

Certificats Logiciel

Manuel d'installation

Internet Explorer et Chrome sous Windows 7



V.12022014-01



Procédure d'installation du certificat logiciel pour Internet Explorer et Chrome sous Windows 7

Introduction

Ce manuel décrit comment installer un certificat logiciel dans le magasin de confiance de Windows. Ce magasin de confiance est le coffre fort de Windows qui contient les certificats. Il est utilisé par les navigateurs Internet Explorer (IE) et Chrome. La procédure d'installation du certificat sur les 2 navigateurs est donc la même.

Pré-requis

Pour installer votre certificat logiciel vous devez au préalable :

- Disposer des droits suffisants pour installer un certificat.
- L'avoir téléchargé sur votre ordinateur.
- Connaitre le mot de passe qui protège votre certificat et que vous avez choisi lors de son retrait .

Installation

1- Double cliquer sur le fichier qui correspond à votre certificat. C'est un fichier qui doit avoir une extension « .P12 »



La fenêtre suivante se lance automatiquement vous permettant de suivre les étapes d'importation. Cliquez sur « Suivant » :

Bienvenue !
Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats depuis votre disque vers un magasin de certificats.
Un certificat, émis par une autorité de certification, est une confirmation de votre identité et contient des informations utilisées pour protéger vos données ou établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés.
Cliquez sur Suivant pour continuer.
 < Précédent Suivant > Annuler





2- Dans la fenêtre suivante laissez l'emplacement tel quel ensuite cliquer sur suivant :

Assistant Importation de certificat	×	
Fichier à importer		
Spécifiez le fichier à importer.		
Nom du fichier :		
C:\Users\m.samimi\Downloads\TEST F	GS 1 ETOILE AUTHENTIFICA Parcourir	
Remarque : des certificats peuvent être stockés dans un fichier aux formats suivants :		
Échange d'informations personnelles - PKCS #12 (.PFX,.P12)		
Standard de syntaxe de message de chiffrement - Certificats PKCS #7 (.P7B)		
Magasin de certificats sérialisés Microsoft (.SST)		
En savoir plus sur les <u>formats de fichiers de certificats</u>		
	< Précédent Suivant > Annuler	

3- Saisissez le mot de passe qui protège votre certificat puis cliquez sur « Suivant » :

Assistant Importation de certificat		
Mot de passe Pour maintenir la sécurité, la dé privée a été protégée avec un mot de passe.		
Entrez le mot de passe de la dé privée.		
Mot de passe :		
Activer la protection renforcée de clés privées. Une confirmation vous sera demandée à chaque utilisation de la dé privée par une application.		
Marquer cette dé comme exportable. Cela vous permettra de sauvegarder et de transporter vos dés ultérieurement.		
Indure toutes les propriétés étendues.		
En savoir plus sur la <u>protection des dés privées</u>		
< Précédent Suivant > Annuler		



5- Sélectionnez le choix suivant et cliquez sur suivant :

maya	sin de certificats
b	es magasins de certificats sont des zones système ou les certificats sont stockes.
v	/indows peut sélectionner automatiquement un magasin de certificats, ou vous
P	ouvez speciner remplacement ou certincat.
+	Sélectionner automatiquement le magasin de certificats selon le type de certifica
	Placer tous les certificats dans le magasin suivant
	Magasin de certificats :
	Parcourir
En sav	roir plus sur les <u>magasins de certificats</u>
En sav	roir plus sur les <u>magasins de certificats</u>
En sav	voir plus sur les <u>magasins de certificats</u>

6- Il suffit de cliquer sur terminer dans cette dernière fenêtre afin d'installer le certificat dans le magasin de certificats.

Assistant Importation de ce	rtificat	X	
	Fin de l'Assistant Importation de certificat		
	Ce certificat sera importé après que vous aurez diqué sur Terminer. Vous avez spécifié les paramètres suivants :		
	Magasin de certificats sélection Contenu Nom du fichier	nné Déterminé automatiqu PFX C:\Users\m.samimi\Do	
	< <u> </u>	ł	
	< Précédent	Terminer Annuler	



Si vous ne disposez pas déjà d'un certificat Certeurope l'écran suivant va s'afficher pour vous informer que le certificat « racine » de Certeurope va être installé. Cliquer sur « oui ».

Avertissement de sécurité	
Vous êtes sur le point d'installer un certificat à partir d'u certification (CA) demandant à représenter : Certeurope Root CA 3 Windows ne peut pas valider que le certificat vient réell "Certeurope Root CA 3". Vous devriez confirmer son or contactant "Certeurope Root CA 3". Le numéro suivant effectuer cette tâche :	une autorité de lement de rigine en t va vous aider à
Aperçu (sha1) : 9E0B281C E8EAF568 11E09C8D 65905B1 Avertissement : Si vous installez ce certificat racine, Windows va autom approuver tout certificat émis par cette autorité de cert L'installation d'un certificat avec un aperçu non confirr de sécurité. Si vous cliquez sur "Oui" vous reconnaissez Voulez-vous installer cette certification ?	9 14E169FD latiquement ification. né est un risque : ce risque.
Oui	Non

La fenêtre suivante indique le bon déroulement du processus d'installation :



Vérification de la bonne installation de votre certificat

Afin de valider la bonne installation de votre certificat nous vous invitons à accéder à un site qui requiert l'authentification par Certificat en utilisant Chrome ou Internet explorer. Voici une URL qui requiert l'authentification forte : <u>https://services.certeurope.fr</u>.



Sélectionner le certificat installé, puis cliquez sur OK pour afficher la page suivante :



← ⓒ 🌈 https://services.certeurope.fr/	🥖 ::: CertEurope - CertiService 🗙 👘 🏠 😳				
Bonjour TEST OODRIVE	Vous n'avez pas défini de Code de Révocation d'Urgence				
Il expire le 31/01/2017					
Informations sur votre certificat	Définir un code de révocation				
Certiservices Certiservices Une société du groupe oodrive Connecté: TEST OODRIVE Informations sur le certificat Révocation					
téléchargement de votre certificat (notamment utile pour l'inscription au Service d'Immatriculation des Véhicules).	 Choisir ou modifier votre code de Revocation d'orgence (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. Si votre support cryptographique (clé ou carte à puce) 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 d'un des 				
	Pour renseigner votre CRU cliquer ici.				

L'affichage de cette page vous indique que l'installation c'est correctement effectuée, car vous vous êtes authentifié sur un site web avec le certificat installé.