Startup guide van het transferkanaal SFTP

Versie 10

Inhoudsopgave

1. Wat is SFTP?

SFTP staat voor **SSH File Transfer Protocol** of **Secure File Transfer Protocol**.

Zoals de eerste beschrijving aangeeft, maakt het deel uit van SSH of Secure Shell. Dit is een veilige vervanger voor het opzetten van een terminalsessie op UNIX-machines. SFTP is de component van dit SSH-protocol die instaat voor bestandstransfer.

Een SFTP-client gedraagt zich zoals een klassieke FTP-client, waarbij u zicht hebt op directories en bestanden en met dezelfde commando's als FTP bestanden kan plaatsen, ophalen…

Anders dan bij FTP beschikken Windows-computers niet over een standaardclient. U dient hiervoor dus **extra software** te installeren. Er bestaan zowel gratis als betalende SFTP-softwareclients. Linux-systemen bieden standaardpakketten aan van een open source implementatie van SSH (OpenSSH).

SFTP is echter een volledig ander protocol dan FTP. Het wordt immers beschermd door middel van **cryptografische technieken**. Dit betekent dat alle verkeer tussen een client en een server volledig versleuteld verloopt, van het aanmeldingsproces tot en met de verzending van bestanden. Gezien deze bescherming is SFTP dan ook heel geschikt voor de **beveiligde** uitwisseling van bestanden over het **internet**.

Er zijn een aantal vereisten om zich als gebruiker aan te melden via SFTP. Uiteraard beschikt u steeds over een **gebruikersnaam**. Daarnaast vervangt een elektronisch sleutelpaar het klassieke wachtwoord. Dit sleutelpaar bevat een **private en publieke sleutel**. De private sleutel blijft bij degene die hem heeft aangemaakt en wordt het best nog beschermd door middel van een extra wachtwoord. De publieke sleutel kan naar elke tegenpartij gestuurd worden die de bezitter van de private sleutel wenst te identificeren.

Dit systeem lijkt heel sterk op het X.509-systeem (zoals dat van de elektronische identiteitskaart) waar met private sleutels en certificaten wordt gewerkt. De onderliggende principes zijn dezelfde maar SFTP werkt zelden met certificaten. SFTP heeft dus zijn eigen formaat van sleutels. Deze sleutels kan u niet aankopen zoals een certificaat maar dient u **zelf aan te maken**. De meeste SFTP-clients beschikken over een functie om dit sleutelpaar aan te maken.

Net zoals de client beschikt elke **SFTP-server** ook over een sleutelpaar. Bij het maken van een verbinding met een server zal deze zijn publieke sleutel (ook wel host key genoemd) doorgeven aan de client. Het is dan aan de eindgebruiker om deze sleutel te aanvaarden. Vanaf dit punt kan de beveiligde verbinding worden opgebouwd en kan de gebruiker zich aanmelden.

De identificatie gebeurt op basis van een gebruikersnaam en een private sleutel.

2. Wat heeft u nodig?

- Een internetverbinding
- Een gekwalificeerd digitaal certificaat
- Een SFTP-client
- Een SSH-sleutelpaar
- Een verzendernummer

2.1 Een gekwalificeerd digitaal certificaat

Elk aangiftebestand dat u via SFTP verzendt moeten vergezeld zijn door een handtekeningbestand. Om dit handtekeningbestand aan te maken heeft u een gekwalificeerd digitaal certificaat nodig.

U kan kiezen tussen:

1. Het handtekeningcertificaat van uw elektronische identiteitskaart (http://eid.belgium.be/nl/)

2. Een gekwalificeerd digitaal certificaat van deze certificatiedienstverlener:
   GlobalSign: PersonalSign 3 pro
   (https://www.globalsign.eu/personalsign/personalsign3-pro/)

U zal uw gekwalificeerd digitale certificaat voor 2 acties moeten gebruiken.

- U zal de publieke sleutel van uw gekwalificeerd digitaal certificaat (met de extensie .cer) moeten opladen bij het aanmaken van uw SFTP-kanaal op de portaalsite van de sociale zekerheid (www.socialezekerheid.be).

- U zal op basis van uw gekwalificeerd certificaat (extensie .pfx of.p12) en voor elk aangiftebestand (FI) een handtekeningbestand (FS) moeten aanmaken dat u samen met uw aangiftebestand op de SFTP-server plaatst.

Opmerking:
Bij de keuze van een gekwalificeerd digitaal certificaat is het belangrijk om rekening te houden met de wijze waarop u uw handtekeningbestanden (FS) gaat aanmaken:

U kan uw handtekeningbestand zelf aanmaken via bijvoorbeeld OpenSSL of u kan gebruik maken van programma's die door softwareproducenten of door u zelf zijn ontwikkeld.

Indien u het handtekeningbestand via OpenSSL wenst te aan te maken is het belangrijk dat u aan uw certificatiedienstverlener een certificaat vraagt waarvan u de private sleutel kan exporteren. Bij certificaten die zich op chipkaarten of USB-sleutels bevinden vormt dit een probleem.

2.2 Een SFTP-client

Om te kunnen communiceren met onze SFTP-server heeft u een SFTP-client nodig.

U werkt met Windows:

Windows-computers hebben geen standaard SFTP-client.
U kan via een zoekmachine met bijvoorbeeld als zoekterm “SFTP Client” een SFTP-client vinden. Er zijn verschillende soorten SFTP-clients beschikbaar. Sommige zijn gratis, voor andere dient u te betalen. Sommige SFTP-clients vereisen manuele handelingen en andere zijn automatiseerbaar.
U kan zelf vrij kiezen welke SFTP-client het best aan uw noden voldoet.

U werkt met Linux:

Linux-systemen bieden standaardpakketten aan van een open source implementatie van SSH (OpenSSH).

U werkt met Apple:

Voor Apple bestaan ook verschillende SFTP-clients. U kan ze vinden via een zoekmachine met bijvoorbeeld als zoekterm “SFTP Client & Apple” of op de site www.apple.com.

Documentatie:

Ter informatie vindt u in de technische bibliotheek (https://www.socialsecurity.be/public/doclibrary/nl/batch.htm) documentatie over de manuele SFTP-clients die we zelf getest hebben.

2.3 Een sleutelpaar

Voor verzending via SFTP heeft u een SSH-sleutelpaar nodig. Dit zal u zelf moeten aanmaken.
Sommige SFTP-clients bevatten een sleutelgenerator.
Indien de SFTP-client die u kiest niet over een sleutelgenerator beschikt kan u gebruik maken van een apart programma om de sleutels aan te maken. Het programma Putty Key Generator is hiervoor geschikt. U kan dit vinden via een zoekmachine met als zoekterm “puttygen”
Uw publieke sleutel moet u opladen bij de aanmaak van uw SFTP-kanaal op het portaal van de sociale zekerheid.
Uw private sleutel moet u opladen in de SFTP-client die u gebruikt. Gelieve hiervoor de documentatie van de SFTP-client te raadplegen. Het is aangeraden om uw private sleutel te beveiligen met een wachtwoord.

Vereisten:

- Sleutels compatibel met SSH v2
- De formaten OpenSSH en SSH worden aanvaard
- Sleuteltype: SSH2-RSA
- Sleutellengte: van 2048 t.e.m. 4096 bits.

2.4 Een verzendernummer en een actief SFTP-kanaal

Om gestructureerde berichten via SFTP te kunnen versturen moet u beschikken over een verzendernummer en een actief SFTP-kanaal voor elke hoedanigheid waarvoor u wenst te verzenden.

Enkel de (co-)lokale beheerder van elke hoedanigheid kan een verzendernummer registreren en een kanaal activeren op www.socialezekerheid.be. Dit zijn de stappen die ze moeten doorlopen:

1. Klik op **Gestructureerde berichten(*)**
2. Klik op **De configuratiegegevens opslaan**
3. Klik op **Volgende**
4. Vul de identificatiegegevens van de technische gebruiker in
5. Klik op **Volgende**
6. Kies het kanaaltype **SFTP** en laad de in uw SFTP-client aangemaakte **publieke sleutel** op
7. Klik op **Volgende**
8. **Laad** de **publieke sleutel** van uw gekwalificeerd certificaat (extensie .cer) **op**
9. Duid in de lijst de toepassingen aan waarvoor u via SFTP wenst te verzenden
10. Klik op **Volgende**
11. Kies een **gebruikersnaam** voor de technische gebruiker(**)
12. Klik op **Volgende**
13. Klik op **Bevestigen**

(*) Indien u reeds een ander kanaal heeft slaat u stappen 2 t.em. 5 over en klikt u bij punt 6 op het plusteken naast SFTP.

(**)Indien u in het verleden reeds een FTP-kanaal of een MQLink-kanaal met dial-up heeft aangemaakt zal u dit scherm niet krijgen en dus geen technische gebruikersnaam moeten kiezen aangezien de technische gebruikersnaam die voor FTP en/of MQLink werd gekozen ook van toepassing blijft voor SFTP. Ga verder naar punt 13.

3. Welke bestanden toevoegen aan de gestructureerde berichten?

Twee bestanden moeten toegevoegd worden aan de gestructureerde berichten die u via SFTP naar de RSZ(PPO) stuurt:

- Het handtekeningbestand (FS)
- Het GO-bestand

3.1 Het handtekeningbestand (FS)

Het handtekeningbestand wordt toegevoegd aan een bestand dat de originele aangiften, de wijzigende aangiften en de consultatieaanvragen bevat. Indien deze bestanden in de testomgeving werden aangemaakt, zal er geen enkel handtekeningbestand toegevoegd moeten worden.

U kan het handtekeningbestand (FS) zelf aanmaken via bijvoorbeeld OpenSSL of gebruik maken van programma's die door softwareproducenten of door u zelf zijn ontwikkeld.

Indien u het handtekeningbestand via OpenSSL wenst te aan te maken is het belangrijk dat u aan uw certificatiedienstverlener een certificaat vraagt waarvan u de private sleutel kan exporteren. Bij certificaten die zich op chipkaarten of USB-sleutels bevinden vormt dit een probleem.

Indien u met de eID een handtekeningbestand wenst aan te maken kan u gebruik maken van de toepassing Belgian eID Signer of een procedure met behulp van Cryptonit. U kan de toepassing en de procedure vinden in de technische bibliotheek:
(https://www.socialsecurity.be/public/doclibrary/nl/batch.htm).

Hoe een handtekeningbestand aanmaken via OpenSSL?

Om een handtekeningbestand aan te maken met OpenSSL dient eerst deze sofware te installeren op de PC waarop u het handtekeningbestand gaat aanmaken.
Via een zoekmachine kan heel eenvoudig gezocht worden naar OpenSSL.

Na installatie maakt u best een map aan op uw PC waarin u uw certificaat (formaat .pfx of .p12) en uw te ondertekenen FI-bestand(en) plaatst.

1. Open een dos-venster. Ga hiervoor naar Start en klik op **Run**
2. Typ **cmd** in en klik op 'OK'
3. Vervolgens moet u naar de C-prompt gaan (dit betekent dat u een lijn heeft waar enkel 'C:\>' staat)
Om daar te komen moet u verschillende keren het commando **cd..** gevolgd door de [ENTER]-toets invoeren.
4. Open de directory OpenSSL via het commando **cd openssl** gevolgd door [ENTER]
5. Open de subdirectory bin via het commando **cd bin** gevolgd door [ENTER]
6. Open OpenSSL via het commando **openss**l gevolgd door [ENTER]

7. Na de prompt moet u het commando om het **.pem bestand** aan te maken invoeren. Opgelet u moet hierbij gebruik maken van uw certificaat (formaat .pfx, .p12) en niet van de publieke sleutel van het certificaat (.cer)
U geeft volgend commando met het volledige pad waar uw map met het certificaat en uw te ondertekenen FI-bestand staat in achter de prompt: **pkcs12 -in** LOCATIE VAN UW MAP****UW CERTIFICAAT **-passin pass:**WACHTWOORD VAN UW CERTIFICAAT **-out** LOCATIE VAN UW MAP ****NAAM VAN UW .PEM-BESTAND **-clcerts -nokeys** gevolgd door [ENTER]
8. Nu geeft u om uw **.key-bestand** aan te maken volgend commando in na de prompt OpenSSL> : **pkcs12 -in** LOCATIE VAN UW MAP****UW CERTIFICAAT **-passin pass:**WACHTWOORD VAN UW CERTIFICAAT **-passout pass:**WACHTWOORD DAT U KIEST VOOR UW .KEY **-out** LOCATIE VAN UW MAP****NAAM VAN UW .KEY-bestand gevolgd door [ENTER]
9. Om nu uw **FS-bestand** aan te maken geeft u volgend commando in na de prompt OpenSSL> : **smime -sign -in** LOCATIE VAN UW MAP****NAAM VAN UW FI-BESTAND **-signer** LOCATIE VAN UW MAP****NAAM VAN UW .PEM-bestand **-inkey** LOCATIE VAN UW MAP****NAAM VAN UW .KEY-BESTAND **- passin pass:** WACHTWOORD DAT U KIEST VOOR UW .KEY **-outform PEM -out** LOCATIE VAN UW MAP ****NAAM VAN UW FS-BESTAND gevolgd door [ENTER]
10. Voor u het bestand kan versturen moet u nog enkele manuele aanpassingen aan uw FS-bestand doen.
U opent het FS-bestand met een teksteditor zoals Textpad, Notepad of Wordpad en verwijdert de eerste (-----BEGIN PKCS7-----)en de laatste lijn (-----END PKCS7-----) inclusief de eventuele blanco lijnen ten gevolge van ENTER (carriage return).

Structuur van de naam van een FS-bestand:
FS.toepassing.verzendernummer.datum.volgnummer.werkomgeving.aantal delen.nummer van het deel
Bv. FS.DMFA.101380.20100920.00001.T.1.1

Let op: wanneer een aangifte in meerdere delen opgestuurd wordt, zal een handtekeningbestand aan elk deel van het bestand toegevoegd worden.

3.2 Het GO-bestand

Elk uitgewisseld gegevensbestand wordt vergezeld van een GO-bestand. Dit geeft aan dat de transfer van het gegevensbestand afgerond is.

Een GO-bestand maakt u door een leeg bestand te openen en dit te bewaren met de correcte bestandsnaam.

Structuur van de naam van een GO-bestand:
GO.toepassing.verzendernummer.datum.volgnummer.werkomgeving.aantal delen
Bv. GO.DMFA.101380.20100920.00001.T.1

Let op: wanneer een aangifte in meerdere delen opgestuurd wordt, wordt er slechts één GO-bestand toegevoegd.

4. Hoe een gestructureerd bericht overmaken?

4.1 Instellen van de SFTP-client

Om verbinding te maken met de SFTP-server (host) van de sociale zekerheid moet u onderstaande gegevens instellen in uw SFTP-client:

- De naam van de host in: '**sftp.socialsecurity.be**'
- Het poortnummer in: '**8022**'
- De **gebruikersnaam** (begint met EXP) die u gekozen heeft bij het aanmaken van uw SFTP-kanaal op het portaal van de sociale zekerheid. (Indien u in het verleden reeds een technische gebruikersnaam heeft aangemaakt kan het zijn dat deze met UM begint.)
- Laad uw **private SSH-sleutel** in uw SFTP-client op indien u deze in een aparte sleutelgenerator heeft aangemaakt
- De eerste keer dat u zich aanmeldt zal u de publieke sleutel (**host-key**) van de SFTP-server van de sociale zekerheid moeten **aanvaarden**.
- Indien u uw **private sleutel** heeft beschermd met een **wachtwoord** zal uw SFTP-client ook vragen om dit wachtwoord op te geven.

4.2 Bestanden plaatsen

Open in uw SFTP-client de map waarin u uw bestanden wenst te plaatsen.

- Productiebestanden DmfA, ASR, Dimona, Tijdelijke Werkloosheid en Unieke Werfmelding (extensie **R**) -> map **IN**
- Test-/Simulatiebestanden ASR, Dimona, Tijdelijke Werkloosheid en Unieke Werfmelding en DmfA-circuittestbestanden (extensie **T**) -> map **INTEST**
- DmfA-aangiftetestbestanden (extensie **S**) -> map **INTEST-S**

4.3 Bestanden ophalen

Van zodra de aangiftes verwerkt zijn zal u de antwoorden (ACRF's, Notificaties, ..) terugvinden in de respectievelijke mappen :

- Productiebestanden DmfA, ASR, Dimona, Tijdelijke Werkloosheid en Unieke Werfmelding (extensie **R**) -> map **OUT**
- Test-/Simulatiebestanden ASR, Dimona, Tijdelijke Werkloosheid en Unieke Werfmelding en DmfA-circuittestbestanden (extensie **T**) -> map **OUTTEST**
- DmfA-aangiftetestbestanden (extensie **S**) -> map **OUTTEST-S**

Het is de bedoeling dat u de bestanden in deze mappen kopieert naar een plaats op een server of PC bij u, en de gekopieerde bestanden vervolgens wist uit de OUT-mappen op onze server.

Aangezien wij ruimte moeten voorzien voor alle verzenders kunnen wij de uitgaande bestanden niet onbeperkt ter beschikking houden.