Prévention de la perte de données dans Entrust

## Pourquoi utiliser le chiffrement?

Avez-vous besoin d’envoyer des documents ou des courriels « Protégé B » à un collègue ou à un client qui figure dans la liste du carnet d’adresses Outlook de EDSC? Il est essentiel à tout le moins de protéger ces documents au moyen d’un mot de passe, mais le chiffrement est aussi fortement recommandé.

Avez-vous besoin de sécuriser des renseignements de nature délicate à des fins de protection personnelle? L’utilisation d’Entrust est une façon simple et très efficace de protéger des fichiers.

Le but du chiffrement d’un fichier ou d’un courriel est de s’assurer qu’il ne peut être consulté par personne d’autre que le destinataire. On peut aussi utiliser Entrust pour signer un fichier numériquement, ce qui constitue une preuve de sécurité supplémentaire pour le destinataire sachant que le message a été créé par un expéditeur de confiance.

**NOTA : Entrust est utilisé pour envoyer des fichiers et des courriels chiffrés à l’intérieur des ministères du gouvernement du Canada (GC) et entre eux. Le destinataire du document chiffré doit figurer dans la liste du carnet d’adresses Outlook du GC de l’expéditeur. Des renseignements concernant la façon de sécuriser des documents en vue de leur diffusion externe sont en cours d’élaboration.**

## Qu’est‑ce que maCLÉ?

maCLÉ est la nouvelle norme du gouvernement du Canada en ce qui touche le chiffrement et le déchiffrement des fichiers et des courriels, de même que l’accès aux renseignements sur votre paye par l’intermédiaire du site des applications Web de la rémunération.

Si vous n’êtes pas encore inscrit sur maCLÉ, consultez les deux sites suivants pour obtenir des renseignements supplémentaires :

* Applications Web de la rémunération : <http://www.tpsgc-pwgsc.gc.ca/remuneration-compensation/txt/index-fra.html>
* maCLÉ : [https://eajl-orca.securise-secure.gc.ca/O/vw/bienvenue-welcome-fra.pub](https://srv532.services.gc.ca/m49/exchweb/bin/redir.asp?URL=https://eajl-orca.securise-secure.gc.ca/O/vw/bienvenue-welcome-fra.pub" \t "_blank)

**IMPORTANT : S’assurer de sauvegarder les fichiers maCLÉ sur le lecteur F:.**

***Ouvrir une session dans maCLÉ :***

1. Dans le coin inférieur droit de l’écran, dans la barre des tâches, cliquer avec le bouton droit de la souris sur l’icône « ESP » () et choisir « Log In ».
2. Cliquer sur « Browse ».
3. Accéder à l’emplacement du lecteur F: et sélectionner le dossier « maCLÉ‑myKEY ».
4. Cliquer sur le seul fichier dans le dossier (nomdelutilisateur.epf).
5. Cliquer sur « Open ». Le champ du nom se remplira automatiquement dans la boîte Entelligence Security Provider d’Entrust.
6. Saisir le mot de passe maCLÉ (le même que celui utilisé pour accéder aux applications Web de la rémunération, c’est-à-dire pour les talons de chèques de paye) et cliquer sur « OK » pour terminer le processus d’authentification.

Il est maintenant possible de chiffrer ou de déchiffrer un fichier ou de signer un fichier par voie numérique.

## Chiffrement ou signature numérique d’un fichier :

1. Une fois que la session est ouverte dans Entrust, accéder au dossier contenant le fichier à chiffrer.
2. Cliquer avec le bouton droit de la souris sur le fichier à chiffrer ou signer. Sélectionner l’option applicable :
	1. « Encrypt File »
	2. « Digitally Sign File »
	3. « Encrypt and Digitally Sign File ».
3. L’assistant d’Entelligence Security Provider d’Entrust lancera le processus de chiffrement et guidera l’utilisateur durant le processus de chiffrement.

***Chiffrement ou signature numérique d’un courriel dans Outlook :***



**Chiffrer un courriel**

1. Une fois que la session est ouverte dans Entrust, lancer Outlook.
2. Créer un nouveau message courriel à chiffrer.
3. Dans la barre des tâches du courriel, cliquer sur le bouton « Encrypt ».
4. Sélectionner les destinataires.

**IMPORTANT : Ne pas oublier que les destinataires doivent avoir un certificat Entrust valide pour pouvoir ouvrir et déchiffrer le fichier ainsi qu’être considéré comme un utilisateur en règle d’ICP Entrust sans quoi une erreur s’affichera lors de la tentative d’envoi du courriel.**

1. Cliquer sur « Send ». Le courriel est maintenant chiffré et envoyé aux destinataires.

## Signer un courriel par voie numérique

1. Une fois que la session est ouverte dans Entrust, lancer Outlook.
2. Créer un nouveau message courriel à chiffrer.
3. Dans la barre des tâches du courriel, cliquer sur le bouton « Sign ».
4. Sélectionner les destinataires.
5. Cliquer sur « Send ». Le courriel est maintenant signé par voie numérique et envoyé aux destinataires.
6. Lorsque le destinataire reçoit le courriel, il sera invité à ouvrir une session dans Entrust et recevra une confirmation que le courriel a été signé par voie numérique par l’expéditeur.

**NOTA : Pour chiffrer et signer par voie numérique un courriel, cliquer sur les boutons « Encrypt » et « Sign » dans la barre de tâches du courriel avant de l’envoyer aux destinataires.**

***Déchiffrer les fichiers et les courriels :***

Afin de déchiffrer un fichier, il faut faire partie des destinataires durant le processus de chiffrement. Une invite à ouvrir une session dans Entrust s’affichera lors de la tentative d’ouverture du fichier chiffré.

Pour déchiffrer un fichier chiffré initialement par l’utilisateur, ouvrir une session dans Entrust, cliquer avec le bouton droit de la souris sur le fichier, sélectionner « Decrypt, Verify and Open » pour ouvrir immédiatement le fichier ou sélectionner « Decrypt and Verify » pour déchiffrer le fichier sans l’ouvrir.

Pour ouvrir un courriel chiffré, il faut avoir un certificat maCLÉ valide et figurer dans la liste de distribution au moment du chiffrement. Une invite à ouvrir une session dans Entrust s’affichera lors de la tentative d’ouverture du courriel chiffré.

Les employés dont les courriels ou les documents sont chiffrés à l’aide de l’ancien certificat d’ICP de RHDCC **doivent** les déchiffrer puis les chiffrer à nouveau à l’aide de maCLÉ. Une fois que l’ancien certificat d’ICP d’Entrust est complètement mis hors service, les employés ne pourront pas accéder aux fichiers plus anciens qui sont toujours chiffrés à l’aide de l’ICP. Tous les documents ou les courriels pertinents doivent faire l’objet du processus de déchiffrement et de rechiffrement afin de veiller à ce que l’information ne soit pas perdue. Pour toute question ou pour obtenir de l’aide, consulter la section [Besoin d’aide supplémentaire?](#_Require_Further_Assistance?) ci‑dessous.

## Récupération de maCLÉ :

Dans l’un cas des suivants :

* Oubli du mot de passe
* Certificat expiré
* Fichiers maCLÉ perdus ou égarés

Puis cliquer [ICI](https://eajl-orca.securise-secure.gc.ca/O/vw/bienvenue-welcome-fra.pub) pour obtenir de l’aide pour récupérer votre certificat d’ICP maCLÉ.

## Foire aux questions sur maCLÉ :

<http://www.tpsgc-pwgsc.gc.ca/gji-icm/300/63_72_fra.html>

## Besoin d’aide supplémentaire?

Pour obtenir des renseignements détaillés sur le chiffrement, le déchiffrement et la signature numérique, rendez-vous à l’un des sites suivants :

* Site en anglais : [http://rhdcc-hrsdc.prv/eng/iit/csa/ats/itss/iss/identification\_ authentication.shtml](http://rhdcc-hrsdc.prv/eng/iit/csa/ats/itss/iss/identification_authentication.shtml)
* Guide en anglais : [http://rhdcc-hrsdc.prv/eng/iit/csa/ats/itss/iss/documents/user\_guide\_ entrust\_entelligence\_security\_provider\_9\_1\_v2\_e.doc](http://rhdcc-hrsdc.prv/eng/iit/csa/ats/itss/iss/documents/user_guide_entrust_%20entelligence_security_provider_9_1_v2_e.doc)
* Site en français : <http://rhdcc.prv/fra/iit/dpsa/ast/ssti/ssi/identification_authentication.shtml>
* Guide en français : [http://rhdcc.prv/fra/iit/dpsa/ast/ssti/iss/documents/user\_guide\_entrust\_ entelligence\_security\_provider\_9\_1\_v2\_f.doc](http://rhdcc.prv/fra/iit/dpsa/ast/ssti/iss/documents/user_guide_entrust_%20entelligence_security_provider_9_1_v2_f.doc)