

Eén sleutel voor alle wachtwoorden



Verander uw usb-stick in een wachtwoordkluis

Gebruikersnamen en wachtwoorden zijn bedoeld om u als uniek persoon te kunnen identificeren bij allerlei diensten, programma's en websites. Twee of drie moeilijk te raden wachtwoorden kunnen nog wel worden onthouden. Maar omdat we per persoon steeds meer wachtwoorden krijgen wordt het noodzakelijk om ze ergens veilig op te bergen. In dit artikel leest u hoe u met één wachtwoordmanager uw usb-stick omdoopt naar een echte wachtwoord-sleutel.

Steeds meer diensten en programma's maken gebruik van een persoonlijke identificatie en steeds meer systemen worden gekoppeld. Denk bij dit laatste bijvoorbeeld aan DigiD (www.digid.nl) van de overheid of aan uw bankgegevens bij online winkels. U hoeft geen genie te zijn om te weten dat dit ernstige veiligheidsrisico's met zich meebrengt en dat het nadelige financiële gevolgen kan hebben als uw gegevens in verkeerde handen vallen. Goede en unieke wachtwoorden voor alle plaatsen waar u zich dient te identificeren zijn essentieel, maar allesbehalve gebruiksvriendelijk.

Een goed wachtwoord bestaat uit hoofdletters, kleine letters, cijfers en het liefst ook speciale tekens. Uiteraard mag het woord dat u kiest niet in het woordenboek voorkomen en dient het zo lang mogelijk te zijn. Het is menselijk om voor meerdere diensten hetzelfde wachtwoord te gebruiken. Met zoveel inloggegevens wordt het immers bijna onmogelijk om altijd een uniek wachtwoord te kiezen, terwijl dat

laatste toch echt verstandig is. De ontbrekende schakel is een wachtwoordmanager om al die lastige wachtwoorden te beheren en automatisch voor u in te vullen.

KEEPPASS

In dit artikel gebruiken we het gratis opensource-programma KeePass. Deze software slaat logingegevens en wachtwoorden op in een beveiligde kluis. Het gebruikt hiervoor één van twee encryptie-algoritmes AES/Rijndael en TwoFish. Na het invoeren van uw inloggegevens kunt u met één hoofdwachtwoord toegang krijgen tot alle logins. Door KeePass te verplaatsen naar een usb-stick

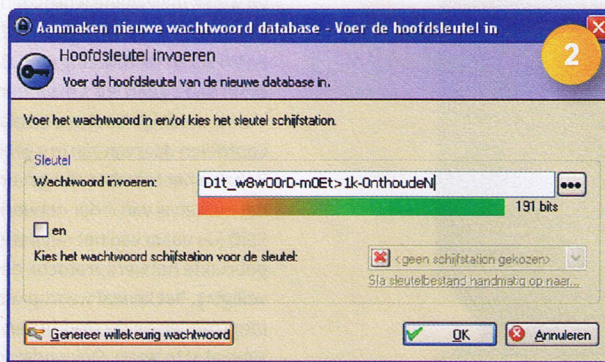
► Maak een nieuwe database aan en geef een hoofdwachtwoord op.

kunt u de wachtwoorden op iedere Windows-pc gebruiken. KeePass kan ook goede, sterke wachtwoorden genereren. Dit kunt u gebruiken voor het aanmaken van nieuwe wachtwoorden of om de wachtwoorden die u op dit moment gebruikt bij te werken. De gegenereerde wachtwoorden zijn complex en moeilijk te onthouden, maar onthouden hoeft ook niet. Na het volgen van het stappenplan doet KeePass dit namelijk voor u.

STAP 1 KEEPPASS INSTALLEREN

Ga naar de website van KeePass, klik op Downloads en Download Latest Stable Release for Win32. Download het bestand KeePass-1.04-Setup.exe. De maker heeft ook de broncode en een zip-versie beschikbaar gesteld, maar deze hebt u niet nodig. Ga nu naar de Translations-pagina op de website en download het bestand Dutch.zip. Start de installatie en accepteer de overeenkomst. Verder kunt u de overige opties ongewijzigd laten.

◀ Installeer KeePass naar de standaardmap C:\Program Files\KeePass Password Safe.



KeePass 1.04

FREEWARE

TAAL Nederlands

MEDIUM 894kB download

OS Windows 9x/Me/NT/2000/XP/2003/Vista

SYSTEEMEISEN 2MB hardeschijfruimte

MAKER Dominik Reichl

WEBSITE keepass.sourceforge.net

► Maak groepen aan in KeePass, om uw wachtwoorden overzichtelijk op te slaan.

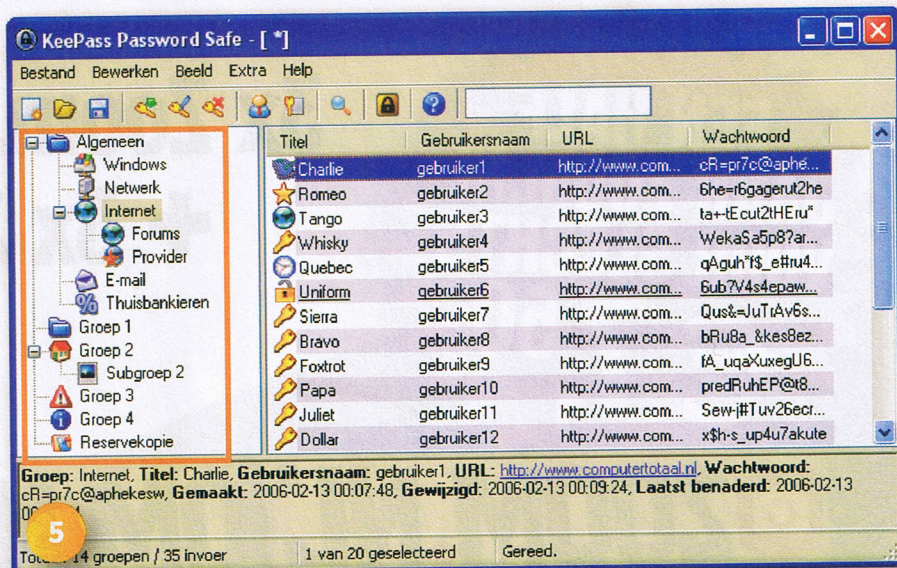
De software wordt geïnstalleerd in de map C:\Program Files\KeePass Password Safe (afbeelding 1). Open het bestand Dutch.zip en kopieer het bestand Dutch.lng naar de KeePass-map.

STAP 2 NIEUWE DATABASE EN HOOFDWACHTWOORD

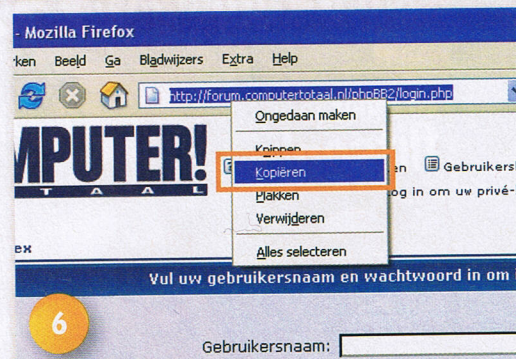
Start KeePass en ga naar het menu View / Change Language. Kies Dutch en herstart het programma. U kunt KeePass gebruiken om meerdere databases te beheren, bijvoorbeeld voor verschillende gebruikers. In dit artikel werken we met één database. Klik op het menu Bestand / Nieuwe database en geef een sterk wachtwoord op. Dat is de hoofdsleutel. De balk onder het invoerveld wordt langer en groener naarmate het wachtwoord sterker is (afbeelding 2). Klik eventueel op de knop Generer willekeurig wachtwoord om KeePass een zeer sterk wachtwoord te laten maken (zie Wachtwoord-Generator). Belangrijk is wel dat u de hoofdsleutel nog kunt onthouden, maar dat hij toch sterk genoeg is, omdat dit wachtwoord al uw andere wachtwoorden en belangrijke gegevens beveiligd! Bewaar de instellingen met OK. Voer het wachtwoord een tweede maal in en klik op OK. Pas als u KeePass voor de eerste keer afsluit zal het u vragen een locatie op te geven waar de wachtwoordkluis wordt opgeslagen.

EXTRA: WACHTWOORD-GENERATOR

Wilt u écht sterke wachtwoorden maken? Gebruik dan de Wachtwoord-Generator van KeePass (af-



beelding 3). U kunt kiezen uit negen opties die bepalen wat voor teken-reeksen er in het wachtwoord worden gebruikt. Geef de lengte op (standaard 16) en klik op het knopje met de drie blauwe bolletjes om het wachtwoord te tonen. Klik op de knop Genereren en gebruik muisbewegingen of typ willekeurige tekens als bron voor de toevallig gekozen tekens in het wachtwoord (afbeelding 4). Klik op Accepteren als u tevreden bent over het wachtwoord. Let op: deze wachtwoorden zijn extreem complex en daardoor moeilijk te onthouden.



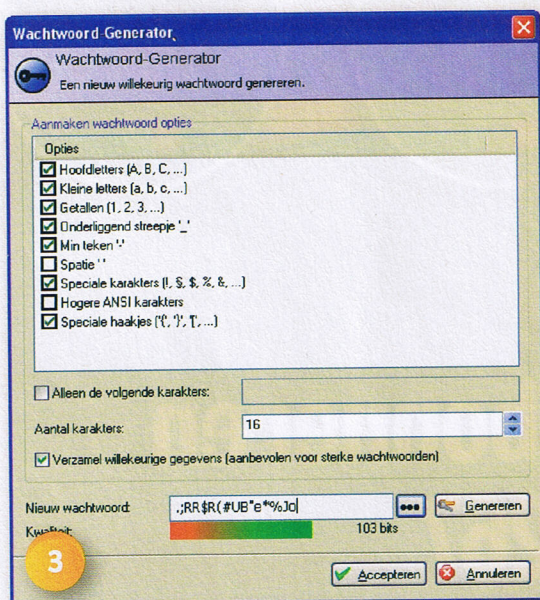
▲ Kopieer het adres van de loginpagina naar het Klembord

subgroepen Windows, Netwerk, Internet, E-mail en Thuisbankieren. Maar u kunt nog extra categorieën aanmaken, zoals Forums, Online Winkels, enzovoort. De groepen zijn eenvoudig aan te maken via opties in het menu Bewerken.

STAP 4 ADRES LOGINPAGINA ZOEKEN

Om later automatisch wachtwoordgegevens in te laten vullen tijdens het surfen, hebben we het adres van de aanmeldpagina nodig van de diensten die u gebruikt. Veel websites bieden de mogelijkheid om automatisch ingelogd te blijven. Staat u ergens automatisch ingelogd, dan moet u

zich eerst afmelden (uitloggen) om de automatische aanmeldprocedure goed te doorlopen. Open uw browser en ga naar de inlogpagina van de website die u wilt toevoegen - in ons voorbeeld is dit het forum van Computer!Totaal. Kopieer het adres van de inlogpagina, via de rechtermuistoets, naar uw klembord (afbeelding 6).

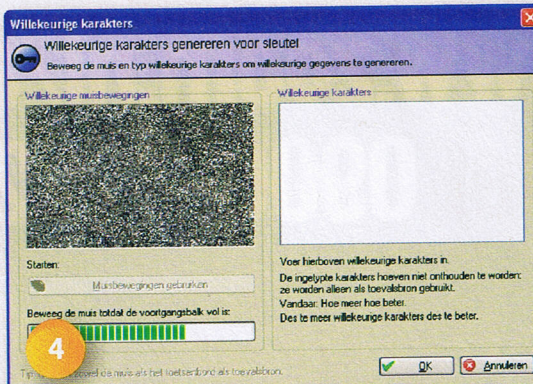


▲ De sterkste wachtwoorden zijn bijna onmogelijk te onthouden.

► Muisbewegingen of willekeurige tekens helpen het wachtwoord nog sterker te maken.

STAP 3 GROEPEN AANMAKEN

KeePass kan alle soorten gegevens veilig bewaren, van pincodes en creditcardnummers tot inloginformatie van websites. Het gevolg is dat u na verloop van tijd kunt verzanden in een onoverzichtelijke brei gegevens. Om dit te voorkomen raden we aan om direct wachtwoordgroepen (afbeelding 5) aan te maken. Standaard bevat een KeePass-database al een wachtwoordgroep Algemeen, met daarin de



WACHTWOORDEN IN INTERNET EXPLORER: WISSEN!

Tijdens het browsen en het invullen van gegevens op websites biedt Internet Explorer de mogelijkheid om uw gegevens te bewaren. Deze worden vervolgens opgeslagen in Internet Explorer Protected Storage. Als u denkt dat uw gegevens hier veilig zijn, hebt u het helemaal mis. Iedereen die is ingelogd op uw pc kan uw wachtwoorden moeiteloos uitlezen. U kunt zelf eenvoudig de proef op de som nemen met het programma Protected Storage PassView van Nirsoft (www.nirsoft.net). Bent u geschrokken? Het is dus verstandig om de lijst in Internet Explorer Protected Storage te wissen en te voorkomen dat Internet Explorer hier in de toekomst weer gegevens aan toevoegt. Start Internet Explorer en klik in het menu Extra op Internet opties. Ga naar het tabblad Inhoud en klik op de knop AutoAanvullen. Laat in dit scherm alleen een vinkje staan bij Webadressen en verwijder de overige vinkjes. Klik achtereenvolgens op de knop Formulieren wissen en Wachtwoorden wissen om de gegevens uit Windows Protected Storage te verwijderen. Bevestig de instellingen met OK.



▲ Wis uw wachtwoorden in Internet Explorer en zorg dat de browser deze in de toekomst niet meer onthoudt.

STAP 5 WEBSITES EN WACHTWOORDEN TOEVOEGEN

Ga terug naar KeePass en navigeer naar de groep waar de nieuwe wachtwoordkaart onder valt: in ons voorbeeld Forums. Klik op deze groep en kies in het menu Bewerken voor Invoer toevoegen. Er wordt een nieuwe wachtwoordkaart aangemaakt. De belangrijkste gegevens van de wachtwoordkaart zijn: gebruikersnaam, URL van de loginpagina, en het wachtwoord (afbeelding 7). Ga in het URL-veld staan en plak via Ctrl+V of via de rechtermuistoets het adres van de loginpa-

gina. Geef in het Titel-veld een titel voor de wachtwoordkaart die u snel kunt herkennen.

KeePass vult al automatisch een sterk wachtwoord in (druk op de knop met de drie bolletjes om dit te tonen). In principe haalt u die weg en vult u hier uw bestaande wachtwoord in. Bevestig de wijzigingen met OK.

Herhaal deze en de vorige stap als u nu direct andere login-gegevens wilt invoeren in KeePass, maar dit kan natuurlijk ook later. Sla de gegevens op met het floppy-pictogram of via menu Bestand / Database Opslaan.

STAP 6 GEMAKKELIJK INLOGGEN

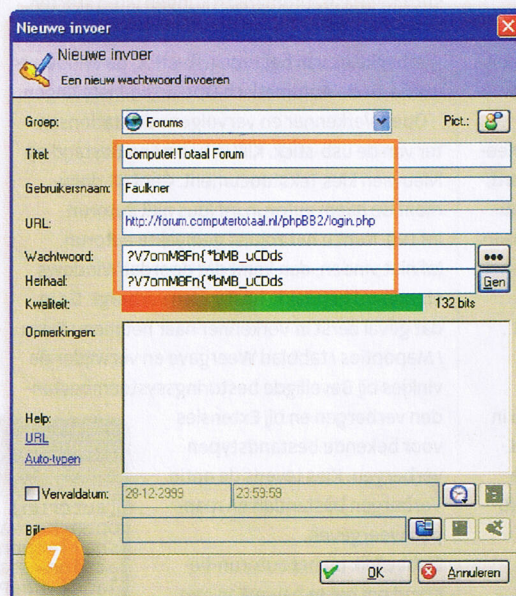
De login-gegevens die u in KeePass bewaart kunnen op meerdere manieren worden gebruikt. Als

u met rechts op een wachtwoordkaart klikt en de optie Open URL(s) selecteert, wordt de loginpagina van de betreffende website geopend. Via twee andere opties voor uw gebruikersnaam en wachtwoord kopieert u deze gegevens tijdelijk naar het klembord (afbeelding 8). Vervolgens kunt u de gebruikersnaam en het wachtwoord weer op de benodigde velden in uw webbrowser plakken. U kunt deze gegevens ook slepen van het KeePass-venster naar de loginpagina.

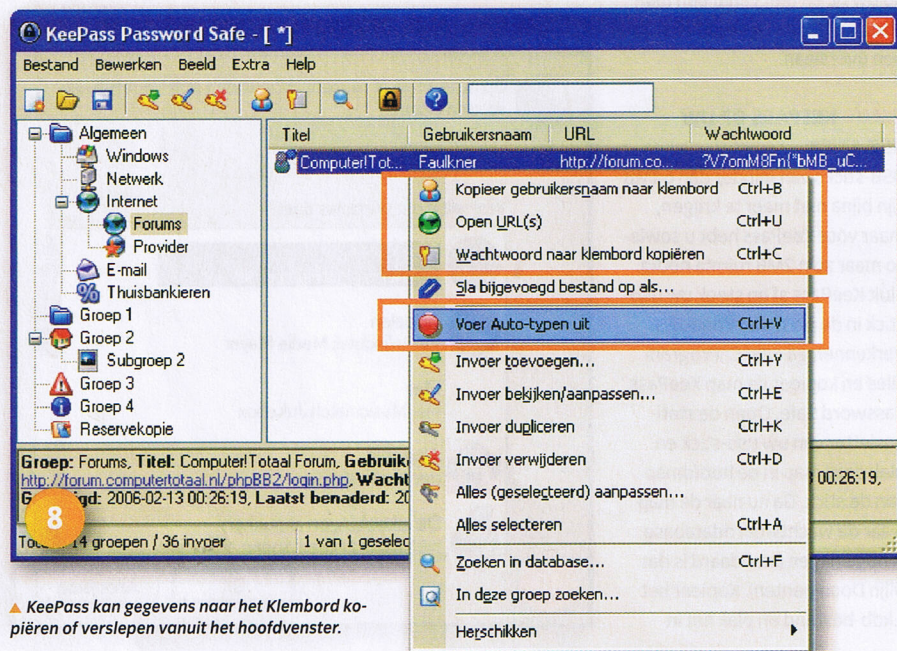
Er is nog een andere manier om in te loggen: ga na de optie Open URL(s), in het veld gebruikersnaam staan op de loginpagina, ga met Alt+Tab terug naar het KeePass-venster, klik weer met rechts op de wachtwoordkaart en kies de optie Voer Auto-typen Uit. KeePass emuleert nu de toetsaanslagen.

EXTRA: AANPASSEN TOETSEMULATIE

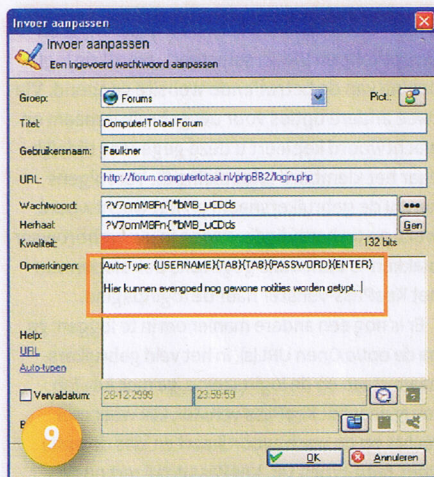
De functie Auto-typen emuleert standaard de toetsaanslagen: {USERNAME}{TAB}{PASSWORD}{ENTER}. KeePass zal eerst de gebruikersnaam intikken, dan een Tab-commando geven zodat de cursor naar het volgende invulveld springt en afsluiten met een Enter. Dit gaat vaak goed, maar voor sommige websites is het nodig meerdere tabs te geven. Dit kunt u per wachtwoordkaart instellen in het Opmerkingen-veld. Stel dat het nodig is om na de gebruikersnaam twee tabs te geven, dan typt u een extra tabcode (afbeelding 9). In het helpbestand van KeePass staat een lijst met alle codes die het ondersteunt. Daar staat ook uitgelegd hoe u met de toetscombinatie Ctrl+Alt+Tab automatisch kunt inloggen.



▲ Geef alle login-gegevens op die nodig zijn om u aan te melden.



▲ KeePass kan gegevens naar het Klembord kopiëren of verslepen vanuit het hoofdenster.



STAP 7 INLOGGEN MET 1 KLIK (OPTIONEEL)

Om het automatisch invullen van wachtwoorden nog eenvoudiger te maken, kunt u een aparte plug-in voor KeePass downloaden: KeeForm. Nadat u de twee bestanden KeeForm.exe en KeePrg2.exe naar de KeePass-map hebt gekopieerd, kunt u de wachtwoordkaarten verder automatiseren. In plaats van de link naar de inlogpagina in het URL-veld te plakken, geeft u bijvoorbeeld het commando

```
cmd://KeeForm http://forum.computertotaal.nl/phpBB2/login.php {USERNAME} {PASSWORD} {ENTER}
```

Sla de wijzigingen op met OK en dubbelklik nu in het KeePass-hoofdvenster op de link in de URL-kolom. De browser wordt geopend, de pagina geladen en de gegevens ingevuld. Met één dubbelklik bent u ingelogd.

<http://keepass.sourceforge.net/plugins.php#formfiller>

Opmerking: als u KeePass alleen wilt gebruiken op uw pc en niet vanaf een usb-stick, kunt u de resterende stappen overslaan.

STAP 8 KEEPASS OP UW USB-STICK

USB-sticks van minder dan 64MB zijn bijna niet meer te krijgen, maar voor KeePass hebt u sowieso maar zo'n 2MB ruimte nodig. Sluit KeePass af en steek uw usb-stick in de pc. Open Windows Verkenner, ga naar C:\Program Files en kopieer de map KeePass Password Safe. Open de stationsletter van uw usb-stick en plak deze map in de hoofdmap van de stick. Ga nu naar de map waar de wachtwoorddatabase is opgeslagen (standaard is dat Mijn Documenten). Kopieer het *.kdb-bestand en plak het in

◀ Met speciale codes emuleert KeePass toetsaanslagen.

KeePass-map op de usb-stick.

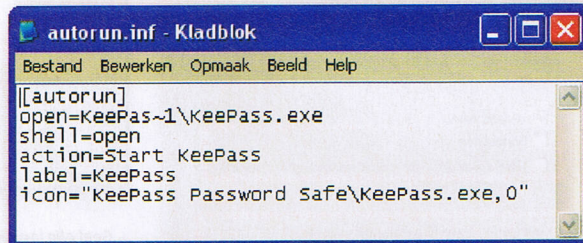
Dubbelklik op het bestand KeePass.exe. Als u nu inlogt, zal het programma de database vanaf de laatst bekende locatie proberen te starten. Klik daarom op Annuleren, ga naar het menu Bestand / Database Openen en open de database vanaf de usb-stick.

Eventueel kunt u KeePass nu van uw pc deinstalleren, maar dat hoeft niet.

STAP 9 USB-STICK AUTOMATISCH LATEN STARTEN

Het mooiste is als we na het plaatsen van de usb-stick KeePass automatisch kunnen laten starten. Helaas werkt deze methode niet op alle pc's: het is afhankelijk van het type usb-stick, de Windows-versie en de Automatisch Opstarten-instellingen.

Open Verkenner en vervolgens de stationsletter van de usb-stick. Klik in het menu Bestand op Nieuw en kies Tekstdocument. Geef dit document de naam autorun.inf (dus niet autorun.inf.txt). Kunt u het zojuist gemaakte autorun.inf niet vinden, dan komt dat doordat Windows standaard bepaalde bestanden verbergt. Ga in dat geval eerst in Verkenner naar het menu Extra / Mapopties / tabblad Weergave en verwijder de vinkjes bij Beveiligde besturingssysteembestanden verbergen en bij Extensies voor bekende bestandstypen verbergen. Kies tevens de optie Verborgen bestanden en mappen weergeven. Dubbelklik op het autorun-bestand om het te bewerken met Kladblok. Geef de volgende regels op:



```
[autorun]
open=KeePas~1\KeePass.exe
shell=open
action=Start KeePass
```

Sluit Kladblok af en bewaar het bestand autorun.inf. Afhankelijk van eerdergenoemde beperkingen zal bij het plaatsen van de usb-stick een dialoogvenster verschijnen, waarin u de mogelijkheid krijgt om KeePass te starten (afbeelding 10). Na het opgeven van uw hoofdsleutel krijgt u toegang tot al uw wachtwoorden.

TOT SLOT

Na het volgen van dit stappenplan kunt u uw usb-stick letterlijk gebruiken als een wachtwoord-sleutel. Dit kan op uw eigen pc, maar ook bij pc's van anderen en op het werk (als uw systeembeheerder dit toestaat). Nooit meer wachtwoorden onthouden: met één hoofdwachtwoord hebt u toegang tot al uw digitale registraties.

Eén ding moet u goed onthouden: sluit KeePass af voordat u de usb-stick uit de pc trekt. Hiermee voorkomt u niet alleen dat het programma vastloopt, maar ook dat uw gegevens op een andere pc open blijven staan. Verder is het verstandig om periodiek een backup te maken van het kluisbestand op uw usb-stick. Mocht u de stick verliezen dan is de data weliswaar beveiligd en voor derden onleesbaar, maar zonder backup bent u wel uw gegevens kwijt. ☹



◀ KeePass start automatisch, zodra de usb-stick in de pc wordt gestoken.

ALTERNATIEVEN

KeePass is een prima programma, maar helemaal perfect is het niet. Het automatisch inloggen is een beetje omslachtig in te stellen. Gebruiksvriendelijker is RoboForm (27 euro) of Pass2Go speciaal voor usb-sticks (36 euro). Evaluatieversies kunt u downloaden via www.roboform.com.

Een alternatief gratis programma is ID Manager (www.woodensoldier.info/en), dat minder encryptiemogelijkheden biedt maar wel kan worden bediend vanaf een pictogram in het systeemvak. Een uitgebreid stappenplan voor deze software vindt u in het artikelenforum van CIT.