel est son pilote

Insérez la clé dans un port USB de votre machine.

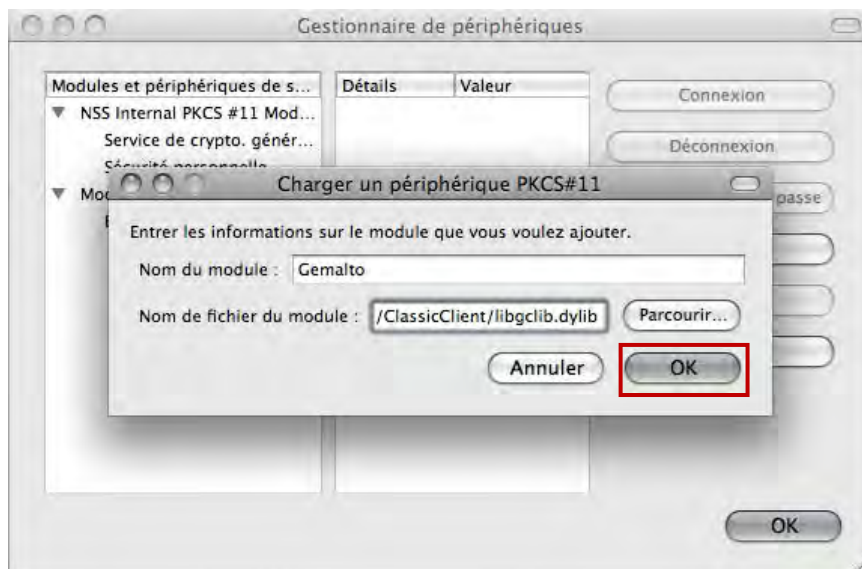
Lancez Firefox. Dans le menu **Firefox** cliquez sur **Préférences**.



Dans l'onglet **Chiffrement** du menu **Avancé** cliquez sur **Périphériques de Sécurité**



Cliquez sur **Charger** pour définir le nouveau dispositif

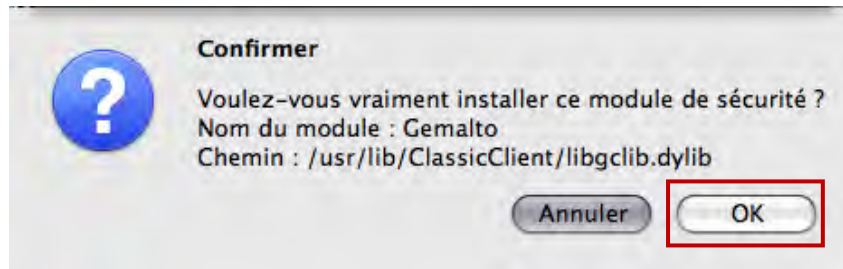


Saisissez le nom du Module : **Gemalto**

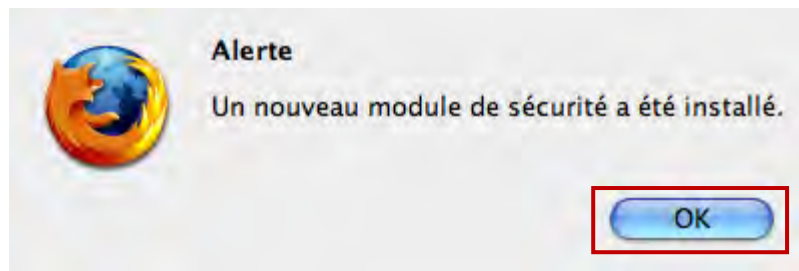
Saisissez **manuellement** le nom du fichier du module (le pilote)  
**/usr/lib/ClassicClient/libgclib.dylib**

Cliquez sur **OK**

*Les deux fenêtres suivantes n'apparaissent que pour la version Mac OS X 10.5.5 à 10.5.9*



Cliquez sur **OK**



Cliquez sur **OK**



Votre certificat est installé

**Attention** : Quittez Firefox puis redémarrez l'ordinateur.

# Test de bon fonctionnement

Après le redémarrage de votre ordinateur, lancez votre navigateur (Safari ou Firefox) et entrez dans la barre d'adresse <https://services.certeurope.fr>

Une fenêtre vous demande de saisir votre code PIN ou mot de passe principal (code PIN du courrier).

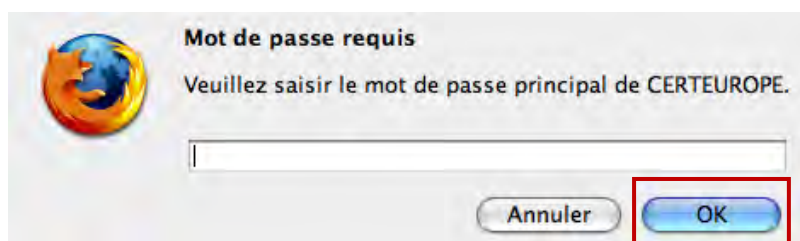
Si le code PIN a été changé c'est le dernier code enregistré qui doit être pris en compte.

## Pour Apple Safari :

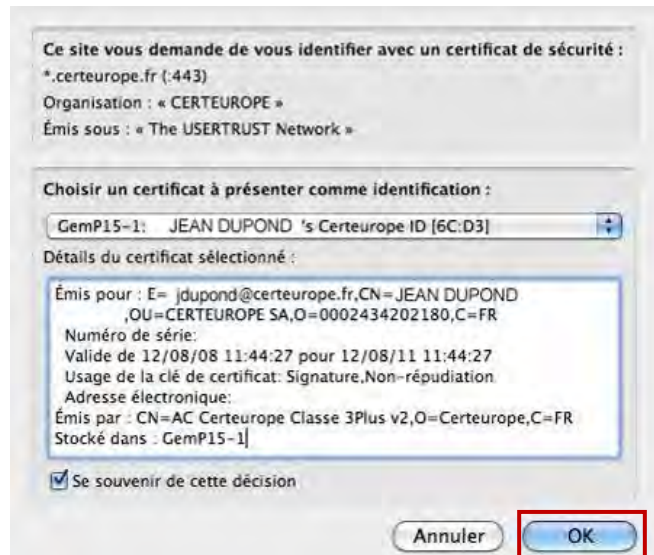


Cliquez sur **OK**

## Pour Mozilla Firefox :



Après l'avoir saisi, sélectionnez votre certificat.



Cliquez sur **OK**

Vous voici sur la page **Certiservices**.

Bonjour <b>JEAN DUPONT</b> Votre certificat est <b>valide</b> . Il expire le <b>30/03/2013</b> Informations sur votre certificat	Vous avez un code de déblocage (PUK). Voir votre Code de Déblocage	Vous n'avez pas défini de Code de Révocation d'Urgence Définir un code de révocation
 <b>CertEurope</b> Opérateur de Services de e-Confiance	<b>CERTISERVICES</b> Connecté: JEAN DUPONT	 <b>CertEurope</b> Opérateur de Services de e-Confiance
<b>Informations sur le certificat</b> Vous trouverez sur cette page le détail de votre certificat et le lien de téléchargement de votre certificat (notamment utile pour l'inscription au Service d'Immatriculation des Véhicules).	<b>Code PUK</b> Le code PUK ou code de déblocage permet de débloquent votre certificat si ce dernier est bloqué suite à 3 saisies d'un mauvais code PIN. <b>Le code PUK n'est délivré qu'une seule fois</b> , notez-le et conservez-le précieusement. Pour retirer votre code PUK, cliquez sur le bouton « Retirer votre code de déblocage » en haut et au centre de la page CertiService.	<b>Révocation</b> <b>Choisir ou modifier votre code de Révocation d'Urgence (CRU):</b> Ce code vous servira à révoquer votre certificat en cas de perte ou de vol de votre clé. Ce code vous est strictement confidentiel, nous serons dans l'impossibilité de vous le communiquer en cas d'oubli. Assurez-vous donc de choisir un code de 6 à 8 caractères que vous n'oublierez pas. Pour renseigner votre CRU cliquer ici. Pour révoquer votre certificat, munissez vous de votre CRU et contactez le numéro de téléphone suivant: <b>+33 (0) 826 300 412</b> (disponible 24H/24 - 7J/7). <b>Révoquer votre certificat en ligne:</b> Vous quittez votre société ou n'êtes plus amené à utiliser votre certificat. Vous pouvez le révoquer depuis cette page.
CertiServices - ©CertEurope - mentions légales		

Votre certificat est valide et installé

**VOUS DEVEZ A CETTE OCCASION ENREGISTRER VOTRE CODE DE REVOCATION D'URGENCE (CRU)**

# Révocation d'Urgence

## ▪ Saisie de votre Code de Révocation d'Urgence

Votre certificat a une durée de validité de 3 ans, cependant, il peut arriver que vous soyez amené à demander sa révocation dans différentes situations :

- Perte de votre clé USB
- Oubli de votre code PIN ou blocage de votre certificat
- Départ de la personne abonnée au sein de l'entreprise (démission, mutation, licenciement,...)

Si votre clé contient 2 certificats, vous avez la possibilité d'enregistrer un CRU, identique ou différent, pour chacun des certificats. Il faudra alors associer le bon CRU au bon certificat.

**Sachez cependant que la révocation d'un des certificats entraîne systématiquement la révocation de l'autre.**

Connectez-vous au site CertiService (<https://services.certeurope.fr/>) en sélectionnant le certificat pour lequel vous souhaitez définir le Code de Révocation d'Urgence (CRU). Puis entrez votre code PIN. Vous êtes alors authentifié sur la page CertiService.

Cliquez sur définir un code de révocation en bas à droite de la page puis suivez les indications données.

<p>Bonjour <b>JEAN DUPONT</b>          Votre certificat est <b>valide</b>          Il expire le <b>30/03/2013</b>          Informations sur votre certificat</p>	<p>Vous avez un code de déblocage (PUK).          Voir votre Code de Déblocage</p>	<p>Vous n'avez pas défini de Code de Révocation d'Urgence          Définir un code de révocation</p>
 <b>CertEurope</b> Opérateur de Services de e-Confiance  <b>CertEurope</b> Opérateur de Services de e-Confiance		
<p><b>Informations sur le certificat</b></p> <p>Vous trouverez sur cette page le détail de votre certificat et le lien de téléchargement de votre certificat (notamment utile pour l'inscription au Service d'Immatriculation des Véhicules).</p>	<p><b>Code PUK</b></p> <p>Le code PUK ou code de déblocage permet de débloquent votre certificat si ce dernier est bloqué suite à 3 saisies d'un mauvais code PIN. <b>Le code PUK n'est délivré qu'une seule fois</b>, notez-le et conservez-le précieusement. Pour retirer votre code PUK, cliquez sur le bouton « Retirer votre code de déblocage » en haut et au centre de la page CertiService.</p>	<p><b>Révocation</b></p> <p><b>Choisir ou modifier votre code de Révocation d'Urgence (CRU):</b></p> <p>Ce code vous servira à révoquer votre certificat en cas de perte ou de vol de votre clé. Ce code vous est strictement confidentiel, nous serons dans l'impossibilité de vous le communiquer en cas d'oubli. Assurez-vous donc de choisir un code de 6 à 8 caractères que vous n'oublierez pas.</p>

Ce code est strictement confidentiel, et nous serons dans l'impossibilité de vous le communiquer en cas d'oubli. Assurez-vous donc de choisir un code de 6 à 8 caractères que vous n'oublierez pas !

*A savoir :* dès la génération de votre certificat, le représentant légal ainsi que le mandataire de certification reçoivent chacun leur code de révocation d'urgence leur permettant de révoquer votre certificat si nécessaire.

▪ **Révocation d'Urgence**

Pour révoquer votre certificat, 2 possibilités :

- munissez-vous de votre Code de Révocation d'Urgence et contactez le numéro de téléphone suivant : **+33 (0)826 300 412** disponible 24h/24 et 7j/7 (0,15 € TTC/min)
- connectez-vous sur <https://services2.certeurope.fr/revocation> et suivez les indications données

## Changement du code pin

Dès réception de votre code secret par courrier, il vous est conseillé de le changer pour des raisons de sécurité.

**Attention, au bout de 3 mauvaises saisies du code PIN, votre clé sera bloquée.**

Insérez votre clé et lancez le programme Classic Client PIN Management :  
Applications → Gemalto → Classic Client PIN Management.



Dans l'onglet **Change PIN**, notez votre ancien code PIN à droite du champ Old PIN Code.

Indiquez un nouveau code PIN (New PIN Code) et confirmez-le (Confirm User PIN).

Puis cliquez sur **Change PIN**.

Votre code secret a été changé.









***Chambres de Métiers  
et de l'Artisanat***

*Assemblée Permanente*

**ASSEMBLÉE PERMANENTE DES CHAMBRES DE MÉTIERS**

12, avenue Marceau - 78008 Paris - Tél. : +33 1 44 43 10 00 - Télécopie. : +33 1 47 20 34 48  
Internet : [www.artisanat.fr](http://www.artisanat.fr) - Courriel : [certimetiersartisanat@apcma.fr](mailto:certimetiersartisanat@apcma.fr)