Le Service de certification du ministère de la Justice

Justice Québec

Contenu de la présentation

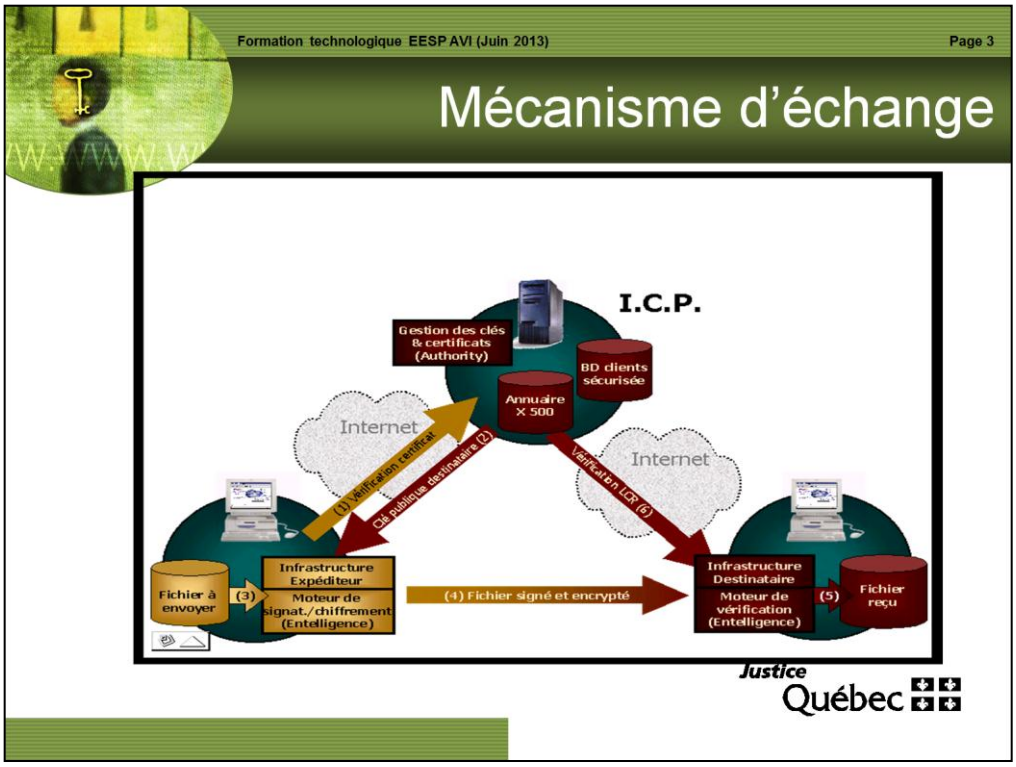
- ICPG : Mécanisme d'échange
- Création des certificats
- Récupération des certificats

- Utilisation d'Entrust
- Options Entrust

- Chiffrement des documents
- Expédition – Outlook
- Expédition – Groupwise
- Déchiffrement des documents

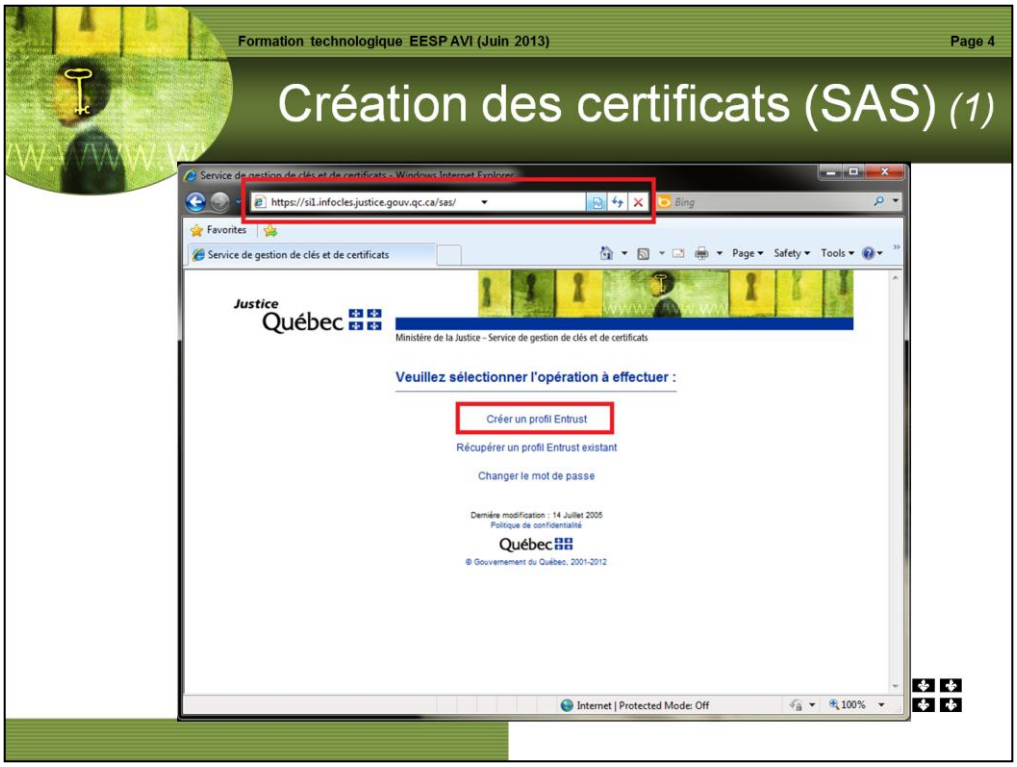
- Suppression sûre des documents
- Fichiers rejetés
- Trucs et astuces

Justice Québec



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 sécurisé 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.

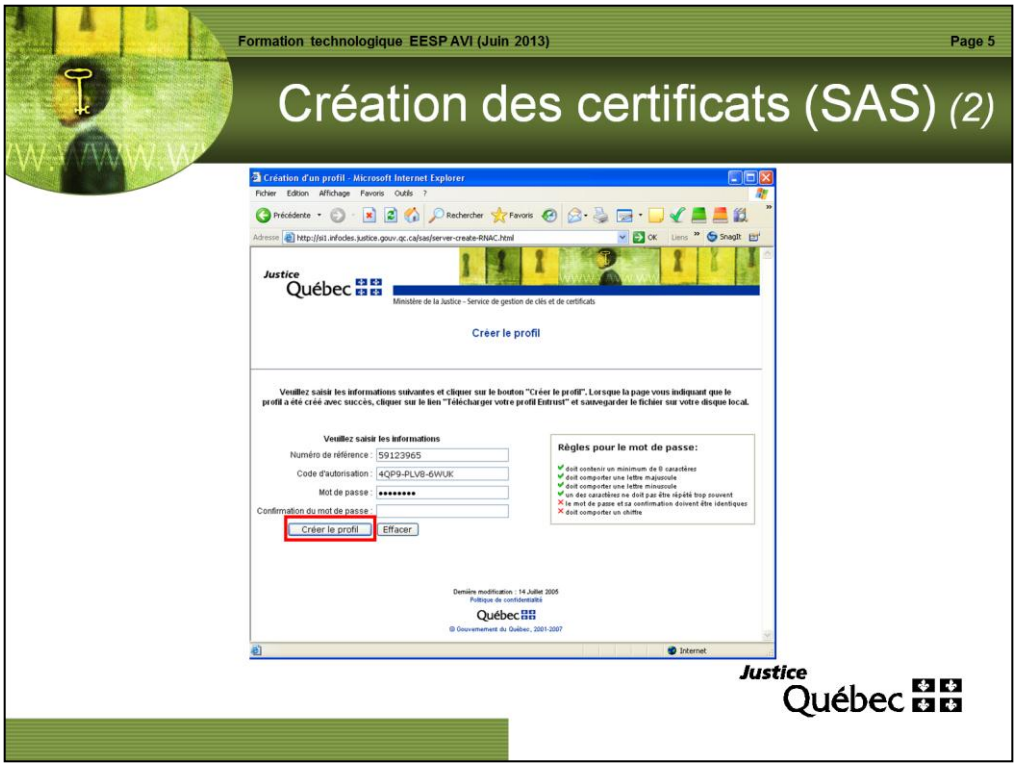


Le Service de certification va transmettre à l'AVI, dans un courriel, un hyperlien correspondant au site internet SAS :

www.infocles.justice.gouv.qc.ca/sas

On utilisera cette page pour:

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



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 débuter la délivrance.
- Ce mot de passe ne sera connu que de vous et il n'est pas connu du Service de certification.

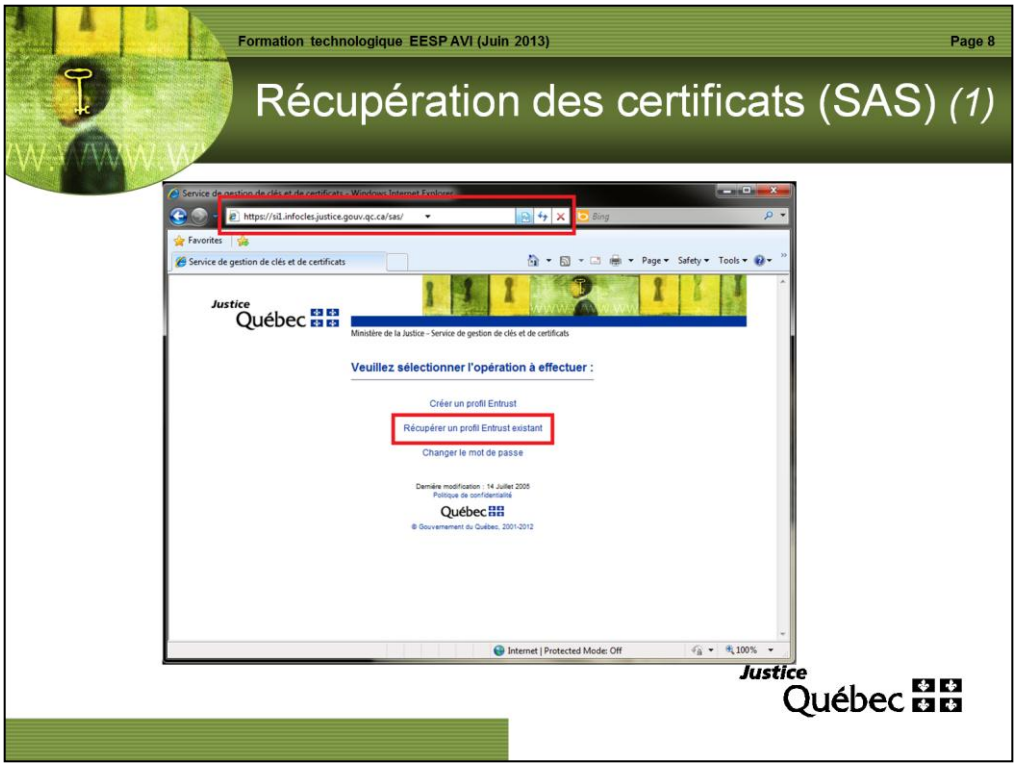
- Si vous oubliez ce mot de passe, prière d'aviser le Service de certification qui vous aidera à faire une récupération, opération qui vous permettra notamment de choisir un nouveau mot de passe.

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

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*.



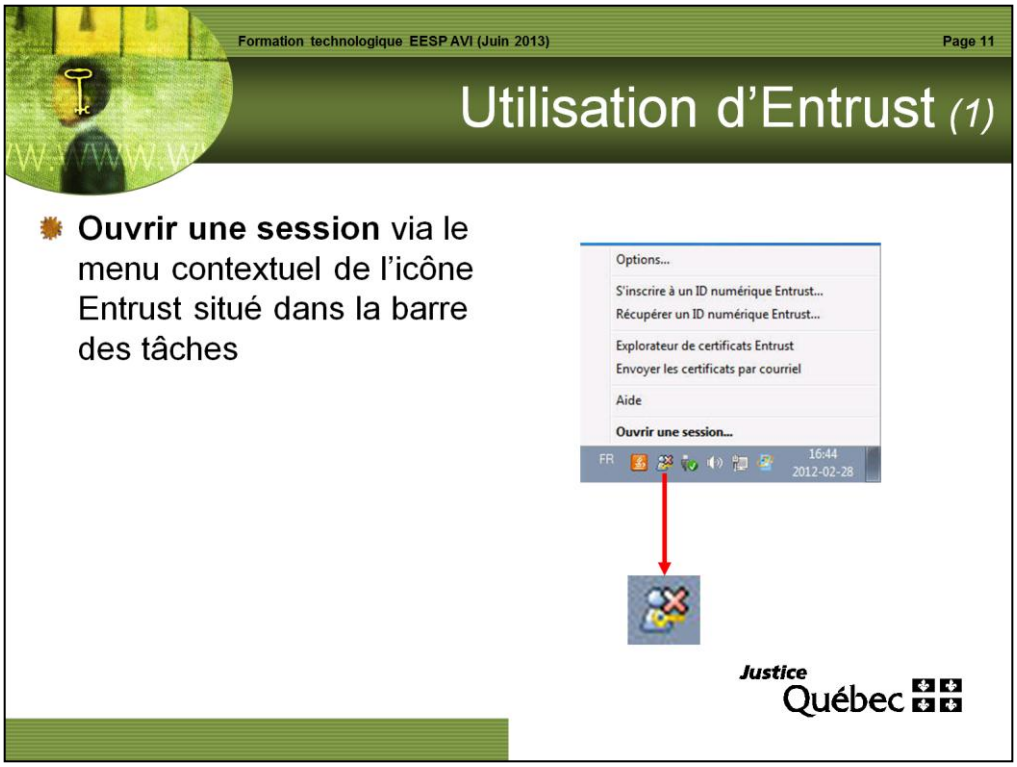
Dans l'éventualité où votre fichier de signature serait égaré, endommagé ou si vous avez oublié votre mot de passe, une récupération du certificat sera nécessaire:

• 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.

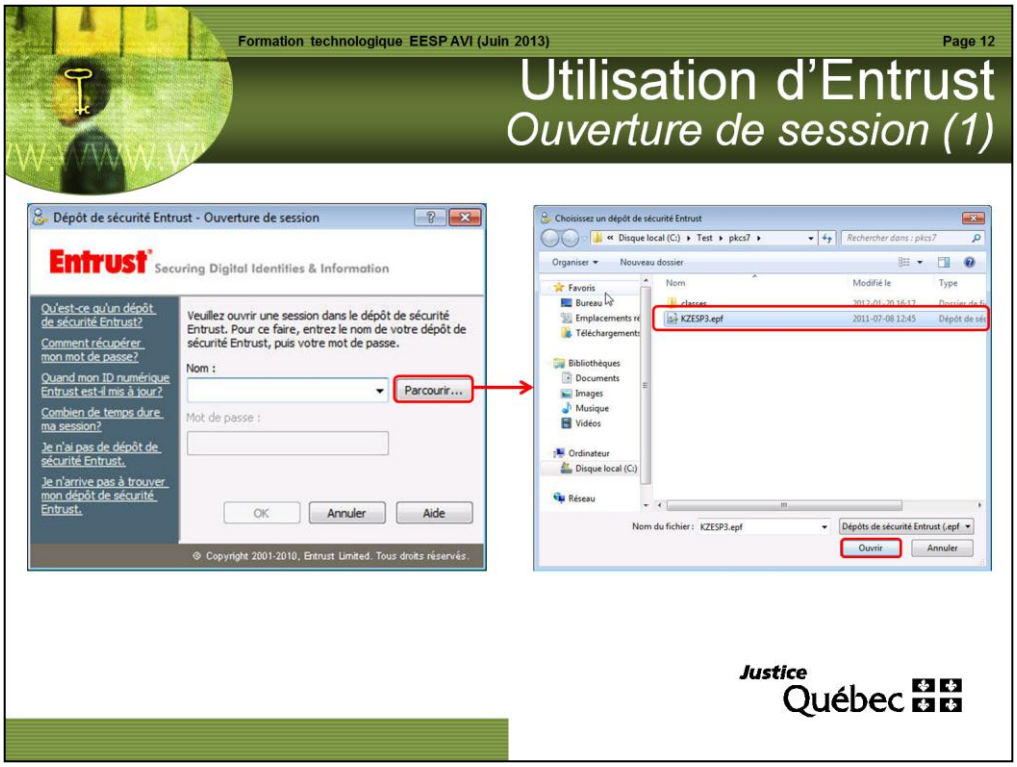
Récupération des certificats (SAS) *(2)*

Justice Québec

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

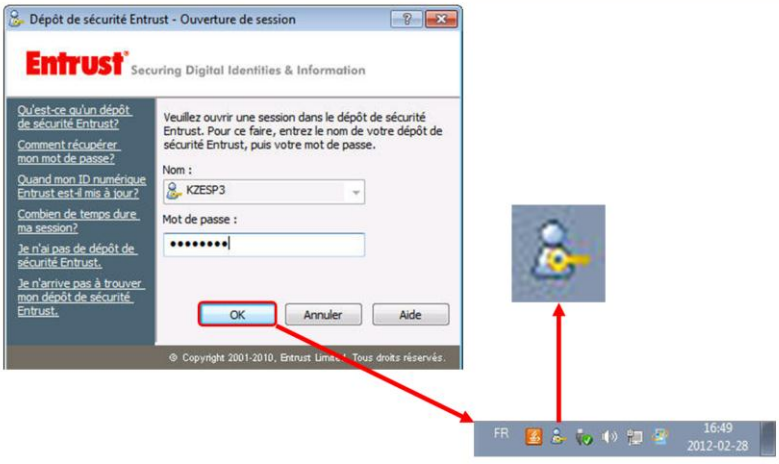


Positionner le curseur sur la clé d'*Entrust* puis cliquer sur le bouton droit de la souris.

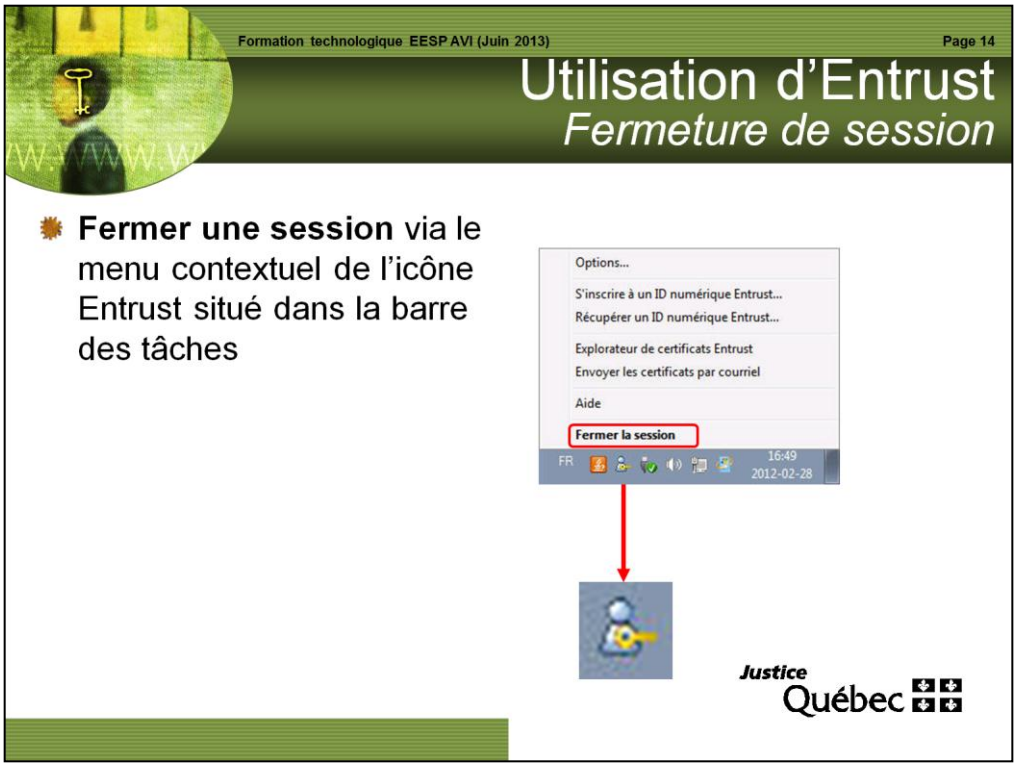


Après l'ouverture de la session *Entrust*, une icône de clé apparaît au bas de l'écran indiquant qu'une session sécurisée est en cours.

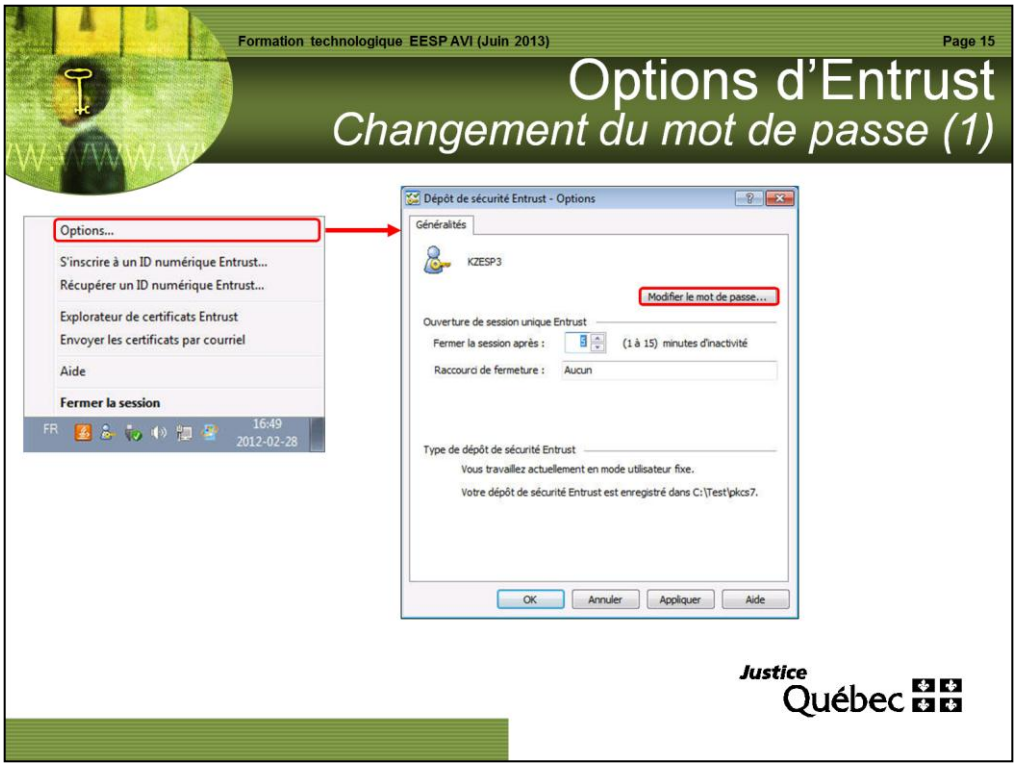
Utilisation d'Entrust
Ouverture de session (2)



Justice Québec

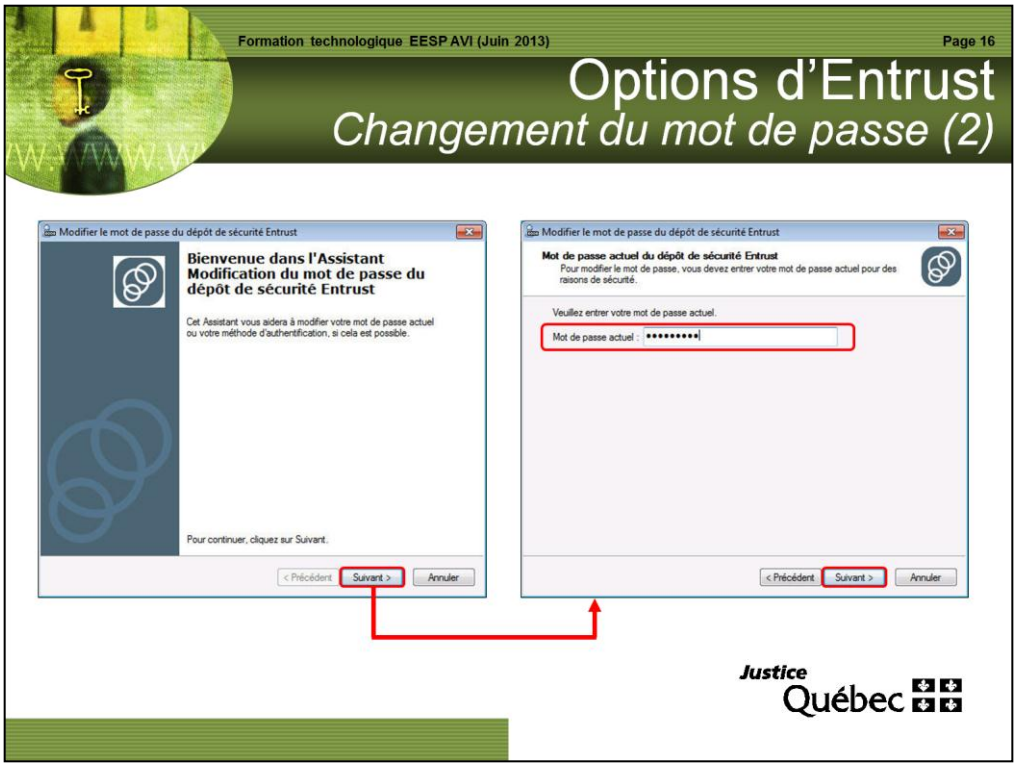


Positionner le curseur sur la clé d'*Entrust* puis cliquer sur le bouton droit de la souris.

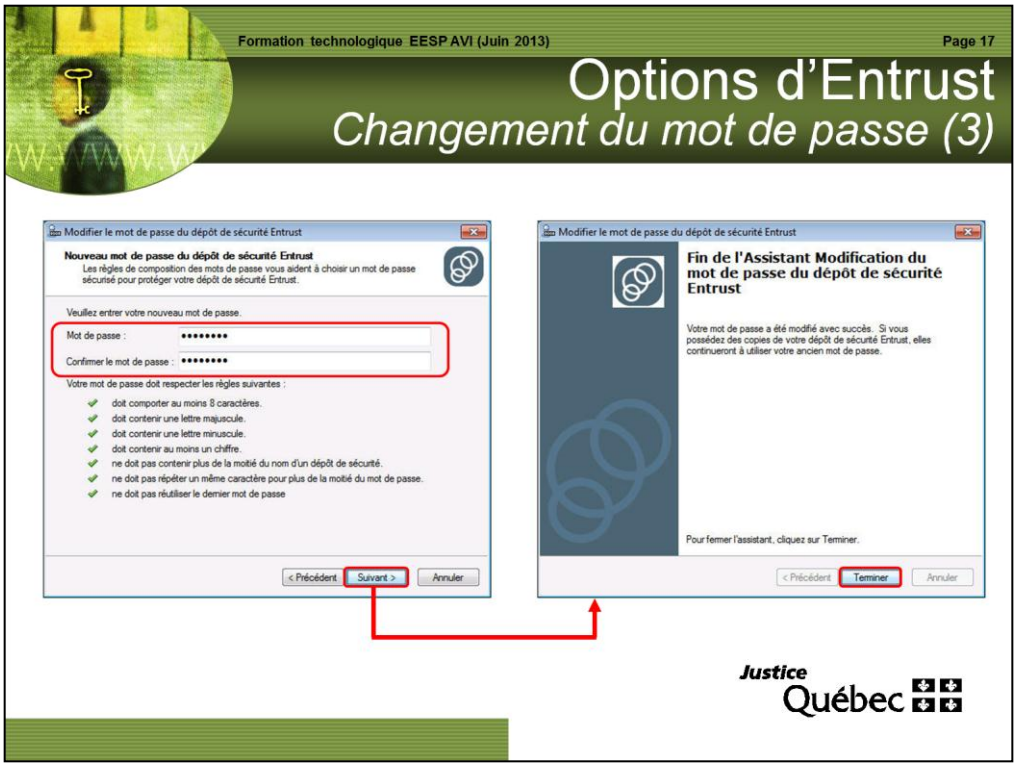


- Positionner le curseur sur la clé d'*Entrust* puis cliquer sur le bouton droit de la souris.

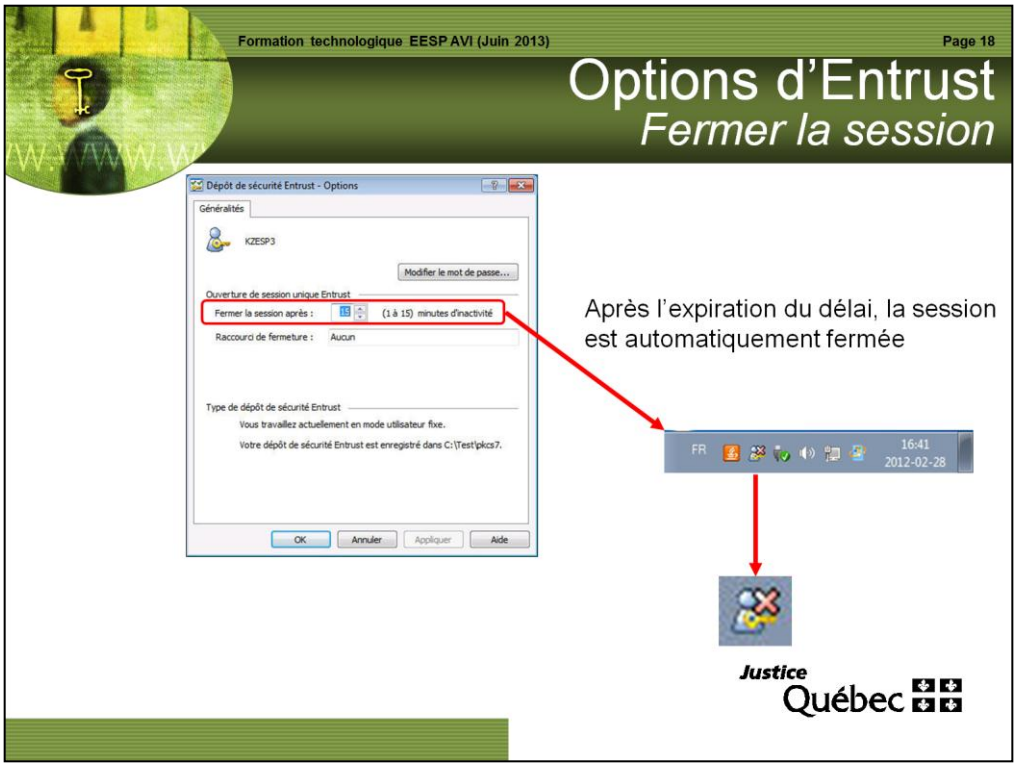
- Sélectionner « Options » puis cliquer sur le bouton « Modifier le mot de passe ».



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



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



- 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.

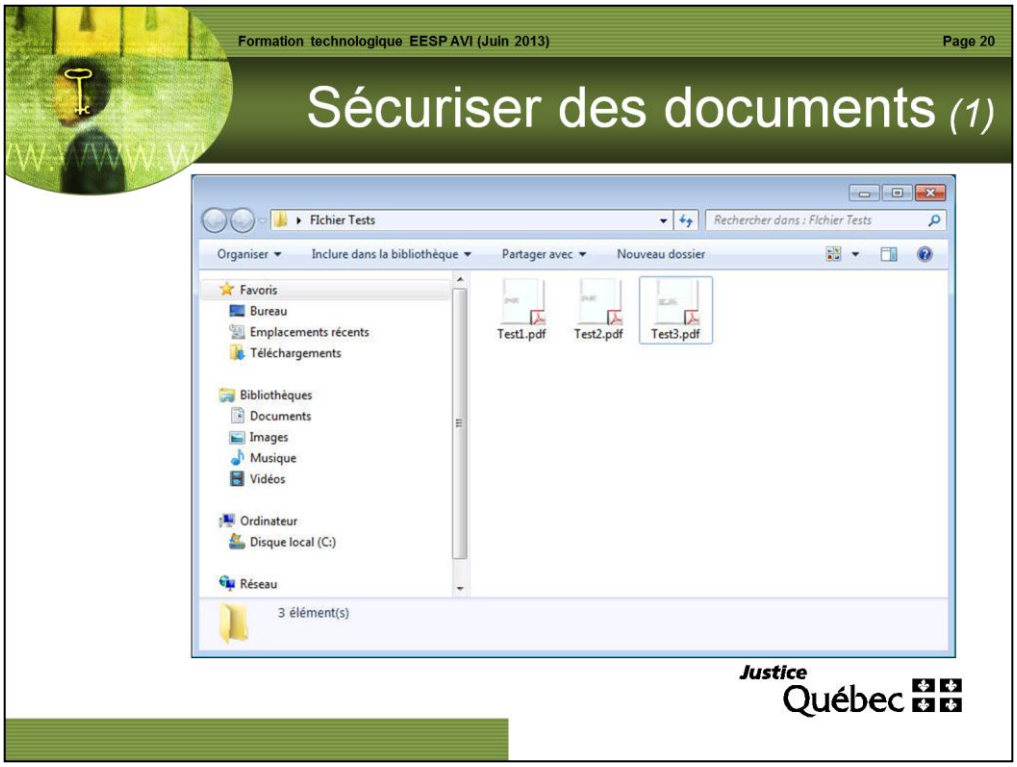
Options d'Entrust

- États de la session Entrust

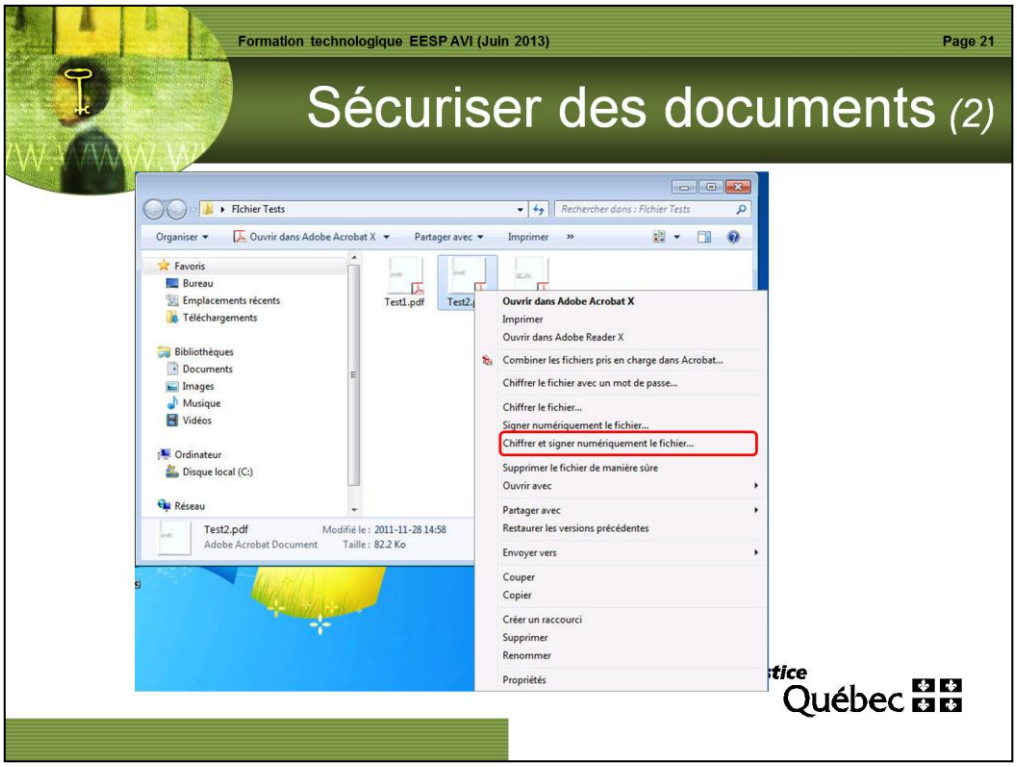
Session active – Connectée

Session fermée – Déconnectée

Justice Québec

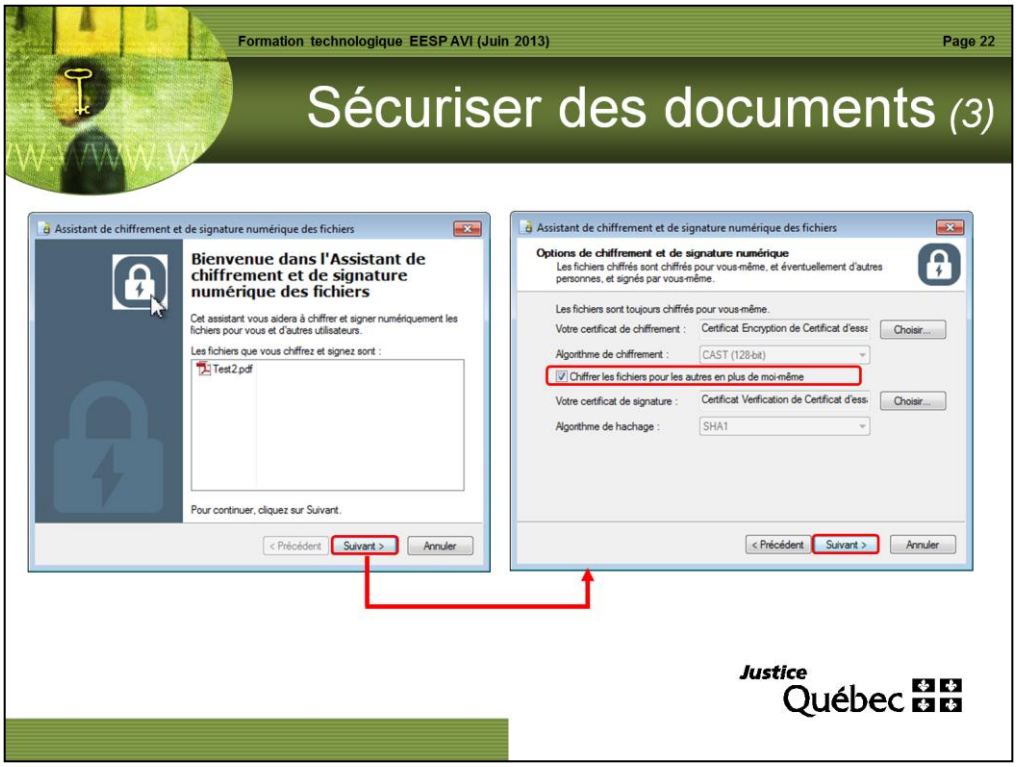


- Lorsque l'on signe et chiffre un fichier, le fichier résultant du traitement apparaît sous la forme d'une icône de document accompagné d'un cadenas
- Le fichier peut être chiffré seulement pour nous ou inclure également une liste de destinataire.
- Si la session est fermée, *Entrust* exigera l'ouverture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



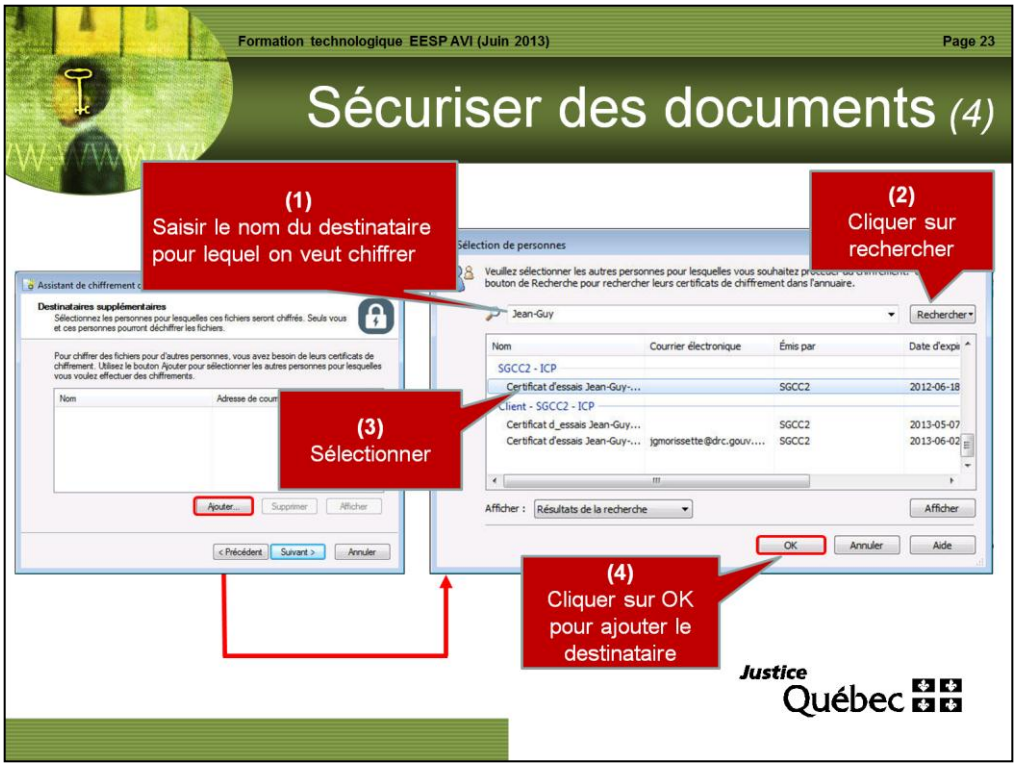
- Quand on sécurise un fichier pour un destinataire, on sécurise également le fichier pour soi-même.

- 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 ».



- 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 ».



- Cliquer sur le bouton « Ajouter »;

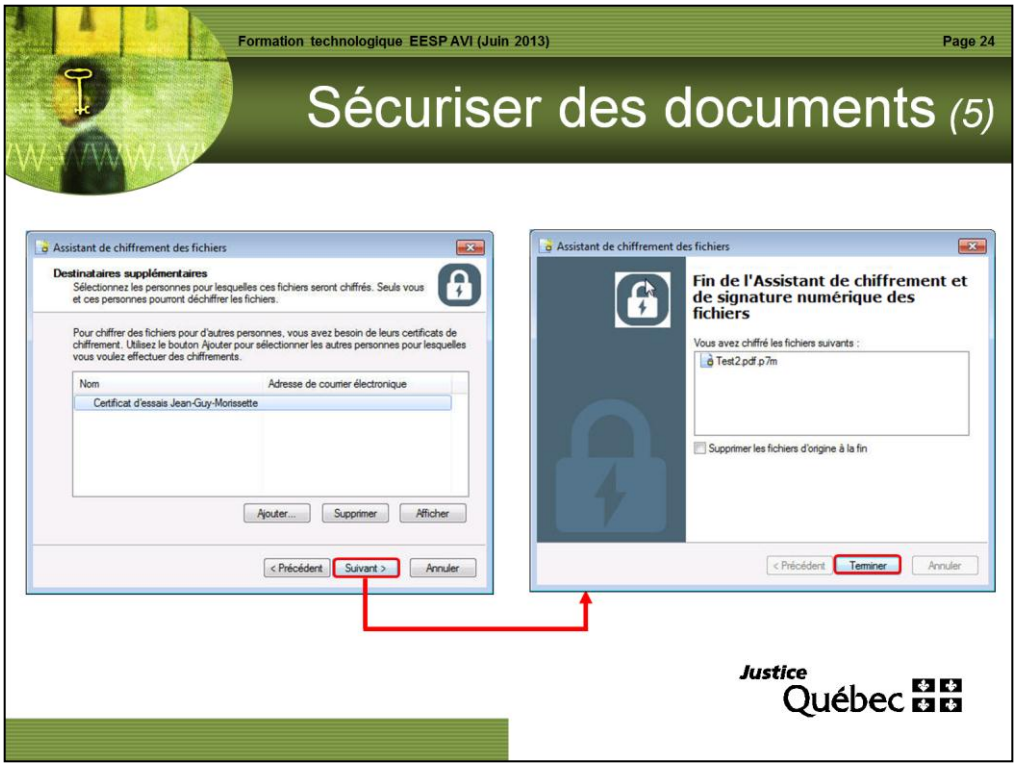
- Spécifier les critères de recherche ex. pour le Service de certification « *(GCC)* et cliquer sur le bouton « Rechercher ».

- 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.

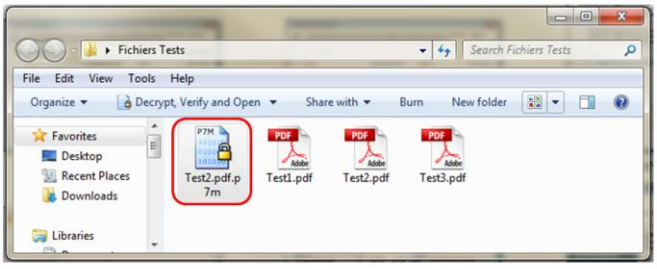
- Si la recherche est sans résultats et le nom recherché contient des accents, réessayer avec le même nom mais sans accent.

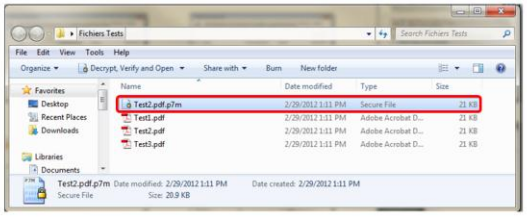


- Répéter la même procédure que précédemment montré pour ajouter d'autres destinataires à la liste
- Lorsque la section « Supprimer les fichiers d'origine à la fin » est cochée le fichier original non sécurisé sera automatiquement supprimé.

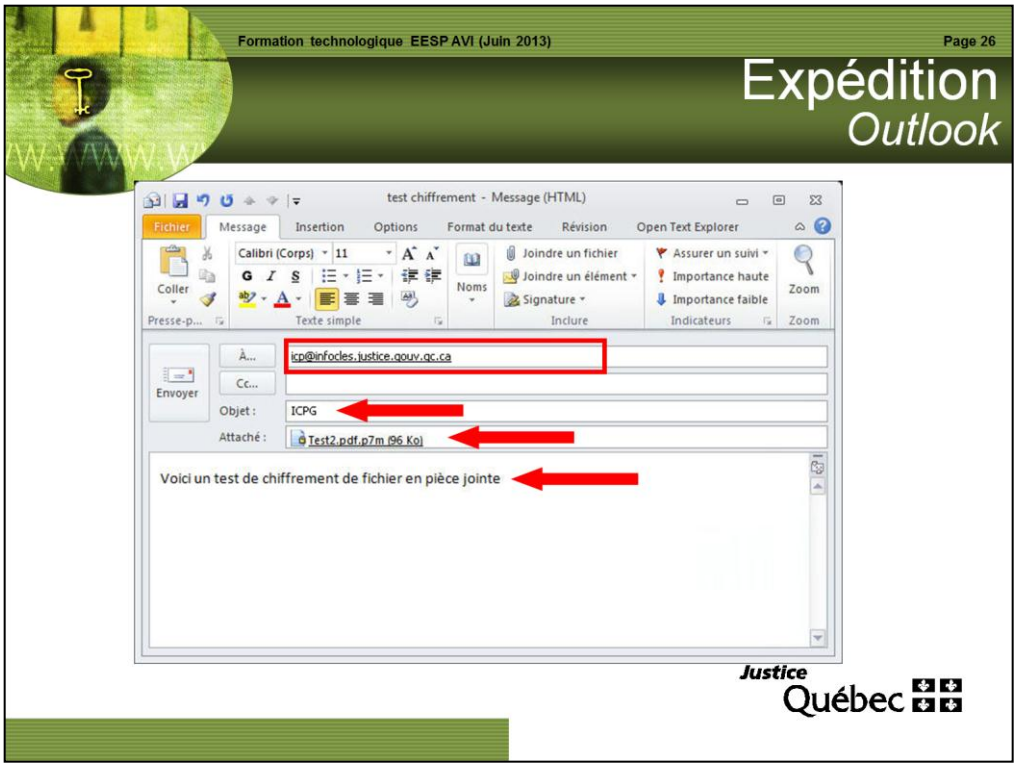
Sécuriser des documents *(6)*

- Différentes vues des documents sécurisés





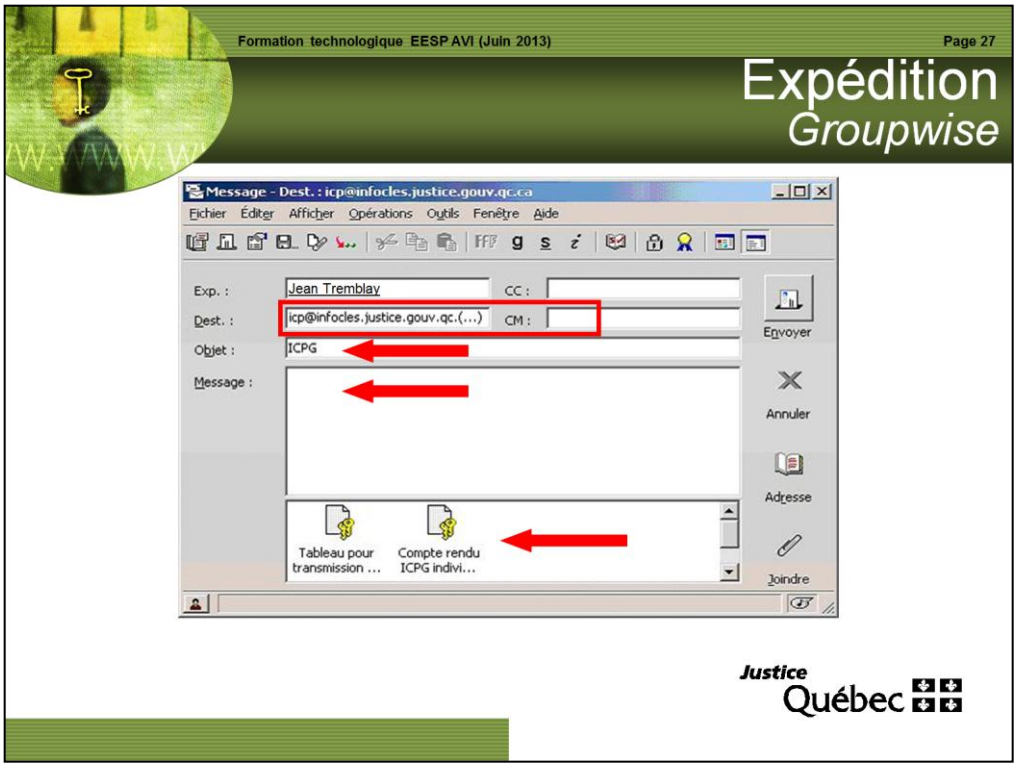
Justice Québec



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» :

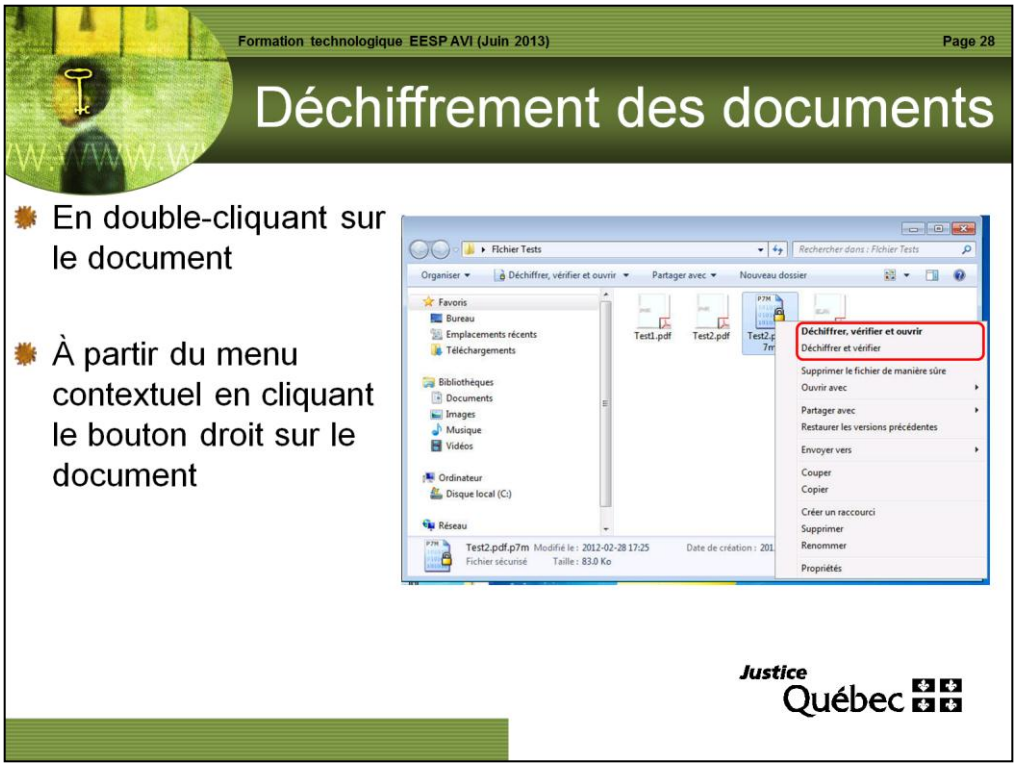
L'adresse est : icp@infocles.justice.gouv.qc.ca;

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.

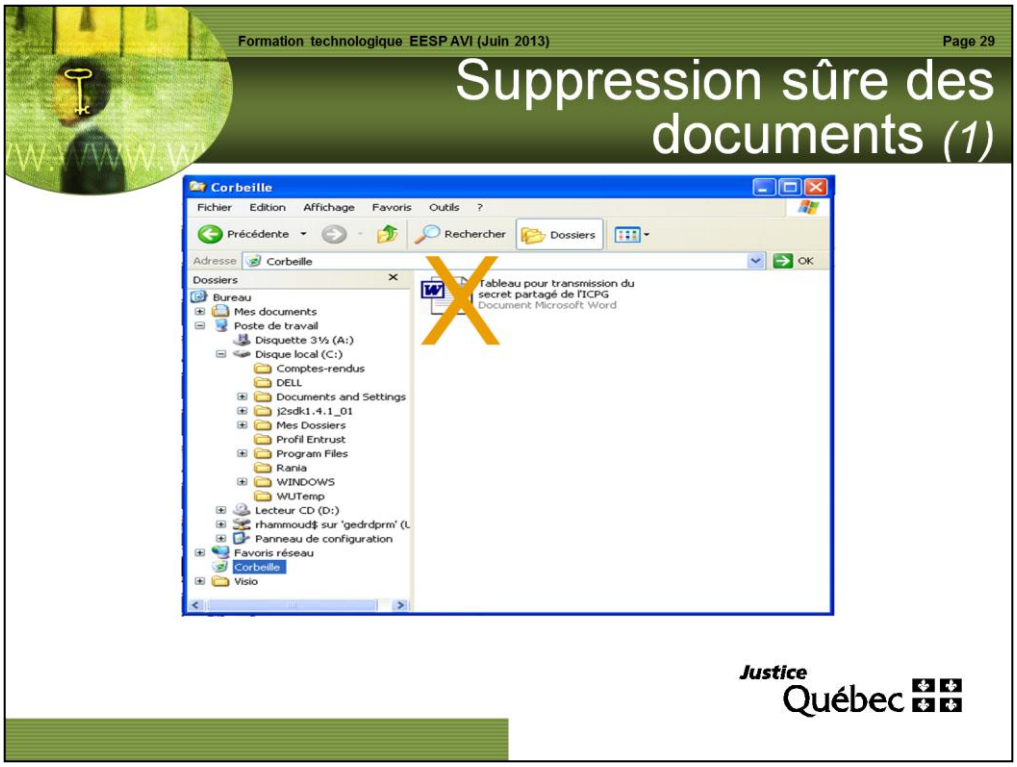
S'assurer que les fichiers soient signés et chiffrés avant de les joindre!



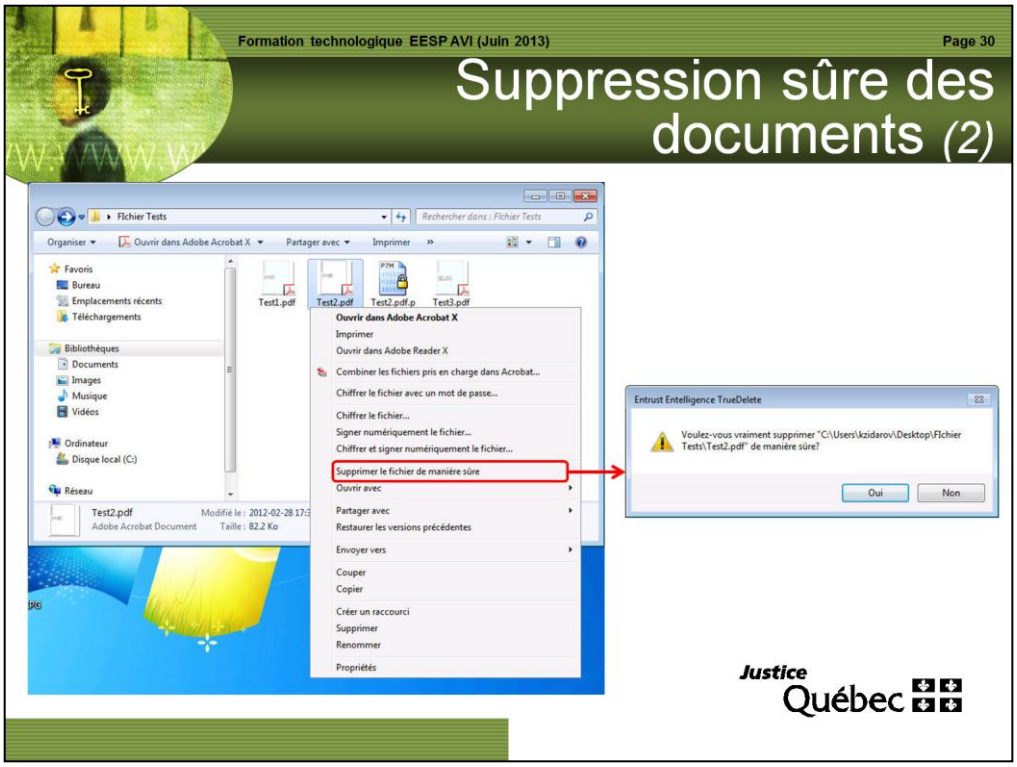
- Déchiffrer, vérifier et ouvrir : déchiffre le document, valide le certificat, et ouvre le document dans son application d'origine (ex. Word).

- 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.

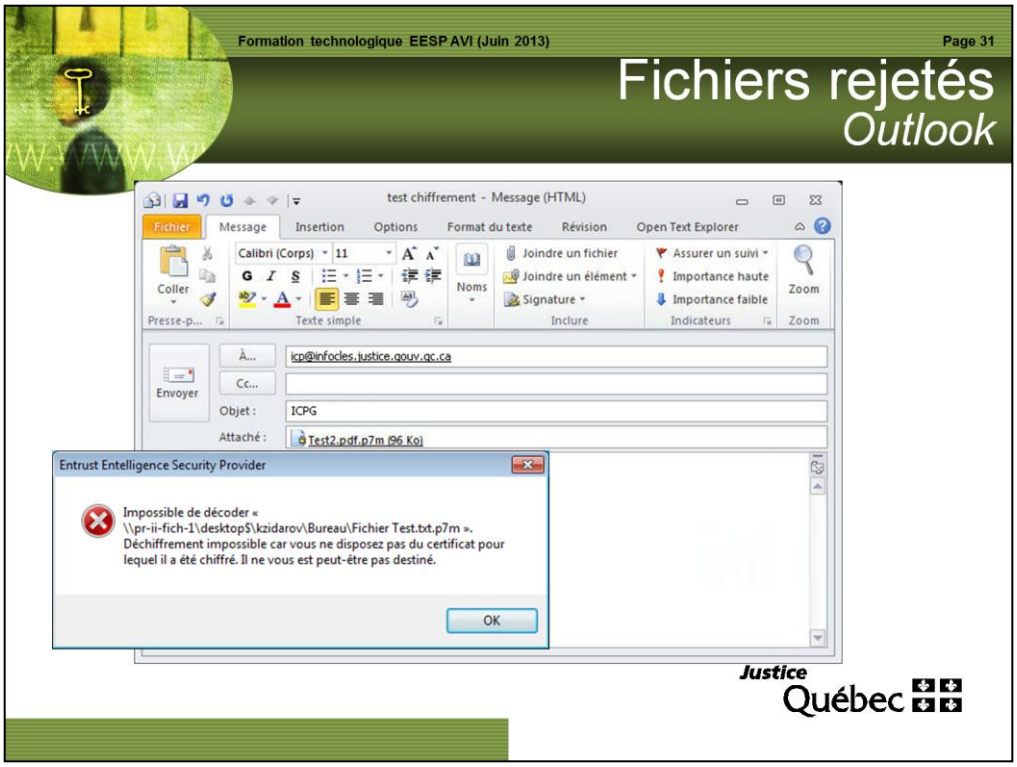


- La « Suppression » régulière rend les renseignements confidentiels vulnérables et accessibles à une personne malveillante.

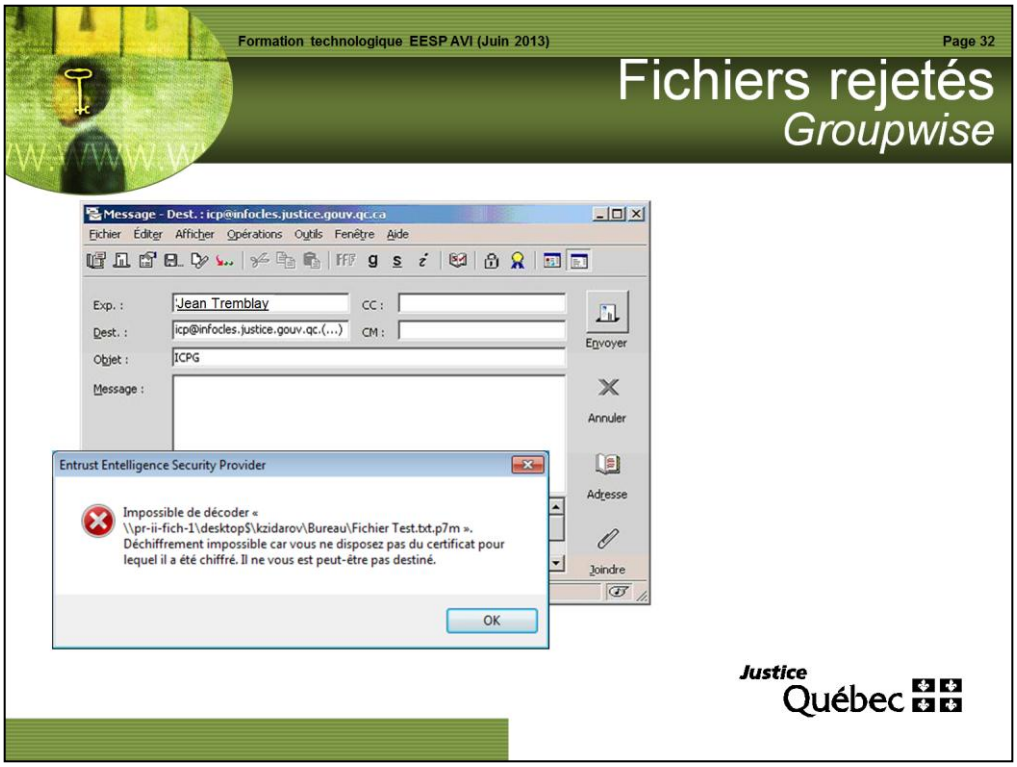


- L'option « Supprimer le fichier de manière sûre » permet de chiffrer un fichier avant de le supprimer (mettre dans la corbeille).

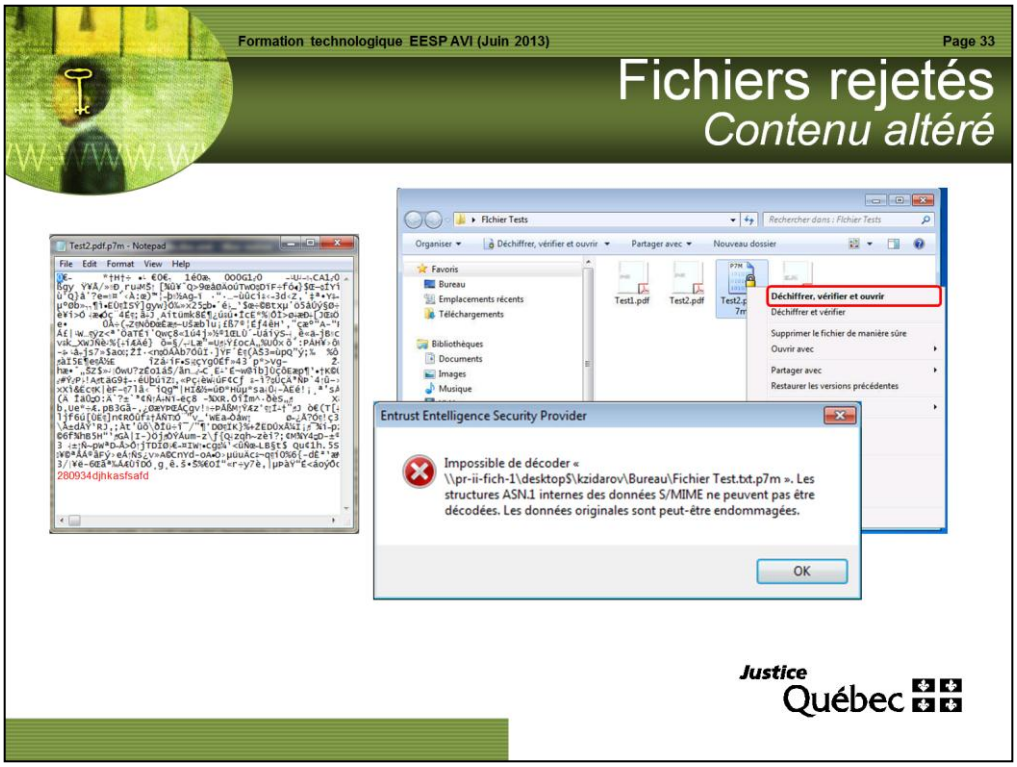
- De cette façon, nous sommes assurés que, même si une personne malveillante tente de récupérer le document supprimé, il lui sera impossible de le déchiffrer.



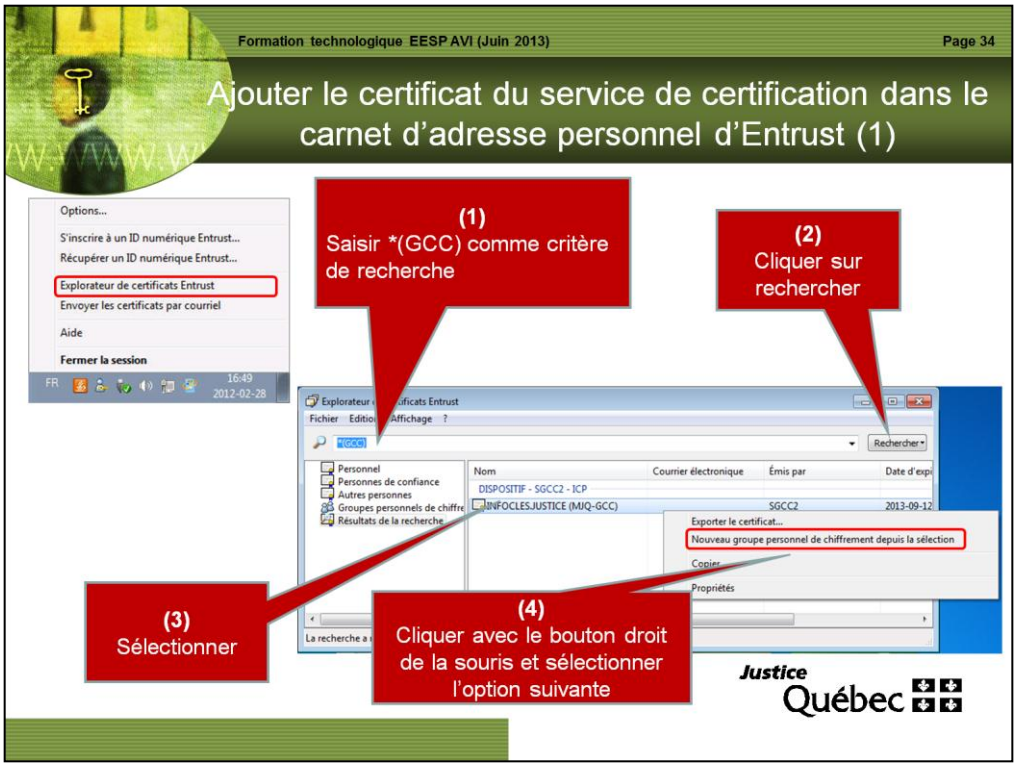
Lorsqu'on tente d'ouvrir un fichier qui ne nous a pas été destiné, le document est rejeté.



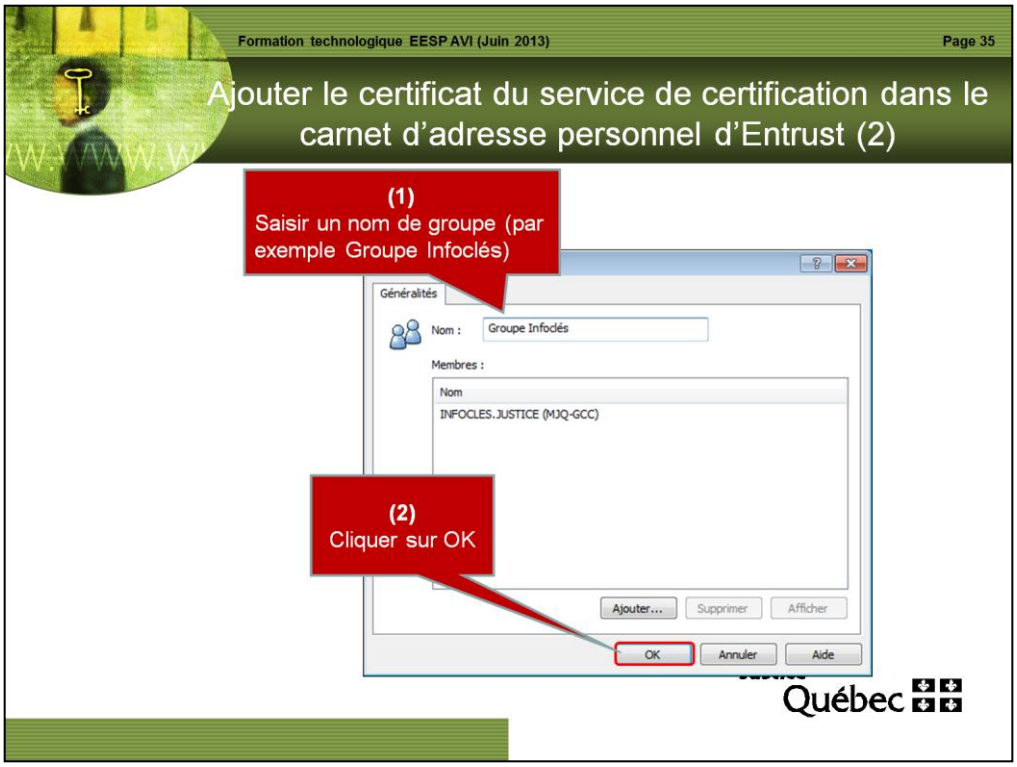
Un document est rejeté s'il a été chiffré pour le mauvais destinataire.



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



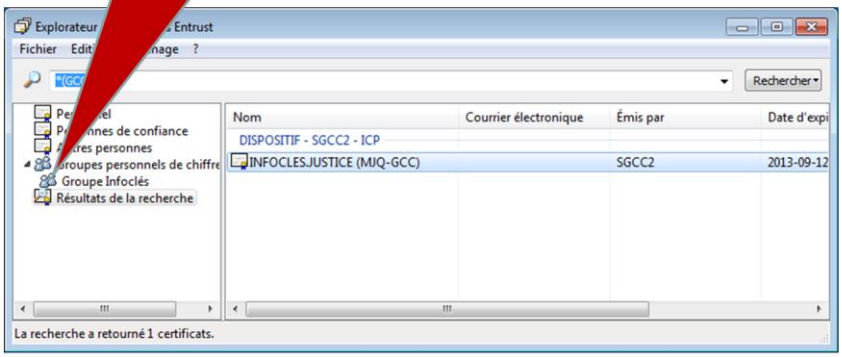
Cette fonctionnalité est utile si vous signez souvent pour les mêmes personnes. Cela vous évite de faire des recherches manuelles à chaque fois que vous voulez signer/chiffrer pour un groupe de personnes spécifique.



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)

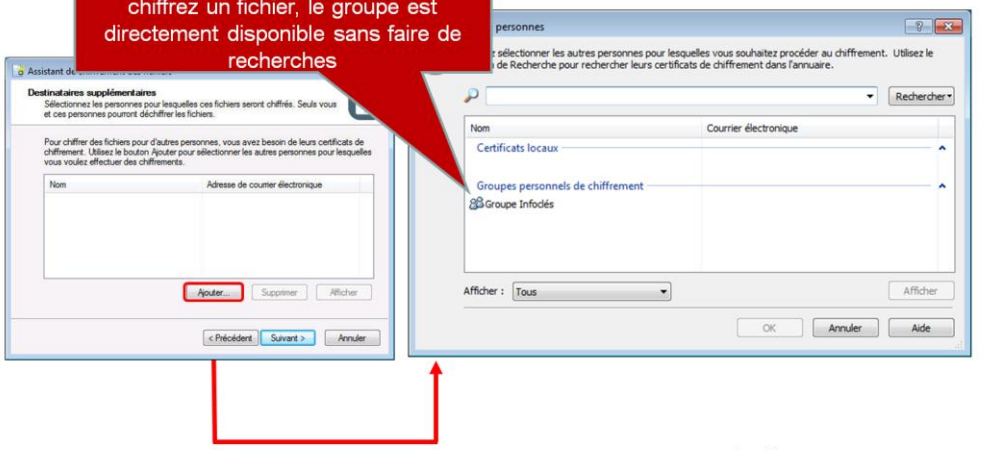
Le groupe infoclés est maintenant créé et il contient le certificat du MJQ-GCC



Justice Québec

Ajouter le certificat du service de certification dans le carnet d'adresse personnel d'Entrust (4)

La prochaine fois que vous signez-chiffrez un fichier, le groupe est directement disponible sans faire de recherches



Justice Québec

Questions

Justice Québec