KeePass, een wachtwoordkluis

Reviewer

Aad Munsterman

Versie

2.36

Samenvatting

KeePass is een programma dat zich gedraagt als een kluis voor, primair, het opbergen van gebruikersnamen en wachtwoorden die je gebruikt om op systemen of websites in te loggen. Het is een open source-programma en beschikbaar voor Windows, slimme telefoons en, via Windows-emulatie, ook voor Linux en Mac OS X. Er zijn vele plug-ins ontwikkeld, onder andere voor import, export en back-up van de gegevens. KeePass is een actief product, waar regelmatig updates voor verschijnen. Door deze veelzijdigheid en open structuur is het uitermate geschikt voor de computerhobbyist.

Functionaliteit

KeePass maakt een database aan, die wordt afgeschermd met een masterwachtwoord. In die database worden door de gebruiker records aangemaakt met alle inloggegevens en eventueel andere informatie. Via knoppen kan deze informatie overgenomen worden om direct een website te openen en de gebruikersnaam en het wachtwoord in te vullen. KeePass beschikt over een geavanceerde wachtwoordgenerator en biedt via plug-ins aanvullende functionaliteit, waaronder automatische back-up van de gegevens.

Waardering

4 (op schaal 1 (slecht) t/m 5 (uitmuntend))

Inleiding

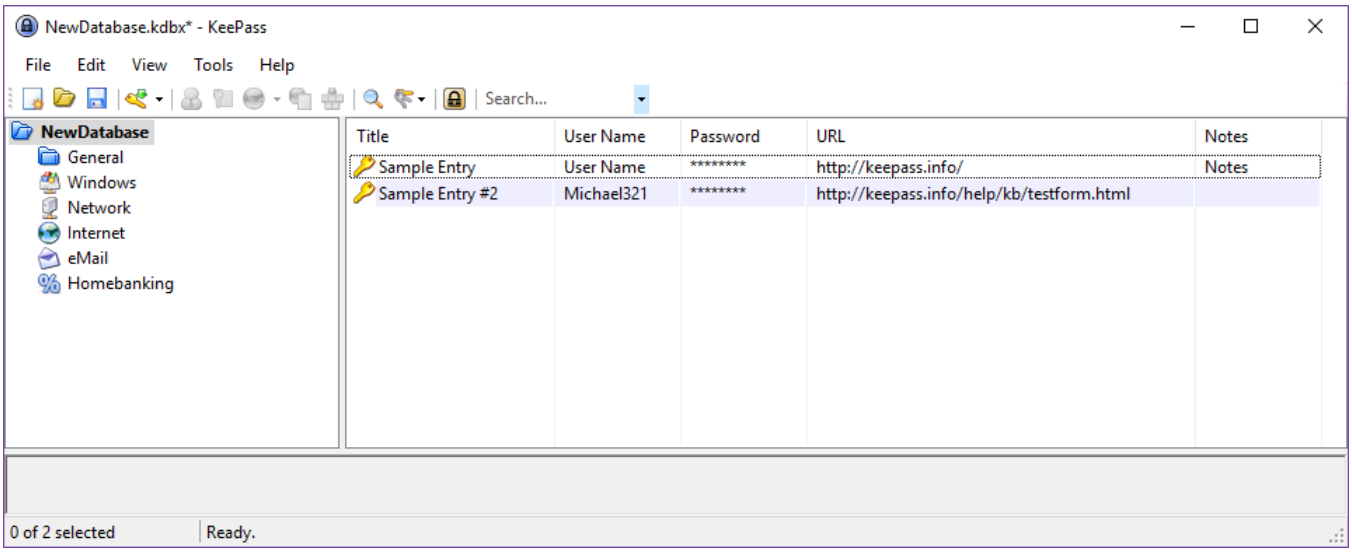
Voor toegang tot systemen en websites hebben we gebruikersnamen en wachtwoorden nodig. Om onze privacy te beschermen zijn maatregelen nodig om de risico's van het gebruik van deze toegangscodes te beperken. Risico's worden onder andere veroorzaakt door toegangsgegevens vastgelegd op een velletje papier, het gebruiken van gemakkelijk te raden zwakke paswoorden en het gebruik van dezelfde paswoorden voor verschillende systemen. KeePass heeft een antwoord op deze beveiligingrisico's.

Wat is het?

KeePass is een Windows-programma dat zich gedraagt als een kluis voor het opbergen van, primair, gebruikersnamen en wachtwoorden die je gebruikt om op systemen of websites in te loggen. Het is een populair programma omdat het niets kost (freeware) en je persoonlijke gegevens op je eigen pc bewaart en niet in de (al dan niet betrouwbare) Cloud. Het programma is tevens 'open source', waardoor gecontroleerd kan worden dat er geen geheime achterdeuren in geprogrammeerd zijn.

Naast gebruikersnamen en wachtwoorden kun je er bijvoorbeeld ook licentiecodes, paspoortnummers en dergelijke in opbergen. Je kunt er zelfs documenten in opslaan. Je hoeft maar één wachtwoord te onthouden om de kluis te openen. Het programma is standaard in de Engelse taal beschikbaar, maar er kan een Nederlandse taalmodule gedownload en geïnstalleerd worden. De applicatie is primair beschikbaar voor Windows en slimme telefoons, en via Windows-emulatie ook voor Linux en Mac OS X. Daarnaast zijn er ook (open source-) klonen beschikbaar voor directe installatie onder Linux. Voor Windows wordt Microsoft.Net als basis gebruikt. Er zijn vele plug-ins ontwikkeld voor

onder andere import, export en back-up van de gegevens. KeePass is een actief product waar regelmatig updates voor verschijnen. Door deze veelzijdigheid en de open structuur is het uitermate geschikt voor de computerhobbyist.



Wat doet het?

KeePass maakt na installatie een database aan waarbij gebruik gemaakt wordt van zeer sterke versleuteling (AES, SHA 256). Daarnaast bevat het beveiliging tegen het raden van het kluiswachtwoord, beveiliging tegen toegang tot de database en bescherming tegen het zoeken in het geheugen naar gegevens van de database.

Na installatie kunnen gegevens toevoegd worden in zogenoemde records. Elk record betreft de gegevens voor toegang tot een systeem of website. Records worden in groepen geplaatst. Een basisset Groepen is al aanwezig. Nieuwe groepen, bijvoorbeeld ‘Webshops’, kunnen worden aangemaakt. Je kunt de records later ook nog naar een bepaalde groep slepen.

KeePass beschikt over een krachtige wachtwoordgenerator. Voor nieuwe invoer wordt al gelijk een sterk paswoord gegenereerd. Voor websites die voor jou al een wachtwoord genereren, kun je met invoer van dat wachtwoord een nieuwe genereren die aan dezelfde eisen voldoet. De eisen waaraan een wachtwoord moet voldoen kunnen gewijzigd worden door de wachtwoordgenerator te openen.

Heb je al wachtwoorden opgenomen in een andere wachtwoordbeheerder of als CSV-bestand opgeslagen, dan kun je ze importeren. De importfunctie van KeePass biedt een scala aan mogelijkheden.

Hoe te gebruiken?

Opstarten van KeePass doe je door op het betreffende KeePass-icoon te klikken en het masterwachtwoord in te voeren. Direct na de installatie zijn er twee voorbeeldrecords.

· **Invoer genereren**

Een nieuw record wordt gegenereerd met **Control+I** of **rechtermuisknop met Add Entry** of **Invoer toevoegen**. De invoervelden spreken voor zich.

Van boven naar beneden:

· Geef in **Titel** het record een logische naam, zodat je het via het zoekveld terug kunt vinden.

· **Gebruikersnaam** is de naam die nodig is voor toegang tot het systeem/website.

· **Wachtwoord** wordt initieel gegenereerd, maar kan ook handmatig ingevoerd worden.

· **Herhaal** is voor het opnieuw invoeren van hetzelfde wachtwoord. Gaat automatisch door op de drie puntjes te klikken.

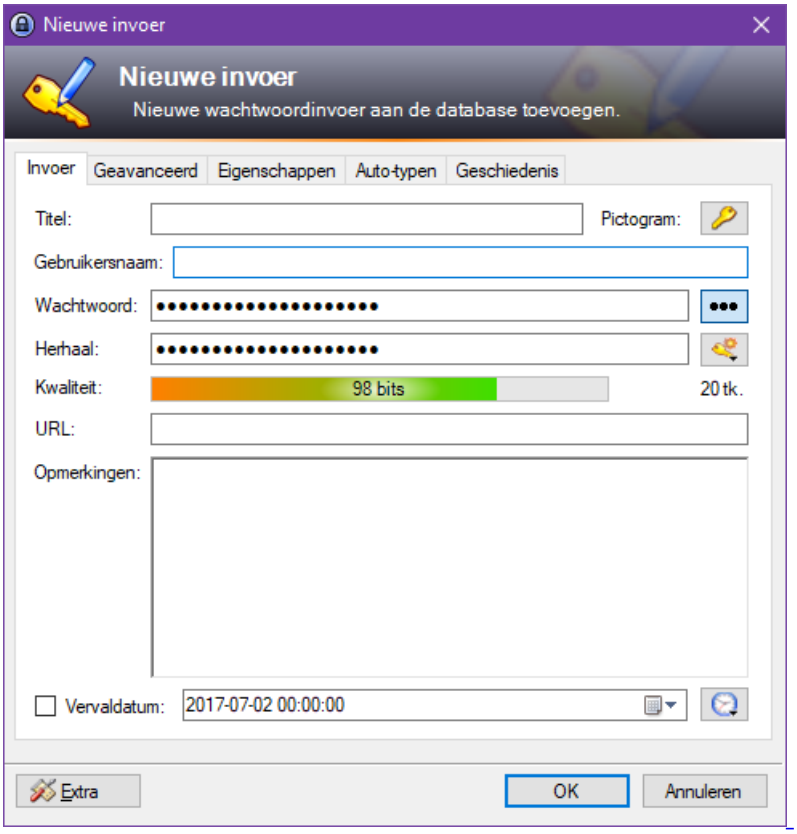
· Met de drie puntjes maak je ook het wachtwoord zichtbaar.

· De kwaliteit en de lengte in bits van het wachtwoord wordt weergegeven:**Groen** is OK.

· **URL** is de weblink om toegang te krijgen tot de website met het inlogscherm. Deze links kunnen, bij aanpassing van de website, in de loop der tijd wijzigen.

· In het veld **Opmerkingen** kan van alles geplaatst worden wat relevant is voor deze nieuwe invoer.

· Eventueel kan een **Vervaldatum** worden geactiveerd waarbij dit record op de vervaldatum een rood kruis geeft. Dit kun je gebruiken om een signaal te krijgen om een wachtwoord te vervangen.



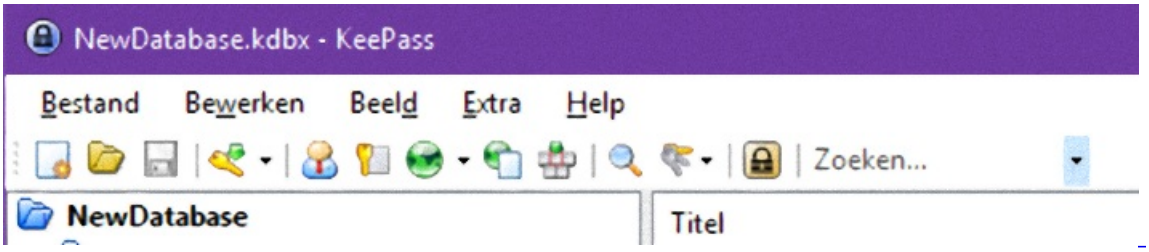
Er zijn nog meer tabs op het invoerscherm, daarbij is het tabblad**Auto-typen** interessant. Hierin kun je tekststrings wijzigen wanneer Auto-typen – het automatisch invoeren van gebruikersnaam en wachtwoord op het inlogscherm- niet goed werkt. Tevens kun je daar *'Auto-typen via twee kanalen aanvinken'* om het keyloggers lastiger te maken je inlogggevens te achterhalen.

Voor elk systeem of website kan op deze manier een record worden aangemaakt.

Als je na wijzigingen KeePass afsluit, dan krijg je vanzelf de vraag of je de wijzigingen wilt bewaren.

· **Invoer gebruiken**

Na heropenen van KeePass wordt een lijst van records getoond die je zelf hebt ingevoerd. In het zoekveld bovenin geef je een paar letters op van de website of het systeem waartoe je toegang wilt krijgen. Er verschijnt een lijst met records die aan die criteria voldoen. Klik eenmalig op het record met de gegevens die je zoekt, dan wordt dit record gemarkeerd.



Klik op het wereldbolletje, bovenin het scherm. De website die je in het record hebt ingevoerd wordt geopend met je standaard browser. Indien je met een andere browser wilt openen, dan kun je dat selecteren met het pijltje naast het wereldbolletje.

Voor het in één keer invoeren van je gebruikersnaam en wachtwoord, in een programma of de browser, kun je gebruik maken van de **Auto-typenknop**, dat is de knop bovenin, links naast het vergrootglas. Zorg eerst dat je muisaanwijzer in het veld staat van de gebruikersnaam als er meerdere invoervelden op het scherm staan.

Werkt dit niet, omdat de velden niet achter elkaar staan, dan kun je de tekststring wijzigen in het tabblad**Auto-typen**

of de volgende twee stappen als alternatief gebruiken:

Klik op de *persoon*, bovenin het scherm. De gebruikersnaam wordt gekopieerd naar het prikbord. Ga met de muis op het invoerveld staan voor de gebruikersnaam. **Enter Control+V** of **Rechtermuisknop -> Plakken**.

Klik op het sleuteltje, bovenin het scherm. Het wachtwoord wordt naar het prikbord gekopieerd, zonder dat het voor anderen zichtbaar is. Ga met de muis op het invoerveld staan voor het wachtwoord. **Enter Control+V** of **Rechtermuisknop -> Plakken**.

Klik op *Inloggen* op het scherm van het systeem waartoe je toegang wenst, als dit nog niet automatisch is gedaan.

Met **Control+L** of het slotje naast het zoekveld, sluit je de database af, maar niet de applicatie. Door op he**KeePass-icoon** te klikken kan de database met invoer van het wachtwoord weer geopend worden.

Tips

Het is van belang dat in noodgevallen het masterwachtwoord beschikbaar komt. Berg het op in een kluis of equivalent, zodat het voor je naasten beschikbaar is.

De toegang tot de Keepass-database kun je nog extra beveiligen door er ook een sleutelbestand aan te koppelen.

Voor het geval je nadere informatie wenst, heeft de KeePass-website uitgebreide Help- en FAQ-instructies; zie **http://keepass.info/help/base/index.html** (externe link)

Categorie
Handige Hulpen (Tools)
Veiligheid

Voor- en nadelen

Voordelen

- Gratis, open source, veilig, eigen beheer, multifunctioneel, multiplatform, uitbreidbaar.

Nadelen

- Vereist nauwkeurigheid en discipline van de gebuiker.

- Niet geheel waterdicht voor keyloggers; gebruik Auto-typen via twee kanalen om het risico te beperken.

Taal
Nederlands
Engels
Platform
Windows
Linux
macOS
Android

Installatie

Windows-installatie

KeePass is beschikbaar in een 1.x- en een 2.x-versie. We gaan uit van de 2.x-versie, daar die meer functionaliteit en bredere platformondersteuning biedt. Daarnaast is er een versie voor standaard installatie onder het Windows-besturingssysteem en een zogenoemde Portable-versie voor installatie op een USB-stick. Deze versie is voor als je geen installatierechten hebt op een systeem, zoals bij bedrijven.

- **De installatie op je systeem, met Installer, gaat als volgt:**

Ga naar: http://keepass.info/download.html (externe link)

KeePass-2.xx-Setup.exe verschijnt in je map **Downloads**.

Dubbelklik op **KeePass-2.xx-Setup.exe**.

Klik op **Ja** om te installeren -> Klik op **OK** voor *Nederlands*, Klik op **Ik accepteer de licentieovereenkomst** en **Volgende ->** Klik op **Volgende** bij *Doelmap* -> Klik op **Volgende** bij *Volledige installatie* -> Klik op **Volgende** bij *Selecteer extra taken*, maak je keuze voor *snelkoppelingen* -> Klik op **Installeren** bij *Voorbereiden van de installatie is gereed.*

KeePass wordt geïnstalleerd en gestart als op **Voltooien** wordt geklikt.

Klik op **Enable automatic update check.**

KeePass verschijnt met een leeg scherm.

Ga naar *File -> New ->*

Je krijgt hierbij de optie om een nieuwe database met de naam *NewDatabase.kdbx* in de map **Documenten** op te slaan.

Indien gewenst kun je de database een andere naam geven en een andere **locatie**/**map** uitzoeken.

Hierna krijg je de vraag naar het masterpassword voor de database. Kies hiervoor een sterk wachtwoord, dat je ook nog kunt onthouden. De kwaliteit van het wachtwoord verschijnt in *Estimated Quality.* **Groen** betekent dat het wachtwoord OK is.

Het wachtwoord moet herhaald worden in de regel eronder. Klik op **OK**.

Er zijn nog andere opties om toegang tot de database te krijgen, maar daar gaan we in deze uitleg niet op in.

Er volgt een scherm met de mogelijkheid om de Database-settings te wijzigen. Dat is niet nodig, klik op **OK**.

De database wordt getoond met twee voorbeelden, die later verwijderd kunnen worden.

Portable installatie

Steek een USB-stick in je systeem (capaciteit: ten minste 8 MB).

Ga naar: **http://keepass.info/download.html** (externe link).

Download de Professional Edition, KeePass 2.x Portable versie:

KeePass-2.xx.zip verschijnt in je map **Downloads**.

Open deze map met *Rechtermuisknop -> Open met Windows Verkenner.*

Sleep de getoonde inhoud naar je USB-stick.

Klik op *KeePass.exe*.

KeePass verschijnt met een leeg scherm, of met een inlogscherm als op het systeem een andere KeePass wordt gezien.

Bij het inlogscherm: klik op *Cancel*; dit roept een leeg KeePass-scherm op.

Ga naar *File -> New ->*

Je wordt gevraagd een nieuwe database met de naam **NewDatabase.kdbx** op je USB-stick op te slaan.

Indien gewenst kun je de database een andere naam geven.

Hierna krijg je de vraag naar het masterpassword voor de database. Kies hiervoor een sterk wachtwoord dat je ook nog kunt onthouden. De kwaliteit van het wachtwoord verschijnt in Estimated Quality. **Groen** betekent dat het wachtwoord OK is.

Het wachtwoord moet herhaald worden in de regel eronder. Klik op **OK**.

Er volgt een scherm met de mogelijkheid om Database-settings te wijzigen. Dat is niet nodig, klik op **OK**.

De database wordt getoond met twee voorbeelden, die later verwijderd kunnen worden.

Als je eerder op je systeem een KeePass-databasebestand hebt aangemaakt en gevuld, dan kun je dat, indien gewenst, ook kopiëren naar je USB-stick.

Maak je gebruik van een USB-stick met meerdere Portable apps en een menustructuur, dan kun je KeePass daar ook in opnemen.

De Nederlandse taal instellen

Ga naar **View -> Change Language …**

Klik op *Get more languages…*

http://keepass.info/translations.html (externe link) wordt geopend.

Zoek naar de regel met de taal **Dutch** en klik op de *Download knop 2.xx+*

KeePass-2.XX-Dutch.zip wordt gedownload en is terug te vinden in de map**Downloads**.

Open het bestand met *Rechter muisknop -> Openen met Windows Verkenner* en sleep het bestand **Dutch.lngx** naar:

1. C:\Program Files (x86)\KeePass Password Safe 2
2. of bij Portable naar je USB-schijf

Sluit KeePass af en start het weer op.

KeePass start nu op in het Nederlands.

Back-up instellen

Van deze belangrijke database is het vanzelfsprekend gewenst om continu een back-up beschikbaar te hebben. Om dit te realiseren is een plug-in beschikbaar.

Sluit KeePass af en open de KeePass-directory.

Ga naar: http://keepass.info/plugins.html (externe link).

Zoek naar **DataBaseBackup voor KeePass 2.x.**

Download de plug-in: het bestand **DataBaseBackup-2.xxx.zip** verschijnt in de map **Downloads**.

Open de zip met *Rechtermuisknop -> Openen met Windows Verkenner.*

Sleep het bestand **dbBackup.plgx** naar de KeePass-directory.

Start KeePass en voer het masterwachtwoord in.

Ga naar **Extra > BD Backup plug-in > Configure.**

Geef een back-up-locatie op bij **Destination**, klik op **Add,** klik op **OK**.

Dit kan een lokale back-up-schijf of NAS zijn, maar ook een Cloudservice zoals Dropbox of OneDrive.

Ga naar *T***ools > BD Backup plug-in > Backup DB NOW!**

Controleer of *Automatically Back DB* aangevinkt is.

In het vervolg zal automatisch een back-up gemaakt worden.

Opties:

KeePass in combinatie met Synology NAS Cloud.

Er zijn ook KeePass-apps beschikbaar voor iOS en Android. De KeePass-database moet dan beschikbaar komen voor deze apps, waarbij het KeePass-databasebeheer plaats vindt op de pc/laptop.

Hierbij moet ervoor gezorgd worden dat het KeePass-databasebestand niet in**Documenten** wordt geplaatst, maar in je **Synology Cloud Station Drive**.

Op je telefoon/tablet installeer je**DS Cloud** en de voor het apparaat geschikte Keepass-app.

Open **DS Cloud** op je telefoon/tablet en klik op het *<naam>.kdbx-bestand*. Er wordt gevraagd *Open met ….* Kies *Kopieer naar MiniKeePass (iOS)* of *KeePass2Android Offline (Android)*. De KeePass-app wordt geopend met de vraag om het databasewachtwoord.

Zodra dit is ingevoerd verschijnt de inhoud van de database zoals die op je pc is aangemaakt.

Bij wijziging van de KeePass-database op de pc zal op de telefoon en tablet de aangepaste KeePass weer gekoppeld moeten worden aan de KeePass-app.

Naast de (privé) **Synology Cloud** kunnen ook andere (publieke) Cloud-oplossingen gebruikt worden.

Prijs

Gratis

Veilige downloadpagina

http://keepass.info/download.html