

Guide technique d'exportation des clés privées *d'Entrust*

Direction des registres et de la certification
du ministère de la Justice

Mise en garde

Ce document vise à faciliter l'exportation des clés privées des certificats *Entrust*. Selon l'environnement technologique utilisé, le comportement du logiciel peut différer de celui décrit dans ce document. Il est donc fortement recommandé de vérifier d'abord les exigences techniques requises puis, si l'environnement technologique de l'utilisateur diffère de celui indiqué dans le présent document, de communiquer avec le Centre d'assistance technologique du Service de certification du ministère de la Justice.

Note

Ce document comporte plusieurs noms composés de mots ou d'expressions qui constituent des marques de commerce. Afin d'alléger le texte et d'en faciliter la lecture, les symboles « ^{MC} », « TM », « ^{MD} » ou « [®] » ne sont pas mentionnés à la suite de ces mots ou expressions.

Service de certification
Direction des registres et de la certification
Ministère de la Justice
1, rue Notre-Dame Est, bureau 7.35
Montréal (Québec) H2Y 1B6

Site Web : www.infocles.justice.gouv.qc.ca
Courriel : services@infocles.justice.gouv.qc.ca
Téléphone : 514 864-4949* (Montréal et les environs)
418 646-4949* (Québec et les environs)
1 800 465-4949* (sans frais)
* Choisir l'option 3
Télécopieur : 514 864-2346

Table des matières

1.	Introduction.....	4
2.	Systèmes d'exploitation et logiciel requis.....	4
3.	Notes sur l'utilisation de PKCS12	4
4.	Exportation des clés privées	5
	4.1 Étapes d'exportation	5
	4.2 Explication des options	7
5.	Importation des clés privées dans le magasin de <i>Windows</i>	7
	5.1 Étapes d'importation	7
	5.2 Explication des options	10

1. Introduction

Le logiciel *Entrust Entelligence* est une application dont le rôle est d'assurer la gestion transparente et automatique des certificats, des opérations de signature et de chiffrement ainsi que l'exportation des clés en différents formats, par exemple PKCS12 ou PKCS7.

Ce document a pour but de décrire les étapes et les précautions à suivre pour exporter des clés privées, en format PKCS12, d'une façon sécuritaire à l'aide du logiciel *Entrust Entelligence*¹, puis les importer dans le magasin des certificats *Windows*.

Les clés exportées en format PKCS12 peuvent être utilisées avec d'autres applications pour :

- ▶ authentifier des dispositifs à partir des services Web;
- ▶ authentifier les clients à une application Web (ex. : clicSécur);
- ▶ signer un document à partir d'une page Web;
- ▶ utiliser avec WS-FTP.

2. Systèmes d'exploitation et logiciel requis

- ▶ Systèmes d'exploitation : *Microsoft Windows* NT 4.0, 2000 ou XP.
- ▶ Logiciel : *Entrust Entelligence*.
- ▶ Un certificat d'*Entrust Entelligence* valide et exportable en format **PKCS12**.

3. Notes sur l'utilisation de PKCS12

- ▶ Par défaut, l'exportation en format PKCS12 n'est pas disponible pour les certificats. Pour avoir cette option, contacter le [Service de certification](#).
- ▶ En exportant le certificat .epf d'*Entrust* en format **PKCS12**, trois fichiers sont générés (ex. : jtremblay.epf) :
 - le certificat et la clé de signature
 - ex. : jtremblay signature.p12
 - le certificat et la clé de chiffrement
 - ex. : jtremblay déchiffrement.p12
 - un fichier contenant des références aux deux fichiers ci-dessus
 - ex. : jtremblay.p12
- ▶ L'exportation ne peut continuer que si une session d'*Entrust* est ouverte et active.
- ▶ Les fichiers doivent être créés dans un dossier sur le disque local. *Entrust* refuse de faire l'exportation dans un dossier partagé sur le réseau.
- ▶ Les trois fichiers de format **PKCS12** (.p12) contiennent un mot de passe, que l'utilisateur définit durant l'exportation des clés, pour protéger la clé privée.
- ▶ Durant l'exportation, ce mot de passe est créé et doit respecter les règles sécuritaires d'*Entrust*.
- ▶ Ce mot de passe est différent de celui utilisé avec les logiciels d'*Entrust*.
- ▶ Ce mot de passe est utilisé pour déchiffrer le contenu du fichier **PKCS12** durant l'importation des clés.
- ▶ Une fois les clés exportées, elles seront utilisables à partir d'autres applications, mais sans validation Entrust.

L'utilisateur peut importer le fichier de signature ou de déchiffrement. Si le troisième fichier est importé (ex. : jtremblay.p12), les deux fichiers (de signature et de déchiffrement) sont importés automatiquement.

¹ Dans ce document, les captures d'écran ont été réalisées à partir d'*Entrust Entelligence* 7.0.

4. Exportation des clés privées

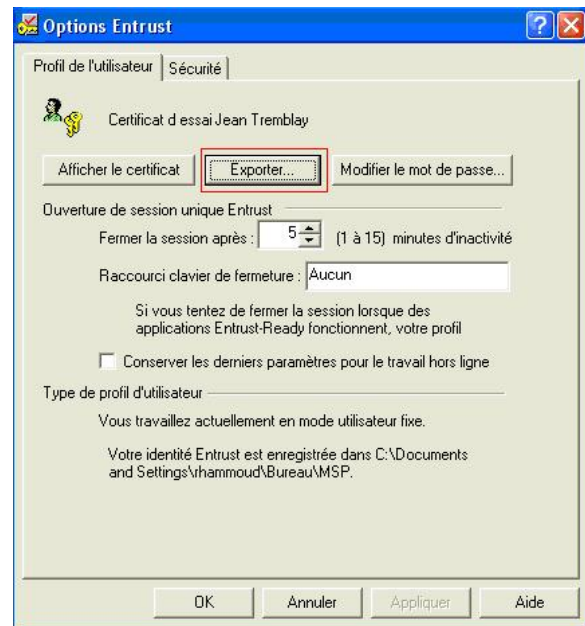
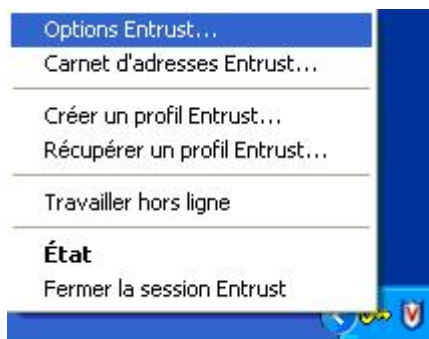
Pour obtenir le logiciel *Entrust Entelligence*, il faut d'abord communiquer avec le [Service de certification](#).

4.1 Étapes d'exportation

Une session d'*Entrust* doit cependant être ouverte pour effectuer l'exportation.

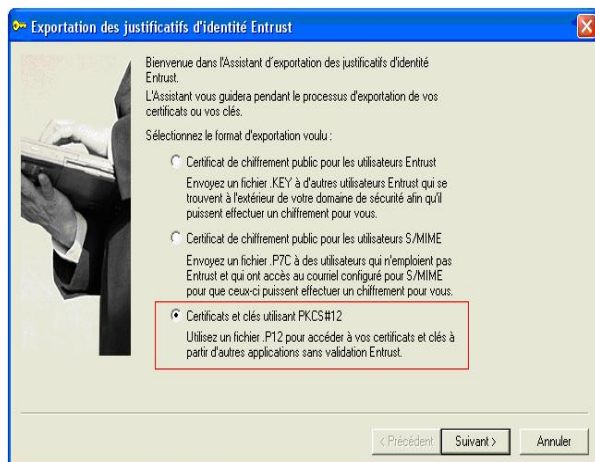
Pour exporter les clés, suivre les étapes suivantes :

1. Positionner le curseur sur l'icône *Entrust* représentant une clé jaune et cliquer sur le bouton droit de la souris. À l'aide du bouton gauche de la souris, cliquer sur « Options Entrust... ».
2. Sous l'onglet « Profil de l'utilisateur », cliquer sur le bouton « Exporter... ».

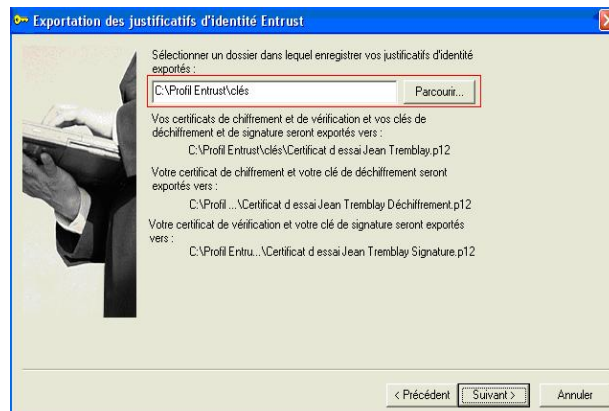


Une première fenêtre apparaîtra pour confirmer l'authentification du demandeur. Puis, si ce dernier s'authentifie correctement, la fenêtre permettant la modification du mot de passe apparaîtra.

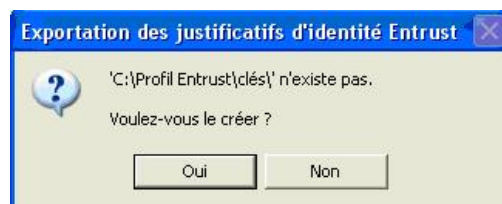
3. La fenêtre suivante apparaîtra. Choisir la troisième option « Certificats et clés utilisant PKCS#12 ». Cliquer sur le bouton « Suivant ».



4. La fenêtre suivante apparaîtra. Spécifier le dossier où les clés exportées seront classées. Cliquer sur le bouton « Suivant ».



Si le dossier n'existe pas, la fenêtre suivante apparaîtra

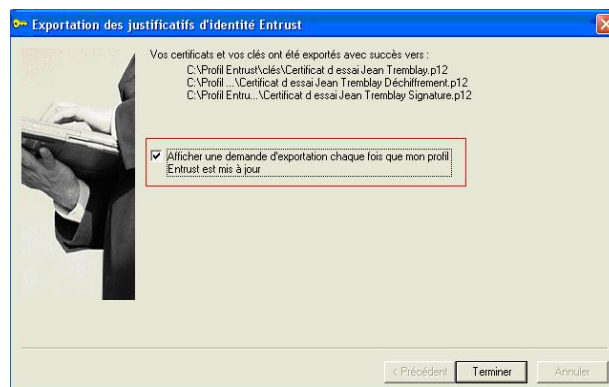


- Cliquer sur le bouton « Oui ».

5. La fenêtre suivante apparaîtra. Choisir un nouveau mot de passe. **Il est fortement recommandé de choisir un mot différent que celui du certificat lui-même.** Cliquer sur le bouton « Exporter ».



6. La fenêtre suivante apparaîtra. Cocher l'option « Afficher une demande d'exportation chaque fois que mon profil Entrust est mis à jour »².
7. Cliquer sur le bouton « Terminer ». Les clés sont prêtes à être importées.



² Consulter la section suivante pour l'explication de cette option.

4.2 Explication des options

Option	Cochée	Non cochée
Afficher une demande d'exportation chaque fois que mon profil <i>Entrust</i> est mis à jour.	La prochaine fois qu'une session d' <i>Entrust</i> est ouverte et que le profil d' <i>Entrust</i> est mis à jour, un message <u>sera affiché</u> pour rappeler l'utilisateur à répéter l'exportation des clés privées. <u>Les clés déjà exportées ne seront pas mises à jour automatiquement.</u>	La prochaine fois qu'une session d' <i>Entrust</i> est ouverte et que le profil d' <i>Entrust</i> sera mis à jour, le message de rappel <u>ne sera pas</u> affiché. <u>Les clés déjà exportées ne seront pas mises à jour automatiquement.</u>

5. Importation des clés privées dans le magasin de *Windows*

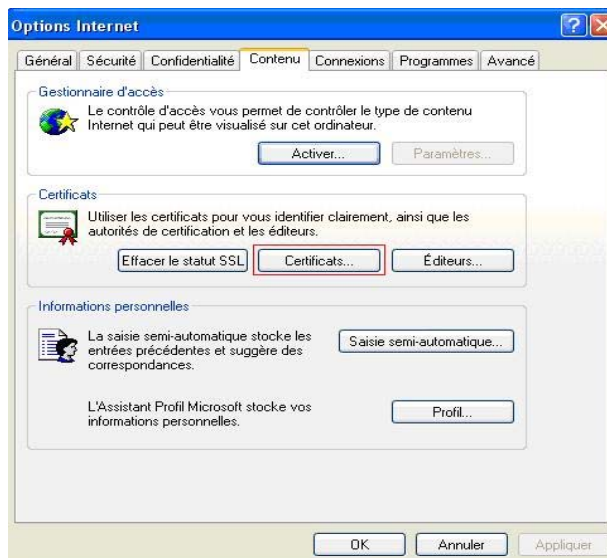
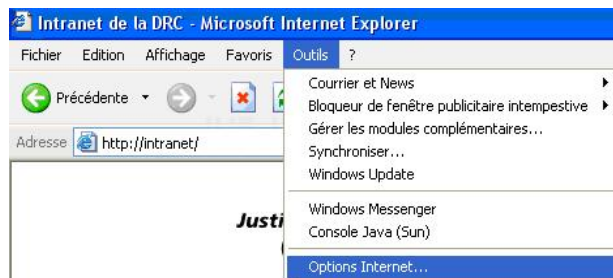
Une fois les clés exportées, elles sont prêtes à être utilisées avec différentes applications. Dans ce document, on va décrire les étapes de l'importation dans le magasin de *Windows*, afin de les utiliser avec les pages Web.

5.1 Étapes d'importation

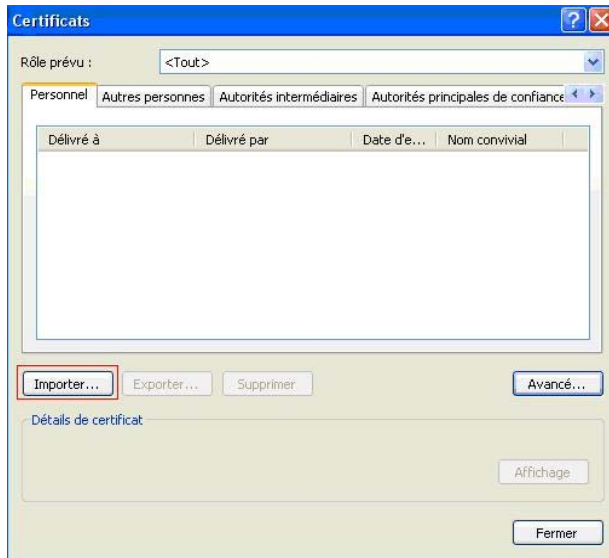
Une session d'*Entrust* n'est pas requise pour effectuer l'importation.

Pour importer les clés, suivre les étapes suivantes :

1. Ouvrir une page d'*Internet Explorer*, cliquer sur le menu déroulant « Outils » et choisir l'option « Options Internet... ».
2. La fenêtre suivante apparaîtra. Cliquer sur l'onglet « Contenu » puis cliquer sur le bouton « Certificats... ».



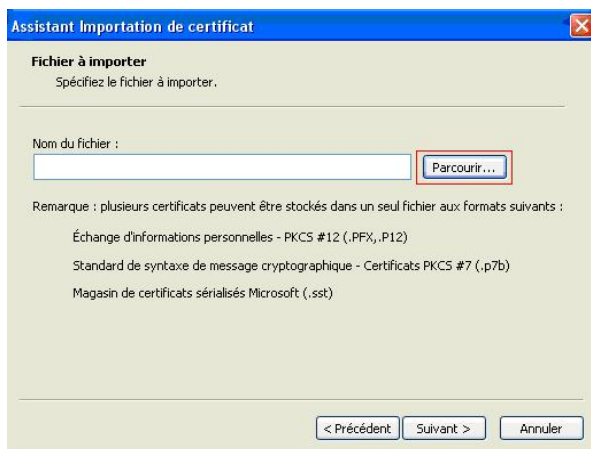
3. La fenêtre suivante apparaîtra. Cliquer sur le bouton « Importer... ».



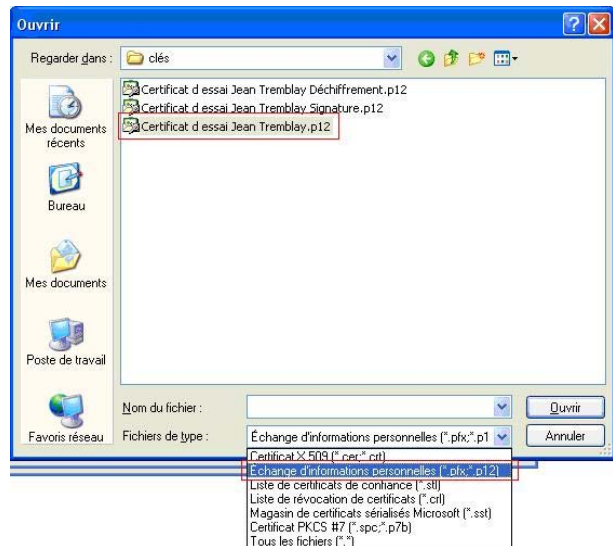
4. La fenêtre suivante apparaîtra. Cliquer sur le bouton « Suivant ».



5. La fenêtre suivante apparaîtra. Cliquer sur le bouton « Parcourir... » pour chercher le fichier des clés privées.

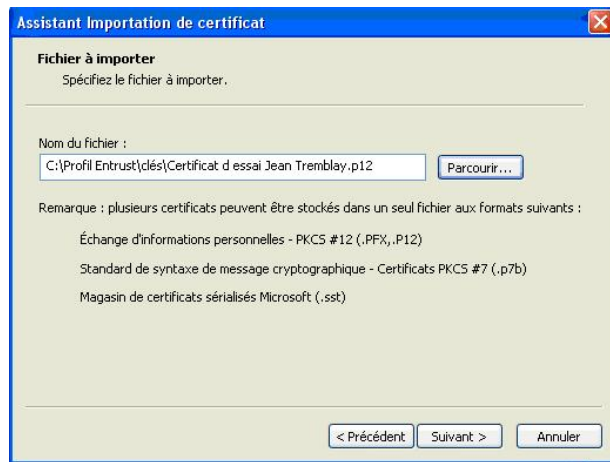


6. La fenêtre suivante apparaîtra. Naviguer jusqu'au dossier où les clés étaient exportées. S'assurer que le type de fichiers est changé pour « Échange d'informations personnelles (*.pfx, *.p12) ».



7. Sélectionner le fichier qui contient le nom du profil seulement.
8. Cliquer sur le bouton « Ouvrir ».

9. Cliquer sur le bouton « Suivant ».

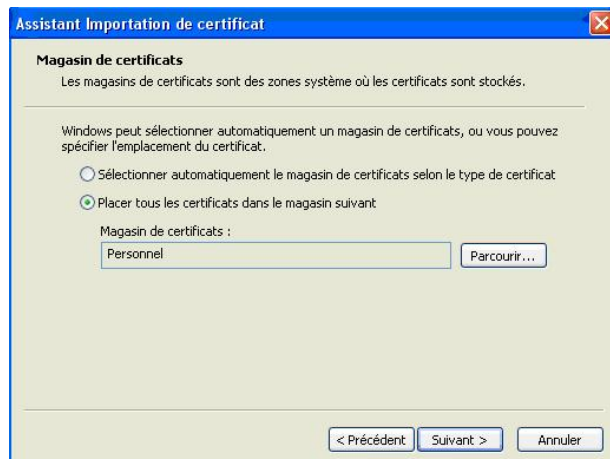


10. La fenêtre suivante apparaîtra. Saisir le mot de passe qui a été choisi dans l'étape de l'exportation des clés privées et cliquer sur le bouton « Suivant ».

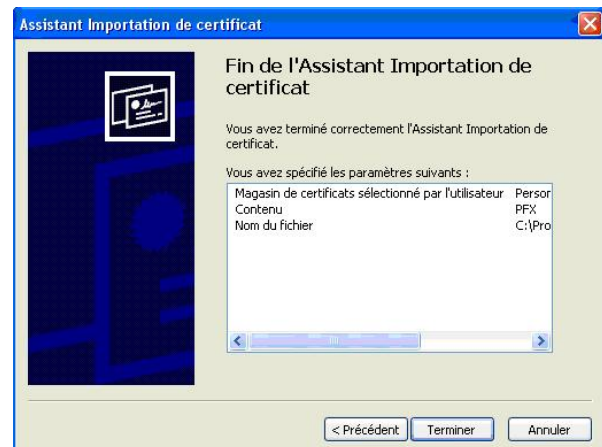
- Consulter la section suivante pour choisir les options affichées.



11. La fenêtre suivante apparaîtra. Cliquer sur le bouton « Suivant ».



12. La fenêtre suivante apparaîtra. Cliquer sur le bouton « Terminer ».



13. La fenêtre suivante apparaîtra. Cliquer sur le bouton « OK ».



5.2 Explication des options

Option	Cochée	Non cochée
Activer la protection renforcée de clés privées. La clé privée vous sera demandée chaque fois qu'elle est utilisée par une application si vous activez cette option.	L'utilisateur devra saisir le mot de passe chaque fois une application utilisera ces clés.	Rien
Marquer cette clé comme exportable. Cela vous permettra de sauvegarder et de transporter vos clés ultérieurement.	Les clés publiques et privées pourront être exportées du magasin des certificats.	Seules les clés publiques pourront être exportées du magasin des certificats.