

le certificat électronique des Greffes des Tribunaux de Commerce

# CERTIFICATS ELECTRONIQUES SUR CLE USB CERTIGREFFE

Cert

infogreffe.fr

## Autorités de certification : CERTEUROPE ADVANCED CA V3 Certeurope Classe 3 plus



## MANUEL D'INSTALLATION WINDOWS INTERNET EXPLORER ET MOZILLA FIREFOX

V.09/11



## SOMMAIRE

NOTIONS SUR LE CERTIFICAT
UN DOUBLE CERTIFICAT SUR VOTRE CLE C@RTEUROPE
UTILISATION D'UN CERTIFICAT ELECTRONIQUE CLASSE 3+ OU RGS**
POINTS IMPORTANTS
CONFIGURATION WINDOWS VISTA ET 7 AVANT INSTALLATION (*)
PROCEDURE D'INSTALLATION
ACTIVATION DE LA CLE
PARAMETRAGE INTERNET EXPLORER SOUS WINDOWS VISTA ET 7 (*)
UTILISATEURS INTERNET EXPLORER SEULEMENT
INSTALLATION DES AUTORITES DE CONFIANCE - MOZILLA FIREFOX
UTILISATEURS MOZILLA FIREFOX SEULEMENT
PARAMETRAGE MOZILLA FIREFOX
UTILISATEURS MOZILLA FIREFOX SEULEMENT
TEST DE BON FONCTIONNEMENT
REVOCATION D'URGENCE
CODE PUK (CODE DE DEBLOCAGE)
CHANGEMENT DE CODE PIN

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

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 CERTIGREFFE**

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 Certeurope 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.

INFOGREFFE agit en tant qu'Autorité d'Enregistrement Administrative et technique des Autorités de Certification AC Certeurope 3+ V2, et CERTEUROPE ADVANCED CA V3. Le certificat numérique C@rteurope délivré par INFOGREFFE est commercialisé sous le nom commercial Certigreffe. On parlera donc indifféremment du certificat C@rteurope ou de Certigreffe.

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 Certeurope 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. Vous trouverez la liste des plateformes certifiées compatibles avec les certificats opérés par CertEurope sur le site www.certeurope.fr rubrique marchés publics.
- 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.

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.certigreffe.fr,

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

#### 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)

#### Votre ordinateur fonctionne sous :

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

#### Vous utilisez le navigateur :

- Internet Explorer (version 6 minimum)
- Mozilla Firefox

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

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.

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

Certains paramétrages 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  $\rightarrow$  Paramètres  $\rightarrow$  Panneau de configuration  $\rightarrow$  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.

Attendez que l'installation soit complètement terminée avant d'insérer votre certificat Certigreffe

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- Insérer le CD-ROM fourni dans votre lecteur CD. Normalement, le programme d'installation se lance automatiquement. Si ce n'est pas cas, double cliquer sur le CD-ROM dans l'explorateur ou cliquer sur l'exécutable setup.exe présent à la raçine du programme (sur le CD-ROM)

4- L'écran d'accueil apparaît. Cliquez sur Installer.



5- Si vous avez déjà installé un certificat CertEurope sur votre machine, des fenêtres vous demandant si vous souhaitez supprimer des certificats du magasin principal peuvent apparaître. Cliquez sur **Non**.

Exemple de fenêtre qui peut apparaître :

Magasin	de certificats principal 🛛 🗙
	Voulez-vous supprimer le certificat suivant du magasin principal ?
•	Objet : Certeurope Root CA, Certeurope, FR
	Limite de validité : de jeudi 23 mai 2002 à vendredi 23 mai 2014
	Numero de serie : 01 Empreinte numérique (sha1) : 91A96B7D 6F9DC6C1 1E5E736E 088F8BCE DE4640CB
	Empreinte numérique (md5) : 186ED050 436246FE 538A872D 1680F3D4
	Oui Non

6- Puis plusieurs fenêtres proposant l'installation de certificat d'Autorités de Certification peuvent s'afficher.

Cliquez sur oui pour importer l'ensemble des certificats d'Autorité de Certification.

#### Exemple de fenêtre qui peut apparaître :

Avertiss	sement de sécurité
	Vous êtes sur le point d'installer un certificat à partir d'une autorité de certification (CA) demandant à représenter :
	Certeurope Root CA 2
	Windows ne peut pas valider que le certificat vient réellement de "Certeurope Root CA 2". Vous devriez confirmer son origine en contactant "Certeurope Root CA 2".Le numéro suivant va vous aider à effectuer cette tâche :
	Aperçu (sha1) : FA088259 5F9CA6A1 1ECCBEAF 65C764C0 CCC311D0
	Avertissement : Si vous installez ce certificat racine, Windows va automatiquement approuver tout certificat émis par cette autorité de certification. L'installation d'un certificat avec un aperçu non confirmé est un risque de sécurité.Si vous cliquez sur "Oui" vous reconnaissez ce risque.
	Voulez-vous installer cette certification ?
	Oui Non

puis patientez....

Windows Installer
Préparation de l'installation
Annuler
Classic Client 6.0
Veuillez patienter pendant que Windows configure Classic Client 6.0
Collecte des informations requises en cours
Annuler



7- A l'apparition de cet écran, votre installation est terminée. Cliquez sur **Oui** pour redémarrer votre ordinateur.

Le certificat Certigreffe peut être installé sur autant de postes que vous le souhaitez.

- 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.

assic Client				gemalto
TOCIOCA	Certificats			۵.
Contenu de la carte	1.12.11.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1	G Code P	'IN	Se connecter
Certificats		Gemplus USB JEAN DUPC Glé pu JEAN DUPC Sé Clé pu	Key Smart Card Rea DNT'S CERTEUROPE ID Jblique RSA 2048 bit: DNT'S CERTEUROPE II Jblique RSA 2048 bit:	der 0 5 5 5
	Dét	tails	Effacer	Par défaut
Administration Carta		ortor	Texterafference	++->->-
Auministration carte	impo	Uncer	TUULEInduer	Tout enregistrer

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



De nouvelles clés appelées « clés privées » apparaissent.

100100X			
	Certificats		
Contenu de la carte	1.1.1.1.1.	🚽 Code PIN	Se déconnecter
Certificats		Semplus USB Key Smart LEAN DUPONT'S CERT	t Card Reader 0 TEUROPE ID A 2048 bits
Propriétés Carte		Clé privée RSA JEAN DUPONT'S CER Clé publique RS Clé privée RSA	2048 bits TEUROPE ID A 2048 bits 2048 bits
Propriétés Carte	Dé	Clé privée RSA JEAN DUPONT'S CER Clé publique RS Clé privée RSA	2048 bits TEUROPE ID A 2048 bits 2048 bits 2048 bits

#### 5- Cliquez sur Tout enregistrer.

Toolbox				gemaic
	Certificats			Α.
Contenu de la carte	1. 1. 1. 1.	🚽 Code F	PIN	Se déconnecter
Certificats	Contificate	Cemplus USB	Key Smart Card Rea	der 0
Propriétés Carte	Certificat(s) clier	pt(s) epregistré(s): 2	ublique RSA 2048 bit: rivée RSA 2048 bits	s
			rt's CERTEUROPE ID Jublique RSA 2048 bit: rivée RSA 2048 bits	s
		Détails	Effacer	Par défaut:
			-	10

6- A l'apparition du message « Certificat(s) client(s) enregistré(s) : 2», cliquez sur **OK** et fermez le Toolbox.

Sur certaines versions de la clé Certigreffe, il est possible qu'un 3<sup>ème</sup> certificat apparaisse. La procédure reste identique dans ce cas précis.

## PARAMETRAGE INTERNET EXPLORER SOUS WINDOWS VISTA ET 7 (\*)

#### UTILISATEURS INTERNET EXPLORER SEULEMENT

Les systèmes d'exploitation Windows Vista et Windows 7 nécessitent une modification dans le paramétrage du navigateur Internet Explorer.

En effet, Microsoft a ajouté des éléments de sécurité pouvant perturber le bon fonctionnement de la carte.

1- Ouvrez une page Internet Explorer et allez sur **Outils** puis sélectionnez **Options Internet**.

A A I Cócuritó -	01. m.m.s. [	La la	1
eneral securite Con	fidentialite   Contenu	Connexions   Pr	ogrammes   Avances
Cliquez sur une zone po	our afficher ou modifie	r les paramètres d	e sécurité.
	(A)	1	0
		$\checkmark$	V
Internet I	Intranet local Sites	de confiance 🛛 Sit	tes sensibles
Internet	61 - 82	81 IS	Sites
Cette zone es	t destinée aux sites V	/eb Internet, à	
confiance et S	ites sensibles.	s les zones sites di	E
Niveau de sécurité po	our cette zone		
Niveaux autorisés p	our cette zone : Movi	en à Haut	
. T. Moven-h	aut		
- Adapt	é pour la plupart des :	sites Web	
- Messa	ges avant le téléchar	gement de conteni	u éventuellement non
- Les co	e Intrôles ActiveX non si	onés ne seront pa	s téléchargés
(m) = (707633		<b>-</b> 1997-976, 576-7865, <b>5</b> 75	
Activer le mode	e protégé (redémarrag	je d'Internet Explo	rer requis)
	Person	aliser le niveau	Niveau par défaut
	[1 <u>2</u> (30)	langer ie nivedarri	
	Rétabli	r toutes les zones	au niveau par défaut

- 2- Sur l'onglet Sécurité, décochez la case « Activer le mode protégé (redémarrage d'Internet Explorer requis) ».
- 3- Cliquez sur Appliquer puis OK.
- 4- Fermez Internet Explorer.

<sup>\*</sup> Uniquement pour les utilisateurs de Windows Vista et Windows 7.

## **INSTALLATION DES AUTORITES DE CONFIANCE - MOZILLA FIREFOX**

#### UTILISATEURS MOZILLA FIREFOX SEULEMENT

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**.

ptions						
Général	Onglets	Contenu Applic	ations Vie priv	ée Sécurité	Avancé	
Démarrag Au <u>d</u> émar	ie rage de Fir	efox : Afficher ma	page d'accueil		~	
Page d'ac	cueil : h	ttp://fr.start2.mozill Page courante	a.com/firefox?clie Marque-page	nt=firefox-a&rls	≔org.mozilla la configurat	:fr:official
Télécharg	ements ner la fenêt a refermer	re Téléchargements lorsque tous les télé	lors du télécharge chargements sont	ment d'un fichie terminés	भ	
<ul> <li>Enreg</li> <li>Toujo</li> </ul>	gistrer les f ours deman	chiers dans le dossie der où enregistrer le	er 🕜 Bureau es fichiers			Parcourir
Modules c Modifie le:	omplément s options p	aires our vos modules		Gérer les <u>r</u>	nodules comp	plémentaires )
			(	ок	Annuler	<u>Aide</u>

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 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

• Si la fenêtre suivante apparait, cliquez sur OK

féléchargement du certificat	×
On vous a demandé de confirmer une nouvelle autorité de certification (AC).	
Voulez-vous faire confiance à « Certeurope Root CA » pour les actions suivantes ?	
Confirmer cette AC pour identifier des sites Web.	
Confirmer cette AC pour identifier les utilisateurs de courrier.	
Confirmer cette AC pour identifier les développeurs de logiciels.	
Avant de confirmer cette AC pour quelque raison que ce soit, vous devriez l'examiner elle, ses méthodes et ses procédures (si possible).	
Voir Examiner le certificat d'AC	
OK Annuler	

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



Cliquez sur Enregistrer le fichier

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

Options	
Général Onglets Contenu Applications	Vie privée Sécurité
Général Réseau Mises à jour Chiffrement	
Protocoles	Utiliser TLS <u>1</u> .0
Certificats	
Lorsqu'un serveur demande mon certificat perso <u>e</u> n sélectionner un automatiquement	nnel : me demander à chaque fois
Afficher les certificats	n <u>V</u> alidation <u>P</u> ériphériques de sécurité
<u></u>	
	OK Annuler Aide

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

La fenêtre suivante apparaît :

is certificats    Personnes    Serveurs    4000	rites   Autres	
Nom du certificat	Périphérique de sécurité	臣
🖃 (c) 2005 TÜRKTRUST Bilgi İletişim ve Bi	ilişim	~
ABA.ECOM, INC.     ABA.ECOM Root CA     AC Camerfirma SA CIF A82743287	Builtin Object Token	
Chambers of Commerce Root	Builtin Object Token	
Global Chambersign Root	Builtin Object Token	~
Voir Modifier Import	er Exporter Supprimer	

Cliquez sur Importer.

Sélectionner u	n fichier contena	nt un (ou des) certif	icat(s) d'AC à in	nporter	? 🛛
Regarder dans :	🞯 Bureau		V 0 Ø	• 🗊 🔊	
Mes documents récents	Mes documents Poste de travail Favoris réseau Contrat d'Abonn Copies d'ecran Helvetica Neue site Ecerteurope_root	ement			
Mes documents					
Poste de travail					
	Nom du fichier :	certeurope_root_ca		<u>~</u>	Ouvrir
Favoris réseau	Fichiers de type :	Fichiers de certificat		×	Annuler

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

Téléchargement du certificat	×
On vous a demandé de confirmer une nouvelle autorité de certification (AC).	
Voulez-vous faire confiance à « Certeurope Root CA » pour les actions suivantes ?	
Confirmer cette AC pour identifier des sites Web.	
Confirmer cette AC pour identifier les utilisateurs de courrier.	
Confirmer cette AC pour identifier les développeurs de logiciels.	
Avant de confirmer cette AC pour quelque raison que ce soit, vous devriez l'examiner elle, ses méthodes et ses procédures (si possible).	
Voir Examiner le certificat d'AC	
OK Annuler	

Cliquez sur **OK**.

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

Veuillez maintenant procéder à la même manipulation pour les certificats de l'Autorité Racine ROOT CA V2, de l'Autorité CERTEUROPE ADVANCED CA V3 et de l'Autorité Certeurope Classe 3Plus v2.

#### 2. Installer le certificat de l'Autorité 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

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

Téléchargement du certificat 🛛 🛛 🗙
On vous a demandé de confirmer une nouvelle autorité de certification (AC).
Voulez-vous faire confiance à « Certeurope Root CA 2 » pour les actions suivantes ?
Confirmer cette AC pour identifier des sites Web.
Confirmer cette AC pour identifier les utilisateurs de courrier.
Confirmer cette AC pour identifier les développeurs de logiciels.
Avant de confirmer cette AC pour quelque raison que ce soit, vous devriez l'examiner elle, ses méthodes et ses procédures (si possible).
Voir Examiner le certificat d'AC
OK Annuler

Cliquez sur **OK**.

#### 3. Installer le certificat de l'Autorité 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

Téléchargez le certificat certeurope\_advanced\_v3 puis importez-le dans Firefox de la même manière que précédemment.

Téléchargement du certificat
On vous a demandé de confirmer une nouvelle autorité de certification (AC).
Voulez-vous faire confiance à « CERTEUROPE ADVANCED CA V3 » pour les actions suivantes ?
Confirmer cette AC pour identifier des sites Web.
Confirmer cette AC pour identifier les utilisateurs de courrier.
Confirmer cette AC pour identifier les développeurs de logiciels.
Avant de confirmer cette AC pour quelque raison que ce soit, vous devriez l'examiner elle, ses méthodes et ses procédures (si possible).
Voir Examiner le certificat d'AC
OK Annuler

Cliquez sur **OK**.

#### 4. 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

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

féléchargement du certificat	×
On vous a demandé de confirmer une nouvelle autorité de certification (AC).	
Voulez-vous faire confiance à « AC Certeurope Classe 3Plus v2 » pour les actions suivantes ?	
Confirmer cette AC pour identifier des sites Web.	
Confirmer cette AC pour identifier les utilisateurs de courrier.	
Confirmer cette AC pour identifier les développeurs de logiciels.	
Avant de confirmer cette AC pour quelque raison que ce soit, vous devriez l'examiner elle, ses méthodes et ses procédures (si possible).	
Voir Examiner le certificat d'AC	
OK Annuler	

Cliquez sur **OK**.

## PARAMETRAGE MOZILLA FIREFOX

#### UTILISATEURS MOZILLA FIREFOX SEULEMENT

- 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.

🕲 Charger un périphérique PKCS#11 📃 🗖 🔀
Saisir les informations sur le module à ajouter.
Nom du module : gem
Nom de fichier du module : C:\Program Files\Gemalt [Parcourir]
OK Annuler

4- Entrez le nom du module : gem

5- Cliquez sur **Parcourir** et rechercher gclib.dll dans : Poste de travail (*pour 2000 ou XP*) C:\Program Files\Gemalto\ClassicClient\BIN\gclib.dll

Ordinateur (pour Vista et 7 32bits) C:\Programmes\ Gemalto\ClassicClient\BIN\gclib.dll

Ordinateur (pour 7 64bits) C:\Program files (ou Program files x86)\ Gemalto\ClassicClient\BIN\gclib.dll

6- Puis cliquez sur OK.



7- Si cette fenêtre apparait, cliquez sur OK.



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

1odules et périphériques de sécurité	Détails	Valeur	Connexion
NSS Internal PKCS #11 Module	Statut	Non connecté	
Service de Crypto générique	Description	Gemplus USB K	Déconnexion
Sécurité personnelle	Fabriquant	Gemplus	Changer le <u>m</u> ot de passe
Module de base intégré	Version HW	0.0	
Builtin Object Token	Version FW	0.0	Charger
gem	Étiquette	GemP15-1	Décharger
<sup>i</sup> GemP15-1	Fabriquant	Gemplus S.A.	
	Numéro d	0440000343A	Activer EIPS
	Version HW	59.125	
	Version FW	2.1	

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**.

Modules et périphériques de sécurité	Détails	Valeur	Connexion
NSS Internal PKCS #11 Module	Statut	Connecté	
-Service de Crypto générique	Description	Gemplus USB K	
Sécurité personnelle	Fabriquant	Gemplus	Changer le <u>m</u> ot de passe
Module de base intégré	Version HW	0.0	
Builtin Object Token	Version FW	0.0	C <u>h</u> arger
gem	Étiquette	GemP15-1	Décharger
<sup>i</sup> GemP15-1	Fabriquant	Gemplus S.A.	
	Numéro d	0440000343A	Activer <u>F</u> IPS
	Version HW	59.125	
	Version FW	2.1	

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.certeurope.fr/

2- 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).

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 (SI DISPONIBLE)

#### 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,...)

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 entraine 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 PUK. 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.



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 <a href="https://services2.certeurope.fr/revocation/">https://services2.certeurope.fr/revocation/</a> et suivez les indications données

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

#### 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.



399242

Qu'est ce que le CODE PUK:Le Code PUK ou Personnal Unbloking Key est un code composé de 6 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.

Classic Client		gemalto
G	estion des PIN	
Contenu de la carte		
Administration Carte	Sélectionn	er un lecteur
Gestion des PIN	Ge	mplus USB Key Smart Card Rea
	Sélectionn 9 Ge	er une action mP15-1
	C	Changer le PIN
	۲	Débloquer le PIN

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

Classic Client		gemalto
TOOIOCX	Gestion des PIN	<u>A</u>
Contenu de la carte		
Administration Carte	and the second second	Sélectionner un lecteur
- <u></u>		Gemplus USB Key Smart Card Rea
Gestion des PIN	2160	
		Sélectionner une action
		Changer le PIN
Diagnostic/Aide		Suivant >>

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

assic Client		gemalto
	Gestion des PIN	
Contenu de la carte		
Administration Carte	Gemplus USB Key Smart Card Reader 0	
Gestion des PIN	Action sur les PIN	stégie pour PIN
	PIN Admin : Stra	itégie pour PIN non définie
	Nouveau PIN :	
	Confirmer le PIN :	
	Changement du PIN obligatoire Débloquer le PIN	
		<< Précédent

5- Notez votre code PUK sous PIN Admin. Indiquez un nouveau code PIN et confirmer-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.

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**.

issic Client		gemalto
Teelex	Gestion des PIN	
Contenu de la carte Administration Carte	Gemplus USB Key Smart Card Reader 0 Action sur les PIN User Ancien PIN : Confirmer le PIN	tégie pour PIN
Discussion (Miles	Changer le PIN	<< Précédent

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, 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.