Guide d’utilisation des principales fonctions d’*Entrust Entelligence Security Provider*

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

Québec

Mise en garde

Selon l'environnement technologique utilisé, le fonctionnement 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 diffère de celui indiqué dans le présent document, de communiquer avec son centre d'assistance technologique.

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 : 418-643-5140, option 2 (Québec et les environs)
1-866-536-5140, option 2 (sans frais)
Télécopieur : 514 864-2346

Table des matières

1. Introduction

Ce document décrit les principales fonctions du logiciel *Entrust Entelligence Security Provider 10* (EESP). Ce logiciel est le cœur de la famille des produits *Entrust.* Il est notamment requis pour signer et chiffrer des fichiers et, lorsqu'il est utilisé avec le logiciel approprié[1], pour signer ou chiffrer des courriels ou des répertoires.

Pour plus de renseignements sur l'utilisation du logiciel, le lecteur doit s'adresser à son centre d'assistance technologique.

Les fonctionnalités décrites dans ce guide sont valables pour les certificats d'individu et pour les certificats de groupe. Comme son nom l'indique, le certificat d'individu est rattaché à un seul individu et n'est donc pas partageable. Le certificat de groupe est partageable. Il appartient au responsable du certificat de groupe de désigner les personnes qui seront autorisées à l'utiliser. Les documents sécurisés avec un certificat de groupe peuvent être déchiffrés par toutes les personnes ainsi désignées.

2. Systèmes d'exploitation, logiciel requis et préalable

- Systèmes d'exploitation :
  - Microsoft Windows 7 – Toutes les versions 32 bits et 64 bits ayant la rustine Windows « 10.0.40 » et plus
  - Microsoft Windows 8.1 Pro et 8.1 Enterprise
  - Microsoft Windows 10 Pro et 10 Enterprise
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2016
- Logiciel requis : EESP 10.
- Préalable : Détenir des clés et des certificats valides délivrés par le Service de certification du ministère de la Justice (MJQ).

3. Conventions

Ce symbole indique une note importante pour le lecteur.

Ce symbole indique un avertissement ou une mise en garde importante.

4. Principales fonctions d'EESP 10

Une fois EESP installé sur le poste de travail, il sera possible de :

- **signer numériquement un fichier** : cette fonction permet notamment d'authentifier le signataire d'un fichier. Puisque le fichier a été seulement signé, toute personne possédant des clés et des certificats valides délivrés par le Service de certification du MJQ peut accéder à son contenu.
- **chiffrer un fichier pour soi-même** : cette fonction permet de protéger un fichier pour que seule la personne qui a chiffré ce fichier puisse avoir accès à son contenu.
- **chiffrer un fichier pour d'autres personnes** : cette fonction permet de protéger un fichier et de rendre son contenu accessible seulement aux personnes pour lesquelles le fichier a été chiffré. Ces

[1] La composante *Outlook* d'*Entrust Entelligence* permet de signer et de chiffrer des courriels.

personnes doivent détenir des clés et des certificats valides délivrés par le Service de certification du MJQ.

- **chiffrer et signer un fichier pour soi-même et pour d'autres personnes** : cette fonction permet notamment d'authentifier le signataire du fichier tout en rendant le contenu du fichier accessible seulement aux personnes pour lesquelles il a été chiffré.
- **déchiffrer et vérifier un fichier sécurisé** : le déchiffrement permet à l'utilisateur d'accéder au contenu des fichiers qui ont été préalablement chiffrés pour lui et de vérifier la validité des clés et des certificats qui ont été utilisés pour signer et chiffrer le fichier.

Avant d'utiliser l'une de ces fonctions, il faut s'assurer de connaître la gestion des sessions (ouverture et fermeture d'une session *Entrust* et gestion du certificat *Entrust*).

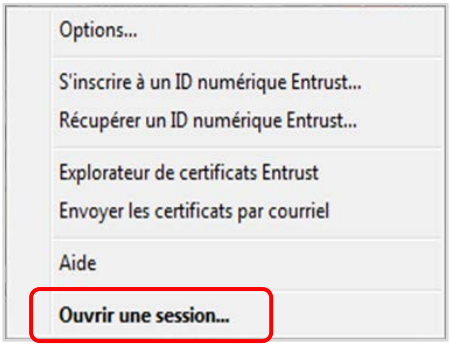
4.1 Ouvrir une session *Entrust*

L'ouverture d'une session *Entrust* est préalable à l'utilisation des fonctions d'*Entrust*.

Pour ouvrir une session *Entrust*, il faut posséder un fichier « *.epf » (ce dernier devrait avoir été créé après un appel au Service de certification du MJQ). Ce fichier est indispensable à l'ouverture d'une session *Entrust* puisqu'il contient tous les renseignements pertinents pour authentifier l'utilisateur et pour chiffrer et déchiffrer les fichiers.

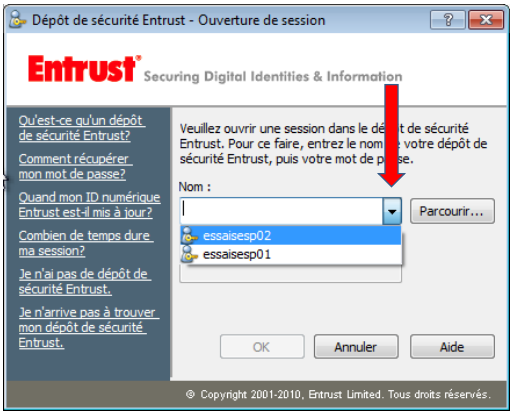
Pour ouvrir une session *Entrust* :

1. Dans la barre de notification de *Windows*, cliquer, en utilisant le bouton droit de la souris, sur l'icône et sélectionner l'option « Ouvrir une session… ».



2. Trois situations peuvent se présenter :

   a. Si le nom de profil apparaît dans le champ « Nom », saisir le mot de passe lié aux clés et certificats et cliquer sur le bouton « OK ».
   b. Si le nom de profil n'apparaît pas, cliquer sur le menu déroulant, sélectionner le nom et saisir le mot de passe et cliquer sur le bouton « OK ».



   c. Si le nom n'apparaît pas lorsque l'on clique sur le menu déroulant, cliquer sur le bouton « Parcourir… » et sélectionner le fichier « *.epf ».

Ne pas saisir le nom manuellement dans le champ « Nom ». Le lien entre le fichier « *.epf » et le nom du profil doit être établi par *Entrust*.

Si l'utilisateur ne trouve pas son profil *Entrust* avec la fonction « Parcourir », il peut faire une recherche du fichier « *.epf » sur le disque dur de son ordinateur :

- ***Windows 7*** : Cliquer sur « Démarrer→Rechercher » et saisir « *.epf » dans le champ « Rechercher les programmes et fichiers ». Une fois le fichier trouvé, cliquer sur ce fichier avec le bouton droit de la souris et sélectionner l'option « Ouvrir l'emplacement du fichier » pour prendre connaissance de sa localisation sur le poste de travail. Par la suite, dans la fenêtre d'ouverture de session d'*Entrust*, il sera possible d'utiliser l'option « Parcourir ».
- ***Windows* 8** : Cliquer sur « Démarrer » dans le coin inférieur gauche de l'écran, sélectionner « Rechercher » et appuyer sur la touche « Retour ». Dans la boîte de recherche à la droite de l'écran, saisir « *.epf » dans le champ prévu à cet effet. Une fois le fichier trouvé, cliquer sur ce fichier avec le bouton droit de la souris pour voir son emplacement. On peut également accéder au fichier en sélectionnant l'icône « Ouvrir le dossier » pour prendre connaissance de sa localisation sur le poste de travail. Par la suite, dans la fenêtre d'ouverture de session d'*Entrust*, il sera possible d'utiliser l'option « Parcourir ».
- ***Windows* 10** : Cliquer sur « Démarrer » dans le coin inférieur gauche de l'écran et saisir « *.epf » dans la boîte de recherche. Une fois le fichier trouvé, cliquer sur ce fichier avec le bouton droit de la souris et sélectionner l'option « Ouvrir le dossier » pour prendre connaissance de sa localisation sur le poste de travail. Par la suite, dans la fenêtre d'ouverture de session d'*Entrust*, il sera possible d'utiliser l'option « Parcourir ».

4.2 Fermer une session *Entrust*

À des fins de sécurité, EESP fermera automatiquement la session lorsque l'un des événements suivants se produira :

- fermeture de la session *Windows*;
- fermeture de *Windows*;
- verrouillage de *Windows*;
- activation de l'écran de veille;
- utilisation d'un raccourci-clavier précédemment créé dans *Entrust*.

Pour fermer la session *Entrust* manuellement, à partir de la zone de notification de *Windows*, à l'aide du bouton droit de la souris, cliquer sur l'icône  , puis sur « Fermer la session ».

Pour éviter l'usurpation de son identité, l'utilisateur doit s'assurer de toujours fermer sa session *Entrust* avant de quitter son poste.

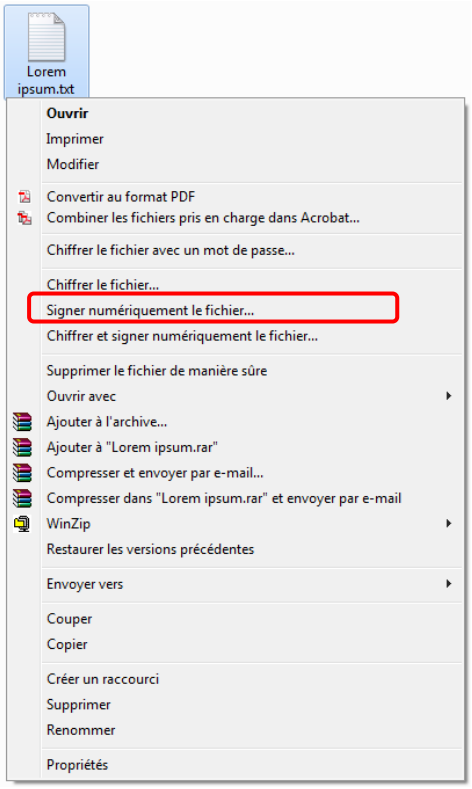
4.3 Signer numériquement un fichier

L'utilisation de cette fonction permet notamment d'authentifier l'auteur d'un document électronique et de garantir l'intégrité du document.

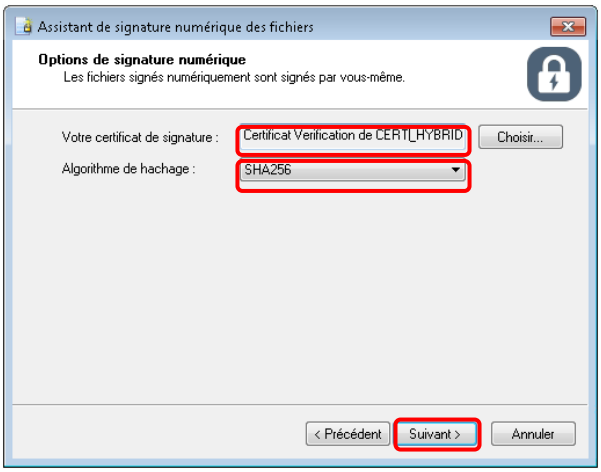
Toute personne possédant des clés et des certificats valides délivrés par le Service de certification du MJQ pourrait ouvrir le document en utilisant ses propres clés et certificats. Il n'est donc pas nécessaire de sélectionner des destinataires lors de l'utilisation de cette fonction.

Pour signer numériquement un fichier :

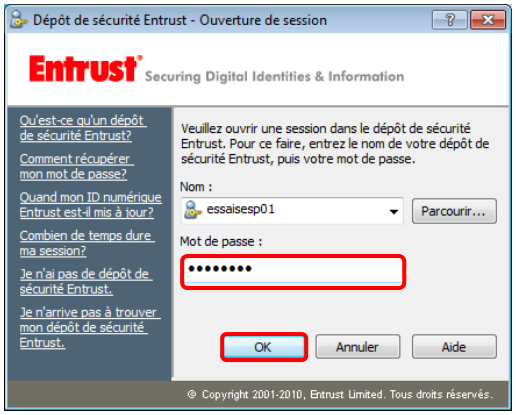
1. À l'aide du bouton droit de la souris, cliquer sur le fichier et sélectionner l'option « Signer numériquement le fichier… ».



2. L'assistant de signature numérique *Entrust* apparaîtra. Cliquer sur le bouton « Suivant > ». Dans la fenêtre suivante, le certificat doit apparaître dans le champ « Votre certificat de signature ». Sinon, cliquer sur le bouton « Choisir… » pour sélectionner le certificat. L'algorithme de hachage « SHA256 » doit être sélectionné. Cliquer sur le bouton « Suivant > ».



3. Si la session *Entrust* est ouverte, passer à l'étape 4. Sinon, la fenêtre d'ouverture de session d'*Entrust* apparaîtra. Saisir le mot de passe et cliquer sur le bouton « OK ».



4. Pour supprimer les fichiers originaux et conserver uniquement les fichiers signés, cocher la case « Supprimer les fichiers d'origine à la fin ». Sinon, une copie en clair (non signée) du fichier sera conservée. Cliquer sur le bouton « Terminer ».

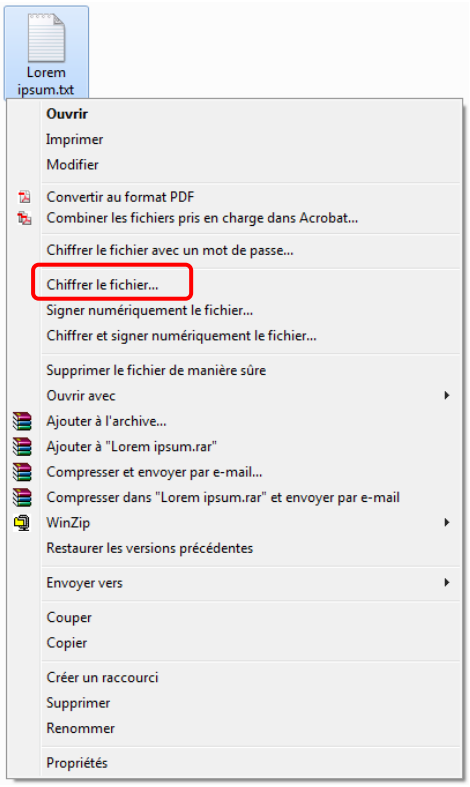
Une fois le fichier signé, il est possible de vérifier la signature en cliquant sur le fichier avec le bouton droit de la souris et en sélectionnant « Propriétés », puis « État de la sécurité ».

4.4 Chiffrer un fichier pour soi-même

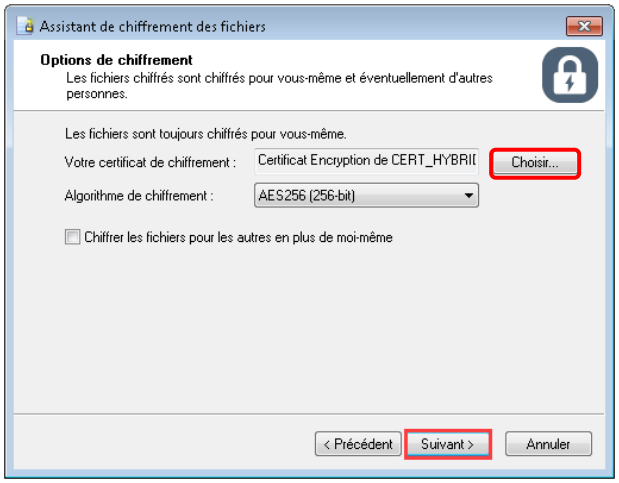
L'utilisateur peut protéger un fichier pour que lui seul puisse y avoir accès.

Pour chiffrer numériquement un fichier :

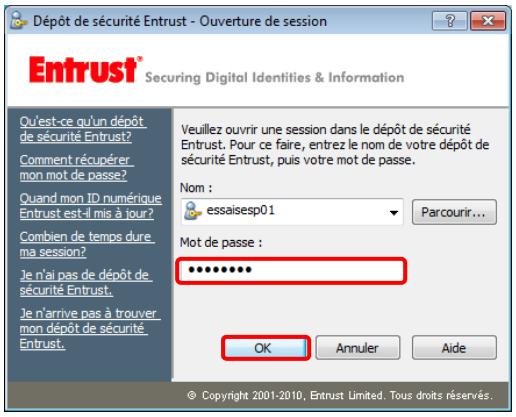
1. À l'aide du bouton droit de la souris, cliquer sur le fichier et sélectionner l'option « Chiffrer le fichier… ».



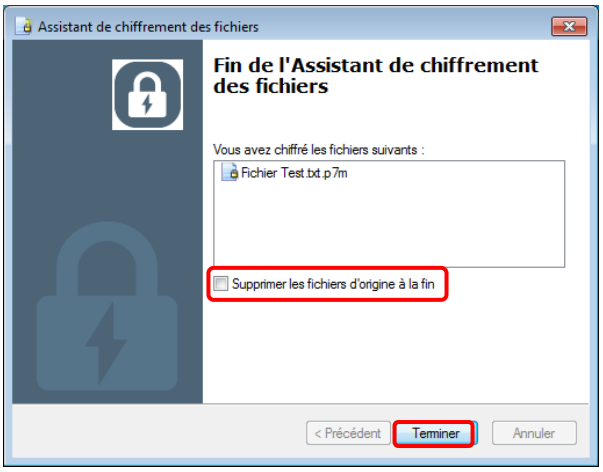
2. L'assistant de signature numérique *Entrust* apparaîtra. Cliquer sur le bouton « Suivant > ». Dans la fenêtre suivante, le certificat doit apparaître dans le champ « Votre certificat de chiffrement ». Sinon, cliquer sur le bouton « Choisir… » pour sélectionner le certificat. L'algorithme de chiffrement doit être « AES 256 (256-bit) ». Cliquer sur le bouton « Suivant > ».



3. Si la session *Entrust* est ouverte, passer à l'étape 4. Sinon, la fenêtre d'ouverture de session d'*Entrust* apparaîtra. Saisir le mot de passe et cliquer sur le bouton « OK ».



4. Pour supprimer les fichiers originaux et conserver uniquement les fichiers chiffrés, cocher la case « Supprimer les fichiers d'origine à la fin ». Sinon, une copie en clair (non chiffrée) du fichier sera conservée. Cliquer sur le bouton « Terminer ».



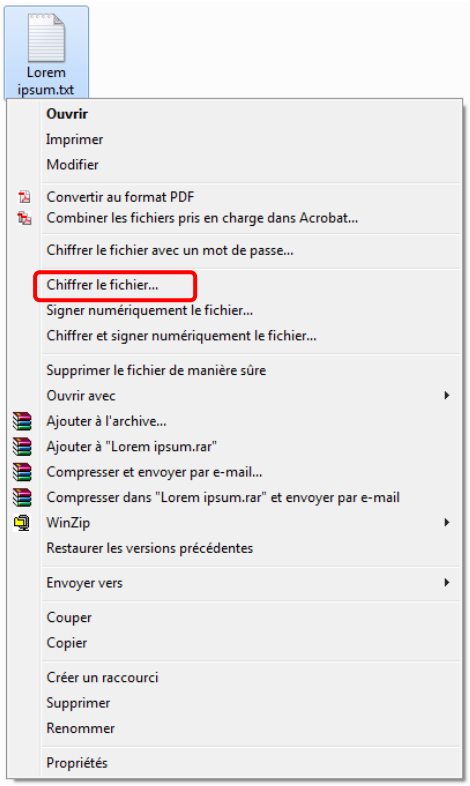
4.5 Chiffrer un fichier pour soi et pour d'autres personnes

L'utilisateur peut chiffrer un fichier pour que lui seul et d'autres personnes désignées possédant des clés et des certificats valides délivrés par le Service de certification du MJQ puissent y avoir accès.

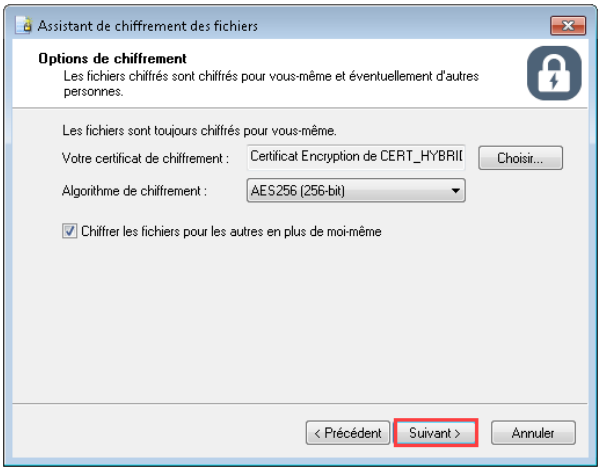
> Il faut être connecté à Internet pour utiliser cette fonction, car *Entrust* doit accéder à la liste des utilisateurs qui possèdent un certificat de chiffrement.

Pour chiffrer numériquement un fichier :

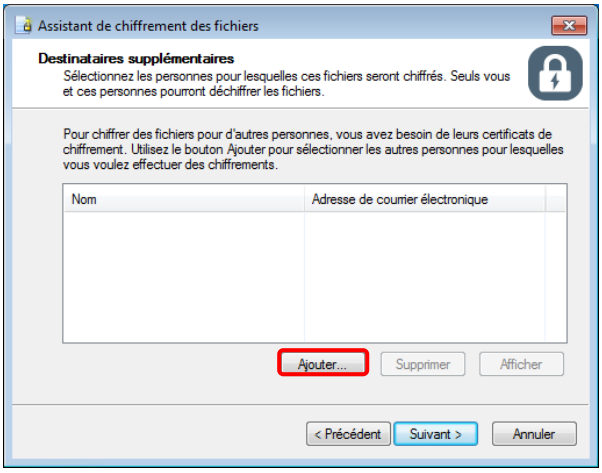
1. À l'aide du bouton droit de la souris, cliquer sur le fichier et sélectionner l'option « Chiffrer le fichier… ».



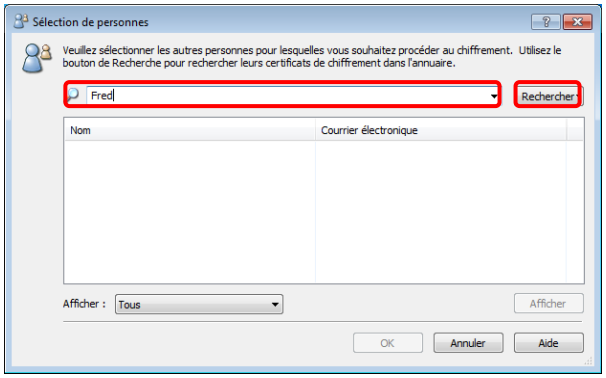
2. L'assistant de chiffrement des fichiers *Entrust* apparaîtra. Cliquer sur le bouton « Suivant > ». Dans la fenêtre suivante, le certificat doit apparaître dans le champ « Votre certificat de chiffrement ». Sinon, cliquer sur le bouton « Choisir… » pour sélectionner le certificat. Cocher la case « Chiffrer les fichiers pour les autres en plus de moi-même ». L'algorithme de chiffrement doit être « AES256 (256-bit) ». Cliquer sur le bouton « Suivant > ».



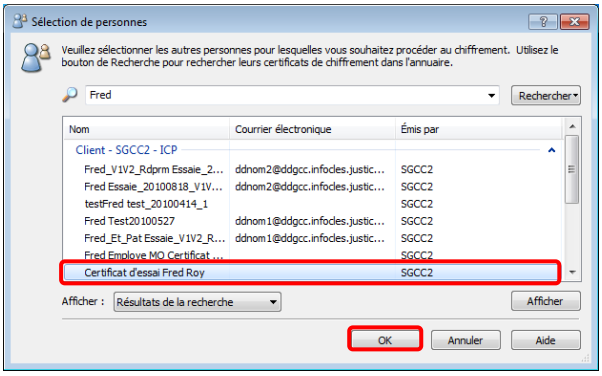
3. Pour sélectionner les personnes pour lesquelles le ou les fichiers seront chiffrés, cliquer sur le bouton « Ajouter… ».



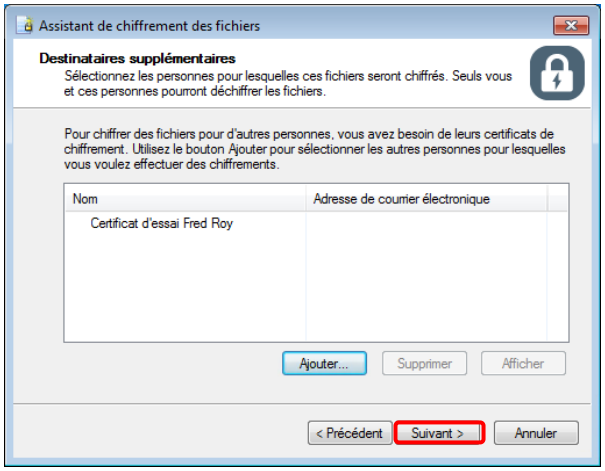
4. Saisir le nom de la personne pour laquelle le document sera chiffré et cliquer sur le bouton « Rechercher ».



5. Sélectionner le nom et cliquer sur le bouton « OK ».



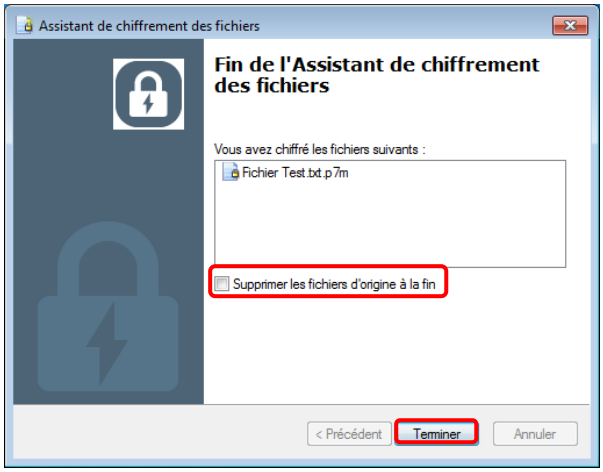
6. Le nom de la personne apparaîtra dans la liste des destinataires. Pour ajouter d'autres destinataires, cliquer sur le bouton « Ajouter… » et répéter les étapes 4 et 5. Une fois tous les destinataires ajoutés, cliquer sur le bouton « Suivant > ».



Si les noms affichés ne permettent pas d'identifier un destinataire, il est possible, en cliquant sur le bouton « Afficher », de consulter les certificats pour obtenir des renseignements additionnels (voir section 4.8).

Il est possible de créer une liste rapide de destinataires. Cela permet d'accélérer le processus de sélection des destinataires pour lesquels des fichiers sont régulièrement sécurisés (voir section 5.6).

7. Pour supprimer les fichiers originaux et conserver uniquement les fichiers chiffrés, cocher la case « Supprimer les fichiers d'origine à la fin ». Sinon, une copie en clair (non chiffrée) du fichier sera conservée. Cliquer sur le bouton « Terminer ».



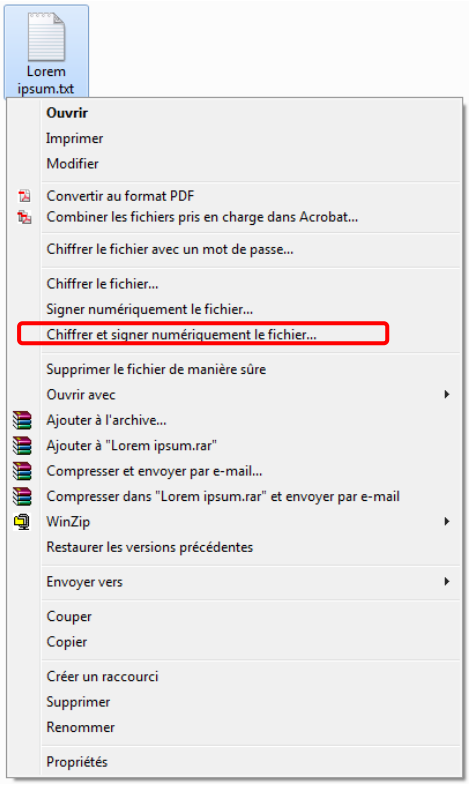
Un nouveau fichier apparaîtra et portera le même nom que le fichier original, mais avec une extension différente. Le fichier est maintenant sécurisé pour les destinataires choisis ainsi que pour soi-même.

4.6 Chiffrer et signer numériquement un fichier pour soi-même et pour d'autres personnes

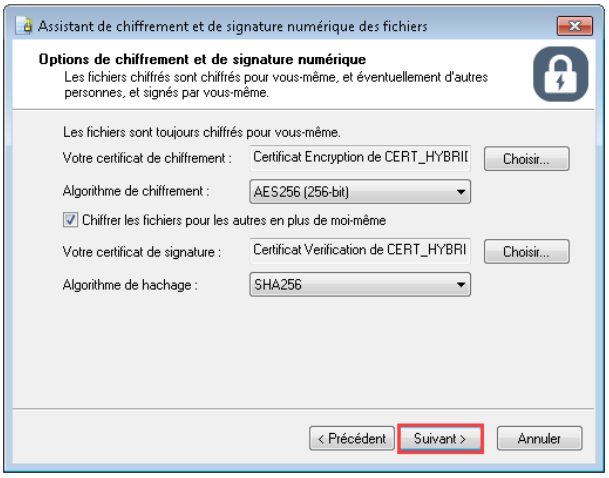
L'utilisateur peut chiffrer et signer numériquement un fichier pour lui-même et pour d'autres personnes désignées possédant des clés et des certificats valides délivrés par le Service de certification du MJQ.

Pour chiffrer et signer numériquement un fichier pour soi et pour d'autres personnes :

1. À l'aide du bouton droit de la souris, cliquer sur le fichier et sélectionner l'option « Chiffrer et signer numériquement le fichier… ».

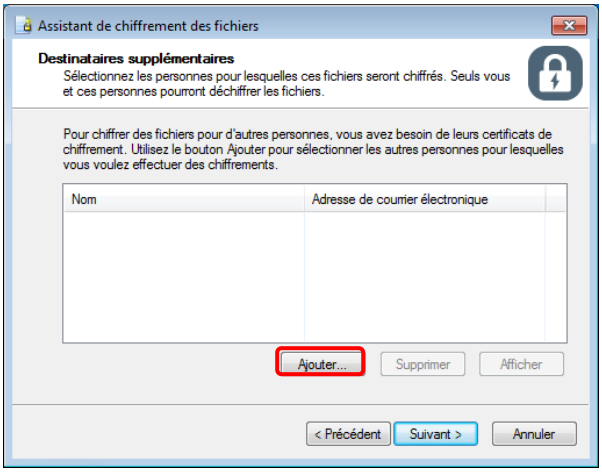


2. L'assistant de chiffrement et de signature numérique des fichiers apparaîtra. Cliquer sur le bouton « Suivant > ». Dans la fenêtre suivante, le certificat doit apparaître dans le champ « Votre certificat de chiffrement ». Sinon, cliquer sur le bouton « Choisir… » pour sélectionner le certificat. Cocher la case « Chiffrer les fichiers pour les autres en plus de moi-même ». L'algorithme de chiffrement doit être « AES256 (256-bit) » et l'algorithme de hachage doit être « SHA256 ». Cliquer sur le bouton « Suivant > ».

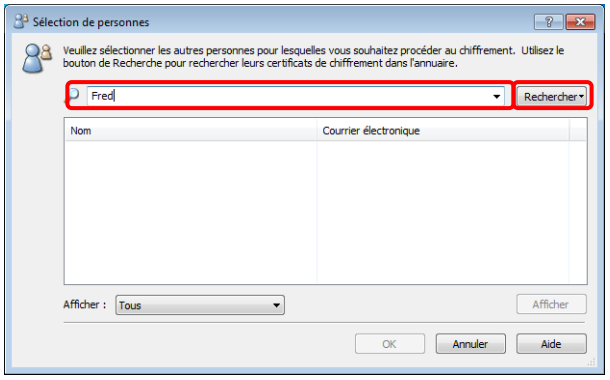


Si la case « Chiffrer les fichiers pour les autres en plus de moi-même » n'est pas cochée, le fichier sera signé et chiffré pour l'utilisateur seulement.

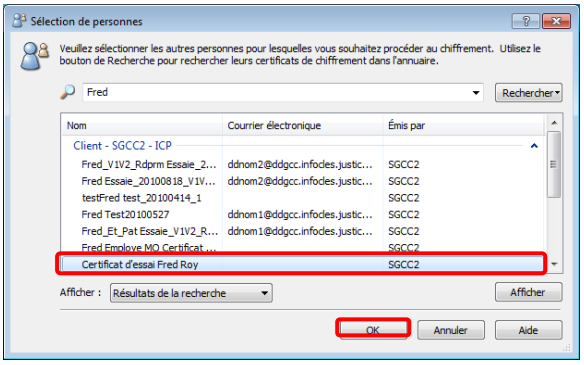
3. Pour sélectionner les personnes pour lesquelles le ou les fichiers seront chiffrés, cliquer sur le bouton « Ajouter… ».



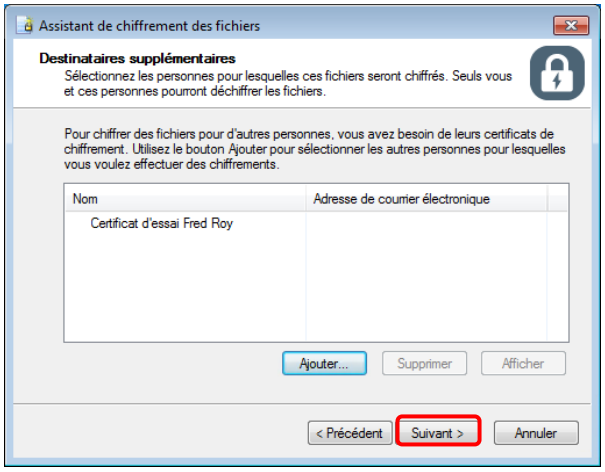
4. Saisir le nom de la personne pour laquelle le document sera chiffré et cliquer sur le bouton « Rechercher ».



5. Sélectionner le nom et cliquer sur le bouton « OK ».



6. Le nom de la personne apparaîtra dans la liste des destinataires. Pour ajouter d'autres destinataires, cliquer sur le bouton « Ajouter… » et répéter les étapes 4 et 5. Une fois tous les destinataires ajoutés, cliquer sur le bouton « Suivant > ».

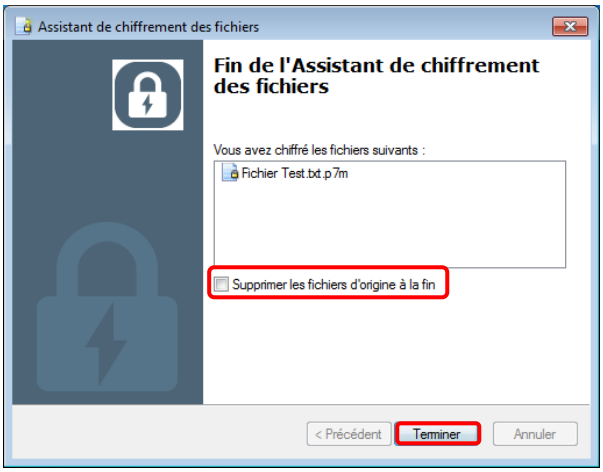


Si les noms affichés ne permettent pas d'identifier un destinataire, il est possible, en cliquant sur le bouton « Afficher », de consulter les certificats pour obtenir des renseignements additionnels (voir section 4.8).

Il est possible de créer une liste rapide de destinataires. Cela permet d'accélérer le processus de sélection des destinataires pour lesquelles des fichiers sont régulièrement sécurisés (voir section 5.6).

Si la session *Entrust* est fermée, la fenêtre d'ouverture d'*Entrust* apparaîtra. Saisir le mot de passe et cliquer sur le bouton « OK ». Cette étape est nécessaire pour mettre fin à l'assistant de chiffrement et de signature numérique des fichiers.

7. Pour supprimer les fichiers originaux et conserver uniquement les fichiers chiffrés et signés, cocher la case « Supprimer les fichiers d'origine à la fin ». Sinon, une copie en clair (non chiffrée et non signée) du fichier sera conservée. Cliquer sur le bouton « Terminer ».



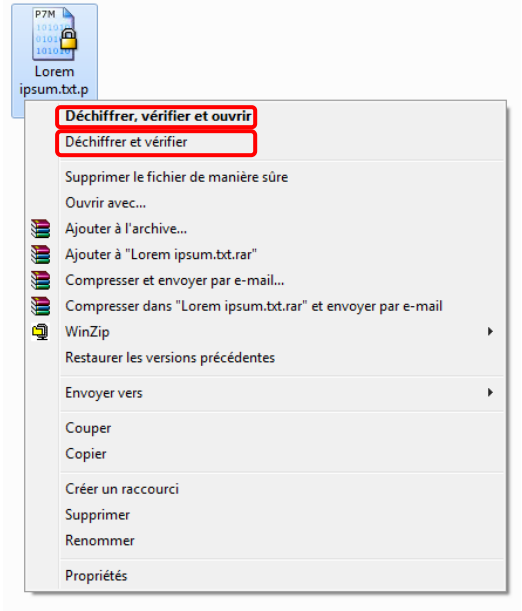
Un nouveau fichier apparaîtra et portera le même nom que le fichier original, mais avec une extension différente. Le fichier est maintenant sécurisé pour les destinataires choisis ainsi que pour soi-même.

S'assurer d'avoir inséré tous les destinataires dans la liste pendant la sécurisation du fichier. Sinon, la personne qui recevra le fichier obtiendra un message d'erreur d'*Entrust* lui indiquant qu'il est impossible de décoder le fichier (voir section 6).

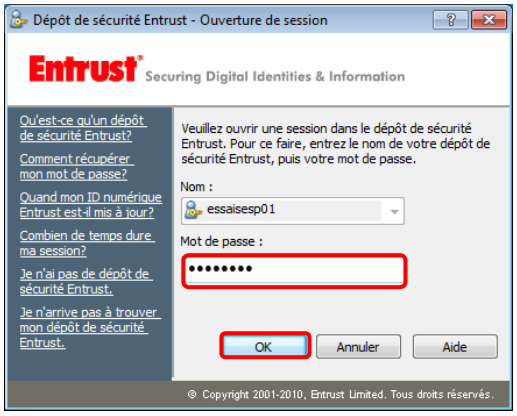
4.7 Déchiffrer, vérifier et ouvrir un fichier chiffré

Cette fonction permet de déchiffrer un fichier préalablement chiffré à l'aide des clés et des certificats.

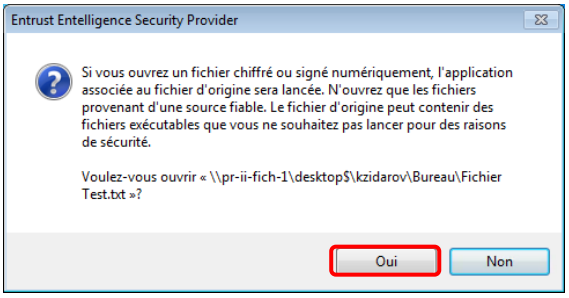
1. Pour ouvrir automatiquement le fichier une fois déchiffré, à l'aide du bouton droit de la souris, cliquer sur le fichier et sélectionner l'option « Déchiffrer, vérifier et ouvrir ». Pour déchiffrer le fichier sans l'ouvrir, cliquer sur l'option « Déchiffrer et vérifier ».



2. La fenêtre d'ouverture de session apparaîtra. Saisir le mot de passe et cliquer sur le bouton « OK ».



3. Si l'option « Déchiffrer, vérifier et ouvrir » est sélectionnée, le message suivant apparaîtra. Cliquer sur le bouton « Oui » pour que le fichier s'ouvre dans son format original.



Si l'option « Déchiffrer et vérifier » est sélectionnée, *Entrust* déchiffrera le document et vérifiera si le destinataire fait partie de la liste des destinataires, sans toutefois ouvrir le document dans son format d'origine.

En double-cliquant directement sur le fichier chiffré, on obtient le même résultat que lorsque l'on sélectionne l'option « Déchiffrer, vérifier et ouvrir ».

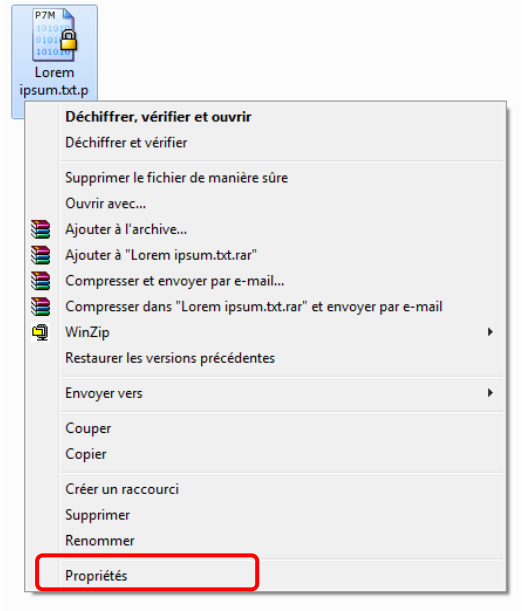
Si un message indique qu'il est impossible de décoder le fichier, voir la section 6.

4.8 Vérifier l'identité du signataire

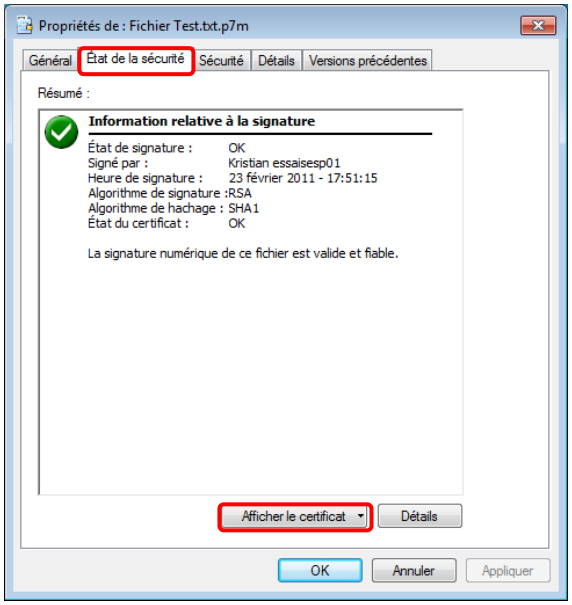
Cette fonction permet de vérifier et de confirmer l'identité du signataire d'un fichier signé.

Pour vérifier l'identité du signataire :

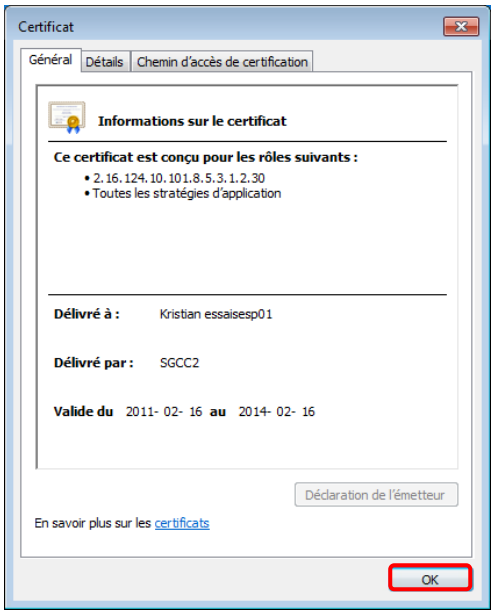
1. À l'aide du bouton droit de la souris, cliquer sur le fichier et sélectionner l'option « Propriétés ».



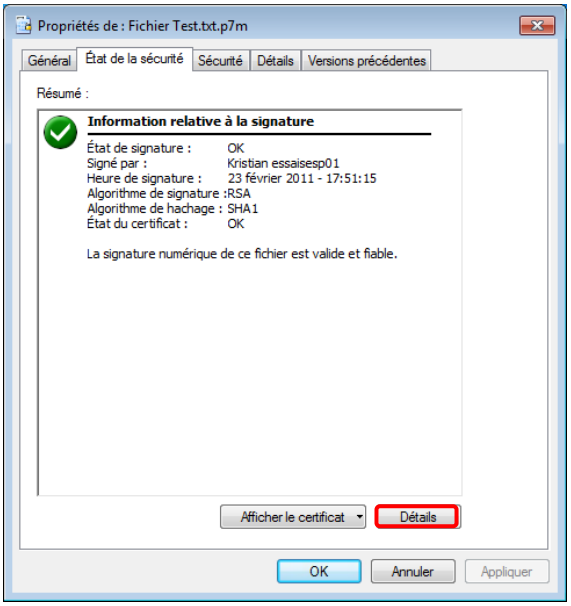
2. Cliquer sur le second onglet intitulé « État de la sécurité » pour voir l'information relative à la signature, puis sur le bouton « Afficher le certificat » pour avoir des renseignements additionnels sur le certificat (autorité de certification ayant délivré le certificat, nom de la personne à qui le certificat a été délivré, etc.).



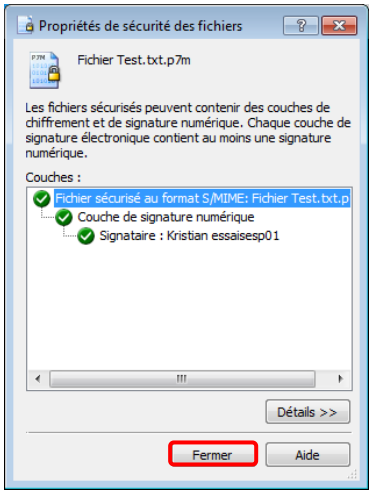
3. Cliquer sur le bouton « OK » pour revenir à l'écran précédent.



4. Cliquer sur le bouton « Détails » pour visualiser les propriétés de sécurité du fichier signé.



5. Le détail des couches de chiffrement et de la signature numérique apparaîtra. Cliquer sur le bouton « Fermer », puis sur le bouton « OK ».

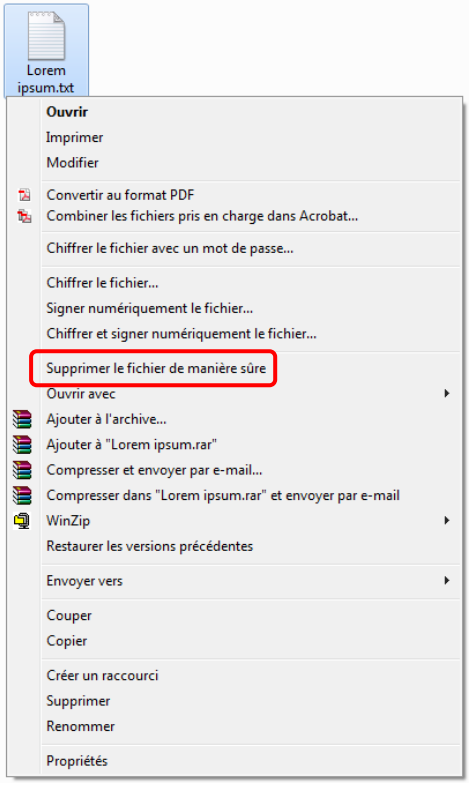


4.9 Supprimer un fichier de manière sûre

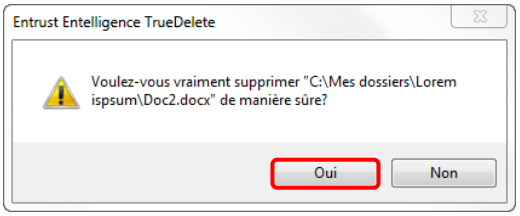
Cette fonction permet de supprimer un fichier de manière sûre pour rendre le fichier irrécupérable après sa suppression.

Pour supprimer un fichier de manière sûre :

1. À l'aide du bouton droit de la souris, cliquer sur le fichier et sélectionner l'option « Supprimer le fichier de manière sûre ».



Le message suivant apparaîtra. Cliquer sur le bouton « Oui » pour supprimer le fichier de manière sûre.



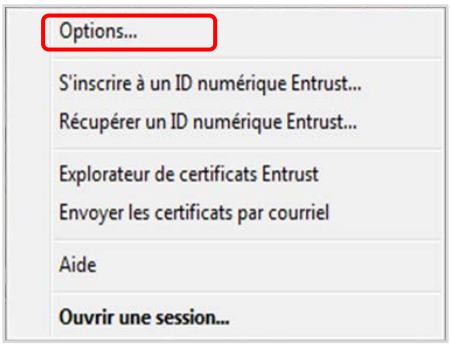
Les fichiers supprimés de manière sûre sont irrécupérables puisqu'ils sont chiffrés par *Entrust* durant le processus de suppression.

5. Utilisation avancée d'EESP

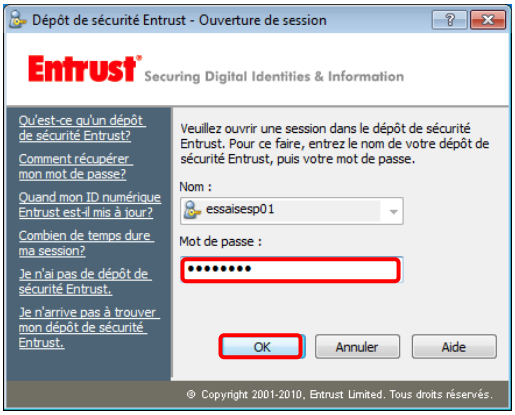
5.1 Modifier le mot de passe

Pour modifier le mot de passe lié aux clés et aux certificats :

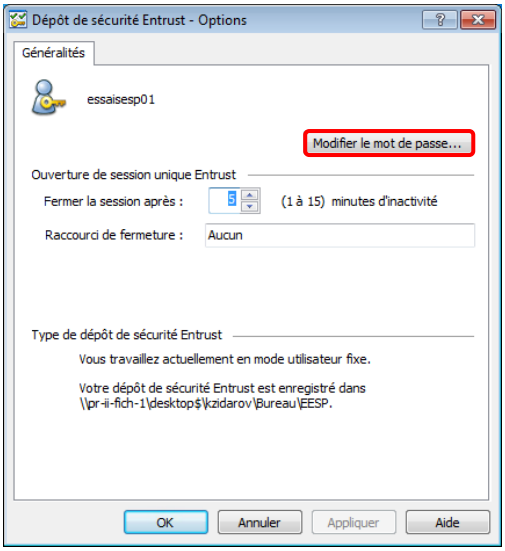
1. À l'aide du bouton droit de la souris, cliquer sur l'icône dans la zone de notification de *Windows* et sélectionner « Options… ».



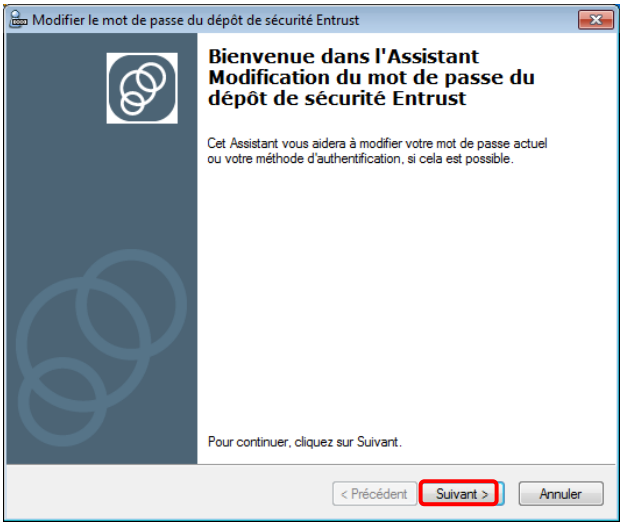
2. Si la session *Entrust* est ouverte, passer à l'étape 3. Si la session *Entrust* est fermée, la fenêtre d'ouverture de session apparaîtra. Saisir le mot de passe et cliquer sur le bouton « OK ».



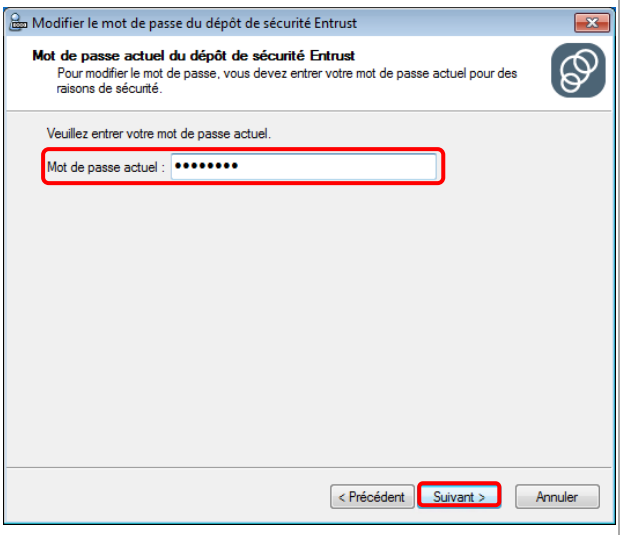
3. Cliquer sur le bouton « Modifier le mot de passe… ».



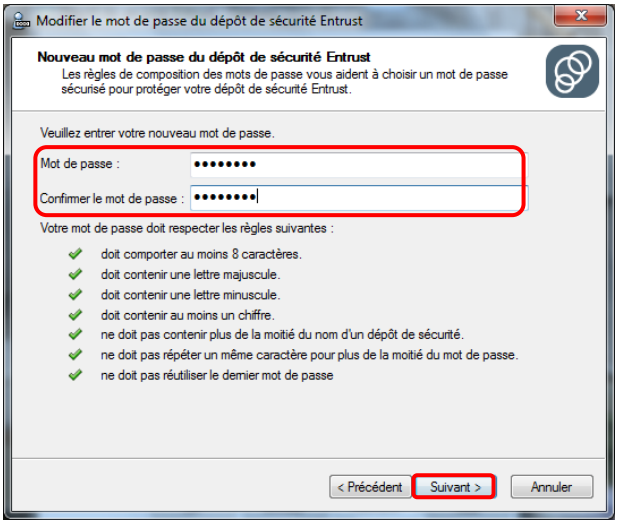
4. L'assistant de modification du mot de passe du dépôt de sécurité *Entrust* apparaîtra. Cliquer sur le bouton « Suivant > ».



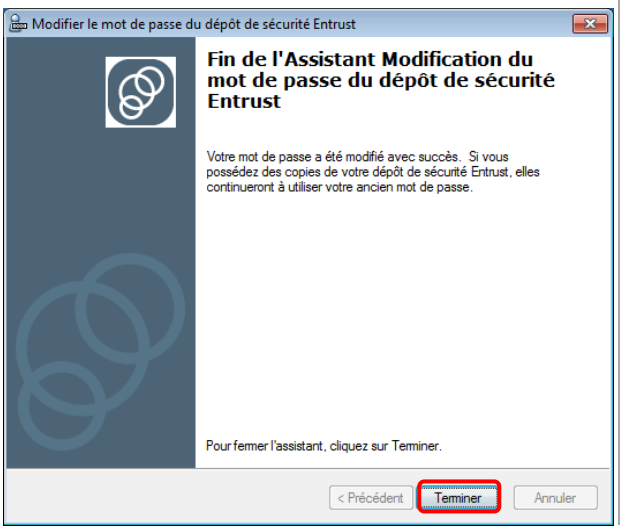
5. Saisir le mot de passe actuel dans le champ « Mot de passe actuel » et cliquer sur le bouton « Suivant > ».



6. Saisir le nouveau mot de passe dans les zones de saisie en s'assurant de respecter les règles énoncées. Cliquer sur le bouton « Suivant > ».



7. Cliquer sur le bouton « Terminer ».



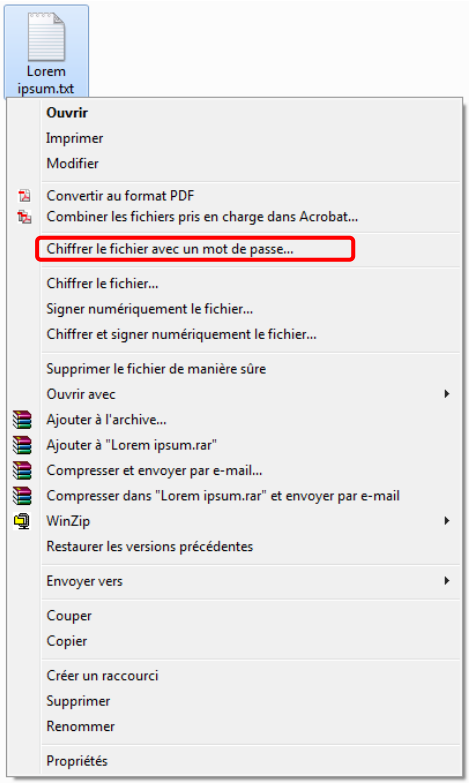
5.2 Chiffrer un fichier avec un mot de passe

L'utilisateur peut chiffrer un seul fichier à la fois avec un mot de passe différent de celui lié aux clés et aux certificats. Cette fonction ne requiert pas l'utilisation des clés et des certificats, sauf si l'option « En plus du mot de passe, chiffrer les fichiers de mon certificat de chiffrement » est sélectionnée. L'utilisation de cette fonction permet de protéger un document pour soi-même ou pour quelqu'un d'autre (dans ce cas, il faudra divulguer au destinataire le mot de passe lié au fichier chiffré).

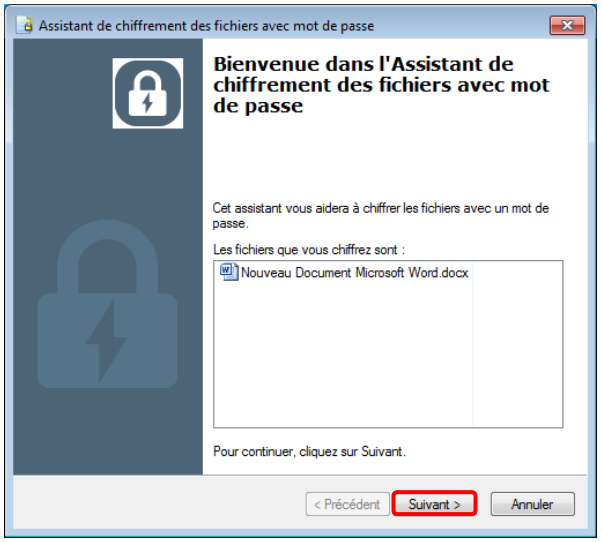
Les fichiers chiffrés par mot de passe portent une extension « *.pp7m ».

Pour chiffrer un fichier par mot de passe :

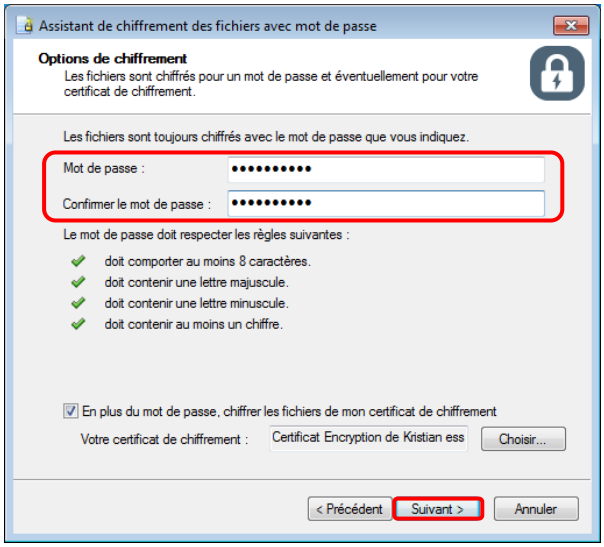
1. À l'aide du bouton droit de la souris, cliquer sur le fichier et sélectionner l'option « Chiffrer le fichier avec un mot de passe… ».



2. L'assistant de chiffrement des fichiers avec mot de passe apparaîtra. Cliquer sur le bouton « Suivant > ».



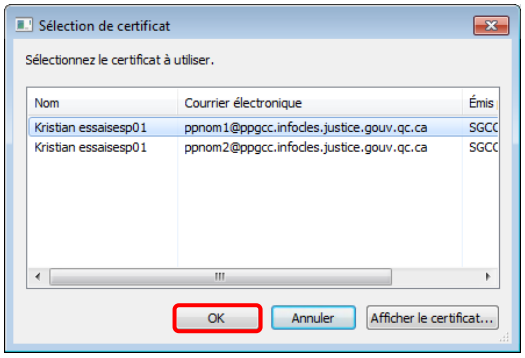
3. Saisir le nouveau mot de passe dans les zones de saisie en s'assurant de respecter les règles énoncées. Cliquer sur le bouton « Suivant > ».



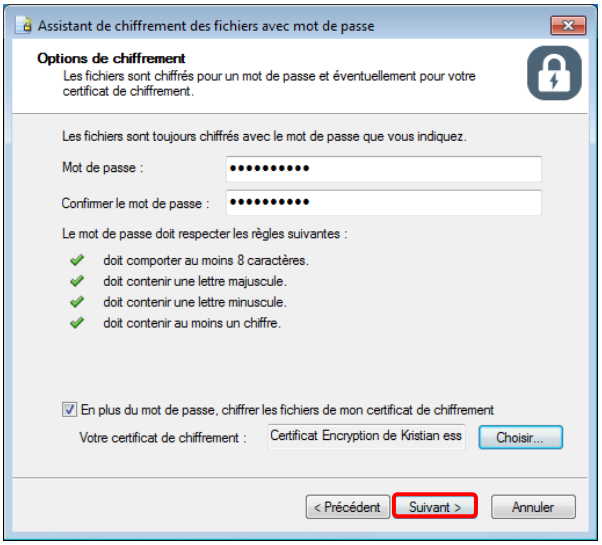
La case « En plus du mot de passe, chiffrer les fichiers de mon certificat de chiffrement » est cochée par défaut. Cette option est utile si un document est chiffré pour quelqu'un, mais que le mot de passe a été oublié. Si la case est cochée, le fichier pourra être déchiffré avec le mot de passe du certificat en ouvrant une session *Entrust*.

Si la case n'est pas cochée et que le mot de passe est oublié, il sera impossible de récupérer le contenu du fichier chiffré.

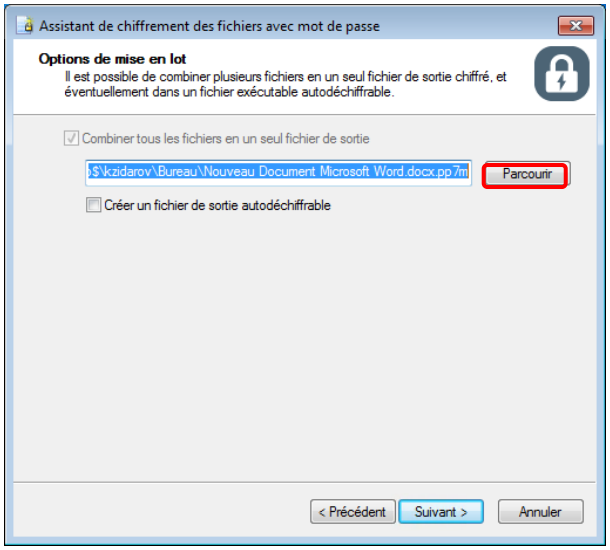
4. Si la case « En plus du mot de passe, chiffrer les fichiers de mon certificat de chiffrement » n'est pas cochée, passer à l'étape 5. Sinon, cliquer sur le bouton « Choisir… » pour s'assurer que le bon certificat a été choisi. Sélectionner le certificat et cliquer sur le bouton « OK ».



5. Saisir le nouveau mot de passe dans les zones de saisie en s'assurant de respecter les règles énoncées. Cliquer sur le bouton « Suivant > ».

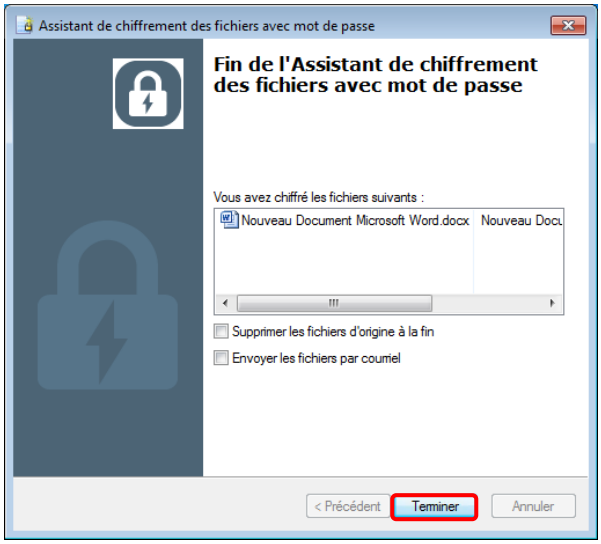


6. Sélectionner l'emplacement de sauvegarde du fichier en cliquant sur le bouton « Parcourir ». Par défaut, l'emplacement est celui du fichier en cours de chiffrement.



La fonction « Créer un fichier de sortie autodéchiffrable » permet de créer un fichier chiffré exécutable. L'avantage d'un tel format de fichier est qu'il peut être partagé avec des personnes qui ne disposent pas d'un logiciel de déchiffrement ou de certificats sur leur ordinateur. Si ces personnes connaissent le mot de passe du fichier, elles pourront déchiffrer le fichier sans l'aide d'un logiciel. Le principal inconvénient est que ce format de fichier (*.exe) peut être bloqué par des logiciels antivirus.

7. Cliquer sur le bouton « Terminer ».



Si la case « Supprimer les fichiers d'origine à la fin » n'est pas cochée, les fichiers originaux ayant servi au chiffrement seront conservés en clair (non chiffrés).

Si la case « Envoyez les fichiers par courriel » est cochée, le programme de courriel démarrera à la fin de l'assistant de chiffrement.

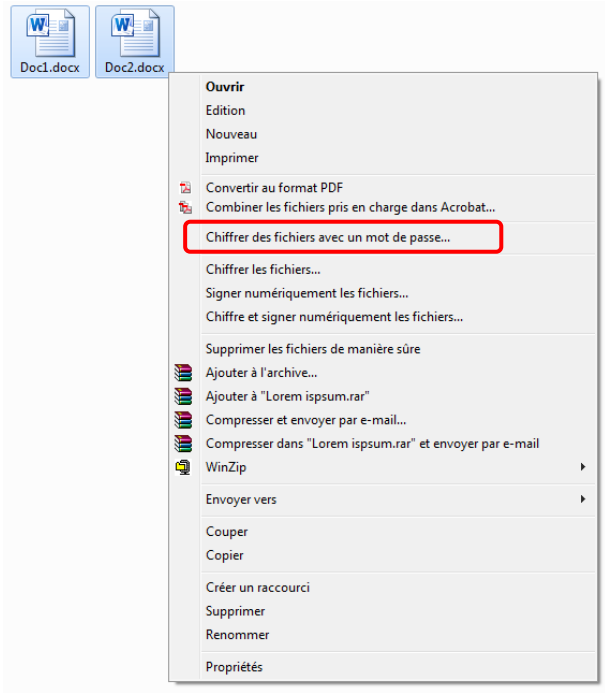
5.3 Chiffrer plusieurs fichiers avec un mot de passe

L'utilisateur peut chiffrer plusieurs fichiers à la fois avec un mot de passe différent de celui lié aux clés et aux certificats. Cette fonction ne requiert pas l'utilisation des clés et des certificats, sauf si l'option « En plus du mot de passe, chiffrer les fichiers de mon certificat de chiffrement » est sélectionnée. L'utilisation de cette fonction permet de protéger des fichiers pour soi-même ou pour quelqu'un d'autre (dans ce cas, il faudra divulguer au destinataire le mot de passe lié aux fichiers chiffrés).

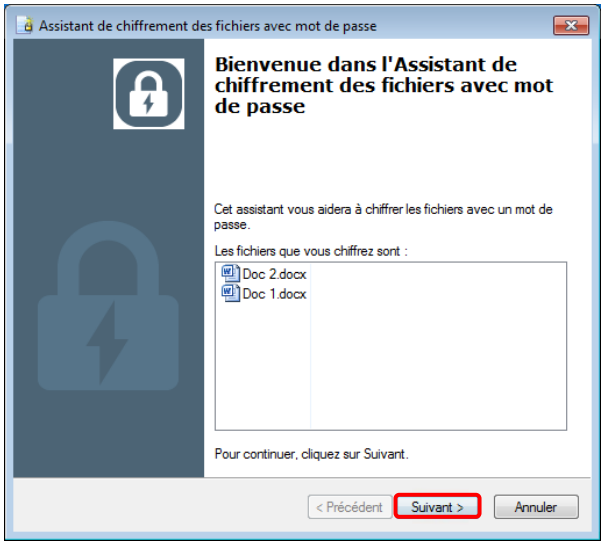
Les fichiers chiffrés par mot de passe portent une extension « *.pp7m ».

Pour chiffrer plusieurs fichiers par mot de passe :

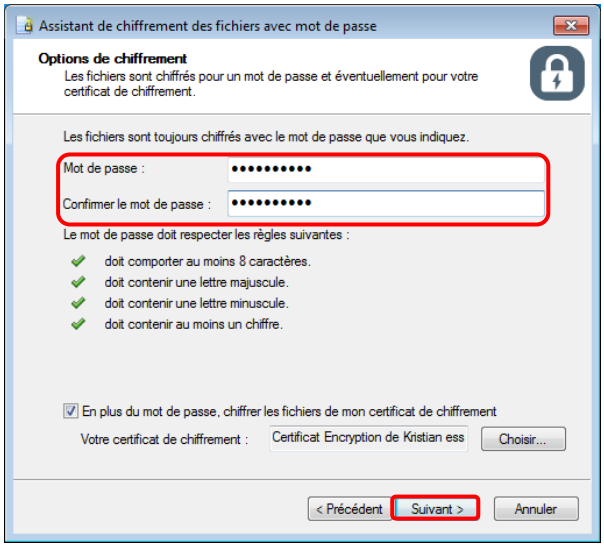
1. À l'aide du bouton droit de la souris, cliquer sur l'un des fichiers et sélectionner l'option « Chiffrer des fichiers avec un mot de passe… ».



2. L'assistant de chiffrement des fichiers avec mot de passe apparaîtra. Cliquer sur le bouton « Suivant > ».



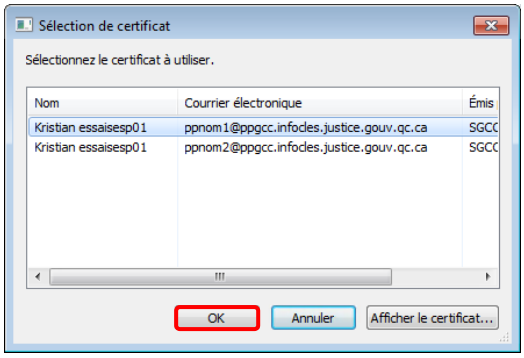
3. Saisir le nouveau mot de passe dans les zones de saisie en s'assurant de respecter les règles énoncées. Cliquer sur le bouton « Suivant > ».



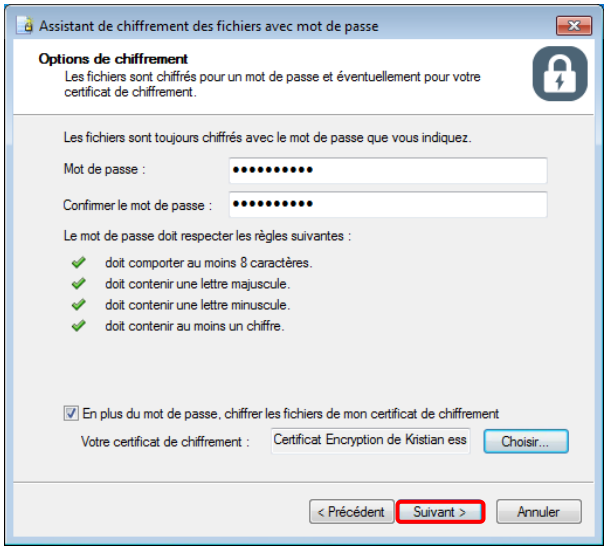
La case « En plus du mot de passe, chiffrer les fichiers de mon certificat de chiffrement » est cochée par défaut. Cette option est utile si un document est chiffré pour quelqu'un, mais que le mot de passe a été oublié. Si la case est cochée, le fichier pourra être déchiffré avec le mot de passe du certificat en ouvrant une session *Entrust*.

Si la case n'est pas cochée et que le mot de passe est oublié, il sera impossible de récupérer le contenu du fichier chiffré.

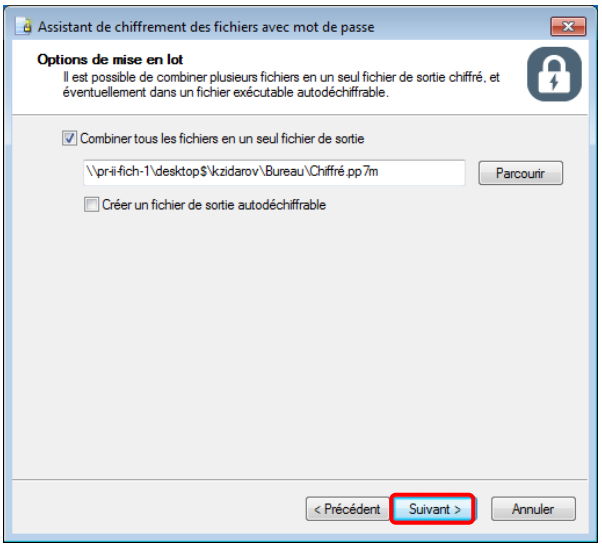
4. Si la case « En plus du mot de passe, chiffrer les fichiers de mon certificat de chiffrement » n'est pas cochée, passer à l'étape 7. Sinon, cliquer sur le bouton « Choisir… » pour s'assurer que le bon certificat a été choisi. Sélectionner le certificat et cliquer sur le bouton « OK ».



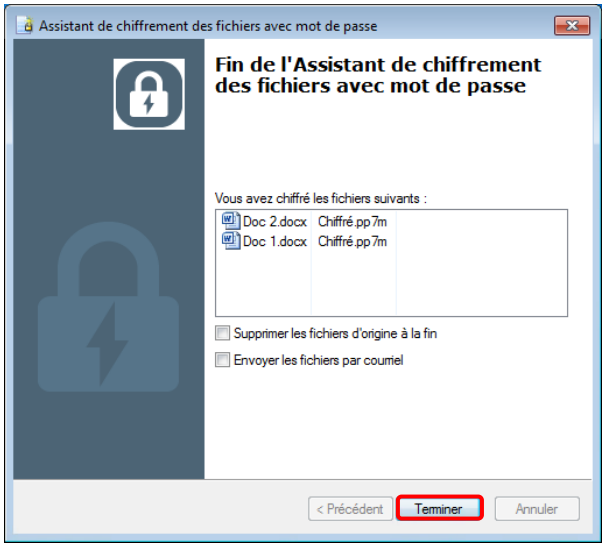
5. Cliquer sur le bouton « Suivant > ».



6. Sélectionner l'emplacement de sauvegarde du fichier en cliquant sur le bouton « Parcourir ». Par défaut, l'emplacement est celui des fichiers sources en cours de chiffrement. Si la case « Combiner tous les fichiers en un seul fichier de sortie » est cochée, tous les fichiers seront regroupés dans un seul fichier. Cliquer sur le bouton « Suivant > ».



7. Cliquer sur le bouton « Terminer ».



La fonction « Créer un fichier de sortie autodéchiffrable » permet de créer un fichier chiffré exécutable. L'avantage d'un tel format de fichier est qu'il peut être partagé avec des personnes qui ne disposent pas d'un logiciel de déchiffrement ou de certificats sur leur ordinateur tel que *Entrust Security Provider*. Si ces personnes connaissent le mot de passe du fichier, elles pourront déchiffrer le fichier sans l'aide d'*Entrust Security Provider*. Le principal inconvénient est que le format de ce fichier (*.exe) peut être bloqué par des logiciels antivirus.

Si la case « Supprimer les fichiers d'origine à la fin » n'est pas cochée, les fichiers originaux ayant servi au chiffrement seront conservés en clair (non chiffrés).

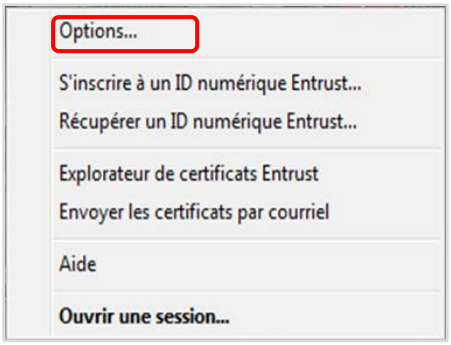
Si la case « Envoyez les fichiers par courriel » est cochée, le programme de courriel démarrera à la fin de l'assistant de chiffrement des fichiers avec mot de passe.

5.4 Créer un raccourci-clavier pour fermer une session active

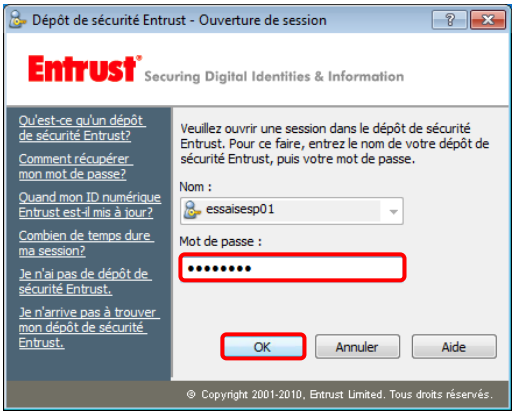
Cette fonction permet de créer un raccourci-clavier pour fermer une session *Entrust* active.

Pour fermer une session active :

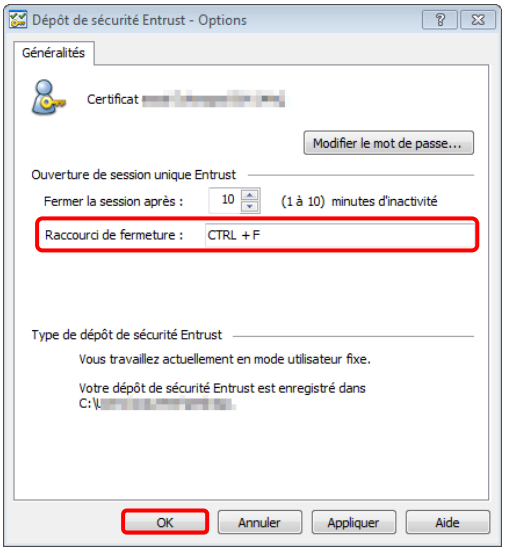
1. À l'aide du bouton droit de la souris, cliquer sur l'icône dans la zone de notification de *Windows* et sélectionner « Options… ».



2. Si la session *Entrust* est ouverte, passer à l'étape 3. Si la session *Entrust* est fermée, la fenêtre d'ouverture de session apparaîtra. Saisir le mot de passe et cliquer sur le bouton « OK ».



3. Cliquer dans la zone de saisie de la section « Raccourci de fermeture » et entrer au clavier le raccourci choisi. Par exemple, pour utiliser « CTRL+F » maintenir enfoncé la touche « CTRL » du clavier tout en appuyant sur la lettre « F ». Cliquer sur le bouton « OK ».

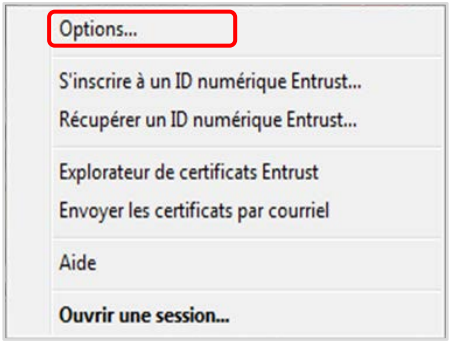


5.5 Changer le temps d'inactivité pour une fermeture de session automatique

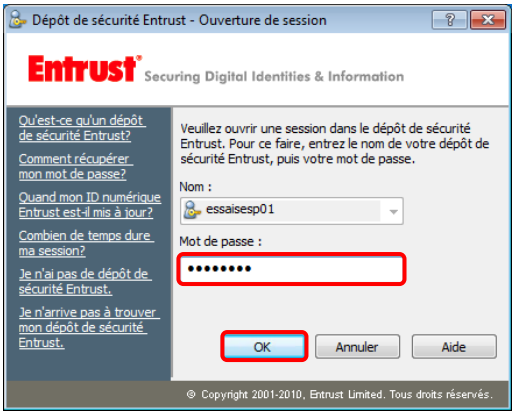
Cette fonction permet de changer le temps d'inactivité avant qu'*Entrust* ferme automatiquement la session. Le temps d'inactivité par défaut est de 10 minutes.

Pour changer le délai d'inactivité :

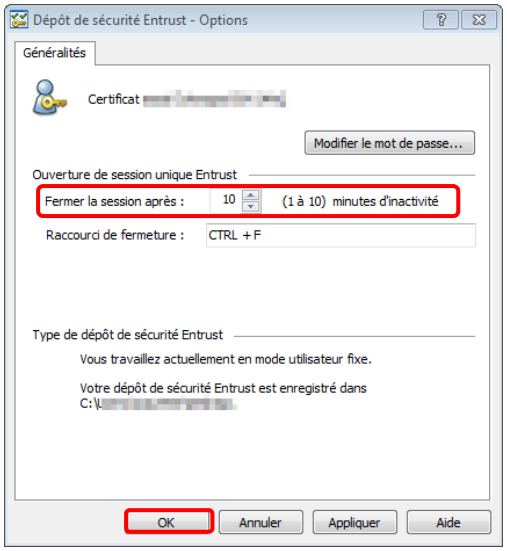
1. À l'aide du bouton droit de la souris, cliquer sur l'icône dans la zone de notification de *Windows* et sélectionner « Options… ».



2. Si la session *Entrust* est ouverte, passer à l'étape 3. Si la session *Entrust* est fermée, la fenêtre d'ouverture de session apparaîtra. Saisir le mot de passe et cliquer sur le bouton « OK ».



3. Cliquer dans la zone de saisie de la section « Fermer la session après » et sélectionner un chiffre de 1 à 10. Cliquer sur le bouton « OK ».

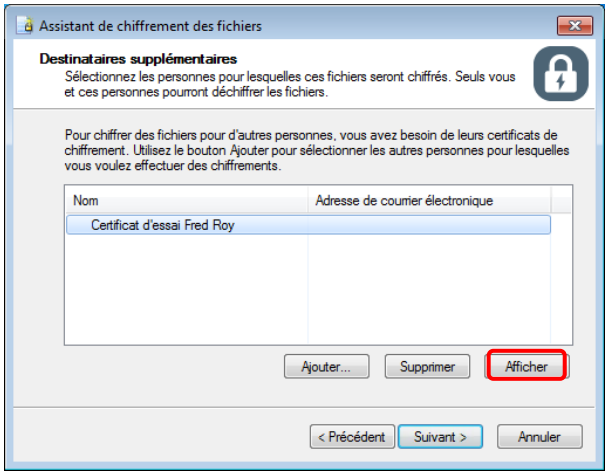


5.6 Créer une liste rapide de destinataires

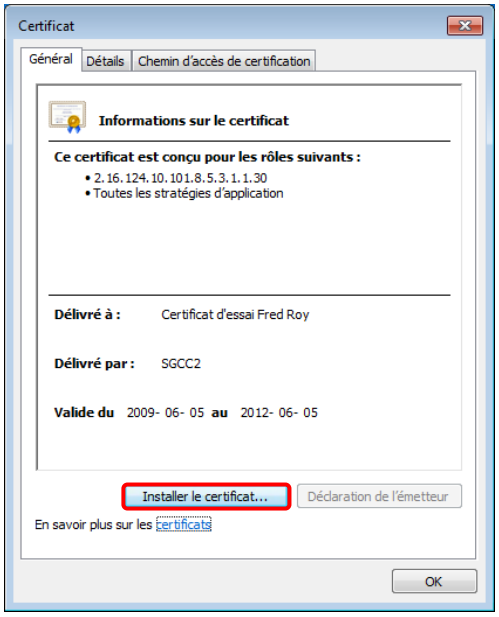
Cette fonction permet de créer une liste rapide de destinataires pour lesquels des fichiers sont régulièrement chiffrés. Cela évite d'effectuer des recherches dans le répertoire de certificats et accélère l'ajout de destinataires.

Pour créer une liste rapide de destinataires :

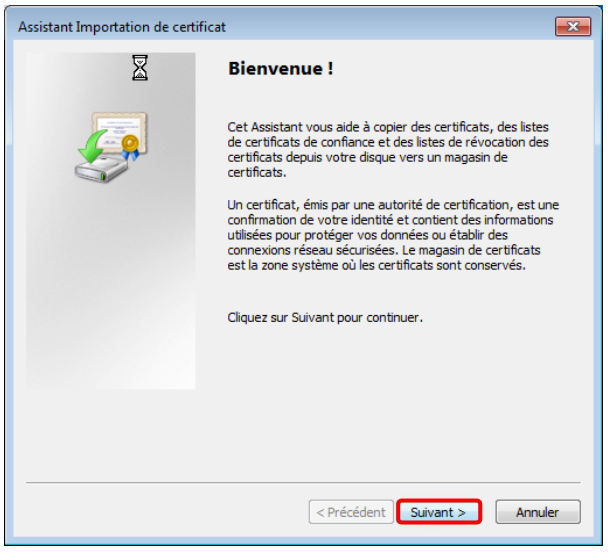
1. Suivre les étapes 1 à 6 des sections 4.5 « Chiffrer un fichier pour soi et pour d'autres personnes » ou 4.6 « Chiffrer et signer numériquement un fichier pour soi-même et pour d'autres personnes » SANS CLIQUER SUR LE BOUTON « Suivant > » à l'étape 6. Avant d'ajouter d'autres destinataires à la liste, cliquer sur le bouton « Afficher ».



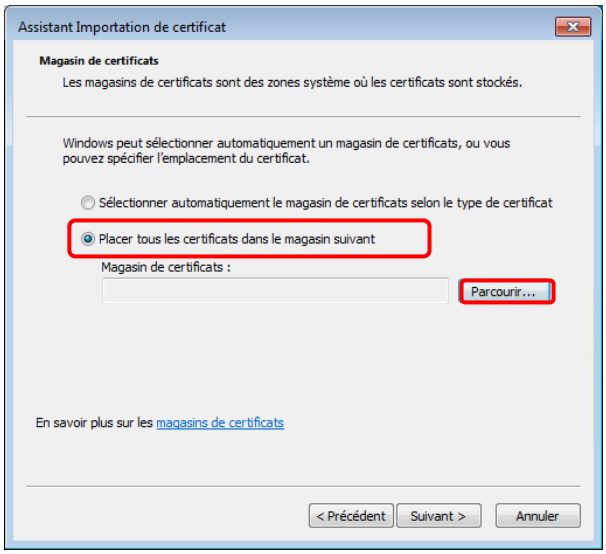
2. Cliquer sur le bouton « Installer le certificat… ».



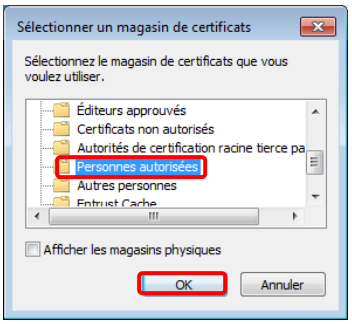
3. L'assistant d'importation de certificat apparaîtra. Cliquer sur le bouton « Suivant > ».



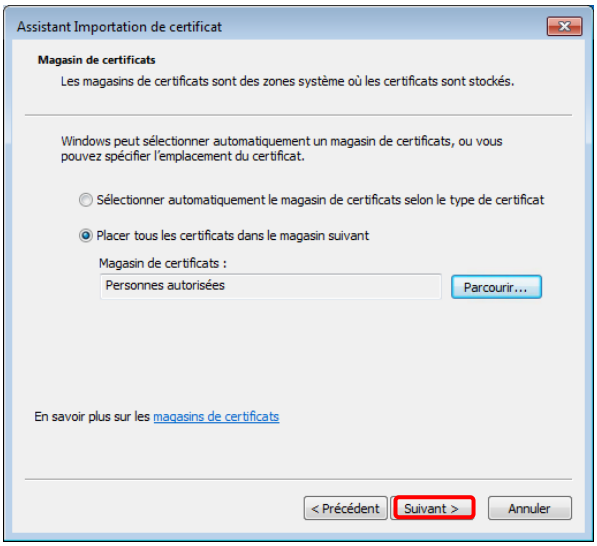
4. Sélectionner la case d'option « Placer tous les certificats dans le magasin suivant » et cliquer sur le bouton « Parcourir… ».



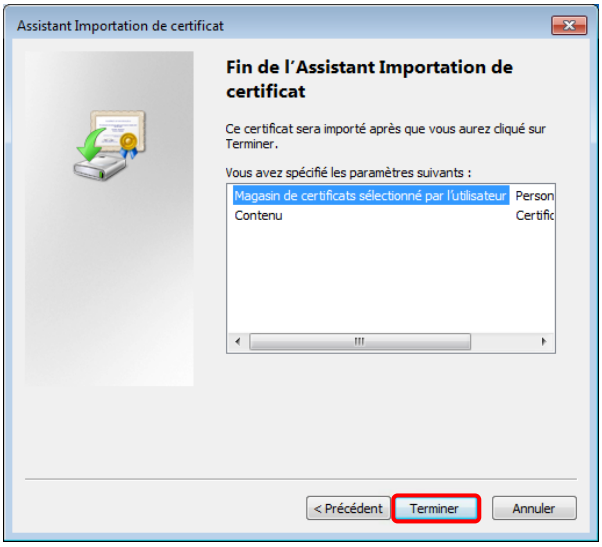
5. Dans la liste de magasins de certificats, sélectionner « Personnes autorisées » et cliquer sur le bouton « OK ».



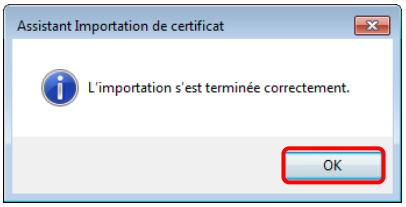
6. Le magasin de certificats apparaîtra dans le champ « Magasin de certificats ». Cliquer sur le bouton « Suivant > ».



7. Cliquer sur le bouton « Terminer ».



8. Une fois l'importation terminée, un message avisera que l'importation s'est terminée correctement. Cliquer sur bouton « OK ».



9. Répéter les étapes précédentes pour ajouter des destinataires supplémentaires.

La liste créée sera disponible lors de la prochaine sécurisation de fichiers destinés à d'autres personnes.

Lorsque le chiffrement de fichiers est souvent requis pour un même groupe de destinataires, il peut être utile de créer un groupe personnel de chiffrement (voir section 5.7).

5.7 Créer un groupe personnel de chiffrement

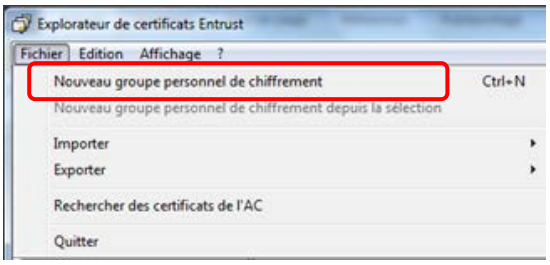
Cette fonction permet de regrouper des destinataires et d'éviter d'avoir à les sélectionner individuellement avant chaque envoi.

Les groupes imbriqués (groupes à l'intérieur d'autres groupes) ne sont pas autorisés.

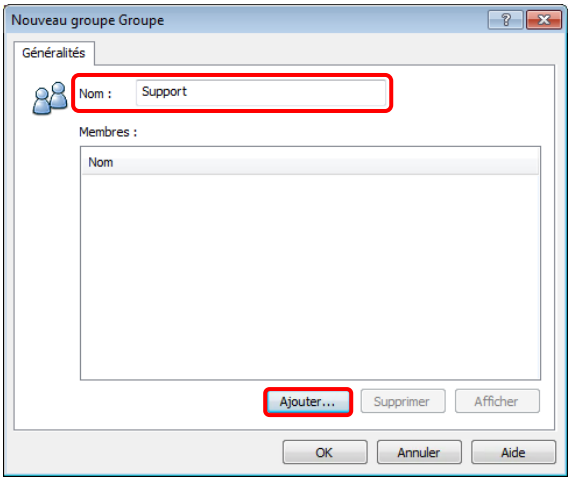
Pour créer un groupe personnel de chiffrement :

1. À l'aide du bouton droit de la souris, cliquer sur l'icône , dans la zone de notification de *Windows* et sélectionner « Explorateur de certificats Entrust ».

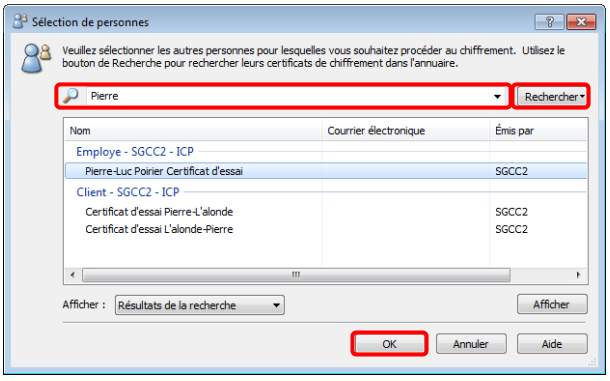
2. À partir du menu, sélectionner « Fichier → Nouveau groupe personnel de chiffrement ».



3. Dans le champ « Nom », saisir le nom du groupe et cliquer sur le bouton « Ajouter… ».

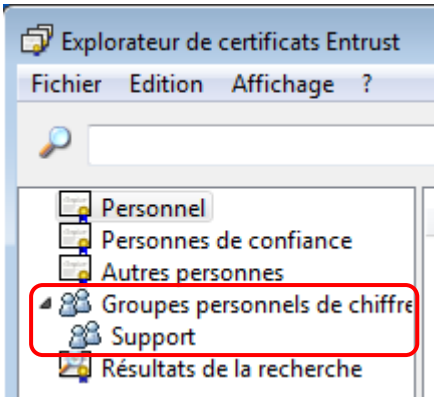


4. La fenêtre de sélection de personnes apparaîtra. Saisir le nom de la personne recherchée et cliquer sur le bouton « Rechercher ». Cliquer sur le nom de la personne à ajouter et cliquer sur le bouton « OK ».



Répéter les étapes 3 et 4 pour ajouter d'autres personnes.

5. Cliquer sur le bouton « OK » pour finaliser la création du groupe. Ce groupe s'affichera dans la section gauche de la fenêtre d'explorateur de certificats.

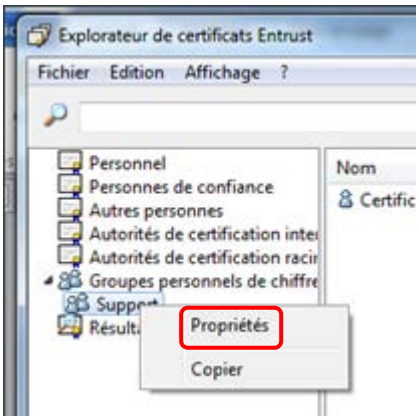


5.8 Ajouter ou supprimer une nouvelle personne à un groupe déjà créé

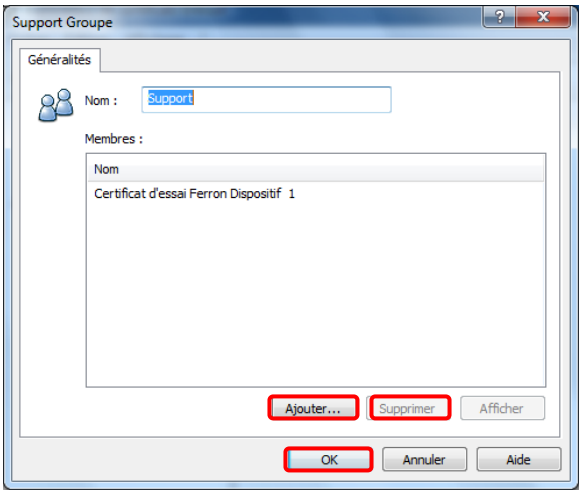
Cette fonction permet d'ajouter ou de supprimer le nom d'une personne à un groupe déjà existant.

Pour ajouter ou supprimer le nom d'une personne dans un groupe existant :

1. À l'aide du bouton droit de la souris, cliquer sur le nom du groupe et sélectionner l'option « Propriétés ».

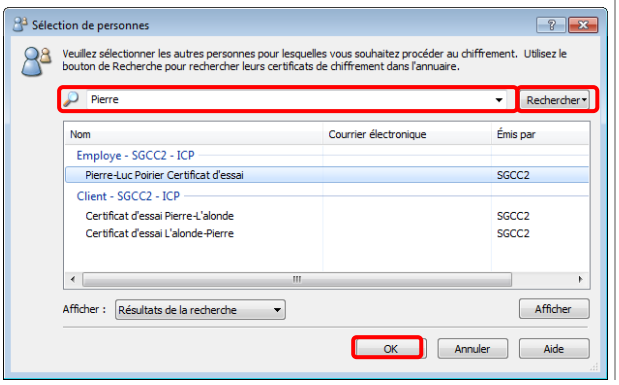


2. Pour ajouter le nom d'une personne, cliquer sur le bouton « Ajouter… » et passer à l'étape 3.



Pour supprimer le nom d'une personne, cliquer sur le nom de cette personne, puis sur le bouton « Supprimer ».

3. Saisir le nom de la personne et cliquer sur le bouton « Rechercher ». Cliquer sur le nom de la personne, puis sur le bouton « OK ».



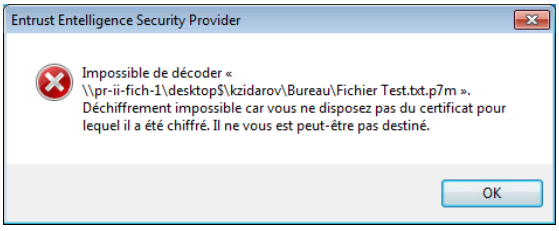
Pour ajouter le nom d'autres personnes, répéter les étapes 2 et 3.

6. Messages d'erreur lors de l'ouverture d'un fichier chiffré

Deux messages d'erreur peuvent s'afficher à l'ouverture d'un fichier chiffré. Ces messages indiquent qu'*Entrust* est incapable de décoder le fichier. Deux situations peuvent générer ces messages.

6.1 La personne qui tente d'ouvrir le fichier ne fait pas partie de la liste des destinataires

Si une personne tente d'ouvrir un fichier et que son nom n'apparaît pas dans la liste des destinataires, l'erreur suivante apparaîtra :

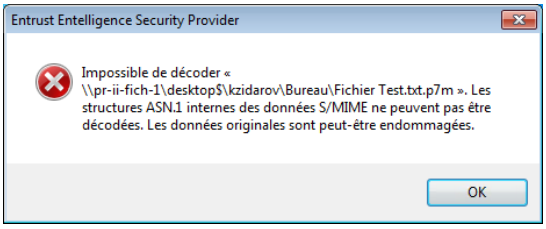


Pour qu'elle puisse ouvrir le fichier, cette personne devra communiquer avec l'expéditeur du fichier et faire ajouter son nom dans la liste des destinataires. L'opération de chiffrement devra toutefois être recommencée.

Pour des raisons de sécurité, il est impossible de voir la liste des personnes pour lesquelles un fichier a été sécurisé.

6.2 Le fichier a été altéré

Si un fichier a été altéré entre le moment où il a été chiffré et celui où il est ouvert, l'erreur suivante apparaîtra :



Pour qu'il puisse ouvrir le fichier, le destinataire devra contacter l'expéditeur pour qu'il réachemine une nouvelle copie n'ayant pas subi d'altérations.