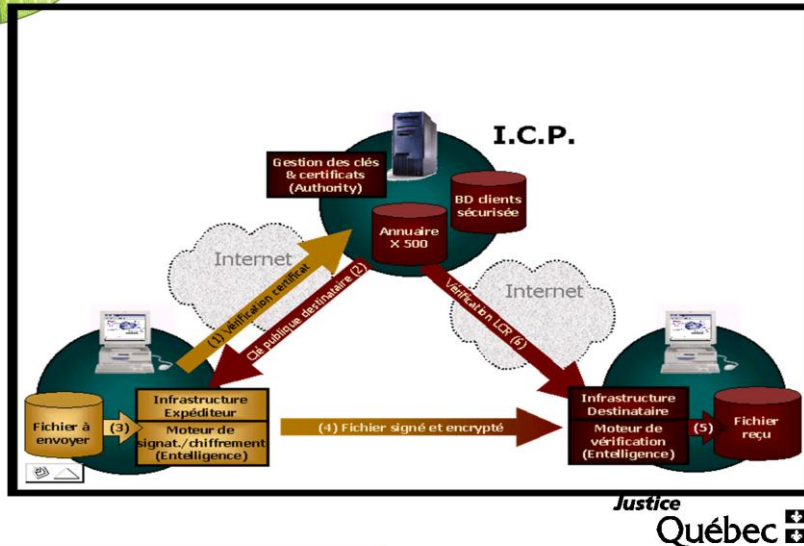


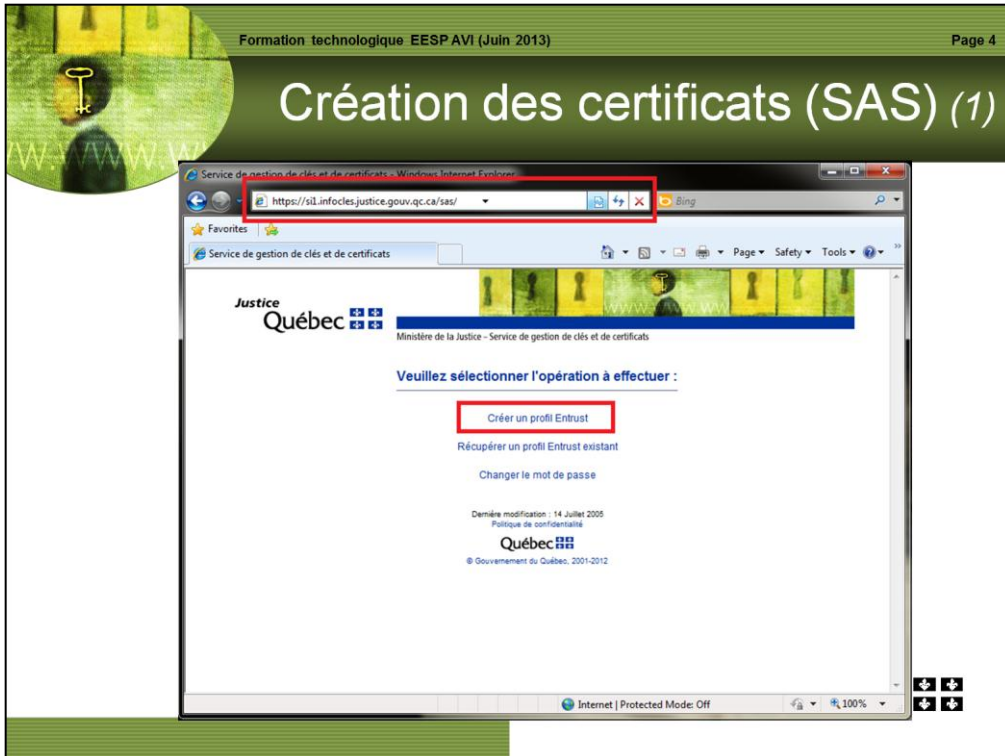
Mécanisme d'échange



Ce schéma illustre le mécanisme d'échange sécurisé de fichiers entre l'agent de vérification de l'identité (AVI) (expéditeur) et le Service de certification du MJQ (destinataire) :

1. L'AVI se connecte à *Entrust* avec son certificat.
2. *Entrust* vérifie la validité du certificat de l'AVI à l'infrastructure à clés publiques (ICP).
3. L'AVI sélectionne le certificat public de chiffrement du Service de certification au répertoire.
4. Les fichiers contenant le compte rendu de vérification de l'identité et le secret partagé sont chiffrés en utilisant la clé publique de chiffrement du Service de certification et signés à l'aide de la clé privée de signature de l'AVI.
5. Les fichiers sécurisés sont ensuite expédiés par courriel au Service de certification.
6. Le Service de certification reçoit le courriel, vérifie la validité du certificat de signature de l'AVI dans l'ICP, plus particulièrement dans la liste des certificats révoqués (LCR).
7. Le Service de certification déchiffre le document avec sa clé privée de déchiffrement.

Création des certificats (SAS) (1)



Le Service de certification va transmettre à l'AVI, dans un courriel, un hyperlien correspondant au site internet SAS :
[www.infocles.justice.gouv.qc.ca/sas](https://sil.infocles.justice.gouv.qc.ca/sas)

On utilisera cette page pour:

- Créer un profil;
- Récupérer un profil;
- Modifier son mot de passe de signature.

Création des certificats (SAS) (2)

Création d'un profil - Microsoft Internet Explorer

Précédente Recherche Favoris OK Lancer SnapIt

Adresse http://92.infocles.justice.gouv.qc.ca/bas/serveur-creer-RNAC.html

Justice Québec
Ministère de la Justice - Service de gestion de clés et de certificats

Créer le profil

Veuillez saisir les informations suivantes et cliquer sur le bouton "Créer le profil". Lorsque la page vous indiquant que le profil a été créé avec succès, cliquer sur le lien "Télécharger votre profil Entrust" et sauvegarder le fichier sur votre disque local.

Veuillez saisir les informations

Numéro de référence: 59123965

Code d'autorisation: 4QP9-PLVB-6WUK

Mot de passe: *****

Confirmation du mot de passe:

Créer le profil Effacer

Règles pour le mot de passe:

- doit contenir un minimum de 8 caractères
- doit contenir une lettre majuscule
- doit contenir une lettre minuscule
- un des caractères ne doit pas être égalé trop souvent
- le mot de passe et sa confirmation doivent être identiques
- doit compter un chiffre

Dernière modification: 16 Juillet 2005
Politique de confidentialité
Québec
© Gouvernement du Québec, 2001-2007

Justice Québec

1. Lors de la création de votre certificat, vous allez devoir saisir les informations que le Service de certification vous donnera au téléphone et par courriel;
2. Le numéro de référence est expédié par courriel par le Service de certification;
3. Le code d'autorisation est transmis au téléphone par un technicien du Service de certification;
4. Vous devez choisir un nom de fichier qui est généralement composé de la première lettre du prénom, suivi du nom de famille;
5. Vous devez choisir un mot de passe avec les règles suivantes:
 - Minimum de 8 caractères;
 - Doit contenir une lettre majuscule;
 - Doit contenir une lettre minuscule;
 - Doit contenir au moins un chiffre;
 - Ne doit pas contenir, pour plus de la moitié du mot de passe, une partie du nom de profil;
 - Ne doit pas répéter un même caractère pour plus de la moitié du mot de passe.
 - Ne doit pas contenir de caractère accentué;
 - Ne doit pas contenir de caractère spécial.
6. Il est à noter que lors de la création, un technicien du Service de certification vous accompagnera. De plus, la page Web de création contient un aide-mémoire sur les règles relatives au mot de passe.
 - Dans le cas où il y a des règles non respectées dans le mot de passe, ces règles seront marquées d'une croix rouge.
 - On suggère de préparer à l'avance, le mot de passe avant de débiter la délivrance.
 - Ce mot de passe ne sera connu que de vous et il n'est pas connu du Service de certification.

- Si vous oubliez ce mot de passe, prière d'aviser le Service de certification qui vous aidera à faire une récupération, opération qui vous permettra notamment de choisir un nouveau mot de passe.

Création des certificats (SAS) (3)



- Enregistrez le certificat sur un répertoire sécurisé, une clé USB ou tout autre emplacement permettant d'en préserver la sécurité.

Création des certificats (SAS) (4)

Faire une copie de sauvegarde ????



Les copies de sauvegarde ne sont pas mises à jour automatiquement. Vous devrez en assumer la gestion...!

Justice
Québec 

Il est déconseillé de conserver des copies de sauvegarde du certificat de signature à cause de la mise à jour de ces copies.

Les copies de sauvegarde exigent une gestion des mises à jour, ce qui peut occasionner des problèmes. Ainsi on peut oublier d'effectuer les mises à jour comme:

- Changement de mot de passe;
- Mise à jour du produit *Entrust*.

Récupération des certificats (SAS) (1)



The screenshot shows a web browser window displaying the 'Service de gestion de clés et de certificats' page from the Québec government. The address bar shows the URL 'https://s1.infocles.justice.gouv.qc.ca/sas/'. The page content includes the 'Justice Québec' logo and the text 'Ministère de la Justice - Service de gestion de clés et de certificats'. Under the heading 'Veillez sélectionner l'opération à effectuer :', there are three options: 'Créer un profil Entrust', 'Récupérer un profil Entrust existant' (highlighted with a red box), and 'Changer le mot de passe'. At the bottom of the page, it states 'Dernière modification : 14 Juillet 2005', 'Politique de confidentialité', and '© Gouvernement du Québec, 2001-2012'. The 'Justice Québec' logo is also present in the bottom right corner of the slide.

Dans l'éventualité où votre fichier de signature serait égaré, endommagé ou si vous avez oublié votre mot de passe, une récupération du certificat sera nécessaire:

- Communiquer avec le Service de certification pour demander une récupération. Cette opération consiste à vous délivrer de nouvelles clés et un certificat de signature tout en vous retournant vos clés et certificat de chiffrement. Il faudra vous identifier à l'aide de votre secret partagé et ce, afin de donner droit à la récupération. En cas de perte de votre secret partagé, vous devrez refaire vérifier votre identité par un AVI.



Récupération des certificats (SAS) (2)

Récupération d'un profil - Microsoft Internet Explorer

http://s1.infodes.justice.gouv.qc.ca/sas/server-recover-41NAC.html

Justice Québec
Ministère de la Justice - Service de gestion de clés et de certificats

Récupérer le profil

Veuillez saisir les informations suivantes et cliquer sur le bouton "Récupérer le profil". Lors que la page vous indiquant que le profil a été récupéré avec succès, cliquer sur le lien "Télécharger votre profil Entrust" et sauvegarder le fichier sur votre disque local.

Veuillez saisir les informations

Numéro de référence:

Code d'autorisation:

Mot de passe:

Confirmation du mot de passe:

Règles pour le mot de passe:

- ✗ doit contenir un minimum de 8 caractères
- ✓ doit comporter une lettre majuscule
- ✓ doit comporter une lettre minuscule
- ✓ les deux caractères ne doit pas être adjacés l'un à côté de l'autre
- ✗ le mot de passe et sa confirmation doivent être identiques
- ✓ doit comporter un chiffre

Dernière modification : 14 Juillet 2005
Politique de confidentialité

Justice Québec
© Gouvernement du Québec, 2001-2007



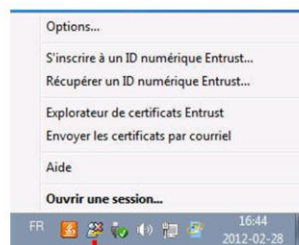
Récupération des certificats (SAS) (2)



- Enregistrez le certificat sur un répertoire sécurisé, une clé USB ou tout autre emplacement permettant d'en préserver la sécurité.

Utilisation d'Entrust (1)

- ☀ **Ouvrir une session** via le menu contextuel de l'icône Entrust situé dans la barre des tâches



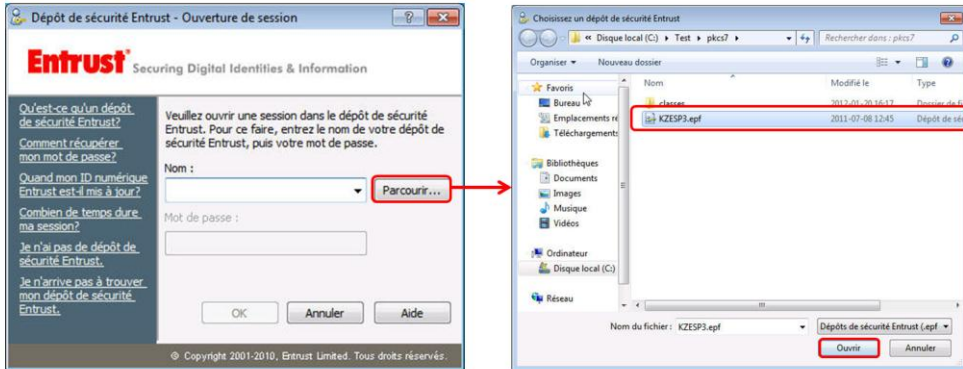
Justice
Québec

Positionner le curseur sur la clé d'Entrust puis cliquer sur le bouton droit de la souris.



Utilisation d'Entrust

Ouverture de session (1)



Justice
Québec

Après l'ouverture de la session *Entrust*, une icône de clé apparaît au bas de l'écran indiquant qu'une session sécurisée est en cours.



Utilisation d'Entrust

Ouverture de session (2)

Dépôt de sécurité Entrust - Ouverture de session

Entrust Securing Digital Identities & Information

Qu'est-ce qu'un dépôt de sécurité Entrust?
Comment récupérer mon mot de passe?
Quand mon ID numérique Entrust est-il mis à jour?
Combien de temps dure ma session?
Je n'ai pas de dépôt de sécurité Entrust.
Je n'arrive pas à trouver mon dépôt de sécurité Entrust.

Vous devez ouvrir une session dans le dépôt de sécurité Entrust. Pour ce faire, entrez le nom de votre dépôt de sécurité Entrust, puis votre mot de passe.

Nom :
KZESP3

Mot de passe :

OK Annuler Aide

© Copyright 2001-2010, Entrust Limited. Tous droits réservés.

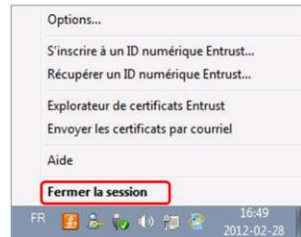


Justice
Québec

Utilisation d'Entrust

Fermeture de session

- ☀ **Fermer une session** via le menu contextuel de l'icône Entrust situé dans la barre des tâches

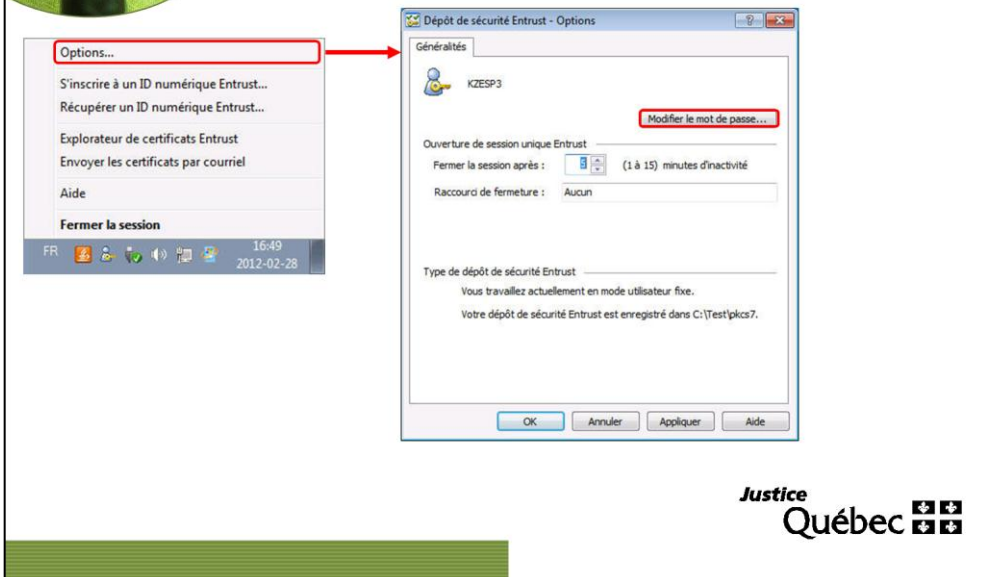


Justice
Québec

Positionner le curseur sur la clé d'Entrust puis cliquer sur le bouton droit de la souris.

Options d'Entrust

Changement du mot de passe (1)

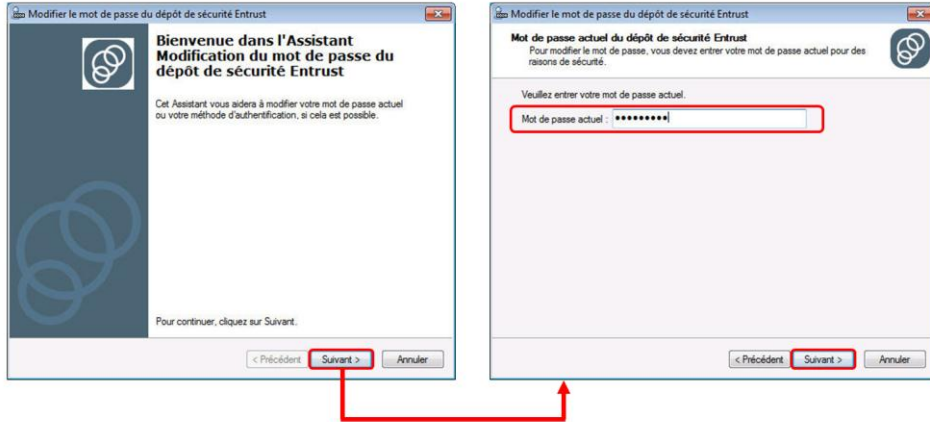


- Positionner le curseur sur la clé d'Entrust puis cliquer sur le bouton droit de la souris.
- Sélectionner « Options » puis cliquer sur le bouton « Modifier le mot de passe ».



Options d'Entrust

Changement du mot de passe (2)



L'utilisateur doit saisir son mot de passe actuel avant de pouvoir le modifier.

Options d'Entrust

Changement du mot de passe (3)

Modifier le mot de passe du dépôt de sécurité Entrust

Nouveau mot de passe du dépôt de sécurité Entrust

Les règles de composition des mots de passe vous aident à choisir un mot de passe sécurisé pour protéger votre dépôt de sécurité Entrust.

Veillez entrer votre nouveau mot de passe.

Mot de passe :

Confirmer le mot de passe :

Votre mot de passe doit respecter les règles suivantes :

- ✓ doit comporter au moins 8 caractères.
- ✓ doit contenir une lettre majuscule.
- ✓ doit contenir une lettre minuscule.
- ✓ doit contenir au moins un chiffre.
- ✓ ne doit pas contenir plus de la moitié du nom d'un dépôt de sécurité.
- ✓ ne doit pas répéter un même caractère pour plus de la moitié du mot de passe.
- ✓ ne doit pas réutiliser le dernier mot de passe

< Précédent **Suivant >** Annuler

Modifier le mot de passe du dépôt de sécurité Entrust

Fin de l'Assistant Modification du mot de passe du dépôt de sécurité Entrust

Votre mot de passe a été modifié avec succès. Si vous possédez des copies de votre dépôt de sécurité Entrust, elles continueront à utiliser votre ancien mot de passe.

Pour fermer l'assistant, cliquez sur Terminer.

< Précédent **Terminer** Annuler

Justice Québec

Les spécifications relatives au choix du nouveau mot de passe sont identiques à celles de l'étape de la création.

Options d'Entrust

Fermer la session

Dépôt de sécurité Entrust - Options

Généralités

KZESP3

Modifier le mot de passe...

Ouverture de session unique Entrust

Fermer la session après : 15 (1 à 15) minutes d'inactivité

Raccourci de fermeture : Aucun

Type de dépôt de sécurité Entrust

Vous travaillez actuellement en mode utilisateur fixe.

Votre dépôt de sécurité Entrust est enregistré dans C:\Test\pica7.

OK Annuler Appliquer Aide

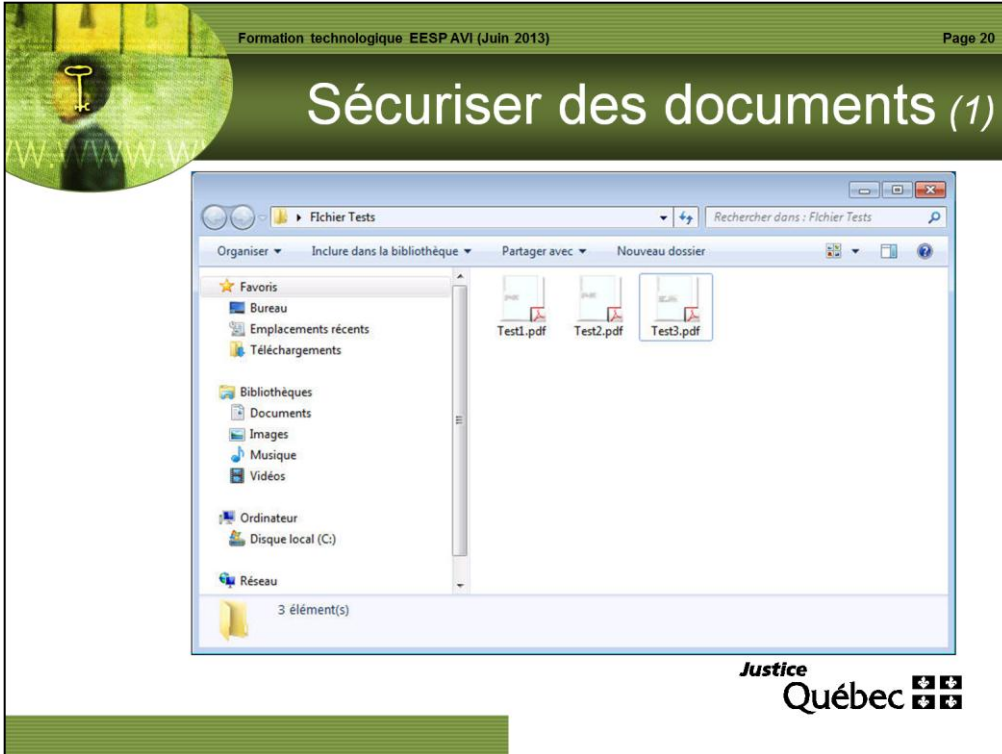
FR 16:41 2012-02-28

Justice Québec

Après l'expiration du délai, la session est automatiquement fermée

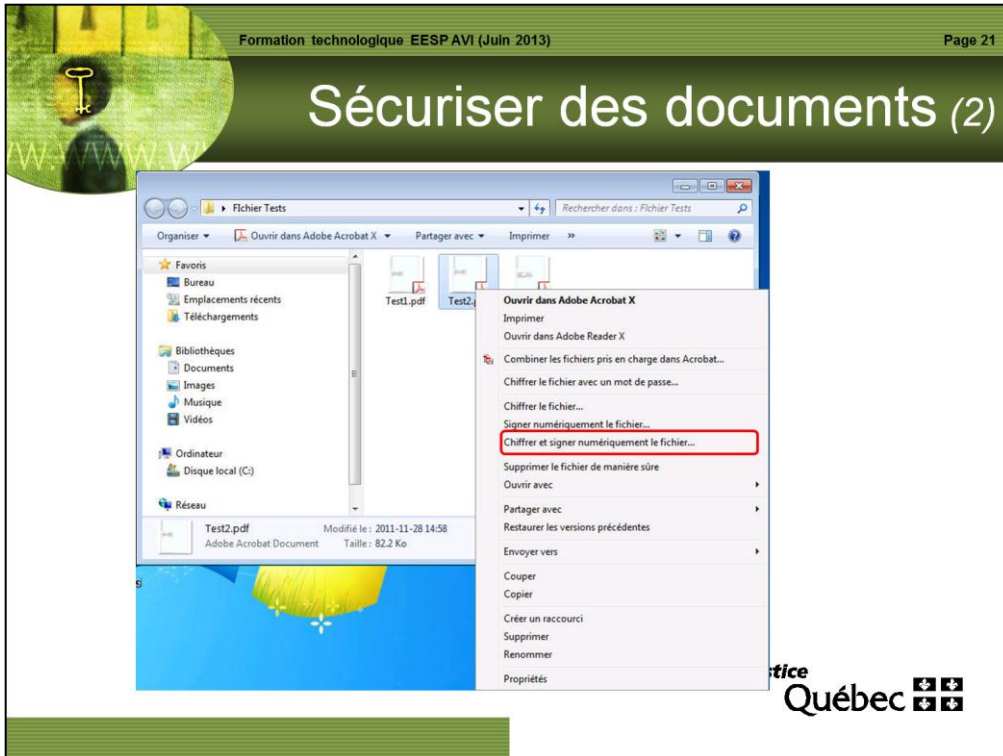
- Dans un délai maximum de 15 minutes, s'il n'y a aucune activité sur le poste de travail, la session *Entrust* va se fermer dans les cas suivants :
 - Si un logiciel ou une composante d'*Entrust* est ouverte, la session est fermée.
 - Si aucun logiciel ou composante n'est ouvert, la session est fermée.
- Le mot de passe sera exigé afin d'activer ou ouvrir la session *Entrust* de nouveau.

Sécuriser des documents (1)



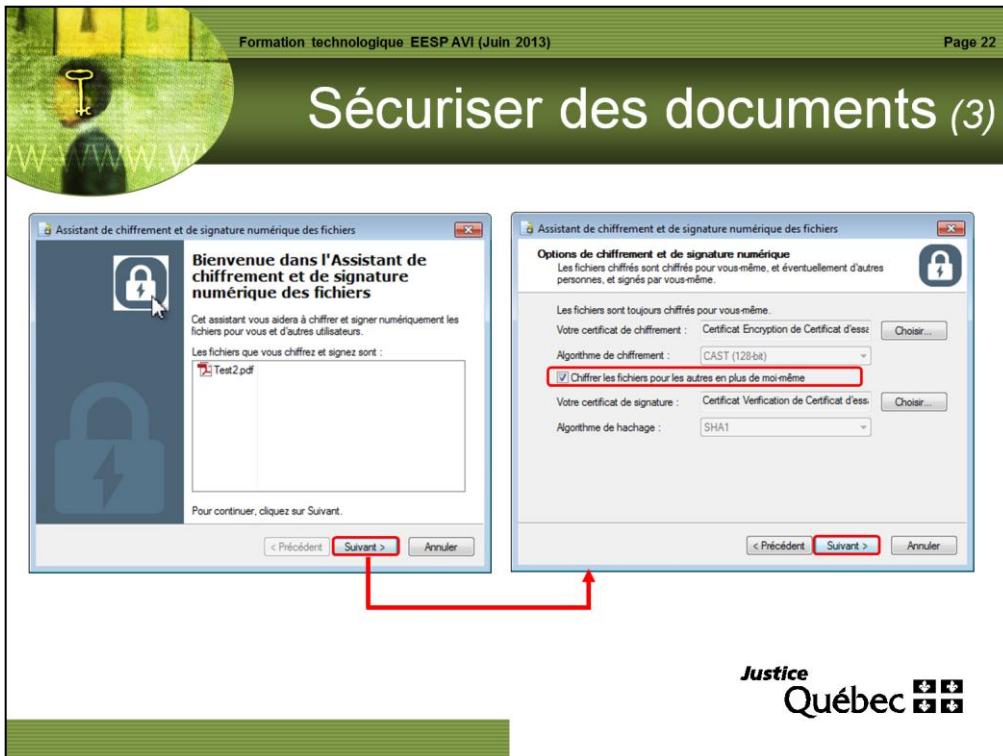
- Lorsque l'on signe et chiffre un fichier, le fichier résultant du traitement apparaît sous la forme d'une icône de document accompagné d'un cadenas
- Le fichier peut être chiffré seulement pour nous ou inclure également une liste de destinataire.
- Si la session est fermée, *Entrust* exigera l'ouverture d'une session pour effectuer la signature et le chiffrement du fichier.

Sécuriser des documents (2)



- Quand on sécurise un fichier pour un destinataire, on sécurise également le fichier pour soi-même.
- Lors du premier chiffrement, durant une même session, un message de confirmation apparaît demandant l'autorisation pour que le logiciel accède au répertoire d'*Entrust*. Dans ce cas, cliquer sur « Oui ».

Sécuriser des documents (3)



- L'option « Chiffrer les fichiers pour les autres en plus de moi-même » sécurise le document pour soi et d'autres destinataires.
- Lors du premier chiffrement, durant une même session, un message de confirmation apparaît demandant l'autorisation pour que le logiciel accède au répertoire d'Entrust. Dans ce cas, cliquer sur « Oui ».

Sécuriser des documents (4)

(1) Saisir le nom du destinataire pour lequel on veut chiffrer

(2) Cliquer sur rechercher

(3) Sélectionner

(4) Cliquer sur OK pour ajouter le destinataire

Nom	Courrier électronique	Émis par	Date d'expir
SGCC2 - ICP			
Certificat d'essais Jean-Guy...		SGCC2	2012-06-18
Client - SGCC2 - ICP			
Certificat d_essais Jean-Guy...		SGCC2	2013-05-07
Certificat d'essais Jean-Guy...	igmorissette@dr.c.gouv...	SGCC2	2013-06-02

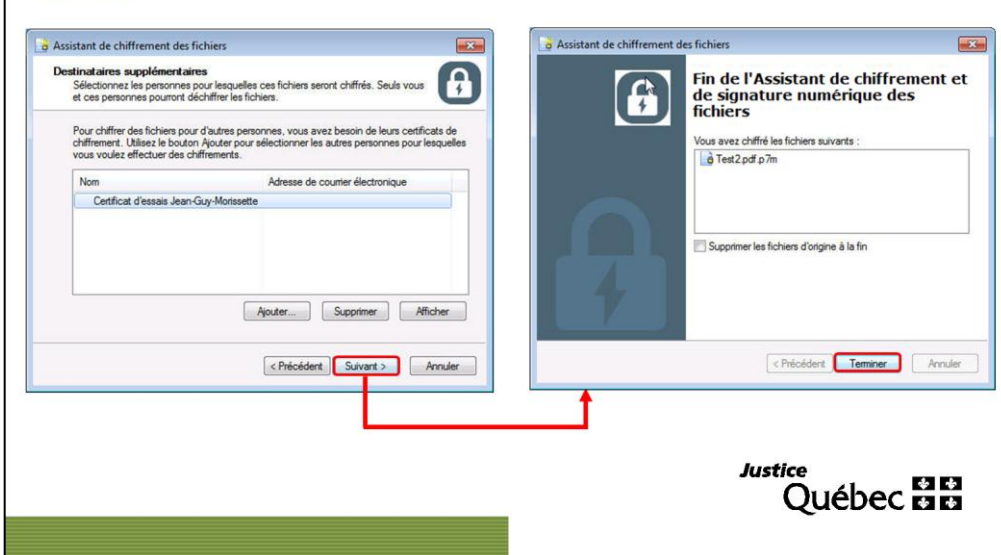
Justice Québec

- Cliquer sur le bouton « Ajouter »;
- Spécifier les critères de recherche ex. pour le Service de certification « *(GCC)* » et cliquer sur le bouton « Rechercher ».
- Sélectionner le destinataire pour qui le fichier doit être sécurisé et cliquer sur « OK ».

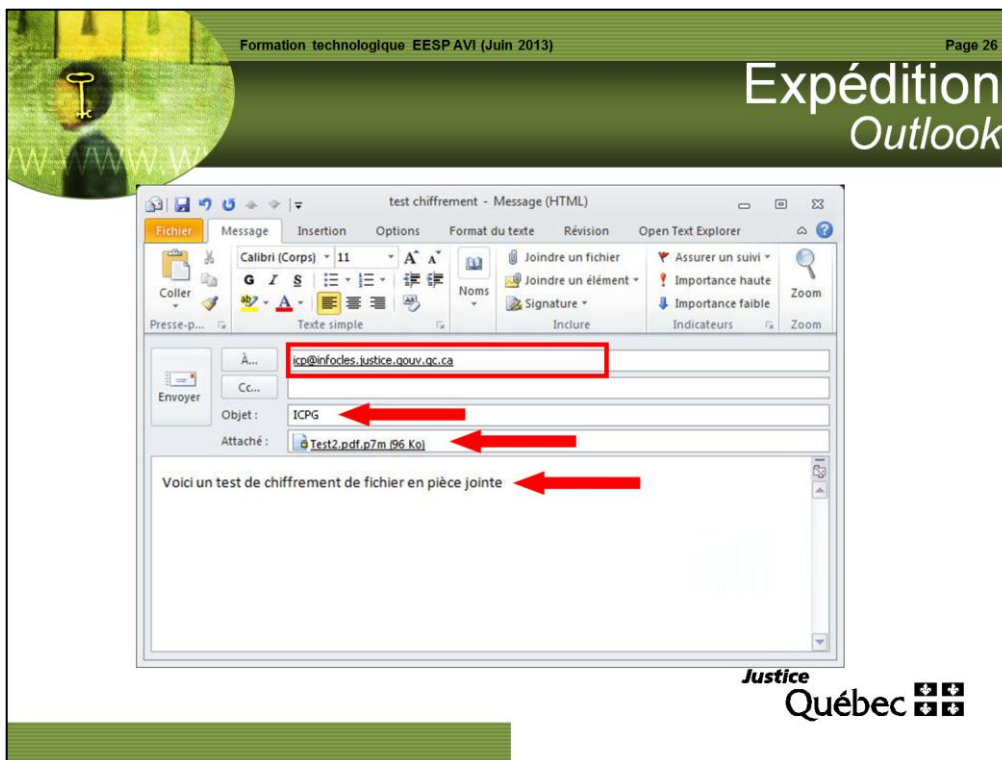
Note :

- Généralement, la recherche est faite avec le dernier nom de famille (last name). Si une personne a deux noms de familles, la recherche est faite par son second nom de famille.
- Si la recherche est sans résultats et le nom recherché contient des accents, réessayer avec le même nom mais sans accent.

Sécuriser des documents (5)



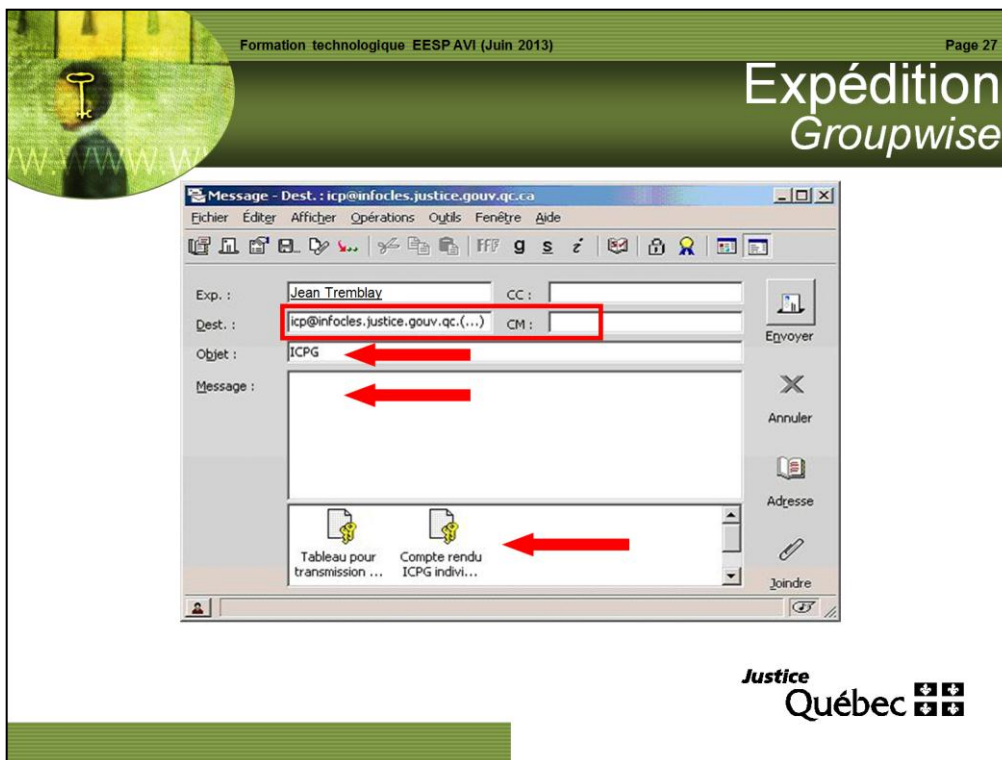
- Répéter la même procédure que précédemment montré pour ajouter d'autres destinataires à la liste
- Lorsque la section « Supprimer les fichiers d'origine à la fin » est cochée le fichier original non sécurisé sera automatiquement supprimé.



Dans le courriel, indiquer les renseignements nécessaires pour l'envoi des « compte rendu de vérification de l'identité » et « tableau de secret partagé » :

- L'adresse d'expédition du courriel est : icp@infocles.justice.gouv.qc.ca;
- L'objet doit être : ICPG;
- Le texte ne peut pas contenir de renseignements personnels. Le laisser vide ou ajouter simplement une phrase de courtoisie;
- Joindre les fichiers sécurisés.

S'assurer que les fichiers soient signés et chiffrés avant de les joindre!



Dans le courriel, indiquer les renseignements nécessaires pour l'envoi des « Procès Verbaux » et « Tableaux de secrets partagés » :

L'adresse est : icp@infocles.justice.gouv.qc.ca;

L'objet doit être : ICPG;

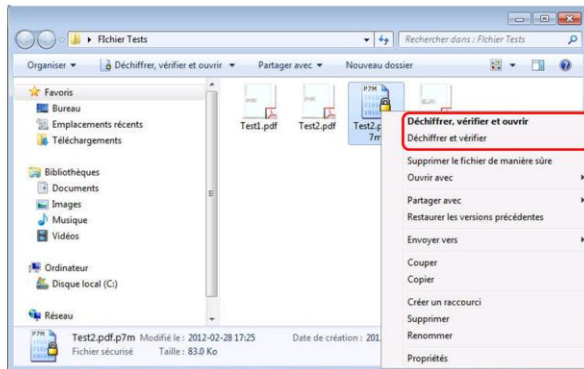
Le texte ne peut pas contenir de renseignements personnels. Le laisser vide ou ajouter simplement une phrase de courtoisie;

Joindre les fichiers concernés.

S'assurer que les fichiers soient signés et chiffrés avant de les joindre!

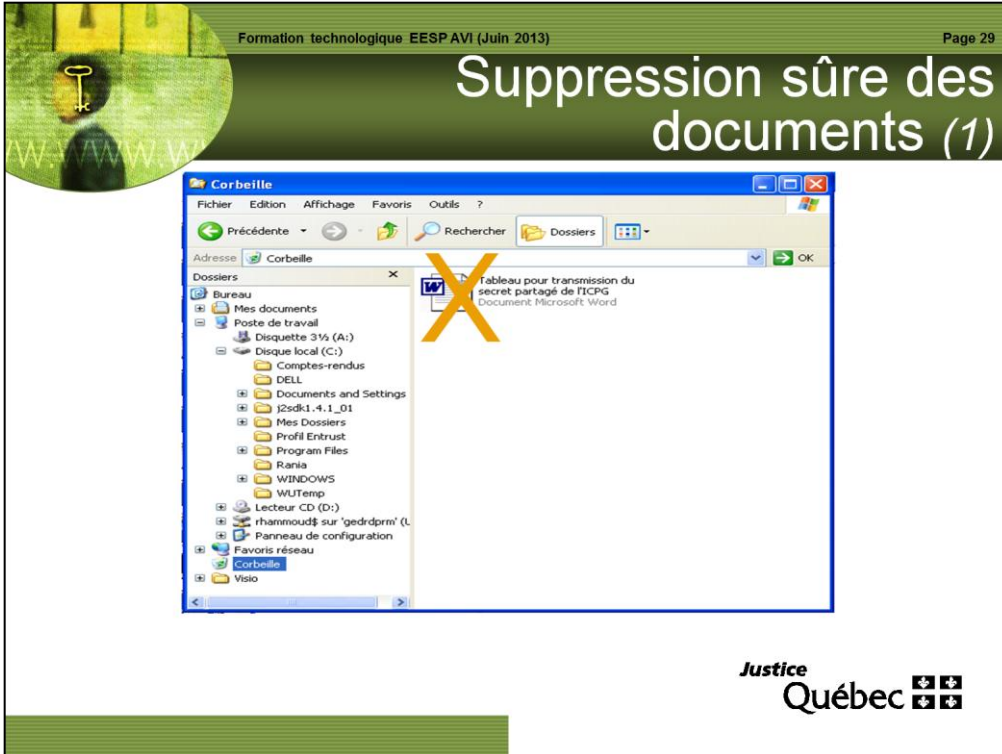
Déchiffrement des documents

- ☀ En double-cliquant sur le document
- ☀ À partir du menu contextuel en cliquant le bouton droit sur le document



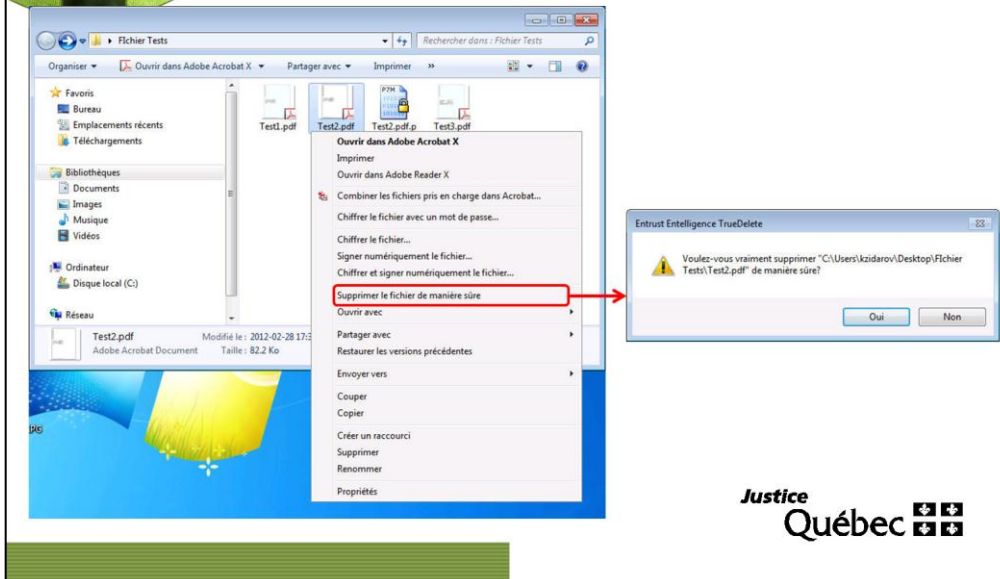
- Déchiffrer, vérifier et ouvrir : déchiffre le document, valide le certificat, et ouvre le document dans son application d'origine (ex. Word).
- Également, le fichier se déchiffre et s'ouvre en double-cliquant sur le document chiffré.
- Déchiffrer et vérifier : déchiffre le document et valide le certificat, sans ouvrir le document.

Suppression sûre des documents (1)



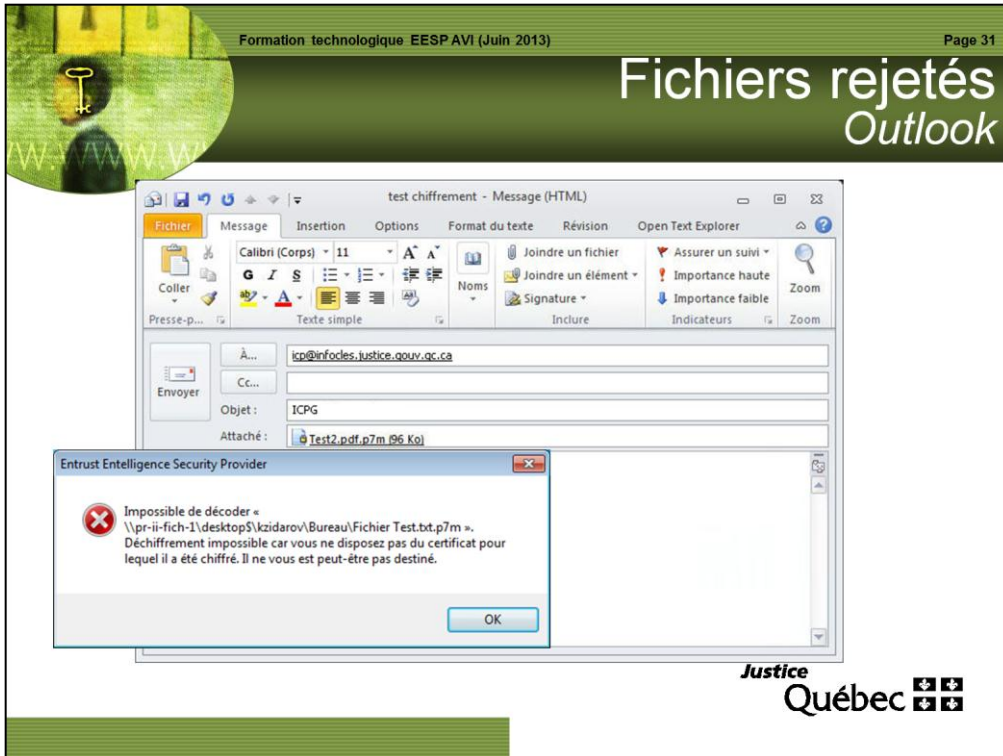
- La « Suppression » régulière rend les renseignements confidentiels vulnérables et accessibles à une personne malveillante.

Suppression sûre des documents (2)



- L'option « Supprimer le fichier de manière sûre » permet de chiffrer un fichier avant de le supprimer (mettre dans la corbeille).
- De cette façon, nous sommes assurés que, même si une personne malveillante tente de récupérer le document supprimé, il lui sera impossible de le déchiffrer.

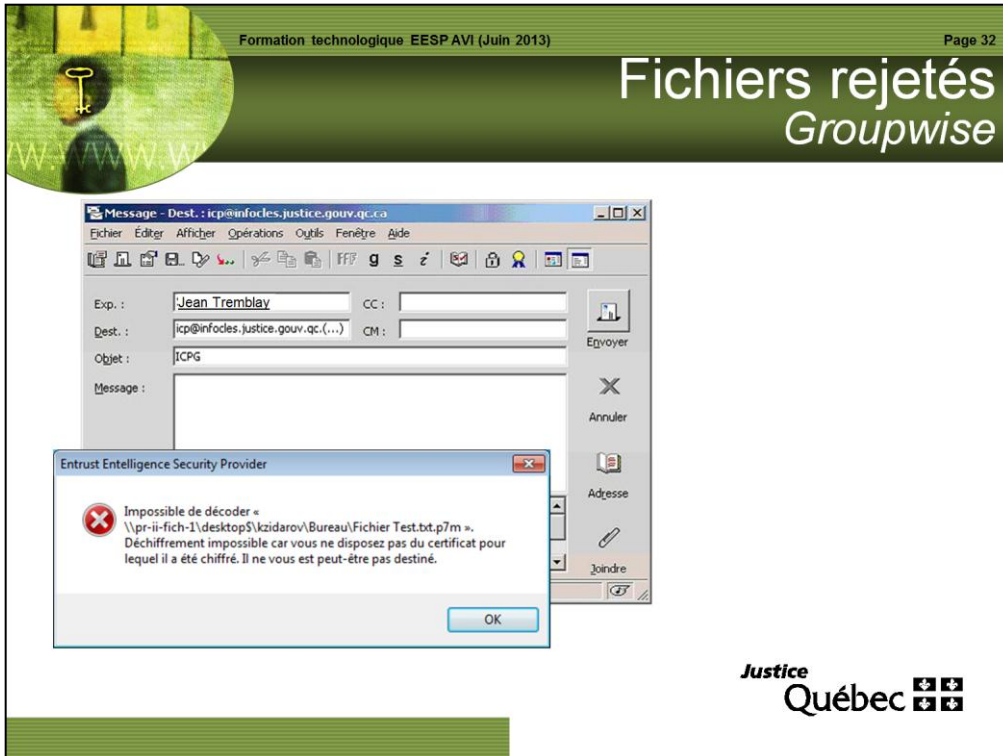
Fichiers rejetés Outlook



Lorsqu'on tente d'ouvrir un fichier qui ne nous a pas été destiné, le document est rejeté.

Fichiers rejetés

Groupwise



Un document est rejeté s'il a été chiffré pour le mauvais destinataire.



Fichiers rejetés Contenu altéré

The screenshot displays a Windows desktop environment. On the left, a Notepad window titled 'Test2.pdf (7m) - Notepad' shows a corrupted PDF file with garbled text. In the center, a File Explorer window titled 'Fichier Tests' shows a folder containing two PDF files, 'Test1.pdf' and 'Test2.pdf'. The 'Test2.pdf' file is selected, and the context menu is open, with the 'Déchiffrer, vérifier et ouvrir' option highlighted. In the foreground, an error dialog box from 'Entrust Entelligence Security Provider' is displayed, with the message: 'Impossible de décoder « \\pr-ii-fich-1\desktop5\kzidarov\Bureau\Fichier Test.bt.p7m ». Les structures ASN1 internes des données S/MIME ne peuvent pas être décodées. Les données originales sont peut-être endommagées.' The dialog box has an 'OK' button.

Justice
Québec

Un document est rejeté si son contenu chiffré a été altéré.

Ajouter le certificat du service de certification dans le carnet d'adresse personnel d'Entrust (1)

(1) Saisir *(GCC) comme critère de recherche

(2) Cliquer sur rechercher

(3) Sélectionner

(4) Cliquer avec le bouton droit de la souris et sélectionner l'option suivante

Nom	Courrier électronique	Émis par	Date d'exp
DISPOSITIF - SGCC2 - ICP		SGCC2	2013-09-12
INFOCLES.JUSTICE (MIQ-GCC)			

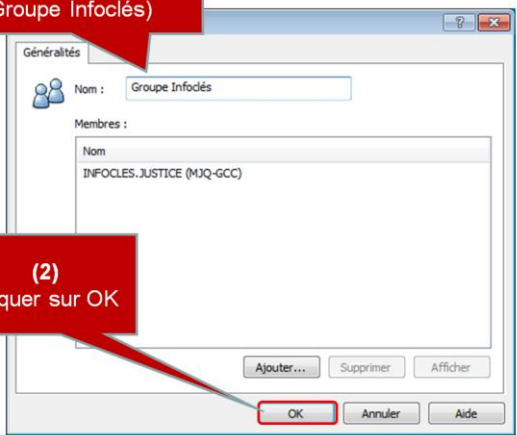
Justice Québec

Cette fonctionnalité est utile si vous signez souvent pour les mêmes personnes. Cela vous évite de faire des recherches manuelles à chaque fois que vous voulez signer/chiffrer pour un groupe de personnes spécifique.



Ajouter le certificat du service de certification dans le carnet d'adresse personnel d'Entrust (2)

(1)
Saisir un nom de groupe (par exemple Groupe Infoclés)



(2)
Cliquer sur OK

Québec

Le bouton « Ajouter » permet d'ajouter d'autres membres au groupe que vous venez de créer.



Ajouter le certificat du service de certification dans le carnet d'adresse personnel d'Entrust (3)

Le groupe infoclés est maintenant créé et il contient le certificat du MJQ-GCC

Nom	Courrier électronique	Émis par	Date d'expir
DISPOSITIF - SGCC2 - ICP			
INFOCLESJUSTICE (MIQ-GCC)		SGCC2	2013-09-12

La recherche a retourné 1 certificats.



Questions



Justice
Québec 
