Handleiding sFTP verbinding opzetten

Versie 3 (2024)

Vlaams Instituut voor Kwaliteit van Zorg

Zorgkwaliteit.be

De kwaliteit van de zorg
in Vlaanderen in kaart gebracht

INHOUD

Inleiding 3

Een sleutelpaar genereren (publiek-privé) 3

Starten 3

Het sleutelpaar genereren en configureren 3

Het sleutelpaar opslaan 5

Publieke sleutel doorgeven 5

Connecteren met Cyberduck 6

Connecteren met WinSCP 9

Opladen van een beveiligde sleutel in WinSCP 9

Connecteren met Filezilla 10

Aanmaken van een verbinding in Filezilla 10

Bestandsbeheer op de server: hash 11

Referenties 12

sFTP 12

Software 12

Hulplijn 12

INLEIDING

Deze handleiding beschrijft hoe u een veilige verbinding met de VIKZ-sFTP-server kan opzetten en gebruiken voor de uitwisseling van gegevens in het kader van de VIKZ-metingen van kwaliteitsindicatoren. Gegevens die via deze verbinding worden verzonden, zijn steeds geëncrypteerd.

Er wordt **eerst** toegelicht hoe u een **sleutelpaar** kan **genereren** dat u toegang geeft tot de server. In principe is dit een **eenmalige voorbereidende stap**. Enkel wanneer de sleutel niet meer geldig is of gecompromitteerd werd, zal u deze procedure opnieuw moeten uitvoeren.

Vervolgens wordt beschreven hoe u **Cyberduck, Filezilla of WinSCP** moet **configureren** om toegang te krijgen tot de dataserver. Cyberduck wordt doorgaans als gebruiksvriendelijker ervaren. Echter, bij problemen kan het gebruik van Filezilla (of eventueel WinSCP) uw IT-dienst meer inzicht geven in wat er precies misloopt (al is onderzoek van de firewall ook steeds nuttig).

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.

In dit document gaan we ervan uit dat u werkt in een Windowsomgeving. Indien u echter gebruik maakt van een Unix-omgeving, gelieve equivalente hulpmiddelen te gebruiken (zie referenties onderaan). Bij twijfel kan u de hulplijn van QI Dataserver (QiD) contacteren (zie onderaan).

EEN SLEUTELPAAR GENEREREN (PUBLIEK-PRIVÉ)

STARTEN

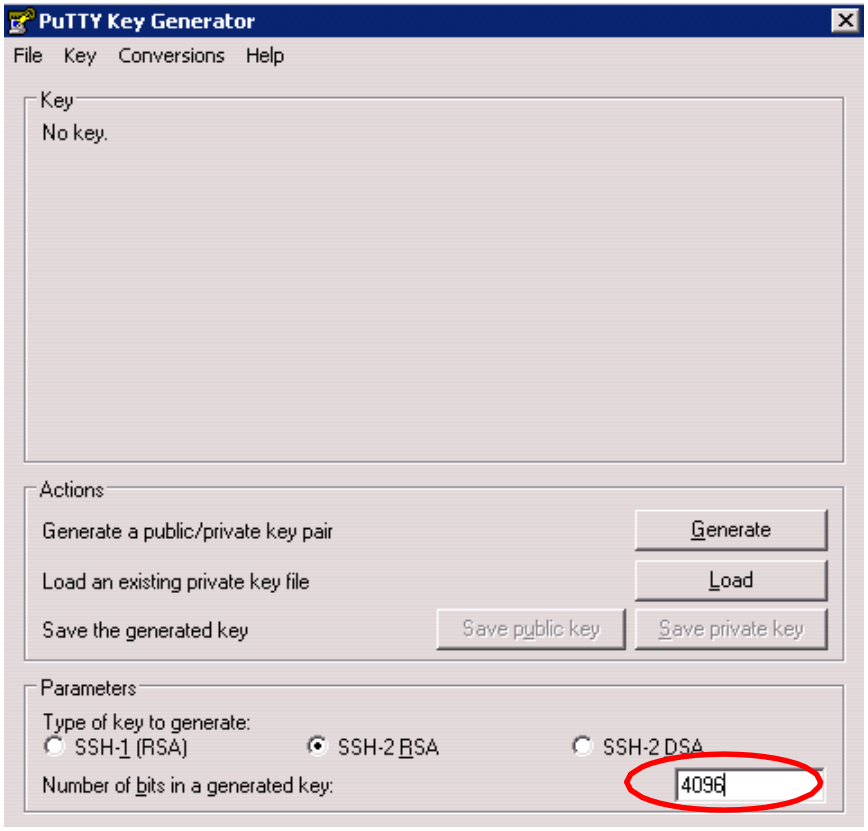
Een sleutelpaar is nodig om toegang te krijgen tot de sFTP server. Voor meer uitleg over sFTP verwijzen we naar de informatie bij het socialezekerheidsportaal. Wij stellen voor het programma PuTTY Key Generator te gebruiken. Dit is echter geen verplichting.

Na downloaden (hier of in Windows store) en installatie vindt u volgend pictogram op uw Bureaublad.

HET SLEUTELPAAR GENEREREN EN CONFIGUREREN

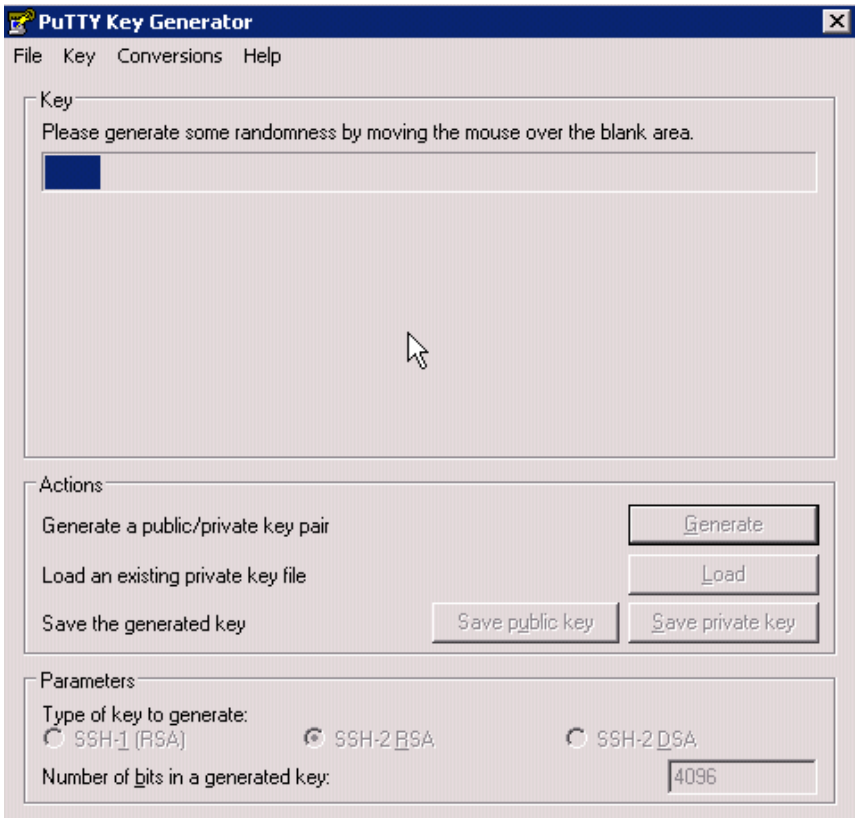
1) Start PuTTY Key Generator door te dubbelklikken op het pictogram.
2) Het aanvaarde sleuteltype is het model SSH-2 RSA. Standaard stelt PuTTY Key Generator altijd dit sleuteltype voor. Hier hoeft u dus niets te wijzigen.

3) 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 (rood omcirkeld in figuur hierboven)**.



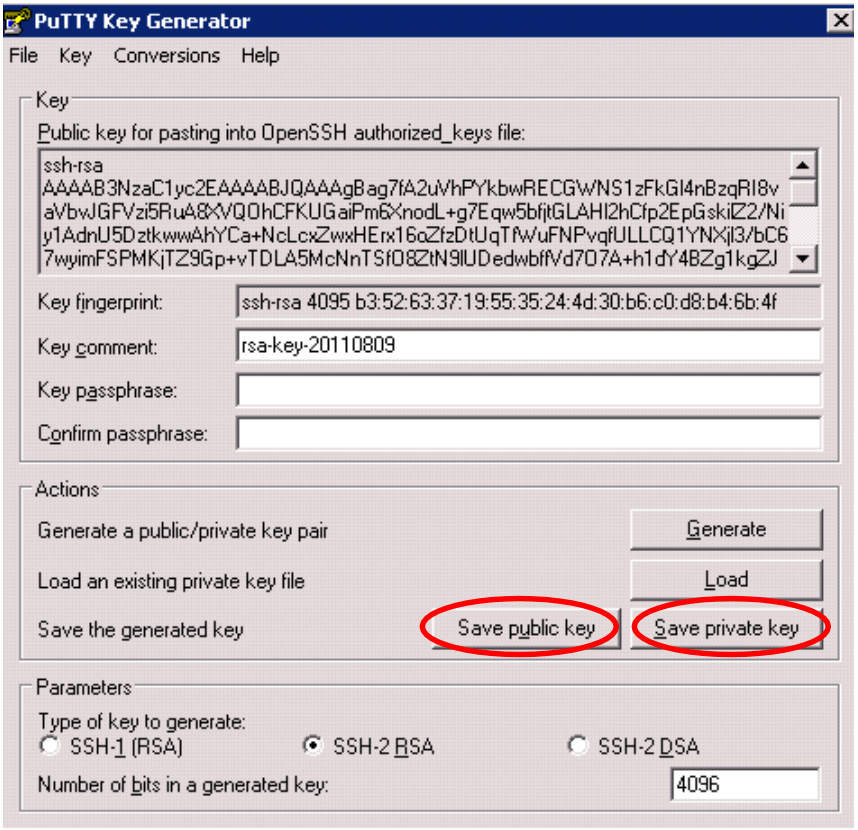
4) Klik op "Generate".

5) Beweeg de muis over het lege gebied op het scherm tot de sleutel volledig is aangemaakt (te volgen o.b.v. de balk die beetje bij beetje blauw wordt bij het aanmaken).



HET SLEUTELPAAR OPSLAAN

Vervolgens vult u een wachtwoordzin in (Key passphrase) en bevestigt u die (Confirm passphrase). Daarna moet u de publieke sleutel en de private sleutel opslaan op uw pc. Klik op "Save public key" en "Save private key". Geef het bestand met de private key een herkenbare naam, zodat u die later gemakkelijk terugvindt. De public key moet opgeslagen worden onder de naam "publicKey_IDENT.asc".



PUBLIEKE SLEUTEL DOORGEVEN

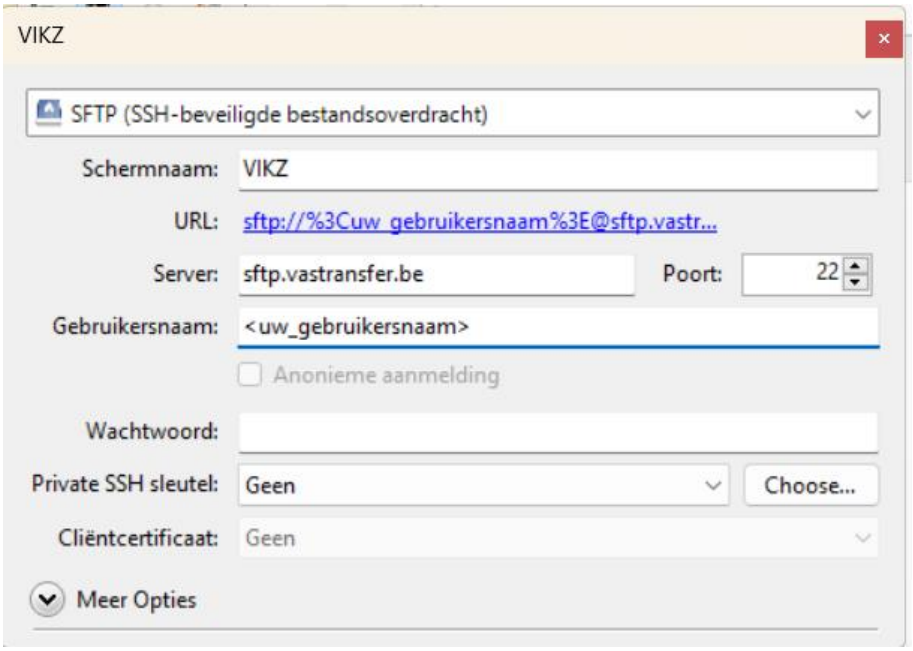
Enkel de **publieke** sleutel (met extensie .asc) wordt doorgegeven aan de Trusted Third Party (TTP), in dit geval Smals. Dat doe je door deze te mailen naar 'UserGa-stat@smals.be', met als onderwerp 'VIKZ en uw gebruikersnaam [Z-***nummer*** voor de sector algemene ziekenhuizen of ***P-nummer*** voor de sector geestelijke gezondheidszorg]. Vraag aan het VIKZ je gebruikersnaam, indien je die niet kent. Je plaatst ook best kwaliteit.az@vikz.be of kwaliteit.ggz@vikz.be in cc van de e-mail, alsook de hoofdarts (de directie in geval er geen hoofdarts is) die akkoord moet zijn dat jij de verantwoordelijke bent voor het toegangsbeheer tot de server voor jullie voorziening.

Nu is het wachten op een bevestigingsmail van 'UserGa-stat@smals.be'. Daarna kan u overgaan naar de volgende stap, namelijk connecteren met Cyberduck, Filezilla óf WinSCP.

CONNECTEREN MET CYBERDUCK

Cyberduck is een open source toepassing voor FTP en sFTP, WebDAV, Cloud en Google Docsvoor Mac OS X en Windows, die o.m. toelaat om op een veilige manier wachtwoorden op te slaan. Een Nederlandstalige versie is beschikbaar. Voor meer informatie over het gebruik met sFTP vindt u in de handleiding (in het Engels).

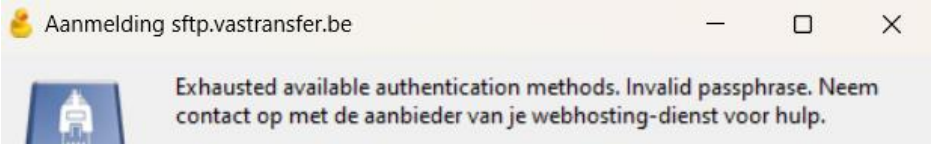
1) U kan de toepassing hier downloaden. Zorg voor regelmatige updates. Momenteel is de versie 8.8 of hoger vereist voor de verbinding.
2) Na installatie opent u de toepassing en kiest u onder het menu “Bladwijzer” voor “Nieuwe bladwijzer” en vult die met de volgende informatie. Kies bij “Private sleutel SSH: je private sleutelbestand dat je hierboven hebt aangemaakt..



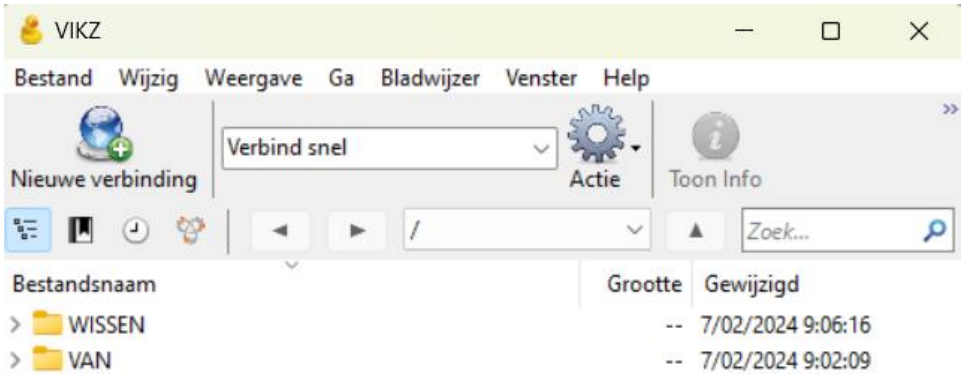
3) Dubbelklik op de aangemaakte bladwijzer. De eerste maal zal je een bericht krijgen van een onbekende vingerafdruk. De huidige vingerafdruk van de server is fd:96:72:06:33:f1:ca:d0:db:e2:fa:c2:c4:12:59:4f. Als die overeenkomt, klik dan eerst op “Altijd”, zodat het in de toekomst niet meer gevraagd wordt en daarna op “Toestaan”. Als dit niet snel genoeg gebeurt, zal het programma aangeven dat er geen verbinding kon gemaakt worden. Start dan opnieuw. Tenslotte zal je wachtwoordzin van je sleutel gevraagd worden en wordt de verbinding gemaakt.

4) Bij problemen kan het log-venster geopend worden, waarin de communicatie met de server wordt weergegeven. Dit kan aan- en afgezet worden met het menu Weergave of Ctrl-L. De informatie die Cyberduck verschaft is echter relatief beperkt; programma’s als Filezilla of WinSCP geven doorgaans meer inzicht in de reden van een gefaalde verbindingspoging, en kunnen daarom om analytische redenen geïnstalleerd worden. Bij problemen is inspectie van de firewall ook aan te bevelen.

   Bij een foutieve instelling (verkeerde gebruikersnaam, sleutel of wachtwoordzin), zal onderstaand bericht worden getoond en kan een nieuwe poging gewaagd worden.

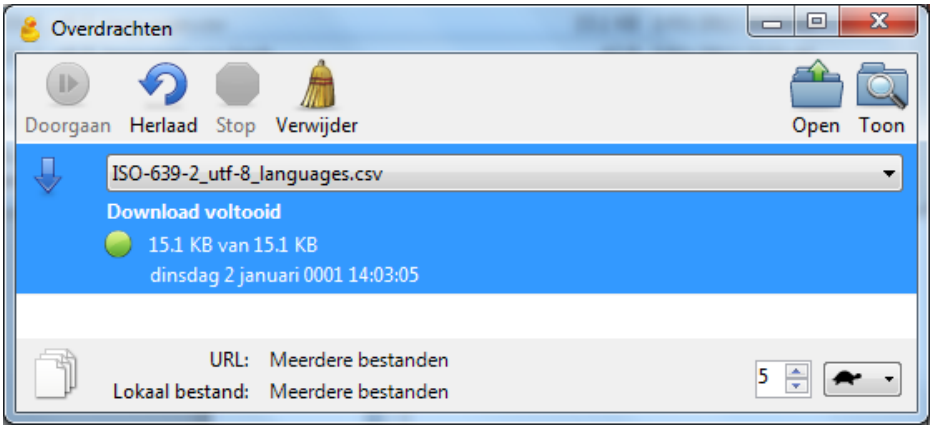


5) Na aanmelding, ziet u in het venster de lijst van bestanden op de server. Verschillende bewerkingen, waaronder kopiëren (downloaden), opladen en een mapkopie (synchronisatie) zijn mogelijk. Kies wat u het meest gebruiksvriendelijk vindt. Er kunnen ook bestanden vanuit en naar Windows Verkenner gesleept worden.



6) Als men kiest voor synchroniseren van een map of voor “download naar”, dient men een map op te geven.

Wanneer bestanden worden uitgewisseld, dan opent het “Overdrachten venster”waarin de transfer kan gevolgd worden.



De bestanden kunnen vanuit dit venster ook rechtstreeks geopend worden of in Verkenner getoond worden. In “Geschiedenis” kan men zien welke verbindingen er zijn aangegaan. Nieuwe verbindingen kunnen zo ook opgestart worden.

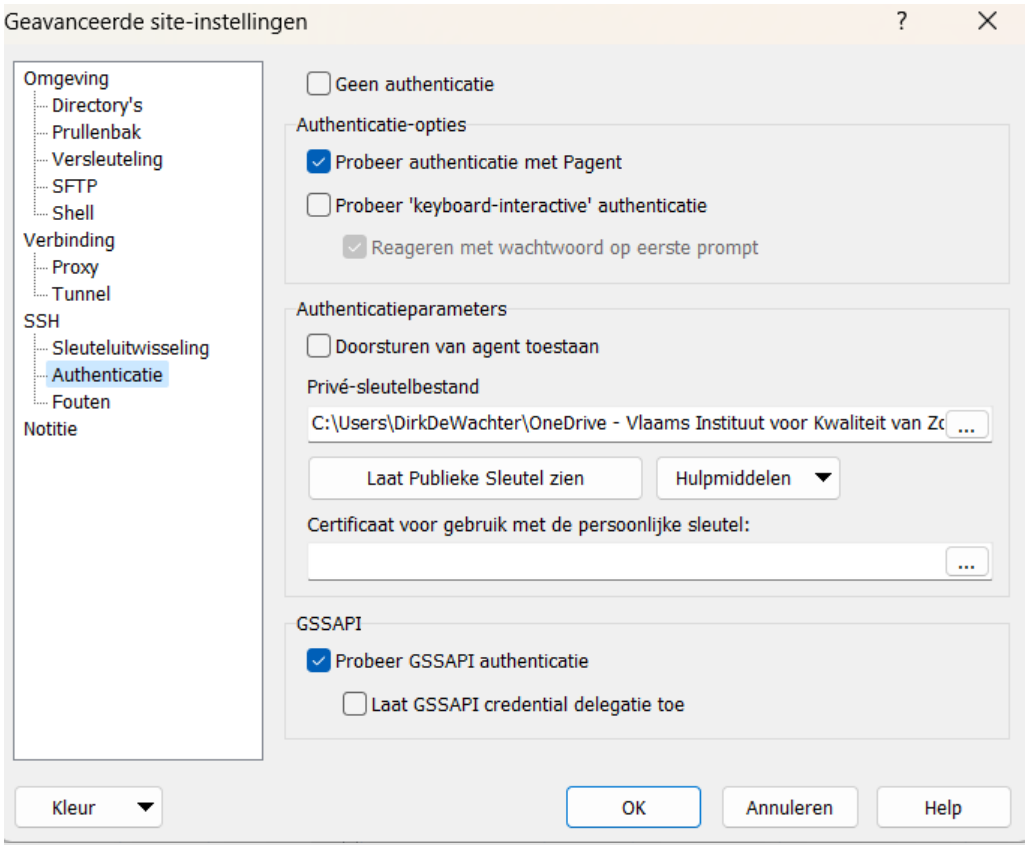
7) Om af te sluiten, selecteer “Verbinding verbreken” onder het Menu “Ga” (Ctrl-Y) of via de knop uiterst rechts op de knoppenbalk.

CONNECTEREN MET WINSCP

WinSCP is een alternatief voor Cyberduck. Het veilig opzetten van een verbinding met wachtwoordzin wordt doorgaans als iets complexer beschouwd. U kan WinSCP hier downloaden. Voor deze toepassing is Pageant nodig. Pageant is deel van de PuTTY-tools, en kan u hier downloaden.

OPLADEN VAN EEN BEVEILIGDE SLEUTEL IN WINSCP

WinSCP zal pageant zelf opstarten. WinSCP laat u bovendien toe om de wachtwoordzin op te slaan, zodat u die niet steeds opnieuw moet intikken (Instellingen > Geavanceerd > SSH > Authenticatie), zie figuur hieronder.



CONNECTEREN MET FILEZILLA

Filezilla is een gekend programma voor verbinding met sFTP-servers. Recente versies laten ook toe om eenvoudig met een sleutelbestand te werken. Dit programma geeft meer informatie wanneer het niet lukt om een verbinding op te zetten. Zo heeft u meer handvatten ter remediëring. U kan FileZilla hier downloaden. Informatie over het opzetten van een verbinding met sleutels staat hier (Engels).

AANMAKEN VAN EEN VERBINDING IN FILEZILLA

1) Kies onder "Bestand" voor Sitebeheer. Klik op de knop "Nieuwe site" en vul volgende informatie in.

2) U kan daarna ook kiezen of en hoe wachtwoorden opgeslagen worden. Kies na het aanmaken de knop "Hernoemen" om de site een naam te geven.
3) Bij de eerste aanmelding zal de vingerafdruk getoond worden
   Vingerafdrukken: SHA256:9y5sKhK4oKVT9RRMiG9JhQdIntEuXgh41cjHGNXIPTw
   Controleer deze en klik dan "Deze host altijd vertrouwen…" aan, zodat deze vraag niet langer wordt gesteld.
4) Bij de verbinding zal dan eventueel de wachtwoordzin van je sleutel gevraagd worden.
5) Na verbinding kan je bestanden uitwisselen.

BESTANDSBEHEER OP DE SERVER: HASH

Om de integriteit van de gegevens te waarborgen, worden de gegevens met een berekende hash-waarde (SHA-1) verstuurd. Concreet zal u steeds twee samenhorende bestanden samen op de server moeten zetten. Het ene bevat uw gegevens, het andere is een controlebestand, dat dezelfde naam heeft als het eerste, maar met toegevoegde extensie ".hash". (Dus een bestand "gegevens.dat" gaat samen met het controlebestand "gegevens.dat.hash".)

Vanuit de TTP worden zoveel mogelijk templates voorzien van een macro die automatisch het bijpassende hash-bestand van uw dataset creëert. Mocht het bijhorende hash-bestand niet vanzelf gecreëerd worden, stellen wij voor 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 die dan de hash berekent. Op die wijze kan de beheerder van die server immers al je gevoelige gegevens lezen.

REFERENTIES

sFTP

https://www.socialsecurity.be/site_nl/general/helpcentre/batch/sftp/aboutsftp.htm
https://support.google.com/youtube/answer/3071034?hl=nl

SOFTWARE

PuTTY / Pageant: https://apps.microsoft.com/detail/xpfnzksklbp7rj?hl=nl-nl&gl=BE , https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.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

HULPLIJN

De hulplijn voor de sFTP kan bereikt worden via kwaliteit.az@vikz.be
(voor de algemene ziekenhuizen en revalidatieziekenhuizen) of
kwaliteit.ggz@vikz.be (voor de geestelijke gezondheidszorg).