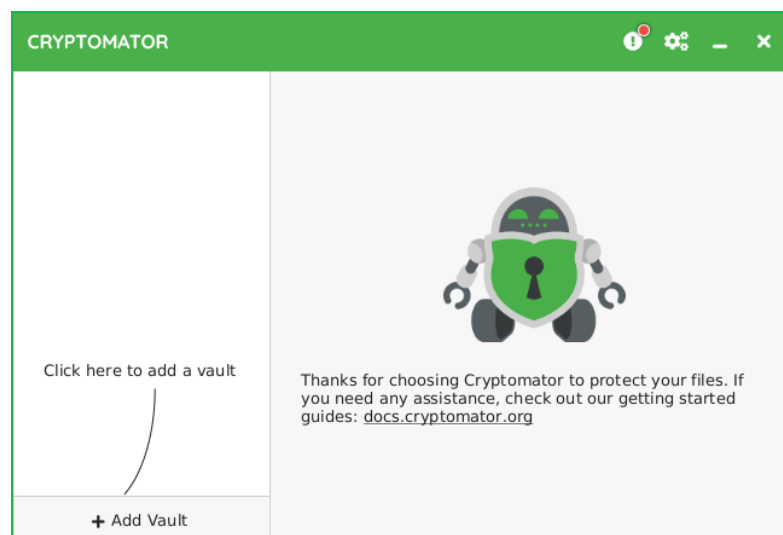


# CRYPTOMATOR ALS KLUIS IN DE CLOUD

Cryptomator is een encryptieprogramma waarmee je één of meer gecodeerde mappen (kluizen) kan beheren. Toegang tot zo'n kluismap is beschermd met een wachtwoord. Een kluismap kan je lokaal toevoegen, maar als je deze toevoegt binnen de lokale synchronisatiemap van een clouddienst, dan kan je de kluismap via de cloud met meerdere apparaten delen.

Cryptomator is “Open source” en beschikbaar voor Windows, macOS, Linux, iOS en Android (gratis desktop app; eenmalige aankoop mobiele app; geen abonnement nodig).

Getest is met Windows 10 Pro / Home en Ubuntu 20.04 LTS / 22.04 LTS en de Microsoft OneDrive clouddienst<sup>(1)</sup>.



## Wat kan je met Cryptomator aan de hand van deze handleiding?

- ➡ Cryptomator installeren en instellen in Linux en Windows.
- ➡ Cryptokluizen gebruiken in lokale mappen of te verwijderen opslagmedium (usb-stick).
- ➡ Cryptokluizen via een clouddienst synchroniseren over meerdere apparaten met verschillende bedrijfssystemen door één of meer kluizen in de synchronisatiemap van de betreffende cloud-provider te plaatsen (OneDrive).
- ➡ Alleen in Windows: Cryptomator starten en waar je wilt kluizen gebruiken vanaf een te verwijderen medium op computers zonder Cryptomator (met behulp van Cryptomator-portable).

<sup>1)</sup> Voor een Nederlandstalige handleiding “OneDrive in Ubuntu Linux gebruiken” zie [bron \[7\]](#) (HCC open source site).

## Inhoudsopgave

Inleiding .....	3
Ubuntu Linux – Cryptomator installeren .....	4
De algemene voorkeuren aanpassen.....	6
Een of meer kluizen toevoegen .....	8
Cryptomator gebruiken en instellen per kluis.....	12
De Cryptomator kluis openen en er in werken.....	12
Acties en voorkeuren per kluis .....	13
Koppelen aan een bestaande kluis.....	15
De gebruikte paden en instellingen van Cryptomator .....	17
Windows – Cryptomator installeren .....	18
De algemene voorkeuren aanpassen.....	18
Een of meer kluizen toevoegen .....	21
Cryptomator gebruiken en instellen per kluis.....	24
De Cryptomator kluis openen en erin werken.....	24
Acties en voorkeuren per kluis .....	25
Koppelen aan een bestaande kluis.....	28
De gebruikte paden en instellingen van Cryptomator .....	30
Kluis op een usb-stick.....	31
De usb-stick voorbereiden in Linux.....	31
Een USB kluis openen in de Linux bestandsverkenner .....	32
De usb-stick voorbereiden in Windows.....	33
Cryptomator portable installeren op de usb-stick (alleen Windows) .....	34
De gebruikte paden en instellingen van Cryptomator portable .....	35
Cryptomator-portable op andere Windows computers gebruiken.....	36
Bronnen (Engels- of Nederlandstalig).....	38

### Opmerking:

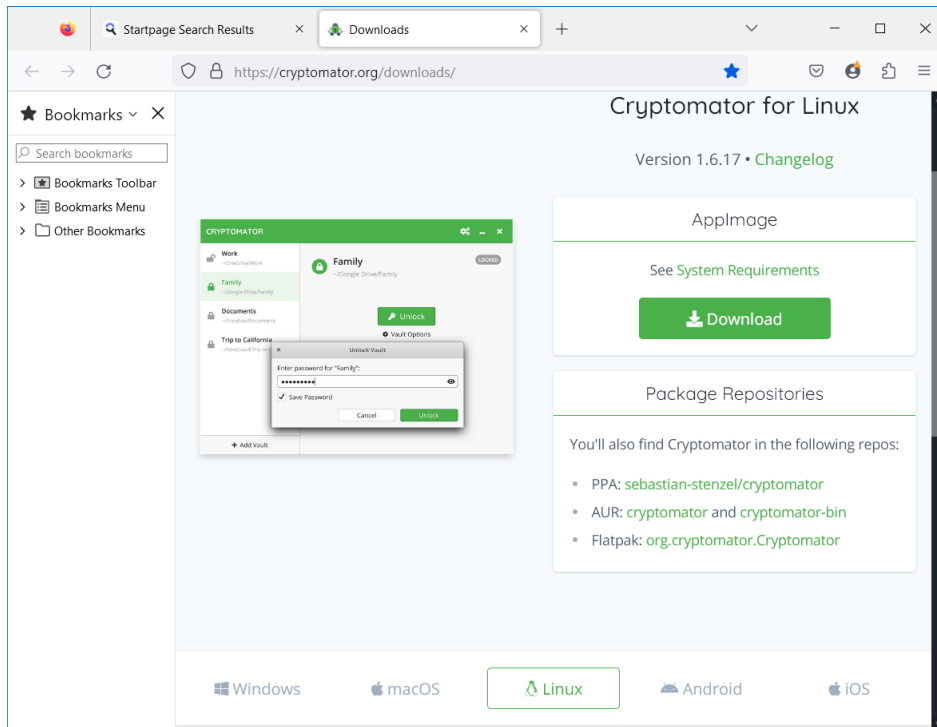
In dit document zijn hyperlinks en kruisverwijzingen gebruikt. Hyperlinks zijn onderstreept en verwijzen naar websites of interne bladwijzers. Kruisverwijzingen verwijzen naar koppen of genummerde items. Bronvermeldingen zijn bijvoorbeeld [bron](#) [1].

Hier is [bron](#) de hyperlink naar de betreffende website; [1] is de bijbehorende kruisverwijzing naar het volgnummer in de lijst van [Bronnen \(Engels- of Nederlandstalig\)](#).

## Inleiding

Cryptomator voor verschillende besturingssystemen kan je downloaden vanaf [bron \[1\]](#).

De Engelstalige online handleiding vind je op [bron \[2\]](#); een Engelstalige handleiding in PDF formaat kan je downloaden vanaf [bron \[3\]](#).



Voor Linux zit achter de knop “Download” – op het moment van schrijven <sup>(2)</sup> – de *cryptomator-1.7.2-x86\_64.AppImage* download; voor Windows is dit *Cryptomator-1.7.2-x64.exe*. Dit document is gebaseerd op deze versies en de cryptomator-portable.exe versie 1.6.10 (zie [bron \[8\]](#)).

### Let op:

Cryptomator slaat alle instellingen – waaronder de locatie van elke kluis – op in een *settings.json* bestand. Je kan hier desgewenst een back-up <sup>(3)</sup> van maken. De standaard paden zijn:

Linux: `/home/<gebruikersnaam>/config/Cryptomator/settings.json`

Windows: `C:\Gebruikers\<gebruikersnaam>\AppData\Roaming\Cryptomator\settings.json`  
voor de geïnstalleerde Cryptomator.

`C:\portapps\cryptomator-portable\data\settings.json`  
voor de portable Cryptomator (zie [bron \[8\]](#)).

<sup>2)</sup> Dit schrijven begon met versie 1.7.1, maar ging ondertussen naar 1.7.2. Deze “bugfixes” update heeft geen invloed op de gebruikersinterface beschrijving. In de schermafbeeldingen kan je beide versienummers aantreffen.

<sup>3)</sup> Je kan deze back-up ook gebruiken om de instellingen van de ene computer naar de andere over te zetten – maar alleen van Windows naar Windows of van Linux naar Linux – voordat je Cryptomator start. Dat scheelt weer wat werk.


## Ubuntu Linux – Cryptomator installeren

In Linux hoef je een .appimage bestand <sup>(4)</sup> alleen maar in een map te plaatsen en het uitvoerbaar <sup>(5)</sup> te maken om het uit te kunnen voeren – installeren is niet nodig. Het maakt ook niet uit waar het bestand staat, zolang je (in het terminalvenster of starter) het juiste pad opgeeft.

### Opmerking:

Het is aan te raden om de versie eraf te halen (dus alleen *cryptomator.Appimage*). Dan hoef je bij een update niet steeds je koppelingen ernaartoe bij te werken.

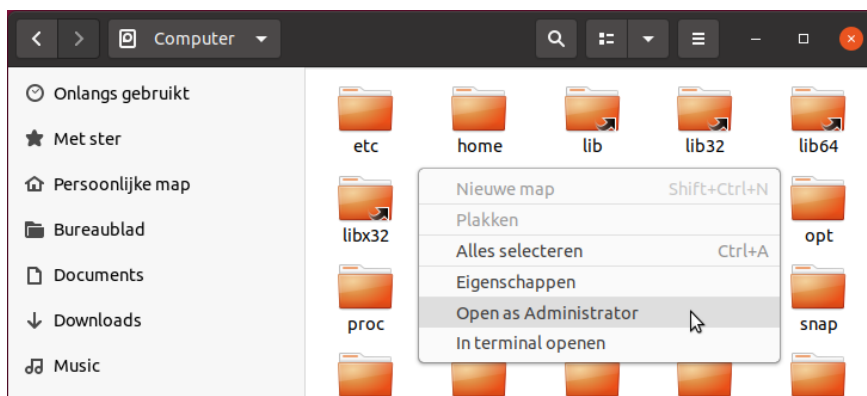
In deze handleiding wordt een map appimages in / (de systeem root) aangemaakt voor het plaatsen van .appimage bestanden. Dit maakt Cryptomator beschikbaar voor alle gebruikers. In de root moet de map appimages met Administrator rechten worden aangemaakt. Met de bestandsverkenner kan dit als hieraan de “Open als Administrator” optie is toegevoegd volgens [bron \[4\]](#).

Een starter is een scriptbestand met de extensie .desktop. Starters kan je in de favorieten balk (links in het scherm) of op het bureaublad plaatsen, of je kan Cryptomator via “Toepassingen tonen”  opzoeken. Zo kan je veel gebruikte applicaties eenvoudig met de muis starten.

### Cryptomator installeer je als volgt:

Onderstaande procedure is de multi-user versie. Als enige gebruiker kan je het appimage bijvoorbeeld ook als */home/<gebruikersnaam>/.local/share/applications/cryptomator.AppImage* of waar dan ook plaatsen, stap 6 uitvoeren en het betreffende pad in het [starterscript](#) specificeren.

1. Navigeer in de bestandsverkenner naar de root /.
2. Ga met de muisaanwijzer op een leeg plekje staan en rechtsklik om het menu te openen.

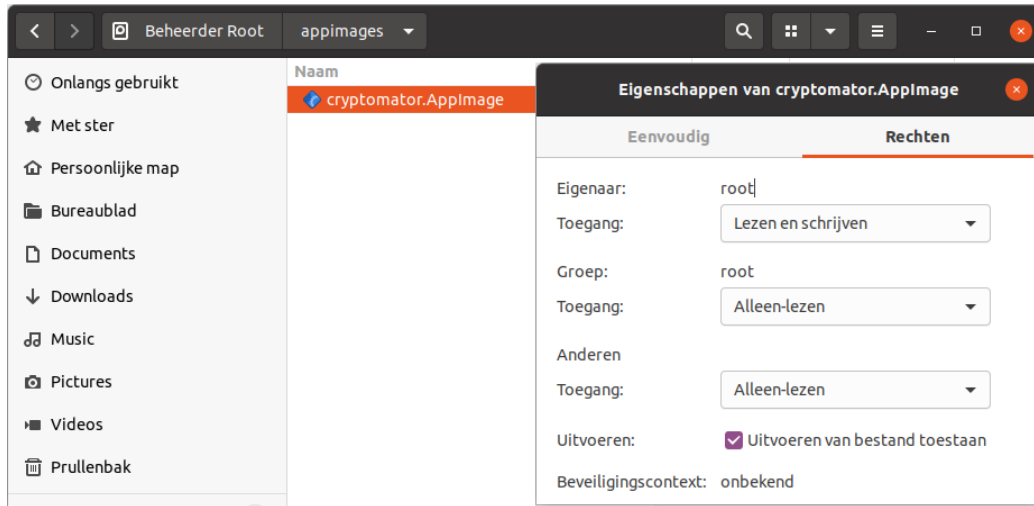


3. Kies “Open als Administrator” en log in met het beheerderswachtwoord (2 keer).
4. Voeg de map *appimages* toe en kopieer het gedownloade Cryptomator installatiebestand er in.

<sup>4)</sup> Een .appimage applicatie is min of meer vergelijkbaar met een Windows portable applicatie.

<sup>5)</sup> Dit werkt zelfs op een usb-stick – mits je deze formatteert als bijvoorbeeld NTFS bestandssysteem. Op eenvoudige FAT en EXFAT bestandssystemen kan je “Uitvoeren van bestand toestaan” niet toekennen. Helaas heb ik niet kunnen vinden of en hoe je de paden naar cryptomator administratieve bestanden (bijvoorbeeld settings.json) kan veranderen naar de usb-stick. Een volledig portable Cryptomator zit er voor Linux niet in.

5. Rechtsklik het bestand en kies “Eigenschappen”.



6. Op tabblad “Rechten” stel je de rechten in en vink je “Uitvoeren van bestand toestaan” aan.

### In het geval dat je Cryptomator weer wilt verwijderen:

Cryptomator verwijder je door het .appimage bestand te verwijderen.

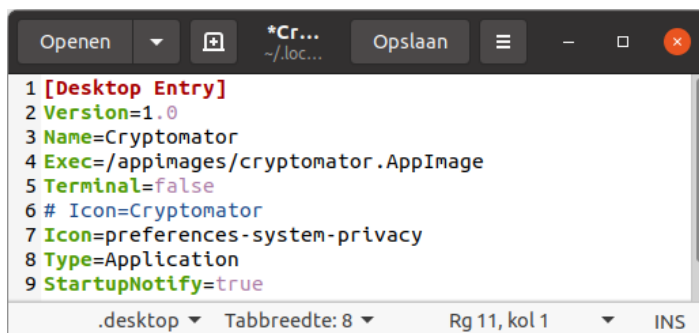
Dit verwijdert niet de kluismap(pen) – die moet je handmatig verwijderen.

Ook moet je dan nog de map `/home/<gebruikersnaam>/.local/share/Cryptomator` verwijderen.

### Vervolgens maak je met een tekst editor (bijvoorbeeld gedit) het starterscript:

Het in de starter gebruikte pictogram `preferences-system-privacy.png` wordt – indien aanwezig – automatisch gevonden in de systeemmap `/usr/share/icons/gnome/256x256/apps/`. Een pad en de extensie `.png` zijn in dat geval niet nodig. Een compleet pad vanuit de root `/` naar een pictogram specificeren kan ook; dan moet de extensie (bijvoorbeeld `.png`) wel toegevoegd worden.

De starter voor Cryptomator plaats je in de systeemmap `/usr/share/applications/` (alle gebruikers) of in de gebruikersmap `/home/<gebruikersnaam>/.local/share/applications/` (huidige gebruiker).



1. Open gedit en stel hierin het starterscript samen.
2. Sla je starter “CryptomatorPrivacy.desktop” eerst op in een gebruikersmap, bijvoorbeeld `~/Documents` <sup>(6)</sup>.

<sup>6)</sup> In plaats van `/home/<gebruikersnaam>/` kan meestal ook `~/` gebruikt worden, maar bijvoorbeeld niet in starterscripts.


3. Open in een tweede bestandsverkenner `/usr/share/applications/` met beheerdersrechten [bron \[4\]](#), of `~/.local/share/applications/` (geen beheerdersrechten nodig).



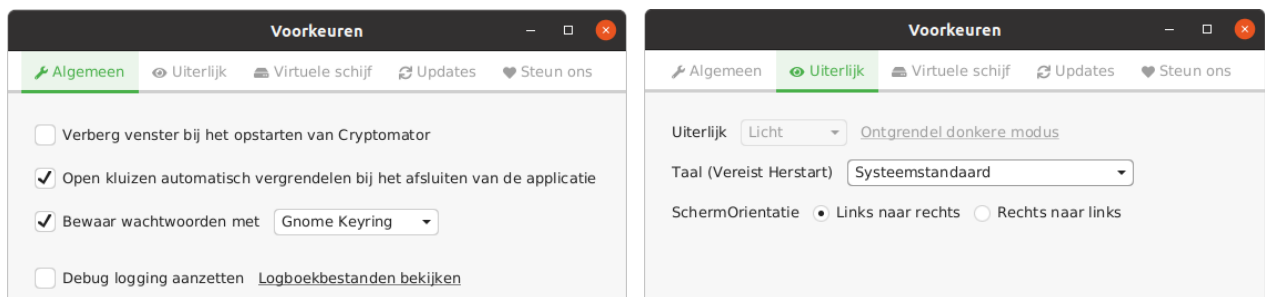
4. Kopieer CryptomatorPrivacy.desktop van `~/Documents` naar de betreffende map.  
 en/of  
 Kopieer CryptomatorPrivacy.desktop van `~/Documents` naar `~/Desktop`,  
 rechtsklik het pictogram op de desktop en kies “Toepassingen starten toestaan”.

## De algemene voorkeuren aanpassen

Voordat je een kluis aanmaakt, is het zaak ten minste de “Taal (Vereist Herstart)” en “Virtuele schijf” in te stellen. Later kan je deze en andere instellingen alsnog wijzigen.

Klik  om de algemene “Voorkeuren” te openen.

De onderstaande vensters laten zien wat je kan instellen.



“Algemeen” voorkeuren:

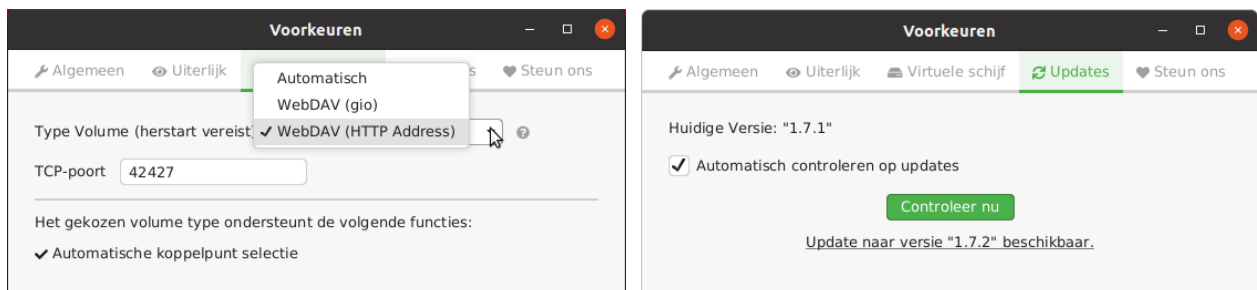
- ➡ Met “Verberg venster bij het opstarten van Cryptomator” verdwijnt het Cryptomator venster na starten direct van het scherm. Klikken op het pictogram in favorieten brengt het weer tevoorschijn.



- Met “Open kluizen automatisch vergrendelen bij het afsluiten van de applicatie” hoef je de kluizen niet eerst te sluiten voor het stoppen van Cryptomator en je wordt niet meer lastig gevallen met het “Applicatie afsluiten” venstertje na het stoppen van Cryptomator.
- Met “Bewaar wachtwoorden met...” kan je Cryptomator aanpassen aan een Gnome desktop (de “Gnome Keyring” wordt gebruikt) of een KDE desktop (de “KDE Wallet” wordt gebruikt). Deze instelling staat toe wachtwoorden op te slaan. Maar per kluis bepaal je of je daadwerkelijk het wachtwoord voor die kluis automatisch laat toepassen of niet (zie “[Nu ontgrendelen](#)”).

“Uiterlijk” voorkeuren:

- Met “Taal (Vereist Herstart)...” kan je de taal kiezen (Nederlands is beschikbaar) of de “Systeem standaard” taal toepassen.
- De “SchermOrientatie” moet op “Links naar rechts” blijven staan voor westerse talen.



- “Virtuele Schijf” voorkeuren: Voor Linux is “WebDAV (HTTP Address)”<sup>(7)</sup> een goede keuze ([bron \[5\]](#)). Welke keuzes je te zien krijgt hangt af van je bedrijfssysteem.
- “Updates” voorkeuren: Je kan automatisch op updates laten controleren<sup>(8)</sup>. Ook kan je met “Controleer nu” handmatig op updates controleren. Als er een update beschikbaar is zie je in het hoofdvenster de rode indicatie bij het instellingen-tandwiel: .

<sup>7)</sup> Om WebDAV (gio) te kunnen gebruiken moet een extra Gnome gio tool geïnstalleerd worden.

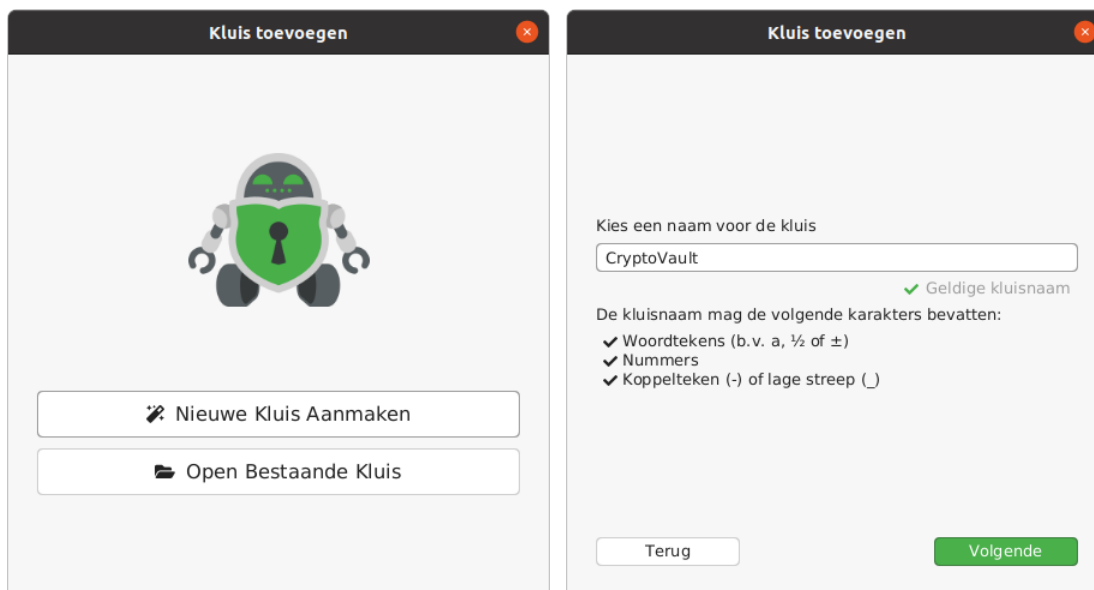
<sup>8)</sup> De mensen van Cryptomator zijn blijkbaar hard aan het werk. Deze “bugfixes” update heeft geen invloed op de hier beschreven gebruikersinterface mogelijkheden. Toch leuk om ze net even te “betrappen” voor een update schermafdruck!

## Een of meer kluizen toevoegen

Een kluis voeg je als volgt toe:



1. Start Cryptomator en klik op “+ Kluis toevoegen”.



2. Kies “Nieuwe Kluis Aanmaken”, vul in het volgende venster de gewenste naam in onder “Kies een naam voor de kluis” en klik op “Volgende”.



### Kluis toevoegen

Waar moet Cryptomator de versleutelde bestanden van je kluis opslaan?

☒ OneDrive  
☐ Andere locatie Kies...

Opslaglocatie

✓ Geschikte locatie voor je kluis

Terug
Volgende

### Kluis toevoegen

Voer een nieuw wachtwoord in

✓ Sterk

Bevestig het nieuwe wachtwoord

✓ Wachtwoorden komen overeen!

Zonder wachtwoord hebt u geen toegang tot uw data. Wilt u een herstelsleutel voor het geval u uw wachtwoord verliest?

☒ Ja graag, voorkomen is beter dan genezen  
☐ Nee bedankt, ik verlies mijn wachtwoord niet

Terug
Kluis aanmaken

- Vink "OneDrive" aan <sup>(9)</sup> of kies met "Opslaglocatie" een andere lokale map <sup>(10)</sup> en klik "Volgende".
- Geef een sterk wachtwoord op (2x), vink "Ja graag, voorkomen is beter dan genezen" aan om een herstelsleutel aan te maken <sup>(11)</sup> en klik op "Kluis aanmaken".

### Kluis toevoegen

De volgende herstelsleutel kan worden gebruikt om "CryptoVault" te herstellen:

Afdrukken
Kopieer

Bewaar het op een veilige plek, bv:

- Bewaar het in een wachtwoordmanager
- Sla het op op een USB-stick
- Print het op papier

Volgende

### Kluis toevoegen

✓

Toegevoegde kluis "CryptoVault".  
Ontgrendel deze kluis om toegang te krijgen tot of om inhoud toe te voegen. Optioneel kunt u deze op elk later tijdstip ontgrendelen.

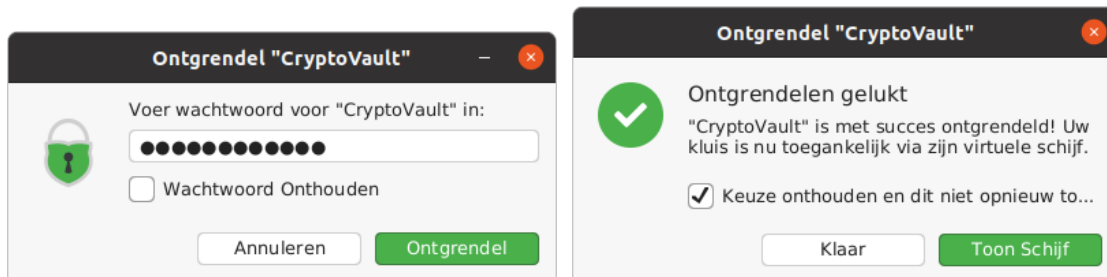
Klaar
Nu Ontgrendelen

<sup>9)</sup> In dit geval is de applicatie "onedrive" voor Ubuntu geïnstalleerd zie [bron \[7\]](#) (HCC open source site). De standaard OneDrive locatie is hier `/home/<gebruikersnaam>/OneDrive/...` Cryptomator vult deze automatisch in.

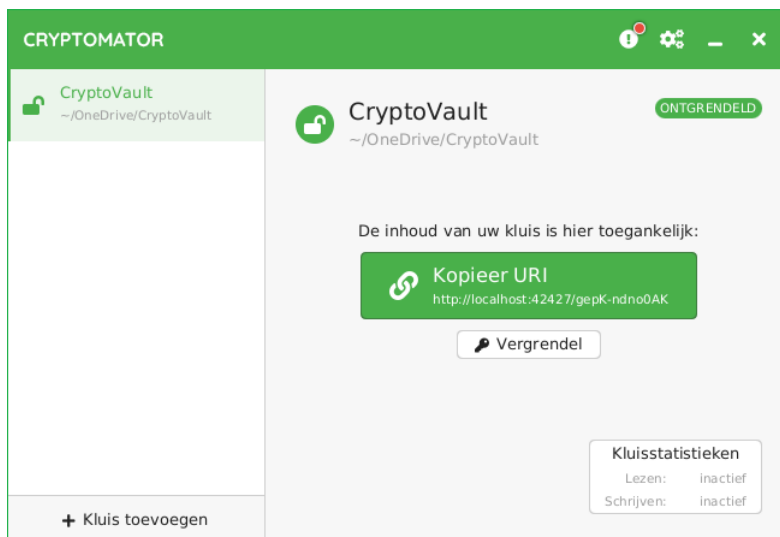
<sup>10)</sup> Die andere lokale map kan een willekeurige map zijn, maar ook de lokale synchronisatiemap van een andere cloud-provider (getest met MegaDrive).

<sup>11)</sup> Een herstelsleutel maken kan achteraf ook nog; zie "[Toon herstelsleutel](#)".

5. Print de getoonde herstelsleutel met “Afdrukken” en berg deze veilig op of sla deze met “Kopieer” elektronisch veilig op, bijvoorbeeld in een wachtwoordmanager<sup>(12)</sup> of op een goed opgeborgen usb-stick.
6. Klik op “Volgende” en in het laatste venster op “Klaar” om terug te keren naar het Cryptomator [hoofdvenster](#) of op “Nu Ontgrendelen” om “CryptoVault” meteen te openen.



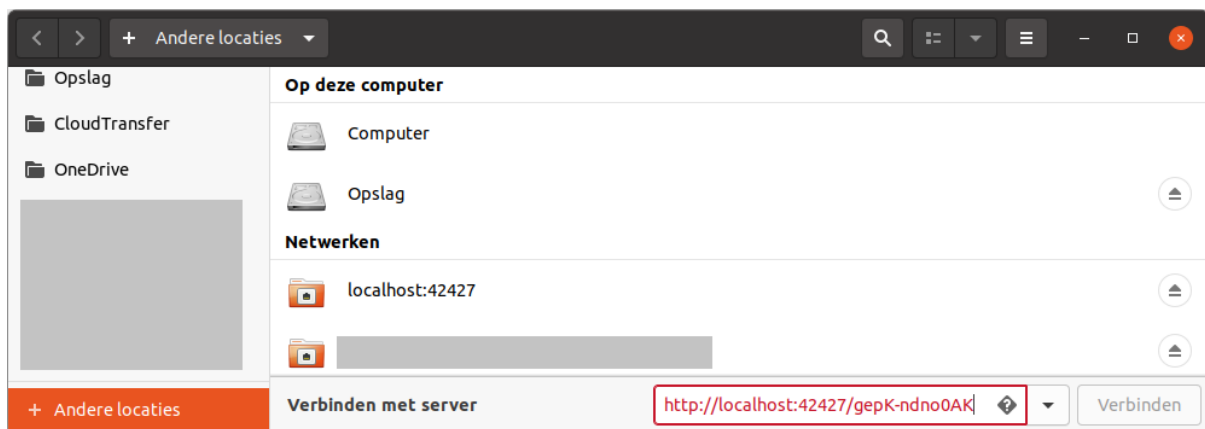
7. Voer het wachtwoord in, vink desgewenst “Wachtwoord onthouden” aan<sup>(13)</sup> en klik op “Ontgrendel”.
8. Vink in het vervolgvenster “Keuze onthouden en dit niet opnieuw tonen” aan. Klik dan op “Klaar” (bij het WebDAV protocol werkt “Toon Schijf” niet).  
Je gaat nu naar het Cryptomator [hoofdvenster](#) terug. Dit toont de situatie met ontgrendelde kluis.



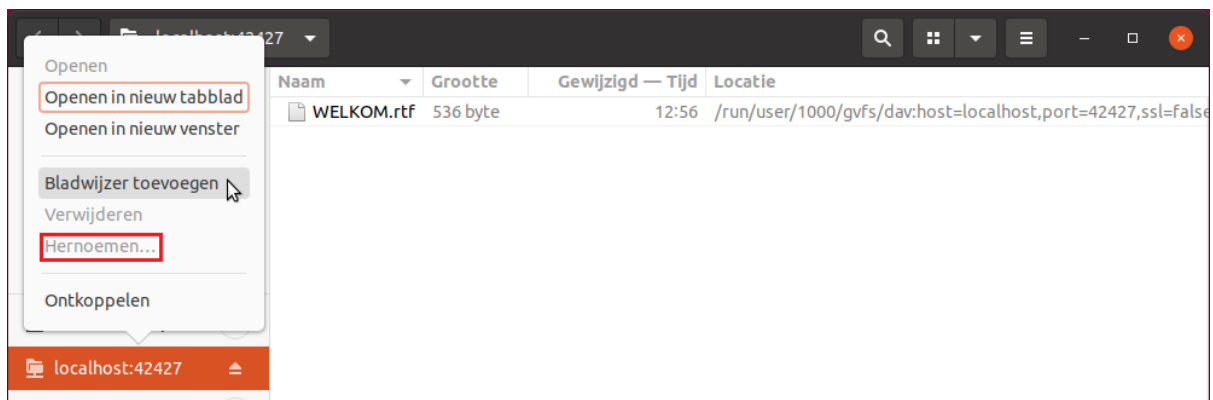
9. Indien de kluis vergrendeld is, klik je op “Ontgrendelen...” om de kluis te openen. Je ziet dan de “Kopieer URI” toets.

<sup>12)</sup> De sleutel is erg lang. Ik heb deze in een .txt bestandje gezet en dat opgeslagen in de KeePass wachtwoordmanager.

<sup>13)</sup> Voor het onthouden van het wachtwoord moet wel “[Store passwords with...](#)” in de algemene voorkeuren aangevinkt zijn en moet de juiste sleutelring ingesteld zijn.



10. Open de bestandsverkenner, scroll in het linker vak naar beneden en klik op “+ Andere locaties”.
11. Druk op de Cryptomator “Kopieer URI” toets en plak de URI in het verkenner veld “Voer server adres in” (achter “Verbinden met server:”).
12. Vervang nu *http:* door *dav:* (de rode tekst wordt zwart) en klik “Verbinden”. Je ziet dan in het rechter vak van de verkenner de leesbare inhoud (WELKOM.rtf<sup>(14)</sup>) van de geopende kluis.



13. Omdat “localhost:42427” weinig zegt (vooral als je meerdere kluisen met dat poortnummer hebt), kan je een “Bladwijzer toevoegen” en die de gewenste kluisnaam geven met “Hernoemen...”.

De bladwijzer kan je in het vervolg gebruiken om deze “Locatie op afstand” in de verkenner zichtbaar te maken. De bladwijzer is bovendien back-up; zonder deze moet je iedere keer weer de URI invoeren als je per ongeluk op “Ontkoppelen” van de localhost hebt geklikt.

Heb je meerdere bladwijzers in de bestandsverkenner, dan kan je ze met de muis in de gewenste volgorde slepen.

<sup>14)</sup> WELKOM.rtf mag je desgewenst verwijderen. Het heeft verder geen functie meer.

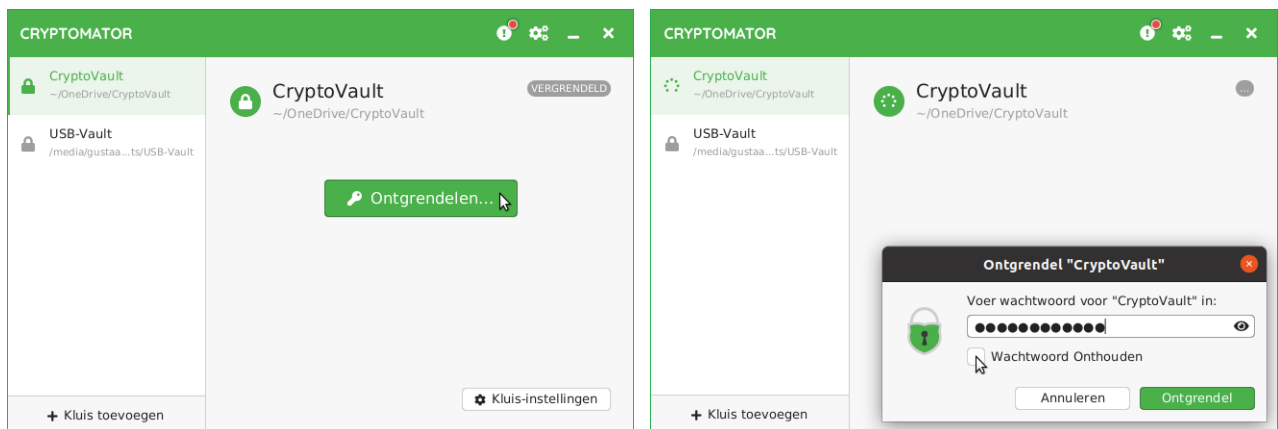
## Cryptomator gebruiken en instellen per kluis

De Cryptomator kluismap(pen) in de gekozen lokale map(pen) zijn en blijven altijd onleesbaar. Als je voor een kluis “Ontgrendelen” (wachtwoord nodig) of “Nu Ontgrendelen” (wachtwoord is opgeslagen) kiest dan komt de kluis als WebDAV localhost beschikbaar. In de bestandsverkenner kan je de leesbare inhoud van deze map tonen door op de hiervoor toegevoegde [bladwijzer](#) te klikken.

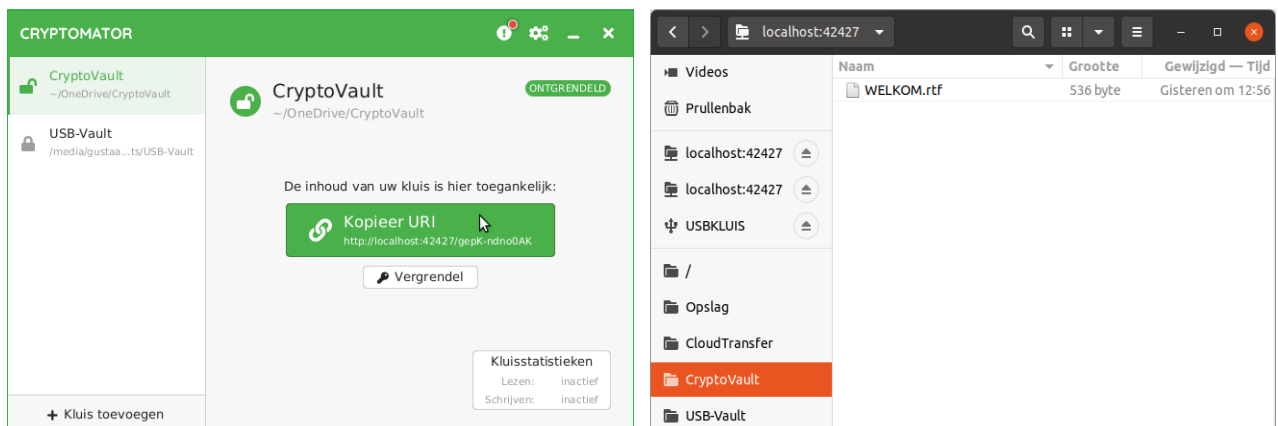
## De Cryptomator kluis openen en er in werken

### Opmerking:

Heb je meerdere kluisen, dan kan je ze in het Cryptomator hoofdvenster met de muis in de gewenste volgorde slepen.



1. Start Cryptomator en kies een kluis (CryptoVault) om die te “Ontgrendelen”<sup>(15)</sup>. Je kan “Wachtwoord onthouden” aanvinken, dan opent deze kluis in het vervolg vanzelf bij het ontgrendelen, mits het opslaan van het wachtwoord in de [algemene voorkeuren](#) is toegestaan.

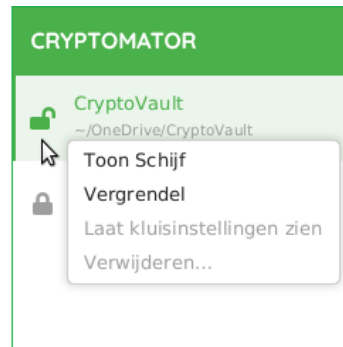
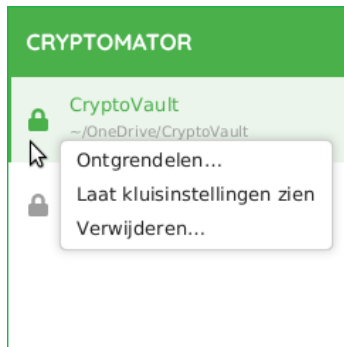


2. Met de [bladwijzer](#) in de bestandsverkenner open je de local host<sup>(16)</sup> map en kan je daarin werken.
3. Met “Vergrendel” sluit je een kluis weer.

<sup>15)</sup> De groene lijnen heb ik zelf om de vensters geknutseld; de schermafdrucken hadden deze niet geheel rondom.

<sup>16)</sup> Je ziet twee identieke local host shares (voor CryptoVault en USB-Vault). Met de bladwijzers kan je deze kluisen uit elkaar houden en ze openen.

## Acties en voorkeuren per kluis



(dit zijn uitsneden uit het hoofdvenster)

- ➡ Je kan met “Ontgrendelen” of met “Nu Ontgrendelen” een gesloten kluis openen. Als het wachtwoord opgeslagen is dan opent “Nu Ontgrendelen” meteen de kluis. Zo niet, dan verschijnt na “Ontgrendelen” het “Ontgrendel...” wachtwoordvenstertje als in stap 1.
- ➡ Met “Laat kluisinstellingen zien” kan je de voorkeuren per gesloten kluis aanpassen.
- ➡ Met “Verwijderen...” kan je een gesloten kluis verwijderen uit Cryptomator. De door de kluis gebruikte mappen blijven wel gewoon bestaan; er gaat geen data verloren.
- ➡ “Toon Schijf” doet niets bij gebruik van het WebDAV protocol.
- ➡ Met “Vergrendel” zet je de betreffende kluis weer op slot.

Als een kluis gesloten is dan kan je met “Laat kluisinstellingen zien” de kluis-voorkeuren openen.

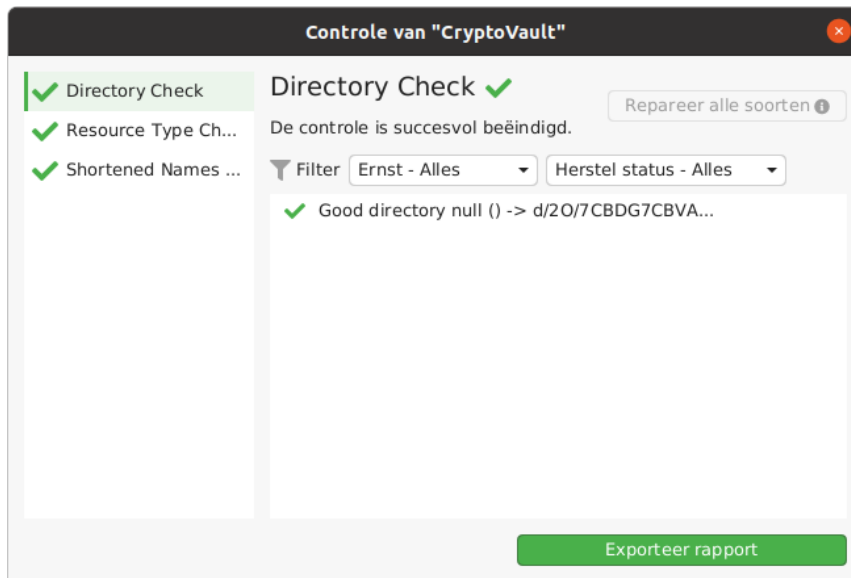


Op tabblad “Algemeen” vind je de volgende voorkeuren:

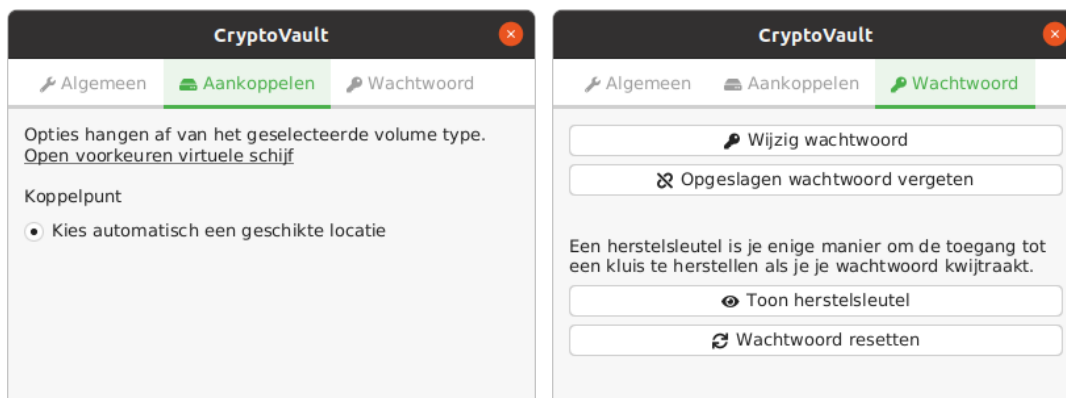
- ➡ “Kluisnaam” – Het lijkt erop dat je hier de naam van je kluis kan veranderen. Doe dit niet<sup>(17)</sup>!
- ➡ Met “Vergrendel wanneer inactief voor...” kan je een time-out periode instellen waarna de kluis gesloten wordt als je er niet meer in werkt.

<sup>17)</sup> In ieder geval niet met OneDrive waarop deze handleiding is gebaseerd; dat ging fout!

- ➡ Met “Ontgrendel kluis bij het starten van Cryptomator” wordt de kluis automatisch geopend als Cryptomator gestart wordt. Hiervoor moet je wel “Bewaar wachtwoorden met...” in de [algemene voorkeuren](#) aangevinkt hebben en moet de juiste sleutelring ingesteld zijn.
- ➡ Het keuze-venstertje “Na een succesvolle ontgrendeling...” is bij gebruik van het WebDAV protocol niet zinvol. Je kan het beste “Niets doen” instellen.



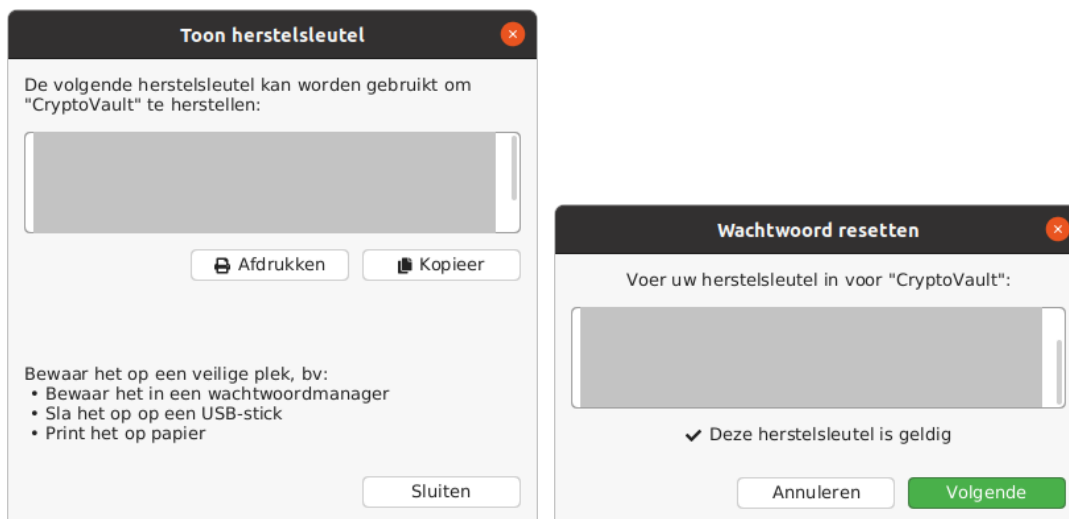
- ➡ Met “Start Controle” kan je een test starten die de consistentie van de kluis test en – indien mogelijk – deze herstelt als er iets mis is.



Op tabblad “Aankoppelen” valt bij gebruik van het WebDAV protocol niets te kiezen.

Op tabblad “Password” vind je de volgende voorkeuren:

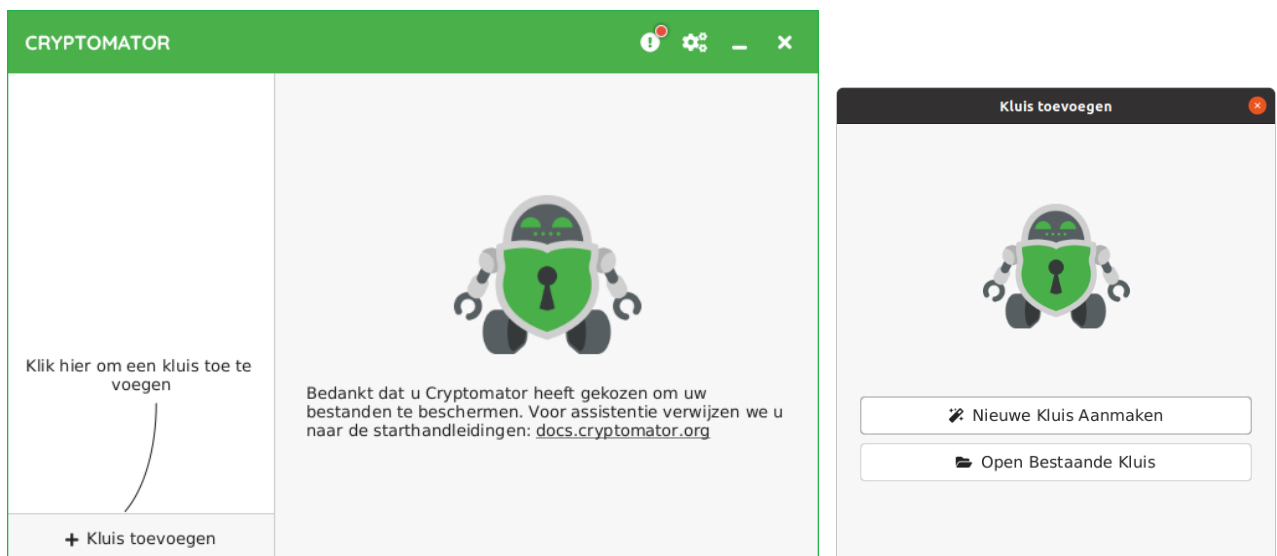
- ➡ Met “Wijzig wachtwoord” kan je een ander wachtwoord instellen.  
**Je krijgt dan ook een nieuwe herstelsleutel!**
- ➡ Met “Opgeslagen wachtwoord vergeten” kan je het wachtwoord van de betreffende kluis uit de Gnome keyring of KDE wallet verwijderen (zie [algemene voorkeuren](#)). Je moet dan bij het openen van die kluis het bestaande wachtwoord weer handmatig ingeven.



- ➡ Met “Toon herstelsleutel” kan je de herstelsleutel opvragen die bij het huidige wachtwoord hoort. Om de herstelsleutel op te kunnen vragen moet je wel met je huidige wachtwoord inloggen.
- ➡ Met “Wachtwoord resetten” kan je met je herstelsleutel een nieuw wachtwoord aanmaken. Na “Volgende” vul je tweemaal je nieuw gekozen wachtwoord in en klik je op “Reset”.  
**Je krijgt dan ook een nieuwe herstelsleutel!**

## Koppelen aan een bestaande kluis

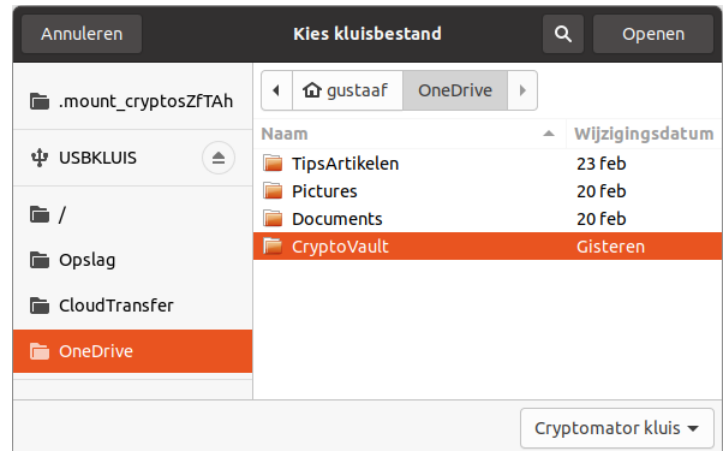
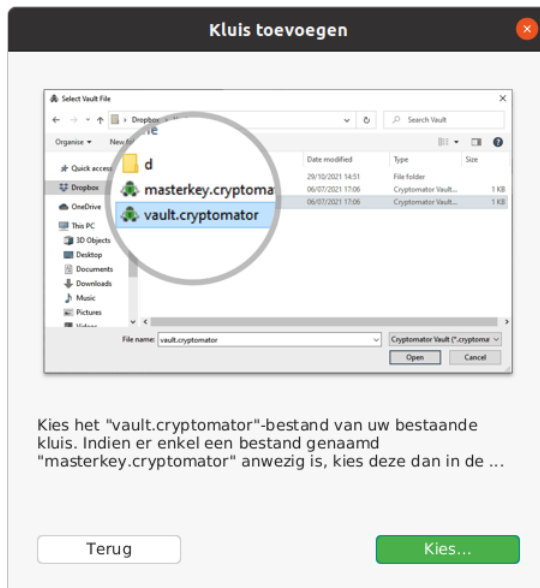
In Linux koppelen aan een bestaande kluis (hier: CryptoVault in de OneDrive cloud <sup>(18)</sup>, <sup>(19)</sup>) doe je als volgt:



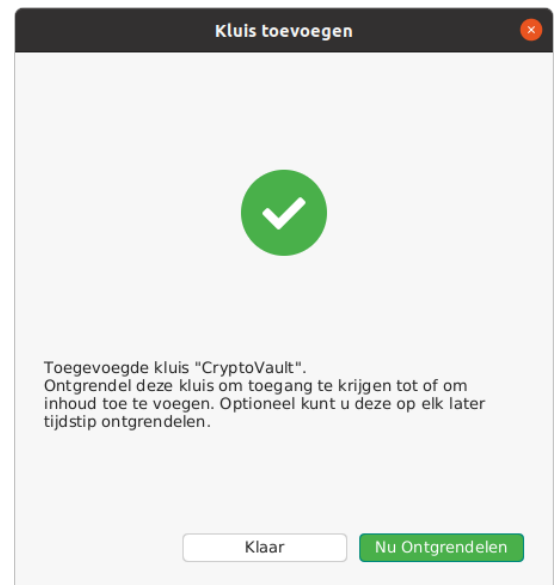
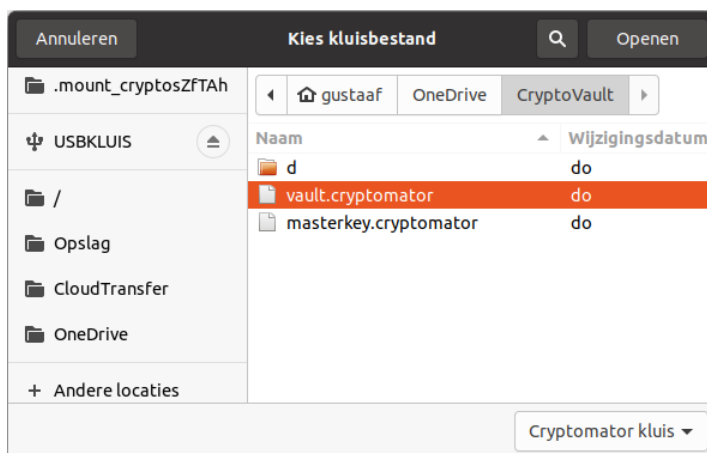
<sup>18)</sup> In dit geval is de applicatie “onedrive” voor Ubuntu geïnstalleerd zie [bron \[7\]](#) (HCC open source site). De standaard OneDrive locatie is hier `/home/<gebruikersnaam/OneDrive/CryptoVault`.

<sup>19)</sup> Je kan in OneDrive aangeven welke mappen gesynchroniseerd moeten worden. Als je het standaard “Alle bestanden beschikbaar maken” hebt uitgeschakeld, dan moet je nu eerst je kluismap voor synchronisatie inschakelen. Zie [bron \[9\]](#).

1. Start Cryptomator en klik op “+ Kluis toevoegen”.
2. Klik op “Open Bestaande Kluis”.

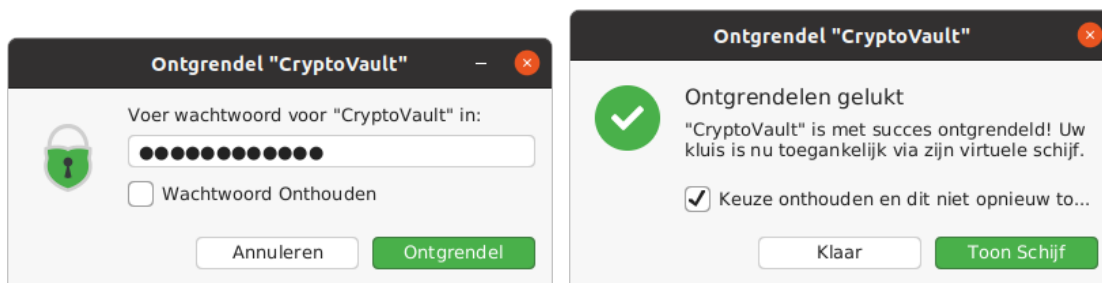


3. Klik op de knop “Kies...” en navigeer naar de synchronisatiemap van OneDrive of een lokale map met een Cryptomator kluis.
4. Kies daarin de bestaande kluis; hier “CryptoVault” en klik op de knop “Openen”.



5. Kies in Cryptovault bij voorkeur het bestand vault.cryptomator, maar als dit niet aanwezig is kies dan masterkey.cryptomator en klik op de knop “Openen”.
6. Je kan nu op “Klaar” klikken om naar het Cryptomator [hoofdvenster](#) te gaan of op “Nu Ontgrendelen” om de kluis te openen. In dat laatste geval krijg je de volgende vensters:





7. Voer het wachtwoord in, vink desgewenst “Wachtwoord onthouden” aan<sup>(20)</sup> en klik op “Ontgrendel”.
8. Vink in het vervolgvenster “Keuze onthouden en dit niet opnieuw tonen” aan. Klik dan op “Klaar” (bij het WebDAV protocol werkt “Toon Schijf” niet). Je gaat nu naar het Cryptomator [hoofdvenster](#) terug.

## De gebruikte paden en instellingen van Cryptomator

Maak wel eerst een back-up van deze bestanden als je wat wilt gaan wijzigen!



De Cryptomator algemene instellingen en kluispaden en -instellingen vind je in `/home/<gebruikersnaam>/.config/Cryptomator/settings.json`.

Je kan hierin te gebruiken paden en instellingen aanpassen in bijvoorbeeld Gedit.

<sup>20)</sup> Voor het onthouden van het wachtwoord moet wel “[Store passwords with...](#)” in de algemene voorkeuren aangevinkt zijn en moet de juiste sleutelring ingesteld zijn.

## Windows – Cryptomator installeren

### Installeren:

Download het Cryptomator installatiebestand zoals aangegeven in de [Inleiding](#).

Dubbelklik het .exe bestand om het te installeren (in *C:\Program Files\Cryptomator*).

### In het geval dat je Cryptomator weer wilt verwijderen:


Als je het Cryptomator installatiebestand nog hebt: Dubbelklik dit en kies “Uninstall”.

Zo niet dan kan het als volgt met behulp van Windows “Taakbeheer” en “Instellingen”:

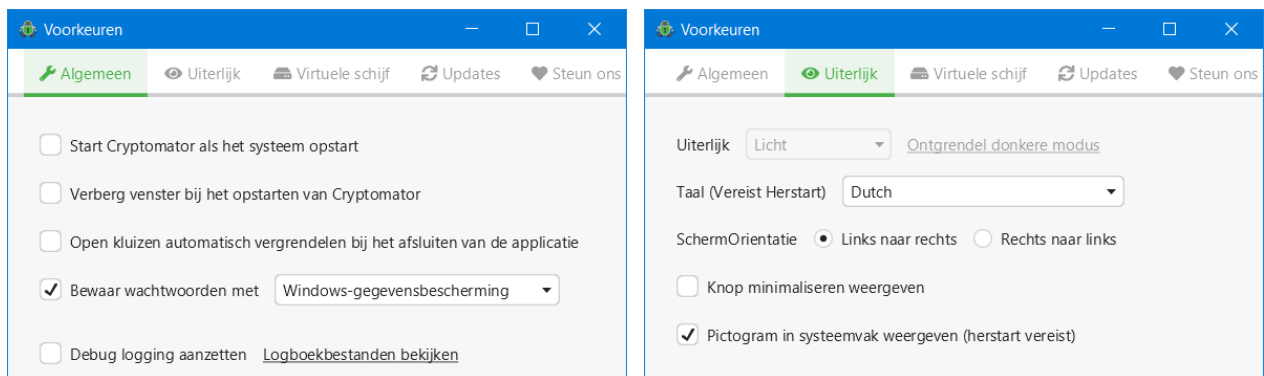
1. Sluit Cryptomator.
2. Start Taakbeheer – rechtsklik “Cryptomator” – kies “Beëindigen”.
3. Ga naar “Instellingen” – “Apps” – “Apps en onderdelen” – klik Cryptomator – kies “Verwijderen”.
4. Verwijder desgewenst de gebruikte kluismappen.

## De algemene voorkeuren aanpassen

Voordat je een kluis aanmaakt, is het zaak met name de “Taal” en “Virtuele schijf” in te stellen. Later kan je deze en andere instellingen alsnog wijzigen.

Klik  om de algemene voorkeuren te openen.

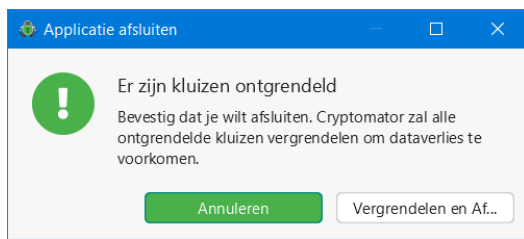
De onderstaande vensters laten zien wat je kan instellen.



### “Algemeen” voorkeuren:


- ➡ Met “Start Cryptomator als het systeem opstart” kan je aangeven dat Cryptomator altijd automatisch moet opstarten zodra Windows opgestart is. Als dit fout gaat, kan je als alternatief een snelkoppeling naar *C:\Program Files\Cryptomator\Cryptomator.exe* plaatsen in <sup>(21)</sup> *%appdata%\Microsoft\Windows\Start Menu\Programs\Startup*.
- ➡ Met “Verberg venster bij het opstarten van Cryptomator” verdwijnt het Cryptomator venster na starten direct van het scherm. Klikken op het pictogram in de taakbalk brengt het weer tevoorschijn.

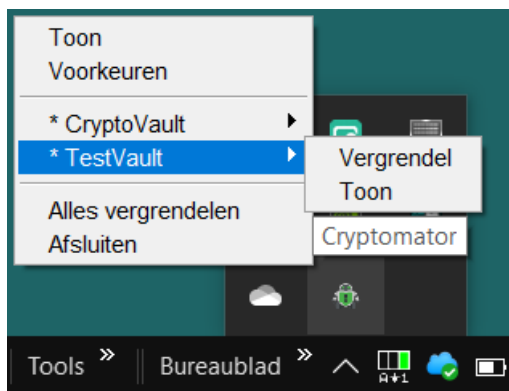
<sup>21)</sup> *%appdata%* (kan je intypen in de bestandverkenner) staat voor de locatie van het roaming profile – standaard: *C:\Gebruikers\<gebruikersnaam>\AppData\Roaming*.




- ➔ Met “Open kluisen automatisch vergrendelen bij het afsluiten van de applicatie” hoef je de kluisen niet eerst te sluiten voor het stoppen van Cryptomator en je wordt niet meer lastig gevallen met het “Applicatie afsluiten” venstertje na het stoppen van Cryptomator.
- ➔ Met “Bewaar wachtwoorden met...” kan je wachtwoorden al of niet opslaan in de “Windows-gegevensbescherming”. Maar per kluis bepaal je of je daadwerkelijk het wachtwoord voor die kluis automatisch laat toepassen of niet (zie [“Nu ontgrendelen”](#)).

“Uiterlijk” voorkeuren:

- ➔ Met “Taal (Vereist Herstart)...” kan je de taal kiezen (Nederlands is beschikbaar).
- ➔ De “SchermOriëntatie” moet op “Links naar rechts” blijven staan voor westerse talen.
- ➔ Met “Knop minimaliseren weergeven” kan je deze knop  aan het hoofdvenster toevoegen als die ontbreekt. Met deze knop kan je het hoofdvenster van het bureaublad naar de taakbalk verbannen. Je kan het weer tonen door op het icoontje in de taakbalk te klikken.



- ➔ “Pictogram in systeemvak weergeven...” levert een pictogram met keuzemenu op. Als je niet alle kluisen eerst sluit en op afsluiten  klikt, krijg je niet het “Applicatie afsluiten” venster, maar in plaats daarvan wordt Cryptomator geminimaliseerd naar het systeemvak.

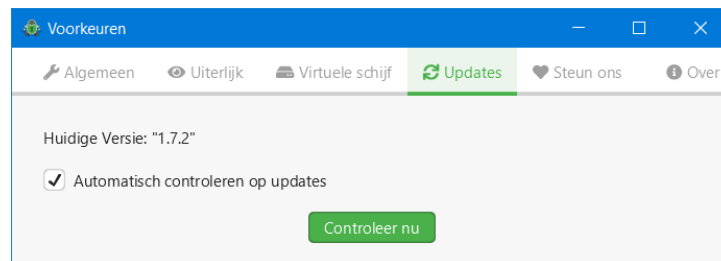
**De kluisen blijven open, ook al klap je je laptop dicht (slaapstand) en weer open.**

Al naar gelang de omstandigheden kan hier bij onzorgvuldig handelen toch een veiligheidslek op de loer liggen – je kan beslissen om dit al of niet te activeren.

Met het taakbalkmenu kan je het volgende:

- “Toon” opent het hoofdvenster weer.
- “Voorkeuren” opent de algemene voorkeuren.

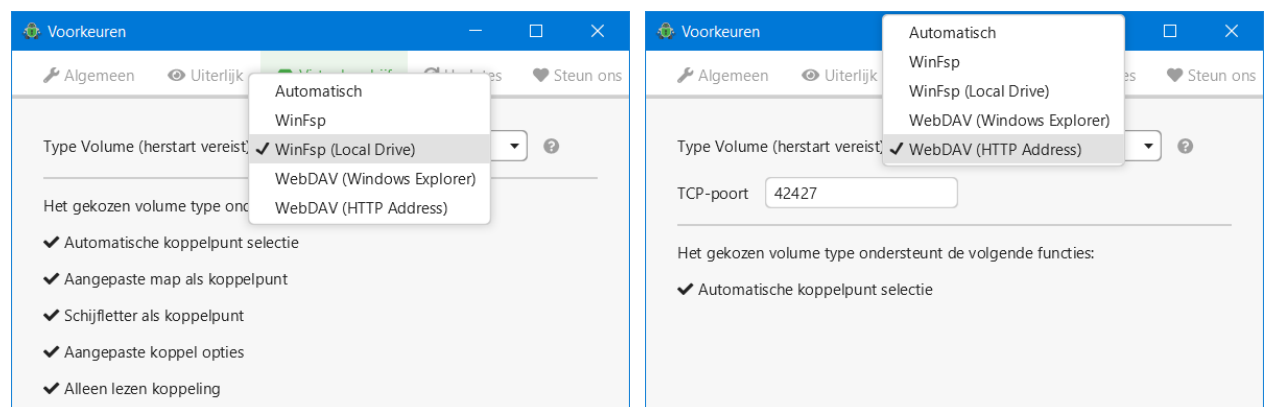
- Elke kluis kan je “Vergrendelen” of je kan met “Toon” het verkennervenster met de kluisinhoud openen. Als een kluis vergrendeld is, dan verandert het menu voor die kluis in “Ontgrendel”.
- Met “Alles vergrendelen” sluit je alle kluisen tegelijk.
- Met “Afsluiten” stop je Cryptomator nu echt.



- ➞ “Updates” voorkeuren: Je kan automatisch op updates laten controleren <sup>(22)</sup>. Ook kan je met “Controleer nu” handmatig op updates controleren. Als er een update beschikbaar is zie je in het hoofdvenster de rode indicatie bij het instellingen-tandwiel: .

### ➞ De “Virtuele schijf” kiezen.

Het kiezen van de virtuele schijf staat los van de gecodeerde verbinding naar de kluismap(pen). Je kan onafhankelijk per apparaat kiezen welk te kiezen protocol je voorkeur heeft.



In Windows geeft het protocol “WinFsp (Local Drive)” de meeste mogelijkheden. Hierin kan je voor je gedecodeerde data de volgende mogelijkheden kiezen:

- De eerste vrije schijfletter laten kiezen. De gedecodeerde data ontsluit je dan als schijf.
- Ergens een map naar wens aanmaken en vervolgens aanwijzen voor je gedecodeerde data. Desgewenst kan je deze map toevoegen aan “Snelle toegang” van de bestandsverkenner.
- Een bepaalde schijfletter aanwijzen als vaste schijfletter.
- Aangepaste koppeloptyes gebruiken (maar waarvoor je die nodig zou kunnen hebben??).

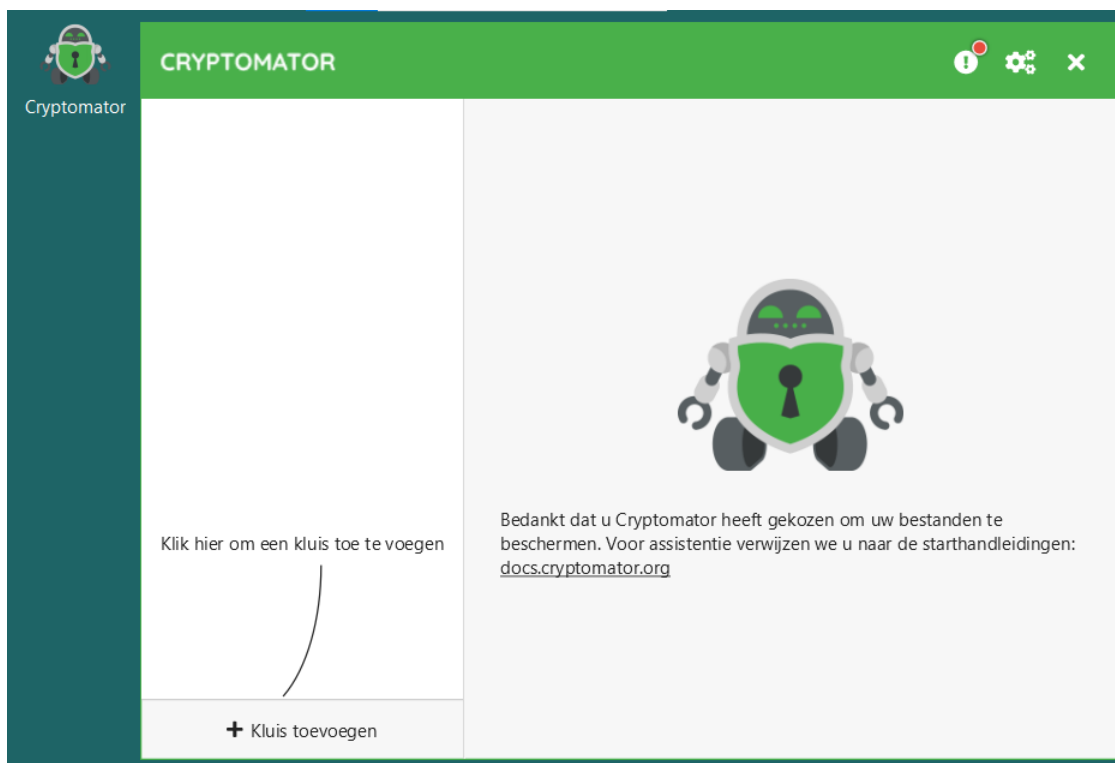
<sup>22)</sup> De mensen van Cryptomator zijn blijkbaar hard aan het werk. Deze “bugfix” update schijnt geen invloed te hebben op de hier beschreven gebruikersinterface mogelijkheden ten opzichte van de 1.7.1 versie.

- De gedecodeerde data al of niet als “Alleen lezen koppeling” aanwijzen.  
Je hebt dan leestoegang tot de gedecodeerde data, maar je kan niets toevoegen aan – of veranderen in – de gecodeerde kluismap.

Het protocol “WebDAV (HTTP Address)” ([bron \[5\]](#)) voegt je gedecodeerde data toe als server share. In de verkenner is bij geopende kluis je gedecodeerde data direct onder “Deze PC” zichtbaar als servermap (en hoef je deze niet aan “Snelle toegang” toe te voegen).

## Een of meer kluizen toevoegen

Een kluis voeg je als volgt toe:



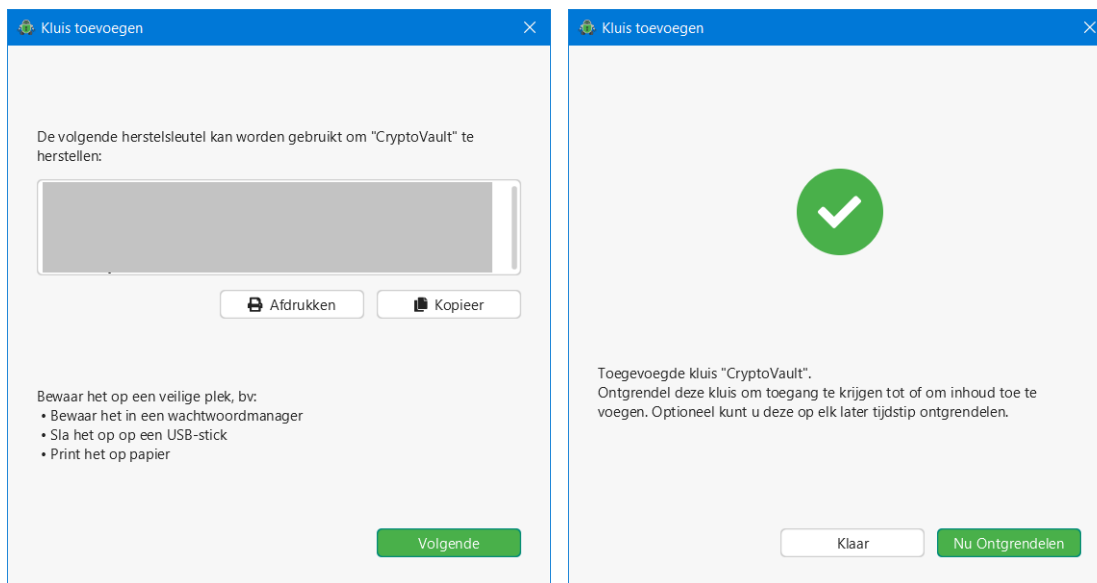
1. Start Cryptomator en klik op “+ Kluis toevoegen”.

2. Kies “Nieuwe Kluis Aanmaken”, vul in het volgende venster de gewenste naam in onder “Kies een naam voor de kluis” en klik op “Volgende”.

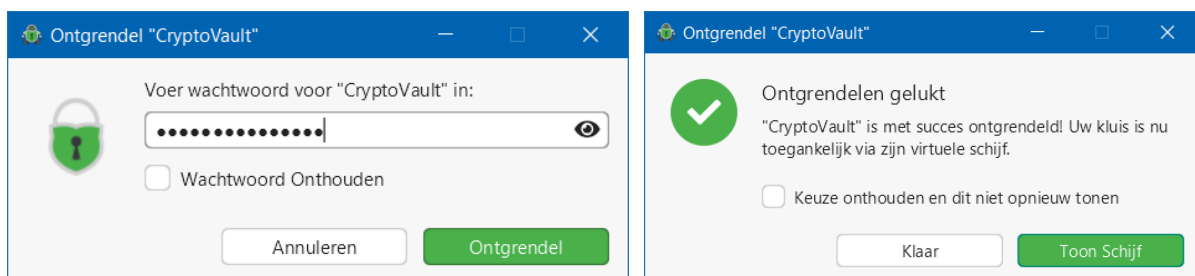
3. Vink “OneDrive” aan of kies met “Andere locatie” een andere lokale map<sup>(23)</sup> en klik op “Volgende”.
4. Geef een sterk wachtwoord op (2x), vink “Ja graag, voorkomen is beter dan genezen” aan om een herstelsleutel aan te maken<sup>(24)</sup> en klik op “Kluis aanmaken”.

<sup>23)</sup> Die andere lokale map kan een willekeurige map zijn, maar ook de lokale synchronisatiemap van een andere cloud-provider (getest met MegaDrive). De Windows standaardmap is `C:\Gebruikers\<gebruikersnaam>\OneDrive\...`

<sup>24)</sup> Een herstelsleutel maken kan achteraf ook nog; zie “[Toon herstelsleutel](#)”.



5. Print met “Afdrukken” de getoonde herstelsleutel en berg deze veilig op of sla deze met “Kopieer” elektronisch veilig op, bijvoorbeeld in een wachtwoordmanager<sup>(25)</sup> of op een goed opgeborgen usb-stick.
6. Klik op “Volgende” en in het laatste venster op “Klaar” om terug te keren naar het Cryptomator hoofdvenster of op “Nu ontgrendelen” om “CryptoVault” meteen te openen.



7. Voer het wachtwoord in, vink desgewenst “Wachtwoord onthouden” aan<sup>(26)</sup> en klik op “Ontgrendel”. In het vervolgvenster kan je desgewenst “Keuze onthouden en dit niet opnieuw tonen” aanvinken.

Als je dan “Toon schijf” klikt dan zal dit in de toekomst altijd bij openen gebeuren.

Als je “Klaar” klikt zal de schijf in de toekomst niet automatisch getoond worden.

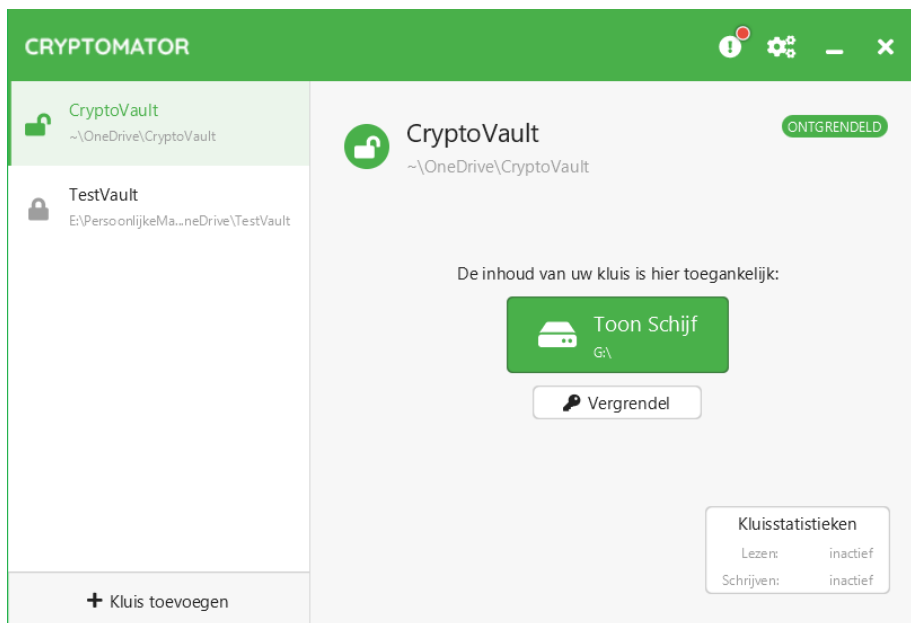
Dit kan je later nog aanpassen.

Je gaat nu naar het Cryptomator [hoofdvenster](#) terug<sup>(27)</sup>

<sup>25)</sup> De sleutel is erg lang. Ik heb deze in een .txt bestandje gezet en dat opgeslagen in de KeePass wachtwoordmanager.

<sup>26)</sup> Voor het onthouden van het wachtwoord moet “[Bewaar wachtwoorden met...](#)” in de algemene voorkeuren actief zijn.

<sup>27)</sup> In het hoofdvenster wordt het CryptoVault pad hier aangegeven als `~\OneDrive\CryptoVault`. Dit is in werkelijkheid `C:\Gebruikers\Gustaaf\OneDrive\CryptoVault`. Maar alleen op de laptop (Windows Home), want op de desktop computer (Windows Pro) wordt wel het volledige pad gebruikt.



Cryptomator hoofdvenster

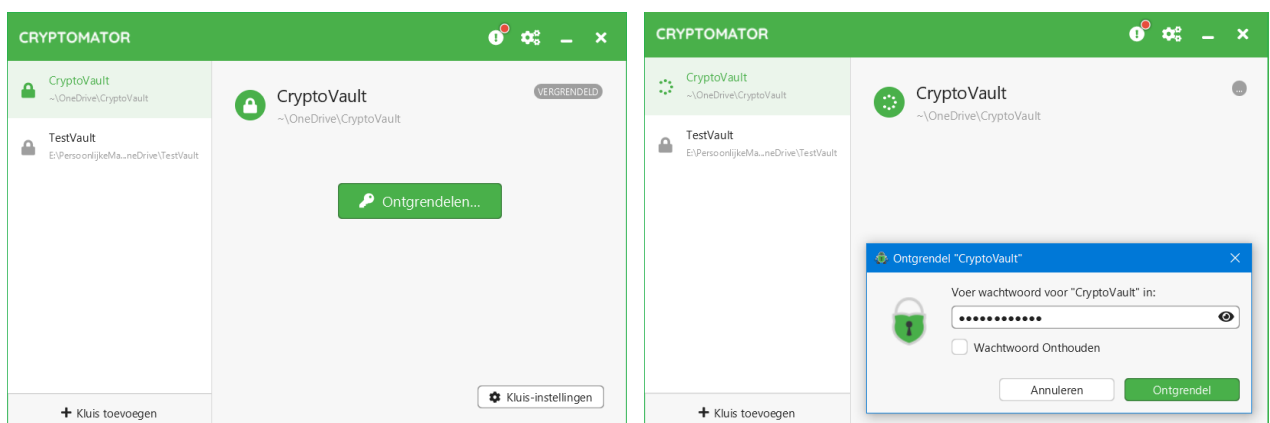
## Cryptomator gebruiken en instellen per kluis

De Cryptomator kluismap(pen) in de gekozen lokale map(pen) zijn en blijven altijd onleesbaar. Als je voor een kluis (CryptoVault) “Ontgrendelen...” kiest wordt deze bijvoorbeeld leesbaar als een schijf met een toegekende schijfletter (hier de eerst ongebruikte: “G:\”). Als je in het Cryptomator hoofdvenster op de “Toon Schijf G:\” toets – zichtbaar na het ontgrendelen van de betreffende kluismap – drukt dan wordt deze schijf met leesbare inhoud meteen in de bestandsverkenner geopend.

### Opmerking:

Heb je meerdere kluizen, dan kan je ze in het hoofdvenster met de muis in de gewenste volgorde slepen.

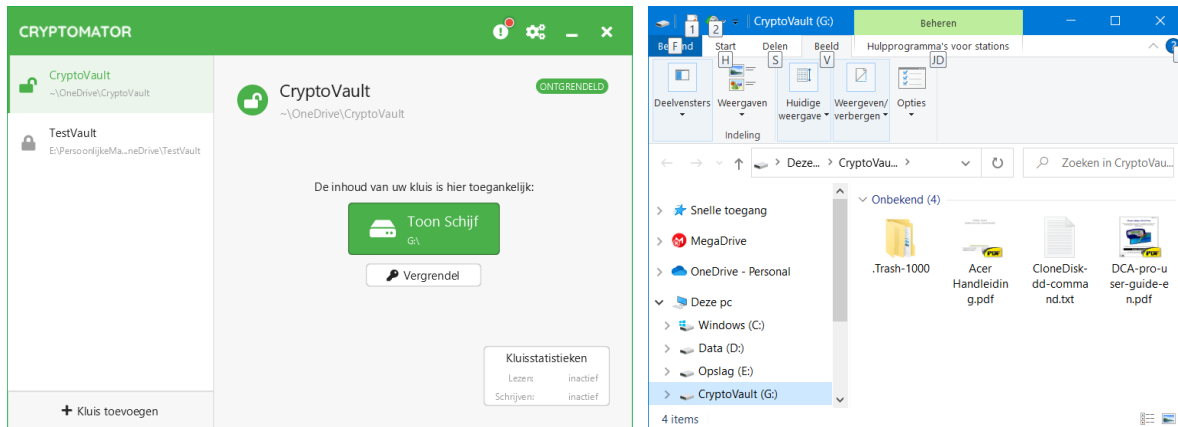
## De Cryptomator kluis openen en erin werken



1. Start Cryptomator en kies een kluis (CryptoVault) om die te “Ontgrendelen...”. Je kan “Wachtwoord Onthouden” aanvinken, dan opent deze kluis in het vervolg vanzelf bij het

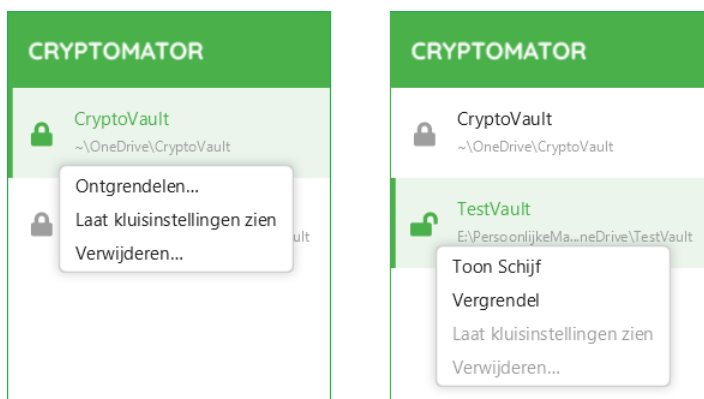


ontgrendelen, mits het opslaan van het wachtwoord in de [algemene voorkeuren](#) is toegestaan.



2. Met “Toon Schijf” open je de lokale kluismap in de bestandsverkenner en kan je daarin werken.
3. Met “Vergrendel” sluit je een kluis weer.

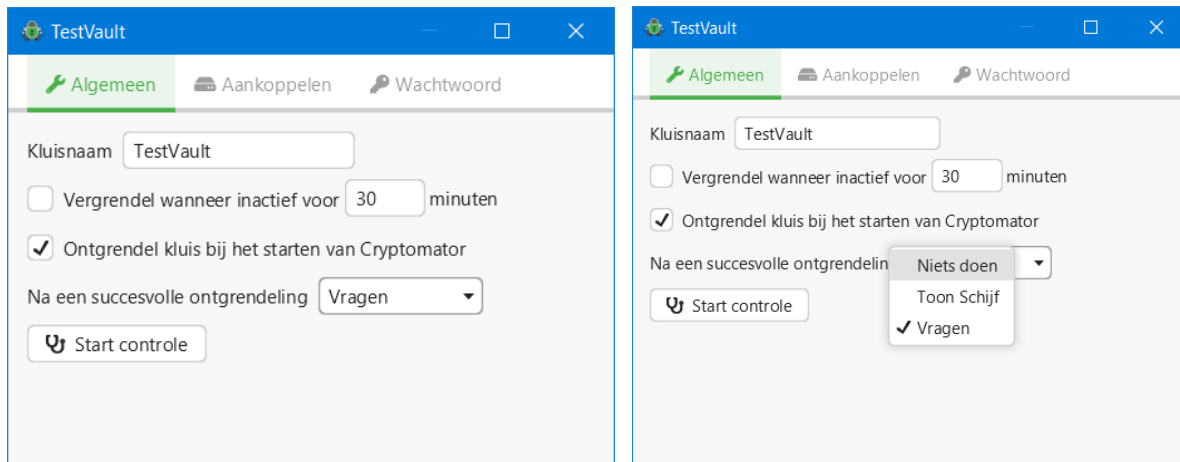
## Acties en voorkeuren per kluis



(dit zijn uitsneden uit het hoofdvenster).

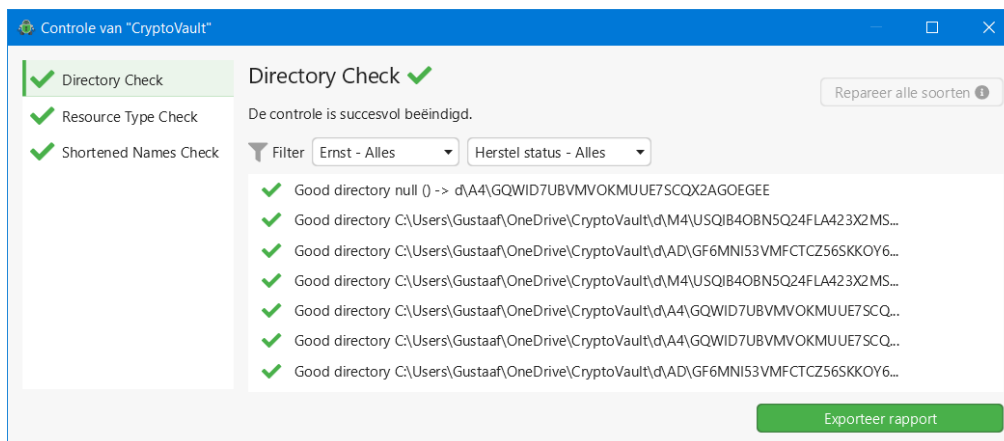
- ➡ Je kan met “Ontgrendelen” of met “Nu ontgrendelen” een gesloten kluis openen. Als het wachtwoord opgeslagen is dan opent “Nu Ontgrendelen” meteen de kluis. Zo niet, dan verschijnt na “Ontgrendelen” het “Ontgrendelen...” venstertje zoals in stap 1.
- ➡ Met “[Laat kluisinstellingen zien](#)” kan je de voorkeuren per gesloten kluis aanpassen.
- ➡ Met “Verwijderen...” kan je een gesloten kluis verwijderen uit Cryptomator. De door de kluis gebruikte mappen blijven wel gewoon bestaan; er gaat geen data verloren en je kan de kluis weer gewoon toevoegen en als tevoren gebruiken.
- ➡ Als de kluis geopend is dan opent “Toon Schijf” de kluismap in de bestandsverkenner, net als de grotere knop in stap 2.
- ➡ Met “Vergrendel” zet je de betreffende kluis weer op slot.

## Laat kluisinstellingen zien – instellingen per kluis:



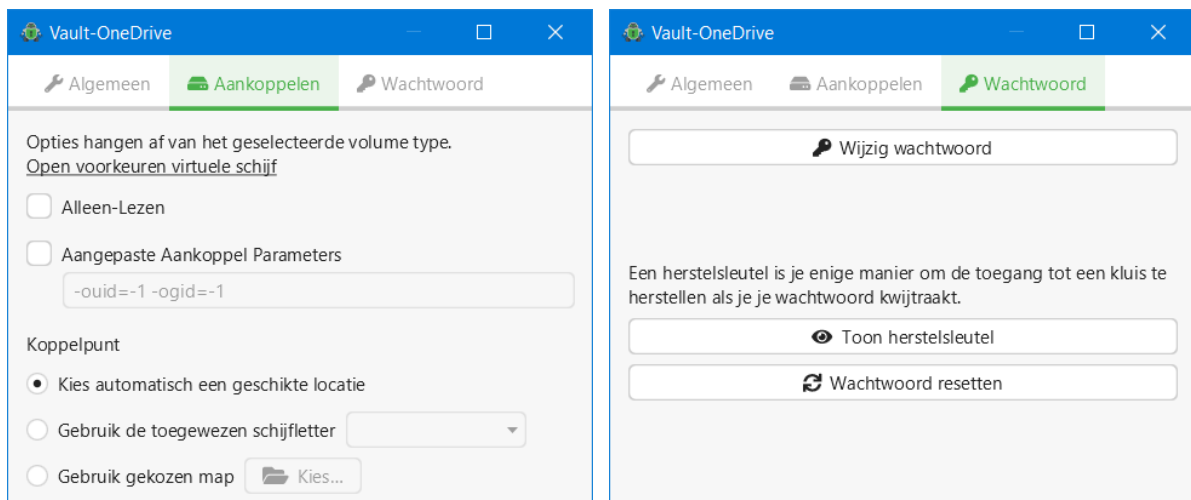
Op tabblad “Algemeen” vind je de volgende voorkeuren:

- ➡ “Kluisnaam” – Het lijkt erop dat je hier de naam van je kluis kan veranderen.  
**Doe dit niet** <sup>(28)</sup>!
- ➡ Met “Vergrendel wanneer inactief voor...” kan je een time-out periode instellen waarna de kluis gesloten wordt als je er niet meer in werkt.
- ➡ Met “Ontgrendel kluis bij het starten van Cryptomator” wordt de kluis automatisch geopend als Cryptomator gestart wordt. Hiervoor moet je wel “Bewaar wachtwoorden met...” in de [algemene voorkeuren](#) aangevinkt hebben.
- ➡ Met “Na een succesvolle ontgrendeling...” kan je instellen of je de dan gemounte kluismap direct wilt laten openen in de bestandsverkenner. De mogelijkheden zijn “Niets doen”, “Toon schijf” of een vraagvenstertje openen waarin je iedere keer kan aanklikken wat je wenst. (rechteraftbeelding).



- ➡ Met “Start controle” kan je een test starten die de consistentie van de kluis test en – indien mogelijk – deze herstelt als er iets mis is.

<sup>28)</sup> In ieder geval niet met OneDrive waarop deze handleiding is gebaseerd; dat ging fout!



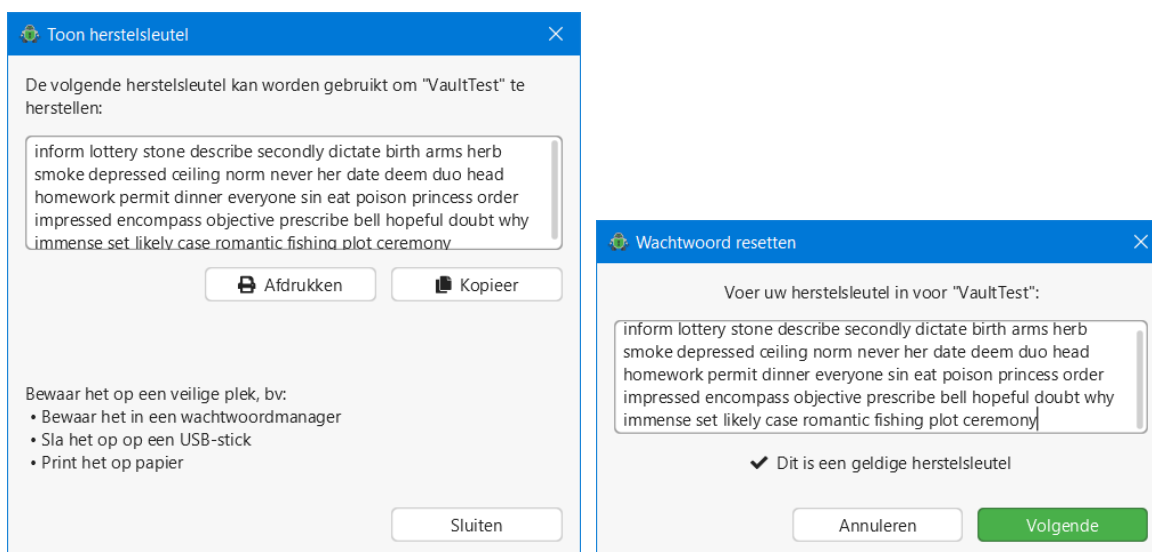
Op tabblad “Aankoppelen” vind je de volgende voorkeuren (verschillend per [virtuele schijf protocol](#)):

- ➔ Met “Alleen-Lezen” kan je de gecodeerde kluis inzien, maar de inhoud ervan niet veranderen.
- ➔ Helaas, geen informatie gevonden met betrekking tot “Aangepaste Aankoppel Parameters”.
- ➔ “Koppelpunt” bepaalt waar je lokale kluismap zich bevindt.  
Met “Kies automatisch een geschikte locatie” wordt dat de eerste beschikbare schijfletter.  
Met “Gebruik de toegewezen schijfletter...” kan je een willekeurige vrije schijfletter toewijzen <sup>(29)</sup>.  
Met “Gebruik gekozen map” kan je zelf ergens – op een schijf of in een map – een lege map aanmaken en toewijzen. Dit is onder andere nuttig als je krap in je schijfletters komt te zitten.

Op tabblad “Wachtwoord” vind je de volgende voorkeuren:

- ➔ Met “Wijzig wachtwoord” kan je een ander wachtwoord instellen.

**Je krijgt dan ook een nieuwe herstelsleutel!**

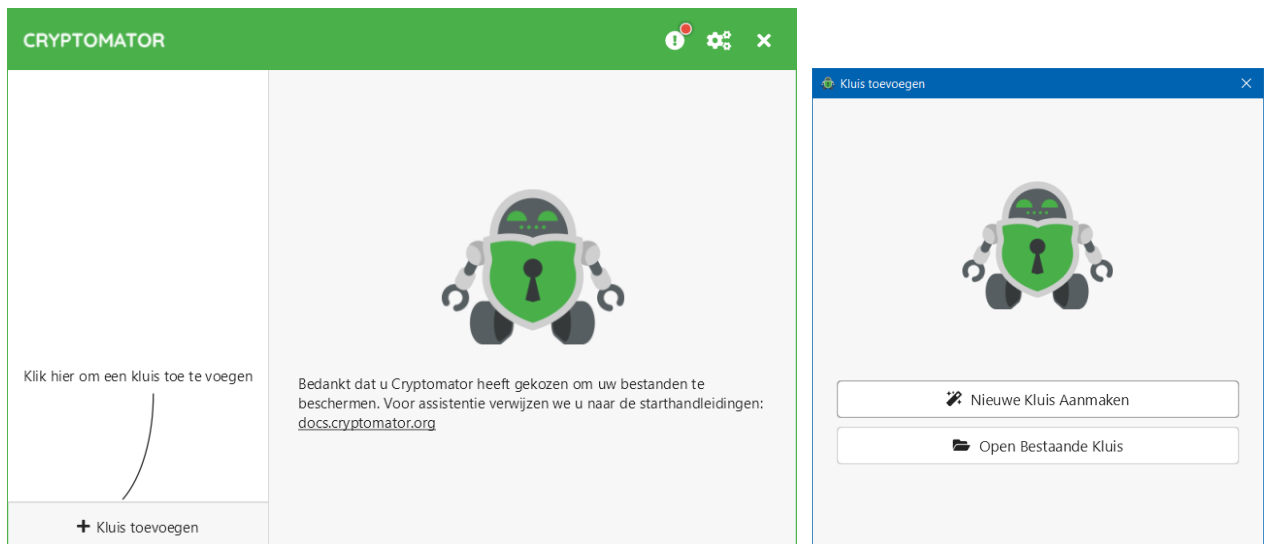


<sup>29)</sup> Als je geen floppy drive hebt, kan je schijfletter A: of B: gebruiken. Windows wijst die verder nooit zelf toe. Daar Windows van D: naar Z: toewijst, kan je ook kluisletters van Z: naar D: toewijzen (meeste kans op onbezet blijven).

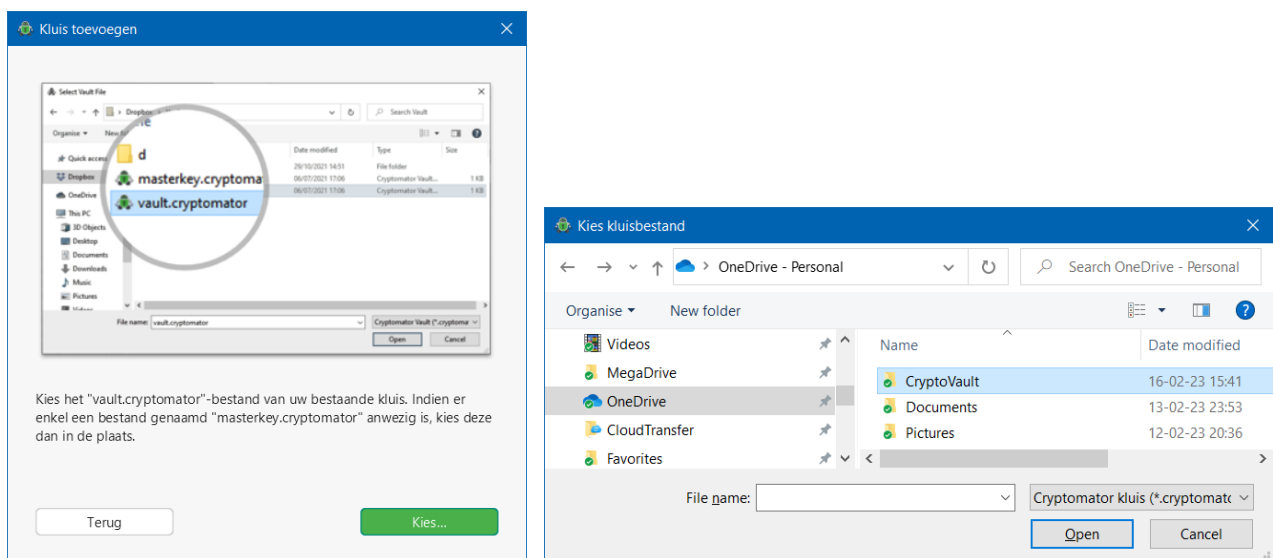
- Met “Toon herstelsleutel” kan je de herstelsleutel opvragen die bij het huidige wachtwoord hoort. Om de herstelsleutel op te kunnen vragen moet je wel met je huidige wachtwoord inloggen.
- Met “Wachtwoord resetten” kan je na het invullen van je herstelsleutel een nieuw wachtwoord aanmaken. Na “Volgende” vul je tweemaal je nieuw gekozen wachtwoord in en klik je op “Resetten”. Je oude herstelsleutel komt te vervallen en je krijgt een nieuwe.

## Koppelen aan een bestaande kluis

Om in Windows te koppelen aan een bestaande kluis – hier CryptoVault in de OneDrive cloud<sup>(30)</sup> – ga je als volgt te werk:

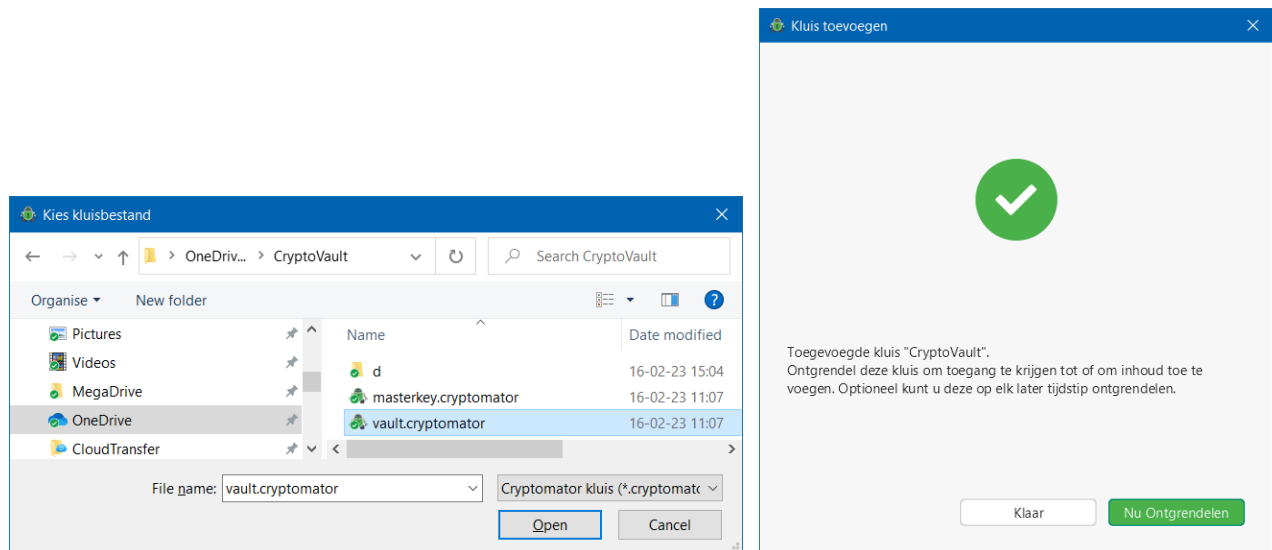


1. Start Cryptomator en klik op “+ Kluis toevoegen”.
2. Klik op “Open Bestaande Kluis”.

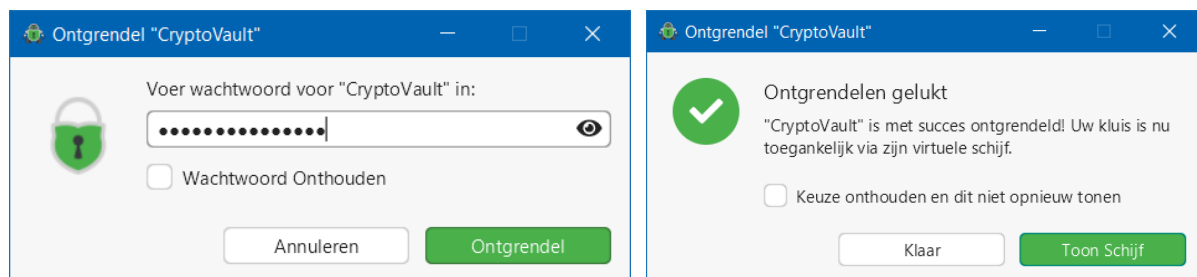


<sup>30)</sup> Je kan in OneDrive aangeven welke mappen gesynchroniseerd moeten worden. Als je het standaard “Alle bestanden beschikbaar maken” hebt uitgeschakeld, dan moet je nu eerst je kluismap voor synchronisatie inschakelen. Zie [bron \[9\]](#).

3. Klik op de knop “Kies...” en navigeer naar de synchronisatiemap van OneDrive<sup>(31)</sup> of een lokale map met een Cryptomator kluis.
4. Kies daarin de kluis Cryptovault en klik de toets “Open” om de inhoud te zien.



5. Kies in Cryptovault bij voorkeur het bestand vault.cryptomator, maar als dit niet aanwezig is kies dan masterkey.cryptomator en klik op de knop “Open”.
6. Je kan nu op “Klaar” klikken om naar het Cryptomator [hoofdvenster](#) te gaan of op “Nu Ontgrendelen” om de kluis te openen. In dat laatste geval krijg je de volgende vensters:



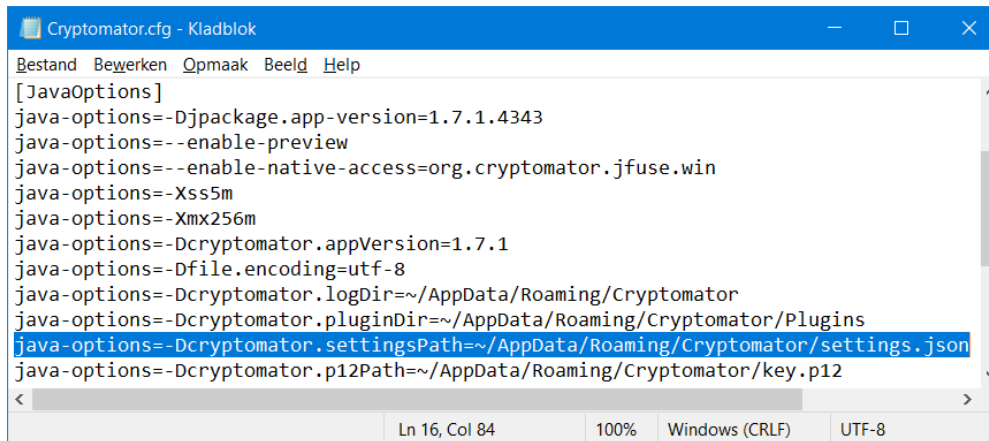
7. Voer het wachtwoord in, vink desgewenst “Wachtwoord onthouden” aan<sup>(32)</sup> en klik op “Ontgrendel”. In het vervolgvenster kan je desgewenst “Keuze onthouden en dit niet opnieuw tonen” aanvinken.  
 Als je dan “Toon schijf” klikt dan zal dit in de toekomst altijd bij openen gebeuren, maar als je “Klaar” klikt zal de schijf in de toekomst niet automatisch getoond worden, (dit kan je later nog aanpassen).  
 Je gaat nu naar het Cryptomator [hoofdvenster](#) terug.

<sup>31)</sup> De Windows standaardmap is `C:\Gebruikers\<gebruikersnaam>\OneDrive\<Kluisnaam>`.

<sup>32)</sup> Voor het onthouden van het wachtwoord moet wel “Wachtwoorden onthouden met...” in de [algemene voorkeuren](#) aangevinkt zijn.

## De gebruikte paden en instellingen van Cryptomator

Maak wel eerst een back-up van deze bestanden als je wat wilt gaan wijzigen!

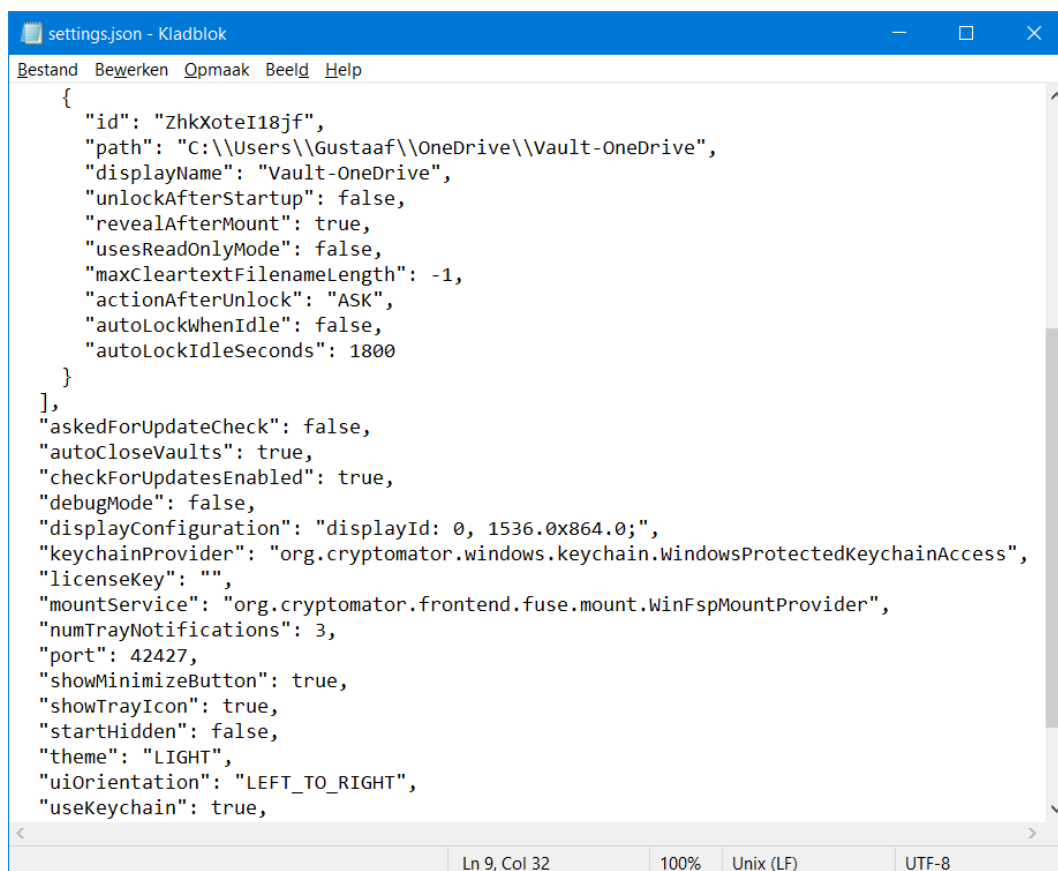


```

Cryptomator.cfg - Kladblok
Bestand Bewerken Opmaak Beeld Help
[JavaOptions]
java-options=-Djpackage.app-version=1.7.1.4343
java-options=--enable-preview
java-options=--enable-native-access=org.cryptomator.jfuse.win
java-options=-Xss5m
java-options=-Xmx256m
java-options=-Dcryptomator.appVersion=1.7.1
java-options=-Dfile.encoding=utf-8
java-options=-Dcryptomator.logDir=~/.AppData/Roaming/Cryptomator
java-options=-Dcryptomator.pluginDir=~/.AppData/Roaming/Cryptomator/Plugins
java-options=-Dcryptomator.settingsPath=~/.AppData/Roaming/Cryptomator/settings.json
java-options=-Dcryptomator.p12Path=~/.AppData/Roaming/Cryptomator/key.p12
Ln 16, Col 84 100% Windows (CRLF) UTF-8

```

Het configuratiebestand Cryptomator.cfg waarin onder andere de belangrijke paden van de app bepaald worden bevindt zich in <sup>(33)</sup> *C:\Program Files\Cryptomator\app\Cryptomator.cfg*.



```

settings.json - Kladblok
Bestand Bewerken Opmaak Beeld Help
{
  "id": "ZhkXoteI18jf",
  "path": "C:\\Users\\Gustaaf\\OneDrive\\Vault-OneDrive",
  "displayName": "Vault-OneDrive",
  "unlockAfterStartup": false,
  "revealAfterMount": true,
  "usesReadOnlyMode": false,
  "maxCleartextFilenameLength": -1,
  "actionAfterUnlock": "ASK",
  "autoLockWhenIdle": false,
  "autoLockIdleSeconds": 1800
},
"askedForUpdateCheck": false,
"autoCloseVaults": true,
"checkForUpdatesEnabled": true,
"debugMode": false,
"displayConfiguration": "displayId: 0, 1536.0x864.0;",
"keychainProvider": "org.cryptomator.windows.keychain.WindowsProtectedKeychainAccess",
"licenseKey": "",
"mountService": "org.cryptomator.frontend.fuse.mount.WinFspMountProvider",
"numTrayNotifications": 3,
"port": 42427,
"showMinimizeButton": true,
"showTrayIcon": true,
"startHidden": false,
"theme": "LIGHT",
"uiOrientation": "LEFT_TO_RIGHT",
"useKeychain": true,
Ln 9, Col 32 100% Unix (LF) UTF-8

```

De Cryptomator algemene instellingen en kluispaden en -instellingen vind je in

*C:\Gebruikers\<gebruikersnaam>\AppData\Roaming\Cryptomator\settings.json*.

Je kan hierin te gebruiken paden en instellingen aanpassen in bijvoorbeeld Kladblok (= Notepad).

<sup>33)</sup> Hier wordt de Linux notatie voor home ~/ gebruikt voor de Windows home *C:\Gebruikers\<gebruikersnaam>\*.

## Kluis op een usb-stick

Je kan één of meer Cryptomater kluisen ook opslaan op een extern medium, zoals een usb-stick. Deze kluisen zijn dan zowel in Linux als in Windows bruikbaar.

Je hebt de mogelijkheid om kluisen op je usb-stick aan te maken met – of toe te voegen aan – de Cryptomator app die is geïnstalleerd in Windows en/of Linux op je computer(s). Je usb-kluisen zijn dan benaderbaar vanaf die computer(s) als de usb-stick aanwezig is.

Maar in Windows je kan ook verdergaan en een portable Cryptomator app installeren op de usb-stick zelf. Dan kan je deze ook gebruiken op andere Windows computers zonder Cryptomator installatie.

Cryptomator kan er goed tegen als een kluis ontbreekt bij een afwezige usb-stick.

Insteken en verwijderen van het extern medium terwijl Cryptomator actief is kan geen kwaad. Wel blijft het van belang om de stick volgens de regels uit te werpen. Vooraf de kluis in Cryptomator vergrendelen is wel zo netjes, maar geen must.

Als je de usb-stick zowel in Linux als in Windows wilt gebruiken, kan je deze het beste voorbereiden in Windows, in verband met het toewijzen van een vaste schijfletter op je eigen Windows computer.

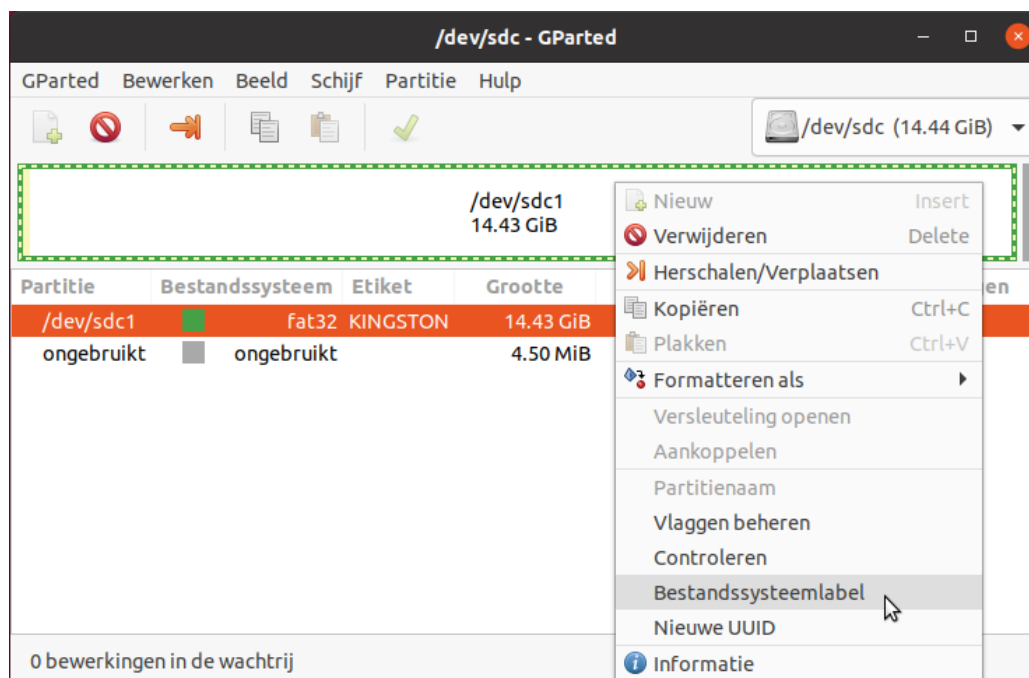
Voor de Windows beschrijving ga naar [Windows](#); de Ubuntu Linux beschrijving begint [hier](#).

## De usb-stick voorbereiden in Linux

Als je de usb-stick insteekt, dan wordt deze zichtbaar in `/media/<gebruikersnaam>/<sticklabel>`.

Dat sticklabel<sup>(34)</sup> verschijnt in de bestandsverkenner. Daar wil je waarschijnlijk een zinvolle naam zien (bijvoorbeeld USBKLUIS), waarmee je de usb-stick duidelijk kan identificeren.

Dit kan je regelen met bijvoorbeeld de standaard Linux partitie manager Gparted:



<sup>34)</sup> In de Nederlandstalige Gparted heet het sticklabel "Etiket"; de usb-stick had in de schermafdruck nog label "KINGSTON".

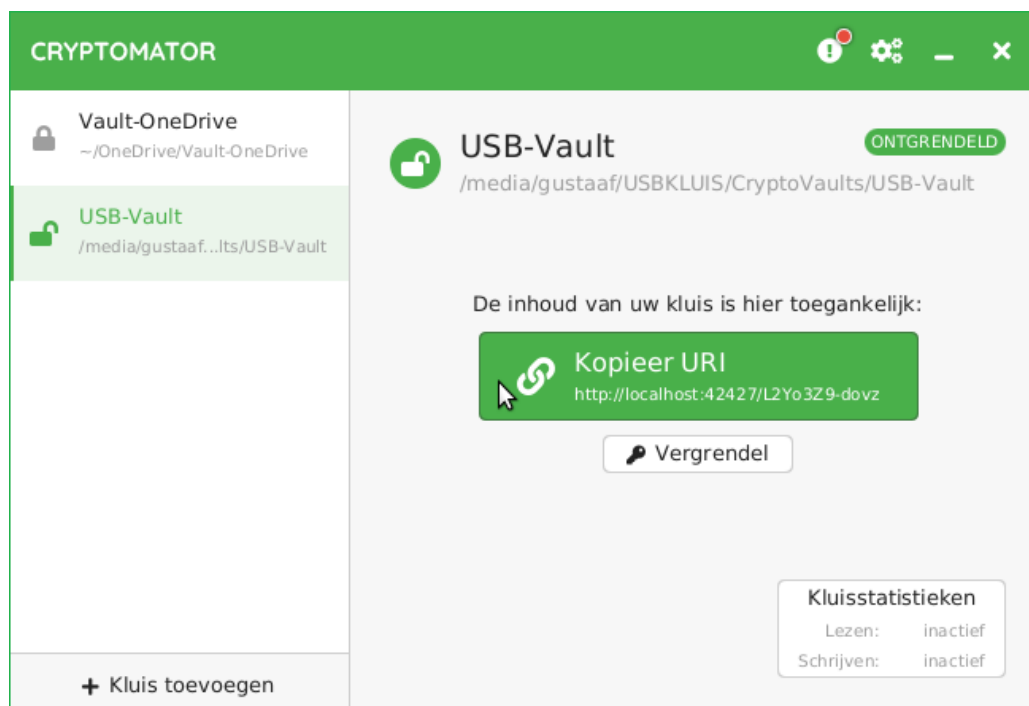
1. Start Gparted en selecteer rechtsboven het juiste opslagmedium – hier de 14.44 GiB /dev/sdc schijf.
2. Rechtsklik op de partitie en kies “Ontkoppelen” (verandert in “Aankoppelen”).  
Pas als de usb-stick ontkoppeld is kan je veranderingen aanbrengen.
3. Kies vervolgens “Bestandssysteemplaatje”.  
Er verschijnt een venstertje waarin je het gewenste label kan invullen of aanpassen.
4. Als de bewerking links beneden in de wachtrij staat, klik je op het groene vinkje in de bovenbalk om de bewerking daadwerkelijk toe te passen. Als dit afgerond is sluit je Gparted.
5. Wanneer je nu de bestandsverkenner opent, zie je de usb-stick nu met het nieuwe label als naam. Is de usb-stick niet zichtbaar, dan kan je dit oplossen door deze los te nemen en weer aan te sluiten.

Je kan nu in Cryptomator één of meer kluisen aanmaken op de usb-stick.

## Een USB kluis openen in de Linux bestandsverkenner

Voor alle details wordt verwezen naar de Ubuntu Linux beschrijving vanaf [Een of meer kluisen toevoegen](#). Er is geen wezenlijk verschil tussen een kluis op een te verwijderen extern opslagmedium en een kluis op een intern opslagmedium.

Met WebDAV (HTTP Address) <sup>(35)</sup> als “Virtuele schijf” is het tonen van de kluisinhoud in de Linux bestandsverkenner net even wat bewerkelijker in vergelijking met de Windows mogelijkheden. Dit moet éénmalig per kluis.



<sup>35)</sup> Om WebDAV (gio) te kunnen gebruiken moet een extra Gnome gio tool geïnstalleerd worden.



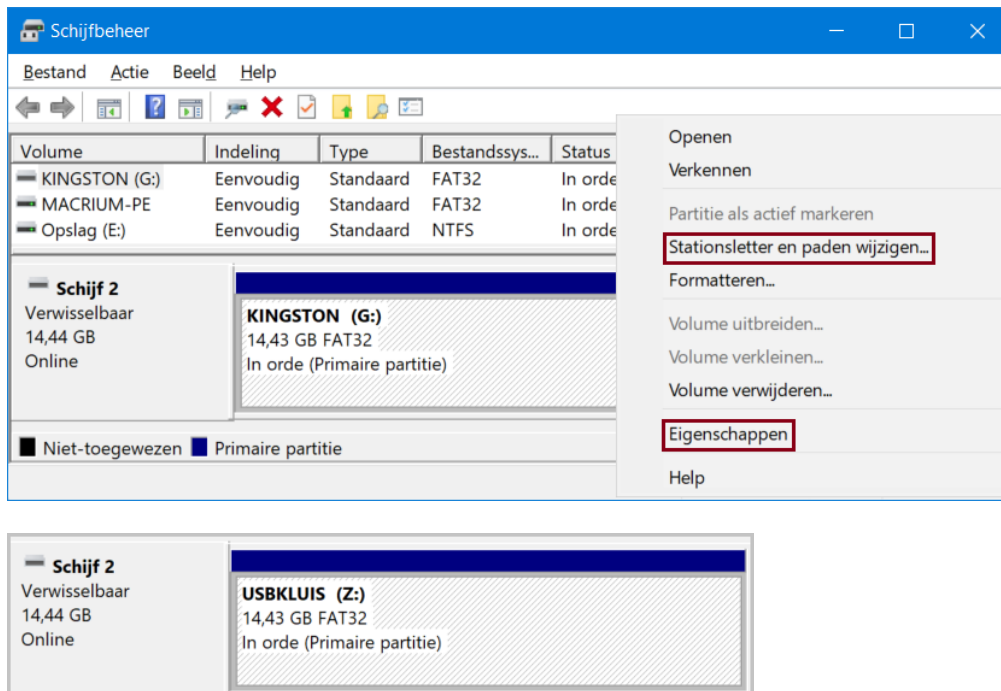
1. Als de kluis geopend is, klik je op “Kopieer URI” voor het adres van de geopende kluis.



2. In de bestandverkenner kies je “Andere locaties”.
3. In het “Verbinden met server” venster plak je het kluisadres, maar je vervangt *http:* door *dav:* met als resultaat bijvoorbeeld *dav://localhost:42427/CZb242p2j5pU*.
4. Vervolgens maak je een bladwijzer die je de gewenste naam geeft, zoals [hier](#).

## De usb-stick voorbereiden in Windows

Als je de usb-stick vanuit een geïnstalleerde Cryptomator wilt benaderen is het wel noodzakelijk dat deze steeds bij insteken dezelfde schijffletter<sup>(36)</sup> toegewezen krijgt (hier Z:). Bovendien wil je de usb-stick waarschijnlijk ook wel een herkenbaar label laten tonen (hier USBKLUIS). Dit kan je in Windows regelen met de Windows “Disk Management” partitie manager.



<sup>36)</sup> Als je geen floppy drive hebt, kan je schijffletter A: of B: gebruiken. Windows wijst die letters nooit zelf toe. Daar Windows van D: naar Z: toewijst, kan je ook schijffletters van Z: naar D: handmatig toewijzen (dat geeft de meeste kans op onbezet blijven).

De naam en stationsletter van de usb-stick wijzigen doe je als volgt:

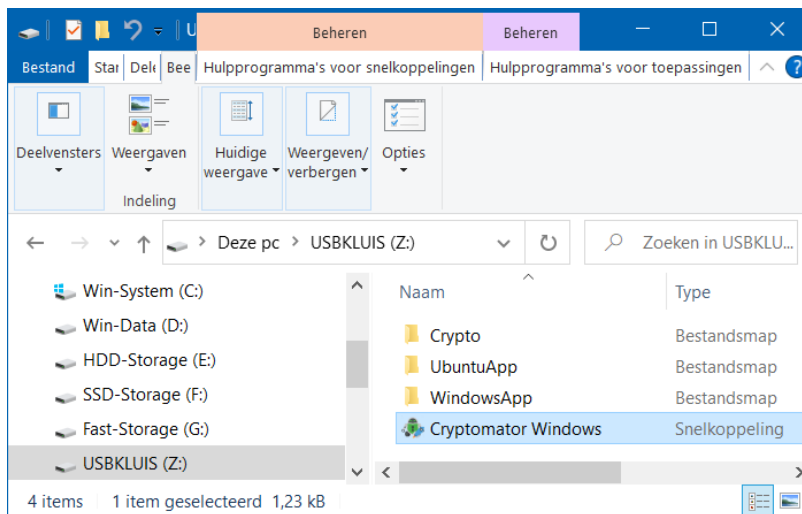
1. Start Windows applicatie “Schijfbeheer” (zoek: Partities op harde schijf maken en formatteren).
2. Rechtsklik de partitie van de betreffende usb-stick (hier Kingston (G:)).
3. Selecteer in de achtereenvolgende vensters “Stationsletter en paden Wijzigen...” – “Wijzigen” – selecteer stationsletter “Z:” – klik “OK” gevolgd door “Ja”.  
De stationsletter is nu gewijzigd in “Z:”.
4. Rechtsklik de partitie van de betreffende usb-stick weer en kies “Eigenschappen” om het “Eigenschappen” venster te openen.
5. Wijzig in tabblad “Algemeen” de getoonde naam van de usb-stick (hier in USBKLUIS) en klik op “OK”. De nieuwe naam is nu vastgelegd op de usb-stick.

**Let wel:** de schijfletter wordt niet vastgelegd op het opslagmedium, maar in het Windows register. Je moet dit daarom doen voor al je Windows installaties.

Als het je te doen is om één of meer kluizen te hebben die je kan loskoppelen van je computer en veilig op te bergen, dan kan je die nu vanuit de Cryptomator installatie in Windows of Linux aanmaken op de usb-stick.

Maar je kan ook verdergaan en een portable Cryptomator app installeren op de usb-stick zelf om deze ook te kunnen gebruiken op Windows computers zonder geïnstalleerde Cryptomator.

## Cryptomator portable installeren op de usb-stick (alleen Windows)



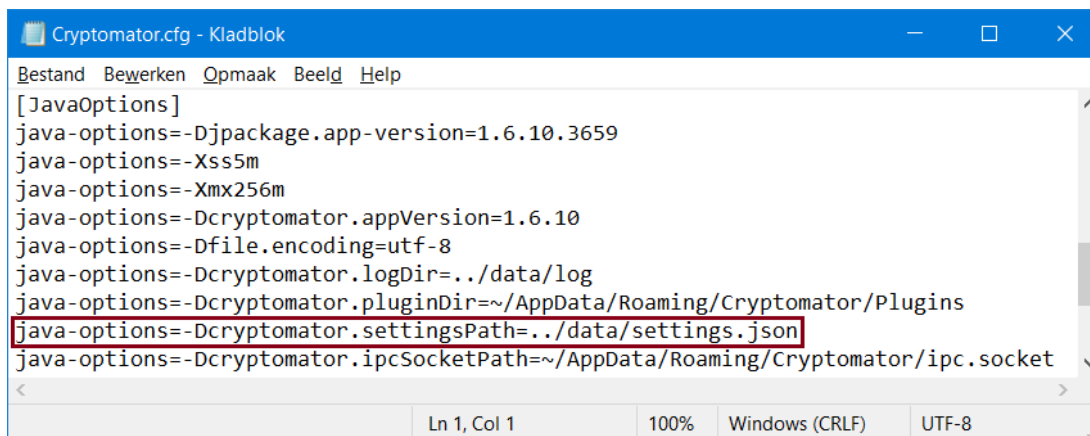
1. Download Cryptomator portable, bijvoorbeeld van [bron \[8\]](#).
2. Als je de aanbevolen .exe versie hebt gedownload en je voert deze uit, dan wordt in `C:\portapps\` van Windows de map `cryptomator-portable` geplaatst met daarin de benodigde executable en de hulpbestanden.

3. Kopieer de map *cryptomator-portable* naar je usb-stick (dit is het portable geheel waar het om gaat). In bovenstaande afbeelding is de cryptomator map in de map WindowsApp geplaatst. Je kan desgewenst de map *portapps* met inhoud van je C: schijf verwijderen.
4. Het pad naar de Cryptomator executable in dit voorbeeld is: *Z:\WindowsApp\cryptomator-portable\cryptomator-portable.exe*. Je kan nu een snelkoppeling maken en die naar Z: verplaatsen. Zie snelkoppeling "Cryptomator Windows" in de afbeelding. Door hierop te dubbelklikken kan je Cryptomator starten.
5. Desgewenst kan je de snelkoppeling naar je Windows bureaublad kopiëren om daar Cryptomator te starten als de usb-stick aanwezig is.

Je kan nu één of meer kluizen op de usb-stick aanmaken en desgewenst koppelen naar kluizen op je computer. Ga hiervoor door met [De algemene voorkeuren aanpassen](#) en wat daarop volgt. Als je daarmee klaar bent, dan heb je een usb-stick die zelfstandig op je eigen Windows goed werkt.

## De gebruikte paden en instellingen van Cryptomator portable

Maak wel eerst een back-up van deze bestanden als je wat wilt gaan wijzigen!

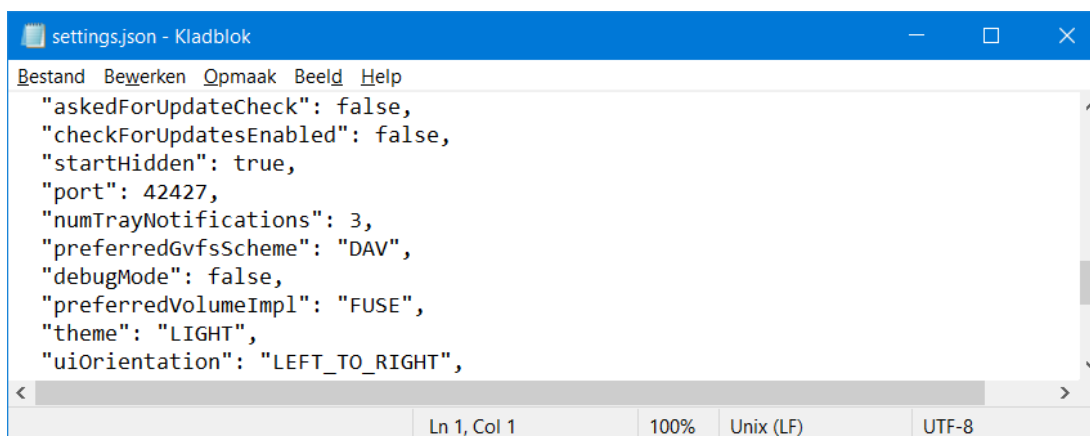


```

Cryptomator.cfg - Kladblok
Bestand Bewerken Opmaak Beeld Help
[JavaOptions]
java-options=-Djpackage.app-version=1.6.10.3659
java-options=-Xss5m
java-options=-Xmx256m
java-options=-Dcryptomator.appVersion=1.6.10
java-options=-Dfile.encoding=utf-8
java-options=-Dcryptomator.logDir=../data/log
java-options=-Dcryptomator.pluginDir=~/.AppData/Roaming/Cryptomator/Plugins
java-options=-Dcryptomator.settingsPath=../data/settings.json
java-options=-Dcryptomator.ipcSocketPath=~/.AppData/Roaming/Cryptomator/ipc.socket
Ln 1, Col 1    100%    Windows (CRLF)    UTF-8

```

Uitgaande van de map *cryptomator-portable* bevindt het configuratiebestand *Cryptomator.cfg* – waarin onder andere de belangrijke paden van de app bepaald worden – zich in  
*...\cryptomator-portable\app\app\Cryptomator.cfg*.



```

settings.json - Kladblok
Bestand Bewerken Opmaak Beeld Help
{
  "askedForUpdateCheck": false,
  "checkForUpdatesEnabled": false,
  "startHidden": true,
  "port": 42427,
  "numTrayNotifications": 3,
  "preferredGvfsScheme": "DAV",
  "debugMode": false,
  "preferredVolumeImpl": "FUSE",
  "theme": "LIGHT",
  "uiOrientation": "LEFT_TO_RIGHT",
}
Ln 1, Col 1    100%    Unix (LF)    UTF-8

```

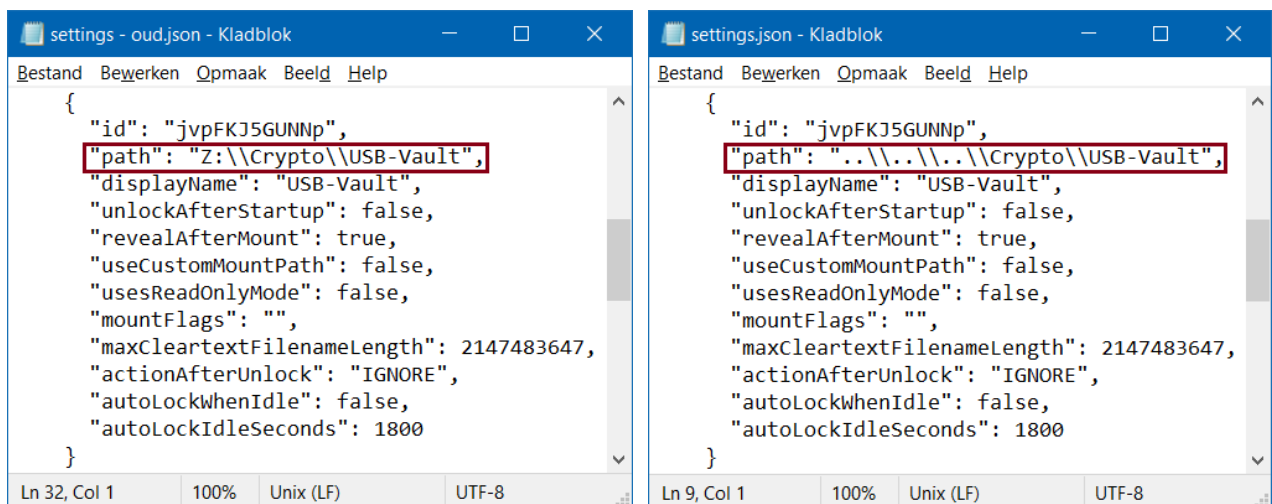
De Cryptomator algemene instellingen en kluispaden en -instellingen vind je in  
`...\\cryptomator-portable\\data\\settings.json`.

Je kan hierin te gebruiken paden en instellingen aanpassen in bijvoorbeeld Kladblok (= Notepad).

## Cryptomator-portable op andere Windows computers gebruiken

Voor je eigen computer(s) heb je een vaste schijfletter ingesteld. De paden naar de kluisen die je hebt aangemaakt of toegevoegd op je usb-stick zijn opgeslagen als absolute paden, uitgaande van deze vaste schijfletter. Maar op andere Windows computers krijgt de usb-stick met hoge waarschijnlijkheid een andere schijfletter toegewezen. En dan zijn plotseling de kluisen op de stick onbereikbaar<sup>(37)</sup>. Om dit op te lossen moeten de paden naar de kluisen die op de stick opgeslagen zijn veranderd worden in relatieve paden ten opzichte van de locatie van de app `cryptomator.exe`. Dit doe je door het bestand `...\\cryptomator-portable\\data\\settings.json` te bewerken in bijvoorbeeld Kladblok (Notepad). Het is een goed idee om van `settings.json` een kopie te maken voordat je dit bestand gaat wijzigen.

In dit voorbeeld is de situatie op de eigen computer als volgt:



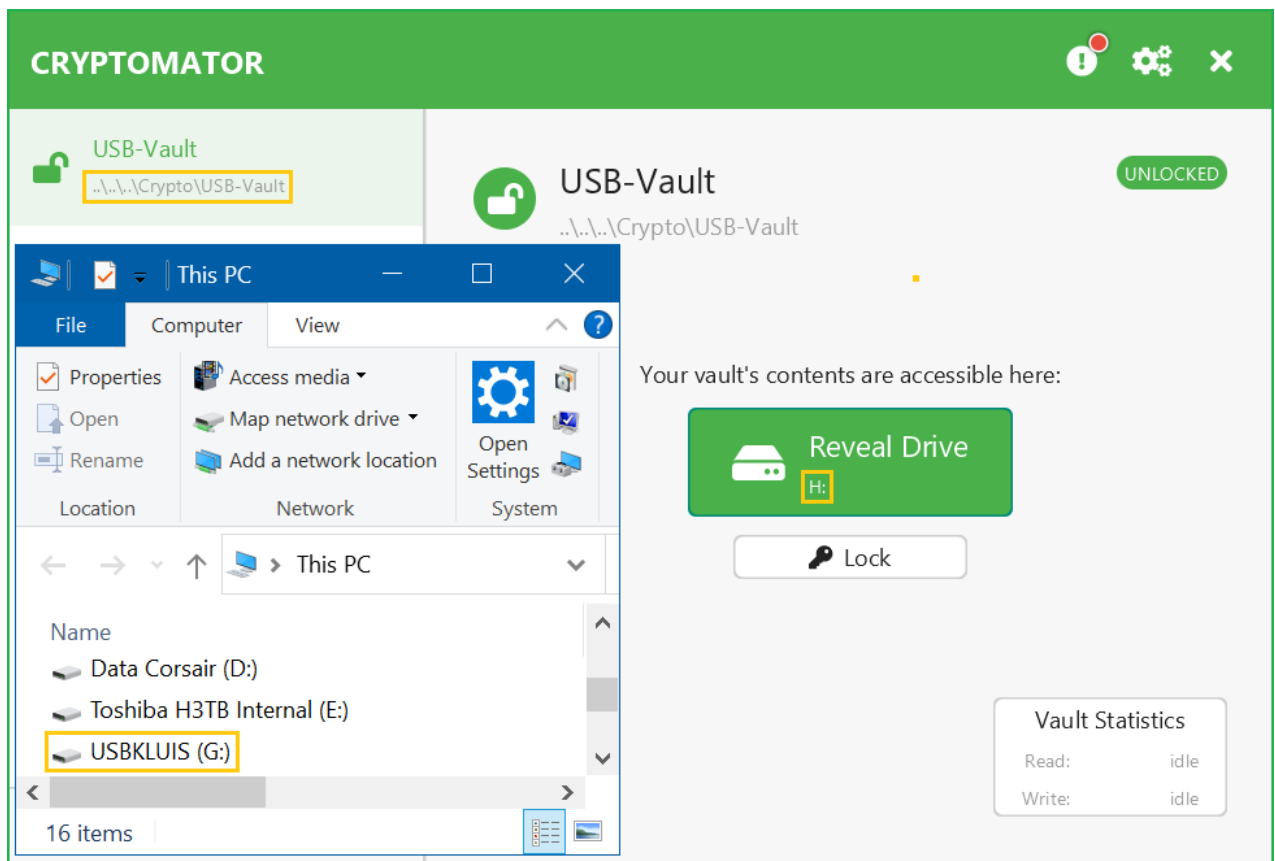
Het bestand `settings.json` zit op `Z:\\WindowsApp\\cryptomator-portable\\data\\settings.json`.

De kluismap USB-Vault zit op: `Z:\\Crypto\\USB-Vault`.

De app waar het om gaat zit op: `Z:\\WindowsApp\\cryptomator-portable\\app\\Cryptomator.exe`.

Je moet in dit geval vanaf `Cryptomator.exe` drie map-stappen (`..\\`) terug om in Z: te komen en dan ga je naar `Crypto\\USB-Vault` als volgt: `..\\.\\.\\.\\.\\.\\Crypto\\USB-Vault`.

<sup>37)</sup> Op een andere Windows computer zal de snelkoppeling op de usb-stick ook niet werken met andere schijfletter. Je moet dan `...\\cryptomator-portable\\app\\Cryptomator.exe` dubbelklikken.



Op de Engelstalige testcomputer zonder afgedwongen schijftoewijzing wordt nu bij aansluiten van de USB-stick in dit geval schijfletter G: toegekend. Het pad naar de USB-Vault in het hoofdvenster is nu relatief gespecificeerd. In dit geval wordt de kluis geopend op volgende vrije schijfletter H:. Op je eigen computer blijft het gewoon de in dit voorbeeld vastgelegde schijfletter Z: en zie je het absolute pad *Z:\Crypto\USB-Vault*.

## Bronnen (Engels- of Nederlandstalig)

- [1] <https://cryptomator.org/downloads/>  
(Downloads voor installatie van Cryptomator).
- [2] <https://docs.cryptomator.org/en/latest/>  
(Engelstalige online handleiding).
- [3] [https://docs.cryptomator.org/\\_/downloads/en/latest/pdf/](https://docs.cryptomator.org/_/downloads/en/latest/pdf/)  
(Engelstalige handleiding (.pdf) download).
- [4] <https://ubuntuhandbook.org/index.php/2022/04/open-as-administrator-ubuntu-22-04/>  
("Open als Administrator" optie toevoegen aan de bestandsverkenner "Files" (= nautilus).
- [5] <https://docs.cryptomator.org/en/latest/desktop/vault-mounting/>  
(Keuze intern protocol FUSE / WebDAV / Dokany).
- [6] <https://bloatwareremover.com/removal-guides/how-to-uninstall-cryptomator/>  
(Cryptomator verwijderen in Windows).
- [7] <https://opensource.hcc.nl/downloads/publieke-downloads/16-microsoft-onedrive-gebruiken-in-ubuntu-linux-en-linux-mint/file>  
(Download van Nederlandse handleiding hoe je de OneDrive client in Ubuntu Linux installeert)
- [8] <https://portapps.io/app/cryptomator-portable>  
(Download van portable Cryptomator).
- [9] <https://support.microsoft.com/nl-nl/office/kiezen-welke-onedrive-mappen-worden-gesynchroniseerd-met-uw-computer-98b8b011-8b94-419b-aa95-a14ff2415e85>  
(Mappen al of niet synchroniseren in OneDrive).