Bestanden encrypteren met Cryptomator

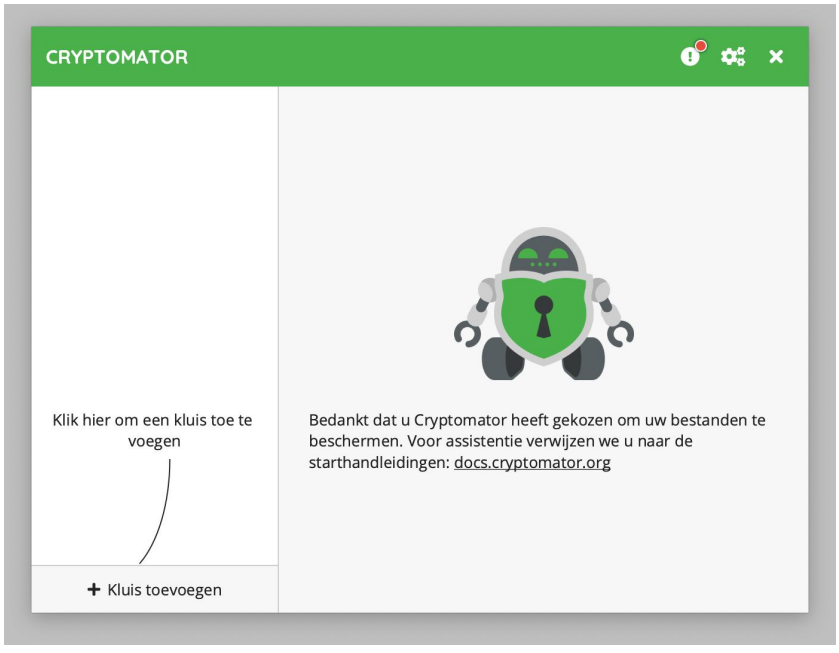
Cryptomator is de beste tool is om bestanden te gaan encrypteren alvorens je ze naar de cloud stuurt. Ontdek hier hoe je er zelf mee aan de slag gaat.

Wellicht besef je dat het belangrijk is om een kopie van je belangrijkste bestanden te bewaren in de cloud, zodat je ze niet verliest. Maar dan maak je je – volledig terecht – zorgen om je privacy.

Want uiteindelijk: wie zegt dat Google of Microsoft niet stiekem in je bestanden aan het neuzen is? Door je bestanden te encrypteren alvorens je ze naar de cloud stuurt, weet je zeker dat niemand je bestanden kan onderscheppen.

1.1. Stap 1 / Cryptomator installeren

Het fijne aan Cryptomator, is dat de applicatie (gratis) bestaat voor alle platformen: Windows, macOS, Linux, Android en iOS.
Zo weet je zeker dat je op elk apparaat je bestanden kan encrypteren en – niet onbelangrijk – ze ook kan decrypteren wanneer je ze wil inkijken.



Om Cryptomator de eerste keer in te stellen, raad ik je aan om de computerversie te gebruiken (en niet de app).

Ga naar cryptomator.org/downloads en download de relevante applicatie voor je computer. De installatie zou zichzelf verder moeten uitwijzen. Na installatie opent Cryptomator en kan je een kluis gaan aanmaken.

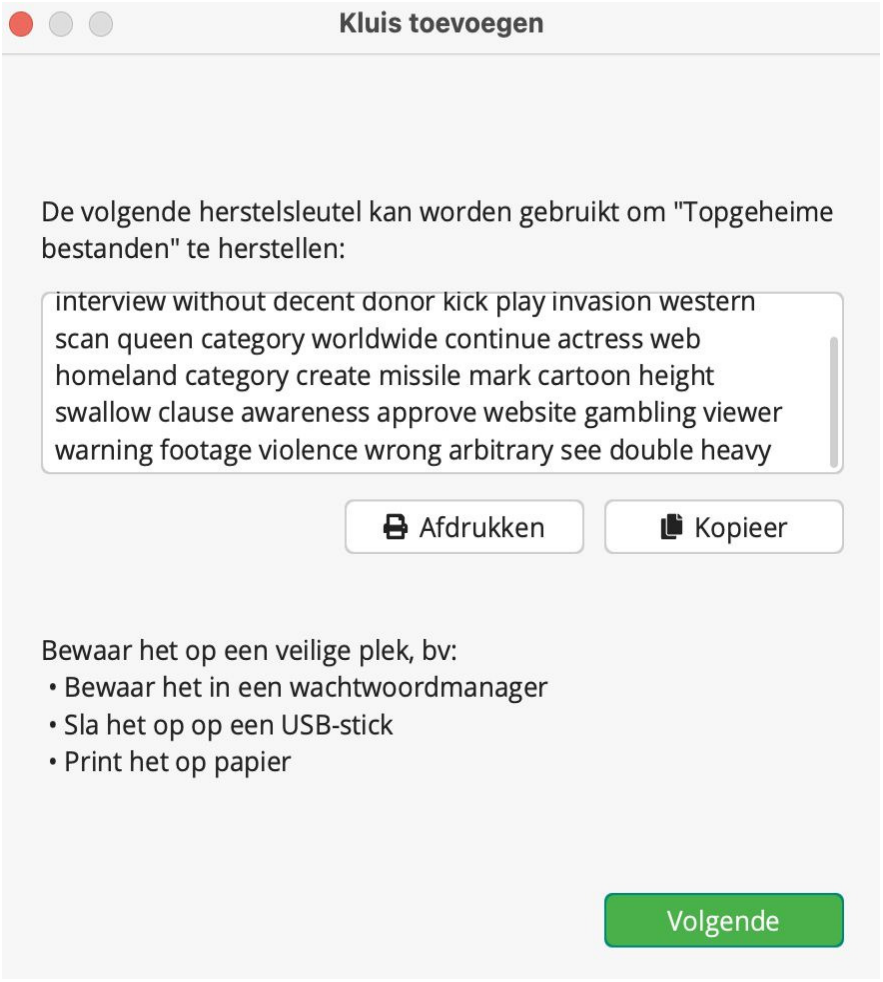
1.2. Stap 2 / Een kluis aanmaken

Cryptomator gebruikt kluizen om je bestanden te beveiligen. Elke kluis heeft zijn eigen wachtwoord en kan zoveel bestanden en mappen bevatten als je maar wil.

Kies voor *Kluis toevoegen* en kies in het nieuwe venster voor *Nieuwe kluis aanmaken*. Geef nu een naam in voor je kluis. Vervolgens wordt er gevraagd waar de bestanden precies moeten worden bewaard. Het is hier de bedoeling dat je kiest voor *Andere locatie* en vervolgens de map van je cloud provider (OneDrive, Google Drive, Dropbox …) kiest. Je kan uiteraard ook een map op je eigen computer kiezen, maar dat is niet bepaald de essentie van deze workshop.

Vervolgens geef je een wachtwoord in. Kies een krachtig wachtwoord, anders heeft de encryptie niet veel zin. Wanneer je dit wachtwoord verliest, dan verlies je ook permanent de toegang tot je bestanden. Er is geen enkele optie om je wachtwoord te resetten.

Wel kan je een herstelsleutel aanmaken, die je kan gebruiken in geval van nood. De herstelsleutel bestaat uit een aantal woorden. Dit kan je best afdrukken en bewaren op een veilige locatie.



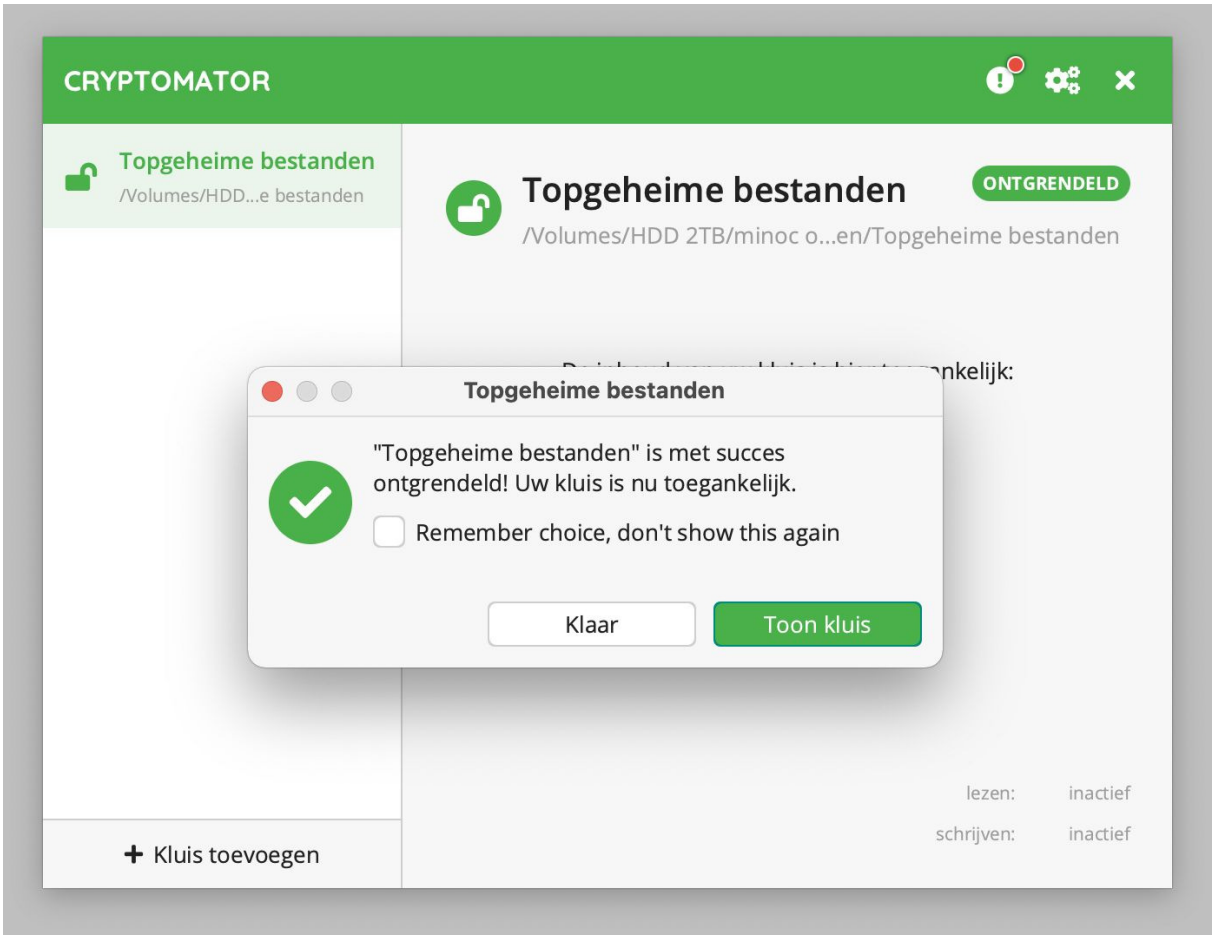
De herstelsleutel kan je bestanden redden wanneer je het wachtwoord vergeet.

1.3. Stap 3 / Kluis ontgrendelen

Neem gerust eens een kijkje naar de map die je in stap 2 hebt aangemaakt. In de map zal je enkel nietszeggende bestanden vinden. Dat is de bedoeling. Je dient namelijk eerst de kluis te 'ontgrendelen' alvorens er gebruik van te maken.

Ga naar Cryptomator, selecteer je kluis en kies voor *Unlock*. Je zal nu het wachtwoord moeten invoeren en vervolgens krijg je de melding dat je kluis werd ontgrendeld.

Er zal nu een speciale virtuele schijf worden geopend op je computer. Wanneer dit niet zo is, kies je in Cryptomator voor *Toon schijf*.



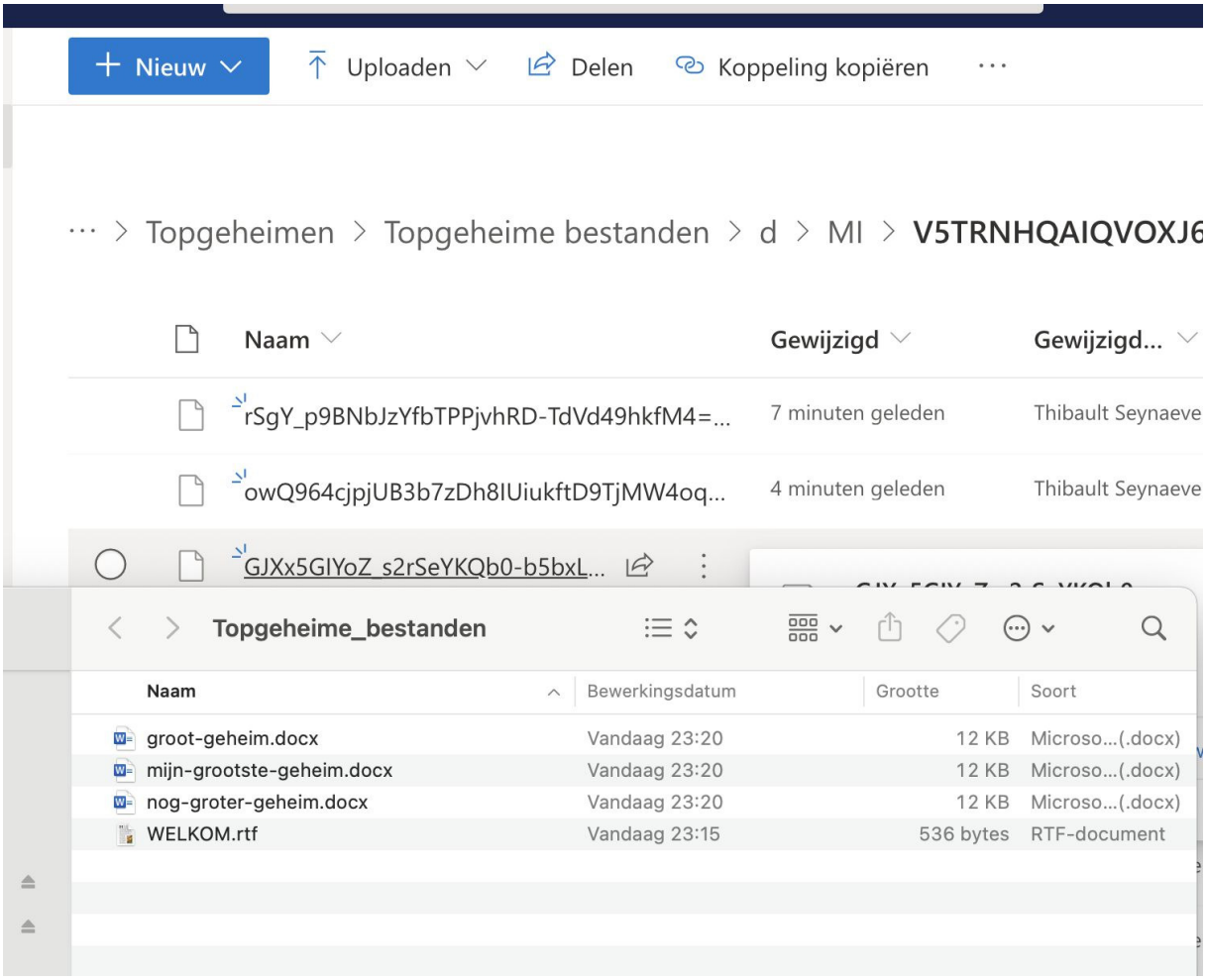
Ontgrendel de kluis en sla je geheime bestanden op in de virtuele schijf.

1.4. Stap 4 / Bestanden encrypteren

Wil je bestanden encrypteren, dan is het belangrijk om al deze bestanden in deze virtuele schijf te plaatsen. Gebruik dus niét het mapje dat je hebt aangemaakt in OneDrive, Google Drive, Dropbox of een andere cloud provider.

Probeer het even uit en sla wat bestanden op in de virtuele schijf van Cryptomator. Wacht nu tot de bestanden worden opgepikt door je cloud provider (in mijn geval OneDrive). Open daar de map die je hebt aangemaakt, en je zal zien dat er hier geen spoor is van de bestanden die je net hebt aangemaakt.

Toch zijn ze er wel, maar dan in geëncrypteerde vorm. Wil je de bestanden inkijken, dan zal je de Cryptomator-applicatie moeten gebruiken om de kluis eerst te ontgrendelen.



Bovenaan hoe OneDrive de bestanden ziet, onderaan hoe de bestanden in de ontgrendelde kluis staan.

Bron: TechPulse van 14 januari 2021