

Trusted Key Manager et Certificat CE Sur Clé USB ou Carte à puce

Manuel d'installation Windows Internet Explorer et Firefox



V. 25-01-2018-01



AVERTISSEMENT

Sans préjudice des droits réservés et sauf autorisation, aucune partie de ce document ne peut être ni reproduite, ni enregistrée ou introduite dans un système de consultation, ni transmis sous quelque forme ou par quelque moyen que ce soit sans la permission écrite du GROUPE OODRIVE.

Toute autre demande de permission de reproduire et d'exemplaires du présent document doit être adressée au GROUPE OODRIVE.

LISTE DE DIFFUSION

Société	Rôle
CertEurope	Collaborateurs et clients de CertEurope

MODIFICATIONS

Date	État	Version	Auteur	Comment	
17/02/2016	Publié	V 17-02-2016-01	Maurice SAMIMI	Document finalisé	
07/03/2016	Publié	V 07-03-2016-01	Guillaume CESBRON	Ajout de prérequis relatifs à l'utilisation d'une ancienne clé	
24/03/2016	Publié	V 24-03-2016-01	Romain THIODAT	Modifications liées aux paramètres de sécurité	
10/05/2016	Publié	V 10-05-2016-01	Quynh Tran	Remplacement liens de téléchargement	
01/07/2016	Publié	V01-07-2016-01	Romain THIODAT	Corrections dans l'indexation de chapitres	
08/08/2016	Publié	V08-08-2016-01	Romain THIODAT	Corrections diverses	
10/08/2016	Publié	V10-08-2016-01	Romain THIODAT	Mise à jour des écrans pour Firefox	
24/08/2017	Publié	V. 24-08-2017-01	Romain THIODAT	Mise à jour suite à la règlementation eIDAS	
12/10/2017	Publié	V. 12-10-2017-01	Romain THIODAT	Mise à jour suite à la suppression des certificats dans Firefox	
25/01/2018	Publié	V. 25-01-2018	Romain THIODAT	Mise à jour de liens + nouveau logo CertEurope	



SO	MMAIRE	
AVE	RTISSEMENT	2
LIST	E DE DIFFUSION	2
MO	DIFICATIONS	2
INT	RODUCTION : NOTIONS CONCERNANT LE CERTIFICAT	4
L'U1	TILISATION D'UN CERTIFICAT ELECTRONIQUE RGS**	4
POII	NTS IMPORTANTS	5
1.	Prérequis d'installation	6
1.1	Prérequis dans le cas d'une ancienne clé de certification préinstallée	6
1.1.	1 Prérequis relatifs à l'utilisation unique de la nouvelle clé	6
1.1.	2 Prérequis relatifs à l'utilisation concomitante de clés de différents types	8
1.1.	3 Lancer Internet Explorer en mode bureau	12
2.	La Procédure d'installation du logiciel Trusted Key Manager (TKM)	12
2.1	Première étape : le téléchargement et l'installation du logiciel TKM	13
2.2	Deuxième étape : l'activation de la clé	14
2.3	Troisième étape : l'installation des Autorités de Confiance sous Firefox	17
2.3.	1 L'installation de l'Autorité de Confiance Certeurope ROOT CA 3	17
2.3.	2 L'installation de l'Autorité de Confiance CertEurope eID ROOT	22
2.3.	3 L'installation du certificat de l'Autorité Certeurope ADVANCED CA V4	22
2.3.	4 L'installation du certificat de l'Autorité CertEurope eID User	22
2.4	Le paramétrage de Mozilla Firefox	23
3.	Quatrième étape : test de bon fonctionnement de votre certificat	26
3.1	La génération de votre code de « Révocation d'Urgence »	27
3.2	La Révocation d'Urgence	28
3.3	Déblocage de la clé	28
4.	Changement de code PIN	31



INTRODUCTION : NOTIONS CONCERNANT LE CERTIFICAT

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 ** (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.

L'UTILISATION D'UN CERTIFICAT ELECTRONIQUE 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 CERTEUROPE ADVANCED CA V4 sont référencés par l'administration et permettent l'accès aux téléprocédures.



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

Pour toute information :

Le site web : <u>www.certeurope.fr</u>, Ou par mail : <u>support@certeurope.fr</u>

POINTS IMPORTANTS

Vous possédez bien les éléments suivants :

✓ La (ou les) clé(s) USB CertEurope qui vous a (ont) été délivrée(s) par l'Autorité d'Enregistrement.

Votre ordinateur fonctionne sous :

- Microsoft Windows 7
- Microsoft Windows 8
- ✓ Microsoft Windows 8.1
- ✓ Microsoft Windows 10

Vous utilisez le navigateur :

- ✓ Internet Explorer (à jour)
- ✓ Mozilla Firefox (à jour)



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

Certains antivirus empêchent ou ralentissent le lancement du pilote d'installation. Dans le cas où une fenêtre vous alerte, veuillez désactiver votre antivirus le temps de l'installation.

Pour les utilisateurs d'ordinateurs fonctionnant sous Apple MAC OS, veuillez vous rendre sur notre site <u>www.certeurope.fr</u> dans la rubrique « Accès Direct Abonnés ».



1. Prérequis d'installation

Afin de pouvoir utiliser convenablement votre nouveau certificat CertEurope, il convient d'effectuer plusieurs actions, suivant la configuration de votre poste à savoir :

- La version de Windows installée sur votre poste (Windows 7, 8.1 ou 10),
- Si une ancienne clé est déjà installée votre poste.

Cette section vous guidera dans les actions à effectuer.

1.1 Prérequis dans le cas d'une ancienne clé de certification préinstallée

Pour vérifier si une ancienne clé est bien installée, faites une recherche de « Classic Client Toolbox » dans la barre de recherche dédiée.

Si vous êtes sur Windows 8, cliquer sur l'icône de recherche dans la barre latérale pour lancer une recherche. Sur toutes autres versions de Windows, faire apparaître la recherche à partir du menu Démarrer.

Si vous ne trouvez aucune occurrence du logiciel Classic Client Toolbox sur votre poste, nous vous invitons à vous reporter aux sections suivantes du présent manuel.

Si une clé CertEurope a déjà été installée sur votre poste, deux cas de figure se présentent :

- Vous n'allez utiliser que la nouvelle clé sur le poste.
- Vous allez utiliser les deux types de clés (la nouvelle et une clé de l'ancien type) sur le même poste.

1.1.1 Prérequis relatifs à l'utilisation unique de la nouvelle clé

Dans le cas d'une installation de clé consécutive au simple renouvellement de votre clé CertEurope, le pilote de votre ancienne clé doit être désinstallé de votre poste de travail.

Pour lancer le gestionnaire des programmes de votre poste :

Si vous êtes sur Windows 8, faites une recherche de « Panneau de configuration » via la barre latérale (placer la souris dans un coin à droite) puis allez dans Panneau de configuration (affichage par « Catégories ») → Programmes/Désinstaller un programme.

Sur toutes autres versions de Windows, allez dans Démarrer \rightarrow Paramètres \rightarrow Panneau de configuration (affichage par « Catégories ») \rightarrow Programmes/Désinstaller un programme.



Panneau de configuration	
Ajuster les paramètres de l'ordinateur	Afficher par : Catégorie 💌
Système et sécurité Consulter l'état de votre ordinateur Sauvegarder l'ordinateur Rechercher et résoudre des problèmesSouvegarder l'ordinateur Réseau et Internet Choisir les options de groupe résidentiel et de partageSouvegarder l'état et audio Afficher les périphériques et imprimantes Ajouter un périphériqueSouvegarder l'état et un programmes Désinstaller un programmes Obtenir des programmes	Comptes d'utilisateursModifier le type de compteModifier le type de compteModifier le thème Modifier l'arrière-plan du Bureau Modifier la résolution de l'écranModifier les claviers ou les autres méthodes d'entrée Modifier la langueMotifier les claviers ou les autres méthodes d'entrée Modifier la langueMotifier les claviers ou les autres méthodes d'entrée Modifier la langueMotifier les claviers ou les autres méthodes d'entrée Modifier la langueMotifier les claviers ou les autres méthodes d'entrée Modifier la langueMotifier les claviers ou les autres méthodes d'entrée Modifier la langueMotifier les claviers ou les autres méthodes d'entrée Motifier la langueMotifier les claviers ou les autres méthodes d'entrée Motifier la langueMotifier les claviers ou les autres méthodes d'entrée Motifier la langueMotifier les claviers ou les autres méthodes d'entrée Motifier la langueMotifier les claviers ou les autres méthodes d'entrée Motifier la langueMotifier les claviers ou les autres méthodes d'entrée Motifier la langueMotifier les claviers ou les autres méthodes d'entrée Motifier la langueMotifier les claviers ou les autres Motifier la langueMotifier les claviers ou les autres Motifier la langueMotifier les claviers ou les autres Motifier les claviers Dytimiser l'affichage

Rogrammes et fonctionnalités					_ 🗆 ×
🕞 🕞 🗢 🥅 🝷 Panneau de config	guration 🝷 Programmes 🝷 Programmes et fonctionna	lités 🔻 🛂 🛛	Rechercher dans : Progra	ammes et for	ı 🔎
Page d'accueil du panneau de configuration Afficher les mises à jour installées	Désinstaller ou modifier un programme Pour désinstaller un programme, sélectionnez	e -le dans la liste et cliquez sur Dés	sinstaller, Modifier ou Rép	arer.	
Activer ou désactiver des fonctionnalités Windows	Organiser 🔻 Désinstaller Réparer			:==	- 🕐
	Nom 🔺	↓ Éditeur	▼ Install ▼ 1	Taille 🚽	Version
	7-Zip 9.20 (x64 edition)	Igor Pavlov	08/02/2015	4,53 Mo	9.20.00.0
	Classic Client 6.3 Patch2	s Gemalto	19/12/2015	217 Mo	6.30.020.
	Ext2Fsd 0.62	Matt Wu	11/12/2015	11,9 Mo	0.62
	Java 8 Update 73	Oracle Corporation	28/02/2016	20,8 Mo	8.0.730.2
	Microsoft .NET Framework 4.5.2	Microsoft Corporation	28/02/2016	38,8 Mo	4.5.51209
	🥹 Mozilla Firefox 43.0.1 (x86 fr)	Mozilla	20/12/2015	90,4 Mo	43.0.1
	🔯 Mozilla Maintenance Service	Mozilla	20/12/2015	232 Ko	43.0.1
	Oracle VM VirtualBox Guest Additions 5.0.12	Oracle Corporation	19/12/2015		5.0.12.0
	SafeNet Authentication Client 8.3	SafeNet, Inc.	19/12/2015	67,8 Mo	8.3.52.0
	🚾 SumatraPDF	Krzysztof Kowalczyk	30/11/2015	11,5 Mo	3.1.1
	Vim 7.4 (self-installing)		20/12/2015		
	WinCDEmu	Bazis	19/12/2015		3.6
	Gemalto Version du produit : 6.30.	020.001 Lien vers	le support http://www	v.gemalto.co	m

Sélectionnez **Classic Client** dans la liste des programmes installés.

Faites un clic droit sur la sélection puis choisissez Désinstaller.





Cliquez sur **OUI** pour lancer la désinstallation du logiciel Classic Client.



Cliquez sur **OUI** pour redémarrer votre poste de travail et finaliser la désinstallation de logiciel **Classic Client.**

1.1.2 Prérequis relatifs à l'utilisation concomitante de clés de différents types

Dans le cas où une installation de clé de certification de type Gemalto a déjà été effectuée sur votre poste avant le 25 mars 2016, vous devez mettre à jour le logiciel de votre ancienne clé.

La dernière version du logiciel de votre clé peut être téléchargée en vous rendant sur le lien suivant :

https://support.certeurope.fr/telechargement-3/

Dans la partie « Mise à jour du pilote de votre ancienne clé », téléchargez la version correspondant à votre version de Windows affichée en haut de page (soit 32 bits, soit 64 bits).



🚺 Téléchargements				<u> </u>
🕞 🗇 🖟 🔹 grisgrisgc 🔹 1	Téléchargements	👻 🛂 Rec	hercher dans : Télécharg	ements 😥
Organiser 👻 Inclure dans la b	vibliothèque 🔻 Partager avec 👻 Nouveau dossier		:=	•
🔆 Favoris	Nom ^	Modifié le	Туре	Taille
Bureau Emplacements récents Profil Eléchargements Bibliothèques Documents Tages Musique Vidéos	Classic_Client_64_User_setup.msi	01/03/2016 18:07	Package Windows I	55 488 Ko
🤣 Groupe résidentiel	▼			
1 élément				

Une fois le logiciel téléchargé sur votre poste, veuillez effectuer les actions suivantes :

Fermez tous les programmes et applications.

Lancez le programme d'installation (double cliquez sur le fichier qui vient d'être téléchargé). L'écran d'installation ci-après apparaît.





Cliquez sur Suivant.

🔂 Classic Client 6.3.8 for 64 bits - InstallShield Wizard	×
Contrat de licence	gemalto
Lisez attentivement le contrat de licence suivant.	account to be not
Contrat de licence d'utilisation	
IMPORTANT- LIRE ATTENTIVEMENT: Le présent contrat de licence de l après "Contrat") est un contrat passé entre vous et Gemalto NV. ("Gemalto autre entité du groupe Gemalto (ci-après "Gemalto" ou "Concédants") qui d Logiciel (défini ci-dessous) sous les termes et conditions énoncés ci-après. êtes une personne physique ou morale souhaitant utiliser le Logiciel selon l du Contrat. Ce Contrat régit la license de tous les Logiciels de Gemalto ci-im "Logiciel" signifie tous les programmes informatiques ainsi que les medias a tout élément imprimé ou sous format electronique. Télécharger, installer, co ouvrir l'emballage du Logiciel ou utiliser le Logiciel de quelle que façon que	logiciel(ci- ") ou toute distribue le "Vous" les termes aclus. associés, pier, e ce soit, ▼
J'accepte les termes de ce contrat de licence	Imprimer
C Je n'accepte pas les termes de ce contrat de licence	
InstallShield	
< Précédent Suivant >	Annuler

Cliquez sur « J'accepte les termes de ce contrat de licence », puis sur Suivant.



🚼 Classic Cl	lient 6.3.8 for 64 bits - Inst	allShield Wizard		×
Dossier ci	ible			gemalto
Cliquez s les instal	ur Suivant pour installer les fich ler dans un autre dossier.	niers dans ce dossie	r ou sur Modifier po	ur
	Installer Classic Client 6.3.8 f C:\Program Files (x86)\Gemal	or 64 bits vers: to\Classic Client\		Modifier
InstallShield –		< Précédent	Suivant >	Annuler

Cliquez sur à nouveau sur Suivant.



Cliquez sur à nouveau sur Terminer.



🔂 Inform	ations sur l'installation de Classic Client 6.3.8 for 🔀
i	Informations sur l'installation de Classic Client 6.3.8 Vous devez redémarrer votre système pour que les modifications apportées à la configuration de Classic Client 6.3.8 for 64 bits prennent effet. Cliquez sur Oui pour redémarrer maintenant, ou sur Non si vous voulez redémarrer manuellement ultérieurement.
	<u>Q</u> ui <u>N</u> on

Cliquez sur à nouveau sur **Oui** afin de redémarrer et de finaliser l'installation du logiciel.

1.1.3 Lancer Internet Explorer en mode bureau

Dans les cas d'usage de Windows 8.1 et de Windows 10 uniquement.

UTILISATEURS INTERNET EXPLORER SEULEMENT

Attention : Si vous utilisez Internet Explorer pour vos connexions sécurisées (avec notre certificat), il vous faudra être en mode bureau exclusivement.

- 1. Sur le bureau, ouvrez une page Internet Explorer.
- 2. Sinon si vous avez ouvert Internet Explorer en mode tuile :

Effectuez un clic droit sur la fenêtre Internet Explorer pour faire apparaître la barre d'outils en bas, ensuite cliquez sur l'icône molette puis choisissez l'option « Afficher sur le bureau ».



2. La Procédure d'installation du logiciel Trusted Key Manager (TKM)

L'installation et vérification se déroulent en quatre étapes :

- ✓ Le téléchargement et l'installation du logiciel Trusted Key Manager (TKM)
- ✓ L'activation de votre clé
- ✓ L'installation et le paramétrage des certificats pour le navigateur Firefox



✓ Vérification du bon fonctionnement de votre clé

2.1 Première étape : le téléchargement et l'installation du logiciel TKM

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

- 1- Fermez tous les programmes et applications
- 2- Téléchargez le pilote adéquat sur le site https://support.certeurope.fr
- 3- Lancez le programme d'installation (double cliquez sur le fichier qui vient d'être téléchargé).
- 4- L'écran d'accueil apparaît. Cliquez sur « Install »

B Oodrive Trusted Key	/ Manager Suite Setup
	Oodrive Trusted Key Manager Suite will be installed on your device
\$ *	By installing you accept these <u>license terms</u>

5- En fonction de du poste utilisateur, il est possible que les fenêtres d'installation de certificat d'Autorités de Certification s'affichent.

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

Exemple de fenêtre qui peut apparaître :



Puis patientez....

6- À l'apparition de la fenêtre suivante, votre installation est terminée.



授 Oodrive Trusted Key	Manager Suite Setup	
	Setup Successful	
Ö.		
- 1		Close

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

2.2 Deuxième étape : l'activation de la clé

Vous devez impérativement être connecté à Internet pour activer votre clé.

Afin d'activer la clé vous devez :

• l'insérer dans un port USB libre de votre poste

• ensuite lancer le programme Trusted Key Manager.

Afin d'accéder au programme merci de suivre les étapes suivantes :

✓ Pour Windows 7 :

Aller dans le menu Démarrer>Programmes>Oodrive>Trusted Key Manager

- ✓ Pour Windows 8.1
- a) Passez la souris en bas à droite de votre écran afin d'afficher le menu Windows 8.1
- b) Pour le trouver plus rapidement, faites une recherche au niveau de vos programmes.
- c) Entrez l'intitulé « Trusted Key Manager »



✓ Pour Windows 10

Rendez-vous dans le menu Démarrer>Applications>Oodrive>Trusted Key Manager

1- Le programme s'ouvre :



Trusted Key Manager
Pour utiliser et gérer votre clé, vous devez commencer par l'activer.
Pour activer votre carte, il est nécessaire d'être connecté à Internet.
3

- 2- Cliquez sur Activer
- 3- Un code d'activation vous est envoyé selon la modalité choisie lors de la commande de la clé:
 - ✓ soit par email,
 - ✓ soit par SMS sur votre téléphone portable
- 4- Saisissez le code d'activation à l'endroit indiqué et cliquez sur valider.

Trusted Key Manager		×
Entrez le code d'activation reçu par email ou par téléphone		
	900087	
Le code vient d'être envoyé à l'adresse email:	Valider	
r.t***************.fr		
Nous vous invitons à renseigner le code ci-contre.		
• • •	ANNULER	
		?

5- Définissez le PIN de votre clé à l'aide du pavé virtuel et cliquez sur OK.





6- Confirmez le PIN de votre clé de nouveau et cliquez sur OK.



7- Votre PIN est maintenant enregistré, cliquez sur **OK**.

Trusted Key Manager		
VOTRE CLÉ EST PRÊTE À ÊTRE U	JTILISÉE !	Caroline GENEST
Succès		
Votre clé est prête à être	e utilisée !	
		ОК
Modifier le Code PIN		
		Ø
	www.certeurop	pe.fr www.ood

WWW.Certeurope.rr WWW.Oodrive.col CertEurope - une société du groupe Oodrive



2.3 Troisième étape : l'installation des Autorités de Confiance sous Firefox

UTILISATEURS DE FIREFOX UNIQUEMENT

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.

0 Général	Général
 Contenu Applications Vie privée Sécurité Sync Appeé 	Démarrage
	Téléchargements Parcourir Enregistrer les fichiers dans le dossier Ioujours demander où enregistrer les fichiers Parcourir Toujours demander où enregistrer les fichiers Marcourir un nouvel onglet au lieu d'une nouvelle fenêtre Avertir lors de la fermeture de plusieurs onglets Me pas charger les onglets tant qu'ils ne sont pas sélectionnés Me pas charger les onglets tant qu'ils ne sont pas sélectionnés Me pas charger les onglets tant qu'ils ne sont pas sélectionnés Me pas charger les onglets tant qu'ils ne sont pas sélectionnés Me pas charger les onglets tant qu'ils ne sont pas sélectionnés Me pas charger les onglets tant qu'ils ne sont pas sélectionnés

2.3.1 L'installation de l'Autorité de Confiance Certeurope ROOT CA 3

Pour installer le certificat de l'Autorité Certeurope ROOT CA 3, suivez les étapes ci-après.

Entrez l'URL ci-dessous dans la barre adresse de Firefox et tapez sur entrée : http://www.certeurope.fr/reference/certeurope root ca 3.cer

La fenêtre suivante apparaît :



uverture de certeurope_root_ca_3.cer
Vous avez choisi d'ouvrir :
📮 certeurope_root_ca_3.cer
qui est un fichier de type : cer File (1,8 Ko)
à partir de : http://www.certeurope.fr
Que doit faire Firefox avec ce fichier ?
Ouvrir avec Parcourir
Enregistrer le fichier
☐ <u>T</u> oujours effectuer cette action pour ce type de fichier.
OK Annuler

Sélectionnez l'option Enregistrer le fichier, puis cliquez sur le bouton OK.

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



Allez dans Vie privée et sécurité/Sécurité (côté droit, en bas de la page)/Certificats puis cliquez sur Afficher les certificats



néral	10	Rechercher dans les options
cherche	Nous nous efforçons de vous laisser le choix et de recueillir uniquement les informations dont nous a améliorer Firefox pour tout le monde. Nous demandons toujours votre permission avant de recevo Politque de confidentialté	avons besoin pour proposer et ir des données personnelles.
e privée et sécurité	Autoriser Firefox à envoyer automatiquement des données techniques et des données d'inter	action à Mozilla En savoir plus
ompte Firefox	Autoriser Firefox à envoyer les rapports de plantage à Mozilia En savoir plus	
	Sécurité	
	Protection contre le hameçonnage	
	✓ Bloquer les contenus dangereux ou trompeurs	
	✓ Bloquer les téléchargements <u>d</u> angereux	
	Signaler la présence de logiciels indésirables ou peu communs	
	Certificats	
	Lorsqu'un serveur demande votre certificat personnel	
	En sélectionner un automatiquement	
	Vous demander à chaque fois	
	 Interroger le répondeur OCSP pour confirmer la validité de vos certificats 	Afficher les certificats
		Périphériques de sécurité
	Contenu web et données utilisateur hors connexion	
	Le cache d'applications utilise actuellement 295 Ko d'espace disque	Vider maintenant
	✔ Avertir lorsqu'un site souhaite conserver des données pour une utilisation hors connexion	Exceptions
	Les sites suivants sont autorisés à stocker des données pour une utilisation hors connexion :	
		Supprimer

La fenêtre suivante apparaît :

Dans l'onglet Autorités, cliquez sur Importer.

Voue poccód	an des certificats en	vegistrás identifias	nuves	artification :	
Nom du cer	tificat	egisti es identitiai	Périphérique de	sécurité	
Buypas	s Class 3 Root CA		Builtin Object Tok	(en	
Buypas	s Class 2 CA 1		Builtin Object Tok	cen	100
	•				-
Voir	Modifier la confi	ance Impor	rter Exporter	Supprimer ou ne p	olus faire confiance

Sélectionnez le certificat à importer certeurope_root_ca_3 puis cliquez sur Ouvrir.



Gestionnaire de certificats			23
Sélectionner un fichier contenant un (ou des) certificat(s) d'AC à importer	▼ 🍫 Reche	rcher dans : Télécharge	х . р
★ Favoris Nom ↓ Téléchargements ⊆ certeurope_root_ca_3.cer ■ Bureau E certeurope_root_ca_3.cer ↓ Fnac Cloud E certeurope_root_ca_3.cer ● Contraction E certeurope_root_ca_3.cer ● Displacements réce E mplacements réce ● Bibliothèques ↓ Sync	Modifié le 15/02/2016 12:26	Type Certificat de sécur	Taille
Bibliothèques	III Fichiers	de certificat (*.p7b;*.crt rir 🔽 Annuler	•

Cliquez sur OK.

Téléchargement du certificat
On vous a demandé de confirmer une nouvelle autorité de certification (AC).
Voulez-vous faire confiance à « Certeurope Root CA 3 » 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

Le Certificat de l'Autorité Racine est importé dans Firefox.



Nom du certificat	Périphérique de sécurité	世
Buypass Class 3 Root CA Buypass Class 2 CA 1	Builtin Object Token Builtin Object Token	
Certeurope Root CA 3	Sécurité personnelle	

Veuillez maintenant procéder à la même manipulation pour les certificats de l'Autorité Racine **CertEurope eID Root**.



2.3.2 L'installation de l'Autorité de Confiance CertEurope eID ROOT

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

https://www.certeurope.fr/reference/CertEurope_eID_Root.cer

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

Cliquez sur **OK**.

Veuillez maintenant procéder à la même manipulation pour les certificats de l'Autorité Intermédiaire **CERTEUROPE ADVANCED CA V4**.

2.3.3 L'installation du certificat de l'Autorité Certeurope ADVANCED CA V4

Pour installer le certificat de l'Autorité CertEurope ADVANCED CA V4, entrez dans la barre adresse de Mozilla Firefox l'url suivante :

http://www.certeurope.fr/reference/certeurope_advanced_v4.cer

Téléchargez le certificat certeurope_advanced_v4.cer puis importez-le dans Firefox de la même manière que précédemment.

Cliquez sur **OK**.

Veuillez maintenant procéder à la même manipulation pour les certificats de l'Autorité Intermédiaire **CertEurope eID User**.

2.3.4 L'installation du certificat de l'Autorité CertEurope elD User

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

https://www.certeurope.fr/reference/CertEurope_eID_User.cer

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

Cliquez sur **OK**.



2.4 Le paramétrage de Mozilla Firefox

Notre fournisseur Gemalto nous a signalé le risque qu'il pouvait y avoir de supprimer les certificats avec le navigateur Firefox.

CertEurope ne peut être tenu responsable de la suppression des certificats.

UTILISATEURS MOZILLA FIREFOX SEULEMENT

1- La clé toujours insérée, allez dans le menu **Outils/Options** du menu Firefox puis dans Vie privée/Sécurité (côté droit, en bas de page), puis cliquez sur **Périphériques de sécurité**.

néral		Rechercher dans les options
cherche	Nous nous efforçons de vous laisser le choix et de recueillir uniquement les informations dont nous améliorer Firefox pour tout le monde. Nous demandons toujours votre permission avant de receve Politique de conidientiatif	avons besoin pour proposer et bir des données personnelles.
privée et sécurité	Autoriser Firefox à envoyer automatiquement des données techniques et des données d'inter	raction à Mozilla En savoir plus
ompte Firefox	Autoriser Firefox à envoyer les rapports de plantage à Mozila En savoir plus	
	Sécurité	
	Protection contre le hameçonnage	
	✓ Bloquer les contenus dangereux ou trompeurs	
	Bloquer les téléchargements <u>d</u> angereux	
	Signaler la présence de logiciels indésirables ou peu communs	
	Certificats	
	Lorsqu'un serveur demande votre certificat personnel	
	En sélectionner un automatiquement	
	Vous demander à chaque fois	
	 Interroger le répondeur OCSP pour confirmer la validité de vos certificats 	Afficher les certificats
		Périphériques de sécurité
	Contenu web et données utilisateur hors connexion	
	Le cache d'applications utilise actuellement 295 Ko d'espace disque	Vi <u>d</u> er maintenant
	✓ Averțir lorsqu'un site souhaite conserver des données pour une utilisation hors connexion	Exceptions
	Les sites suivants sont autorisés à stocker des données pour une utilisation hors connexion :	

2- Dans l'onglet Certificats, cliquez sur Périphériques de Sécurité.



Modules et périphériques de sécurité	Détails	Valeur	Connexion
▲NSS Internal PKCS #11 Module	·		Déconnexion
Service de crypto. générique			
Sécurité personnelle	1.15		Changer le <u>m</u> ot de passe
	E		Charger
Module de bace intégré			Déc <u>h</u> arger
Builtin Object Token			Activer FIPS
Belgium eID PKCS#11 Module - beid	-		Active in s
tionnaire de périphériques			OK
tionnaire de périphériques	Dásile	Valaur	OK
tionnaire de périphériques Modules et périphériques de sécurité	Détails	Valeur	OK Co <u>n</u> nexion
tionnaire de périphériques Modules et périphériques de sécurité 4NSS Internal PKCS #11 Module Service de crypto, générique	Détails	Valeur	OK Co <u>n</u> nexion <u>D</u> éconnexion
tionnaire de périphériques Modules et périphériques de sécurité ▲NSS Internal PKCS #11 Module Service de crypto. générique Sécurité personnelle	Détails	Valeur	OK Co <u>n</u> nexion <u>D</u> éconnexion Changer le <u>m</u> ot de passe
tionnaire de périphériques Modules et périphériques de sécurité «NSS Internal PKCS #11 Module Service de crypto, générique Sécurité personnelle «Module de base intégré	Détails	Valeur	OK Co <u>n</u> nexion Déconnexion Changer le <u>m</u> ot de passe Charger
tionnaire de périphériques Modules et périphériques de sécurité « NSS Internal PKCS #11 Module Service de crypto. générique Sécurité personnelle « Module de base intégré Builtin Object Token	Détails	Valeur	OK Co <u>n</u> nexion <u>D</u> éconnexion Changer le <u>mot</u> de passe Charger Décharger
tionnaire de périphériques Modules et périphériques de sécurité ANSS Internal PKCS #11 Module Service de crypto. générique Sécurité personnelle AModule de base intégré Builtin Object Token	Détails	Valeur	OK Connexion Déconnexion Changer le mot de passe Charger Décharger
tionnaire de périphériques Modules et périphériques de sécurité ANSS Internal PKCS #11 Module Service de crypto. générique Sécurité personnelle AModule de base intégré Builtin Object Token	Détails	Valeur	OK Co <u>n</u> nexion Déconnexion Changer le <u>m</u> ot de passe Charger Déc <u>h</u> arger Activer <u>F</u> IPS

- 3- Cliquez sur **Charger** pour définir le nouveau dispositif.
- 4- Entrez le nom du module : **TKM**



5- Cliquez sur **Parcourir** et rechercher IDPrimePKCS11.dll dans :

Ordinateur (pour Microsoft Windows -32bits)

C:\Program Files\Gemalto\IDGo 800 PKCS#11\IDPrimePKCS11.dll

www.certeurope.fr

Ordinateur (pour Microsoft Windows -64bits)

- Si Firefox 32 bits alors: C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11\IDPrimePKCS11.dll
- Si Firefox 64 bits alors C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11\IDPrimePKCS1164.dll



Comment connaître ma version de Firefox sur mon poste? Allez dans le menu Outils et sélectionnez "Ouvrir le menu d'aide"



Cliquez sur à propos de Firefox



Votre version de Firefox est alors affichée.





6-Puis cliquez sur OK.

Modules et périphériques de sécurité		Détails	Valeur		Connexion
Service de crypto. générique Sécurité personnelle	^	Statut	Non connecté Gemalto USB Key Smart	-	<u>D</u> éconnexion
Module de base intégré		Fabricant	Unknown	_	Changer le <u>m</u> ot de passe
Builtin Object Token	=	Version HW	0.0	=	Charger
4 TKM		Version FW	0.0		-
Card #E8D6766069EBB7F5		Étiquette	Card #E8D6766069EBB7F5		Decharger
Broadcom Corp Contacted Smart	-	Fabricant	Gemalto		Activer <u>FI</u> PS
Belgium eID PKCS#11 Module - beid	-	Numéro de série	E8D6766069EBB7F5	-	

Le module TKM apparaît dorénavant sur la colonne de gauche (ne pas faire attention si vous n'avez pas de ligne supplémentaire en dessous).

Votre certificat est installé.

Quittez Firefox puis relancez-le.

3. Quatrième étape : test de bon fonctionnement de votre certificat

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.
- Entrez ensuite votre code PIN pour finaliser l'identification. 3-

Attention : Sur Firefox, la demande de mot de passe principal (qui correspond à la demande de code PIN) apparaît avant la sélection du certificat. Il faudra saisir le code PIN, faire OK puis sélectionner le certificat.





Vous voici sur la page CertiServices.

Bonjour Votre certificat est valide Il expire le 31/01/2017 Informations sur votre certificat		Vous n'avez pas défini de Code de Révocation d'Urgence Définir un code de révocation
CertEurope Une société du groupe o odrive	SERVICES	
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).	Choisir ou moo Ce code vous serv strictement confid Assurez-vous don Si votre support ci d'enregistrer un C CRU au bon certifi systématiqueme Pour renseigner vu Pour reisequer vot +33 (0) 826 300 Révoquer votr Vous quittez votre cette page.	Révocation difier votre code de Révocation d'Urgence (CRU): vira à révoquer votre certificat en cas de perte ou de vol de votre clé. Ce code vous est entiel, nous serons dans l'impossibilité de vous le communiquer en cas d'oubli. c de choisir un code de 6 à 8 caractères que vous n'oublierez pas. rryptographique (clé ou carte à puce) contient 2 certificats, vous avez la possibilité RU, identique ou différent, pour chacun des certificats. If fadura alors associer le bon icat. Sachez cependant que la révocation d'un des certificats entraine ent la révocation de l'autre. otre CRU cliquer ici. tre certificat, munissez vous de votre CRU et contactez le numéro de téléphone suivant: o 421 (disponible 24H/24 - 7J/7). re certificat en ligne: société ou n'êtes plus amené à utiliser votre certificat. Vous pouvez le révoquer depuis
CertiServices - ©C	CertEurope - mentions léga	ales

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

Votre certificat est valide et installé.

🔀 Si votre clé contient 2 certificats vous devez effectuer cette procédure avec les 2 certificats.

Pour les utilisateurs de Windows 8.1 : Si vous utilisez Internet Explorer pour vos connexions sécurisées (avec notre certificat), il vous faudra être en mode bureau exclusivement (Procédure indiquée plus haut).

3.1 La génération 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...)

www.certeurope.fr



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 CertiServices (https://services.certeurope.fr/) en sélectionnant le certificat pour lequel vous souhaitez définir le code CRU. Puis entrez votre code PIN. Vous êtes alors authentifié sur la page CertiServices.

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

Bonjour Votre certificat est valide Il expire le 31/01/2017 Informations sur votre certificat			Vous n'avez pas défini de Code de Révocation d'Urgence Définir un code de révocation	
Une société du groupe oodrive	CERTISERVICES Connecté: TEST DODRIVE			
Informations sur le certificat Vous trouverez sur cette page le détail de votre certificat et le lien de télécharger (notamment utile pour l'inscription au Service d'Immatriculation des Véhicules).	ment de votre certificat	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 cité. Ce code strictement confidentiel, nous servas 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 votre support cryptographique (clé qu carte à puce) contient 2 certificats, vous avez la possibil d'enregisterr un CRU, identique ou différent, pour chance des certificats. Il faudra alors associer CRU au bon certificat. Sachez copendant que la révocation d'un des certificats entraine systématiquement la révocation de l'autre. Pour renseigner votre CRU cliquer ici. Pour reisogner votre certificat, munissez vous de votre CRU et contactez le numéro de téléphone +33 (d) 26 5 300 412 (disponible 24/24 - 7.07). Révoquer votre certificat en ligne: Vous suittez votre société ou n'êtes plus amené à utiliser votre certificat. Vous pouvez le révoquer		
	CertiServices - @CertE	UFODE - 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 que vous n'oublierez pas !

À 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.

3.2 La Révocation d'Urgence

Pour révoquer votre certificat, rendez-vous à l'adresse suivante et suivez les étapes indiquées :

https://support.certeurope.fr/revocation

3.3 Déblocage de la clé

La procédure de déblocage de clé est similaire à la procédure d'activation.

Attention : vous devez être connecté à Internet pour pouvoir débloquer votre clé.

- 1- Insérez votre clé.
- 2- Démarrer Trusted Key Manager (voir la section 1.5 pour savoir comment lancer l'application)
- 3- Cliquez sur débloquer



III Trusted Key Manager	– 🗆 X
VOTRE CLÉ EST BLOQUÉE !	Support EIDAS TEST
Délivré à : Support EIDAS TEST	 Authentification, Signature de documents Valide jusqu'au 22/08/2020
Délivré par : CertEurope elD User	Support EIDAS TEST
Numéro de série : B81E057FFC87A7A2	Authentification, Signature de documents Valide jusqu'au 22/08/2020
Modifier le Code PIN Débloquer	
	0

4- Un code d'activation vous est envoyé selon la modalité choisie lors de la commande de la clé: - soit par email,

- soit par SMS sur votre téléphone portable

Entrez le code récupéré par mail ou téléphone et cliquez sur valider.

Trusted Key Manager			
Entrez le code d'activation reçu par email ou par téléphone			
	707109		
Le code vient d'être envoyé à l'adresse email:		Valider	
r.t*******.fr			
Nous vous invitons à renseigner le code ci-contre.			
			ANNULER
			9

5- Saisissez votre PIN sur le clavier virtuel et cliquez sur **OK**.





6- Confirmez le PIN de votre clé de nouveau et cliquez sur OK.



7- Votre clé est débloquée et votre nouveau PIN enregistré.



Trusted Key I	Manager			– 🗆 X
Ø,	VOTRE CLÉ EST PRÊTE À	NÊTRE UTILISÉE !		Support EIDAS TEST
Dáliozá à c				Authentification, Signature de documents
	Succès			
	Votre clé est prête	e à être utilisée !		
			_	
				ОК
•			_	
M	odifier le Code PIN			
				Ø

4. Changement de code PIN

Attention, au bout de 5 mauvaises saisies du code PIN, votre clé sera bloquée.

- 1- Insérez votre clé.
- 2- Démarrer Trusted Key Manager (voir la section 1.5 pour savoir comment lancer l'application)
- 3- Cliquez Modifier le Code PIN

III Trusted Key Manager	- 🗆 X
VOTRE CLÉ EST PRÊTE À ÊTRE UTILISÉE !	Support EIDAS TEST
Délivré à : Support EIDAS TEST	 Authentification, Signature de documents Valide jusqu'au 22/08/2020
Délivré par : CERTEUROPE ADVANCED CA V4	Support EIDAS TEST
Numéro de série : B81E057FFC87A7A2	Authentification, Signature de documents Valide jusqu'au 22/08/2020
Modifier le Code PIN Débloquer	
	0

4- Saisissez le PIN actuel de votre clé à l'aide du pavé virtuel :



Trusted Key Manager					
Entrez votre PIN actuel					
Le code PIN est confidentiel et ne doit pas être communiqué à un tiers	4	1		5	
Votre code PIN est composé de 4 chiffres uniquement.			9	0	
	7	8			
		2	6	ОК	
					_
• • •				ANNULER	
					?

5- Saisissez votre PIN sur le clavier virtuel et cliquez sur OK.



6- Confirmez le PIN de votre clé de nouveau et cliquez sur OK.





7- Votre nouveau PIN enregistré.

