Trusted Third Party

SFTP Extranet via de Filezilla-client

Maart 2013

INDEX

1. Inleiding

Deze handleiding is bedoeld om uit te leggen op welke wijze gebruik kan gemaakt worden van de sFTP server van QI Dataserver (QiD) voor de uitwisseling van gegevens.

Naargelang uw rol in het project zal u zowel gegevens via dit kanaal kunnen aanreiken aan QiD als ontvangen. Nadere instructies voor het gebruik van de eigen bestandsruimte van de sFTP server en de plaats en naamgeving van de gegevensbestanden, maken geen deel uit van deze handleiding.

Deze handleiding gaat uit van een Windowsomgeving. Indien gebruik gemaakt wordt van een Unix-omgeving, gelieve equivalente hulpmiddelen te gebruiken (cfr. Referenties). Bij twijfel, kan u de hulplijn van QiD contacteren (zie onderaan).

De éénmalige voorbereidende stap is het genereren van een sleutelpaar voor toegang tot de server. Enkel in het geval de sleutel niet meer geldig is of gecompromitteerd werd, zal deze procedure opnieuw moeten uitgevoerd worden. Daarnaast moet een sFTP toepassing geïnstalleerd worden. In deze tekst wordt gekozen voor het Filezilla programma.

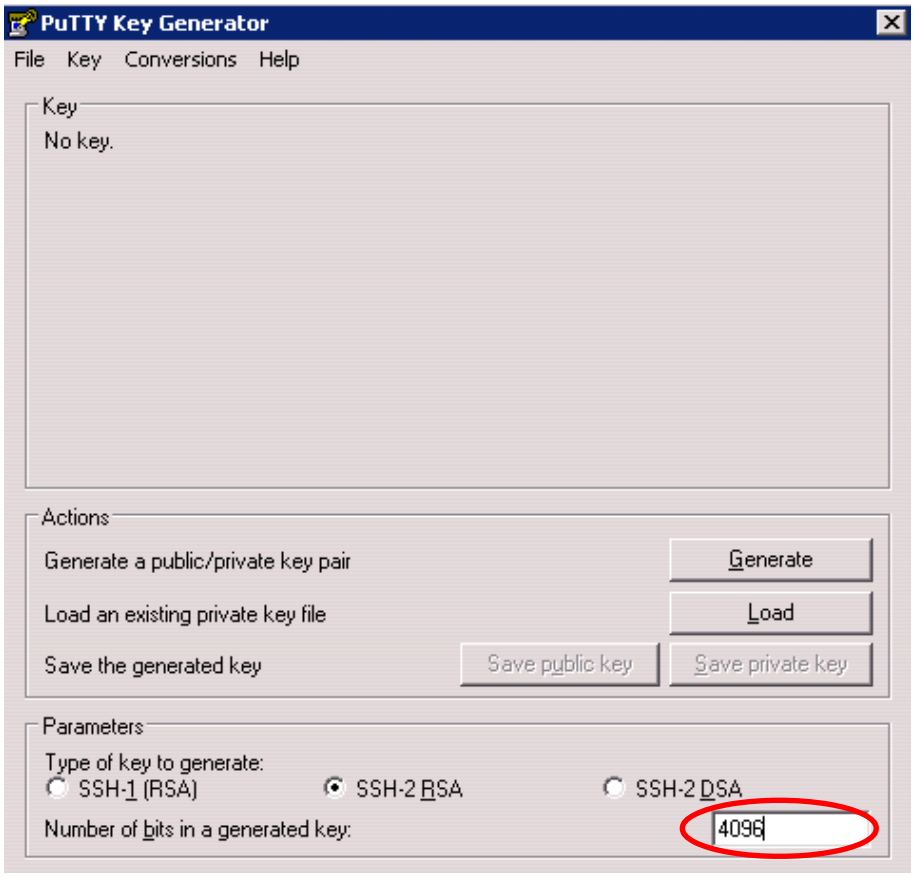
2. Een sleutelpaar genereren (publiek-privé)

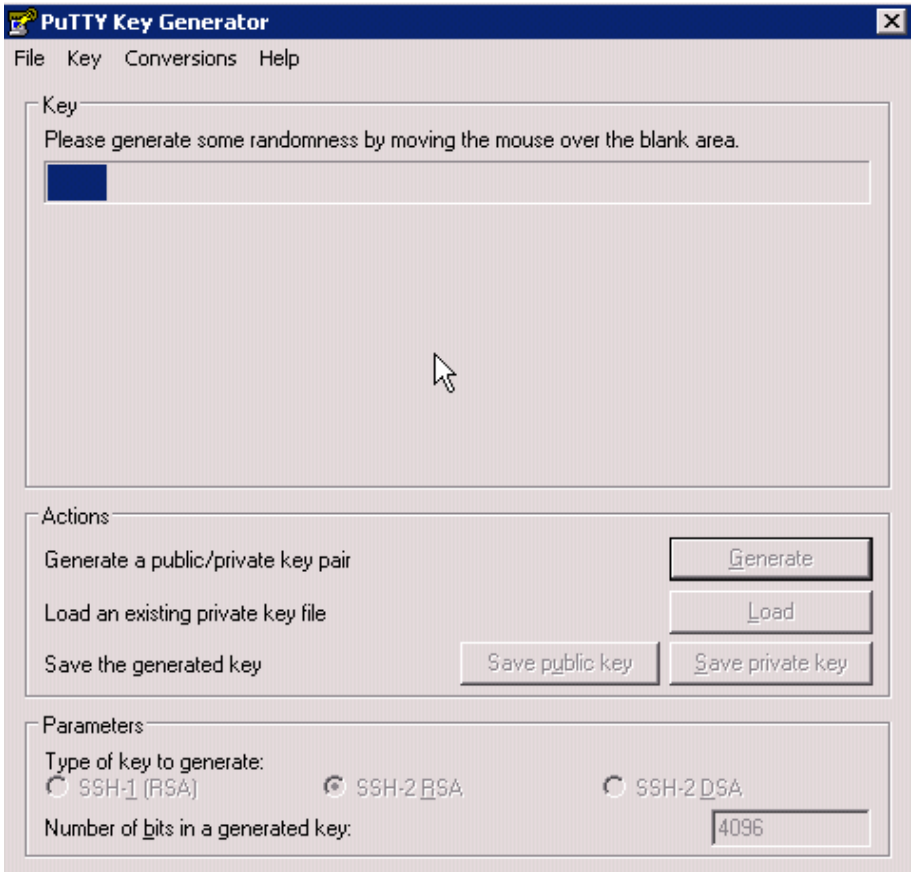
2.1 Starten

Een sleutelpaar is nodig om toegang te krijgen tot de sFTP server. Voor meer uitleg over sFTP verwijzen we naar de informatie bij het socialezekerheidsportaal (zie referenties). Wij stellen voor het programma PuTTy Key Generator te gebruiken. Dit is echter geen verplichting.

2.2 Het sleutelpaar genereren en configureren

1) De sleutel moet altijd 4096 bits lang zijn. Standaard stelt PuTTy Key Generator altijd een lengte van 1024 bits voor. **U moet de lengte dus wijzigen**.
2) Het aanvaarde sleuteltype is het model SSH-2 RSA. Standaard stelt PuTTy Key Generator altijd dit sleuteltype voor, hier hoeft u dus niets te wijzigen.
3) Klik op "Generate".



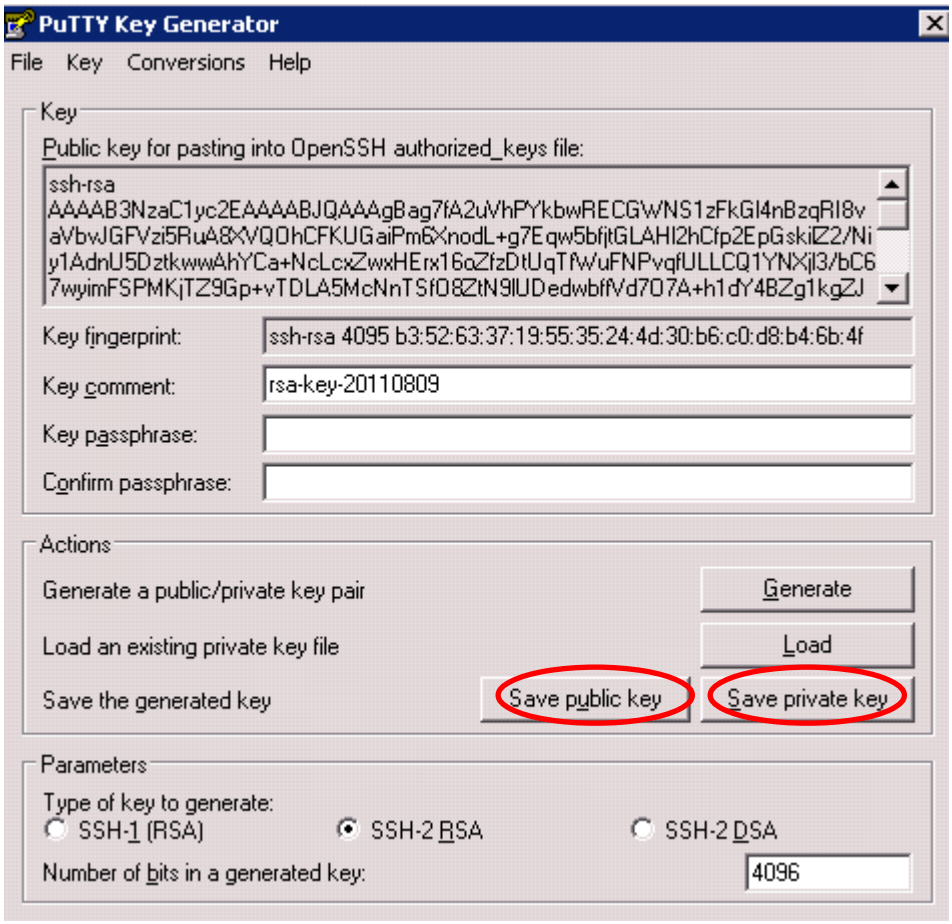


Beweeg de muis over het scherm tot wanneer de sleutel volledig is aangemaakt.

2.3 Het sleutelpaar opslaan

Hier moet u de publieke sleutel en de private sleutel opslaan op uw machine.

Klik op "Save public Key" en "Save private Key". Geef het bestand met de private key een herkenbare naam. De naam van de public key moet aangemaakt worden met "publicKey_IDENT.asc"



Filezilla ondersteunt zelf geen sleutels met een wachtwoordzin (passphrase). Toch wordt aangeraden om de sleutel met een wachtwoordzin te beveiligen om ongeoorloofde toegang tot de sFTP server te vermijden. Om gebruik te kunnen maken van deze sleutels, kan men later pageant, een onderdeel van de Putty programma's, gebruiken. Dit wordt verder in deze handleiding uitgelegd. Voorzie een aangepast beveiligingsniveau voor deze sleutels.

2.4 Publieke sleutel doorgeven

Enkel (i) de **publieke** sleutel (extensie .asc) wordt gemaild naar 'user.tostat@smals.be' en 'UserGa-stat@smals.be', met als subject 'VAZG Z **nummer**'. Het nummer is het erkenningsnummer van het ziekenhuis.

Na een bevestigingsmail van 'user.tostat@smals.be' kan zich men connecteren. Deze mail zal ook de gebruikersnaam bevatten voor het aanmelden.

3. SFTP-client (Filezilla)

3.1. Starten

Start uw SFTP-client via het programma of, als u een icoon geïnstalleerd hebt op uw desktop, via dat icoon.

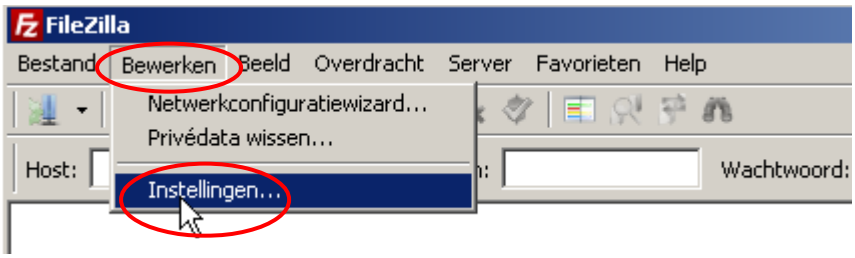
3.2. Uw private sleutel opladen

Doe deze stap alleen als u er mee akkoord gaat dat uw private sleutel niet met een wachtwoordzin wordt beschermd. U zal dan deze sleutel op een andere manier moeten beschermen tegen ongeoorloofd gebruik.

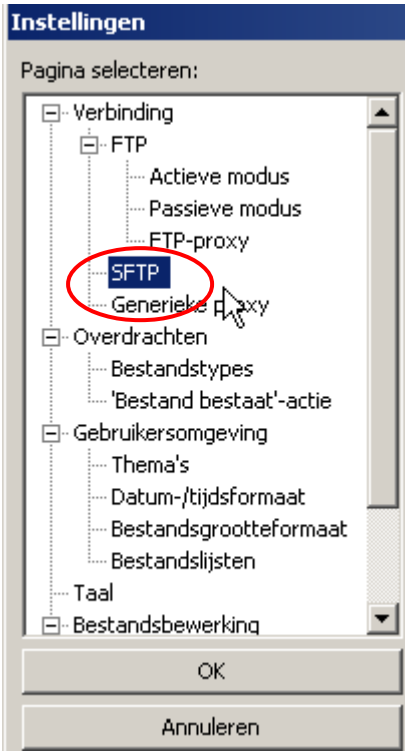
Als er wel een wachtwoordzin is, dan zal Filezilla voorstellen om de sleutel om te vormen naar een sleutel zonder wachtwoordzin en de beveiliging versoepelen. Doe dit liever niet, maar zie verder hoe pageant hierbij kan helpen.

Klik op "Bewerken"/"Instellingen".

Of klik op “Edit”/”Settings” (Engelse versie)

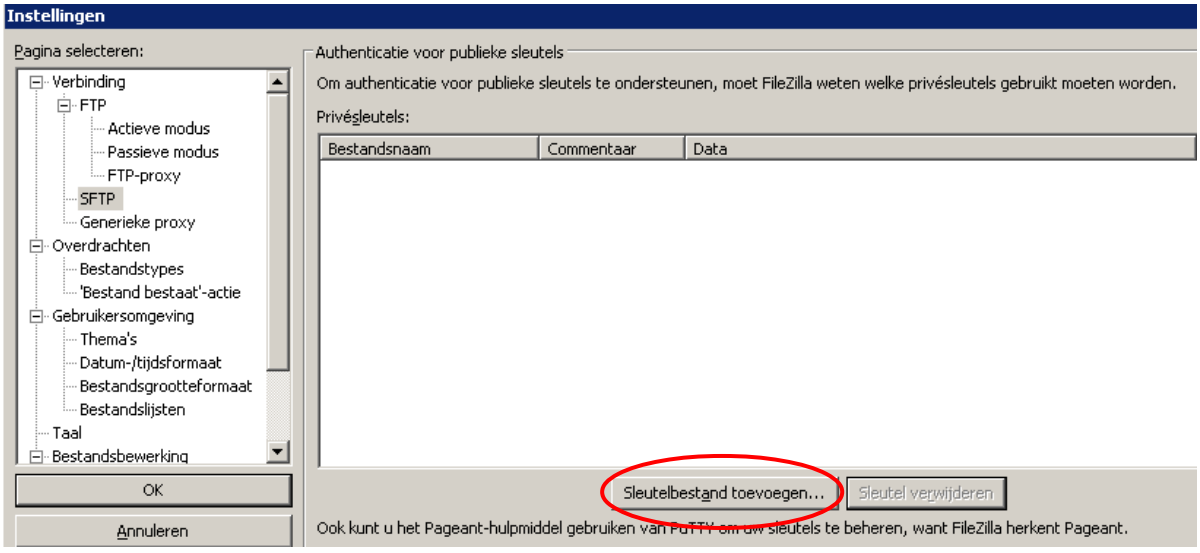


Kies "SFTP".

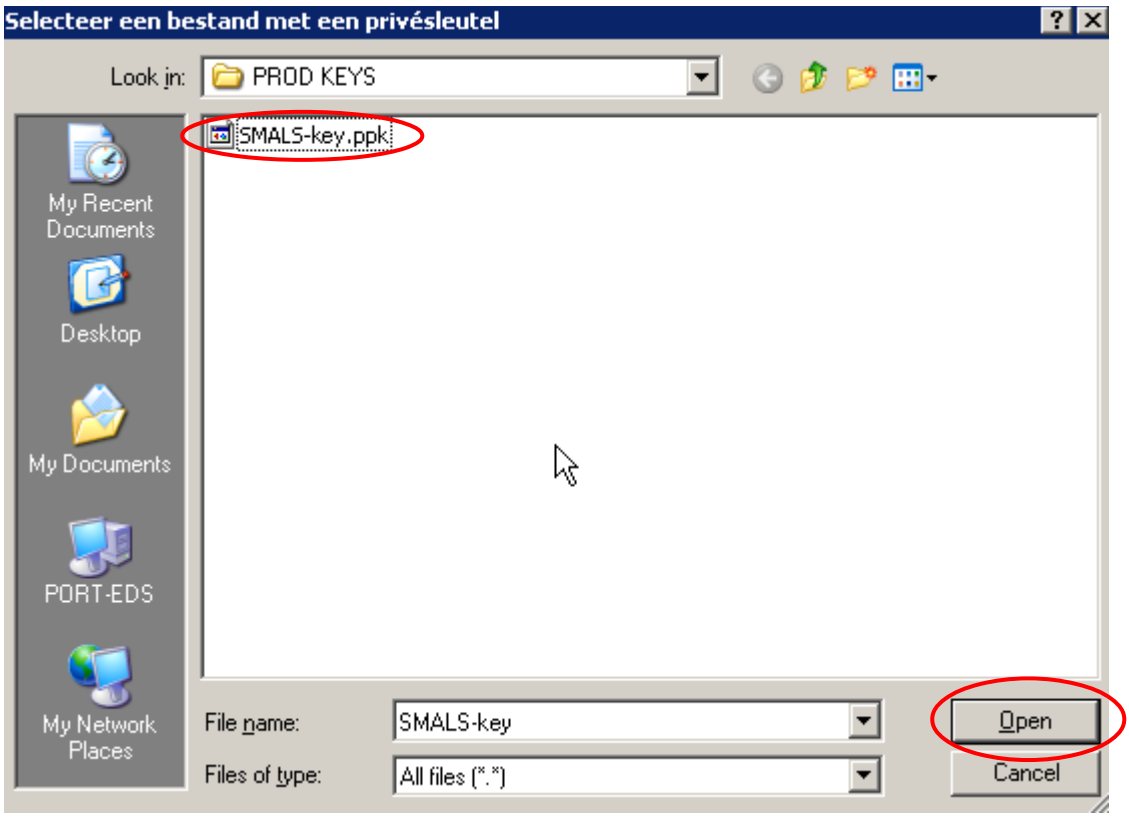


Klik op "Sleutelbestand toevoegen…".

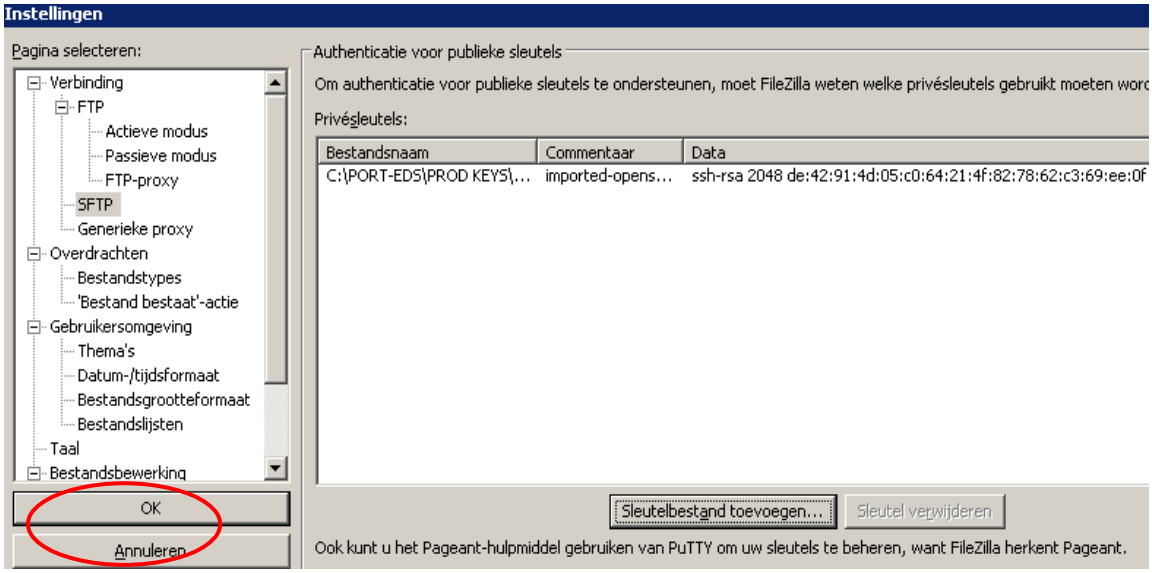
Of klik op "Add keyfile".



Ga naar de locatie waar u uw private sleutel hebt opgeslagen, selecteer het bestand van uw private sleutel en klik op "Open".



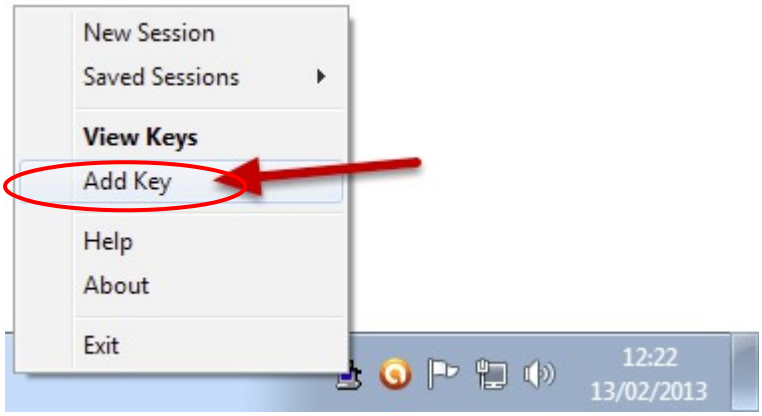
Klik dan op "OK".



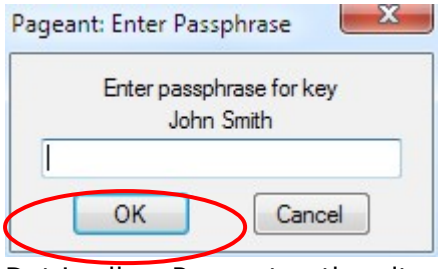
3.3. Gebruik van een beveiligde sleutel

Hier leggen we uit hoe je pageant kan gebruiken met een beveiligde private sleutel. Open de pageant toepassing (deel van de Putty tools – zie referenties voor download). Er lijkt niets te gebeuren, maar kijk onderaan in de taakbalk. Daar is een nieuw icoontje verschenen (eventueel verborgen achter het pijltje), dat lijkt op een computertje met een hoedje op.

Klik met de rechtermuisknop op het icoontje en een context menu verschijnt. Selecteer « Add Key ».



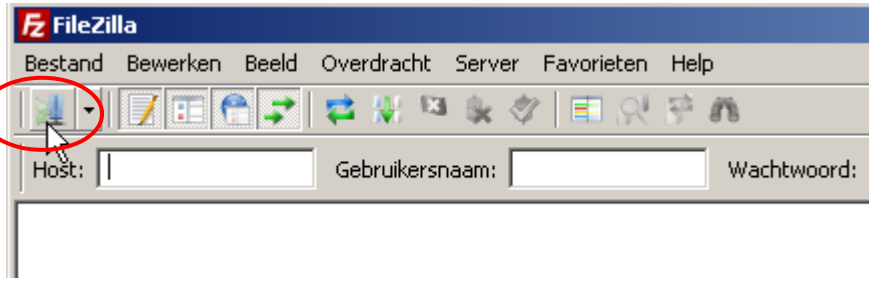
Een venster opent waarin je je private sleutel (extensie .ppk) kan selecteren. Klik op « Open ». Pageant vraagt je om je wachtwoordzin in te geven. Vul in en klik op OK.



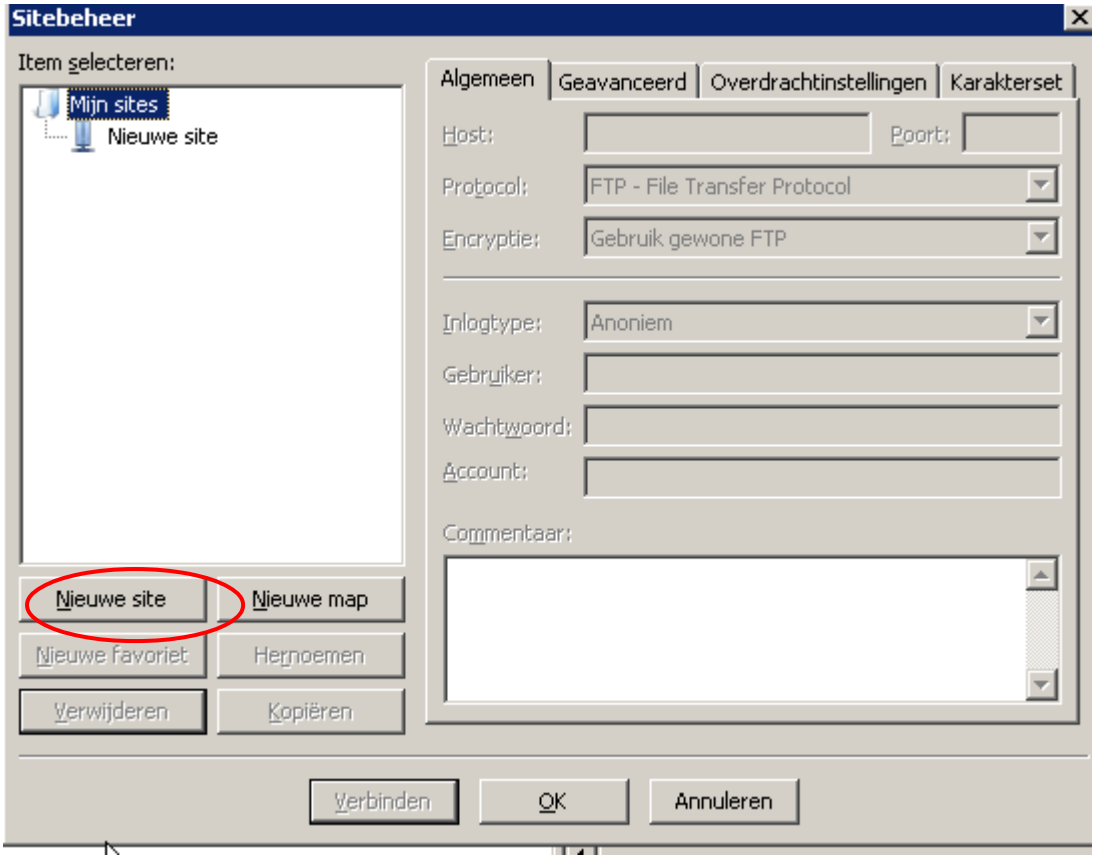
Dat is alles. Pageant onthoudt nu je private sleutel, zolang de toepassing actief is. Dit kan je controleren door het context menu op te roepen en « View Keys » te klikken.

3.4. Verbinding maken met de server

Klik op het icoon  om de Site Manager te openen.



Klik op "Nieuwe Site".



Voer de volgende gegevens in:

Host: sftp.vastransfer.be

Port: 22

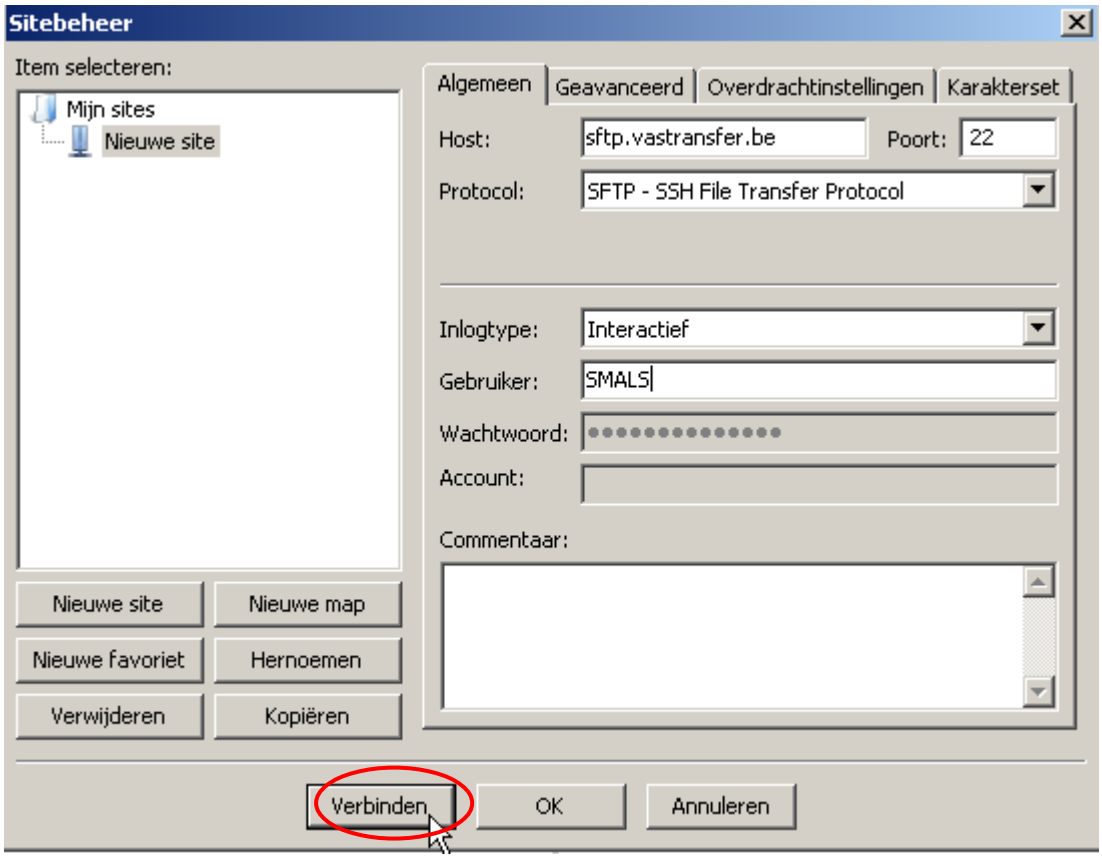
Servertype: SFTP - SSH File Transfer Protocol

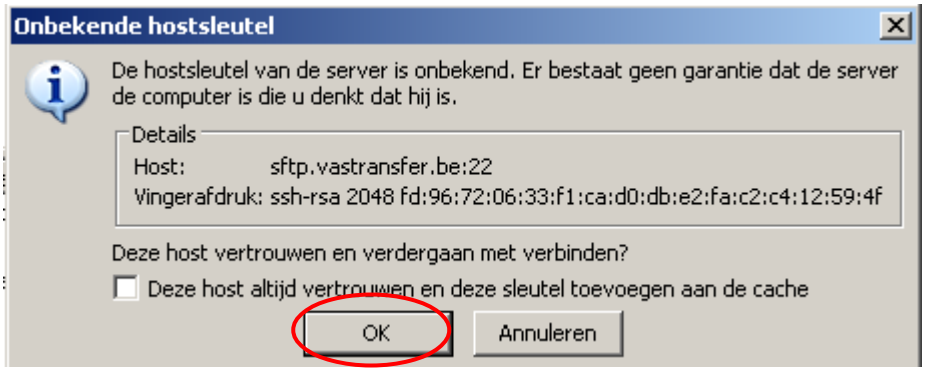
Logontype: Interactief

User: de gebruikersnaam die u meegedeeld werd

Wachtwoord: niet invullen

Klik dan op "Verbinden".

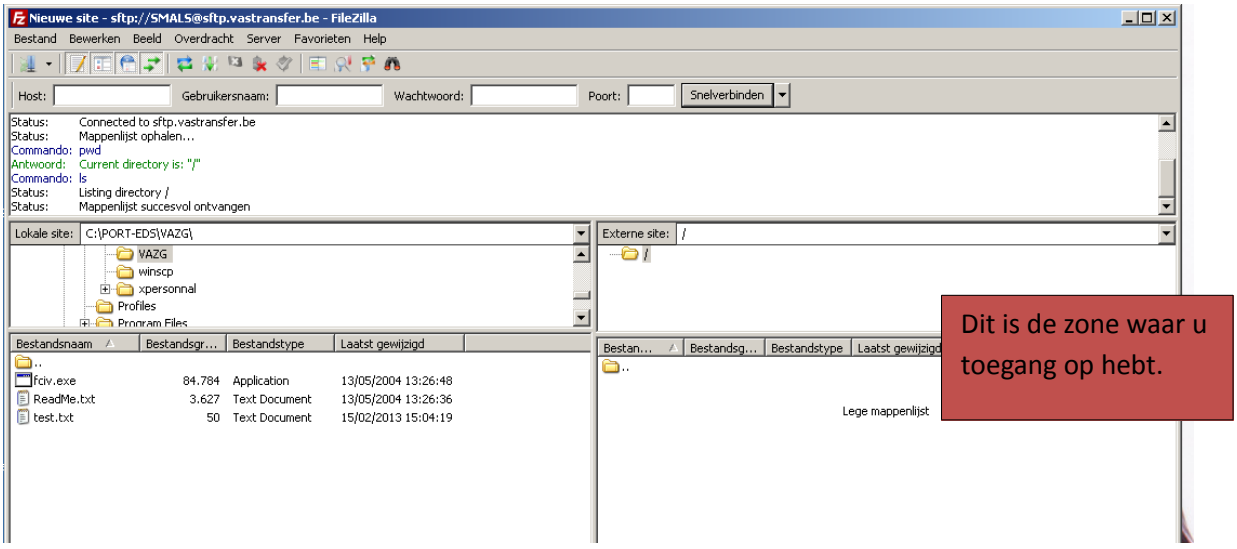




Controleer de vingerafdruk om je er van te gewissen dat het de juiste server betreft. Als dit overeenkomt met het bovenstaande, dan kan je de optie aanklikken om de sleutel toe te voegen aan de cache.

Klik op "OK".

Als alles goed gaat, ben je nu verbonden. Indien je een beveiligde private sleutel gebruikt, dan zal pageant automatisch de juiste sleutel leveren.



4. Bestandsbeheer

4.1 Bestand voorbereiden

Om de integriteit van de gegevens te waarborgen, worden de gegevens met een berekende hash-waarde (SHA-1) verstuurd.

Wij stellen voor om een tool van microsoft te gebruiken, nl http://support.microsoft.com/kb/841290 “**File Checksum Integrity Verifier”**

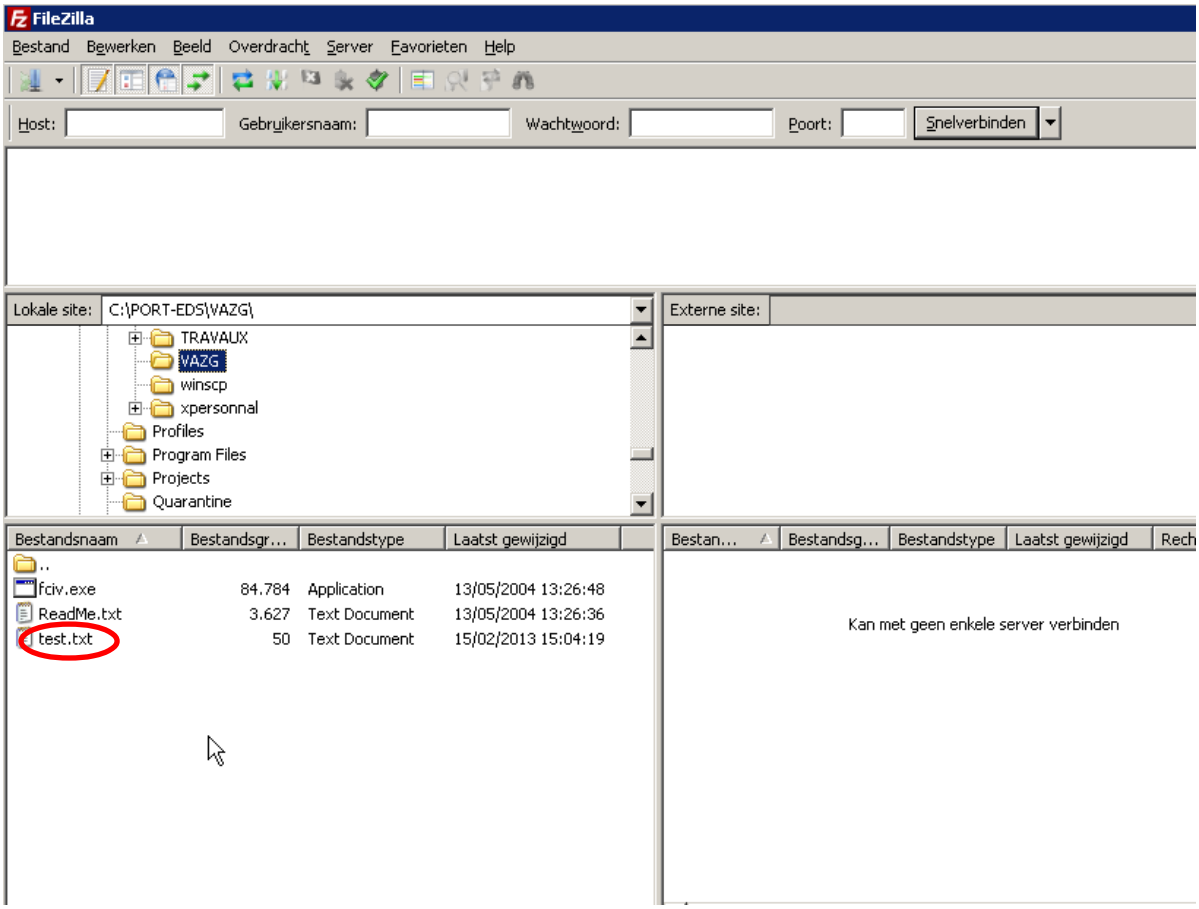
Dit is echter geen verplichting , als maar het algoritme sha-1 wordt gebruikt.

Gebruik alleszins geen online tool waarbij je het bestand naar een webserver uploadt en die dan de hash berekend. Immers op die wijze kan de beheerder van die server al je gevoelige gegevens lezen.

Deze checksum wordt in een controlebestand toegevoegd dat dezelfde naam heeft als het te controleren bestand met de extensie “.hash”. Dus een bestand “gegevens.dat” gaat samen met het controlebestand “gegevens.dat.hash”. Beide bestanden worden dan samen op de sftp server geplaatst.

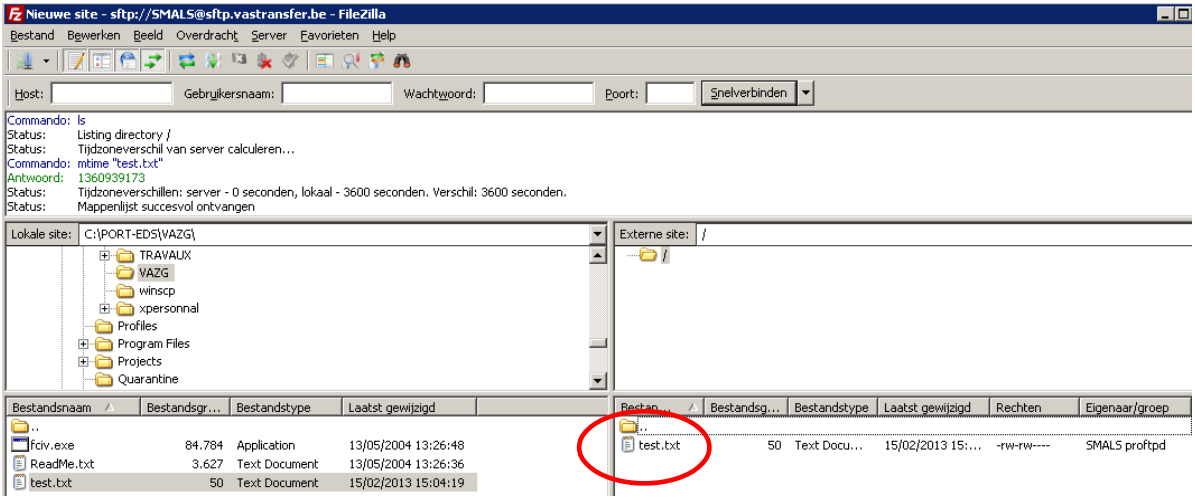
In de softwareset die aangeboden wordt, is een script MakeHash.cmd voorzien die automatisch het .hash bestand aanmaakt.

4.2 Een bestand uploaden



- In het linkerdeel van het scherm zoekt u op uw machine het bestand dat u wil uploaden (hier in het voorbeeld het bestand "TEST.txt").

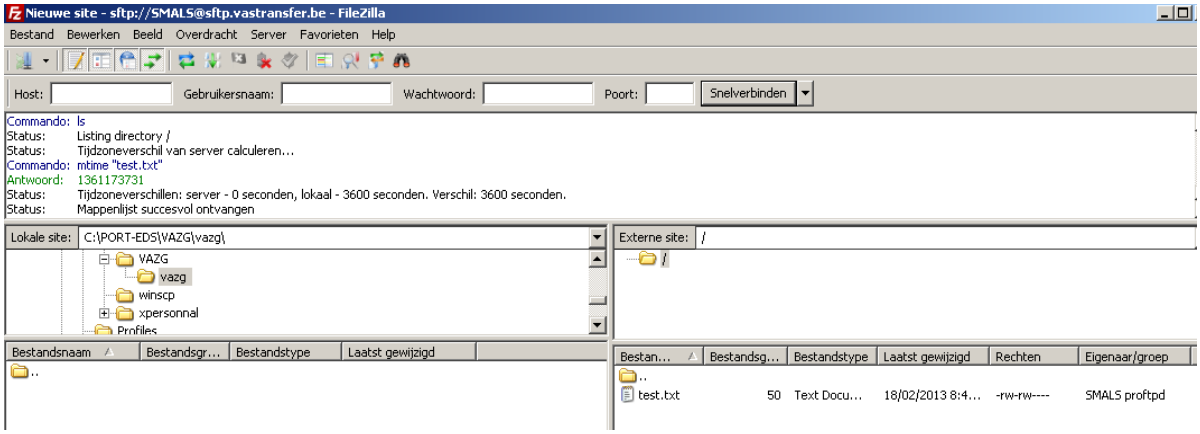
  Sleep het bestand met de muis naar de map van bestemming.



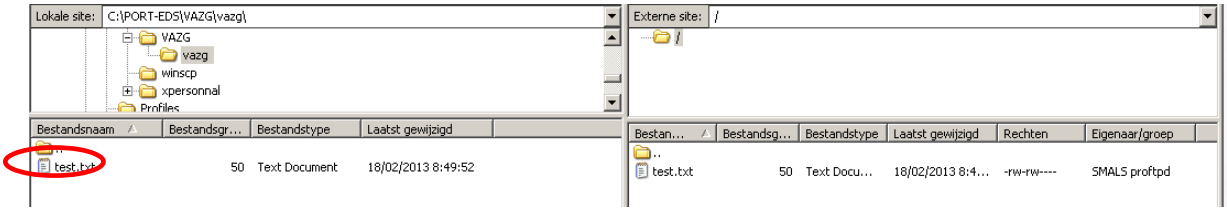
  Het bestand wordt dan in de map van bestemming geplaatst.

4.3 Een bestand downloaden

  Sleep het bestand met de muis van de map naar uw machine.

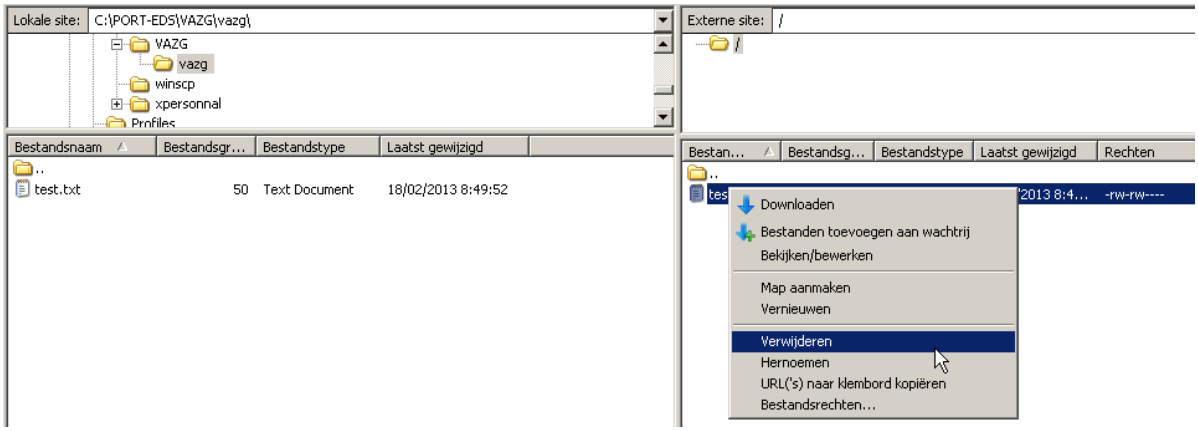


  Het bestand wordt op uw machine geplaatst.



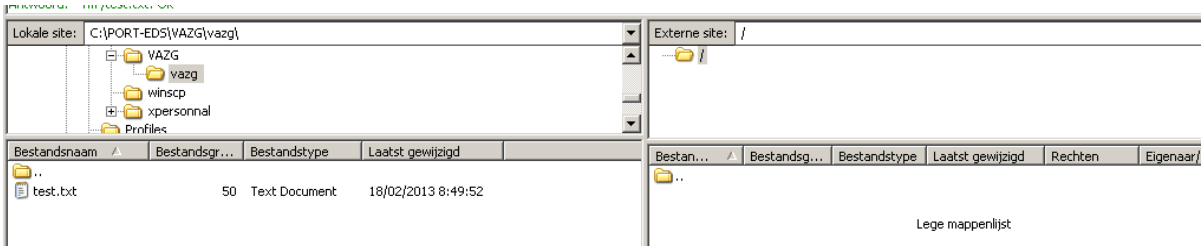
4.4 Een bestand verwijderen

Om een bestand uit een map te verwijderen, volstaat het op dit bestand te klikken met de rechtermuisknop en dan te klikken op “Verwijderen” of "Delete".



Klik op "Yes".

Het bestand is verwijderd.



5. Referenties

5.1 sFTP

Socialezekerheidsportaal :
https://www.socialsecurity.be/site_nl/general/helpcentre/batch/sftp/aboutsftp.htm

https://community.pcextreme.nl/wiki/SSH_en_SFTP_met_public_private_key.

5.2 Software

Putty: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Filezilla : http://wiki.filezilla-project.org/Documentation

Winscp: http://winscp.net/eng/docs/lang:nl

Integriteitsprogramma (SHA1 hash): http://support.microsoft.com/kb/841290

De softwareset voor ZIP en HASH die ter beschikking wordt gesteld via de sFTP server bevindt zich in het bestand sFTP.exe. Voer dit bestand uit of pak het uit met een ZIP programma. Meer uitleg bevindt zich in het ingesloten bestand LeesMij.

5.3 Hulplijn

De hulplijn voor de sFTP kan bereikt worden via 'user.tostat@smals.be' en 'UserGa-stat@smals.be'.

Deze emailadressen mogen maar gebruikt worden voor (technische) problemen met de sFTP-connectie. Voor andere problemen in verband met het project, vind u in de bijgaande documenten de juiste contactadressen.