



GEBRUIKERSHANDLEIDING

Opzetten van een SFTP-kanaal

Inhoudsopgave

1. Wat is SFTP?.....	3
2. Uw gekwalificeerd digitale certificaat kiezen.....	4
3. Uw internetverbinding.....	6
4. Uw SFTP-client kiezen.....	6
5. Uw sleutelpaar aanmaken.....	7
6. Uw SFTP-kanaal aanmaken op het portaal.....	10
7. Uw SFTP-client instellen.....	17
8. Bestanden.....	19
8.1 Structuur van de bestandsnamen:.....	19
8.2 Het Aangiftebestand (FI):.....	22
8.3 Het handtekeningbestand (FS):.....	23
8.4 Het GO-bestand:.....	24
8.5 Het TD-bestand:.....	24
9. Uw bestanden overmaken.....	25
10. Bijlage: Een handtekeningbestand aanmaken via OPENSSL:.....	29
11. Vragen.....	36

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 mappen en bestanden en met dezelfde commando's als bij 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 dient u te beschikken over een **gebruikersnaam**.

Daarnaast vervangt een elektronisch sleutelbaar het klassieke wachtwoord. Dit sleutelbaar bevat een **private en publieke sleutel**. De private sleutel blijft bij degene die hem heeft aangemaakt en wordt 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 sleutelbaar aan te maken.

Net zoals de client beschikt elke **SFTP-server** ook over een sleutelbaar. 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.

Bij het aanmelden op de SFTP-server gebeurt de identificatie op basis van een gebruikersnaam en een private sleutel.

2. Uw gekwalificeerd digitale certificaat kiezen.

Elk aangiftebestand dat u via SFTP verzendt moet 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 (**Signature**) van uw elektronische identiteitskaart (eID) (<http://eid.belgium.be/nl/>)
2. Een gekwalificeerd digitaal certificaat van de volgende certificatie dienstverlener:
GlobalSign: PersonalSign 3 Pro
(<https://www.globalsign.com/en/personalsign/personalsign3-pro>)

Aangezien de aanvraagprocedure bij een certificatie dienstverlener verschillende dagen in beslag kan nemen, raden we u aan dit voldoende ruim op voorhand te doen.

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 portaal site 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.



Belangrijke opmerkingen bij de keuze van uw certificaat:

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

OpenSSL-procedure:

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

Dit houdt in dat de in deel 10. Bijlage: Een handtekeningbestand (FS) aanmaken via OPENSSL: beschreven procedure NIET geschikt is voor certificaten die zich bevinden op een elektronische identiteitskaart (eID) of op een Isabelkaart. In de praktijk is de procedure enkel bruikbaar voor certificaten van Globalsign.

Handtekenen met de elektronische identiteitskaart (eID):

Om een handtekeningbestand aan te maken met de eID gebruikt u een procedure met behulp van **Cryptonit**. U vindt de procedure met Cryptonit vinden in de bibliotheek met complementaire documenten (<https://www.socialsecurity.be/public/doclibrary/nl/batch.htm>). U mag uiteraard ook zelf de nodige programma's ontwikkelen of beroep doen op softwarepakketten die op de markt beschikbaar zijn.

De beschreven procedure met behulp van Cryptonit vereisen dat de eigenaar van de eID aanwezig is.

Bij ieder handtekeningbestand zal de eID in de kaartlezer moeten zitten en zal de eigenaar van de eID zijn pincode moeten ingeven. Dit impliceert dat als de eigenaar van de eID niet aanwezig is, en u voor een verzending van een gestructureerd bericht een handtekeningbestand moet aanmaken, u een andere eID zal moeten gebruiken. Alvorens te verzenden zal uw lokale of co-lokale beheerder in dat geval de publieke sleutel van de andere eID moeten opladen bij de instellingen van uw kanaal op de portaal-site.



Handtekenen met een Isabelkaart:

Het aanmaken van een handtekeningbestand op basis van een Isabelkaart is **niet mogelijk** omdat de private sleutel niet geëxporteerd kan worden. Wij kunnen u hiervoor geen handleiding of techniek aanbieden. Ook de helpdesk van Isabel kan u hierbij niet helpen.

3. Uw internetverbinding.

Voor een snelle en goede overdracht van bestanden via SFTP is de kwaliteit van uw internetverbinding van groot belang. Het loont de moeite om uit te testen vanaf welke PC of server de overdracht het beste werkt. Vermijd het opladen via een draadloze internetverbinding. Kleine storingen in het draadloos netwerk kunnen er immers voor zorgen dat de overdracht van bestanden wordt afgebroken.

Kijk ook de instellingen van uw firewall na. Deze moet SFTP-verkeer naar de poort 8022 toestaan.

Zorg ook dat er tijdens de verzending voldoende bandbreedte ter beschikking is. Andere gelijktijdige processen kunnen de bandbreedte, die nodig is om vlot via SFTP te verzenden, kannibaliseren.

4. Uw SFTP-client kiezen.

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 & 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 (Filezilla, WinSCP, Bitvise Tunnelier) die we zelf getest hebben.

5. Uw sleutelpaar aanmaken

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 uw SFTP-client te raadplegen.

Specificaties:

Formaat

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.

Daarnaast zijn er verschillende formaten voor de publieke sleutels. De meest gangbare zijn deze van de software OpenSSH en de software SSH (commerciële implementatie van SSH-protocol).

Voor de publieke sleutels zullen enkel de formaten van OpenSSH en SSH ondersteund worden.

Algoritme & lengte

Bij de generatie 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.

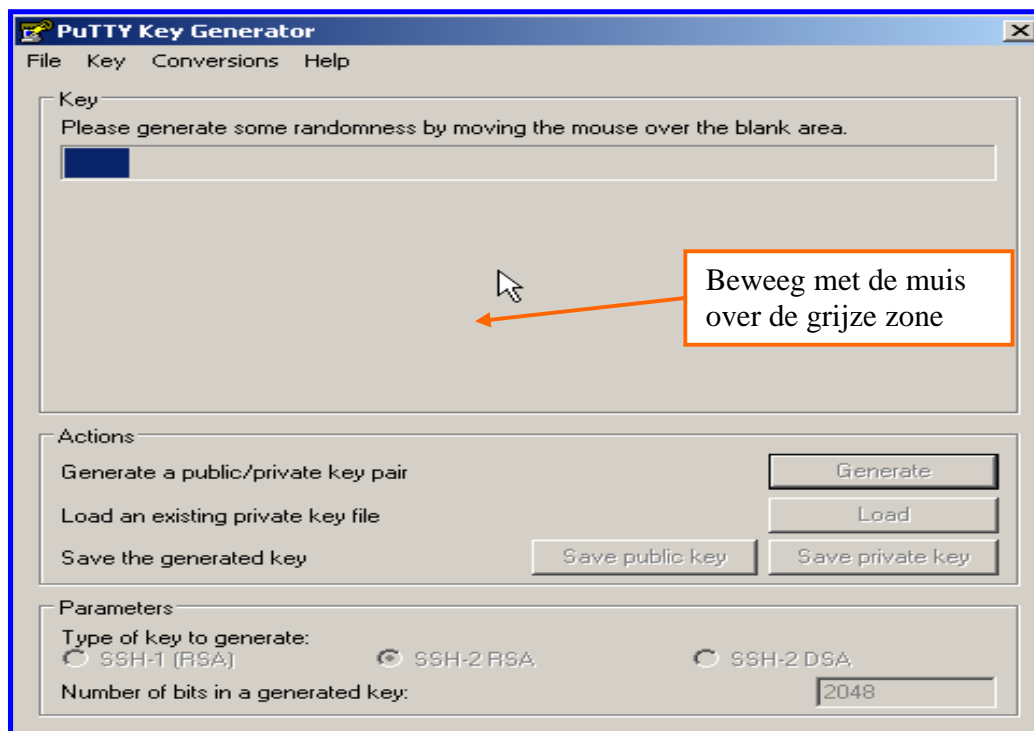
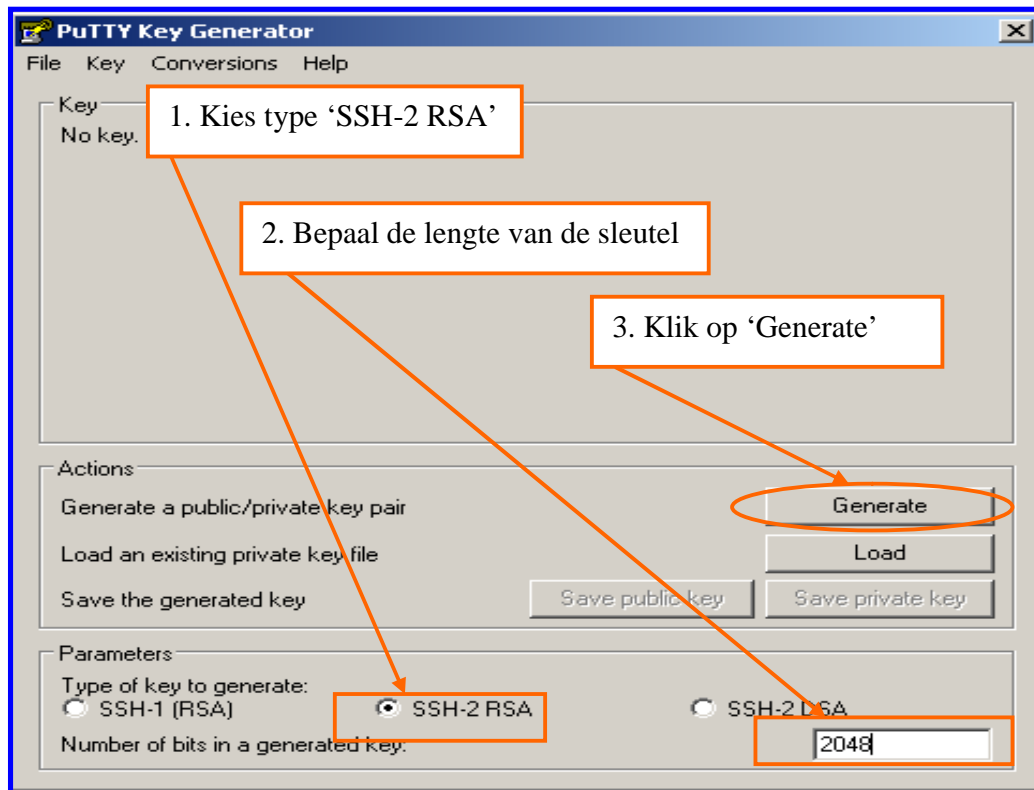
Als sleutellengte kiest u 2048 of hoger (3072, 4096). Kortere sleutels zullen niet aanvaard worden.

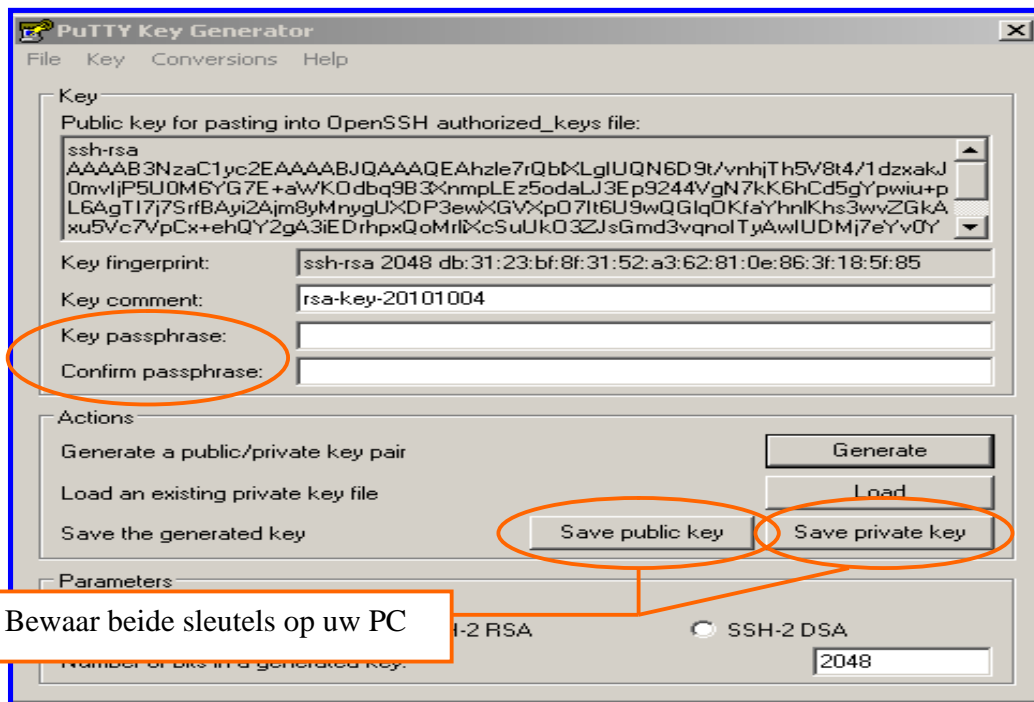
Wij raden u aan om bij de opslag van deze sleutels uw private sleutel te beschermen met een wachtwoord.

Kort samengevat:

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

Voorbeeld: Sleutels aanmaken met Putty Key Generator





Het is aangeraden om uw private sleutel te beveiligen met een wachtwoord. (Key passphrase). Sommige SFTP-clients laten echter niet toe om met een private sleutel die met een wachtwoord beveiligd is te werken.

Indien u de sleutels aanmaakt in uw SFTP-client verwijzen wij u naar de documentatie van uw SFTP-client.

6. Uw SFTP-kanaal aanmaken op het portaal van de sociale zekerheid

Enkel de lokale beheerder of de co-lokale beheerder van de hoedanigheid kan een kanaal aanmaken.

U vindt hierbij de verschillende stappen die u moet doorlopen om uw SFTP-kanaal aan te maken. Indien u voor de hoedanigheid reeds over een verzendkanaal beschikt of indien u in het verleden voor de hoedanigheid reeds een verzendkanaal heeft gehad zal u sommige stappen niet moeten doorlopen.

Toegangsbeheer
voor Ondernemingen en Organisaties

NL | FR | DE Home Help Quit

Benaming: ONDERNEMING; Ondernemingsnummer:
Hoedanigheid: Werkgever **RSZ**; **RSZ Stamnummer**:

Welkom **De heer Dieter Expeditor**, u krijgt toegang tot de portaal van de Sociale Zekerheid als **Lokale Beheerder** voor de volgende hoedanigheid:

Benaming: ONDERNEMING
Ondernemingsnummer:
Creatiedatum: 05/11/2010

Hoedanigheid: Werkgever **RSZ**
RSZ Stamnummer:
Creatiedatum: 05/11/2010

Denk eraan om de door u beheerde [hoedanigheidsgegevens](#) regelmatig te verifiëren.

Functionaliteiten

- Hoedanigheidsbeheer**
 - Beginpagina or Startpagina
 - Gebruikers
 - De details van de hoedanigheid raadplegen of wijzigen
 - Gebruikers opzoeken
- Routingmodule**
 - Informatie
 - De routingmodule raadplegen of wijzigen
- Gestructureerde berichten**
 - Gestructureerde berichten
- Persoonlijke gegevens**
 - Mijn persoonlijke gegevens wijzigen
 - Mijn wachtwoord wijzigen
 - Beheer van het certificaat te gebruiken op het portaal van de sociale zekerheid

Klik op 'Gestructureerde berichten'

Benaming: ONDERNEMING; Ondernemingsnummer:

Hoedanigheid: Werkgever RSZ; RSZ Stamnummer:

• Er is geen actieve verzender.

Functionaliteiten

Hoedanigheidsbeheer

- [Beginpagina or Startpagina](#)
- [Gebruikers](#)
- [De details van de hoedanigheid raadplegen of wijzigen](#)
- [Gebruikers opzoeken](#)

Routingmodule

- [Informatie](#)
- [De routingmodule raadplegen of wijzigen](#)


Gestructureerde berichten

- [De configuratiegegevens opslaan](#)

Persoonlijke gegevens

- [Mijn persoonlijke gegevens wijzigen](#)
- [Mijn wachtwoord wijzigen](#)
- [Beheer van het certificaat te gebruiken op het portaal van de sociale zekerheid](#)

Klik op 'De configuratiegegevens opslaan'^(*)

(*) Indien er voor de hoedanigheid reeds een verzendkanaal bestaat klikt u aan de rechterkant van uw scherm bij 'Gestructureerde berichten' op het icoontje  naast SFTP.



Gestructureerde berichten

- ➔ **Overzicht van de configuratiegegevens**
- [Contactpersoon](#)
- [Verbindingsgegevens](#)
- Kanalen
 - FTP-kanaal 
 - SFTP-kanaal 
 - WBS-kanaal 

Aangezien er dan reeds een technische gebruiker bestaat zal u de twee volgende schermen niet te zien krijgen.

Benaming: ONDERNEMING; Ondernemingsnummer:
Hoedanigheid: Werkgever RSZ; RSZ Stamnummer:

Informatie > Contactpersoon > Gegevens van het kanaal > Bevestiging

Creatie van een technische gebruiker

Naast het beheer van de gebruikers voor de portaal-toepassingen, is er de mogelijkheid om gegevens te beheren in verband met het verzenden van gestructureerde berichten.

Het verzenden van gestructureerde berichten (bestandsoverdracht) heeft vooral nut om zendingen met een groot volume aan aangiften te kunnen doen. Gegevensuitwisseling aan de hand van bestandsoverdracht is momenteel mogelijk via de batch-kanalen SFTP, FTP, MQLink.

Bij het eerst gebruik van de toepassing voor de uitwisseling van gestructureerde berichten, wordt u gevraagd de noodzakelijke informatie te registreren.

Klik op 'Volgende'

Functionaliteiten

Hoedanigheidsbeheer

- [Beiginpagina or Startpagina](#)
- [Gebruikers](#)
- [De details van de hoedanigheid raadplegen of wijzigen](#)
- [Gebruikers opzoeken](#)

Routingmodule

- [Informatie](#)
- [De routingmodule raadplegen of wijzigen](#)

Gestructureerde berichten

➔ [De configuratiegegevens opslaan](#)

Persoonlijke gegevens

- [Mijn persoonlijke gegevens wijzigen](#)
- [Mijn wachtwoord wijzigen](#)
- [Beheer van het certificaat te gebruiken op het portaal van de sociale zekerheid](#)

Benaming: ONDERNEMING; Ondernemingsnummer:
Hoedanigheid: Werkgever RSZ; RSZ Stamnummer:

Vul hier de gegevens van uw technische contactpersoon in en klik op 'Volgende'

Informatie > **Contactpersoon** > Gegevens van het kanaal > Bevestiging

Creatie van een technische gebruiker

Gegevens van de contactpersoon voor de uitwisseling van gestructureerde berichten

Identificatiegegevens

Naam *	:	<input type="text"/>
Voornaam *	:	<input type="text"/>
Titel *	:	<input type="text" value="De heer"/>
Functie *	:	<input type="text"/>
Taalregime *	:	<input type="text" value="Nederlands"/>
Telefoon *	:	<input type="text"/>
Fax	:	<input type="text"/>
Gsm	:	<input type="text"/>
E-mailadressen **	:	<input type="text"/>
	:	<input type="text"/>
	:	<input type="text"/>

* Verplichte velden

** Ten minste één e-mailadres

Functionaliteiten

Hoedanigheidsbeheer

- [Beiginpagina or Startpagina](#)
- [Gebruikers](#)
- [De details van de hoedanigheid raadplegen of wijzigen](#)
- [Gebruikers opzoeken](#)

Routingmodule

- [Informatie](#)
- [De routingmodule raadplegen of wijzigen](#)

Gestructureerde berichten

➔ [De configuratiegegevens opslaan](#)

Persoonlijke gegevens

- [Mijn persoonlijke gegevens wijzigen](#)
- [Mijn wachtwoord wijzigen](#)
- [Beheer van het certificaat te gebruiken op het portaal van de sociale zekerheid](#)

Benaming: ONDERNEMING; Ondernemingsnummer:
Hoedanigheid: Werkgever RSZ; RSZ Stamnummer:

Informatie > Contactpersoon > Gegevens van het kanaal > Bevestiging

Creatie van een technische gebruiker

Kanalen

SFTP-kanaal

Type verbinding * Internet

Lading van de publieke SSH-sleutel : Bladeren...

Let op: conform het gebruikersreglement dient elk bestand een certificaat.

Oplading van het certificaat : Bladeren...

Beveiligde toepassingen

U kunt de toepassingen selecteren waarvoor de uitwisseling via gestructureerde berichten toegelaten is voor het SFTP-kanaal.

Lijst van de toepassingen *

- Multifunctionele aangifte Dmfa
- Aangifte van de sociale risico's
- Tijdelijke werkloosheid
- DIMONA V2: Onmiddellijke aangifte van tewerkstelling
- Unieke werkmeldingen

* Verplichte velden

Annuleren Vorige **Volgende**

Functionaliteiten

Hoedanigheidsbeheer

- [Beginpagina or Startpagina](#)
- [Gebruikers](#)
- [De details van de hoedanigheid raadplegen of wijzigen](#)
- [Gebruikers opzoeken](#)

Routinamodule

Gestructureerde berichten

→ [De configuratiegegevens opslaan](#)

Persoonlijke gegevens

Laad hier uw publieke SSH-sleutel op

Laad hier de publieke sleutel (.cer) van uw digitaal certificaat op (*)

Vink de toepassingen aan waarvoor u via SFTP wenst te verzenden (**)

Klik op 'Volgende'

(*) Indien u kiest voor het gebruik van uw elektronische identiteitskaart (eID) dient u hier het 'Signature'-certificaat van uw eID-kaart op te laden.

(**) Indien u voor de hoedanigheid reeds over een verzendkanaal beschikt en u kiest voor uw SFTP-kanaal dezelfde toepassingen dan zal u per toepassing een voorkeurkanaal moeten aanduiden.

Benaming: ONDERNEMING; Ondernemingsnummer:

Hoedanigheid: Werkgever RSZ; RSZ Stamnummer:

Kies een technische gebruikersnaam^(*)

Informatie > Contactpersoon > Gegevens van het kanaal > Bevestiging

Creatie van een technische gebruiker

Technisch gebruiker

Voer de naam van de technische gebruiker twee keer in. 

Gebruikersnaam* : EXP

Bevestig de gebruikersnaam.* : EXP

Functionaliteiten

Hoedanigheidsbeheer

- [Beginpagina or Startpagina](#)
- [Gebruikers](#)
- [De details van de hoedanigheid raadplegen of wijzigen](#)
- [Gebruikers zoeken](#)

Klik op 'Volgende'

- [De routingmodule raadplegen of wijzigen](#)

Gestructureerde berichten

- ➔ [De configuratiegegevens opslaan](#)

Persoonlijke gegevens

- [Mijn persoonlijke gegevens wijzigen](#)
- [Mijn wachtwoord wijzigen](#)
- [Beheer van het certificaat te gebruiken op het portaal van de sociale zekerheid](#)

Karakteristieken van een technische gebruikersnaam:

- Minimum 8 – maximum 20 karakters
- Enkel cijfers (0-9) en de letters van het alfabet (a-z) zijn toegelaten
- Geen spaties
- Kan eens aangemaakt niet meer gewijzigd worden
- Mag nog niet bestaan in het toegangssysteem van de portaal-site van de sociale zekerheid
- De technische gebruikersnaam is **hoofdlettergevoelig**

(*) Indien u al beschikt over een ander verzendkanaal of in het verleden een verzendkanaal met inbelverbinding heeft gehad zal u dit scherm niet krijgen en dus geen technische gebruikersnaam moeten kiezen aangezien de technische gebruikersnaam die werd gekozen ook van toepassing blijft voor SFTP.

Benaming: ONDERNEMING; Ondernemingsnummer:

Hoedanigheid: Werkgever RSZ; RSZ Stamnummer:

Informatie > Contactpersoon > Gegevens van het kanaal > Bevestiging

Creatie van een technische gebruiker

Contactpersoon

Naam : Expeditortest
Voornaam : Test
Titel : mr
Functie : IT Manager
Taalregime : nl
Telefoon : 025455078
Fax :
Gsm :
E-mailadressen : batch@eranova.fgov.be

Kanaal

Kanaal : SFTP
Type verbinding : Internet
Publieke SSH-sleutel : Geladen

Certificaat

Eigenaar van het certificaat : (Signature)
Naam van de onderneming : Not specified
Leverancier van het certificaat : SERIALNUMBER=200803, CN=Citizen CA, C=BE
Vervaldatum : 26/03/2013
Reeksnummer (decimaal formaat) : 212676479325587081654357723800
Reeksnummer (hexadecimaal formaat) : 10 00 00 00 00 00 0b 7a 21 df 5c 29

Technisch gebruiker

Gebruikersnaam : EXPDEMOONDERNEMING

Beveiligde toepassingen

- Multifunctionele aangifte Dmfa
 - voorkeurkanaal :SFTP
- Aangifte van de sociale risico's
 - voorkeurkanaal :SFTP
- DIMONA V2: Onmiddellijke aangifte van tewerkstelling
 - voorkeurkanaal :SFTP

[Annuleren](#) [Vorige](#) [Bevestigen](#)

Functionaliteiten

Hoedanigheidsbeheer

- [Beginpagina or Startpagina](#)
- [Gebruikers](#)
- [De details van de hoedanigheid raadplegen of wijzigen](#)
- [Gebruikers opzoeken](#)

Routingmodule

- [Informatie](#)
- [De routingmodule raadplegen of wijzigen](#)

Gestructureerde berichten

- ➔ [De configuratiegegevens opslaan](#)

Persoonlijke gegevens

- [Mijn persoonlijke gegevens wijzigen](#)
- [Mijn wachtwoord wijzigen](#)
- [Beheer van het certificaat te gebruiken op het portaal van de sociale zekerheid](#)

Klik op 'Bevestigen'

Benaming: ONDERNEMING; Ondernemingsnummer:

Hoedanigheid: Werkgever RSZ; RSZ Stamnummer:

• De verzender werd met succes aangemaakt.

Overzicht van de configuratiegegevens

Identificatie van de contactpersoon

Naam : Expeditortest
 Voornaam : Test
 Titel : De heer
 Functie : IT Manager
 Taalregime : Nederlands
 Telefoon : 025455078
 Fax :
 Gsm :
 E-mailadressen : batch@eranova.fgov.be

Identificatie van de technische gebruiker

Verzendernummer : 101380
 Inschrijvingsdatum : 05/11/2010
 Gebruikersnaam : EXPDEMOONDERNEMING

SFTP

Type verbinding : Internet

Eigenaar van het certificaat : (Signature)
 Naam van de onderneming : Not specified
 Leverancier van het certificaat : SERIALNUMBER=200803, CN=Citizen CA, C=BE
 Vervaldatum : 26/03/2013
 Reeksnummer (decimaal formaat) : 212676479325587081654357723800
 Reeksnummer (hexadecimaal formaat) : 10 00 00 00 00 00 0b 7a 21 df 5c 29

Beveiligde toepassingen

- Aangifte van de sociale risico's
- Multifunctionele aangifte Dmfa
- DIMONA V2: Onmiddellijke aangifte van tewerkstelling

Functionaliteiten

Hoedanigheidsbeheer

- [Beginpagina or Startpagina](#)
- [Gebruikers](#)
- [De details van de hoedanigheid raadplegen of wijzigen](#)
- [Gebruikers opzoeken](#)

Routingmodule

- [Informatie](#)
- [De routingmodule raadplegen of wijzigen](#)

Gestructureerde berichten

- ➔ Overzicht van de configuratiegegevens**
- [Contactpersoon](#)
- Kanalen**
 - SFTP-kanaal
 - FTP-kanaal
 - MQLink-kanaal
 - WBS-kanaal
- [De verzending via gestructureerde berichten verwijderen](#)

Persoonlijke gegevens

- [Mijn persoonlijke gegevens wijzigen](#)
- [Mijn wachtwoord wijzigen](#)
- [Beheer van het certificaat te gebruiken op het portaal van de sociale zekerheid](#)

Uw verzendernummer^(*) heeft u nodig in de naam van uw bestanden en de gebruikersnaam heeft u nodig om u aan te melden op de SFTP-server.

Na het aanmaken van uw SFTP-kanaal moet u rekening houden met de synchronisatie met de SFTP-server die om de 30 minuten gebeurt. (Omstreeks het uur en omstreeks het halfuur). Zolang deze synchronisatie niet heeft plaats gevonden krijgt u de melding "De configuratie voor de creatie van het kanaal is aan de gang". Pas na deze synchronisatie zal u zich kunnen aanmelden op de SFTP-server.

(*) Indien u voor de hoedanigheid al over een verzendkanaal beschikt of indien u in het verleden reeds een verzendkanaal heeft gehad zal u steeds het verzendernummer behouden dat u reeds had.

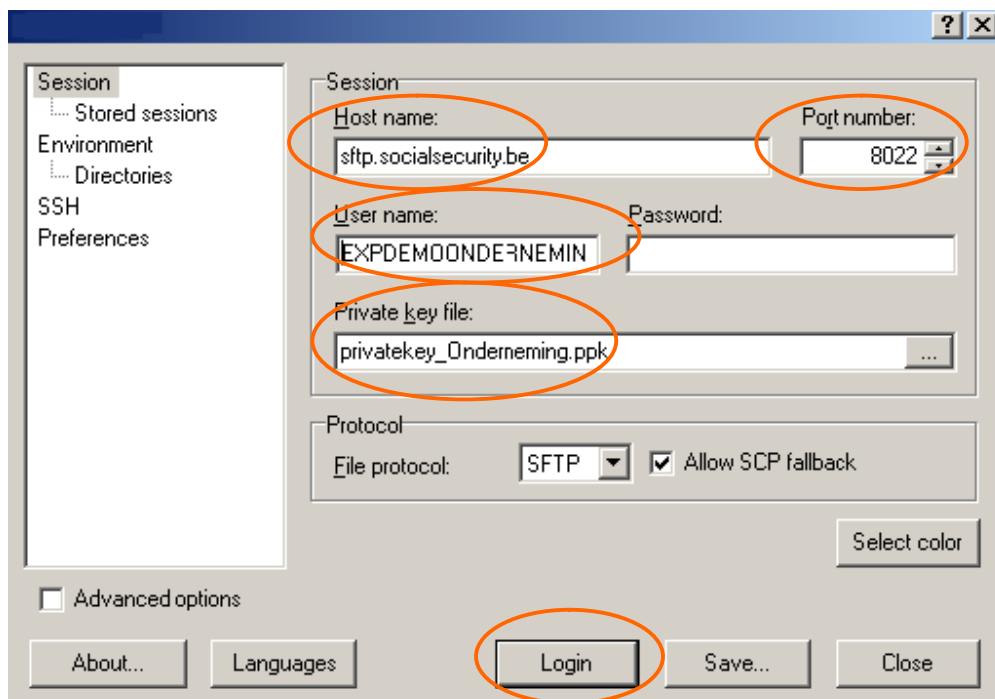
7. Uw SFTP-client instellen

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

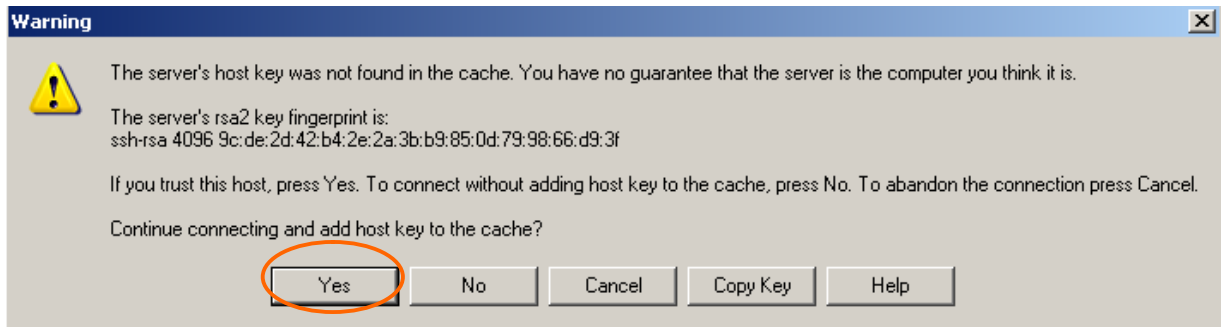
- De naam van de host in: 'sftp.socialsecurity.be'
- Het poortnummer in: '8022'. (Opgelet: het kan zijn dat u de instellingen van uw firewall moet aanpassen om verkeer naar deze poort toe te laten).
- De **gebruikersnaam** (begint met **EXP**) die u gekozen heeft bij het aanmaken van uw SFTP-kanaal op het portaal van de sociale zekerheid. (Indien u in het verleden al een technische gebruikersnaam heeft aangemaakt voor de hoedanigheid kan het zijn dat deze met **UM** begint.) Opgelet, de gebruikersnaam is **hoofdlettergevoelig**.
- 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.

(*) Voor het instellen van uw SFTP-client verwijzen wij u naar de documentatie van uw SFTP-client. Ter informatie vindt u in de technische bibliotheek (<https://www.socialsecurity.be/public/doclibrary/nl/batch.htm>) de aangewezen instellingen voor de manuele SFTP-clients (Filezilla, WinSCP, Bitvise Tunnelier) die we zelf getest hebben.

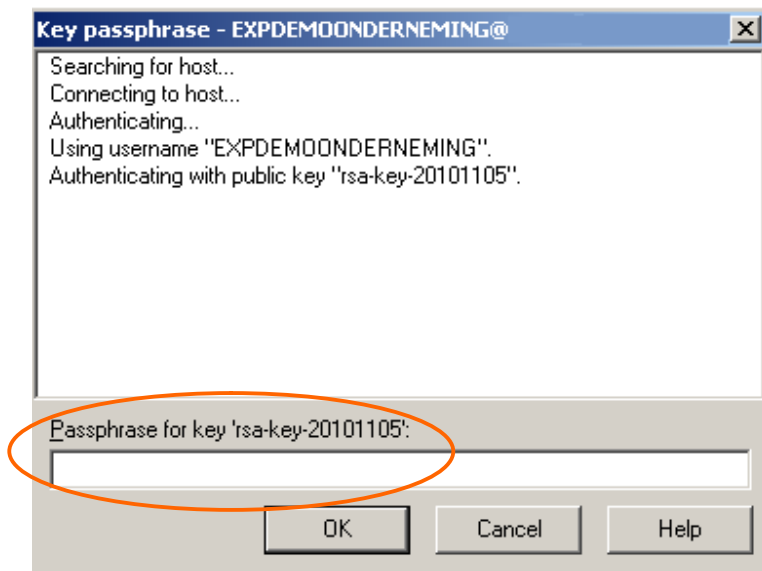
Voorbeeld:



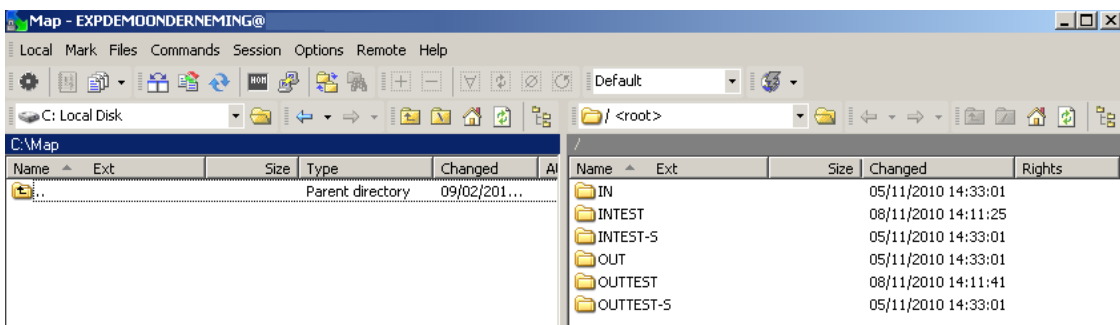
Aanvaard éénmalig de publieke sleutel (host key) van de SFTP-server van de sociale zekerheid. Dit is de publieke sleutel van de server: ssh-rsa 4096 9c:de:2d:42:b4:2e:2a:3b:b9:85:0d:79:98:66:d9:3f



Indien u uw private sleutel heeft beschermd met een wachtwoord zal u gevraagd worden om dit wachtwoord in te geven.



Vervolgens bent u aangemeld. Aan de linkerkant ziet u de mappen op uw eigen PC en aan de rechterkant ziet u uw mappen op de SFTP-server van de sociale zekerheid.



8. Bestanden

Voor de verzending via SFTP in de productieomgeving moet u naast uw aangiftebestand (FI) ook steeds een handtekeningbestand (FS) en een GO-bestand aanmaken en op de server plaatsen.

Enkel in de Simulatie- en Testomgeving is het handtekeningbestand niet vereist. Het GO-bestand is steeds vereist.

8.1 Structuur van de bestandsnamen:

Bij de gestructureerde berichten hebben de bestandsnamen de volgende structuur:

FI.XXXX.123456.20150213.00001.R.1.1
FS.XXXX.123456.20150213.00001.R.1.1
GO.XXXX.123456.20150213.00001.R.1
(TD.XXXX.123456.20150213.00001.R.1)

Eerste deel van de naam:

FI Aangiftebestand
FS Handtekeningbestand
GO Leeg bestand dat de verwerking initieert
TD Leeg bestand dat de verwerking verhindert

Tweede deel van de naam:

XXXX: het tweede element van de naam van het bestand geeft het doel van de bestandsoverdracht weer.

Voorbeelden:

AOAT: voor een aangifte ASR "arbeidsongeval"
DDTN: voor een aangifte van werken
DIMN: voor een aangifte Dimona
DMFA: voor een originele aangifte DmfA
DMRQ: voor een consultatie (Request) DmfA
DMWA: voor een wijzigende aangifte DmfA
PFRQ: voor een consultatie van het personeelsbestand
TWCT: voor een aangifte Tijdelijke Werkloosheid
VBLV: voor een aangifte "Validatieboek"
WECH: voor een aangifte ASR "werkloosheid"
ZIMA: voor een aangifte ASR "uitkeringen"

Derde deel van de naam:

123456: Dit is het verzendernummer dat toegekend is aan de verzender bij de aanmaak van het eerste kanaal voor zijn hoedanigheid.

Vierde deel van de naam:

20120213: Dit is de creatiedatum van het bestand in de vorm JJJJMMDD.

Vijfde deel van de naam:

00001: Betreft een volgnummer dat u vrij mag kiezen en op een **unieke** wijze de naam van het bestand aangeeft, per creatiedatum en per omgeving. Voor een volgnummer mogen alle alfanumerieke karakters gebruikt worden.

Zesde deel van de naam:

Geeft de werkomgeving aan:

«**R**» wordt gebruikt voor de **productie**

«**T**» wordt gebruikt voor een **test** (ASR, Unieke Werfmelding, Dimona of Tijdelijke Werkloosheid) of een **circuittest DmfA**

«**S**» wordt gebruikt voor een **aangiftetest DmfA**

Verschil tussen een aangifte-(S) en een circuittest (T) bij DmfA

Bij DmfA kan u uw testbestanden als aangiftetest (extensie S en map INTEST-S) of als circuittest (Extensie T en map INTEST) verzenden. Voor alle andere toepassingen kan u enkel de extensie T en de map INTEST gebruiken voor uw testbestanden.

Bij een **aangiftetest (bestandsextensie S)** worden alle ontvangstcontroles en alle inhoudscontroles doorlopen. Er is geen controle op de identificatiegegevens van de werknemer(s).

U ontvangt na een positieve ACRF een notificatie maar geen DMNO of PID-bestand. U plaatst uw bestanden in de folder **INTEST-S** en u vindt de het resultaat in de folder **OUTTEST-S**.

Doordat de aangifte niet bewaard wordt in de simulatieomgeving kan u meermaals dezelfde aangifte testen.

Bij een **circuittest (bestandsextensie T)** wordt zoals in de productieomgeving het volledige controlecircuit doorlopen. Er is een controle op de identificatiegegevens van de werknemer(s) maar geen identificatiecontrole via Sigedis.

U ontvangt na een positieve ACRF de antwoordbestanden zoals in de productieomgeving (Notificaties, PID's en DMNO's).

U plaatst uw bestanden in de folder **INTEST** en u vindt de het resultaat in de folder **OUTTEST**.

Bij een positieve notificatie wordt de aangifte bewaard in de simulatieomgeving. Net zoals in de productieomgeving geldt er voor de circuittest de beperking van één aanvaarde aangifte per combinatie RSZ-nummer/kwartaal.

Zevende deel van de naam:

1: geeft het aantal delen van het bestand aan.

Een aangifte mag uit maximaal 9 delen bestaan.

De aangiftes in het kader van ASR en Tijdelijke Werkloosheid mogen niet opgesplitst worden dus mag er geen zevende deel van de naam opgegeven worden.

Bv. FI.WECH.123456.20150213.00001.R

Achtste deel van de naam:

1: geeft het nummer van het deel aan.

De aangiftes in het kader van ASR en Tijdelijke Werkloosheid mogen niet opgesplitst worden dus mag er geen achtste deel van de naam opgegeven worden.

Bv. FI.AOAT.123456.20150213.00001.R

Voorbeelden:

- De verzender stuurt één deel:

FI.DMFA.123456.20150213.00001.R.1.1
FS.DMFA.123456.20150213.00001.R.1.1
GO.DMFA.123456.20150213.00001.R.1

- De verzender stuurt twee delen:

FI.DMFA.123456.20150213.00001.R.2.1
FI.DMFA.123456.20150213.00001.R.2.2
FS.DMFA.123456.20150213.00001.R.2.1
FS.DMFA.123456.20150213.00001.R.2.2
GO.DMFA.123456.20150213.00001.R.2

8.2 Het Aangiftebestand (FI):

De aangiftebestanden (FI) zijn identiek voor alle kanalen.

Structuur van de naam van een FI-bestand:

FI.toepassing.verzendernummer.datum.volgnummer.werkomgeving.aantal delen.nummer van het deel

Bv. FI.DMFA.123456.20150213.00001.T.1.1

Op de startpagina van elke toepassing vindt u op het portaal van de sociale zekerheid in de TechLib alle technische informatie (glossaria, schema's, gestructureerde bijlage en instructies) om uw aangiftebestand op te maken.



Dimona en het personeelsbestand

voor: werkgemers RSZ , werkgemers RSZPPO 


 Sinds 1 oktober kunnen ALLE werkgemers eindelijk gebruikmaken van de nieuwe Dimona. De vernieuwde toepassing heeft tal van voordelen: versterkte technische controles, een snelle opsporing van fouten door duidelijke notificaties, een verhoogde beveiliging, een toegenomen gebruiksgemak, afstemming met andere belangrijke aangiften zoals Dmfa en ASR, enzovoort.

De onmiddellijke aangifte van tewerkstelling, afgekort Dimona (*Déclaration Immédiate/ Onmiddellijke aangifte*), is een elektronisch bericht waarin de werkgemer iedere aanwerving en iedere uitdiensttreding van een werknemer meldt aan de RSZ/PPO. De elektronische dimensie geeft het bericht een direct en ogenblikkelijk karakter.

Het personeelsbestand is een beveiligde databank die toelaat dat de werkgemer het resultaat van de door hem ingevoerde en de door de RSZ/PPO aanvaarde Dimona aangiften kan raadplegen.

De wijzigingen kunnen betrekking hebben op allerlei situaties, bijvoorbeeld:

- Een werknemer komt in dienst.
- Een werknemer gaat uit dienst.
- Een werknemer werkt langer dan voorzien.

 Alle technische info (glossarium, schema's, instructies en vormcontroleprogramma) over Dimona zijn gegroepeerd in de [TechLib](#)

Glossarium	<input type="text" value="--- Kies een glossarium ---"/>	<input type="button" value="Go!"/>
Instructies voor de werkgemer RSZ	<input type="text" value="Instructies voor de werkgemer 2010/03"/>	<input type="button" value="Go!"/>
Instructies voor de werkgemer RSZPPO	<input type="text" value="Administratieve instructies 2010/03"/>	<input type="button" value="Go!"/>

8.3 Het handtekeningbestand (FS):

- Het FS-bestand bevat de elektronische handtekening op basis van uw gekwalificeerd certificaat.
- U kan volgende gekwalificeerde digitale certificaten gebruiken:
 - GlobalSign: PersonalSign 3 pro
(<https://www.globalsign.com/en/personalsign/personalsign3-pro>)
 - Het handtekeningcertificaat (**Signature**) van de elektronische identiteitskaart
- Het handtekeningbestand moet aangemaakt worden met het certificaat dat u bij uw verzendkanaal heeft opgeladen.
- 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.
- Voor OpenSSL^(*) is het belangrijk dat uw certificaten zich niet op een chipkaart of een USB-sleutel bevinden zodat u de private sleutel kan exporteren.
- **Om een handtekeningbestand aan te maken met de eID gebruikt u een procedure met behulp van Cryptonit. U vindt de procedure in de bibliotheek met complementaire documenten:**
(<https://www.socialsecurity.be/public/doclibrary/nl/batch.htm>).
- Bij een aangifte in meerdere delen (FI) wordt aan elk deel een handtekeningbestand (FS) toegevoegd.
- Voor het aanmaken van uw FS-bestand moet u het gekwalificeerde digitale certificaat (.pfx of .p12) gebruiken waarvan u de publieke sleutel (.cer) heeft opgeladen op het portaal van de sociale zekerheid bij de aanmaak van uw SFTP-kanaal.
- Een handtekeningbestand (FS) is verplicht bij een aangifte in de productieomgeving. In de test- en simulatieomgeving bent u niet verplicht om een handtekeningbestand (FS) mee te sturen. Indien u in de test- en simulatieomgeving wel een handtekeningbestand (FS) meestuurt zal dit in de test- en simulatieomgeving ook gecontroleerd worden.

Structuur van de naam van een FS-bestand:

FS.toepassing.verzendernummer.datum.volgnummer.werkomgeving.aantal delen.nummer van het deel
Bv. FS.DMFA.123456.20150213.00001.T.1.1

(*) U vindt de uitleg over het aanmaken van een handtekeningbestand met OpenSSL achteraan in deze handleiding in punt 10. Bijlage: Een handtekeningbestand (FS) aanmaken via OPENSSL:

8.4 Het GO-bestand:

- Is een leeg bestand.
- Is het signaal dat de verzender klaar is met plaatsen van zijn bestanden en dat de verwerking ervan mag beginnen.
- Moet steeds **na** het FI- en FS-bestand als laatste bestand in de **IN-**, **INTEST-** of **INTEST-S**-folder geplaatst worden.
- Bij een aangifte in meerdere delen (FI) wordt slechts één GO-bestand toegevoegd.

Een GO-bestand maakt u door een leeg bestand (bv. een tekstbestand) 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.123456.20150213.00001.T.1

8.5 Het TD-bestand:

- Is een leeg bestand.
- Dient om aan te duiden dat de geplaatste FI- en/of FS-bestanden niet verwerkt mogen worden. (TD = To Delete)
- Moet steeds **na** het FI- en FS-bestand als laatste bestand in de **IN-**, **INTEST-** of **INTEST-S**-folder geplaatst worden.
- Indien u reeds een GO-bestand heeft geplaatst kan u voor de daaraan verbonden FI- en FS-bestanden geen TD-bestand meer plaatsen.
- Bij een aangifte in meerdere delen (FI) wordt slechts één TD-bestand toegevoegd.
- Na het verzenden van het TD-bestand ontvangt u als bevestiging van de schrapping een ACRF-bestand met **ResultCode 0**, **ErrorID ACRF-430** en aan uw bestandsnaam wordt de datum en het uur van de schrapping toegevoegd.
Bv. TD.DMFA.123456.20150213.00001.T.1_20120213_102735

Een TD-bestand maakt u door een leeg bestand (bv. een tekstbestand) te openen en dit te bewaren met de correcte bestandsnaam.

Structuur van de naam van een TD-bestand:

TD.toepassing.verzendernummer.datum.volgnummer.werkomgeving.aantal delen
Bv. TD.DMFA.123456.20150213.00001.T.1

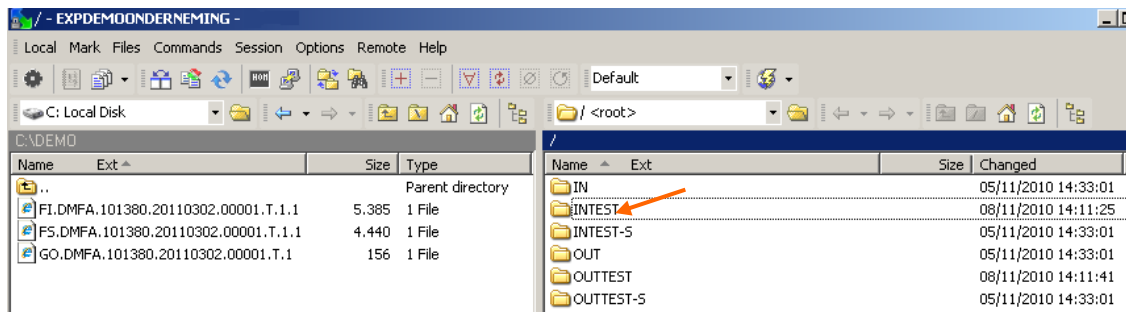
9. Uw bestanden overmaken

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

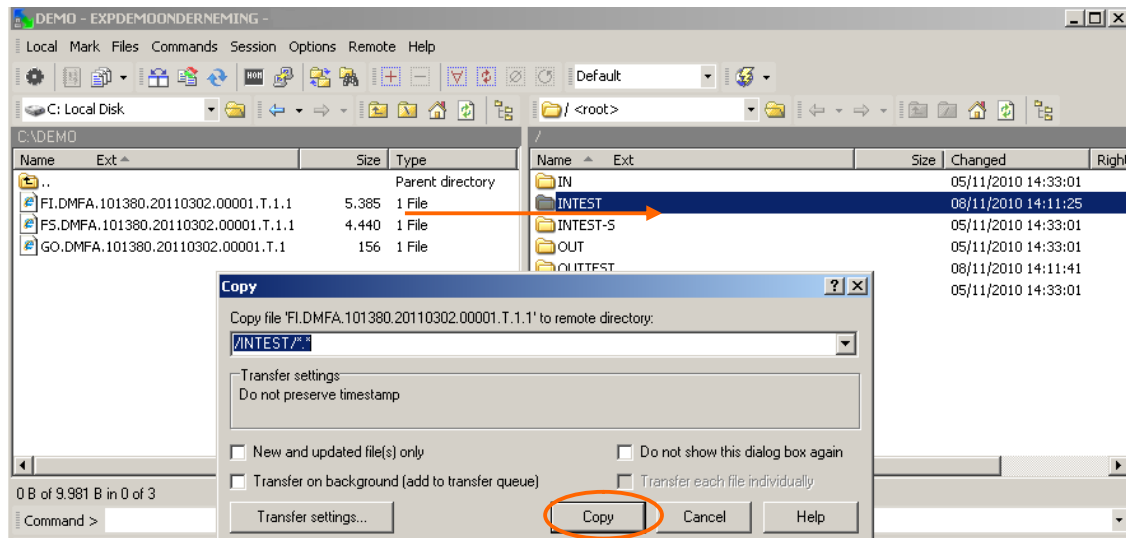
- Productiebestanden DmfA, ASR, Dimona, Tijdelijke Werkloosheid en Unieke Werfmelding (extensie **R**) -> map **IN**^(*)
- Test-/Simulatiebestanden ASR, Dimona, Tijdelijke Werkloosheid en Unieke Werfmelding en DmfA-circuittestbestanden (extensie **T**) -> map **INTEST**^(*)
- DmfA-aangiftetestbestanden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

^(*)Indien u via commando's wenst te werken is het belangrijk dat u de namen van de mappen steeds in hoofdletters vermeldt.

In dit voorbeeld gaan we de INTEST-map openen om daarin onze bestanden te plaatsen.



Vervolgens slepen we de verschillende bestanden (FI, FS en GO) naar de INTEST-map. Omdat het **GO-bestand** de verwerking doet beginnen slepen we dit steeds **als laatste** naar de map.



Van zodra het **GO-bestand** is geplaatst start de verwerking van alle bijhorende bestanden automatisch.

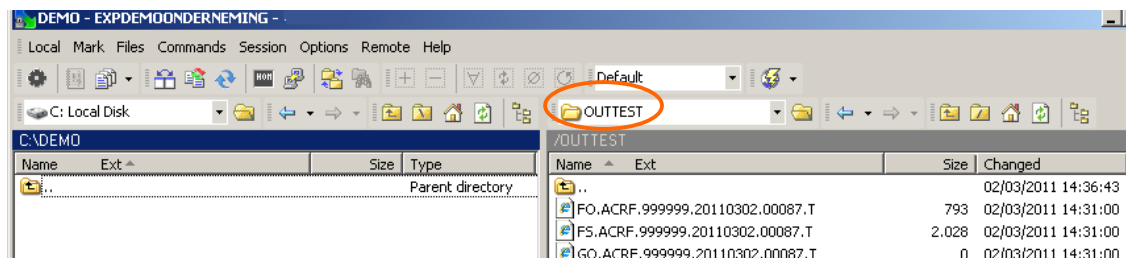
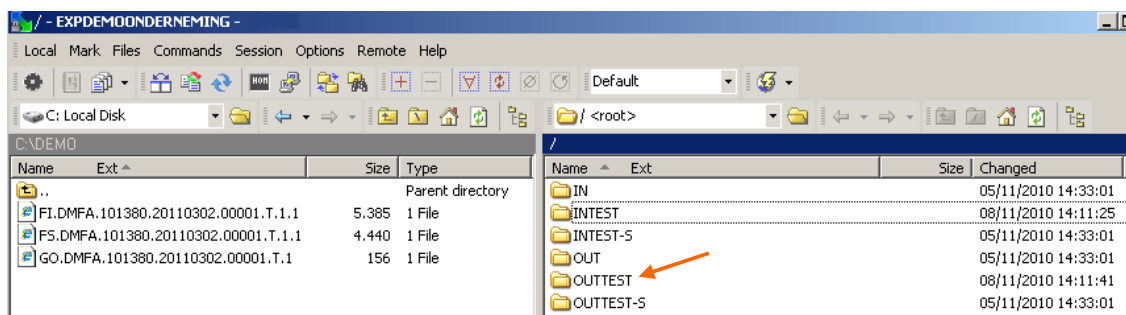


Van zodra de aangiftes verwerkt zijn zal u de antwoorden (ACRF's, Notificaties, ...) terugvinden in de respectievelijke mappen :

- 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**^(*)

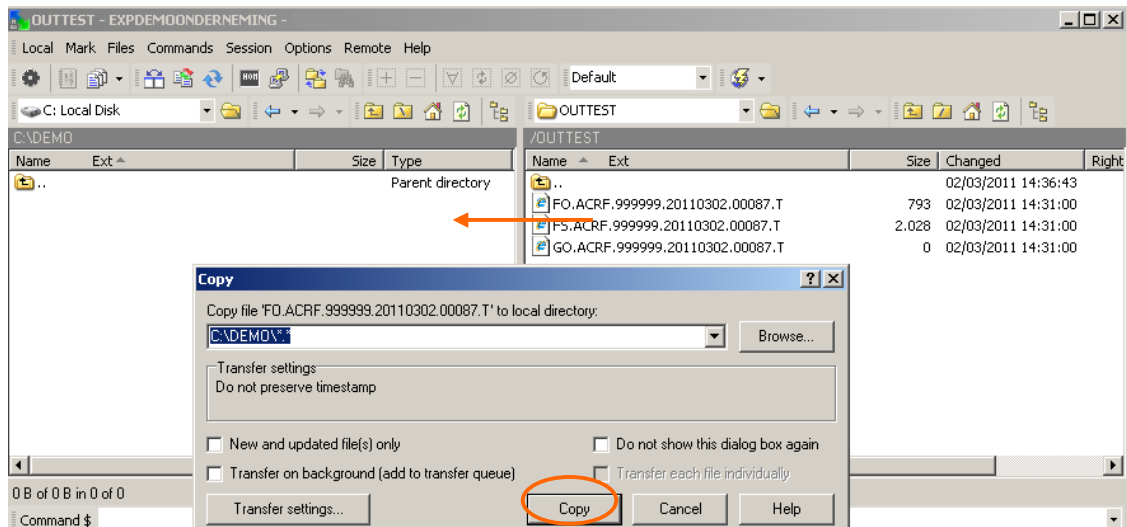
(*) Indien u via commando's wenst te werken is het belangrijk dat u de namen van de mappen steeds in hoofdletters vermeldt.

We openen de map OUTTEST.



- Het ontvangstbewijs of ACRF is een bericht dat bewijst dat we uw bestand ontvangen hebben en dat het aan de vormvereisten voldoet.
- Een positief ontvangstbewijs betekent dat uw bestand verder kan worden behandeld. In dat geval zal u nadien in dezelfde map ook nog een notificatie ontvangen met het resultaat van de inhoudscontrole van uw aangifte.

We slepen de OUT-bestanden naar onze PC.



Na het slepen naar onze PC moeten we de bestanden op de SFTP-server wissen. Op onze eigen PC kunnen we de bestanden openen en verder verwerken.



Beheer van uw Uit-mappen:

Bij SFTP worden de voor u bestemde bestanden ter beschikking gesteld in de mappen OUT, OUTTEST of OUTTEST-S op onze server.

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.

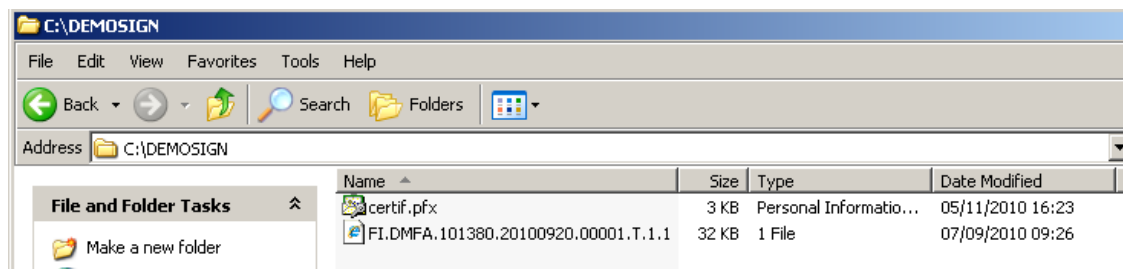
10. Bijlage: Een handtekeningbestand (FS) aanmaken via OPENSLL:

Opgelet:

Deze procedure is NIET geschikt voor certificaten die zich bevinden op een elektronische identiteitskaart (eID) of op een Isabelkaart. In de praktijk is deze procedure enkel bruikbaar voor certificaten van Globalsign.

Om een handtekeningbestand aan te maken met OpenSSL dient u eerst deze software 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.



We leggen dit uit aan de hand van een voorbeeld:

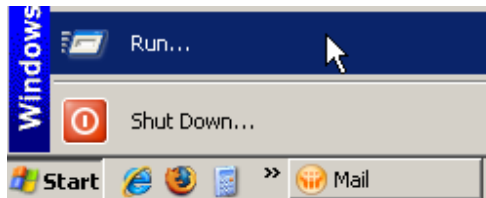
- C:\DEMOSIGN : Map waarin ons FI-bestand en ons certificaat staan
- certif.pfx: naam van ons certificaat
- ww123: wachtwoord dat bij ons certificaat hoort
- ww789: wachtwoord dat we kiezen bij het aanmaken van ons .key bestand

We maken een .pem-, een .key- en een FS-bestand.

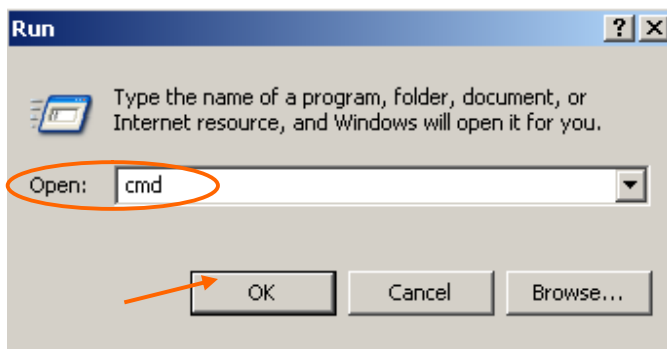
We kiezen in ons voorbeeld om het .pem-bestand en het .key-bestand de naam dmfa te geven. Deze benaming is een vrije keuze. U mag ze dus gerust andere namen geven en indien u ze ook de naam dmfa zou geven mag u ze uiteraard ook voor het tekenen van bestanden voor andere toepassingen gebruiken.

Het is belangrijk om in DOS de juiste commando's en de juiste paden naar de bestanden in te typen.

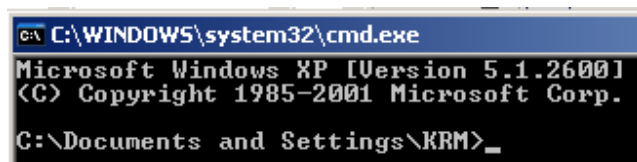
1. Open een dos-venster. Ga hiervoor naar Start en klik op **Run**.



2. Typ **cmd** in en klik op 'OK'.



En het dos-venster gaat open.



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 ingeven.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\KRM>cd..

C:\Documents and Settings>cd..

C:\>
```

4. Open de directory OpenSSL via het commando **cd openssl** gevolgd door [ENTER]

```
C:\>cd openssl
```

5. Open de subdirectory bin via het commando `cd bin` gevolgd door [ENTER]

```
C:\OpenSSL>cd bin
```

6. Open OpenSSL via het commando `openssl` gevolgd door [ENTER]

```
C:\OpenSSL\bin>openssl
```

U krijgt nu de openssl prompt: "OpenSSL>"

```
OpenSSL>
```

7. Nu moet u uw **.pem-bestand** aanmaken.

Na deze prompt moet u dus het commando om het .pem bestand aan te maken ingeven. Opgelet u moet hierbij gebruik maken van uw certificaat formaat .pfx of .p12 en niet van de publieke sleutel van het certificaat (.cer).

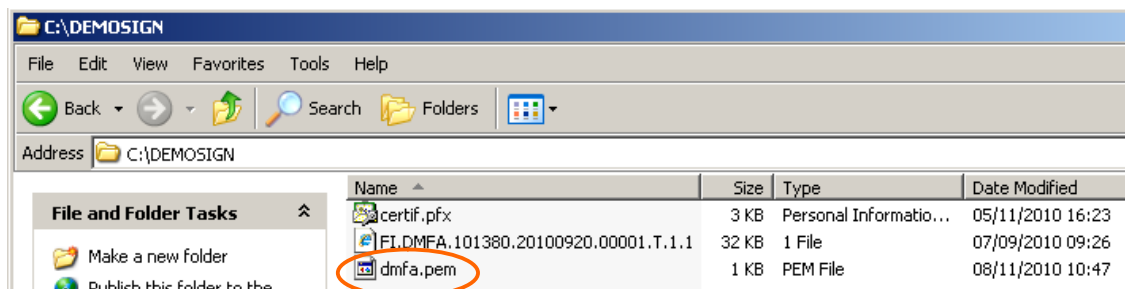
U geeft dus volgend commando met het volledige pad waar uw map met het certificaat en uw te ondertekenen FI-bestand staat in:

`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]

```
OpenSSL> pkcs12 -in C:\DEMOSIGN\certif.pfx -passin pass:ww123 -out C:\DEMOSIGN\dmfa.pem -clcerts -nokeys
```

Uw .pem-bestand wordt aangemaakt en in uw map met uw certificaat en uw aangiftebestand geplaatst.

```
OpenSSL> pkcs12 -in C:\DEMOSIGN\certif.pfx -passin pass:ww123 -out C:\DEMOSIGN\dmfa.pem -clcerts -nokeys  
MAC verified OK
```



8. Nu moet u uw **.key-bestand** aanmaken

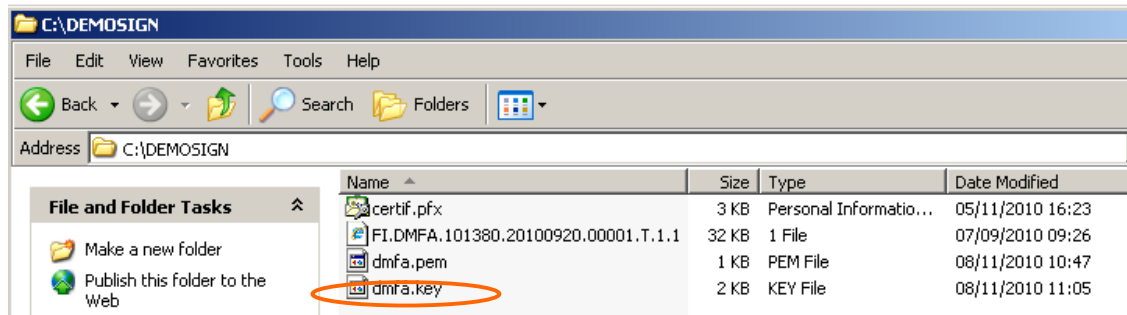
U geeft hiervoor volgend commando in na de prompt OpenSSL > :

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]

```
OpenSSL> pkcs12 -in C:\DEMOSIGN\certif.pfx -passin pass:ww123 -passout pass:ww789 -out C:\DEMOSIGN\dmfa.key
```

Uw **.key**-bestand wordt aangemaakt en in uw map met uw certificaat en uw aangiftebestand geplaatst.

```
OpenSSL> pkcs12 -in C:\DEMOSIGN\certif.pfx -passin pass:ww123 -passout pass:ww789 -out C:\DEMOSIGN\dmfa.key  
MAC verified OK
```



Telkens u een FI-bestand wil doorsturen dient u op basis van het FI-bestand in combinatie met het **.pem** en het **.key** bestand een FS-bestand aan te maken.

De aangemaakte **.pem**- en **.key**-bestanden kan u gebruiken zolang uw certificaat geldig is (zie Expiration Date van uw certificaat). Eens uw certificaat vervallen is moet u een nieuw certificaat opladen bij uw kanaal en moet u met uw nieuwe certificaat opnieuw de **.pem**- en **.key**-bestanden aanmaken.

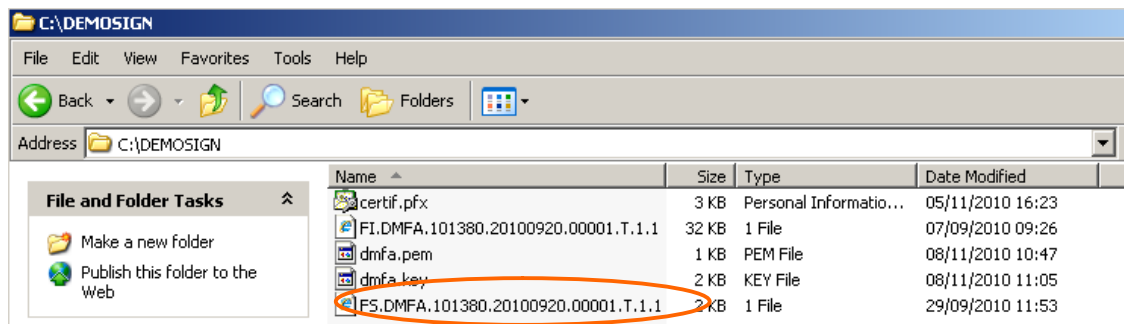
9. Nu moet u uw **FS-bestand** aanmaken.

Dit FS-bestand kan u aanmaken door volgend commando in te geven 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 IN STAP 8 GEKOZEN HEEFT VOOR UW .KEY **-outform PEM -out** LOCATIE VAN UW MAP\NAAM VAN UW FS-BESTAND gevolgd door [ENTER]

```
OpenSSL> smime -sign -in
C:\DEMOSIGN\FI.DMFA.123456.20100920.00001.T.1.1 -signer
C:\DEMOSIGN\dmfa.pem -inkey C:\DEMOSIGN\dmfa.key -passin pass:ww789 -
outform PEM -out C:\DEMOSIGN\FS.DMFA.123456.20100920.00001.T.1.1
```

Uw FS-bestand wordt aangemaakt en in uw map met uw certificaat en uw aangiftebestand geplaatst.

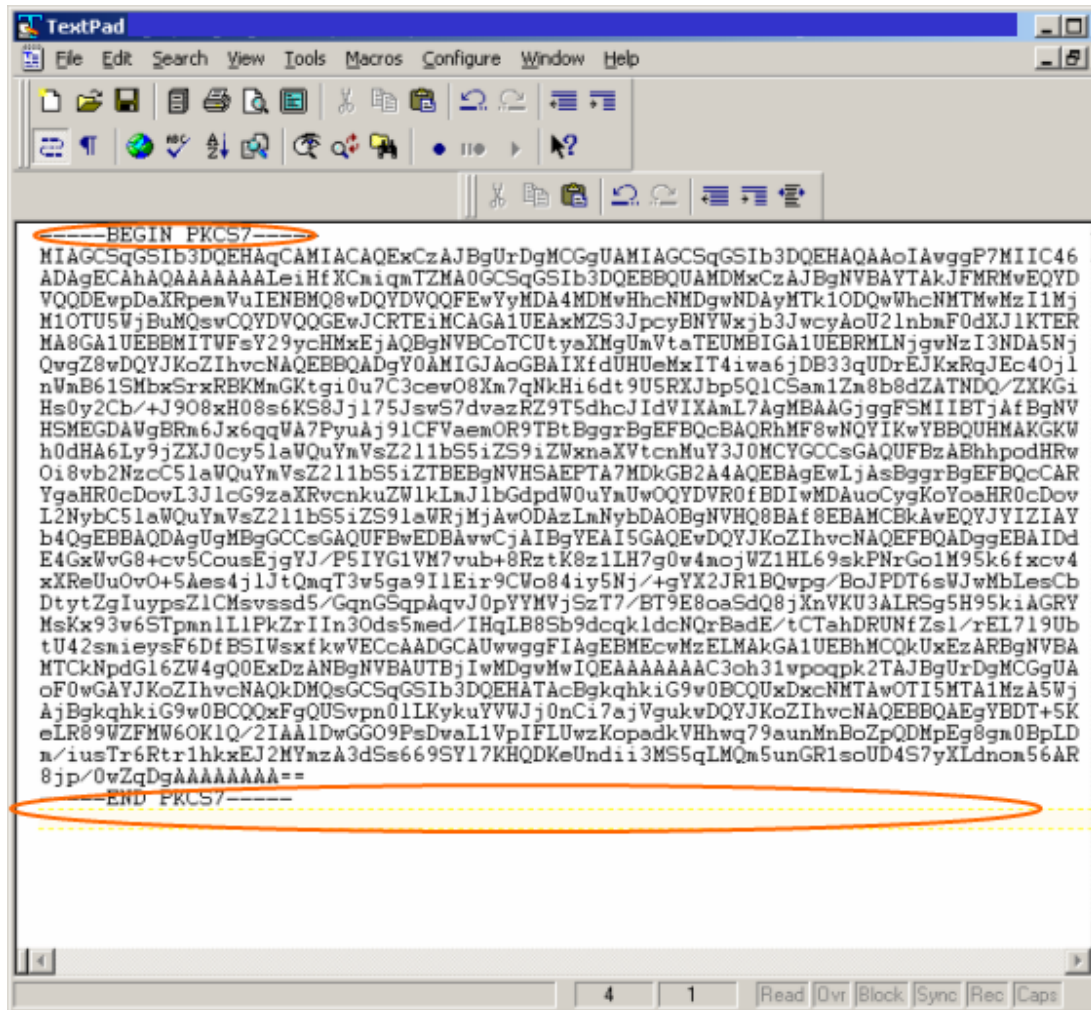


Let op: zodra u uw FS-bestand heeft aangemaakt mag u het FI-bestand niet meer wijzigen. Indien u het FI-bestand toch aanpast zal u een nieuw FS-bestand moeten aanmaken.

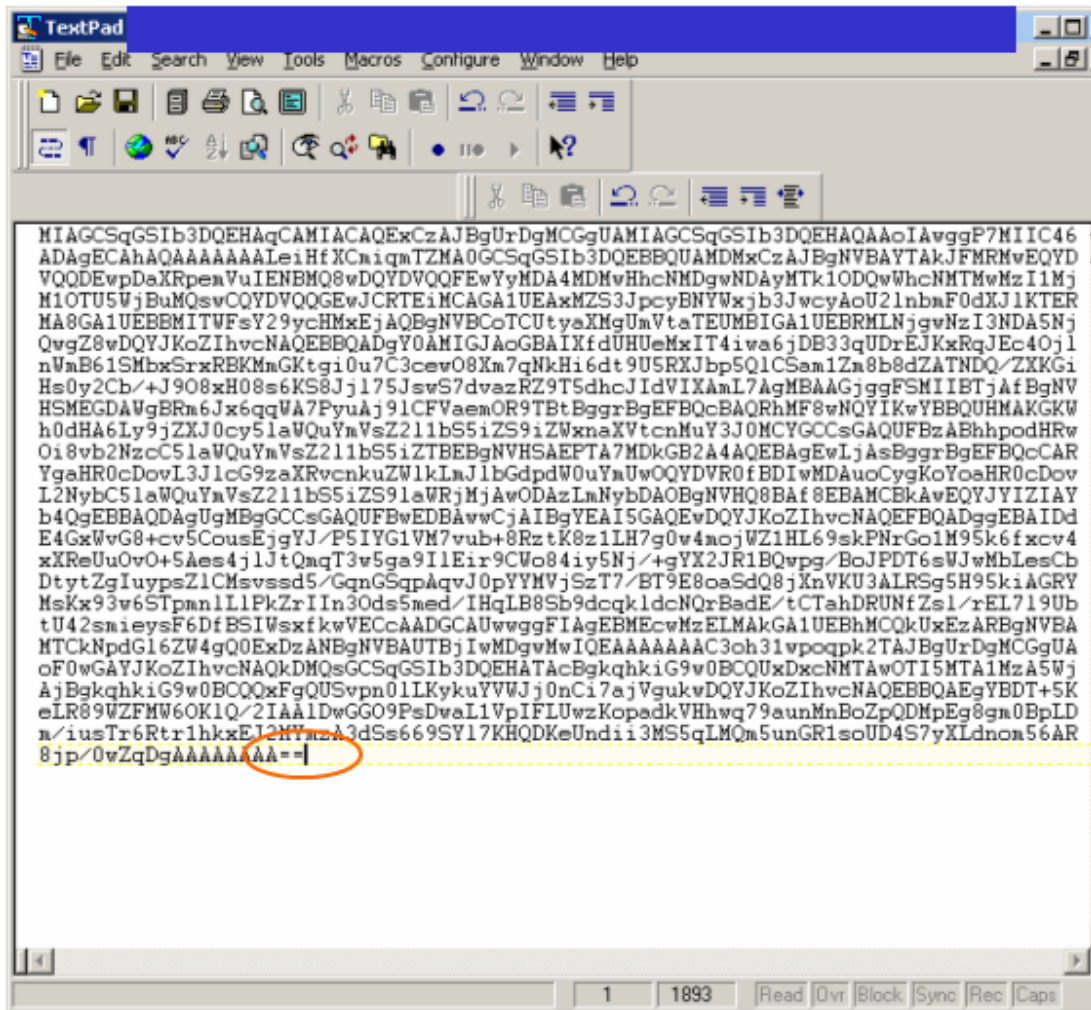
10. Manuele aanpassingen aan uw FS-bestand

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).



Het resultaat van uw FS-bestand wordt m.a.w.:



Na deze aanpassingen bewaart u d.m.v. de toetsencombinatie [CTRL]+[S] het FS-bestand.

11. Vragen

Het Contactcenter kan u hulp en informatie verstrekken bij het opzetten van uw SFTP-kanaal.

Bereikbaar op:

(02/545.50.78
: batch@eranova.fgov.be

Openingsuren:

- Van maandag tot vrijdag, behalve op feestdagen
- Doorlopend van 7u tot 20u