Obligations d'épargne du Canada

Canada Savings Bonds

Guide d'utilisation du serveur FTPS

Version 2.2

Le 19 avril 2013

Guide d'utilisation du serveur FTPS – Historique des mises à jour

Utiliser le tableau ci-dessous pour effectuer le suivi des mises à jour du présent document. Y inscrire la date, la phase et les coordonnées de la personne-ressource pouvant répondre aux questions sur le contenu, le cas échéant.

Date de MAJ	Phase	Motif	Version
9 mai 2007		Ébauche	1.0
24 mai 2007		Deuxième ébauche	1.1
11 septembre 2007		Révision finale	1.2
22 octobre 2007		Ajout des coordonnées des Services de soutien, modification d'un nom de fichier et du titre du document, et intégration d'une préface pour résumer les détails à fournir au moment de la mise en œuvre	1.3
31 janvier 2008		Remplacement des instantanés d'écran temporaires	1.4
19 février 2008		Ajout d'une note sur la configuration du pare-feu des organisations	1.5
18 mars 2008		Changement des règles de désignation des fichiers de données (section 5.1.3) afin de prendre en charge un numéro d'ordre alphanumérique de n'importe quelle longueur	1.6
24 mars 2008		Changement du mode de transfert recommandé	1.7
15 avril 2008		Ajout d'une étape de confirmation de fichier visant les agents administratifs (section 3.3), et suppression des références à FundServ	1.8
21 mai 2008		Ajout du support pour le mode explicite	1.9
6 juillet 2009		Mise à jour de la section 5.1.3 Désignation d'un fichier de données afin d'expliquer séparément les exigences concernant l'attribution des numéros d'ordre aux fichiers de retenues sur salaire et aux fichiers de souscriptions, car elles ne sont pas les mêmes. Mise à jour des liens vers les documents dans le site Web des OEC.	2

Date de MAJ	Phase	Motif	Version
11 mai 2010		Remplacement de l'adresse électronique rpac-pft@eds.com par rpac-pft@oec.gc.ca, suppression de la mention de la période de campagne et remplacement d'EDS par HP.	2.1
19 avril 2013		Changé le traitement des informations de contact de l'agent à la page de préface.	2.2

TABLE DES MATIÈRES

MARQUES DE COMMERCE

Il est possible que les noms de produits mentionnés dans le présent guide soient des marques de commerce ou des marques déposées de leurs entreprises respectives; elles sont reconnues comme telles.

LISTE DES SIGLES

API	*Application Programmer Interface* – interface de programmation d'applications ou interface de programmation
ASCII	*American Standard Code for Information Interchange* – code américain normalisé pour l'échange d'information ou code ASCII
COM	*Component Object Model*
EMC	*EMC Corporation*
FTP	*File* Transfer *Protocol* – protocole de transfert de fichiers ou protocole FTP
FTPS	Protocole FTPS (FTP sécurisé)
GUI	*Graphical User Interface* – interface utilisateur graphique ou interface graphique
HP	Hewlett Packard
JRE	*Java Runtime Environment*
MFC	*Microsoft Foundation Class* (bibliothèque de programmes)
OS	*Operating System* – système d'exploitation
SDK	Software Development Kit – trousse de développement logiciel
SSL	*Secure Socket Layer* – protocole SSL ou protocole sécurisé de cryptage

PRÉFACE

Le présent document décrit la mise en œuvre du serveur FTP sécurisé (FTPS) de la Banque du Canada.

COORDONNÉES DES SERVICES DE SOUTIEN

Les organisations qui transmettent des **fichiers de retenues sur salaire** sont priées de communiquer avec le Service de soutien suivant :

- Service aux employeurs, 1 888 467-5999, ouvert du lundi au vendredi, de 8 h à 18 h, heure de l'Est.

Les agents administratifs qui transmettent des **fichiers de souscription** d'Obligations d'épargne du Canada sont priées de communiquer avec le Service de soutien dont le numéro suit :

- S'il vous plait appelez 1 888 646-2626, ouvert du lundi au vendredi, de 8 h à 20 h, heure de l'Est.

1. INTRODUCTION

1.1. Objet

Le présent guide est destiné aux organisations utilisant un serveur FTPS pour le téléversement de fichiers de données (tels que fichiers de souscriptions et de retenues sur salaire). Il vise un public possédant des connaissances techniques relativement poussées, notamment en ce qui a trait au protocole FTP et aux fichiers à téléverser (voir les références à la section 1.5. Documents de référence).

1.2. Portée du guide

Le guide procure les renseignements techniques nécessaires à l'utilisation du serveur FTPS. Il n'a pas pour but de présenter les processus opérationnels liés au serveur FTPS, mais de compléter, et non de remplacer, les spécifications de fichier évoquées à la section 1.5. Documents de référence.

1.3. Contexte

Le serveur FTPS permet le téléversement de deux types de fichiers de données, soit :

- Fichiers transférés par des agents administratifs et renfermant le détail des souscriptions d'obligations du grand public. Ces fichiers de souscriptions sont transmis chaque année, au cours de la campagne de souscription des Obligations d'épargne du Canada.

- Fichiers transférés par les employeurs et renfermant le détail des retenues sur salaire visant les souscriptions de titres sans certificat. Les fichiers de retenues sur salaire sont transférés à intervalles réguliers, par exemple chaque semaine ou chaque deux semaines, conformément au cycle de paye de l'employeur. Dans un cas comme dans l'autre, les données sont désignées « Protégé B »[1] et, par conséquent, la sécurité du transfert et du traitement nécessite la prise de mesures particulières.

[1] La catégorie Protégé B (nature particulièrement délicate) s'applique dans la fonction publique aux renseignements pour lesquels toute atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice grave à des intérêts autres que l'intérêt national; cette catégorie s'applique souvent à des renseignements dont la divulgation risquerait de constituer une atteinte au respect de la vie privée ou à la réputation ou encore de faire perdre un avantage concurrentiel.

1.4. Structure du guide

Section 1 Introduction. Cette section décrit l'objet, la portée et la structure du guide. Elle indique également le titre des documents de référence cités dans le guide.

Section 2 Aperçu. Cette section présente une vue d'ensemble de l'architecture de réseau et des caractéristiques de sécurité du serveur FTPS.

Section 3 Utilisation d'une interface graphique client pour FTPS. Cette section explique la marche à suivre pour utiliser le serveur FTPS au moyen d'un logiciel client GUI.

Section 4 Utilisation d'une interface de programmation client pour FTPS. Cette section explique la marche à suivre pour utiliser le serveur FTPS au moyen d'un logiciel client personnalisé.

Section 5 Exigences relatives aux fichiers à téléverser. Cette section décrit les caractéristiques que doivent posséder les fichiers à téléverser par le biais du serveur FTPS et cite les documents de référence pertinents.

1.5. Documents de référence

Les documents suivants sont cités en référence dans le présent guide ou ont été consultés en vue de sa rédaction.

Guide des exigences techniques à l'intention des utilisateurs de progiciels de paye privés

http://oec.gc.ca/wp-content/uploads/2009/03/85006_technical_specs_f_v2_x1a.pdf

Système de gestion des titres détenus par les particuliers (SGTP) – *Spécifications relatives au fichier des achats*

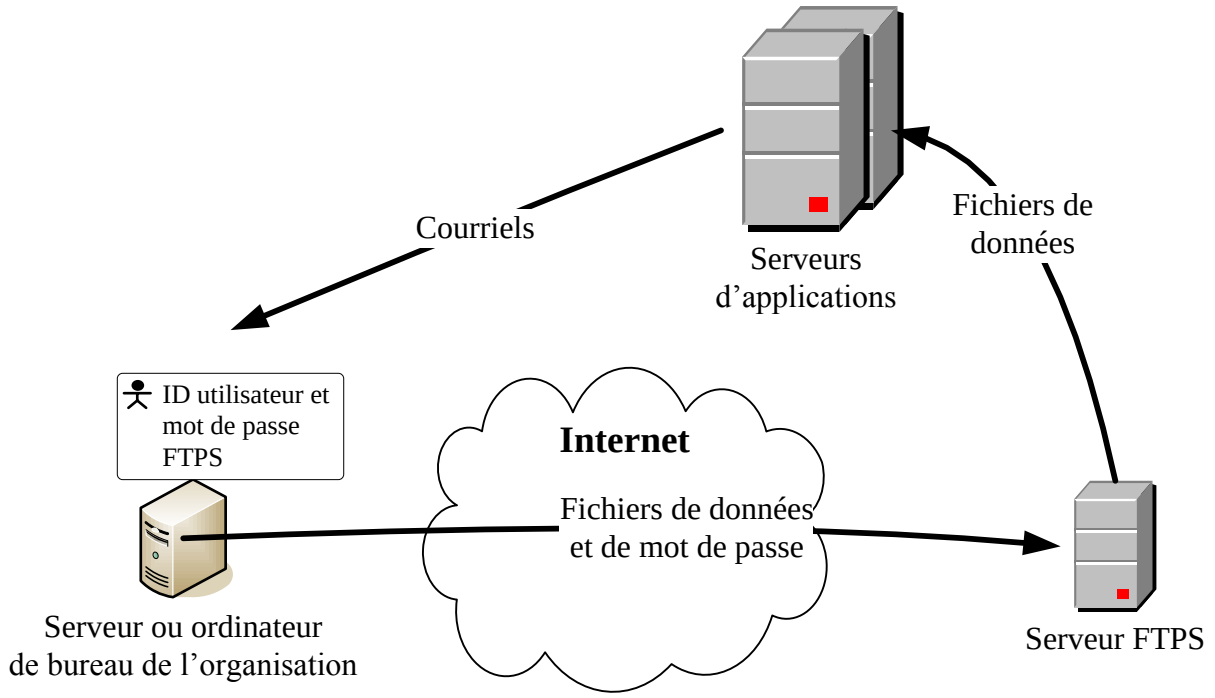
http://oec.gc.ca/financial-institutions-and-investment-dealers-fr/selling-and-processing-s42-fr/?lang=fr

2. APERÇU

Cette section présente une vue d'ensemble de l'architecture de réseau et des caractéristiques de sécurité du serveur FTPS.

2.1. Architecture de réseau

Le diagramme ci-dessous illustre l'architecture de réseau du serveur FTPS. Les organisations participantes utilisent le réseau public Internet pour établir une connexion au serveur FTPS et téléverser les fichiers de données et de mot de passe requis.



Les organisations qui utilisent un pare-feu limitant les connexions sortantes doivent le configurer pour autoriser les connexions vers l'adresse IP 204.104.133.46 (csb-oec.bpmca.com) depuis les ports 990 et 23001 à 23100 au cas où ils utilisent le mode « implicite », ou les ports 21021 et 23001 à 23100 au cas où ils utilisent le mode « explicite ».

2.2. Utilisation du protocole FTPS

Voici la marche à suivre sommaire en vue de l'utilisation du serveur FTPS. Des renseignements plus détaillés figurent dans les sections suivantes.

1. Établir une connexion à Internet.

2. Se connecter au serveur FTPS. Pour cette étape, l'utilisateur a deux options (pour une ou l'autre option, le chiffrement des données doit être activé) :

    a. Mode de sécurisation implicite et type de connexion passif. Cette option doit utiliser le port 990.

    b. Mode de sécurisation explicite et type de connexion passif. Cette option doit utiliser le port 21021.

3. Accéder au serveur FTPS au moyen de l'ID utilisateur assignée à l'organisation et du mot de passe confidentiel de l'organisation.

4. À l'invite, accepter le certificat numérique du serveur FTPS.

5. Sélectionner le mode de transfert ASCII (préférable) ou binaire. Il convient d'essayer le serveur FTPS à l'aide d'un fichier test. Si le mode ASCII ne fonctionne pas (ce qui peut arriver si le fichier contient des caractères spéciaux), utiliser le mode binaire.

6. Répéter l'étape suivante autant de fois que nécessaire :

    a. Téléverser un fichier de données ou de mot de passe (le fichier de mot de passe permet de changer le mot de passe confidentiel de l'organisation).

7. Rompre la connexion au serveur FTPS.

2.3. Sécurité

Les fichiers de données téléversés par le biais du serveur FTPS ne sont pas chiffrés avant le transfert mais ils sont protégés par les mesures de sécurité suivantes :

- Le transfert des fichiers est effectué au moyen d'un protocole FTP sécurisé (avec le protocole SSL) qui assure le chiffrement des fichiers pendant qu'ils sont en circulation dans Internet.

- Chaque organisation est autorisée, et même encouragée, à changer son mot de passe fréquemment, au minimum tous les trois mois.

- Lorsque qu'une organisation change son mot de passe, elle seule le connaît. Le service de dépannage de la Banque du Canada n'y a pas accès.

- Des critères rigoureux relatifs à la composition des mots de passe rendent ces derniers difficiles à déchiffrer. (Pour plus de renseignements sur les critères de sécurité des mots de passe, consulter la section 5.2.1, Contenu d'un fichier de mot de passe.)

- Les utilisateurs du serveur FTPS sont autorisés à téléverser des fichiers mais non à en télécharger, supprimer, afficher ou renommer.

- Le serveur FTPS vérifie le contenu des fichiers de données par rapport à l'ID utilisateur de l'organisation émettrice. Il n'accepte un fichier que si son contenu est conforme aux types de données que l'organisation est autorisée à soumettre. (Pour plus de renseignements, consulter les sections 5.1.1, Contenu d'un fichier de retenues sur salaire et 5.1.2, Contenu d'un fichier de souscriptions.)

3. UTILISATION D'UNE INTERFACE GRAPHIQUE CLIENTE AVEC PROTOCOLE FTPS

Cette section explique la marche à suivre pour utiliser le serveur FTPS au moyen d'un logiciel client GUI.

3.1. Interface graphique recommandée

Le serveur FTPS a fait l'objet d'essais poussés sur Windows XP, au moyen de Secure FTP v2.5.12 de Glub Tech. Ce logiciel est offert pour Windows, Mac OS X et toute plate-forme Unix munie de JRE Java (version 1.4 ou plus récente). On peut l'acheter en ligne auprès de Glub Tech (http://www.glub.com/store/), moyennant 25 $ dollars américains[2].

3.1.1. Installation de l'application Secure FTP de Glub Tech

Se conformer à la marche à suivre ci-dessous pour installer l'application Secure FTP de Glub Tech dans un ordinateur de bureau sous Windows (des instructions similaires s'appliquent aux autres plates-formes) :

- Si l'ordinateur n'est pas muni de JRE Java (version 1.4 ou plus récente), il faut d'abord le télécharger et l'installer. Il suffit d'accéder à la page Web http://java.sun.com/javase/downloads/index_jdk5.jsp à l'aide d'un navigateur tel que Microsoft Explorer et de télécharger *Java Runtime Environment 5.0 Update 12*. (Veuillez noter que ce n'est qu'un exemple : toute version équivalant au moins à la version 1.4 peut être utilisée.)

- Après le téléchargement de JRE, exécuter le fichier téléchargé pour procéder à l'installation (par ex. jre-1_5_0_12-windows-i586-p.exe).

- Se procurer une licence d'utilisation à l'adresse http://www.glub.com/store/ et suivre les instructions du fournisseur.

- Accéder à http://www.glub.com/store/download.jsp?shortname=secureftp_2_5 au moyen d'un navigateur Web et télécharger l'application Secure FTP de Glub Tech.

- Exécuter le fichier téléchargé pour installer l'application Secure FTP de Glub Tech (par ex. secureftp2_5_13_setup.exe).

- Le programme de démarrage de l'application Secure FTP de Glub Tech se trouve à l'emplacement suivant : C:\Program Files\Secure FTP 2.5\ secureftp.bat.

[2] Les prix sont fixés par le fournisseur et ne peuvent être garantis par la Banque du Canada.

3.2. Autres interfaces graphiques clientes FTPS

Les organisations sont libres d'utiliser d'autres logiciels d'interface graphique (GUI) pour FTPS, puisque cette solution se fonde sur des normes bien établies et ne relève pas d'un éditeur de logiciels particulier. Les progiciels ci-dessous sont en principe compatibles, mais n'ont pas été mis à l'essai avec la solution FTPS de la Banque du Canada.

- edtFTPj/PRO (http://www.enterprisedt.com/products/edtftpjssl/overview.html) : interface graphique Java compatible avec toute plate-forme fonctionnant sous Java 1.5.x (ou une version plus récente).

- WS_FTP Professional 2007 (http://www.ipswitch.com/products/ws_ftp/index.asp) : produit compatible avec les plates-formes Windows, dont Windows XP et Windows Vista.

- jMethods JFTP API (http://www.jmethods.com/products/) : interface graphique Java compatible avec toute plate-forme fonctionnant sous Java 1.4.2 (ou une version plus récente).

- FTP Voyager (http://www.ftpvoyager.com/) : produit compatible avec les plates-formes Windows, dont Windows XP et Windows Vista.

3.3. Téléversement d'un fichier

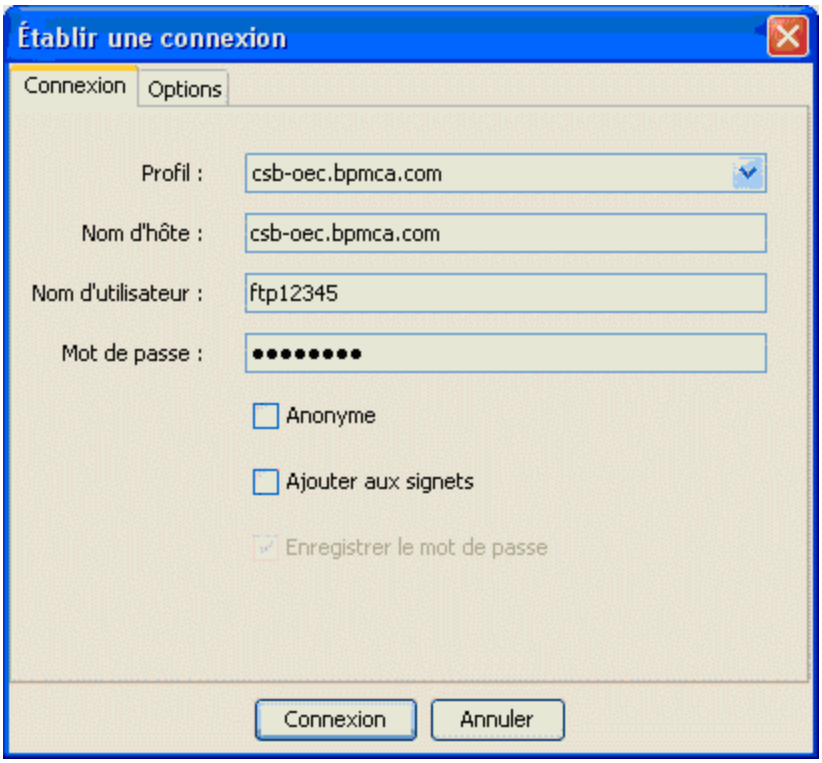
La marche à suivre pour téléverser un fichier au serveur FTPS figure ci-dessous. Les instantanés d'écran supposent l'utilisation de l'application Secure FTP de Glub Tech avec interface graphique cliente (consulter la section 3.1, Interface graphique cliente recommandée pour protocole FTPS). La marche à suivre demeure similaire pour des logiciels clients différents.

Nota :

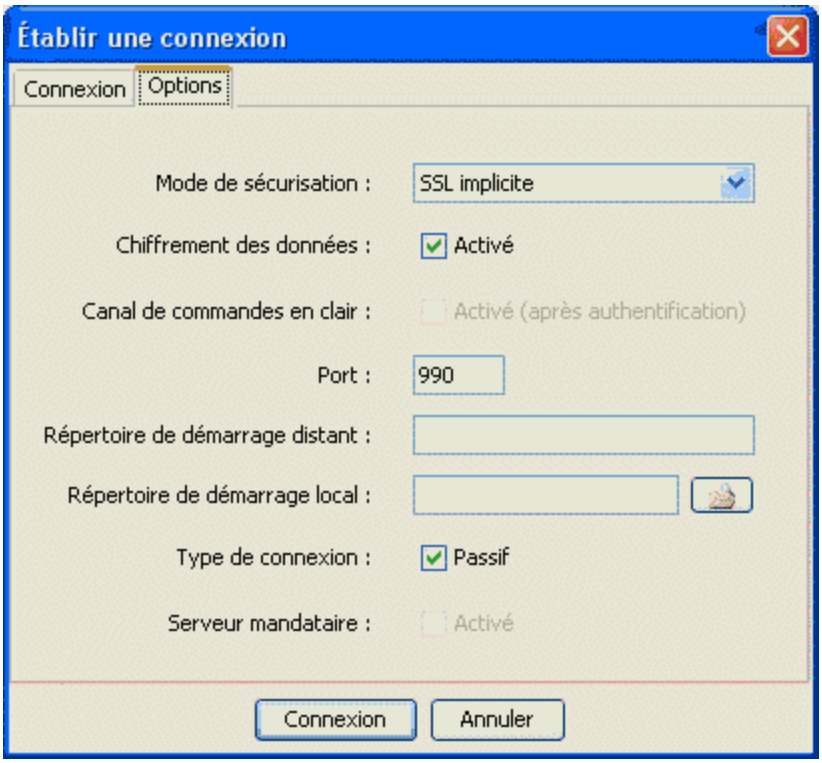
- Si l'organisation utilise un serveur mandataire, sélectionner l'option de menu **Fichier > Préférences** pour définir les paramètres du serveur mandataire dans l'application Secure FTP de Glub Tech.

- Les organisations qui utilisent un pare-feu limitant les connexions sortantes doivent le configurer pour autoriser les connexions vers l'adresse IP 204.104.133.46 (csb-oec.bpmca.com) depuis les ports 990 et 23001 à 23100 au cas où ils utilisent le mode « implicite », ou les ports 21021 et 23001 à 23100 au cas où ils utilisent le mode « explicite ».

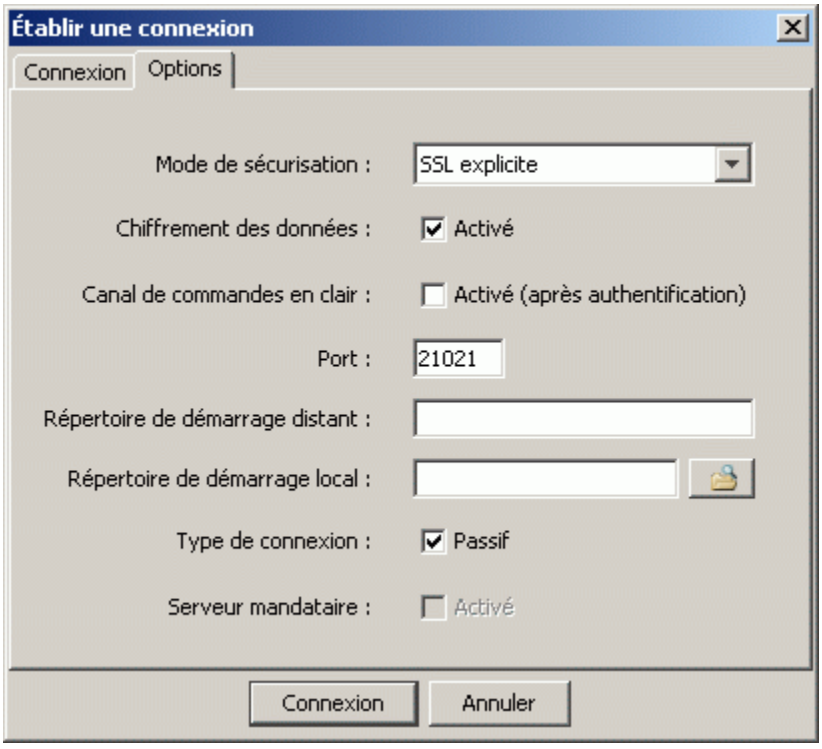
1. Démarrer l'interface graphique cliente. Un écran semblable à celui ci-dessous s'affiche. Autrement, cliquer sur le bouton **Connexion**.



2. Entrer les données ci-dessous dans les champs correspondants, puis sélectionner **Ajouter aux signets** (pour enregistrer les données aux fins d'utilisation future) et cliquer sur l'onglet **Options**.
   - **Nom d'hôte** : entrer csb-oec.bpmca.com ou 204.104.133.46 .
   - **Nom d'utilisateur** : entrer l'ID utilisateur de l'organisation (lettres « ftp » suivies de l'ID de l'organisation).
   - **Mot de passe** : entrer le mot de passe confidentiel de l'organisation.


Établir une connexion
Connexion
Options
Mode de sécurisation :
SSL implicite
Chiffrement des données :
Activé
Canal de commandes en clair :
Activé (après authentification)
Port :
990
Répertoire de démarrage distant :
Répertoire de démarrage local :
Type de connexion :
Passif
Serveur mandataire :
Activé
Connexion
Annuler

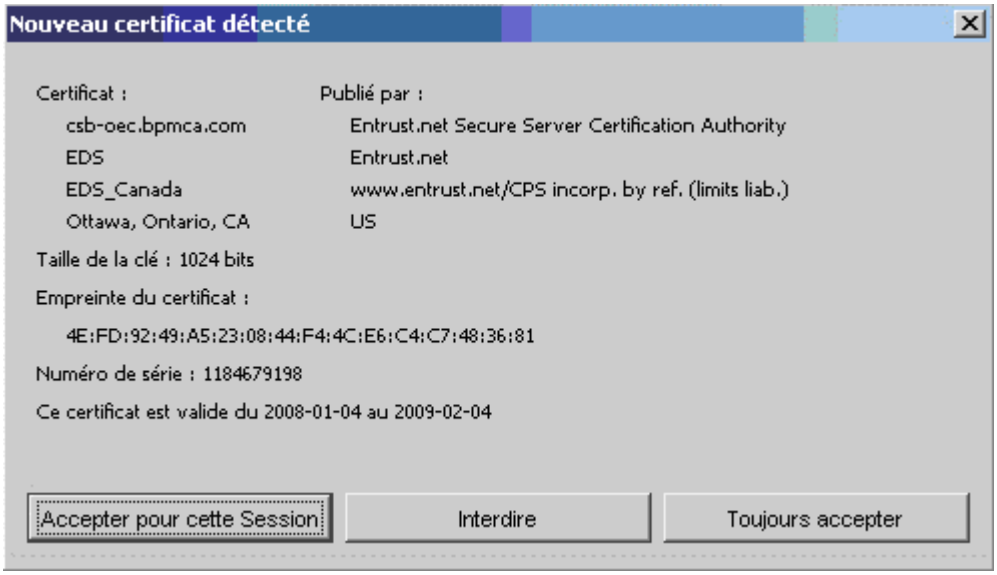
ou


Établir une connexion
Connexion
Options
Mode de sécurisation :
SSL explicite
Chiffrement des données :
Activé
Canal de commandes en clair :
Activé (après authentification)
Port :
21021
Répertoire de démarrage distant :
Répertoire de démarrage local :
Type de connexion :
Passif
Serveur mandataire :
Activé
Connexion
Annuler

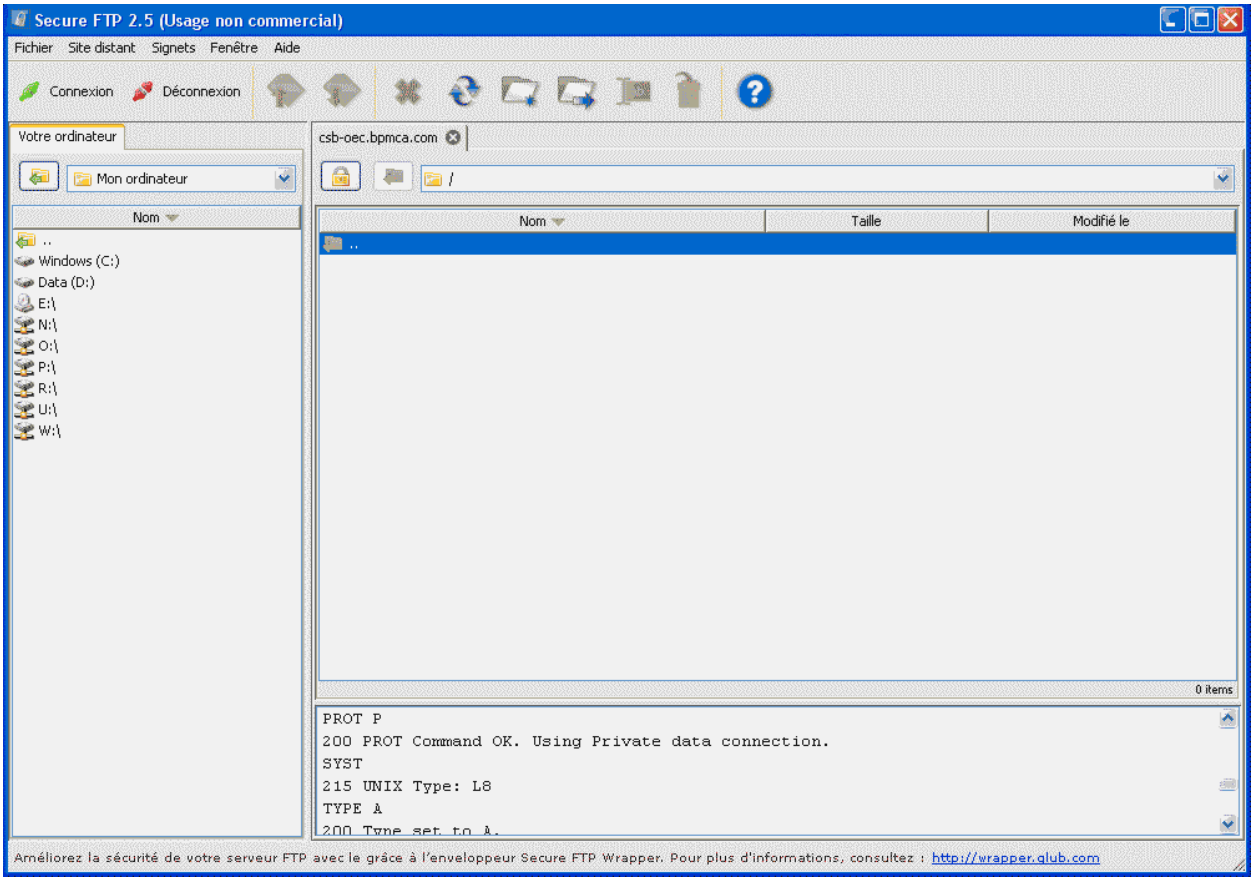
3. Vous avez deux options :

Option « implicite » : Dans la liste déroulante du champ Mode de sécurisation, sélectionner **SSL implicite**; le chiffre 990 devrait s'afficher dans le champ **Port**. S'assurer que les cases **Chiffrement des données** et **Type de connexion** sont cochées (respectivement « Activé » et « Passif »).

Option « explicite » : Dans la liste déroulante du champ Mode de sécurisation, sélectionner **SSL explicite**; le chiffre 21 devrait s'afficher dans le champ **Port** (modifier le chiffre de 21 à 21021). S'assurer que les cases **Chiffrement des données** et **Type de connexion** sont cochées (respectivement « Activé » et « Passif »).

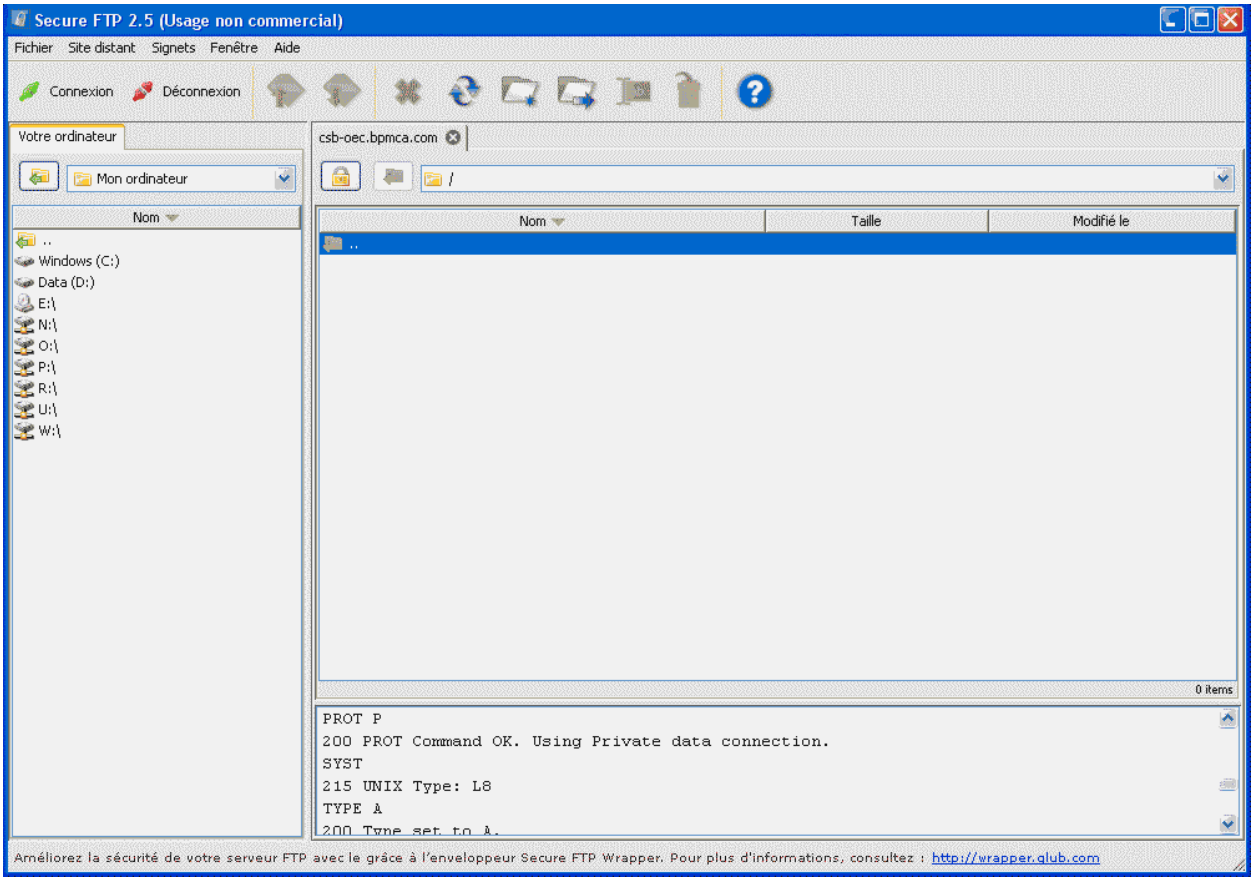


4. Pour accepter le certificat, cliquer sur le bouton **Accepter pour cette session** ou **Toujours accepter**.



5. La partie gauche de l'écran affiche le dossier local de l'utilisateur. Accéder au dossier renfermant les fichiers à téléverser.

6. Sélectionner le mode de transfert (utiliser l'option de menu « Site distant > Mode de transfert > Texte » pour le mode ASCII ou « Site distant > Mode de transfert > Binaire » pour le mode binaire). Faire glisser et déplacer les fichiers à téléverser de la partie gauche à la partie droite de l'écran. Nota : le fichier n'apparaît pas dans la liste même s'il a bien été copié, car le contenu du dossier est bloqué pour des raisons de sécurité.



7. Pour rompre la connexion au serveur FTPS, cliquer sur **Déconnexion**, dans le coin supérieur gauche de l'écran.

8. Nota : Confirmation de fichier (pour les agents administratifs transmettant uniquement des fichiers de souscriptions d'OEC). Les agents doivent donner un préavis avant de soumettre tout fichier de souscriptions. Ils peuvent le faire en envoyant un courriel contenant l'information sur le fichier à l'adresse rpac-pft@oec.gc.ca. Une réponse sera envoyée à l'organisation expéditrice dès réception et traitement de l'information. Cette confirmation devrait parvenir à l'expéditeur dans les 24 heures suivant le traitement. Si ce n'est pas le cas, il convient de récrire à l'adresse rpac-pft@oec.gc.ca pour effectuer un suivi.

4. UTILISATION D'UNE INTERFACE DE PROGRAMMATION CLIENTE AVEC PROTOCOLE FTPS

Cette section explique la marche à suivre pour utiliser le serveur FTPS au moyen d'un logiciel client personnalisé.

4.1. Interface de programmation recommandée

Le serveur FTPS a fait l'objet d'essais poussés au moyen de Secure FTP Bean v2.5.6 de Glub Tech pour Java 5. Ce logiciel est offert pour Windows, Mac OS X, Linux et toute plate-forme Unix munie de JRE Java (version 1.4 ou plus récente). On peut l'acheter en ligne auprès de Glub Tech (http://www.glub.com/store/). Le prix de la licence varie selon l'utilisation prévue : pour usage interne (c'est-à-dire non commercial), le prix est de 500 dollars américains par développeur[3].

4.1.1. Installation de la bibliothèque de programmes Secure FTP Bean de Glub Tech

Se conformer à la marche à suivre ci-dessous pour installer la bibliothèque de programmes Secure FTP Bean de Glub Tech dans un ordinateur de bureau sous Windows (des instructions similaires s'appliquent aux autres plates-formes) :

- Si l'ordinateur n'est pas muni de la trousse de développement Java (JDK version 1.4 ou plus récente), il faut d'abord la télécharger et l'installer. Il suffit d'accéder la page Web http://java.sun.com/javase/downloads/index_jdk5.jsp à l'aide d'un navigateur tel que Microsoft Explorer et de télécharger *JDK 5.0 Update 12*.

- Après le téléchargement de JDK, exécuter le fichier téléchargé pour procéder à l'installation (par ex. jdk-1_5_0_12-windows-i586-p.exe).

- Se procurer une licence du logiciel Secure FTP Bean à l'adresse http://www.glub.com/store/ et suivre les instructions du fournisseur.

- Accéder à http://www.glub.com/store/download.jsp?shortname=bean_2 au moyen d'un navigateur Web et télécharger le logiciel Secure FTP Bean de Glub Tech.

- Décomprimer le fichier téléchargé dans un dossier du bureau pour installer le logiciel Secure FTP Bean de Glub Tech (par ex. gtftps2_5_6.zip).

- Le dossier racine du logiciel Secure FTP Bean de Glub Tech devrait se trouver à l'emplacement suivant : C:\Program Files\SecureFtpBean.

[3] Les prix sont fixés par le fournisseur et ne peuvent être garantis par la Banque du Canada.

4.2. Autres interfaces de programmation clientes FTPS

Les organisations sont libres d'utiliser d'autres logiciels d'interface de programmation (API) pour FTPS puisque cette solution se fonde sur des normes bien établies et ne relève pas d'un éditeur de logiciels particulier. Les progiciels ci-dessous sont en principe compatibles, mais n'ont pas été mis à l'essai avec la solution FTPS de la Banque du Canada.

- edtFTPj/PRO (http://www.enterprisedt.com/products/edtftpjssl/overview.html) : interface de programmation (API) Java compatible avec toute plate-forme fonctionnant sous Java 1.5.x (ou une version plus récente)..

- WS_FTP Professional SDK (http://www.ipswitch.com/products/ws_ftp/devkit/index.asp) : interface de programmation indépendante du langage compatible avec les plates-formes Windows. Est fondée sur l'architecture COM de Windows.

- Secure FTP Factory (http://www.jscape.com/sftp/index.html) : interface de programmation (API) Java compatible avec toute plate-forme fonctionnant sous Java 1.2.2 (ou une version plus récente).

- jMethods Secure FTP API for Java (http://www.jmethods.com/products/) : interface de programmation (API) Java compatible avec toute plate-forme fonctionnant sous Java 1.4.2 (ou une version plus récente).

- FTP Voyager SDK (http://sdk.ftpvoyager.com/) : interface de programmation (API) correspondant à une bibliothèque de programmes MFC C++ Windows.

4.3. Exemple de programmation

Les pages suivantes présentent un exemple de programmation Java applicable au logiciel Secure FTP Bean de Glub Tech.

```
/*
* Example of FTPS client with Glub Tech Secure FTP Bean
* Written by HP
* Last updated in April 2007
*
* Notes:
* - Libraries required (included with Glub Tech Secure FTP Bean):
*  Gtftps.jar, jakarta-regexp-1.4.jar.
* - This example is for learning only. It is NOT a fully-functional
*  production application.
*/

package ftpsexamples;

import com.glub.secureftp.bean.SSLCertificate;
import com.glub.secureftp.bean.SSLFTP;
import com.glub.secureftp.bean.SSLSessionManager;

import java.io.File;

public class FtpsClientExample implements SSLSessionManager {
```

```
private SSLCertificate currentCert = null;

public static void main(String[] args) {

  // This call allows the java.security.SecureRandom object to be
  // generated prior to being used. Class SecureRandom provides a
  // cryptographically strong pseudo-random number generator (PRNG).
  // This secure random number generator is used by Glub Tech Secure
  // FTP Bean.
  SSLFTP.preSeed();

  // Obtain FTPS parameters
  String hostNameOrIpAddress = null;
  int hostPortNumber = 0;
  String ftpsUserId = null;
  String ftpsPassword = null;

  if (args.length < 4) {
    hostNameOrIpAddress = "111.111.111.111"; // Not a real IP address
    hostPortNumber = 990;
    ftpsUserId = "ftp12345";
    ftpsPassword =
        "ftp12345XXXX"; // Not a recommended password in production
  } else {
    hostNameOrIpAddress = args[0];
    hostPortNumber = new Integer(args[1]).intValue();
    ftpsUserId = args[2];
    ftpsPassword = args[3];
  }

  // Perform the upload
  FtpsClientExample ftps = new FtpsClientExample();
  ftps.uploadFile(hostNameOrIpAddress, hostPortNumber, ftpsUserId,
          ftpsPassword, "D:\\tempo\\password.txt");

  // Prints if no exceptions
  System.out.println("Done.");
}

// Connect to FTPS server, upload file, then disconnect

public void uploadFile(String host, int port, String user, String pass,
            String fileName) {

  // Instantiate the SSLFTP object and provide FTPS parameters
  SSLFTP sslFTP =
    new SSLFTP(this, host, port, SSLFTP.IMPLICIT_CONNECTION,
          System.out, System.out);
  try {
    // Connect and login to FTPS server
    sslFTP.connect();
    sslFTP.login(user, pass, null);

    // Ensure that data is encrypted
    // in the communication with the FTPS server
    sslFTP.setDataEncryptionOn(true);

    // Transfer a file to the FTPS server in ASCII mode
    sslFTP.ascii();
    sslFTP.store(new File(fileName), false);

    // Logout
    sslFTP.logout();

  } catch (Exception e) {
    System.err.println("An error occured: " + e.getMessage());
    e.printStackTrace();
```

```
    System.exit(-1);
  }
}

// Callback method required to implement interface SSLSessionManager

public boolean continueWithCertificateHostMismatch(SSLCertificate cert,
                          String actualHost,
                          String certHost) {
  System.out.println("Certificate host mismatch.");
  return false;
}

// Callback method required to implement interface SSLSessionManager

public boolean continueWithExpiredCertificate(SSLCertificate cert) {
  System.out.println("Certificate expired.");
  return false;
}

// Callback method required to implement interface SSLSessionManager

public boolean continueWithInvalidCertificate(SSLCertificate cert) {
  System.out.println("Certificate invalid.");
  return false;
}

// Callback method required to implement interface SSLSessionManager

public boolean continueWithoutServerCertificate() {
  System.out.println("Certificate not sent from server.");
  return false;
}

// Callback method required to implement interface SSLSessionManager

public short newCertificateEncountered(SSLCertificate cert) {
  System.out.println("New certificate found:");
  System.out.println("Common Name.........: " + cert.getCN());
  System.out.println("Start Date..........: " + cert.getStartDate());
  System.out.println("End Date............: " + cert.getEndDate());
  System.out.println("Fingerprint.........: " + cert.getFingerprint());
  System.out.println("Serial Number......: " + cert.getSerialNumber());
  System.out.println("Organization.......: " + cert.getOrg());
  System.out.println("Organizational Unit: " + cert.getOU());
  System.out.println("Locality............: " + cert.getLocality());
  System.out.println("State/Province.....: " + cert.getState());
  System.out.println("Country.............: " + cert.getCountry());
  System.out.println("Email...............: " + cert.getEmail());
  System.out.println("Issuer's Common Name.........: " +
            cert.getIssuerCN());
  System.out.println("Issuer's Organization.......: " +
            cert.getIssuerOrg());
  System.out.println("Issuer's Organizational Unit: " +
            cert.getIssuerOU());
  System.out.println("Issuer's Locality............: " +
            cert.getIssuerLocality());
  System.out.println("Issuer's State/Province.....: " +
            cert.getIssuerState());
  System.out.println("Issuer's Country.............: " +
            cert.getIssuerCountry());
  System.out.println("Issuer's Email...............: " +
            cert.getIssuerEmail());
  return SSLSessionManager.ALLOW_CERTIFICATE;
}

// Callback method required to implement interface SSLSessionManager
```

```
 public short replaceCertificate(SSLCertificate oldCert,
                 SSLCertificate newCert) {
   System.out.println("Replace certificate.");
   return SSLSessionManager.ALLOW_CERTIFICATE;
 }

 // Callback method required to implement interface SSLSessionManager

 public void randomSeedIsGenerating() {
   System.out.print("The random seed is generating... ");
 }

 // Callback method required to implement interface SSLSessionManager

 public void randomSeedGenerated() {
   System.out.println("The random seed is generated... ");
 }

 // Callback method required to implement interface SSLSessionManager

 public void setCurrentCertificate(SSLCertificate currentCert) {
   this.currentCert = currentCert;
 }
}
```

5. EXIGENCES RELATIVES AUX FICHIERS À TÉLÉVERSER

Cette section décrit les caractéristiques que doivent posséder les fichiers à téléverser par le biais du serveur FTPS et cite les documents de référence pertinents.

5.1. Fichier de données

5.1.1. Contenu d'un fichier de retenues sur salaire

Pour connaître les exigences relatives au contenu des fichiers de retenues sur salaire, consulter le document http://csb.gc.ca/wp-content/uploads/2009/03/85006_technical_specs_f_v2_x1a.pdf. Le format des données est demeuré inchangé malgré le basculement sur le serveur FTPS.

Avant d'accepter un fichier de données, le serveur FTPS assure le respect de chacune des exigences suivantes (c'est-à-dire que si une seule d'entre elles n'est pas remplie, le fichier n'est pas traité) :

- Le type correspondant à l'ID utilisateur associé au téléversement du fichier doit être défini comme « employeur » dans le serveur FTPS.

- L'ID de l'organisation émettrice figurant dans l'enregistrement en-tête (type 10) et dans l'enregistrement complémentaire (type 90) de transmission doit correspondre à l'ID utilisateur FTPS associé au téléversement du fichier. Par exemple, si l'ID utilisateur est ftp12345, l'ID de l'organisation émettrice figurant dans les enregistrements en-tête et complémentaire de transmission doit être 12345.

- L'ID de l'organisation émettrice figurant dans l'enregistrement en-tête (type 10) et dans l'enregistrement complémentaire (type 90) de transmission doit correspondre à l'ID de l'organisation figurant dans le nom du fichier (consulter la section 5.1.3, Désignation d'un fichier de données).

- L'ID de l'organisation émettrice doit être définie en vue de la soumission d'enregistrements au nom de chaque ID d'organisation figurant dans l'enregistrement en-tête de lot (type 20), l'enregistrement détail de lot (types 30, 40 ou 50) et l'enregistrement complémentaire de lot (type 80).

5.1.2. Contenu d'un fichier de souscriptions d'OEC

Pour connaître les exigences relatives au contenu des fichiers de souscriptions, se reporter aux *Spécifications relatives au fichier des achats*, soit les documents *Normes relatives aux enregistrements logiques* et *Dictionnaire des éléments d'information*, qui s'appliquent au Système de gestion des titres détenus par les particuliers (SGTP) et sont consultables depuis l'adresse http://oec.gc.ca/financial-institutions-and-investment-dealers-fr/selling-and-processing-

s42-fr/?lang=fr. Le format des données est demeuré inchangé malgré le basculement sur le serveur FTPS.

Avant d'accepter un fichier de données, le serveur FTPS assure le respect de chacune des exigences suivantes (c'est-à-dire que si une seule d'entre elles n'est pas remplie, le fichier n'est pas traité) :

- Le type correspondant à l'ID de l'utilisateur ayant effectué le téléversement du fichier doit être défini comme « purchase agent » (agent acheteur) dans le serveur FTPS.

- L'ID de l'organisation figurant dans l'enregistrement en-tête (type A) et dans l'enregistrement complémentaire (type Z) doit correspondre à l'ID de l'organisation figurant dans le nom du fichier (consulter la section 5.1.3, Désignation d'un fichier de données).

5.1.3. Désignation d'un fichier de données

Le nom d'un fichier de données (retenues sur salaire ou souscriptions) doit se composer comme suit (les règles de désignation des fichiers de données sont demeurées inchangées malgré le basculement sur le serveur FTPS) :

`xxxxxnnn.##T` *(non sensible à la casse) fichier test*

`xxxxxnnn.##P` *(non sensible à la casse) fichier de production*

Où :

xxxxx	ID d'organisation : il s'agit de l'ID d'organisation figurant dans l'en-tête du fichier de données.
nnn	Numéro d'ordre au choix de l'utilisateur. **Fichiers de retenues sur salaire** : Le numéro d'ordre doit se composer uniquement de caractères alphabétiques (A à Z ou bien a à z, mais aucun caractère accentué) ou numériques (0 à 9), et comporter au moins un de ces caractères. Il peut être utilisé pour assurer le respect des règles de désignation de l'organisation, telles que la distinction des groupes de paye ou des jours de paye. Si l'organisation transmet plusieurs fichiers de retenues sur salaire le même jour, un numéro unique doit être attribué à chaque fichier. **Fichiers de souscriptions** : Le numéro d'ordre doit se composer uniquement de caractères alphabétiques (A à Z ou bien a à z, mais aucun caractère accentué) ou numériques (0 à 9), et comporter trois caractères. On doit attribuer des numéros d'ordre uniques à l'intérieur d'une période de campagne. Il est recommandé d'augmenter d'une unité à chaque transmission.

##T / ##P	Utiliser tel quel (non sensible à la casse). Un fichier dont l'extension correspond à « ##P » est traité de la manière habituelle. Un fichier dont l'extension correspond à « ##T » est traité comme un fichier test.

Exemples de noms de fichiers de **retenues sur salaire** valides :

```
123451.##T

1234599999.##P

12345001.##t

12345999.##p
```

Exemples de noms de fichiers de **souscriptions** valides :

```
12345001.##T

12345999.##P

12345678.##T

00001999.##P

12345001.##t

12345999.##p
```

Exemples de noms de fichiers non valides :

`12345Numéro1.##T`	(Caractère accentué « é » inacceptable)
`12345.##p`	(Numéro d'ordre manquant)
`12345999.P`	(Caractères « ## » manquants dans l'extension)
`12345001.###T`	(Caractères « # » trop nombreux dans l'extension)
`12345 1.##T`	(Espaces interdits)
`12345999.#P`	(Caractères « # » insuffisants dans l'extension)
`12345001.TXT`	(« TXT » n'est pas une extension acceptable dans ce cas.)
`12345001##T`	(Point manquant)
`99912345.##P`	(L'ID de l'organisation doit précéder le numéro d'ordre.)

Nota :

- Pour qu'un fichier de données soit considéré comme valide et soit traité, il faut que son nom soit conforme aux règles de désignation.

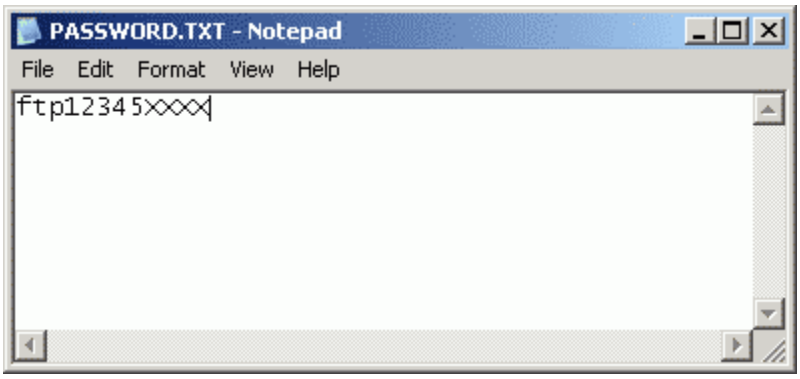
- Le nom du fichier original stocké dans l'environnement de l'organisation ne doit pas obligatoirement être identique au nom du fichier téléversé dans le serveur FTPS; cependant, l'utilisation du même nom ou d'un nom similaire (par ex. « 2009-JAN-05-12345001.##T » dans le cas du fichier téléversé « 12345001.##T ») peut faciliter la corrélation entre les fichiers.

- Il est fortement recommandé de conserver une copie du fichier jusqu'à la réception de la confirmation de transmission et de traitement par lots de la Banque du Canada.

5.2. Fichier de mot de passe

5.2.1. Contenu d'un fichier de mot de passe

Il recommandé, comme cela a déjà été mentionné, de changer régulièrement de mot passe. Le système FTPS permet de modifier son mot de passe par téléversement d'un fichier ad hoc. Ce fichier doit renfermer un seul mot (sensible à la casse), qui correspond au nouveau mot de passe. Voici un exemple de fichier de mot de passe (à noter qu'un tel mot de passe n'est pas recommandé) :



Avant d'accepter un fichier de mot de passe, le serveur FTPS assure le respect de chacune des exigences suivantes :

- Le mot de passe doit être du texte chiffré en caractères ASCII.

- Le mot de passe doit être composé d'un minimum de 12 caractères et d'un maximum de 40.

- Le mot de passe doit renfermer au moins une lettre en minuscule, une autre en majuscule et deux caractères numériques.

- Le mot de passe doit être composé d'une combinaison des caractères suivants : **a** à **z**, **A** à **Z** et **0** à **9**. Aucun autre type de caractères n'est accepté.

- Les huit premiers caractères du mot de passe doivent renfermer un moins un caractère numérique et deux caractères alphabétiques.

- Le mot de passe ne peut résulter du décalage circulaire de l'ID utilisateur (un tel mot de passe serait refusé parce qu'il ne compterait que neuf caractères).

- Le nouveau mot de passe doit être différent du mot de passe précédent et ne peut résulter du décalage inverse ou circulaire de celui-ci. Dans ce cas, les lettres en minuscules et en majuscules sont considérées comme identiques.

- Le nouveau mot de passe doit compter au moins trois caractères différents par rapport au mot de passe précédent. Dans ce cas, les lettres en minuscules et en majuscules sont considérées comme identiques.

Exemples de mots de passe valides :

```
ABCxyz123456

1933to1995ElizabethVictoriaMontgomery
```

Exemples de mots de passe non valides :

`ABCxyz123`	(Moins de 12 caractères)
`1933to1995ElizabethVictoriaMontgomeryWasBewitched`	(Trop de caractères)
`ElizabethVictoriaMontgomery`	(Aucun caractère numérique)
`1933to1995elizabethmontgomery`	(Aucune lettre en majuscule)
`1933TO1995EMONTGOMERY`	(Aucune lettre en minuscule)
`ElizabethMontgomery1933to1995`	(Aucun caractère numérique parmi les huit premiers caractères)
`33-95ElizabethMontgomery`	(Caractère spécial « - » non autorisé)
`33 95 Elizabeth Montgomery`	(Espaces interdits)

5.2.2. Désignation d'un fichier de mot de passe

Le nom d'un fichier de mot de passe doit être « password_xxxxx.txt » (non sensible à la casse), xxxxx étant l'ID d'organisation de l'utilisateur du FTPS qui téléverse le fichier. Tout fichier de mot de passe portant un autre nom ne sera pas traité comme un fichier de mot de passe.

Exemples de noms de fichiers valides :

```
Password_12345.txt

PASSWORD_12345.TXT

password_12345.txt

Password_12345.TXT

PassWord_12345.TXT

PaSsWoRd.TxT
```

Exemples de noms de fichiers non valides :

`PASSWORD_12345`	(Extension manquante)
`PASSWORD_12345.DOC`	(Extension « TXT » obligatoire)
`Pass word_12345.txt`	(Espaces interdits)
`Password_12345-txt`	(Le trait d'union ne peut remplacer le point.)
`OpenSesame_12345.txt`	(Remplacer « OpenSesame » par « password ».)
`Password.txt`	(ID d'organisation manquant)

Nota :

- Pour qu'un fichier de mot de passe soit considéré comme valide et soit traité, il faut que son nom soit conforme aux règles de désignation.
- Le mot de passe est en principe changé en l'espace de quelques minutes après le téléversement du fichier de mot de passe. Après la tentative de changement par le serveur FTPS, l'utilisateur reçoit un courriel indiquant si l'opération a réussi ou échoué.