

CERTIFICATS ELECTRONIQUES SUR CLE USB

C@RTEUROPE



MANUEL D'INSTALLATION MAC OS X :

**Versions 10.5.5 à 10.5.9 / 10.6 / 10.7 et 10.7.3
MOZILLA FIREFOX**

**Versions 10.6.5 à 10.6.7 / 10.7 et 10.7.3
APPLE SAFARI**

V.03/12

SOMMAIRE

NOTIONS SUR LE CERTIFICAT	3
UN DOUBLE CERTIFICAT SUR VOTRE CLE C@RTEUROPE	4
UTILISATION D'UN CERTIFICAT ELECTRONIQUE CLASSE 3+ OU RGS**	5
PRE-REQUIS TECHNIQUES.....	6
TELECHARGEMENT DES PILOTES	7
INSTALLATION DES PILOTES SYSTEMES	8
INSTALLATION POUR APPLE SAFARI	13
INSTALLATION POUR MOZILLA FIREFOX.....	14
1 INSTALLATION DE L'AUTORITE DE CONFIANCE AC CERTEUROPE ROOT CA.....	14
2 INSTALLATION DE L'AUTORITE DE CONFIANCE RACINE ROOT CA V2	18
3 INSTALLATION DE L'AUTORITE DE CONFIANCE CERTEUROPE ADVANCED CA V3	19
4 INSTALLATION DE L'AUTORITE DE CONFIANCE AC CERTEUROPE CLASSE 3PLUS V2.....	20
PARAMETRAGE MOZILLA FIREFOX	22
TEST DE BON FONCTIONNEMENT.....	25
REVOCATION D'URGENCE	27
CODE PUK (CODE DE DEBLOCAGE)	28
CHANGEMENT DU CODE PIN	31

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 CLE C@RTEUROPE

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. CertEurope s'est adapté très rapidement 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 **CERTEUROPE ADVANCED CA V3**. 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 « Certeuropa Classe 3+ » conforme à l'ancien référentiel : PRIS v1. Vous utiliserez ce certificat à chaque fois que l'utilisation de CERTEUROPE ADVANCED CA V3 n'est pas autorisée.

Pendant toute la période de transition, CertEurope 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.

Dans l'attente de l'arrêté officiel sur le RGS, il est impératif de signer vos réponses pour les appels d'offres des marchés publics avec le certificat « AC Certeuropa Classe 3 Plus V2 » ou « AC Certigreffe Classe 3 plus V2 » le cas échéant.

UTILISATION D'UN CERTIFICAT ELECTRONIQUE 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 C@rteurope (CERTEUROPE ADVANCED CA V3, Certeurope Classe 3+) 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 les certificats opérés par CertEurope sur le site www.certeurope.fr

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.certeurope.fr,
- la hotline : 0 899 700 046 (1,349 € TTC + 0,337 €TTC/min) ou par mail : support@certeurope.fr

PRE-REQUIS TECHNIQUES

Vous possédez bien les éléments suivants :

- La (ou les) clé(s) USB C@rteurope 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 10.6.7 Snow Leopard	10.6.8 Snow Leopard	10.7 et 10.7.3 Lion
Apple Safari			✓		✓
Mozilla Firefox	✓	✓	✓	✓	✓

*Uniquement pour les clés générées avant le 01/01/2012.

Pour un plus grand confort d'installation, nous recommandons Apple Safari pour les versions de Mac OS X compatibles.

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.

TELECHARGEMENT DES PILOTES

Pour télécharger les kits d'installations (aussi appelés pilotes) nécessaires au fonctionnement du certificat, veuillez vous rendre sur le site www.certeurope.fr dans la rubrique : Accès Direct.

Les informations suivantes sont nécessaires au téléchargement :

L'identifiant : **certeurope**

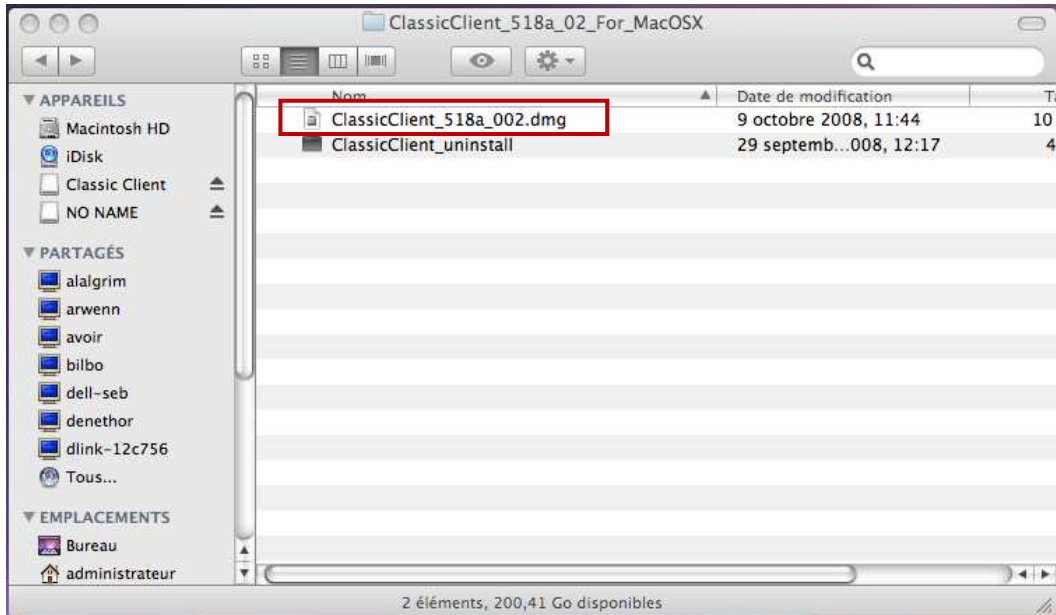
Mot de passe : **gemalto36**

INSTALLATION DES PILOTES SYSTEMES

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 et 10.7 : Après avoir téléchargé le pilote sur votre ordinateur, cliquez sur téléchargement et sélectionnez **Classic Client_60_SnowLeopard_V2_V3_IAS.dmg** ou **ClassicClient_610_Lion_V2.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

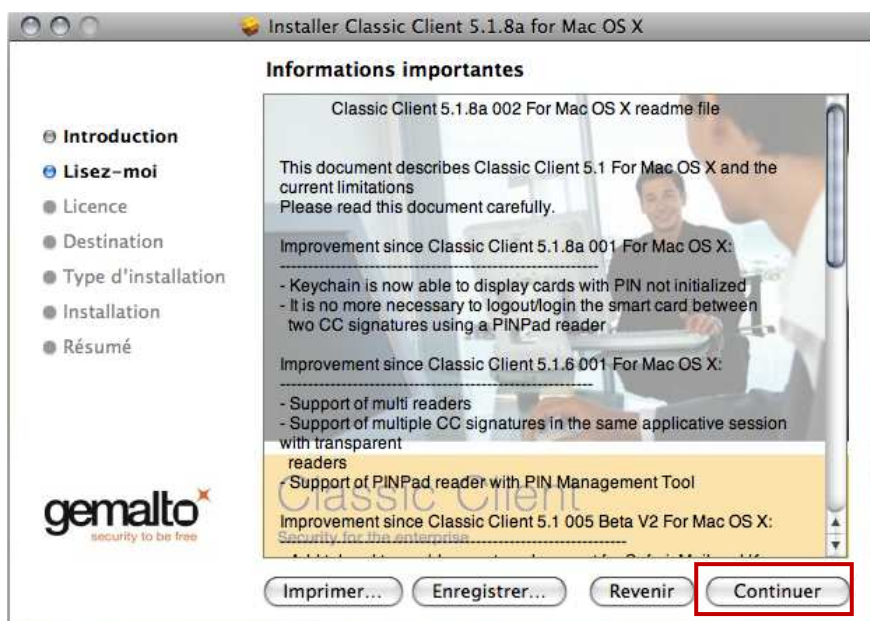


Cliquez sur **Continuer**

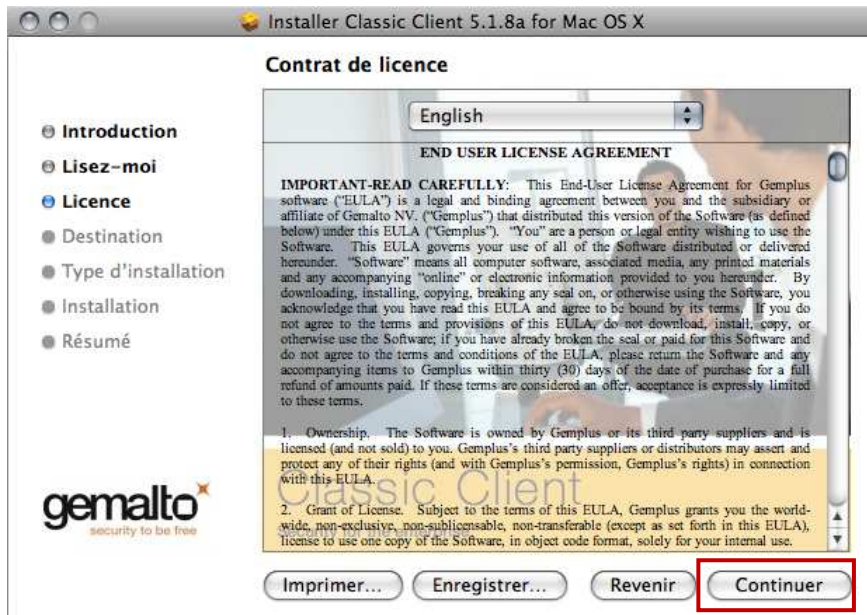


Cliquez sur **Continuer**

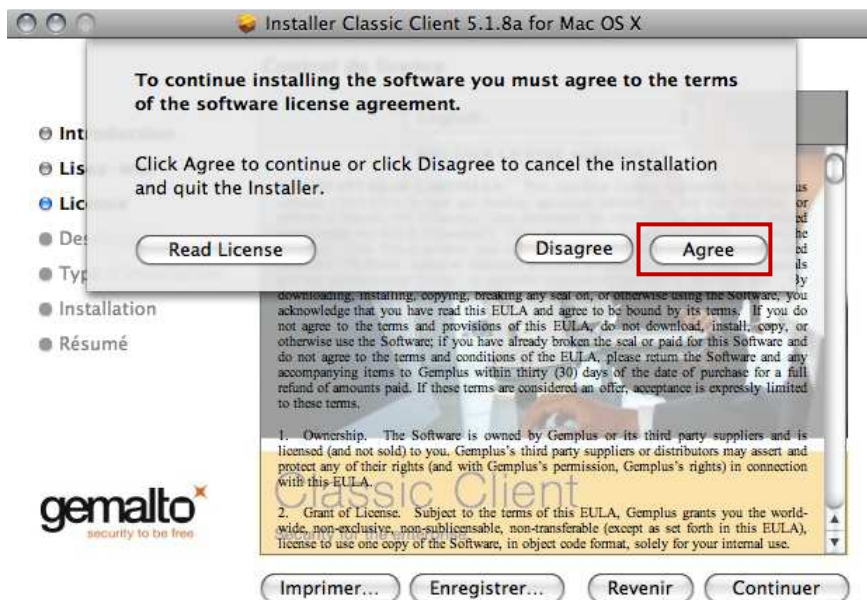
La fenêtre suivante n'apparaît que pour la version Mac OS X 10.5.5 à 10.5.9



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'insérer 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**.

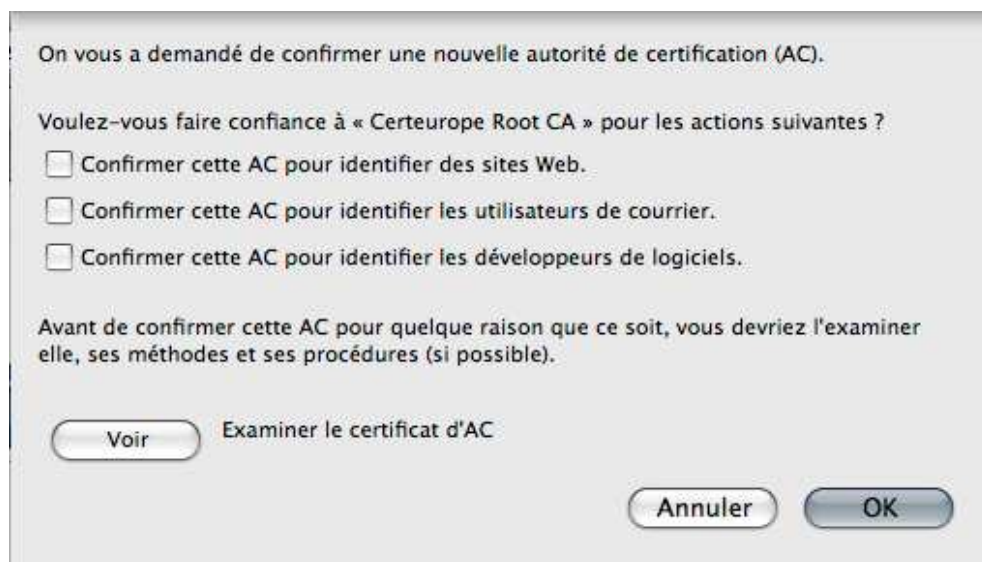
Attention : n'insérez pas la clé avant cette étape !

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 et cliquez sur Entrée

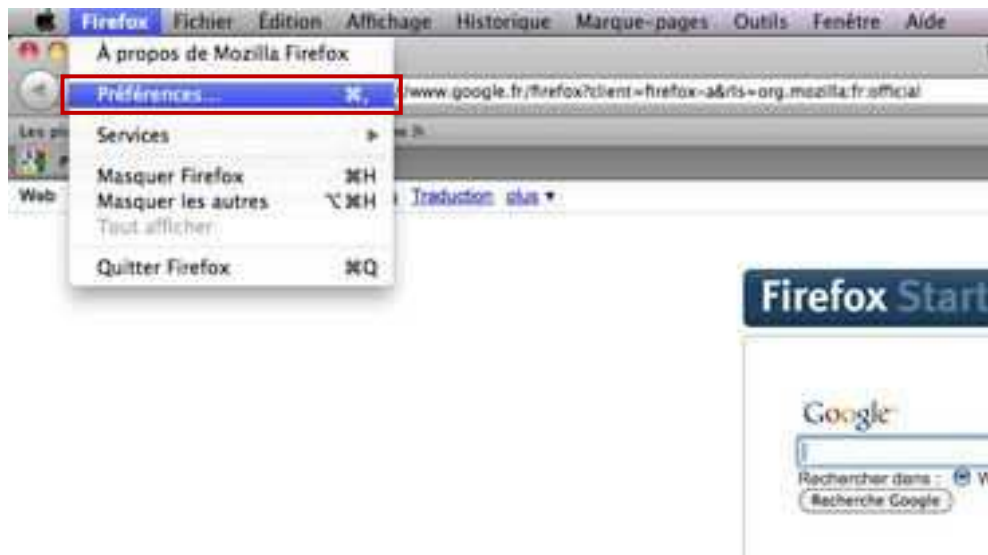
- Si la fenêtre suivante apparaît, cliquez sur **OK**



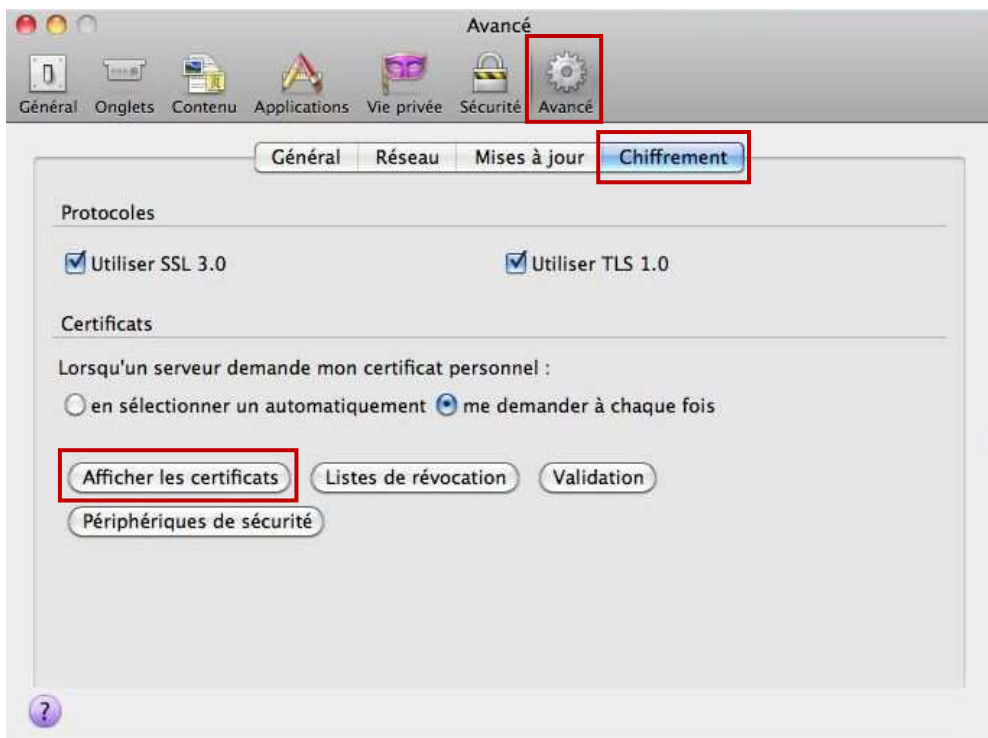
- Si la fenêtre suivante apparaît, suivez les étapes ci-dessous :



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

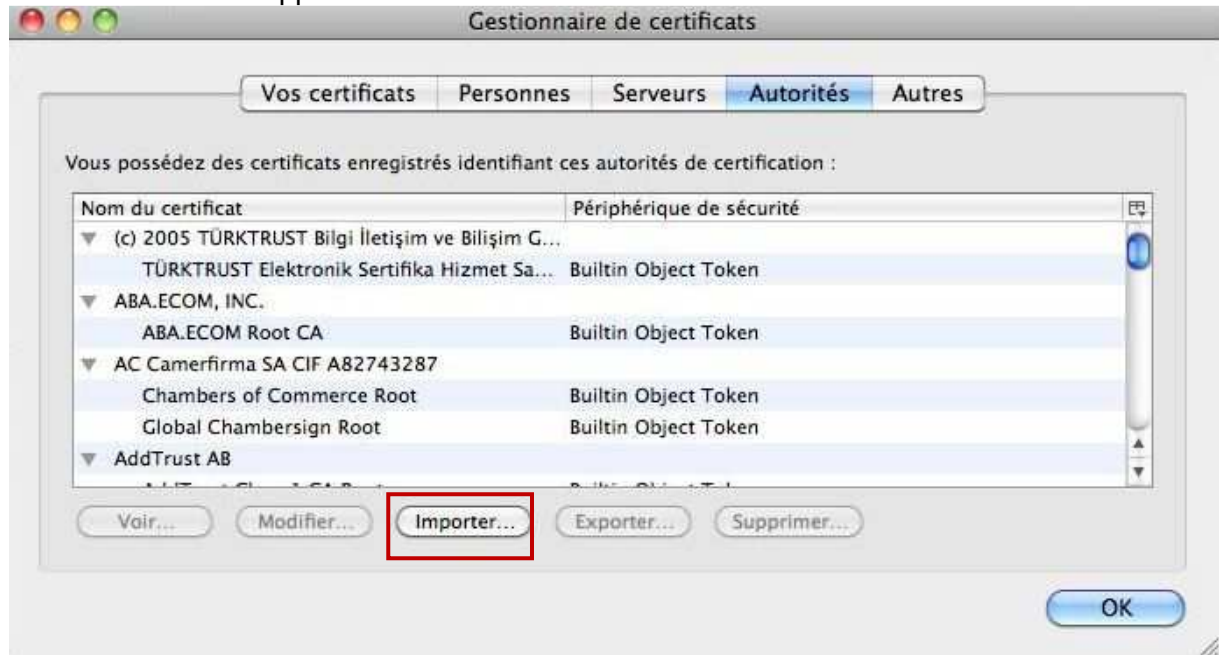


Une fois le téléchargement terminé, cliquez sur **Préférences** du menu **Firefox**

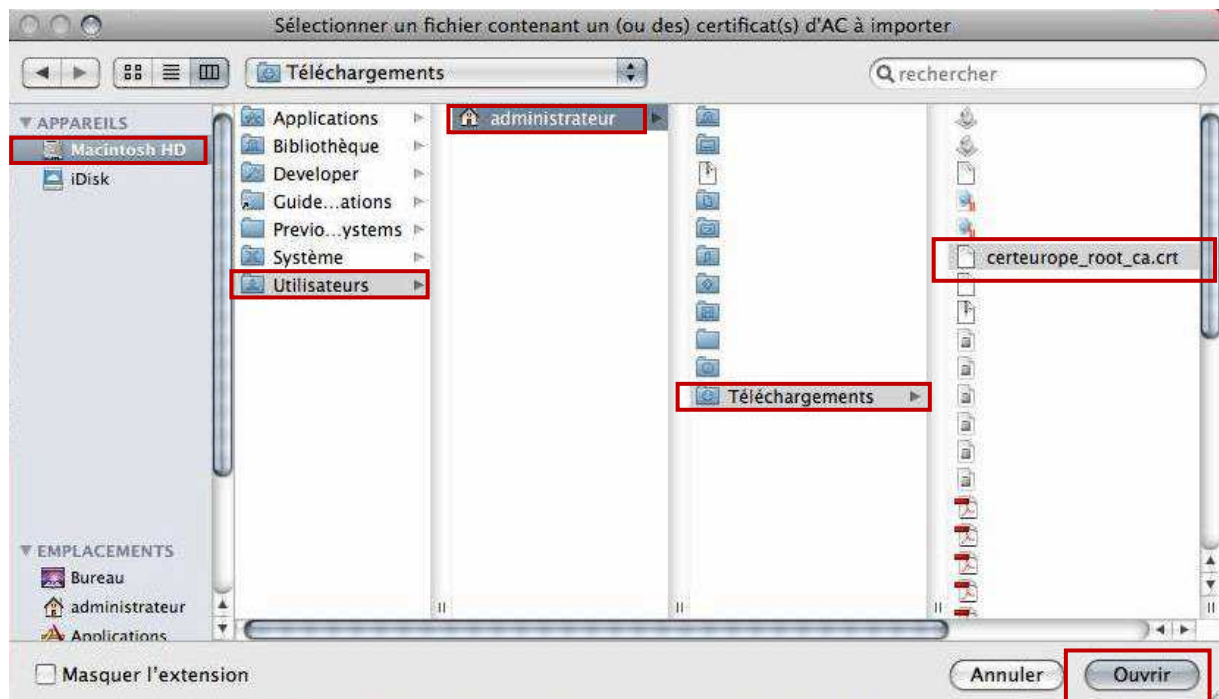


Dans l'onglet **Avancé**, cliquez sur l'onglet **Chiffrement** puis sur **Afficher les certificats**.

La fenêtre suivante apparaît :



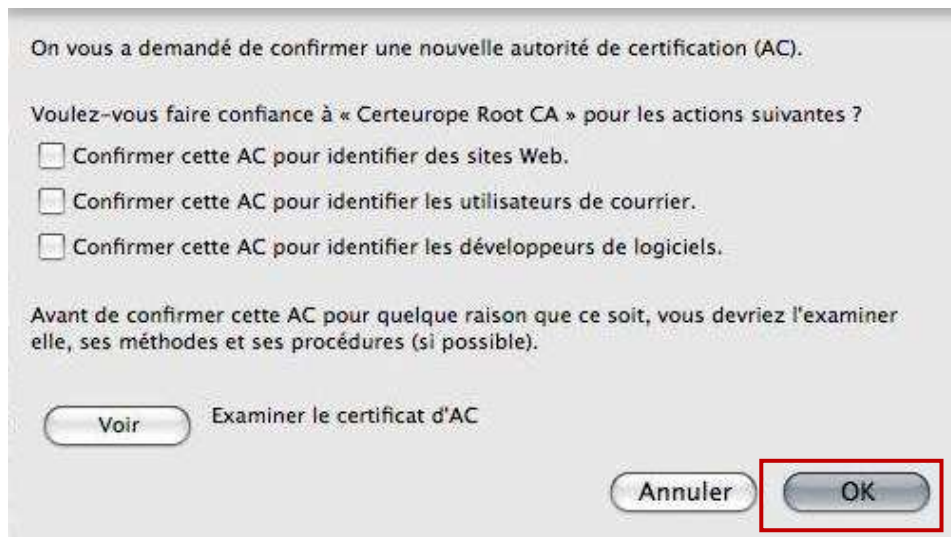
Cliquez sur **Importer**



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.

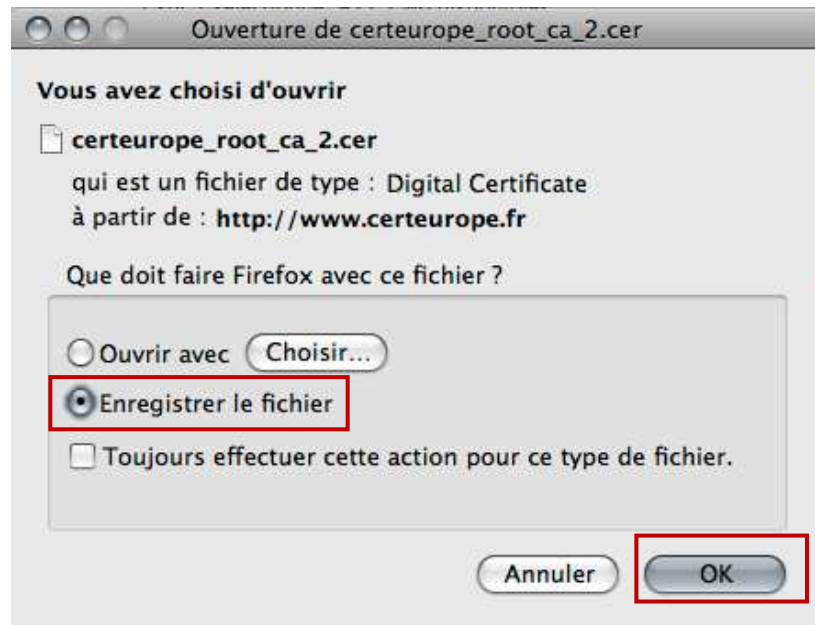
Veillez maintenant procéder à la même manipulation pour les certificats des Autorités ROOT CA V2, CERTEUROPE ADVANCED CA V3 et Certeurope Classe 3Plus v2.

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/referance/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**.

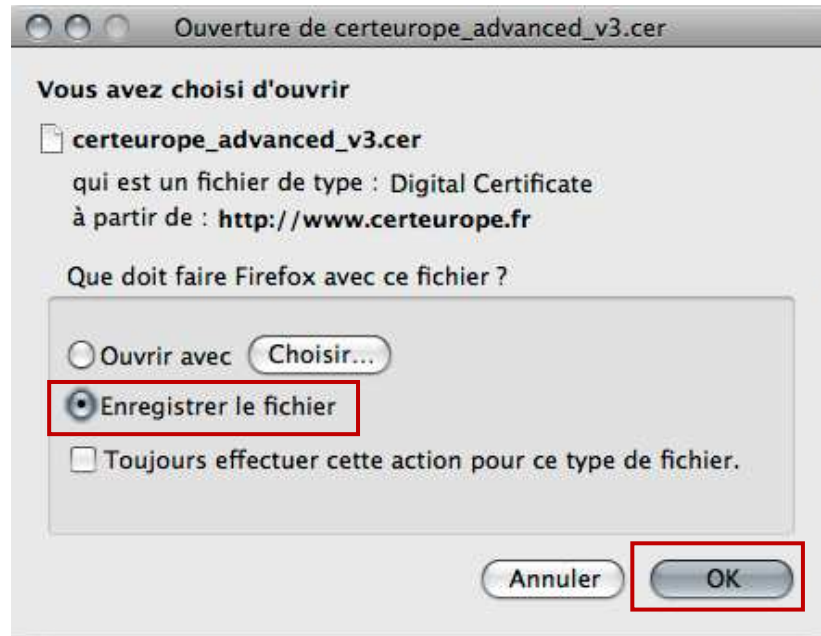
Le Certificat de l'Autorité Racine ROOY CA V2 est Importé dans Firefox.

3 Installation de l'Autorité de Confiance CERTEUROPE ADVANCED CA V3

Pour installer le certificat de l'Autorité CERTEUROPE ADVANCED CA V3, entrez dans la barre adresse de Mozilla Firefox l'url suivante :

http://www.certeurope.fr/reference/certeurope_advanced_v3.cer et cliquez sur Entrée

La fenêtre suivante apparaît :



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

Téléchargez le certificat **certeurope_advanced_v3** 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_advanced_v3**
- cliquez sur **Ouvrir**.
- puis cliquez sur **OK**.

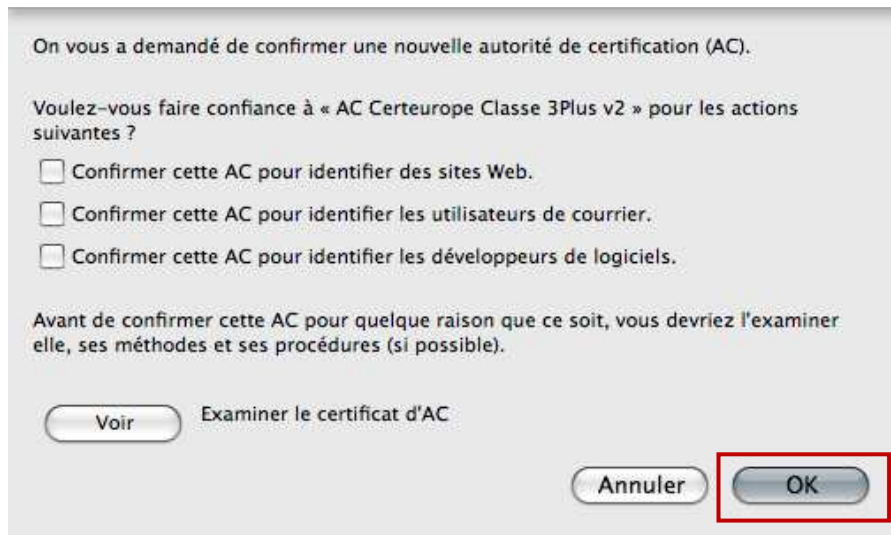
Le Certificat de l'Autorité CERTEUROPE ADVANCED CA V3 est importé dans Firefox.

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 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.

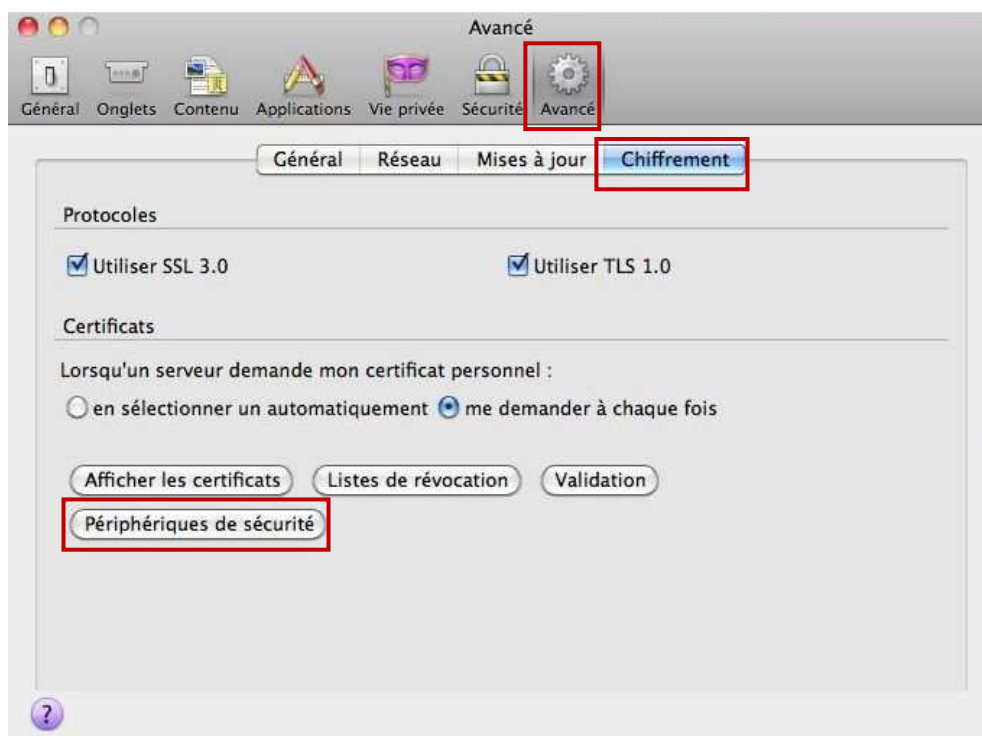
Quittez Firefox avant de le relancer dans l'étape suivante.

PARAMETRAGE MOZILLA FIREFOX

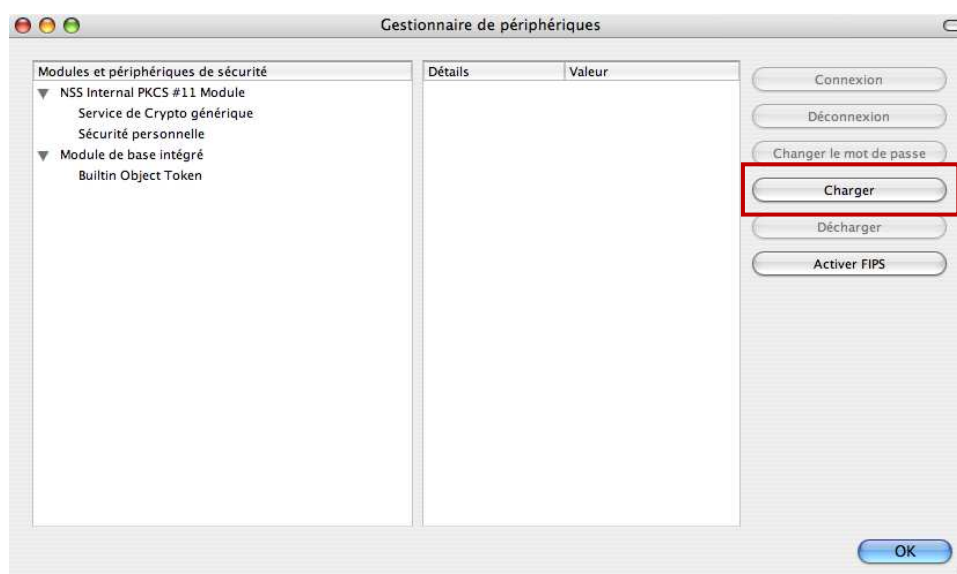
Il faut maintenant préciser à Firefox qu'il y a une clé cryptographique et quel est son pilote

Insérez la clé dans un port USB de votre machine.

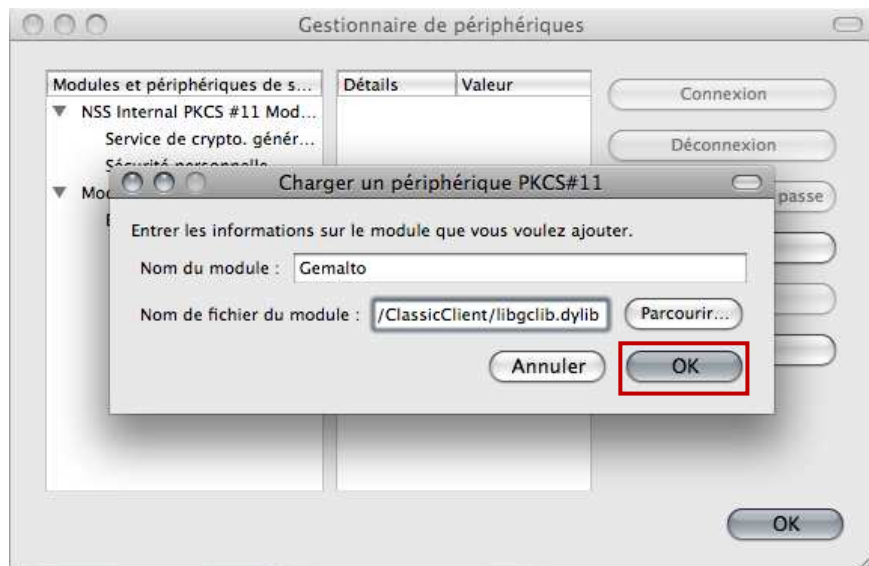
Lancez Firefox. Dans le menu **Firefox** cliquez sur **Préférences**.



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**

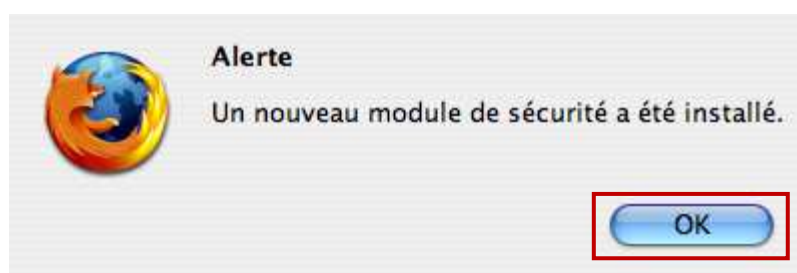
Saisissez **manuellement** le nom du fichier du module (le pilote)
/usr/lib/ClassicClient/libgclib.dylib

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 ET VALIDATION DES INFORMATIONS

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 :

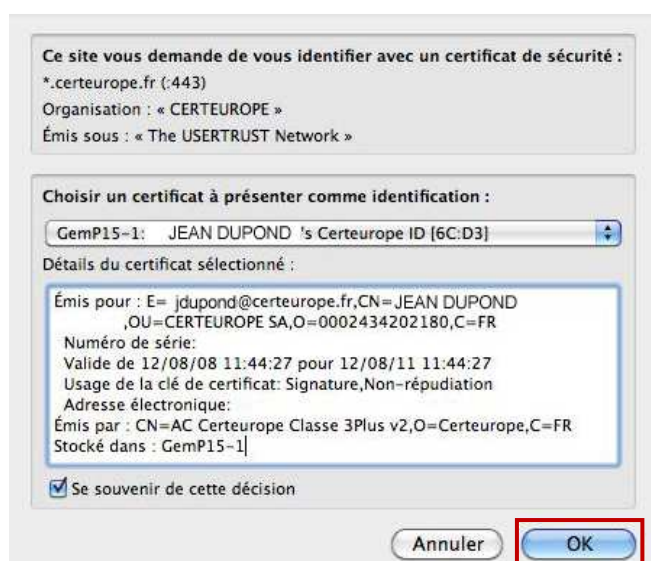


Cliquez sur **OK**

Pour Mozilla Firefox :



Après l'avoir saisi, sélectionnez votre certificat.



Cliquez sur **OK**

Vous voici sur la page **Certiservices**.

Bonjour JEAN DUPONT Votre certificat est valide Il expire le 30/03/2013 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
 CertEurope Opérateur de Services de e-Confiance	CERTISERVICES Connecté : JEAN DUPONT	 CertEurope Opérateur de Services de e-Confiance
Informations sur le certificat 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).	Code PUK 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. Le code PUK n'est délivré qu'une seule fois , 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.	Révocation Choisir ou modifier votre code de Révocation d'Urgence (CRU): 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: +33 (0) 826 300 412 (disponible 24H/24 - 7J/7). Révoquer votre certificat en ligne: Vous quittez votre société ou n'êtes plus amené à utiliser votre certificat. Vous pouvez le révoquer depuis cette page.
CertiServices - ©CertEurope - mentions légales		

Cliquez sur le bouton « Informations sur votre certificat » pour validation,
Si ces données sont inexactes, contactez votre Autorité d'Enregistrement qui vous a remis votre certificat.

Votre certificat est valide et installé

VOUS DEVEZ A CETTE OCCASION ENREGISTRER VOTRE CODE DE REVOCATION D'URGENCE (CRU) ET RECUPERER VOTRE CODE PUK (SI DISPONIBLE)

▪ 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.

The screenshot shows the CertiService user interface. At the top, there are three status boxes: 'Bonjour JEAN DUPONT. Votre certificat est valide. Il expire le 30/03/2013.', 'Vous avez un code de déblocage (PUK).', and 'Vous n'avez pas défini de Code de Révocation d'Urgence'. The third box is highlighted with a red border. Below this is the CertiService header with the CertEurope logo and 'Connecté: JEAN DUPONT'. The main content area has three columns: 'Informations sur le certificat', 'Code PUK', and 'Régulation'. The 'Régulation' column is highlighted with a red border and contains the text: 'Choisir ou modifier votre code de Révocation d'Urgence (CRU): 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.'

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 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

CODE PUK (CODE DE DEBLOCAGE)

Le code PUK n'est disponible que pour certains utilisateurs. Pour plus de renseignements, contactez votre Autorité d'Enregistrement.

▪ Récupération du code PUK

- 1- Insérez votre clé.
- 2- Connectez-vous sur : <https://services.certeurope.fr>
- 3- Sélectionnez votre certificat quand il apparaîtra et validez-le en cliquant sur **OK**.
(Si votre clé contient 2 certificats peu importe le certificat sélectionné. Par défaut, nous vous conseillons de toujours sélectionner votre certificat CERTEUROPE ADVANCED CA V3 quand cela est possible).
- 4- Entrez ensuite votre code PIN pour finaliser l'identification.

Vous voici sur la page **Certiservices**.

Bonjour JEAN DUPONT Votre certificat est valide Il expire le 30/03/2013 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
 CertEurope Opérateur de Services de e-Confiance	CERTISERVICES Connecté: JEAN DUPONT	 CertEurope Opérateur de Services de e-Confiance
Informations sur le certificat 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).	Code PUK Le code PUK ou code de déblocage permet de débloquer votre certificat si ce dernier est bloqué suite à 3 saisies d'un mauvais code PIN. Le code PUK n'est délivré qu'une seule fois , notez-le et conservez-le précieusement. Pour retirer votre code de déblocage, cliquez sur le bouton « Retirer votre code de déblocage » en haut et au centre de la page CertiService.	Révocation Choisir ou modifier votre code de Révocation d'Urgence (CRU): 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.

- 5- Cliquez sur le bouton **Voir votre code de déblocage**.

Bonjour JEAN DUPONT Votre certificat est valide Il expire le 30/03/2013 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
 CertEurope Opérateur de Services de e-Confiance	CERTISERVICES Connecté: JEAN DUPONT	 CertEurope Opérateur de Services de e-Confiance
Votre CODE PUK : 399242		



Notez le code PUK et conservez-le précieusement.

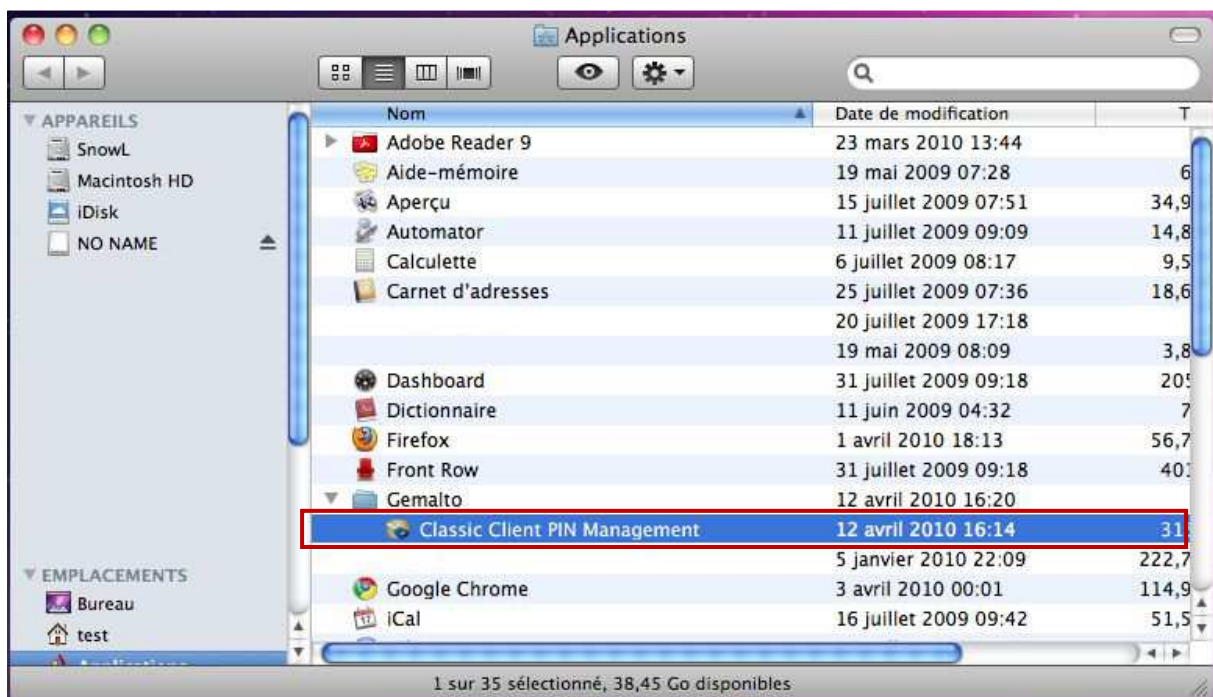
▪ Déblocage du Certificat

Le code PUK est à utiliser lorsque le certificat est bloqué suite à 3 mauvaises saisies du code PIN.

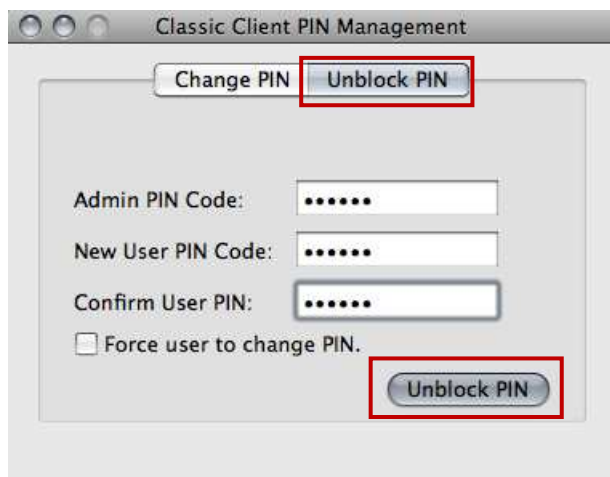
Branchez votre certificat sur un ordinateur où est installé le driver de la clé.



Ouvrez le menu Applications. Dans la barre du menu Finder : Aller → Application



Lancez le programme Classic Client PIN Management dans Applications → Gemalto → Classic Client PIN Management.



Dans l'onglet Unblock PIN, notez votre code PUK à droite du champ PIN Admin Code.

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

Puis cliquez sur **Unblock PIN**.

Votre clé est débloquée.

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.