



Guide de démarrage du canal de transfert FTP

Table des matières

| | |
|---|----|
| 1. Qu'est-ce que le FTP ?..... | 3 |
| 2. De quoi avez-vous besoin ?..... | 3 |
| 2.1 Connexion à l'extranet de la sécurité sociale..... | 3 |
| 2.1.1 Connexion réseau pour les employeurs ONSS..... | 3 |
| 2.1.2 Connexion réseau pour les administrations provinciales et locales..... | 4 |
| 2.1.3 Adresses IP..... | 4 |
| 2.1.3.1 Adresse IP pour les différentes déclarations ?..... | 4 |
| 2.1.3.2 Comment adapter vos firewall et applications ?..... | 5 |
| 2.1.3.3 Comment tester la connexion à l'adresse IP ?..... | 5 |
| 2.1.4 Configuration réseau pour les expéditeurs : DNS..... | 5 |
| 2.2 Un certificat digital qualifié..... | 6 |
| 2.3 Un numéro d'expéditeur et un canal FTP actif..... | 7 |
| 3. Quels fichiers joindre aux messages structurés ?..... | 8 |
| 3.1 Le fichier de signature (FS)..... | 8 |
| 3.2 Le fichier GO..... | 9 |
| 4. Comment envoyer un message structuré ?..... | 10 |
| 4.1 Placer des fichiers..... | 10 |
| 4.2 Extraire des fichiers..... | 10 |

1. Qu'est-ce que le FTP ?

Le **File Transfer Protocol** (FTP) est un protocole facilitant l'échange de fichiers entre ordinateurs. Il standardise plusieurs actions qui diffèrent souvent selon le système d'exploitation.

Les employeurs ONSS et leurs mandataires peuvent utiliser le FTP comme canal de communication pour envoyer des messages structurés.

2. De quoi avez-vous besoin ?

- Une connexion à l'extranet de la sécurité sociale
- [Un certificat digital qualifié](#)
- Un client FTP
- [Un numéro d'expéditeur](#)

2.1 Connexion à l'extranet de la sécurité sociale

Pour envoyer des messages structurés via FTP, vous devez vous connecter à l'**extranet** de la sécurité sociale. L'extranet est une infrastructure réseau commune sur laquelle sont établis tous les contacts avec le monde extérieur, permettant de gérer de manière centralisée la sécurité requise et d'atteindre un niveau de sécurité identique pour toutes les institutions de la sécurité sociale.

Remarque: le FTP n'est pas possible via une connexion internet classique car celle-ci n'est pas suffisamment sûre. Un routeur via une connexion internet n'est donc pas possible. Si vous souhaitez passer par une connexion internet pour effectuer vos envois, le SFTP offre une belle alternative.

2.1.1 Connexion réseau pour les employeurs ONSS

Les expéditeurs peuvent uniquement se connecter par Routeur à l'extranet:

- Ø Routeur (connexion fixe)

Une connexion fixe n'est pas **bon marché** et convient uniquement aux expéditeurs qui doivent envoyer des fichiers très régulièrement.

Il existe deux types :

- Belgacom Explore: connexion réseau de Belgacom
- Une ligne louée (leased line): connexion directe du réseau de votre entreprise à l'extranet

Pour demander une connexion fixe à l'extranet de la sécurité sociale, envoyez un e-mail au centre de contact (batch@eranova.fgov.be).

2.1.2 Connexion réseau pour les administrations provinciales et locales

En plus de la connexion mentionnée sous le point 2.1.1, les employeurs ONSS peuvent utiliser une connexion fixe via les réseaux secondaires suivants:

- ✚ Cipal
- ✚ Irisnet: pour les employeurs de la région de Bruxelles-Capitale
- ✚ Publink: pour toutes les communes
- ✚ Schaubroeck
- ✚ Infrax
- ✚ PubliWin

2.1.3 Adresses IP

2.1.3.1 Adresse IP pour les différentes déclarations ?

Pour pouvoir envoyer vos déclarations par messages structurés à l'ONSS, vous devez avoir accès à l'adresse IP suivante:

| Nom | Adresse IP | Port | Application |
|-----------------------|-------------------|-------------|--|
| ftp.socialsecurity.be | 85.91.172.252 | 21/20 | DRS DmfA Dimona V2 Chômage temporaire Déclaration unique de chantier |

2.1.3.2 Comment adapter vos firewall et applications ?

Lorsque vous vous annoncez sur l'extranet de la sécurité sociale, votre administrateur réseau ou responsable ICT doit vérifier si les adresses IP sont **routées** vers l'extranet par une connexion directe (pour les employeurs ONSS) ou par un réseau secondaire (pour les administrations provinciales et locales).

Attention :

- ∅ Le routage doit être adapté uniquement à l'adresse mentionnée et non à la série complète (85.91.160.0/19).
- ∅ Si vous utilisez Belgacom Explore, demandez Belgacom d'adapter le routage.

Lorsqu'une adresse IP doit être adaptée sur votre firewall, vous devez attribuer à cette nouvelle adresse IP les mêmes droits et ports qu'à l'ancienne :

| Nom | Adresse IP | Port |
|-----------------------|---------------|-------|
| ftp.socialsecurity.be | 85.91.172.252 | 21/20 |

2.1.3.3 Comment tester la connexion à l'adresse IP ?

Vous pouvez tester la connexion à l'adresse IP au moyen, par exemple, d'un **telnet** sur le port 21 (FTP).

Si vous ne pouvez pas vous connecter au serveur FTP, vous pouvez également suivre la procédure de test suivante :

(https://www.socialsecurity.be/site_fr/general/news/ip/documents/testprocedure_dmfa-asr_F.pdf)

2.1.4 Configuration réseau pour les expéditeurs : DNS

Les noms des ordinateurs (hostnames) doivent être traduits en l'adresse IP correspondante. Pour cela, on utilise les serveurs DNS suivants :

| Nom | Adresse IP |
|--------------------|--------------|
| dnsintera.smals.be | 85.91.175.17 |
| dnsinterb.smals.be | 85.91.175.50 |

Ces serveurs sont disponibles via l'internet.

Conseil : si vous n'avez pas accès à l'internet, prévoyez les enregistrements DNS nécessaires dans votre système DNS local.

2.2 Un certificat digital qualifié

Pour effectuer un envoi via FTP, vous avez besoin d'un certificat digital qualifié.

Vous avez le choix entre :

1. Le certificat de signature de votre carte d'identité électronique (<http://eid.belgium.be/fr/>)
2. Un certificat digital qualifié du prestataire de services de certification suivant :
GlobalSign : PersonalSign 3 pro
(<https://www.globalsign.eu/personalsign/personalsign3-pro/>)

Vous devrez utiliser votre certificat digital qualifié pour deux actions :

- Vous devrez charger la clé publique de votre certificat digital qualifié (portant l'extension .cer) lors de la création de votre canal FTP sur le site portail de la sécurité sociale (www.securitesociale.be).
- Sur la base de votre certificat qualifié (extension .pfx ou .p12) et pour chaque fichier de déclaration (FI), vous devrez créer un fichier de signature (FS) que vous placerez sur le serveur FTP avec le fichier de déclaration.

Remarque :

Lors du choix d'un certificat digital qualifié, il est important de tenir compte de la manière dont vous allez créer [vos fichiers de signature \(FS\)](#) :

Vous pouvez créer vous-même votre fichier de signature, via OpenSSL par exemple, ou utiliser des programmes développés par des producteurs de logiciels ou par vous-même (Voir le point 3.1 : le fichier de signature).

Si vous souhaitez créer le fichier de signature via OpenSSL, il est important de demander un certificat à votre prestataire de services de certification, à partir duquel vous pourrez exporter la clé privée. Attention : la procédure avec OpenSSL est souvent problématique pour les certificats contenus sur des cartes à puce ou des clés USB.

Un client FTP

Pour pouvoir communiquer avec notre serveur FTP, vous avez besoin d'un client FTP.

Vous travaillez avec Windows:

Les ordinateurs Windows disposent d'un client FTP standard.

Vous pouvez aussi utiliser un moteur de recherche et effectuer une recherche sur 'FTP Client'. Vous trouverez, parmi les résultats des clients software FTP gratuits et payants.

Vous êtes libre de choisir le client qui correspond le plus à vos besoins.

Vous travaillez avec Linux:

Les systèmes Linux proposent des packages standard contenant un client FTP.

Vous pouvez aussi utiliser un moteur de recherche et effectuer une recherche sur 'FTP Client'. Vous trouverez, parmi les résultats des clients software FTP gratuits et payants.

Vous travaillez avec Apple:

Les ordinateurs Apple disposent d'un client FTP standard.

Il existe également plusieurs autres clients SFTP pour Apple. Vous pouvez les trouver par un moteur de recherche et effectuer une recherche sur 'SFTP & Apple' ou sur le site www.apple.com.

2.3 Un numéro d'expéditeur et un canal FTP actif

Pour pouvoir envoyer des messages structurés via FTP, vous devez disposer d'un numéro d'expéditeur et d'un canal FTP actif pour chaque qualité pour laquelle vous souhaitez envoyer.

Seul le (co-)gestionnaire local de chaque qualité peut enregistrer un numéro d'expéditeur et activer un canal sur www.securitesociale.be. Voici les étapes qu'ils doivent suivre :

Cliquer sur « **Messages structurés** »
Cliquer sur « **Enregistrer les données de configuration** »
Cliquer sur « **Suivant** »
Saisir les données de contact de l'utilisateur technique
Cliquer sur « **Suivant** »
Sélectionner le type de canal **FTP**
Le type de connexion est **Routeur**
Charger la clé publique de votre **certificat**
Choisir dans la liste des applications les **applications** souhaitées
Cliquer sur « **Suivant** »
Saisir le **nom d'utilisateur** de l'utilisateur technique
Saisir le **mot de passe** de l'utilisateur technique
Cliquer sur « **Suivant** »
Cliquer sur « **Confirmer** »

3. Quels fichiers joindre aux messages structurés ?

Deux fichiers doivent être joints aux messages structurés que vous envoyez via FTP à l'ONSS :

- [Le fichier de signature \(FS\)](#)
- [Le fichier GO](#)

3.1 Le fichier de signature (FS)

Le fichier de signature est joint à un fichier contenant les déclarations originales, les déclarations de modification et les demandes de consultation. Si ces fichiers ont été créés dans l'environnement de test, aucun fichier de signature ne devra être joint.

Vous pouvez créer vous-même le fichier de signature (FS), via OpenSSL par exemple, ou utiliser des programmes développés par des producteurs de logiciels ou par vous-même.

Si vous souhaitez créer le fichier de signature via OpenSSL, il est important de demander un certificat à votre prestataire de services de certification, à partir duquel vous pourrez exporter la clé privée. Ceci pose problème pour les certificats figurant sur des cartes à puce ou des clés USB.

Si vous voulez créer un fichier de signature avec l'eID, vous pouvez utiliser la procédure avec Cryptonit. La procédure se trouve dans la bibliothèque technique : (<https://www.socialsecurity.be/public/doclibrary/fr/batch.htm>).

Comment créer un fichier de signature via OpenSSL ?

Pour créer un fichier de signature avec OpenSSL, ce logiciel doit d'abord être installé sur le PC sur lequel vous allez créer le fichier de signature
Via un moteur de recherche, OpenSSL peut être trouvé très facilement.

Après l'installation, il est préférable de créer un répertoire sur votre PC pour y placer votre certificat (format .pfx ou .p12) et votre (vos) fichier(s) FI à signer.

1. Ouvrez une fenêtre dos. Pour ce faire, allez à Start et cliquez sur **Run**.
2. Tapez **cmd** et cliquez sur « OK ».
3. Rejoignez le C-prompt (cela signifie que vous avez une ligne où il figure uniquement 'C:\>').
Pour ce faire, vous devez saisir plusieurs fois la commande **cd..** et appuyer sur la touche [ENTER].
4. Ouvrez le répertoire OpenSSL via la commande **cd openssl** suivie de [ENTER].
5. Ouvrez le sous répertoire bin via la commande **cd bin** suivie de [ENTER].
6. Ouvrez OpenSSL via la commande **openssl** suivie de [ENTER].

7. Après le prompt, vous devez introduire la commande pour créer le **fichier .pem**. Attention : vous devez ici utiliser votre certificat (format .pfx, .p12) et non la clé publique du certificat (.cer).
 Introduisez la commande suivante avec le chemin complet où se trouve votre répertoire avec le certificat et votre fichier FI à signer après le prompt : **pkcs12 -in** EMPLACEMENT DE VOTRE RÉPERTOIRE\VOTRE CERTIFICAT **-passin pass:**MOT DE PASSE DE VOTRE CERTIFICAT **-out** EMPLACEMENT DE VOTRE RÉPERTOIRE\NOM DE VOTRE FICHIER .PEM **-clcerts -nokeys** suivi de [ENTER]
8. Pour créer votre **fichier .key**, introduisez maintenant la commande suivante après le prompt OpenSSL> : **pkcs12 -in** EMPLACEMENT DE VOTRE RÉPERTOIRE\VOTRE CERTIFICAT **-passin pass:**MOT DE PASSE DE VOTRE CERTIFICAT **-passout pass:**MOT DE PASSE QUE VOUS CHOISISSEZ POUR VOTRE .KEY **-out** EMPLACEMENT DE VOTRE RÉPERTOIRE\NOM DE VOTRE fichier .KEY suivi de [ENTER]
9. Pour créer votre **fichier FS**, introduisez maintenant la commande suivante après le prompt OpenSSL> : **smime -sign -in** EMPLACEMENT DE VOTRE RÉPERTOIRE\NOM DE VOTRE FICHIER FI **-signer** EMPLACEMENT DE VOTRE RÉPERTOIRE\NOM DE VOTRE FICHIER .PEM **-inkey** EMPLACEMENT DE VOTRE RÉPERTOIRE\NOM DE VOTRE FICHIER .KEY **-passin pass:** MOT DE PASSE QUE VOUS CHOISISSEZ POUR VOTRE .KEY **-outform PEM -out** EMPLACEMENT DE VOTRE RÉPERTOIRE\NOM DE VOTRE FICHIER FS suivi de [ENTER]
10. Avant de pouvoir envoyer le fichier, vous devez encore apporter manuellement quelques modifications à votre fichier FS.
 Ouvrez le fichier FS avec un éditeur de texte comme Textpad, Notepad ou Wordpad et supprimez la première (-----DEBUT PKCS7-----) et la dernière ligne (-----END PKCS7-----), y compris les éventuelles lignes vierges dues à un ENTER (Retour chariot).

Structure du nom d'un fichier FS :

FS.application.numéro d'expéditeur.date.numéro de suite.environnement de travail.nombre de parties.numéro de la partie
 Exemple : FS.DMFA.101380.20100920.00001.T.1.1

Attention : lorsqu'une déclaration est envoyée en plusieurs parties, un fichier de signature sera joint à chaque partie du fichier.

3.2 Le fichier GO

Tout fichier de données échangé est accompagné d'un fichier GO. Celui-ci indique que le transfert du fichier de données est terminé.

Pour créer un fichier GO, vous devez ouvrir un fichier texte (extension : .txt) vide et le sauvegarder avec le nom de fichier correct. Supprimez ensuite .txt à la fin du nom.

Structure du nom d'un fichier GO :

GO.application.numéro d'expéditeur.date.numéro de suite.environnement de travail.nombre de parties
 Exemple : GO.DMFA.101380.20100920.00001.T.1

Attention : lorsqu'une déclaration est envoyée en plusieurs parties, un seul fichier GO est joint.

4. Comment envoyer un message structuré ?

Pour envoyer des messages via FTP à l'ONSS, vous devez avoir accès au serveur FTP du point de transfert de la sécurité sociale. Pour cela, vous devez vous connecter à l'extranet de la sécurité sociale (voir page 3 point 2.1.) et vous annoncer avec votre nom d'utilisateur technique et le mot de passe correspondant.

Sur ce serveur, vous avez accès à un répertoire qui vous est réservé. Celui-ci comporte plusieurs sous répertoires dans lesquels vous pouvez placer les fichiers que vous souhaitez envoyer à l'ONSS(APL):

- Répertoire IN
- Répertoire INTEST
- Répertoire INTEST-S

Le répertoire contient également plusieurs sous répertoires contenant les fichiers que l'ONSS(APL) a créés pour vous:

- Répertoire OUT
- Répertoire OUTTEST
- Répertoire OUTTEST-S

4.1 Placer des fichiers

Ouvrez dans votre client FTP le répertoire dans lequel vous souhaitez placer vos fichiers.

- Fichiers de production DmfA, DRS, Dimona, Chômage temporaire et Déclaration unique de chantier (extension **R**) -> répertoire **IN**
- Fichiers de test/simulation DRS, Dimona, Chômage temporaire et Déclaration unique de chantier et fichiers de test de circuit DmfA (extension **T**) -> répertoire **INTEST**
- Fichiers de test de déclaration DmfA et « DRS AMI » (extension **S**) -> répertoire **INTEST-S**

4.2 Sauvegarder et supprimer des fichiers

Une fois les déclarations traitées, vous trouverez les réponses (ACRF, notifications...) dans les répertoires respectifs :

- Fichiers de production DmfA, DRS, Dimona, Chômage temporaire et Déclaration unique de chantier (extension **R**) -> répertoire **OUT**
- Fichiers de test/simulation DRS, Dimona, Chômage temporaire et Déclaration unique de chantier et fichiers de test de circuit DmfA (extension **T**) -> répertoire **OUTTEST**
- Fichiers de test de déclaration DmfA et « DRS AMI » (extension **S**) -> répertoire **OUTTEST-S**

Le but est que vous copiez les fichiers dans ces répertoires quelque part sur un serveur ou un PC chez vous et que vous supprimiez ensuite les fichiers copiés des répertoires OUT sur notre serveur.

Étant donné que nous devons prévoir de l'espace pour tous les expéditeurs, nous ne pouvons pas indéfiniment tenir à disposition les fichiers sortants.