4. 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. Het is aangeraden om uw private sleutel te beveiligen met een wachtwoord.

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.

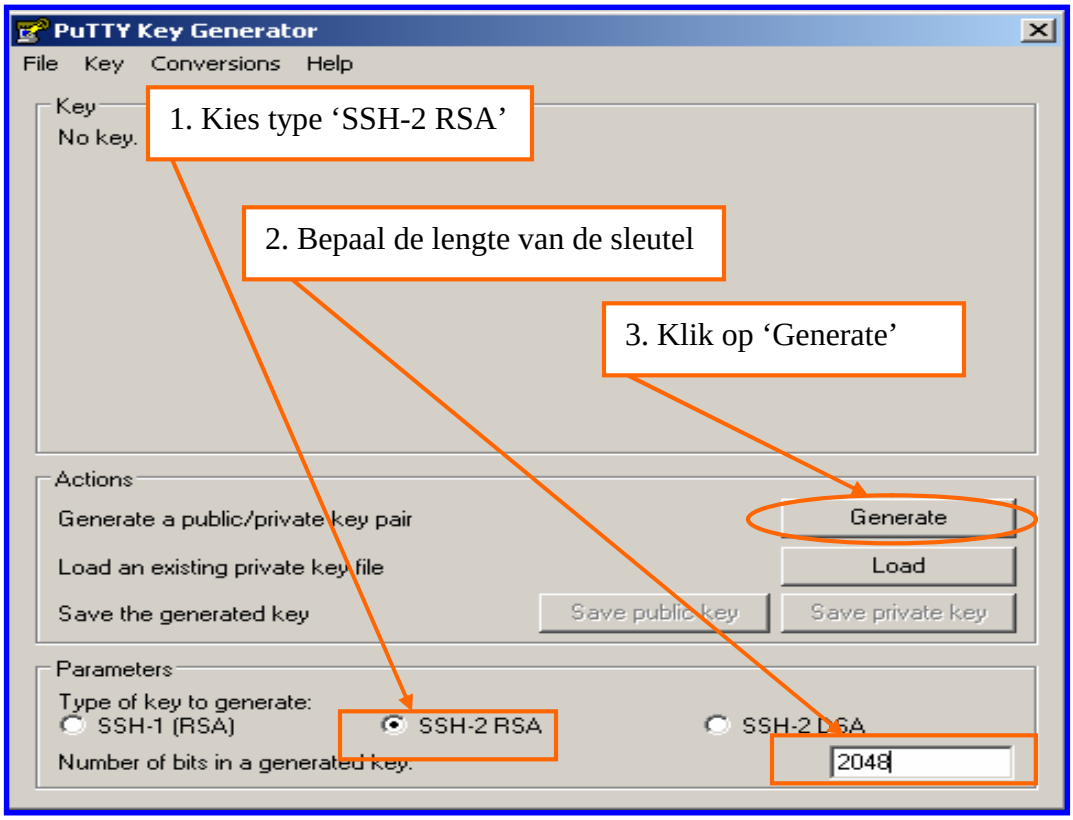
Daarnaast zijn er verschillende formaten voor de publieke sleutels. De meest gangbare zijn deze van de software OpenSSH en de software SSH (commerciële implementatie van SSH-protocol).
Voor de publieke sleutels zullen enkel de formaten van OpenSSH en SSH ondersteund worden.

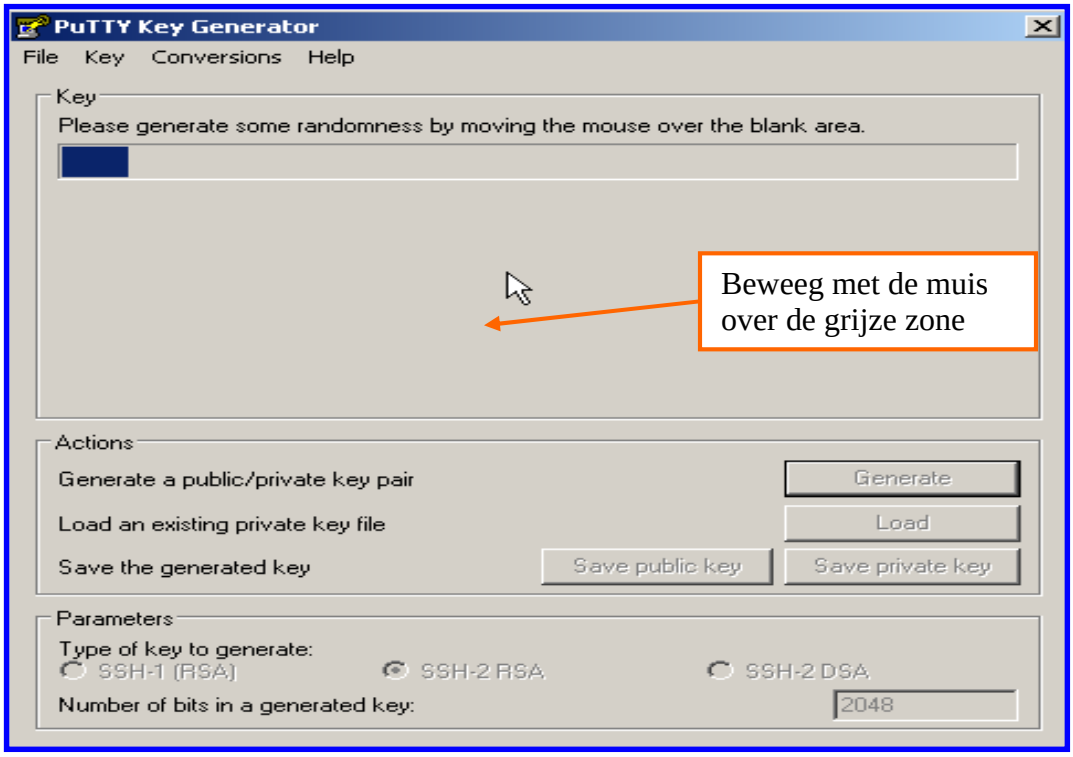
Algoritme & lengte
Bij de generatie van de sleutels dient u op te letten dat u het juiste type sleutel en de juiste sleutellengte kiest.
Er zijn twee mogelijke types (RSA en DSA) waarvan enkel RSA zal aanvaard worden.
Als sleutellengte kiest u 2048 of hoger (3072, 4096). Kortere sleutels zullen niet aanvaard worden.
Wij raden u aan om bij de opslag van deze sleutels uw private sleutel te beschermen met een wachtwoord.

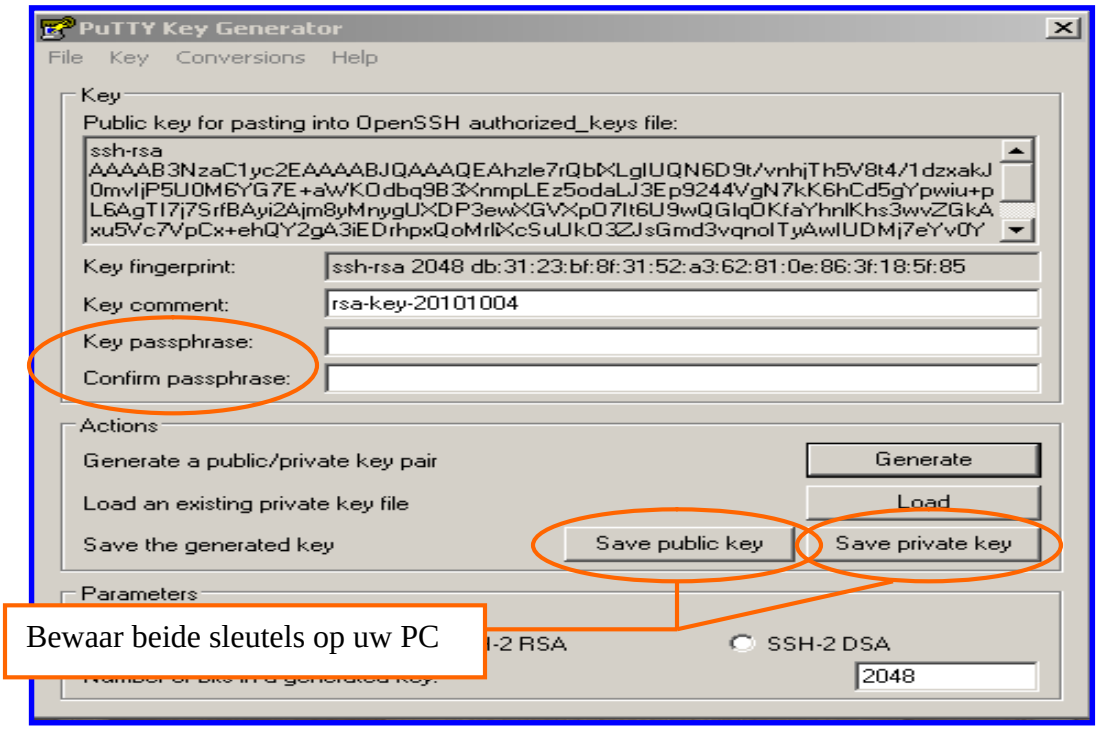
Kort samengevat:

- 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.