Envoi de messages structurés par le canal SFTP

Foire aux Questions (FAQ)

Généralités

Qu'est-ce que SFTP ?

SFTP signifie SSH File Transfer Protocol ou Secure File Transfer Protocol. SFTP est le composant de ce protocole SSH qui assure le transfert de fichiers.

Où trouver SFTP ?

Contrairement à FTP, les ordinateurs Windows ne disposent pas d'un client standard. Vous devez donc pour cela installer un logiciel supplémentaire.

Par un moteur de recherche (ex : chercher sur 'SFTP Client'), vous trouverez sur Internet des clients software SFTP gratuits et payants. Les systèmes Linux proposent des packages standard d'une implémentation open source de SSH (OpenSSH).

Protection de SFTP

SFTP est 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.

Quelles étapes spécifiques faut-il parcourir pour utiliser SFTP ?

1. Vous devez disposer d'un accès aux applications sécurisées sur le site portail de la sécurité sociale.
2. Vous devez posséder un client SFTP de votre choix.
3. Vous devez générer une paire de clés à l'aide de ce client. (clés publique et privée)
4. Votre (co-)gestionnaire local se connecte sur le site portail et, au niveau de la gestion des messages structurés, il/elle doit indiquer le canal SFTP.
5. Le (co-)gestionnaire local doit enregistrer la clé publique que vous avez créée dans votre client SFTP et la clé publique de votre certificat qualifié.

Comment s'enregistrer comme expéditeur SFTP ?

Pour envoyer des messages structurés, vous devez d'abord créer un numéro d'expéditeur pour chaque qualité pour laquelle vous souhaitez envoyer des déclarations.

Seul le gestionnaire local ou le co-gestionnaire local de chaque qualité peut enregistrer un numéro d'expéditeur.
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 userid de l'utilisateur technique
12. Cliquer sur Suivant
13. Cliquer sur Confirmer.

(*) Si vous avez déjà un canal (Isabel) ouvert, passez directement à l'étape 6.

Nom d'utilisateur et mot de passe

Lors de l'activation du canal SFTP pour votre numéro d'expéditeur, votre (co)gestionnaire local devra choisir un nom d'utilisateur sur le site portail. Pour effectuer un envoi via SFTP, vous ne devez pas créer de mot de passe.

Certificats

Comment créer la paire de clés (clé privée + clé publique)?

SFTP possède 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. Si le client SFTP que vous avez choisi n'en possède pas, il faut que vous téléchargiez un générateur de clés sur Internet.

Par un moteur de recherche (ex : chercher sur 'SSH key generator), vous trouverez sur Internet des programmes pour générer la paire de clés.

La partie privée de cette clé doit être localisée dans votre client SFTP. La localisation de la clé privée dépend du client SFTP que vous utilisez. Veuillez pour cela consulter la documentation de votre client SFTP.

Quelle version des clés faut-il créer ?

Il est opéré une distinction entre les clés compatibles avec la version 1 du SSH et les clés compatibles avec la version 2. La version 1 est considérée comme non sûre et ne sera pas acceptée. Uniquement la version 2 est acceptée.

Pour les clés publiques, seuls les formats de OpenSSH et SSH sont supportés.

Lors de la génération des clés, vous devez veiller à choisir les bons type et longueur de clé.

Il y a deux types possibles (RSA et DSA), dont seul RSA est accepté.

Comme longueur de clé, choisissez 2048 ou plus (3072, 4096). Les clés plus courtes ne sont pas acceptées.

Il est conseillé de protéger la clé privée avec un mot de passe lors de la sauvegarde de ces clés.

En bref :

- Clés compatibles avec SSH v2
- Formats OpenSSH et SSH
- Type de clé : RSA
- Longueur de clé : 2048<la longueur<4096

La longueur de la clé SSH n'est pas correcte

La longueur de la clé doit être d'au moins 2048 bits et ne peut dépasser 4096 bits. Les clés plus courtes ou plus longues sont refusées. La solution consiste à créer une nouvelle paire de clés avec une longueur comprise entre 2048 et 4096 bits.

La clé SSH est invalide

Cette erreur peut avoir plusieurs causes :

- Vous avez tenté de charger votre clé privée au lieu de votre clé publique. **Solution** : chargez votre clé publique.
- Vous avez créé votre clé publique dans un mauvais format (par exemple : SSH1-RSA ou SSH2-DSA). **Solution** : créez vos clés au format SSH2-RSA.

Transférer la clé publique

Votre (co)gestionnaire local doit charger votre clé SSH publique avec votre numéro d'expéditeur sur le site portail.

Envoi de messages

Comment envoyer un message structuré ?

1. Etablissez par votre client SFTP une connexion avec sftp.socialsecurity.be (la première fois, vous devez accepter la clé publique du serveur).
2. Identifiez-vous avec votre nom d'utilisateur technique(UMxxxxxx ou EXPxxxxxx) et votre clé privée SSH, en saisissant le mot de passe qui protège votre clé, si vous l'avez protégée.
3. Placez vos fichiers dans le répertoire IN (les fichiers test de circuit dans le répertoire INTEST, les fichiers test de déclaration dans le répertoire INTEST-S).

Après traitement et contrôle de vos fichiers, des fichiers d'acceptation (ACRF) et de notification sont créés dans le répertoire OUT (les fichiers test de circuit dans le répertoire OUTTEST, les fichiers test de déclaration dans le répertoire OUTTEST-S).

Limite de taille des fichiers

Pour des raisons liées au contrôle de la signature, il y a une limite de 200MB par fichier.

Quels fichiers ajouter aux messages structurés ?

Lors de l'envoi par SFTP, vous devez ajouter un fichier de signature (Fichier FS) et un Fichier GO à votre fichier de déclaration (Fichier FI).

Les messages structurés via SFTP sont les mêmes que pour Isabel

Les fichiers de déclaration (fichiers FI) sont identiques pour chaque canal d'envoi utilisé. Tant la structure que la dénomination des fichiers restent identiques.

Connexions

Utilisation de SFTP par leased line

Ce n'est pas prévu dans une première phase. Il est possible, mais pas certain, que ce soit possible dans une deuxième phase.

Host

Le nom du host est sftp.socialsecurity.be
Le port est 8022

Comment configurer votre client SFTP ?

1. Saisissez le nom du host dans sftp.socialsecurity.be
2. Saisissez le port 8022
3. Introduisez le nom d'utilisateur de l'utilisateur technique
4. Chargez votre clé SSH privée