Startup guide du canal de transfert SFTP

Version 10

Table des matières

1. Qu'est-ce que SFTP ?

SFTP signifie **SSH File Transfer Protocol** ou **Secure File Transfer Protocol**.

Comme l'indique la première définition, SFTP fait partie de SSH ou Secure Shell. Il s'agit d'un remplaçant sûr pour l'établissement d'une session de terminal sur des machines UNIX. SFTP est le composant de ce protocole SSH qui assure le transfert de fichiers.

Un client SFTP se comporte comme un client FTP classique, où vous avez une vue sur les répertoires et les fichiers, et où vous pouvez déposer, extraire… des fichiers avec les mêmes commandes que FTP.

Contrairement à FTP, les ordinateurs Windows ne disposent pas d'un client standard. Vous devez donc pour cela installer du **software supplémentaire**. Il existe des clients software SFTP gratuits et payants. Les systèmes Linux proposent des packages standard d'une implémentation open source de SSH (OpenSSH).

SFTP est toutefois un tout autre protocole que FTP. Il est en effet protégé à l'aide de **techniques cryptographiques**, ce qui signifie que tout le trafic entre un client et un serveur est entièrement chiffré, depuis le processus d'identification jusqu'à l'envoi de fichiers. Étant donné cette protection, SFTP convient très bien à l'échange **sécurisé** de fichiers sur **l'internet**.

Il existe plusieurs conditions pour s'identifier comme utilisateur via SFTP.
Bien entendu, on dispose toujours d'un **nom d'utilisateur**.
À côté de cela, une paire de clés électroniques remplace le mot de passe au sens classique du terme. Cette paire de clés comporte **une clé privée et une clé publique**. La clé privée reste chez celui qui l'a créée et sera de préférence encore protégée par un mot de passe additionnel. La clé publique peut être envoyée à toute partie adverse qui souhaite identifier le détenteur de la clé privée.

Ce système ressemble étroitement au système X.509 (comme celui de la carte d'identité électronique) qui utilise des clés privées et des certificats. Les principes sous-jacents sont identiques, mais SFTP utilise rarement des certificats. SFTP possède donc son propre format de clés. Ces clés ne peuvent pas être achetées comme un certificat, il faut les **générer soi-même**. La majorité des clients SFTP disposent d'une fonction pour générer cette paire de clés.

Tout comme le client, chaque **serveur SFTP** dispose également d'une paire de clés. Lors de l'établissement d'une connexion avec un serveur, celui-ci transmettra sa clé publique (également appelée host key) au client. C'est alors à l'utilisateur final qu'il appartient d'accepter cette clé. À partir de ce point, la connexion sécurisée peut être établie et l'utilisateur peut s'identifier.

L'authentification se fait via le nom d'utilisateur et la clé publique.

2. De quoi avez-vous besoin?

- Une connexion internet
- Un certificat digital qualifié
- Un client SFTP
- Une paire de clés SSH
- Un numéro d'expéditeur

2.1 Un certificat digital qualifié

Chaque fichier de déclaration que vous envoyez par SFTP doit être accompagné d'un fichier de signature. Pour générer ce fichier de signature vous avez besoin d'un certificat digital qualifié.

Vous pouvez choisir 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 allez devoir utiliser votre certificat digital qualifié pour 2 actions.

- Vous devez charger la clé publique de votre certificat digital qualifié (avec l'extension .cer) pour ouvrir votre canal SFTP sur le portail de la sécurité sociale. (www.securitesociale.be)

- Vous allez devoir créer un fichier de signature (FS) sur base de votre certificat qualifié (extension .pfx ou .p12) pour chaque fichier de déclaration (FI). Vous allez devoir placer votre fichier de signature avec votre fichier de déclaration (FI) sur le serveur SFTP.

Remarques:
Lors du choix du certificat digital qualifié, il est important de tenir compte de la manière dont vous allez fabriquer vos fichiers de signature (FS) :

Vous pouvez créer votre fichier de signature vous-même via par exemple OpenSSL ou vous pouvez utilisez un programme d'une maison de soft ou le développer vous-même.

Si vous souhaitez créer le fichier de signature via OpenSSL, il est important de demander à votre prestataire de services de certification un certificat ou vous pouvez exporter la clé privée. Pour les certificats qui se trouvent sur une carte à puce ou sur une clé USB cela pose un problème.

2.2 Un client SFTP.

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

Vous travaillez avec Windows:

Les ordinateurs Windows ne disposent pas d'un client SFTP standard.
Vous pouvez utiliser un moteur de recherche et effectuer une recherche sur 'SFTP Client'. Vous trouverez, parmi les résultats des clients software SFTP gratuits et payants.
Certains clients SFTP fonctionnent de manière manuelle, d'autres peuvent être automatisés.
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 d'une implémentation open source de SSH (OpenSSH).

Vous travaillez avec Apple:

Il existe également plusieurs 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.

Documentation:

À titre informatif, vous trouverez dans la bibliothèque technique (https://www.socialsecurity.be/public/doclibrary/fr/batch.htm) de la documentation sur les clients SFTP manuels que nous avons nous-mêmes testés.

2.3 Une paire de clés

Pour effectuer un envoi via SFTP, vous avez besoin d'une paire de clés SSH. Vous devez la créer vous-même.
Dans certains clients SFTP est compris un générateur de clé.
Si le client que vous avez choisi ne dispose pas d'un générateur de clé, vous devrez créer les clés via un autre générateur de clés que vous pouvez trouver facilement via une recherche sur internet. Le programme Putty Key Generator fonctionne très bien. Vous pouvez le retrouver en utilisant « puttygen » dans un moteur de recherche.
Votre clé publique doit être chargée lors de l'ouverture du canal SFTP sur le portail de la sécurité sociale.
Votre clé privée doit être chargé dans le client sftp que vous utilisez. Veuillez pour cette action consulter la documentation de votre client SFTP. Il est conseillé de protéger votre clé privée avec un mot de passe.

Spécifications:

Les clés compatibles avec SSH v2
Les formats OpenSSH et SSH sont acceptés
Type de clé : SSH2-RSA
Longueur de clé : de 2048 à 4096 bits.

2.4 Un numéro d'expéditeur et un canal SFTP actif.

Pour envoyer des messages structurés par SFTP vous devez disposer pour chaque qualité pour laquelle vous souhaitez envoyer d'un numéro d'expéditeur et d'un canal SFTP actif.

Seul le gestionnaire local ou le co-gestionnaire local de chaque qualité peut enregistrer un numéro d'expéditeur et ouvrir un canal sur www.securitesociale.be. Ci-dessous les étapes à parcourir :

1. Cliquer sur **Messages structurés(*)**
2. Cliquer sur **Enregistrement des données de configuration**
3. Cliquer sur **Suivant**
4. Remplir les données d'identification de l'utilisateur technique
5. Cliquer sur **Suivant**
6. Choisir le type de canal **SFTP et enregistrer la clé publique** que vous avez créée dans votre client SFTP.
7. Cliquer sur **Suivant**
8. Charger la **clé publique** de votre certificat qualifié (extension .cer)
9. Choisir dans la liste les **applications** pour lesquelles vous souhaitez utiliser le canal
10. Cliquer sur **Suivant**
11. Introduire le **nom d'utilisateur** de l'utilisateur technique (**)
12. Cliquer sur **Suivant**
13. Cliquer sur **Confirmer.**

(*) Si vous disposez déjà d'un canal actif vous pouvez sauter les étapes 2 à 5 et vous cliquez à l'étape 6 à droite de votre écran sur l'icône + à coté de SFTP.

(**) Si vous disposez déjà d'un canal MQLink avec dial-up ou d'un canal FTP vous ne devrez plus choisir le nom d'utilisateur technique pour le canal SFTP car le nom d'utilisateur technique choisi pour FTP et/ou MQLink sera le même pour le canal SFTP. Dans ce cas vous ne recevrez donc pas cet écran et vous pouvez continuer vers le point 13.

3. Quels fichiers doivent être joints aux messages structurés ?

Deux fichiers doivent toujours être ajoutés aux messages structurés que vous souhaitez transférer à l'ONSS ou à l'ONSSAPL par SFTP :

- Le fichier signature
- Le fichier GO

3.1 Le fichier signature (FS)

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

Vous pouvez créer votre fichier de signature (FS) vous-même via par exemple OpenSSL ou vous pouvez utiliser un programme d'une maison de soft ou le développer vous-même.

Si vous souhaitez créer le fichier de signature via OpenSSL, il est important de demander à votre prestataire de services de certification un certificat ou vous pouvez exporter la clé privée. Pour les certificats qui se trouvent sur une carte à puce ou sur une clé USB cela pose un problème.

Si vous voulez créer un fichier de signature avec l'eID, vous pouvez utiliser l'application Belgian eID Signer ou une procédure avec Cryptonit. L'application et la procédure se trouvent dans la bibliothèque technique : (https://www.socialsecurity.be/public/doclibrary/fr/batch.htm).

Comment générer le fichier de signature par OpenSSL

Pour créer un fichier de signature avec OpenSSL il faut d'abord installer ce software sur le PC sur lequel vous allez créer le fichier de signature.
Via un moteur de recherche, vous pouvez rechercher très simplement OpenSSL.

Après l'installation, le mieux est que vous fabriquez un répertoire sur votre PC dans lequel vous installez votre certificat (format .pfx place ou .p12) et votre fichier de déclaration (FI).

1. Ouvrez une fenêtre dos. Allez sur Start et cliquez sur **Run**
2. Tapez **cmd** et cliquez sur 'OK'
3. Ensuite vous devez aller vers C-prompt (c.a.d. une ligne ou vous n'avez que '**C:\ >**')
   Pour y arriver vous devez taper plusieures fois **cd..** suivi de la touche [ENTER]
4. Ouvrez le répertoire OpenSSL via la commande **cd openssl** puis cliquez sur [ENTER]
5. Ouvrez le sous-répertoire bin via la commande **cd bin** puis cliquez sur [ENTER]
6. Ouvrez OpenSSL via la commande **openss**l puis cliquez sur [ENTER]

7. Après ce prompt vous devez introduire la commande pour créer **le fichier .pem**. Attention, vous devez ici utiliser votre certificat format .pfx ou .p12 et non pas la clé publique du certificat (.cer).
   Vous introduisez la commande suivante avec le chemin complèt du répertoire ou se trouve le certificat et le fichier FI à signer: **pkcs12 -in** Localisation de votre répertoire****votre certificat **-passin pass:** Mot de passe de votre certificat **-out** Localisation de votre répertoire****Nom de votre fichier.PEM-**clcerts -nokeys** puis cliquez sur [ENTER]
8. Vous introduisez maintenant la commande pour créer votre **fichier .key** suivante dans le prompt OpenSSL: **pkcs12 -in** Localisation 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** Localisation de votre répertoire****Nom de votre fichier.KEY puis cliquez sur [ENTER]
9. Vous pouvez maintenant créer votre **fichier FS** en introduisant les commandes suivantes dans le prompt OpenSSL: **smime -sign -in** Localisation de votre répertoire****Nom du fichier FI **-signer** Localisation de votre répertoire****Nom de votre fichier .PEM **-inkey** Localisation de votre répertoire****Nom de votre fichier.KEY **- passin pass:** Mot de passe que vous avez choisi pour le .KEY **-outform PEM -out** Localisation de votre répertoire****Nom du fichier FS puis cliquez sur [ENTER]
10. Avant d'envoyer votre fichier, il y a encore quelques adaptations manuelles à faire dans le fichier FS.
    Vous ouvrez le fichier FS avec un éditeur de texte comme Textpad ou Notepad et vous supprimez la première ligne (-----DÉBUT PKCS7-----) ainsi que la dernière ligne (-----END PKCS7-----) et également des lignes vierges à la fin du texte (retour chariot).

Structure du nom du fichier de signature

FS.application.numéro d'expéditeur.date.le numéro d'ordre.l'environnement de travail.le nombre de parties.le numéro de la partie
Ex. FS.DMFA.101380.20100920.00001.T.1.1

Attention: Lorsqu'une déclaration (FI) est transférée en différentes parties, un fichier de signature (FS) devra être ajouté à chaque partie du fichier.

3.2 Le fichier GO

Tout fichier de données échangé est accompagné d'un fichier GO. Cela permet de déterminer si le transfert du fichier de données est terminé.

Vous pouvez créer un fichier GO en sauvant en fichier vide avec le nom de fichier correct.

Structure du nom du fichier GO:

GO.application.numéro d'expéditeur.date.le numéro d'ordre.l'environnement de travail.le nombre de partie(s)
Ex: GO.DMFA.101380.20100920.00001.T.1

Attention : lorsqu'une déclaration est transférée en différentes parties, un seul fichier GO est ajouté.

4. Comment transférer un message structuré?

4.1 Paramétrer un client SFTP

Pour faire la liaison entre le serveur SFTP de la sécurité social (host) vous devez introduire les données ci-dessous dans votre client SFTP(*).

- Le nom du host est:'**sftp.socialsecurity.be**'
- Le numéro de porte est: '**8022**'
- Le **nom d'utilisateur** (commence par **EXP**) que vous avez choisi lors de la création de votre canal SFTP sur le portail de la sécurité sociale. (Si vous aviez déjà par le passé un nom d'utilisateur technique, il est possible que celui-ci commence par **UM**).
- Chargez la clé privée, que vous avez créé dans le générateur de clé, dans votre client SFTP.
- Lors de la première connexion vous devez **accepter** la clé publique (également appelée **host-key**) du serveur SFTP de la sécurité sociale
- Si vous avez protégé votre **clé privée** par un **mot de passe**, le client SFTP va le demander.

4.2 Transférer des fichiers

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

- Les fichiers de productions DmfA, DRS, Dimona, Chômage Temporaire, Déclaration Unique de Chantier (extension **R**) -> dans le répertoire **IN**
- Tests / fichiers de simulations DRS, Dimona, Chômage Temporaire, Déclaration Unique de Chantier et fichiers test de circuit DmfA (extension **T**) -> dans le répertoire **INTEST**
- Les fichiers test de déclaration DmfA (extension **S**) -> dans le répertoire **INTEST-S**

4.3 Récupérer des fichiers

Dès que les déclarations sont traitées, vous retrouvez les réponses (ACRF, Notifications.) dans les répertoires respectifs :

- Les fichiers de productions DmfA, DRS, Dimona, Chômage Temporaire, Déclaration Unique de Chantier (extension **R**) -> dans le répertoire **OUT**
- Tests / fichiers de simulations DRS, Dimona, Chômage Temporaire, Déclaration Unique de Chantier et fichiers test de circuit DmfA (extension **T**) -> dans le répertoire **OUTTEST**
- Les fichiers test de déclaration DmfA (extension **S**) -> dans le répertoire **OUTTEST-S**

Le but est que vous copiez les fichiers qui sont sur notre serveur vers un endroit sur votre PC. Ensuite, une fois copié, vous supprimez les fichiers des répertoires OUT sur notre serveur.

Etant donné que nous devons prévoir de l'espace pour tous les expéditeurs, nous ne pouvons pas garder les fichiers à disposition de manière indéterminée.