Verzending van gestructu-reerde berichten via SFTP

Veel gestelde vragen (FAQ)

Algemeen

Wat is SFTP ?

SFTP staat voor SSH File Transfer Protocol of Secure File Transfer Protocol en maakt deel uit van SSH of Secure Shell. SFTP is de component van dit SSH-protocol die instaat voor bestandstransfer.

Waar vindt u SFTP ?

Anders dan bij FTP beschikken Windows-computers niet over een standaardclient. U dient hiervoor dus extra software te installeren.

Via een zoekrobot (bijvoorbeeld zoeken op 'SFTP Client') vindt u op het internet zowel gratis als betalende SFTP-softwareclients. Linux-systemen bieden standaardpakketten aan van een open source implementatie van SSH (OpenSSH).

Is SFTP veilig ?

SFTP wordt 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.

Welke specifieke stappen moet u doorlopen om SFTP te gebruiken ?

1. U dient te beschikken over toegang tot de beveiligde toepassingen op de portaalsite van de sociale zekerheid.
2. U dient over een SFTP-client naar keuze te beschikken.
3. U maakt in uw SFTP-client een sleutelpaar aan (private en publieke sleutel)
4. Uw (co-)lokale beheerder meldt zich aan op de portaalsite en kiest bij Toegangsbeheer voor beheer van gestructureerde berichten waar hij/zij het kanaal SFTP kan aanduiden.
5. Hij/zij laadt de in uw SFTP client aangemaakte publieke sleutel en de publieke sleutel van uw gekwalificeerd certificaat op.

Hoe kan u zich registreren als SFTP-verzender ?

Om gestructureerde berichten te kunnen versturen, moet u eerst een verzendernummer aanmaken voor elke hoedanigheid waarvoor u wenst te verzenden.

Enkel de (co-)lokale beheerder van elke hoedanigheid kan een verzendernummer registreren. 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 Isabelkanaal heeft slaat u stappen 2 t.em. 5 over en klikt u bij punt 6 aan de rechterkant van uw scherm op het plusteken naast SFTP.

Welke gebruikersnaam en wachtwoord moet u gebruiken om via SFTP te verzenden ?

Bij het activeren van het SFTP-kanaal voor uw verzendernummer zal uw (co-)lokale beheerder op de portaalsite een gebruikersnaam moeten kiezen. Voor de verzending via SFTP moet u geen wachtwoord aanmaken.

Certificaten

Hoe een sleutelpaar (private & publieke sleutel) aanmaken ?

SFTP heeft zijn eigen formaat van sleutels. Deze sleutels kan u niet aankopen zoals een certificaat maar dient u zelf te aan te maken. Vrijwel elke SFTP-clientsoftware laat toe om een SSH-sleutelpaar aan te maken. Indien de SFTP-client die u gekozen heeft geen module bevat om sleutels aan te maken kan u van het internet een programma om sleutels aan te maken downloaden. Via een zoekrobot (bijvoorbeeld zoeken op 'ssh key generator') vindt u op het Internet programma's waarmee u de SSH-sleutels kan aanmaken.

Het publieke deel van uw sleutel dient u op te laden bij uw verzendernummer op de portaalsite van de sociale zekerheid.

Het private deel van deze sleutel dient u op te laden in uw SFTP-client. De locatie van de private sleutel hangt af van de SFTP-client die u gebruikt. Gelieve hiervoor de documentatie van uw SFTP-client te raadplegen.

Welke versie sleutelpaar aanmaken ?

Er wordt een onderscheid gemaakt tussen sleutels die compatibel zijn met versie 1 van SSH en deze die compatibel zijn met versie 2. Versie 1 wordt als onveilig beschouwd en zal niet aanvaard worden. Enkel versie 2 wordt aanvaard.

Voor de publieke sleutels zullen enkel de formaten van OpenSSH en SSH ondersteund worden.
Bij de aanmaak van de sleutels dient u op te letten dat u het juiste type sleutel en de juiste sleutellengte kiest.

Er zijn twee mogelijke types (RSA en DSA) waarvan enkel RSA zal aanvaard worden.

Als sleutellengte kiest u 2048 of hoger (3072, 4096). Kortere sleutels zullen niet aanvaard worden.

Bij de opslag van deze sleutels raden we u aan de private sleutel te beschermen met een wachtwoord.

Kort samengevat:

- Sleutels compatibel met SSH v2
- Formaten OpenSSH en SSH
- Sleuteltype: RSA,
- Sleutellengte: 2048<lengte<4096

Wat betekent de fout 'De ssh-sleutel heeft niet de correcte lengte' bij het aanmaken van een verzendernummer voor SFTP ?

De sleutellengte moet minimaal 2048 bits lang zijn en mag niet langer zijn dan 4096 bits. Kortere of langere sleutels worden niet aanvaard. De oplossing is een nieuw sleutelpaar aan te maken met een lengte van 2048 t.e.m. 4096 bits

Wat betekent de fout 'De ssh-sleutel is ongeldig' bij het aanmaken van een verzendernummer voor SFTP?

Deze fout kan verschillende oorzaken hebben:

- U probeerde uw private sleutel i.p.v. uw publieke sleutel op te laden. **Oplossing:** laad uw publieke sleutel op.
- U maakte uw publieke sleutel aan in een verkeerd formaat (bv. SSH1-RSA of SSH2-DSA). **Oplossing:** maak uw sleutels aan in SSH2-RSA-formaat.

Hoe moeten we onze publieke SSH-sleutel overmaken ?

Uw (co-)lokale beheerder moet de uw publieke SSH-sleutel opladen bij uw verzendernummer op de portaalsite.

Bericht verzenden

Hoe een gestructureerd bericht verzenden ?

1. Maak met uw SFTP-client een verbinding met sftp.socialsecurity.be (en aanvaard, eenmalig, de host-key van de server)
2. Identificeer u met uw technische gebruikersnaam (UMxxxxxx of EXPxxxxxx) en uw private SSH-sleutel door ingave van het wachtwoord dat uw private sleutel beschermt.
3. Plaats uw bestanden (FI, FS en Go) in de IN-directory (voor circuittestbestanden INTEST-directory, voor aangiftetestbestanden INTEST-S)

Na verwerking en controle van uw bestanden zullen acceptatie-(ACRF) en notificatiebestanden voor u klaargezet worden in de OUT-directory (voor circuittestbestanden OUTTEST-directory, voor aangiftetestbestanden OUTTEST-S-directory)

Zijn er beperkingen in bestandsgrootte ?

Omwille van de controle op de handtekening ligt de beperking op 200MB per bestand.

Welke bestanden toevoegen aan de gestructureerde berichten ?

Bij verzending via SFTP moet u samen met uw aangiftebestand (FI) ook een handtekeningbestand (FS-bestand) en een GO-bestand versturen.

Zijn de gestructureerde berichten die via het kanaal SFTP verstuurd worden dezelfde als de berichten die momenteel via het kanaal Isabel verstuurd worden. Zo niet, hoe zien ze er dan wel uit ?

De aangiftebestanden (FI-bestanden) zijn identiek voor elk gebruikt verzendkanaal. Zowel de structuur als de benaming van de bestanden blijven gelijk.

Verbindingen

Is het mogelijk zijn om SFTP te gebruiken via een leased line ?

Dit is momenteel niet voorzien.

Host

De naam van de host is sftp.socialsecurity.be
De poort is 8022

Hoe uw SFTP-client instellen ?

1. Vul de naam van de host in sftp.socialsecurity.be
2. Vul de poort 8022 in
3. Vul de gebruikersnaam van de technische gebruiker in
4. Laad uw private SSH-sleutel op