

# CERTIFICATS ELECTRONIQUES SUR CLE USB

## CERTEUROPE CLASSE 3+



### MANUEL D'INSTALLATION WINDOWS / MOZILLA FIREFOX

V.11/10 GW



## SOMMAIRE

NOTIONS SUR LE CERTIFICAT .....	3
UTILISATION D'UN CERTIFICAT ELECTRONIQUE DE CLASSE 3+ .....	4
POINTS IMPORTANTS .....	5
CONFIGURATION WINDOWS VISTA ET 7 AVANT INSTALLATION (*) .....	6
PROCEDURE D'INSTALLATION .....	7
ACTIVATION DE LA CLE .....	13
INSTALLATION DES AUTORITES DE CONFIANCE .....	15
PARAMETRAGE MOZILLA FIREFOX .....	19
TEST DE BON FONCTIONNEMENT .....	22
REVOCACTION D'URGENCE .....	23
CODE PUK (CODE DE DEBLOCAGE) .....	24
CHANGEMENT DE CODE PIN .....	27

(\*) Uniquement pour les utilisateurs de Windows Vista et 7

## NOTIONS SUR LE CERTIFICAT

Problème : il est facile, aujourd'hui, de s'octroyer une adresse e-mail sous une fausse identité ou mieux 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 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.

## UTILISATION D'UN CERTIFICAT ELECTRONIQUE DE CLASSE 3+

### ▪ 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.

Certeurope Classe 3+ est la première Autorité de Certification référencée par le MINEFI, dont le support (la clé USB) est validé par les services du Premier Ministre (DSSSI) comme permettant la signature sécurisée.

### ▪ Dans les administrations

Les certificats 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.
- **Immatriculations** via Internet de deux roues et de véhicules automobiles et déclarations d'achat et de cession d'automobiles d'occasion.
- Candidatures aux **Appels d'offres des marchés publics**: dépôt électronique des candidatures. Vous trouverez la liste des plateformes certifiées compatibles avec les certificats opérés par CertEurope sur le site [www.certeurope.fr](http://www.certeurope.fr) rubrique marchés publics.
- **Déclaration des Produits Biocides** par Internet.

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](http://www.certeurope.fr).

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

## POINTS IMPORTANTS

### Vous possédez bien les éléments suivants :

- La (ou les) clé(s) USB Certeurope Classe 3+ 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)

### Votre ordinateur fonctionne sous :

- Microsoft Windows 2000 Professionnel.
- Microsoft Windows XP.
- Microsoft Windows Vista.
- Microsoft Windows 7.

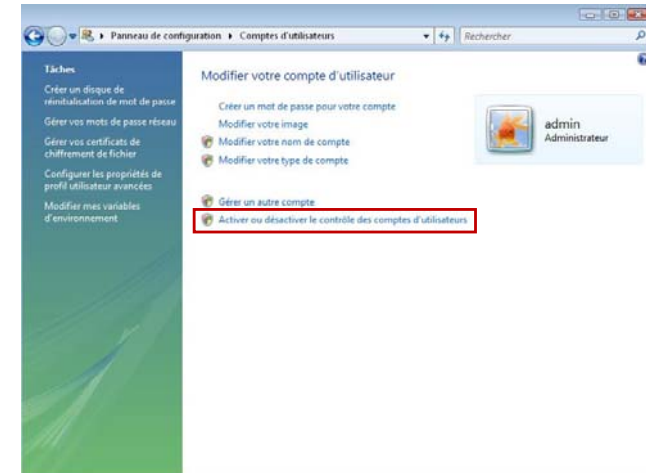
### Vous utilisez le navigateur Mozilla Firefox.

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

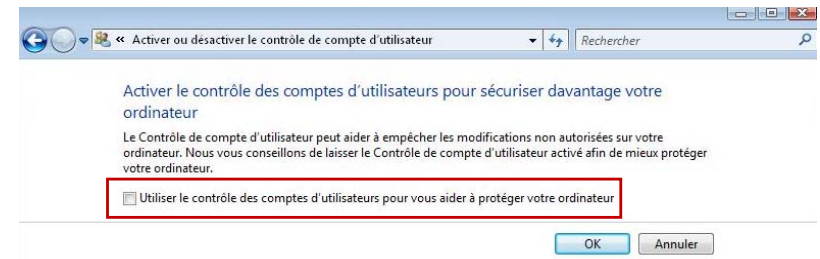
## CONFIGURATION WINDOWS VISTA ET 7 AVANT INSTALLATION (\*)

Certains paramètres de Vista et de Windows 7 peuvent créer des erreurs lors de l'installation du pilote, nous devons donc désactiver ces options.

Allez sur Démarrer → Paramètres → Panneau de configuration → Comptes d'utilisateurs.



Cliquez sur **Activer ou désactiver le contrôle des comptes utilisateurs.**



Décochez la case **Utiliser le contrôle des comptes d'utilisateurs (...)**.

Puis cliquez sur **OK** pour valider les modifications.

Redémarrez l'ordinateur si une fenêtre le demande puis commencez la procédure d'installation.

(\*) Uniquement pour les utilisateurs de Windows Vista et 7

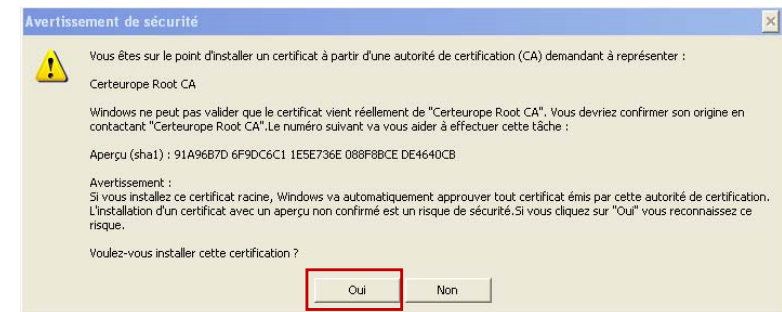
## PROCEDURE D'INSTALLATION

Attendre que l'installation soit complètement terminée avant d'insérer votre clé USB Certeuropa Classe 3+

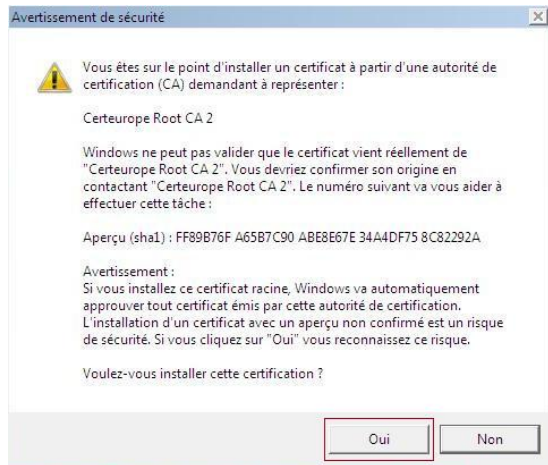
Pour installer les pilotes et le programme de gestion de la clé USB Gemalto, veuillez suivre la procédure suivante :

- 1- Fermez tous les programmes et applications.
- 2- Désinstallez toutes les éventuelles anciennes versions du programme de la clé USB.  
(Pour désinstaller les anciennes versions) :
  - Cliquez sur Démarrer/Panneau de Configuration/Ajouter ou supprimer des programmes
  - Sélectionnez « Gemsafe Standard Edition » ou « Classic Client 5.1.5 »
  - Cliquez sur le bouton supprimer)
- 3- Téléchargez le pilote :
  - Sur le site <http://www.certeurope.fr> rendez-vous dans l'onglet vous concernant de la rubrique « Accès Direct »
  - Cliquez sur le lien « Installation »
  - Puis cliquez sur le lien de téléchargement du kit d'installation correspondant à votre clé et à votre système d'exploitation
  - Pour télécharger le pilote, il faut entrer les identifiants suivants :  
Nom d'utilisateur : certeurope  
Mot de Passe : gemalto36
- 4- Lancez le programme d'installation (double cliquez sur le fichier qui vient d'être téléchargé).

5- L'écran d'accueil apparaît. Cliquez sur **Installer**.

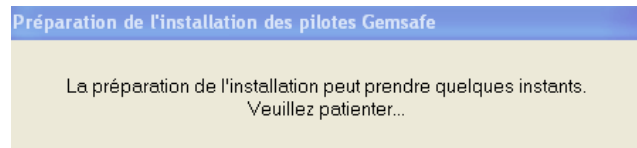


6- Cliquez sur **Oui** pour importer le certificat de l'Autorité de Certification.



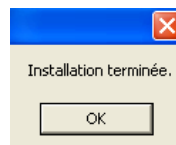
7- Cliquez sur **Oui** pour importer le certificat de l'Autorité de Certification Certeurope Root CA2.

puis patientez....



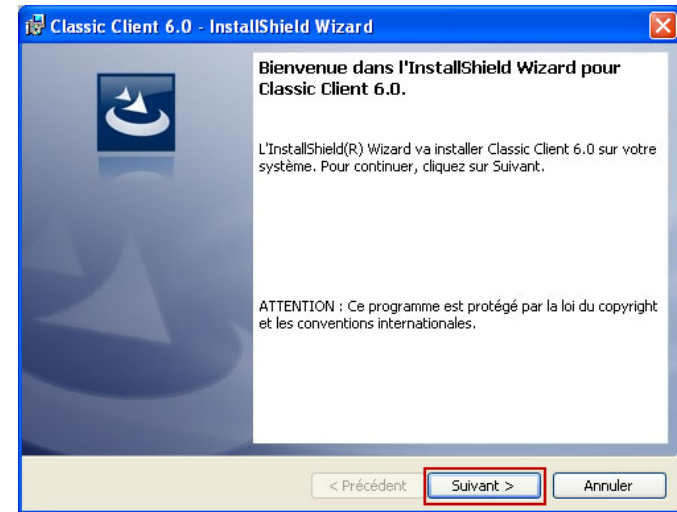
Il se peut que cette fenêtre reste présente lors de l'installation, continuez l'installation, elle se fermera d'elle même.

8- La première partie de l'installation est terminée ; cliquez sur **OK**.

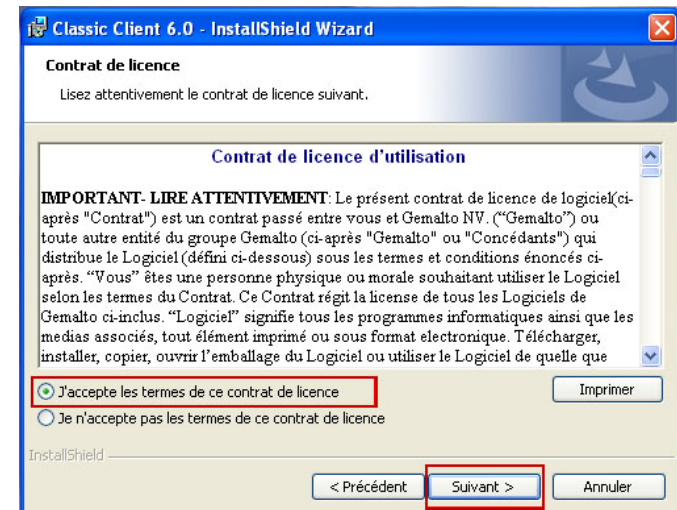


**NB** : Il est possible que la fenêtre de bienvenue apparaisse avant de pouvoir cliquer sur OK. Cela ne pose pas de problème lors de l'installation.

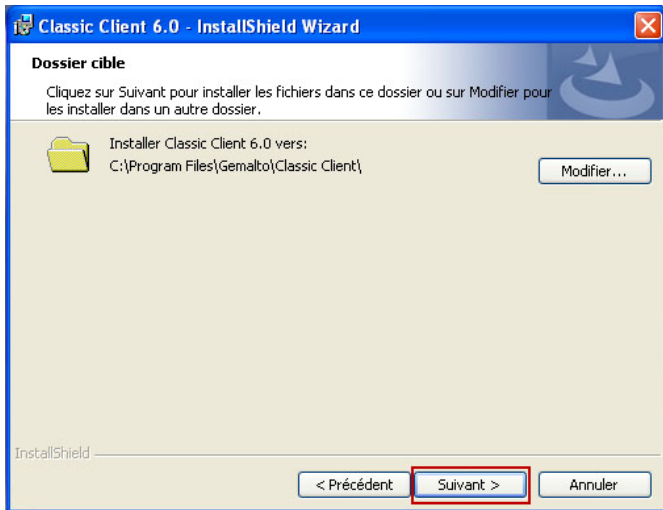
9- Patientez. La deuxième partie de l'installation commence....



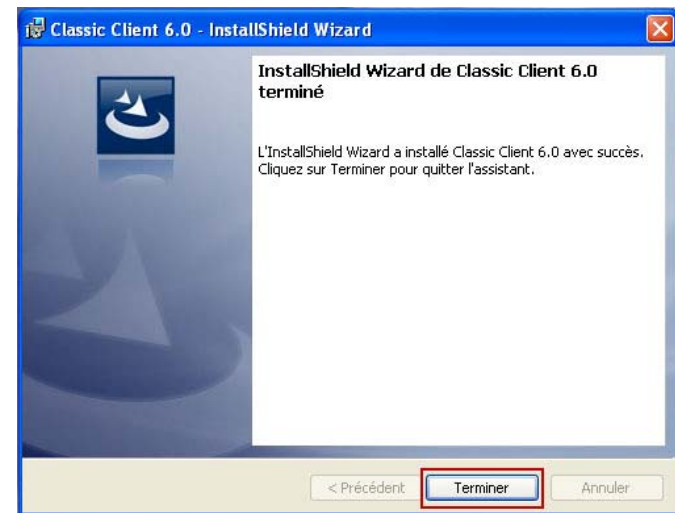
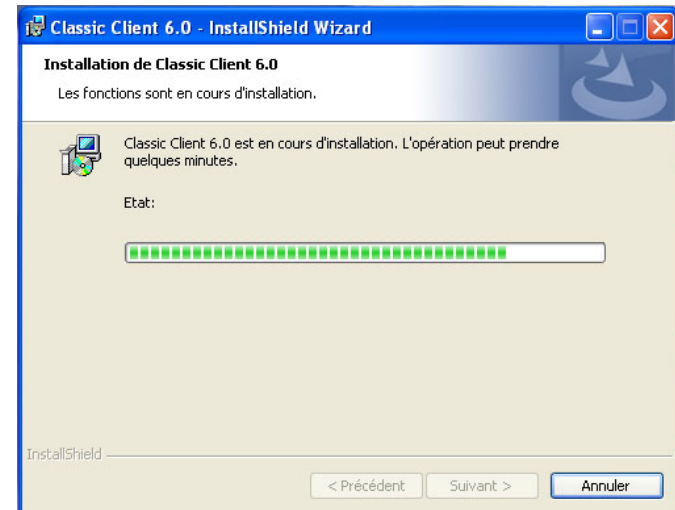
10- Cliquez sur **Suivant**.



11- Pour continuer l'installation, sélectionnez « J'accepte les termes ..... » puis cliquez sur **Suivant**.



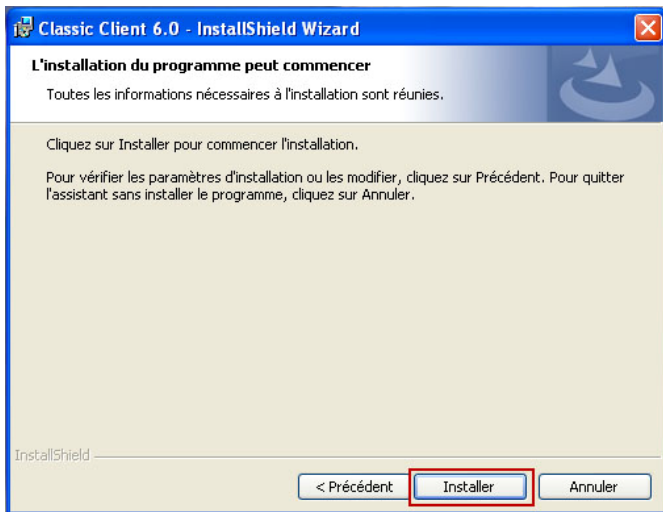
12- Cliquez sur **Suivant** sans faire de modification sur le dossier où sera installé le programme.



14- A l'apparition de cet écran, votre installation est terminée. Cliquez sur **Terminer**.

15- Cliquez sur **Oui** pour redémarrer votre ordinateur.

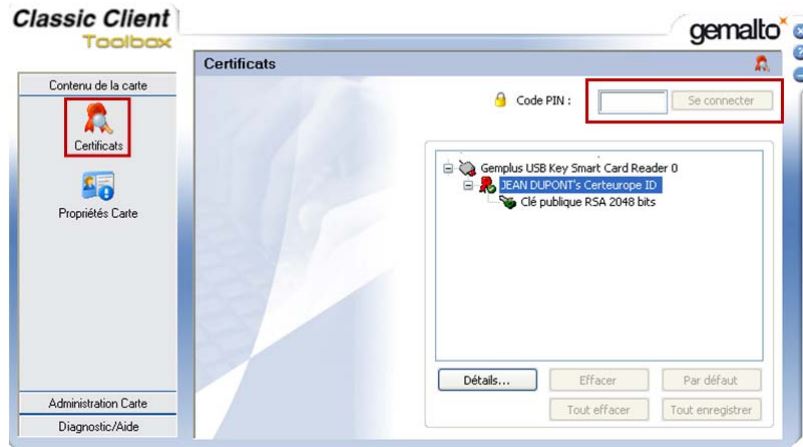
Au redémarrage, une page internet s'ouvre. Veuillez ne pas en tenir compte pour le moment. Il est nécessaire de procéder à quelques étapes supplémentaires afin de pouvoir utiliser le navigateur Firefox.



13- Cliquez sur **Installer**.

## ACTIVATION DE LA CLE

- 1- Insérez votre clé dans votre ordinateur.
- 2- Lancez le programme Classic Client Toolbox qui se situe dans le Menu : Démarrer > programmes > Gemalto > Classic Client > Classic Client Toolbox.

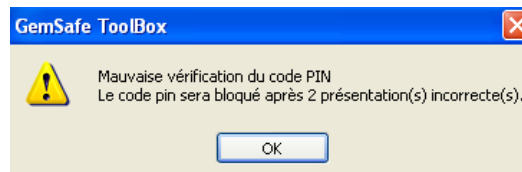


- 3- Cliquez sur **Certificats** (Colonne de gauche).
- 4- Mettez le code PIN à l'endroit indiqué et cliquez sur **Se connecter**.



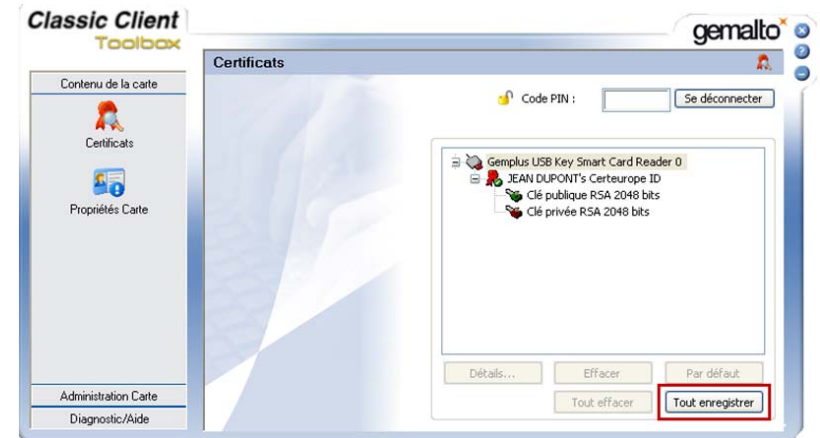
Si après avoir saisi votre code PIN le message ci-dessous apparaît, contactez notre service technique au 0899 700 046.

Cela signifie que le code PIN entré ne correspond pas à la clé qui est insérée.

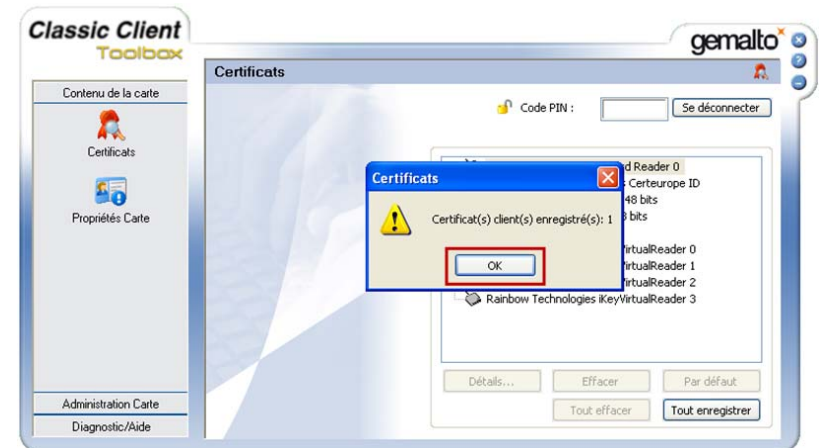


**Attention, au bout de 3 mauvaises saisies du code PIN, votre clé sera bloquée.**

Une deuxième clé appelée « clé privée » apparaît.



- 5- Cliquez sur **Tout enregistrer**.

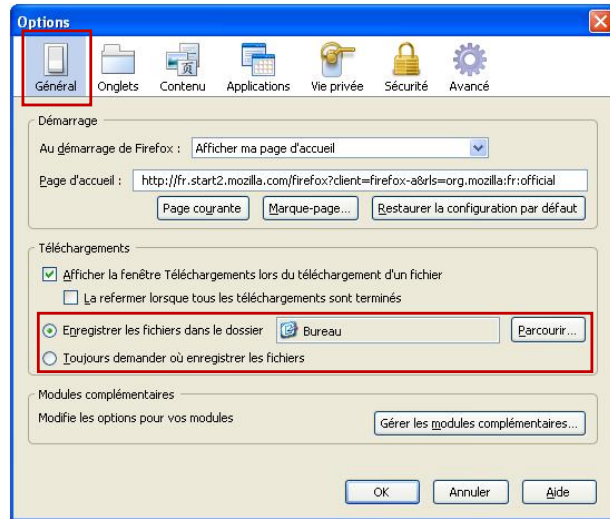


- 6- A l'apparition du message « Certificat client enregistré », cliquez sur **OK** et fermez le Toolbox.

## INSTALLATION DES AUTORITES DE CONFIANCE

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

Pour connaître ou pour modifier le dossier dans lequel seront enregistrés les certificats lors du téléchargement, ouvrez une fenêtre Firefox. Dans le menu **Outils**, sélectionnez **Options**.



Cliquez sur l'onglet **Général**. Vous trouverez le dossier dans lequel les fichiers téléchargés sont enregistrés. Vous pouvez le modifier en cliquant sur **parcourir** ou choisir de toujours demander où enregistrer les fichiers.

### 1. Installer le certificat de l'Autorité Racine

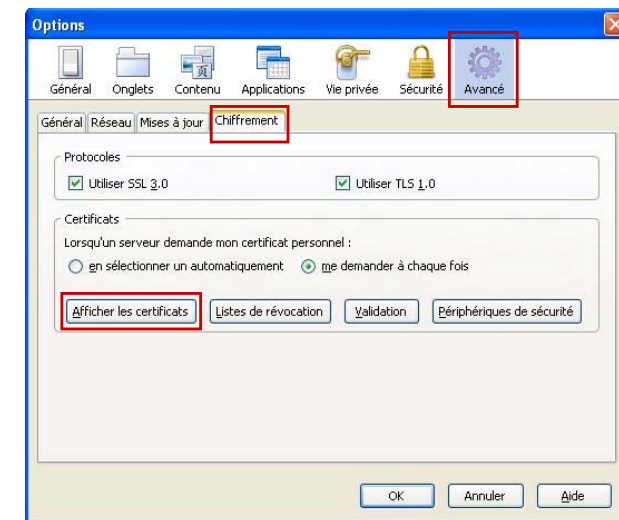
Pour installer le certificat de l'Autorité Racine, entrez dans la barre d'adresse de *Mozilla Firefox* l'url suivante :

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



Cliquez sur **Enregistrer le fichier**

Une fois le téléchargement terminé, cliquez sur **Option** dans le menu **Outils** de Firefox



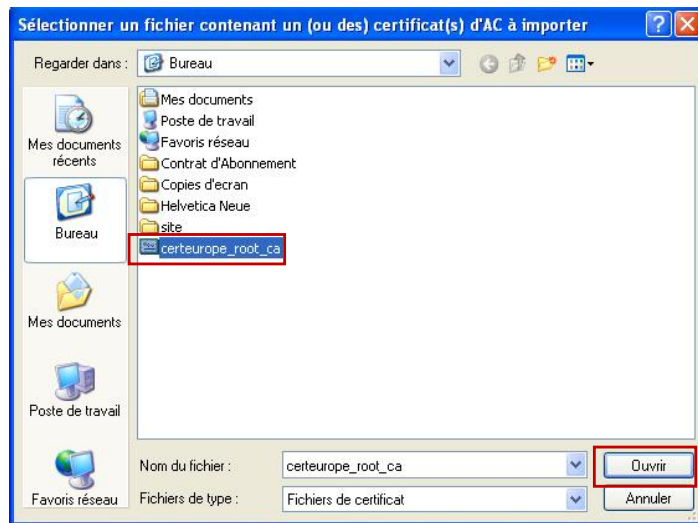
Dans le menu **Avancé**, cliquez sur l'onglet **Chiffrement** puis sur **Afficher les certificats**.



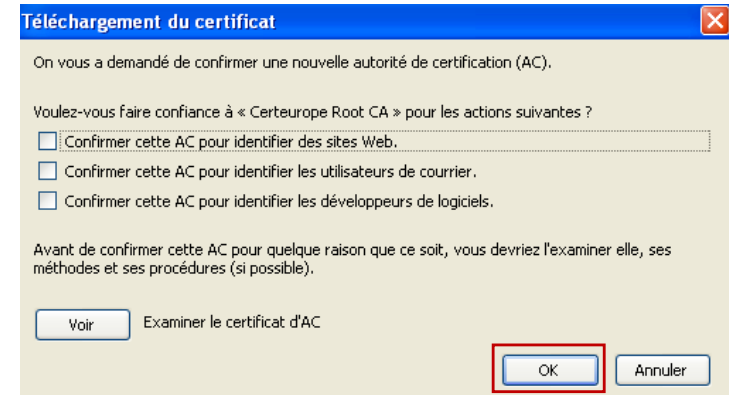
La fenêtre suivante apparaît :



Cliquez sur **Importer**.



Sélectionnez le certificat à importer **certeuropa\_root\_ca** puis cliquez sur **Ouvrir**.



Cliquez sur **OK**.

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

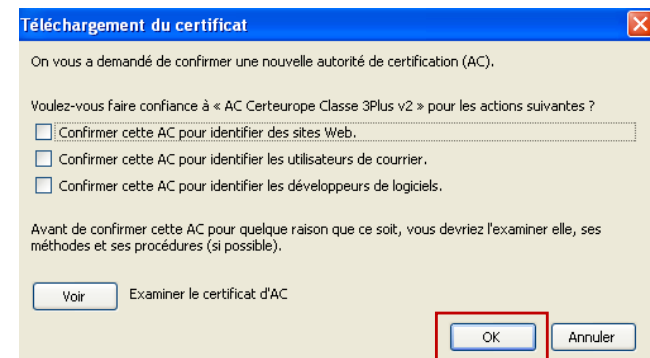
Veillez maintenant procéder à la même manipulation pour le certificat de l'Autorité Certeurope Classe 3Plus v2.

## 2. Installer le certificat de l'Autorité CertEurope Classe 3 Plus v2

Pour installer le certificat de l'Autorité Certeurope Classe 3Plus v2, entrez dans la barre 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)

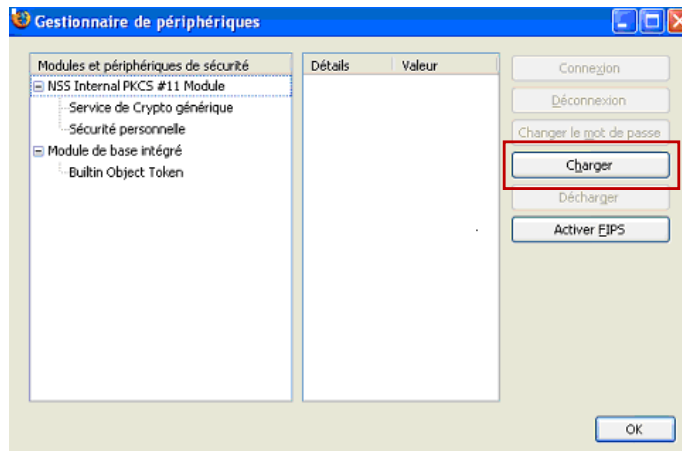
Téléchargez le certificat **ac\_certeurope\_classe\_3P\_v2** puis importez-le dans Firefox de la même manière que précédemment.



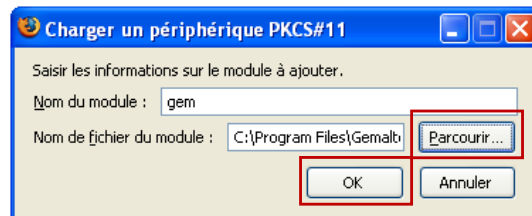
Cliquez sur **OK**.

## PARAMETRAGE MOZILLA FIREFOX

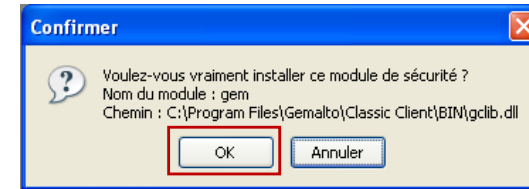
- 1- La clé toujours insérée, allez dans le menu **Outils/Options/Avancé**.
- 2- Dans l'onglet chiffrement (ou sécurité) cliquez sur **Périphériques de Sécurité**.



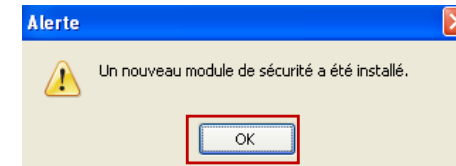
- 3- Cliquez sur **Charger** pour définir le nouveau dispositif.



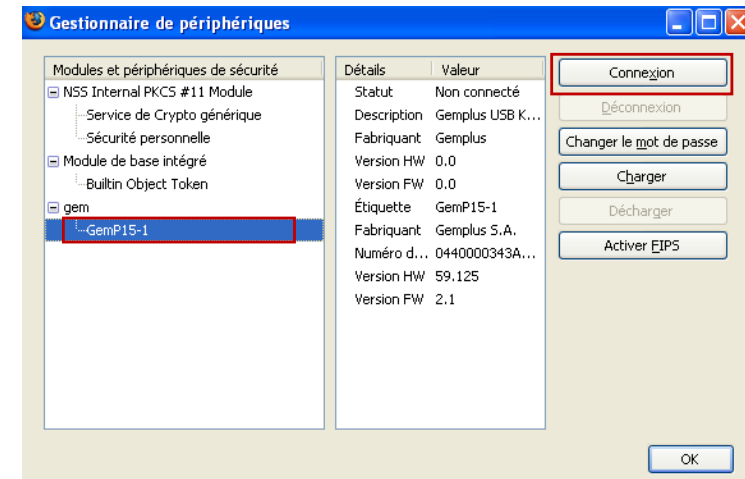
- 4- Entrez le nom du module : gem
- 5- Cliquez sur **Parcourir** et recherchez gclib.dll dans :  
Poste de travail (pour 2000 ou XP)  
C:\Program Files\Gemalto\ClassicClient\BIN\gclib.dll  
Ordinateur (pour Vista et 7)  
C:\Programmes\ Gemalto\ClassicClient\BIN\gclib.dll
- 6- Puis cliquez sur **OK**.



- 7- Cliquez sur **OK**.

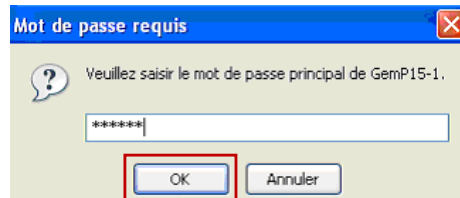


- 8- Un message de confirmation de l'installation du module apparaît. Cliquez sur **OK**.

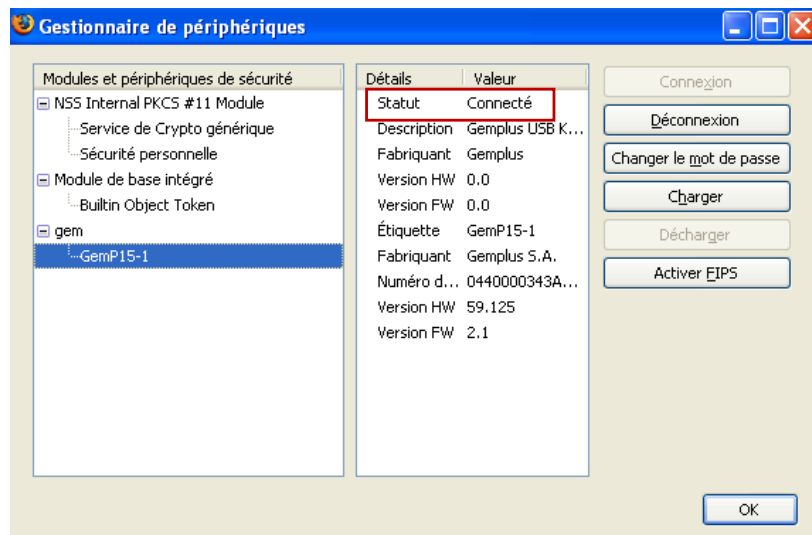


Le module apparaît sur la partie gauche sous le nom de « gem ».

- 9- Mettez en sur brillance GEMP15-1 et cliquez sur **Connexion**.



10- Mettez le code PIN de la clé et cliquez sur **OK**.



Le statut passe en **Connecté**.

11- Cliquez sur **OK** et fermez Mozilla Firefox.

## TEST DE BON FONCTIONNEMENT

- 1- Insérez votre clé dans votre ordinateur puis connectez-vous à l'espace client sécurisé à l'adresse suivante : <https://services.certurope.fr/>
- 2- Sélectionnez votre certificat quand il apparaîtra et validez-le en cliquant sur **OK**.
- 3- Entrez ensuite votre code PIN pour finaliser l'identification.

Vous voici sur la page **Certiservices**.



Votre certificat est valide et installé.

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

### ■ Création 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
- Départ de la personne abonnée au sein de l'entreprise (démission, mutation, licenciement,...)

Depuis l'Espace Clients Sécurisé (<https://services.certeurope.fr/>) vous devez saisir votre Code de Révocation d'Urgence.

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

**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 cliquez 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

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 !

**SI VOUS POSSEDEZ DEJA UNE CLE ET QUE VOUS AVIEZ DEFINI UN CODE DE REVOCAION POUR CETTE DERNIERE, IL NE VOUS SERA PAS POSSIBLE D'EN DEFINIR UN NOUVEAU. IL FAUDRA UTILISER LE CODE DEFINI PRECEDEMMENT POUR VOTRE NOUVELLE CLE.**

### ■ 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

Le code PUK n'est disponible que pour certains utilisateurs. Pour plus de renseignements, contacter votre AE.

### ■ Récupération du code PUK

- 1- Insérez votre clé.
- 2- Lancez Firefox et entrez dans la barre d'adresse : <https://services.certeurope.fr>
- 3- Sélectionnez votre certificat quand il apparaîtra et validez-le en cliquant sur **OK**. 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

**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 cliquez 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).

- 4- 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

Qu'est ce que le CODE PUK Le Code PUK ou Personal Unblocking Key est un code composé de 8 chiffres. Il permet le déblocage du Certificat lorsque ce dernier se retrouve bloqué suite à 3 saisies d'un code PIN erroné. Il s'agit d'un dispositif de protection de la puce électronique.

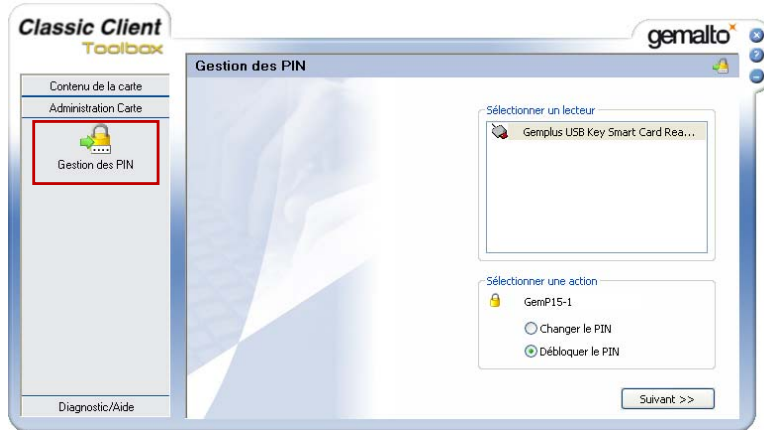


**Notez le code PUK et conservez-le précieusement.**

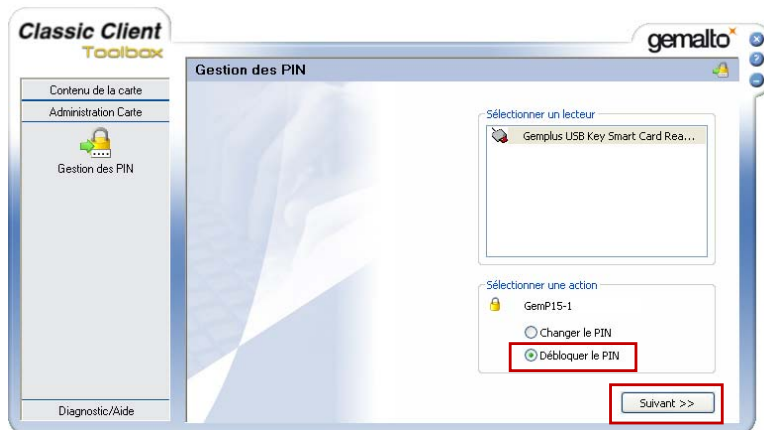
## ▪ Déblocage du Certificat

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

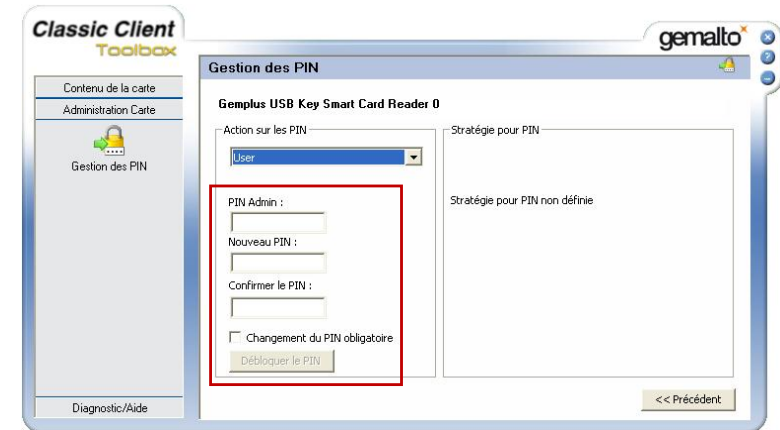
- 1- Branchez votre certificat sur un ordinateur où est installé le pilote de la clé.
- 2- Lancez le programme Classic Client Toolbox qui se situe dans le Menu : Démarrer > programmes > Gemalto > Classic Client > Classic Client Toolbox.



- 3- Sélectionnez **Administration Carte** dans le menu de gauche puis cliquez sur **Gestion des PIN**.



- 4- Sélectionnez un lecteur (ex : Gemplus) et l'action **Débloquer le PIN** puis cliquez sur **Suivant**.



- 5- Notez votre code PUK sous PIN Admin. Indiquez un nouveau code PIN et confirmez-le dans les cases correspondantes. Puis cliquez sur **Débloquer le PIN**.

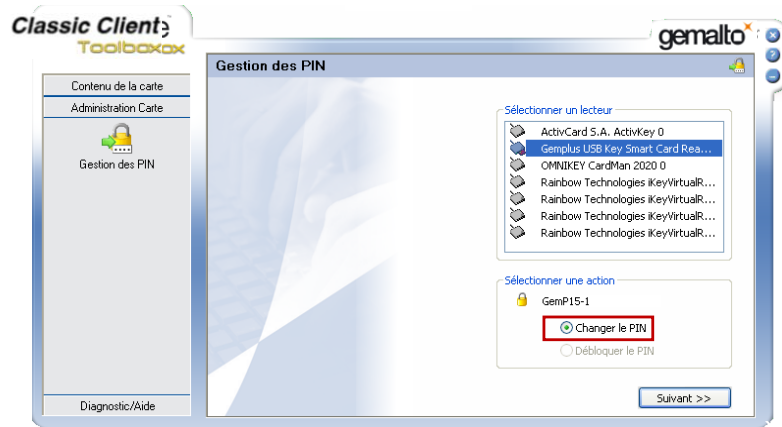
Votre clé est débloquée.

**ATTENTION : la saisie successive de 3 codes PUK erronés bloquera définitivement la clé.**

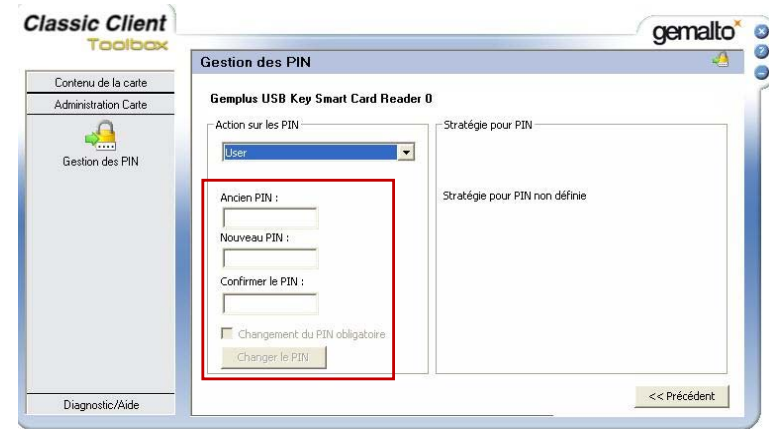
## CHANGEMENT DE CODE PIN

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

- 1- Insérez votre clé et lancez le programme Classic Client Toolbox : Démarrer → programmes → Gemalto → Classic Client Toolbox.
- 2- Sur la colonne de gauche, cliquez sur **Certificats** pour vérifier que votre clé est bien reconnue puis sur **Administration Carte** et pour finir sur l'icône **Gestion des PIN**.



- 3- Sélectionnez un lecteur (ex : Gemplus...) et une action (ex : changer le PIN) puis cliquez sur **Suivant**.



- 4- Entrez l'ancien code PIN suivi de deux fois le nouveau code PIN dans les cases correspondantes puis cliquez sur **Changer le PIN**.

**NB** : Notez soigneusement le nouveau code PIN en cas de perte de celui-ci, il ne pourra vous être restitué.

- 5- La fenêtre suivante apparaît signifiant que le code PIN a été modifié avec succès.



- 6- Cliquez sur **OK**.

**NB** : Pour vous assurer que le changement du code PIN s'est effectué correctement, il est recommandé de faire une activation (voir chapitre « activation de la clé ») avec le nouveau code.