Dataloss Prevention by using Entrust to Encrypt Information

## Why use Encryption?

Do you need to send Protected B documents or e-mails to a colleague or client listed in your ESDC Outlook address book? It is essential that, at a minimum, you password protect these documents but encryption is also highly recommended.

Do you want to secure sensitive information for your own safekeeping? Then using Entrust is a simple and very effective way to protect your files.

The purpose of encrypting a file or e-mail is to ensure that it cannot be viewed by anyone other than the intended recipient(s). You can also use Entrust to digitally sign a file which gives the recipient added security in knowing that message was created by a trusted sender.

**NOTE: Entrust is to be used to send encrypted files/emails internally and between other Government of Canada (GoC) departments. The recipient of the encrypted material must be listed in your GoC Outlook address book. Information regarding how to secure documents for external sharing is currently under development.**

## What is MyKey?

MyKey is the new GoC standard for the purposes of encrypting files, decrypting files, e-mails, and for accessing your pay information via the Compensation Web Access (CWA) website.

If have not yet registered for MyKey, please visit the following 2 locations for further information:

* CWA: <http://www.tpsgc-pwgsc.gc.ca/remuneration-compensation/txt/index-eng.html>
* MyKey: <https://eajl-orca.securise-secure.gc.ca/O/vw/bienvenue-welcome-eng.pub>

**IMPORTANT: Ensure you save your MyKey files to your F: drive.**

## Logging in to MyKey:

1. On the bottom right of your screen, in the taskbar, right click on the ESP tray icon () and choose Log In.
2. Click “Browse”.
3. Navigate to your F: drive location and select the “maCLÉ-myKEY” folder.
4. Click the only file in the folder (username.epf).
5. Click “Open” – this will fill the name field in the Entrust Entelligence Security Provider box.
6. Enter your MyKEY password (the same as you use to access Compensation Web Applications i.e. your paystub) and click “OK” to complete the authentication process.

You are now ready to encrypt or decrypt a file or, digitally sign a file.

## Encrypting and/or Digitally Signing a File:

1. Once you have successfully logged in to Entrust, browse to the folder containing the file you want to encrypt.
2. Right Click on the file you want to encrypt/sign. Select the option you require:
	1. Encrypt File
	2. Digitally Sign File
	3. Encrypt and Digitally Sign File.
3. The Entrust Entelligence Security Provider Wizard will launch and will guide you to the completion of the encryption process.

## Encrypting and/or Digitally Signing E-mails in Outlook:



### Encrypting E-mails

1. Once you have successfully logged in to Entrust, launch Outlook.
2. Create a new e-mail message you wish to encrypt.
3. In the E-mail toolbar, click the Encrypt button.
4. Select your recipients

**IMPORTANT: Remember that the recipients(s) must have their own valid Entrust Certificate to be able to open and decrypt the file and, be a valid Entrust PKI user or an error will occur when you attempt to send the e-mail.**

1. Click Send. Your e-mail has now been encrypted and sent to your targeted reader(s).

### Digitally Signing E-mails

1. Once you have successfully logged in to Entrust, launch Outlook.
2. Create a new e-mail message you wish to encrypt.
3. In the e-mail toolbar, click the Sign button.
4. Select your recipients.
5. Click Send. Your e-mail has now been digitally signed and sent to your targeted reader(s).
6. When the recipient receives the e-mail, they will be prompted to log in to Entrust and will receive confirmation that the e-mail was digitally signed by you, the sender.

**NOTE: To both encrypt and digitally sign an e-mail, click both the Encrypt and Sign Buttons on the e-mail toolbar before sending to your targeted recipients.**

## Decrypting Files and E-mails:

In order to decrypt a file, you must have been included as part of the audience during the encryption process. You will be prompted to login to Entrust when you attempt to open an encrypted file.

To decrypt a file that was originally encrypted by you, login to Entrust, right click on the file, select Decrypt, Verify and Open if you want to open it immediately or select Decrypt and Verify if you want to decrypt it without opening it.

To open an encrypted e-mail, you must have a valid MyKey certificate and have been included in the distribution list at the time of encryption. You will be prompted to log into Entrust when you attempt to open the encrypted e-mail.

Employees who have emails or documents encrypted with the old HRSDC PKI certificate **must** de-encrypt them and then re-encrypt them using MyKey. Once the older Entrust PKI is fully decommissioned, employees will not be able to access older files that are still encrypted using PKI. Any relevant documents or emails need to go through the decryption/re-encryption process to ensure that information is not lost. For questions or assistance, please see the [Require Further Assistance](#_Require_Further_Assistance?) section below.

## MyKey Recovery:

Should you:

* Forget Your Password
* Have an expired Certificate
* Lose or misplace your MyKey files

Then click [HERE](https://eajl-orca.securise-secure.gc.ca/O/vw/bienvenue-welcome-eng.pub) for assistance in recovering your MyKey PKI certificate.

## MyKey FAQ:

[http://www.tpsgc-pwgsc.gc.ca/gji-icm/300/63\_72\_eng.html#101124](http://www.tpsgc-pwgsc.gc.ca/gji-icm/300/63_72_eng.html%22%20%5Cl%20%22101124)

## Require Further Assistance?

For detailed information on Encrypting, Decrypting and Digitally Signing, please visit the following sites/URLs:

* English Site: [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)
* English Guide: [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)
* French Site: <http://rhdcc.prv/fra/iit/dpsa/ast/ssti/ssi/identification_authentication.shtml>
* French Guide: [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)