May it be a bit more?

André Reinink

(Steenkolenengels voor ‘mag het een beetje meer zijn?’)

De USB-stick[1,2,3] is niet meer wat het geweest is.
Je zou gerust kunnen stellen dat de USB-stick van tegenwoordig ‘a bit more’ is. De bekendste functie is natuurlijk gegevensopslag. Maar er zijn meer mogelijkheden en functies. Maar wat zijn die dan?

Kees van der Vlies gaf een mooie voorzet in SoftwareBus nummer 6 van 2020. Een inkoppertje, een 1-2’tje of ga ik toch maar voor het ouderwetse veldwerk?

Ik had een idee…

Ik weet, en u als lezer ook, dat je met een USB-stick veel meer kunt doen dan er bestanden op archiveren. Je kunt er portable (draagbare) programma’s op zetten. Je kunt de stick voorzien van een besturingssysteem, je kunt een stick partitioneren, je kunt je wachtwoorden er op zetten, je kunt het als back-up medium gebruiken en je kunt een stick ook versleutelen. En misschien vergeet ik nog wel iets.

Eerst even iets over USB-sticks in het algemeen.
Ik zou er een hele SoftwareBus mee kunnen vullen. Er zijn zoveel soorten USB-sticks dat je als gebruiker voor het gemak vaak kiest voor een stick die in de aanbieding is. Lekker groot wat data betreft en handzaam in het gebruik.

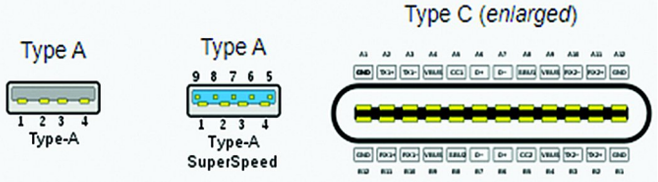
Ze zijn er met een afsluitdop, met een afsluitschuif of een ‘retractable’ uitvoering waarbij de USB-aansluiting van de stick naar binnen schuift. Dan hebben we nog verschillende kleuren en ontelbare vormen. Voor een handvol euro’s heb je al een leuk stickie tot je beschikking. Mocht je er een gaan aanschaffen neem dan even de tijd om de eigenschappen vooraf te bekijken[4].

Welke USB-versie?

Het begon in 1996 met USB 1.1. Daarna volgden 2.0, 3.0, 3.1, 3.2. Versie 4.0 is aangekondigd maar heb ik nog niet gezien.

Welke connector?

Tot nu toe was de USB-A connector de meest gebruikte. Steeds vaker zie je de USB-C connector toegepast.



En natuurlijk heeft Apple haar lightningaansluiting. Waarschijnlijk heb jij thuis meerdere varianten. Kies voor een uitvoering die qua gebruik het beste aansluit op je hardware. Er zijn ook verloopkabels of adapters. En er zijn USB-sticks met een dubbele connector, bijvoorbeeld USB-A aan de ene kant en USB-C aan de andere kant.

Opmerking: de kleuren van een connector zijn niet genormeerd. Een blauwe connector zie je vaak bij USB 3.0, maar een blauwe kleur is geen USB 3.0 garantie.

Je verzamelt heel wat USB-achtigen in de loop der jaren...

Gewoon of OTG?

Een ‘On The Go USB-stick’ kan makkelijk zijn. Bijvoorbeeld om te gebruiken in combinatie met een mobiele telefoon. Het opslagmedium zorgt dan voor extra geheugencapaciteit en het geeft je de mogelijkheid om bestanden uit te wisselen. Soms krijg je bij de aanschaf van een stick een ‘On The Go’-adapter gratis meegeleverd.

Beveiligd of onbeveiligd?

Het gros van de gebruikers beveiligt zijn of haar USB-stick niet. Eenieder die een stick in bezit heeft heeft toegang tot de bestanden op de ‘schijf’. Sommige fabrikanten leveren software mee om de schijf te versleutelen, heel handig. Maar in 9 van de 10 gevallen gaat het om Windows compatibele software. Niet voor iedereen handig. Vaak wordt daarmee dan de stick of een gedeelte ervan omgetoverd tot een beveiligd gebied. Tegenwoordig kun je ook encryptiesoftware van het besturingssysteem inzetten. Windows heeft Bitlocker, Linux heeft Dislocker, macOS heeft File Vault. En natuurlijk zijn ze niet helemaal of helemaal niet compatibel.
Als je veiligheid belangrijk vindt zou je beter kunnen kiezen voor een versleutelde stick, al dan niet met een geïntegreerd numeriek of touchscreen toetsenbord. Voor gebruik moet je eerst een pincode intoetsen, pas daarna krijg je toegang tot de gegevens. Meermaals de verkeerde pincode intoetsen zal leiden tot een geblokkeerde USB-stick.

Via de fabrikantsoftware zijn er dan mogelijkheden om de stick te ontgrendelen. We praten dan over sticks met bijvoorbeeld Military Grade Encryption[5,6]. Prijsindicatie: 32GB stick voor een prijs van 100 euro.

Tijdens mijn speurtocht zag ik ook een Chinese Military Grade Encrypted USB-stick. In de handleiding stond een standaard pincode voor alle USB-sticks van hetzelfde merk om deze te ontgrendelen. Lees je dus goed in voordat je in de buidel tast. Als je altijd met hetzelfde besturingssysteem werkt is het goedkoper en veilig genoeg maar om Bitlocker, Disclocker of File Vault te gebruiken.
Bedenk dat je ook een dubbele beveiliging kunt inzetten: als eerste de stick zelf beveiligen en als tweede ook de bestanden beveiligen. Verderop in dit artikel meer over een USB-stick met versleutelde bestanden.

Snelheid

Helaas zie ik vaak advertenties waarbij een flash-drive aangeprezen wordt om zijn hoge snelheid. Bijna altijd bedoelt men dan de leessnelheid. Persoonlijk vind ik de schrijfsnelheid belangrijker dan de leessnelheid. De maximaal haalbare snelheden zijn altijd afhankelijk van de hardware van de flashdrive in combinatie met de hardware van de pc.
Een USB 3.0 stick aangesloten op een USB 2.0 poort van een computer is langzamer dan dezelfde stick op een USB 3.0 poort van een computer. En andersom: een USB 2.0 stick werkt niet sneller op een pc met USB 3.0 poort.
Theoretische snelheden:
USB 1.1 = 1,5 MB/s
USB 2.0 = 60 MB/s
USB 3.0 = 625 MB/s (SuperSpeed)
USB 3.1 = 1,25 GB/s (SuperSpeed+)
USB 3.2 = 2,5 GB/s (SuperSpeed+)
USB 4.0 = 40 GB/s (SuperSpeed+, Thunderbolt 3 en 4)

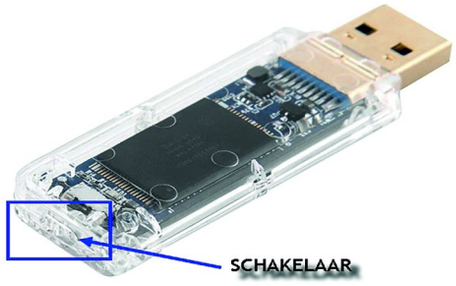
Tegenwoordig is USB 3.0 al een ‘no budget’ aanschaf. En als je zo’n stick koopt met een schrijfsnelheid van 30 MB/s of meer is dat zeker niet langzaam te noemen.
Tip: wil je snelheden van je eigen USB-stick meten en/of vergelijken dan is Nirsoft’s USBDeview[7] een aanrader.
Ik gebruik het om USB-sticks te testen, maar ook om externe harde schijven te testen. Verderop in dit artikel kom ik hier nog op terug.

Een USB-stick partitioneren

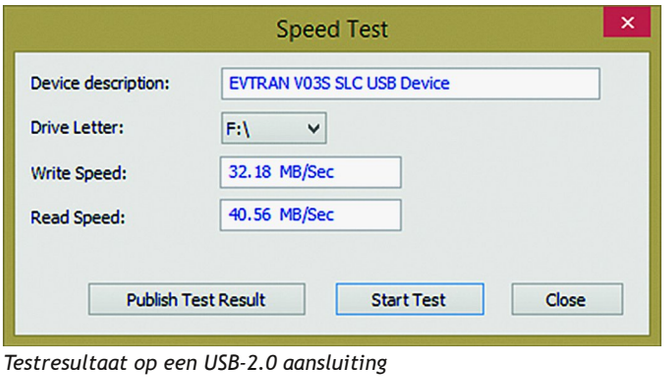
Waarom worden USB-sticks (bijna) nooit gepartitioneerd? Onnodig? Lastig? Je zou een USB-stick kunnen gebruiken om op verschillende pc’s te gebruiken of met verschillende besturingssystemen. Een partitie voor Windows en een partitie voor Linux of macOS. Je kunt ook partities indelen op basis van functioneel gebruik: een partitie voor privédocumenten, een zakelijke partitie of een partitie voor muziekbestanden.
Partitioneren onder Windows kan met ‘Diskmanagement’ of via de de commandline met ‘diskmgmt.msc’ of ‘Diskpart’8.
In Linux met ‘GParted’ of via de commandline met ‘fdisk’ en ‘mkfs’[9]. En op een macOS systeem met ‘disk Utitlity’10. Misschien is een gepartioneerde USB-stick iets voor jou?

USB-stick met live besturingssysteem – deel 1

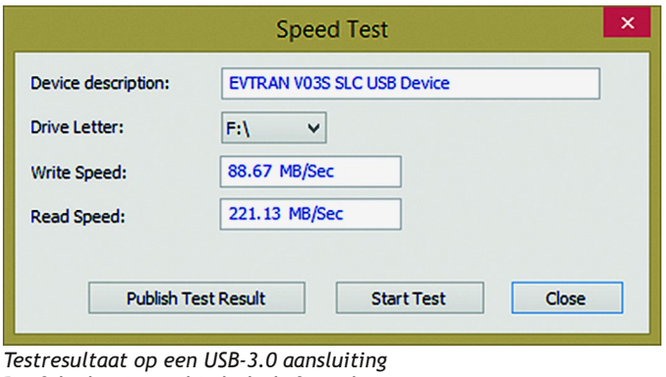
Je kunt een stick voorzien van een live besturingssysteem. Daarmee heb je dan de mogelijkheid een ‘eigen’ besturingssysteem te gebruiken op een systeem dat de USB-stick en software ondersteunt. Je hebt als het ware een pc in je broekzak. Als je zeker wilt weten dat er via een ‘vreemde’ pc niet op je USB-disk wordt geschreven (virus!) kun je er een kopen met een schakelaar die schrijven op de stick onmogelijk maakt. Ik probeerde het uit met een live-versie van Linux Manjaro en ondervond geen problemen.



Om de test nog interessanter voor mijzelf te maken kocht ik een USB-stick die niet alleen een schakelaar aan boord had, maar ook met een Single Level Cell was uitgevoerd. SLC will zeggen: 1 bit geheugenopslag per cel. Dit in tegenstelling tot Multi Level Cell: 2 bits per cel. Een SLC is sneller en energiezuiniger. Helaas zijn SLC USB-sticks ook een stuk duurder. Voor niets gaat de zon op natuurlijk.



Testresultaat op een USB-2.0 aansluiting



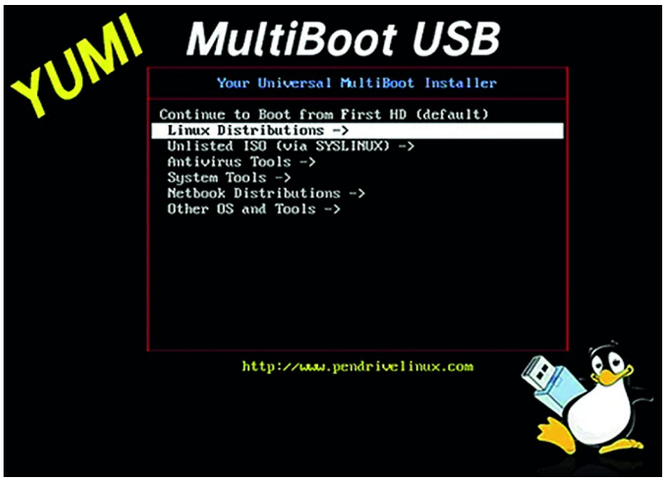
Testresultaat op een USB-3.0 aansluiting
De fabrikant maakt de beloften dus waar.

USB-stick met live besturingssysteem – deel 2

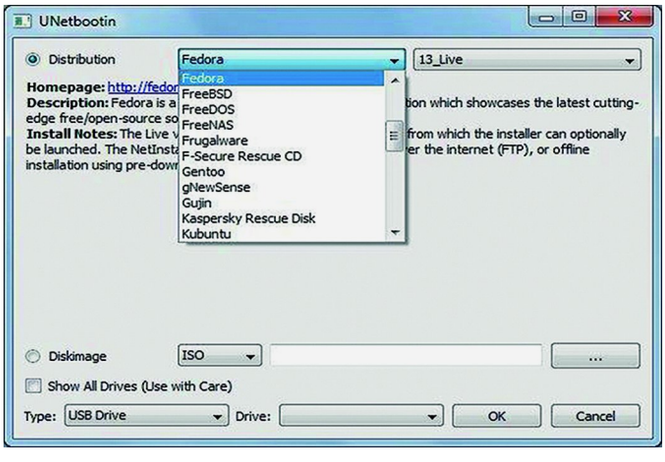
Er zijn legio methoden om een USB-stick van een live besturingssysteem te voorzien. Ik wil eerst een paar bekende tools kort bespreken.

Yumi[11] (Windows): Your Universal Multiboot Installer.
Je download de software en ‘prepareert’ de USB-stick met de software. Er is een ‘legacy’-uitvoering, dat betekent booten via het BIOS. En er is ook een UEFI-uitvoering, dat betekent booten via UEFI of BIOS. De software kan een reeds

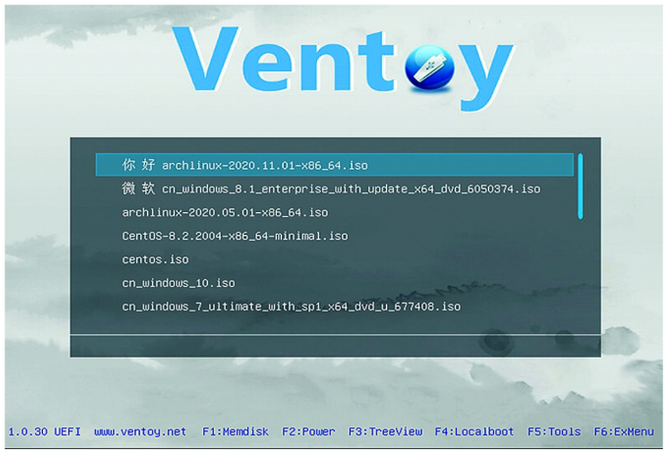
gedownload besturingssysteem op de USB-disk installeren. Dat kan een Linux-systeem zijn of een Windows-systeem. Daarnaast zijn er legio andere ‘gereedschappen’ op de stick te zetten. Yumi kan meerdere besturingssystemen bevatten. De grootte van de stick begrenst je mogelijkheden. Yumi zorgt tevens voor een geordend menu op je stick.



UNetbootin[12] **(Windows, macOS, Linux)**
Deze tool werkt in principe hetzelfde als Yumi.
Software downloaden, besturingssysteem downloaden en installeren maar. Net als Yumi kun je je stick volproppen met diverse besturingssystemen. Ik heb sticks gezien met meer dan 10 systemen aan boord. Wat misschien nog interessanter is: je kunt op zo’n multi-bootstick natuurlijk ook diagnosesoftware zetten. Of reparatiesoftware. Of een up-to-date virusscanner. Of, nou ja, vul het zelf maar in. De interface van UNetbootin ziet er iets gelikter uit dan die van Yumi.



Ventoy[13] is misschien een minder bekend stukje gereedschap (Windows en Linux): ‘A New Bootable USB Solution’.



Ventoy beweert meer dan 720 verschillende images te kunnen verwerken. Van alle denkbare images hebben ze op hun website aangegeven of deze compatibel zijn inclusief de verschillende versiestanden.
In tegenstelling tot Yumi en UNetbootin is het met de gepreppareerde USB-stick niet de bedoeling om er live systemen op te installeren, maar kopieer je simpelweg het ISO-bestand op de stick. Hoe makkelijk kan het zijn?

Een USB-stick beveiligen en versleutelen.

Bij het lezen van het artikel van Kees van der Vlies herinnerde ik me dat ik al eens eerder een poging had gedaan om een ‘Multi OS Encrypted USB-Stick’ te maken. Lang geleden probeerde ik dat met **TrueCrypt**[13].
Later werd TrueCrypt qua naam aangepast in **VeraCrypt**[14]

Aan die naamwisseling hing/hangt een luchtje. Bozetongen beweren dat de makers van TrueCrypt gedwongen werden een ‘backdoor’ in de software te programmeren. Toen men dat weigerde werd het VeraCrypt. Althans zo wil het verhaal.

De eisen die ik mezelf had opgelegd waren:
- portable, geen software op het gastsysteem
- geschikt voor meerdere besturingssystemen
- te gebruiken zonder beheerdersrechten

VeraCrypt is weliswaar op meerdere besturingssystemen bruikbaar, maar heeft software op het gastsysteem nodig en ook nog eens beheerdersrechten.
Uiteindelijk kwam ik uit bij 3 mogelijke kandidaten:
- Securstick (Windows, Linux, macOS)
- Boxcryptor (Windows, Linux, macOS, Android, iOS)
- Cryptomator (Windows, Linux, macOS, Android, iOS)

Securstick[15] Mijn eerste testen met Securstick liepen op niets uit. Het leek allemaal zo simpel. Securstick heeft geen beheerdersrechten nodig en draait op de belangrijkste besturingssystemen. Software op de stick zetten (op andere schijven kan ook), een sterk wachtwoord configureren en klaar. Securstick maakt een beveiligd gebied aan op de schijf en daarin kun je de te beveiligen bestanden archiveren. Het beveiligde gebied kun je benaderen via een WebDAV-verbinding. Dat klinkt ouderwets en vreemd, maar in de praktijk valt het reuze mee. Toen mijn test op niets uitliep (ik kon niet bij mijn beveiligd gebied) heb ik een collega eens gevraagd het thuis te proberen. Hij had onder Windows en Linux geen probleem ondervonden. Ik heb toen de maker van de software benaderd en hem het probleem voorgelegd. Eerste reactie: probeer het volgende eens uit en laat me de resultaten weten. Dat leverde niets op. Uiteindelijk bleek dat de naam van het Windows gebruikersaccount het probleem was. Gebruiker ‘André’ is met een accent op de ‘e’ en daar had de maker geen rekening mee gehouden. André en Andre is niet hetzelfde. Hij paste de software aan en daarna werkte alles zoals het hoort. Als je niet opziet tegen een spartaanse interface, dan is Securstick misschien iets voor jou. Het beveiligde gebied (eigenlijk een bestand) kan ook met een extern programma geopend worden, dus zonder de WebDAV-interface. Als je maar beschikt over het wachtwoord natuurlijk. De download is nog geen 400 kB groot.

Boxcryptor[16] heeft een heel andere, modernere interface. Op de website staat alleen de link naar de standaardversie. De link naar de portable versie[17] is een beetje verstopt, maar is er wel. De download, een gecomprimeerd bestand, is een kleine 200 MB groot. Je pakt het bestand uit op een USB-stick. Daarna start je het programma. Je hoeft geen account aan te maken bij Boxcryptor. Rechtsboven in de interface vind je een menuoptie om een 'local account' te gebruiken.
Om met Boxcryptor te kunnen werken moet je een sleutelbestand aanmaken met extensie: .bckey. Het programma leidt je door deze procedure heen. Boxcryptor gaat er echter vanuit dat je gebruik gaat maken van een cloudopslag. Daarvoor heeft de software zo'n 20 bekende clouddiensten voorgeconfigureerd. Als je voor een lokaal account hebt gekozen krijg je toch het scherm met de clouddiensten te zien, met als laatste een icoon voor een lokaal account. Daarna kun je een map aanmaken voor te beveiligen bestanden. Daarin plaats je de te beveiligen bestanden. Deze krijgen na versleutelen de extensie 'bc'. Het werkt allemaal redelijk rechttoe rechtaan. De versleutelde bestanden blijven, ook al zijn ze versleuteld, gewoon zichtbaar.

Als laatste wil ik **Cryptomator**[18] voorstellen. De standaardversie kun je op de reguliere site downloaden, maar er is ook een portable versie die op een andere site aangeboden wordt. De portable versie[19] is een kleine 50 MB groot. De download pak je uit naar een USB-stick. Vervolgens start je het programma. Daarna wordt er via een duidelijke procedure een aantal zaken ingesteld. Er moet een beveiligde map geconfigureerd worden. Deze map noemt Cryptomator een 'Vault' oftewel een kluis.
Standaard stelt Crypromator een map op het gastsysteem voor. Deze pas je aan naar een map op de USB-stick. Natuurlijk moet je ook een wachtwoord instellen. Cryptomator biedt ook aan een herstelsleutel te maken. Vervolgens, waar heb ik dat eerder gezien, maakt Cryptomator een WebDAV-verbinding aan. Bestanden kun je via een WebDAV-verbinding en een bestandsverkenner 'uploaden'. Bestanden worden versleuteld met een automatische, willekeurig gegenereerde naam.
Kortom: drie programma's die uiteindelijk allemaal zo ongeveer hetzelfde doen: bestanden versleutelen. Probeer ze eens uit en kijk of er een bij zit die je goed kunt gebruiken.
Ik kan me voorstellen dat je denkt: misschien is een versleutelde USB-stick wel een mooie oplossing om mijn wachtwoorden op te slaan.

In de afgelopen jaren is er het nodige geschreven over wachtwoordbeheerders. Maar met zo'n superbeveiligde stick heb je toch geen wachtwoordbeheerder nodig? Die keuze laat ik graag aan de lezer over.
Ik wil nog wel graag een tip op het gebied van wachtwoorden doorgeven. Je zou een wachtwoord kunnen 'opknippen'. Stel dat een wachtwoord als volgt is gedefinieerd:
[applicatiegerelateerd_deel][universeel_geheim_deel]
Voor het inloggen op de site van **Compuser.nl** zou dat bijvoorbeeld kunnen zijn:
[sresupmocroovnelekitrafjirhcski][compusers_is_it!]
Alleen het applicatiegerelateerde deel zet je in het bestand met de wachtwoorden. Het universele deel moet je onthouden. Het voordeel is dat je op een versleutelde stick een simpel wachtwoordbestand kunt beheren. Het enige wat je moet doen is het universele deel goed onthouden.
Een groot voordeel is, vind ik, dat als een ander beschikt over jouw wachtwoorden hij/zij nooit de beschikking heeft over de volledige wachtwoorden. Ik weet dat er nog veel meer mogelijkheden zijn om goed met wachtwoorden om te gaan, maar ik vond het de moeite waarde deze methode[20] in dit artikel te melden.

Uiteindelijk is het natuurlijk je eigen verantwoordelijkheid om op de juiste, en vooral veilige, manier om te gaan met wachtwoorden.

Conclusie

Heeft de USB-stick zijn langste tijd gehad? Of moet het beste nog komen? Als iedereen alles online bewaart, het besturingssysteem van de toekomst een cloudplatform is, iedereen z'n wachtwoorden elders bewaart, ja dan heeft de traditionele USB-stick zijn beste tijd gehad.
Maar voorlopig blijven we de USB-stick gebruiken!
Waarom zelf niet eens aan de slag gaan met een USB-stick aan de hand van dit artikel?
Ik wens iedereen die daarvoor een stick ter hand neemt veel testplezier!

Links:

1 https://en.wikipedia.org/wiki/USB
2 https://nl.wikipedia.org/wiki/USB-stick
3 https://en.wikipedia.org/wiki/USB_flash_drive
4 https://tweakers.net/usb-sticks/
5 https://www.kanguru.com/
6 https://datalocker.com/products/encrypted-usb-flash-drives/
7 https://www.nirsoft.net/utils/usb_devices_view.html
8 https://www.diskpart.com/articles/how-to-partition-usb-drive-3889.html
9 https://www.ultimatetech.org/make-partitions-usb-drive-linux/
10 https://en.ihowto.tips/osx-apps-download-tutorials-tips-hacks-news/partitionare-si-parolare-flash-drive-usb-stick-pe-mac.html
11 https://www.pendrivelinux.com/yumi-multiboot-usb-creator/
12 https://unetbootin.github.io/
13 https://www.ventoy.net/en/index.html
14 http://truecrypt.sourceforge.net/
15 https://www.veracrypt.fr/en/Home.html
16 http://www.withopf.com/tools/securstick/
17 https://www.boxcryptor.com/en/
18 https://www.boxcryptor.com/download?platform=portable
19 https://cryptomator.org/
20 https://portapps.io/app/cryptomator-portable/
21 https://www.blackhillsinfosec.com/the-paper-password-manager/