

Gyakorlati útmutató biztonságos információkezeléshez offline és felhős környezetben

Jelszókezelés, hardverkulcs, titkosítás mindenekfelett

A leggyakoribb jelszókezelési problémák



Könnyű jelszavak létrehozása



Jelszó újrafelhasználás



Jelszavak nem biztonságos megosztása



Jelszavakat leírni, vagy eszközön text-ben tárolni



Többtényezős hitelesítés mellőzése



Hagyni, hogy a böngésző tárolja a jelszavakat

Jelszó feltörésének nehézségi fokozatai



<https://www.security.org/how-secure-is-my-password>

123456

Your password would be cracked

Instantly

Jelszó feltörésének nehézségi fokozatai



password

Your password would be cracked

Instantly

Jelszó feltörésének nehézségi fokozatai

6 karakter: kisbetű



jelszo

It would take a computer about

7 milliseconds

to crack your password

Jelszó feltörésének nehézségi fokozatai

6 karakter: kisbetű és szám



j e 1 s z 0

It would take a computer about

54 milliseconds

to crack your password

Jelszó feltörésének nehézségi fokozatai



6 karakter: kisbetű, nagybetű és szám

Je1sz0

It would take a computer about

1 second

to crack your password

Jelszó feltörésének nehézségi fokozatai



7 karakter: kisbetű, nagybetű, szám és speciális karakter

Je1sz0.

It would take a computer about

9 minutes

to crack your password

Jelszó feltörésének nehézségi fokozatai



8 karakter: kisbetű, nagybetű, szám és speciális karakter

Je1sz0.X

It would take a computer about

12 hours

to crack your password

Jelszó feltörésének nehézségi fokozatai

9 karakter: kisbetű, nagybetű, szám és speciális karakter



Je1sz0.X6

It would take a computer about

1 month

to crack your password

Jelszó feltörésének nehézségi fokozatai

10 karakter: kisbetű, nagybetű, szám és speciális karakter



Je1sz0.X6t

It would take a computer about

9 years

to crack your password

Jelszó feltörésének nehézségi fokozatai

11 karakter: kisbetű, nagybetű, szám és speciális karakter



Je1sz0.X6t?

It would take a computer about

7 hundred years

to crack your password

Jelszó feltörésének nehézségi fokozatai

10 karakteres változatok



| | | |
|-----------------------|---|-------------|
| 5979307601 | – | 2 másodperc |
| hjnznwvpwk | – | 58 perc |
| 8tm3eb4qtd | – | 1 nap |
| Q3rckGzTAd | – | 7 hónap |
| ZAas)J&H%1 | – | 5 év |

A leggyakoribb jelszókezelési problémák



Könnyű jelszavak létrehozása



Jelszó újrafelhasználás



Jelszavak nem biztonságos megosztása



Jelszavakat leírni, vagy eszközön text-ben tárolni



Többtenyezős hitelesítés mellőzése



Hagyni, hogy a böngésző tárolja a jelszavakat



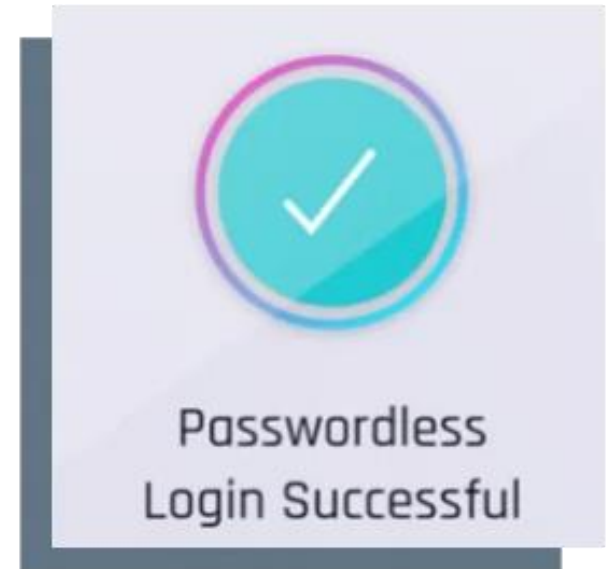
Jelszó nélküli bejelentkezés



Felhasználónév
(Email, ID vagy telszám)



Jelszó nélküli módszerek
(Biometrikus, hardverkulcs,
egyszer használatos jelszó)



Passwordless
Login Successful



Outlook



Bejelentkezés

Tovább ide: Outlook

E-mail, telefon, vagy Skype

Nincs fiókja? [Hozzon létre egyet!](#)

[Nem tud jelentkezni a fiókjába?](#)

Tovább



Bejelentkezési beállítások

Outlook



Bejelentkezési beállítások



Bejelentkezés biztonsági kulccsal
Csak akkor válassza ezt a lehetőséget, ha engedélyezte a biztonsági kulcs használatát a fiókhhoz.



Bejelentkezés GitHub-fiókkal
Csak a személyes fiókok



Bejelentkezés szervezetbe
Azon cégek vagy szervezetek keresése, akikkel együttműködik.

Vissza


Windows biztonság

Személyazonosság ellenőrzése


Jelentkezzen be a(z) login.microsoft.com rendszerbe.

Ez a kérelem innen érkezett: Firefox, közzevő: Mozilla Corporation.

Adja meg a biztonsági kulcs PIN-kódját.



OK Mégse



Windows biztonság

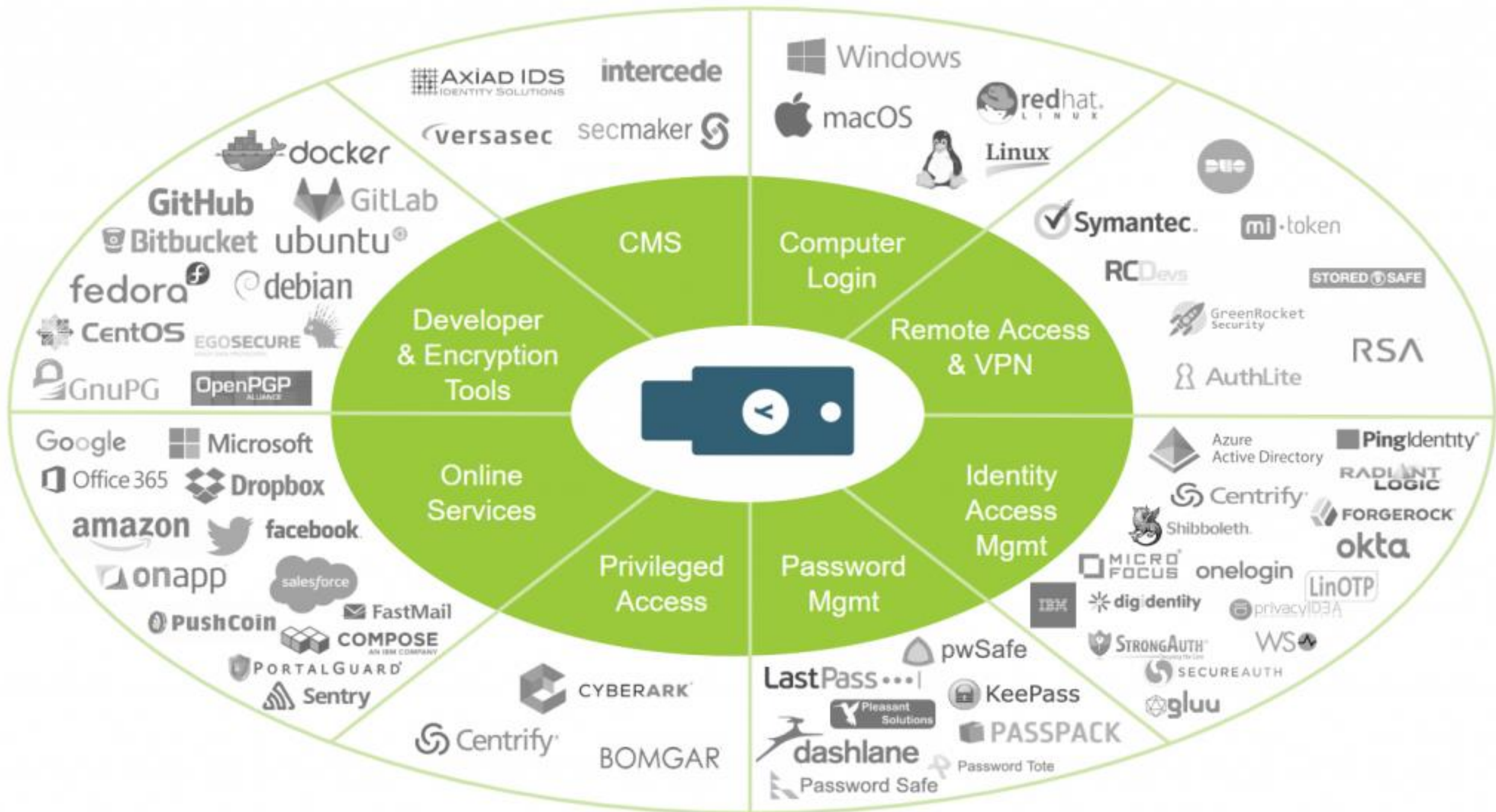
Személyazonosság ellenőrzése

Jelentkezzen be a(z) login.microsoft.com rendszerbe.

Ez a kérelem innen érkezett: Firefox, közzevő: Mozilla Corporation.

Érintse meg a biztonsági kulcsot.

Mégse



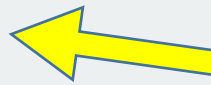
... de mi van, ha nem támogatja



- Egyszerű weboldalak
- Asztali alkalmazások





KeePassXC




 [The Project](#)

 [Screenshots](#)

 [Download](#)

 [Blog](#)

 [Docs / FAQ](#)

 [The Team](#)



KeePassXC - Cross-Platform Password Manager

Never forget a password again.

Securely store passwords using industry standard encryption, quickly auto-type them into desktop applications, and use our browser extension to log into websites.

Encrypted

Complete database encryption using industry standard 256-bit AES. Fully compatible with KeePass Password Safe formats. Your password database works offline and requires no internet connection.

Cross-Platform

Every feature looks, feels, works, and is tested on Windows, macOS, and Linux. You can expect a seamless experience no matter which operating system you are using.

Open Source

The full source code is published under the terms of the GNU General Public License and made available on GitHub. Use, inspect, change, and share at will; contributions by everyone are welcome.



Keresés (Ctrl+F)...



KeePassXC adatbázis feloldása

C:\KeePassXC\Jelszavak.kdbx

Jelszó megadása:

További hitelesítési adatok megadása (ha vannak):

Kulcsfájl: ?

Tallózás...

Hardverkulcs: ?

YubiKey [.....] kihívás-válasz – foglalat 2 - Lenyomás

Frissítés

OK

Mégse



▼ Passwords

▼ Internet

Coding

Gaming

Shopping

Social

My Computer

Real world

Recycle Bin

| | 📎 | 🕒 | Title ▲ | Username | URL | Notes | Modified |
|-------|---|---|-------------------|---------------------|--------------------------|-----------------------|-------------------|
| 🍏 | | | Apple | john.doe@icloud.com | https://www.icloud.c... | Username is the Ap... | 5/29/2020 2:25 PM |
| 📁 | | | Dropbox | john.doe@example... | http://www.dropbox... | | 5/29/2020 2:25 PM |
| 🌐 | | | Example Login ... | john.doe@example... | https://www.w3scho... | | 6/13/2020 5:58 PM |
| 🌐 | | | Google | johndoe@gmail.com | https://google.com | | 5/29/2020 2:27 PM |
| IFTTT | | | IFTTT | johndoe | https://ifttt.com | | 5/29/2020 2:25 PM |
| 📺 | | | Netflix | john.doe@example... | https://www.netflix.c... | | 5/29/2020 2:25 PM |
| 🌐 | | | Nextcloud | john.doe | https://apps.nextclo... | | 5/29/2020 2:25 PM |
| 📁 | | | Pocket | john.doe | http://getpocket.co... | | 5/29/2020 2:25 PM |



Passwords / Internet / Apple

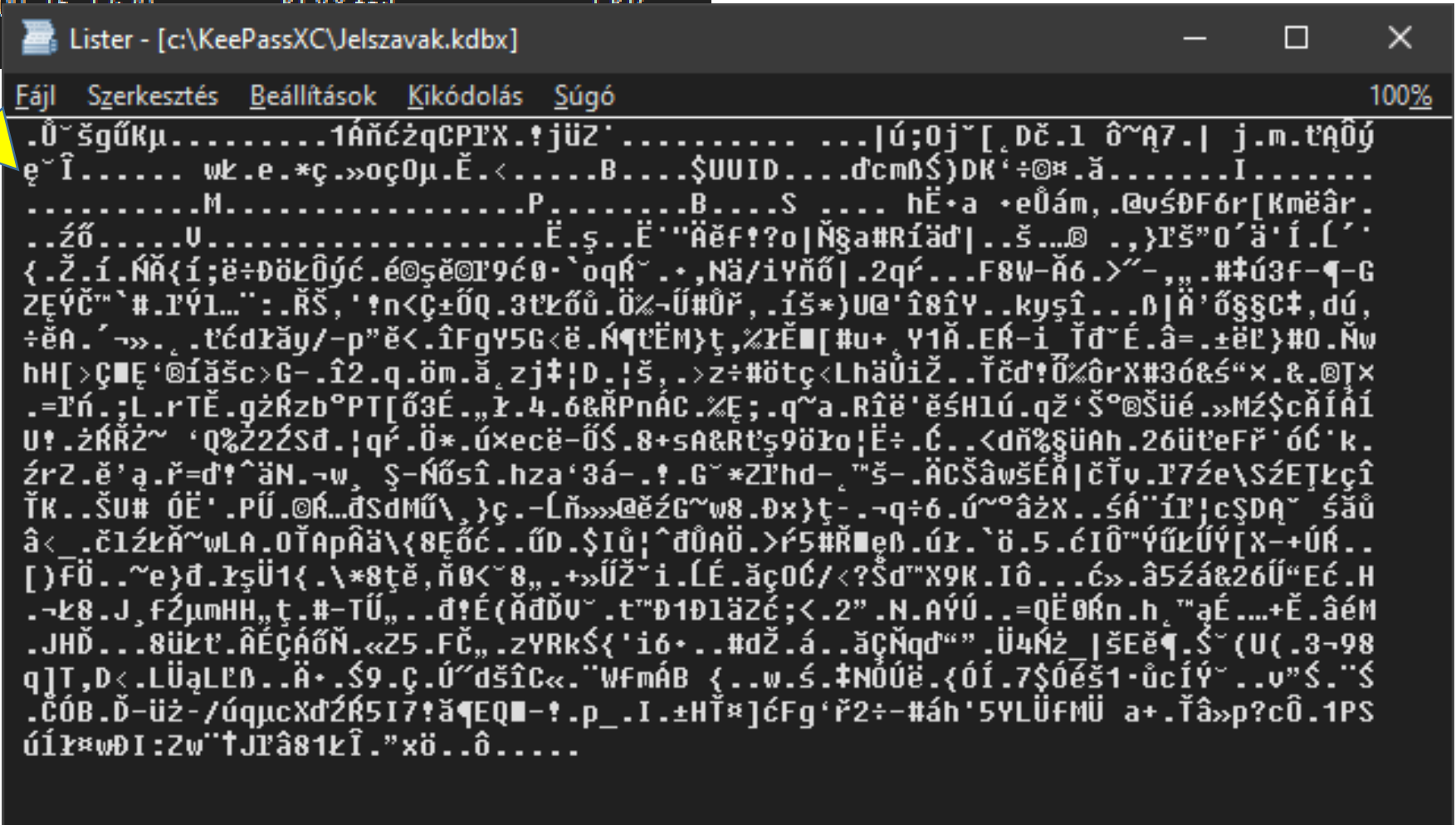
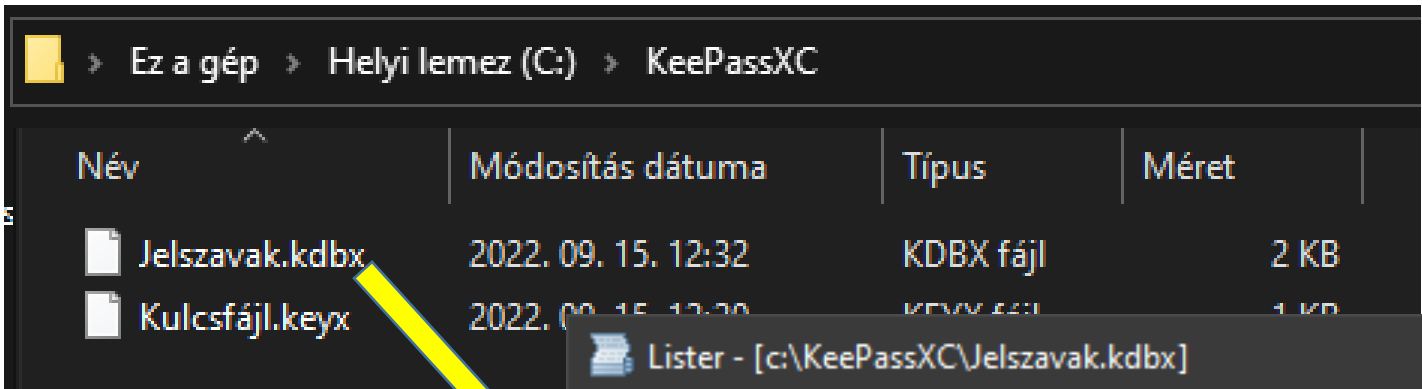


General

Advanced

Autotype

Username john.doe@icloud.com**URL** <https://www.icloud.com>**Password**  ●●●●●●**Expiration** Never**Notes** Username is the Apple ID





Keresés (Ctrl+F)...



Alkalmazásbeállítások



Általános



Biztonság



Böngészőintegráció

 Böngészőintegráció engedélyezése

Általános

Speciális

A böngészőintegráció működéséhez a KeePassXC-böngészőre van szükség.

Letölthető ezen böngészőkre: [Firefox](#), [Google Chrome / Chromium / Vivaldi / Brave](#), [Microsoft Edge](#), 4%**Böngészőintegráció engedélyezése a következőkhöz:**

- Chrome, Vivaldi, and Brave Firefox and Tor Browser Edge
 Chromium

- Adatbázis feloldási kérelem, ha zárolva van
 URL sémákra illeszkedés (pl. https://...)
 Csak a legjobb hitelesítési adatok visszaadása
 Lejárt hitelesítési adatok visszaadásának engedélyezése
 Keresés minden megnyitott adatbázis hitelesítési adataiban
 Illeszkedő hitelesítési adatok rendezése cím szerint
 Illeszkedő hitelesítési adatok rendezése felhasználónév szerint

OK

Mégse

Titkosítsunk mindent

| Mit | Mivel |
|---|--|
| Telefon, pendrive | Beépített titkosítási eszközzel (pendrive-nál például BitLocker) |
| Számítógép, laptop Meghajtók Fájl tárolók | VeraCrypt (free, open source, jól auditált) |



https://www.veracrypt.fr



100%



Home

Source Code

Downloads

Documentation

Donate

Forums

VeraCrypt is a free open source disk encryption software for Windows, Mac OSX and Linux. Brought to you by **IDRIX** (<https://www.idrix.fr>) and based on TrueCrypt 7.1a.

VeraCrypt main features:

- Creates a **virtual encrypted disk** within a file and mounts it as a real disk.
- Encrypts an **entire partition or storage device** such as USB flash drive or hard drive.
- Encrypts a **partition or drive where Windows is installed** ([pre-boot authentication](#)).
- Encryption is [automatic, real-time\(on-the-fly\) and transparent](#).
- [Parallelization](#) and [pipelining](#) allow data to be read and written as fast as if the drive was not encrypted.
- Encryption can be [hardware-accelerated](#) on modern processors.
- Provides [plausible deniability](#), in case an adversary forces you to reveal the password: [Hidden volume](#) (steganography) and [hidden operating system](#).
- More information about the features of VeraCrypt may be found in the [documentation](#)

Rendszermeghajtó titkosítása

VeraCrypt

Kötetek Rendszer Kedvencek Eszközök Beállítások Segítség Weboldal

Me... Kötet

Rendszermeghajtó

A:
B:
D:
E:
F:
G:
H:
I:
J:
L:

Kötet Létrehozása

Kötet

VeraCrypt

Soha ne mentse az előzménye

CSATOL Eszközök Auto-csatolása Mindent Lecsatol Kijelzés

VeraCrypt Kötet Létrehozó Varázsló

VeraCrypt kötetkészítő varázsló

Készíts egy kódolt fájl-tárolót
Egy fájlon belül hoz létre kódolt lemezt. (Tapasztalatlan felhasználóknak ezt javasoljuk választani.)
[További információ](#)

Nem-rendszer partíció/meghajtó Lekódolása
Bármely belső vagy külső meghajtó egészében Lekódolható (Pl. pendrájv).
Opcionálisan rejtett is lehet.

Kódold le a rendszer-partíciót/teljes rendszer-lemezt

Titkosítja azt a partíciót/meghajtót, amelyre a Windows telepítve van. Bárki, aki hozzáférést szeretne kapni a rendszerhez, fájlokat kíván olvasni és írni, stb., a Windows indítása előtt minden alkalommal meg kell adnia a helyes jelszót. Opcionálisan rejtett rendszert hoz létre.

[További információ a rendszer-kódolásról](#)

Súgó < Vissza **Következő >** Mégsem

Rendszermeghajtó titkosítása

The screenshot shows the VeraCrypt application window. The main interface displays a list of drives with columns for 'Kötet' (Volume), 'Méret' (Size), 'Kódolási algoritmus' (Encryption algorithm), and 'Típus' (Type). The 'Rendszermeghajtó' (System drive) is highlighted, with a yellow arrow pointing to it. A dialog box titled 'VeraCrypt Kötet Tulajdonságok' (VeraCrypt Volume Properties) is open, showing a table of properties for the selected volume. A second yellow arrow points to the 'PKCS-5 PRF' property, which is set to 'HMAC-SHA-256'.

| Tulajdonság | Érték |
|--------------------------------------|-----------------------------|
| Hely | Rendszermeghajtó |
| Méret | 120034091520 byte |
| Típus | Rendszer |
| Kódolási algoritmus | AES |
| Elsődleges kulcs mérete | 256 bit |
| Másodlagos kulcs mérete (XTS mód) | 256 bit |
| Blokk Méret | 128 bit |
| Működési mód | XTS |
| PKCS-5 PRF | HMAC-SHA-256 |
| A csatlakoztatás óta olvasott adatok | 18.6 GB |
| A csatlakoztatás óta írt adatok | 61.7 GB |
| VeraCrypt rendszertöltő verzió | 1.24 |
| Titkosított rész | 100% (teljesen titkosított) |

Rendszermeghajtó titkosítása

VeraCrypt Boot Loader 1.21

Keyboard Controls:

[F5] Hide/Show Password and PIM

[Esc] Skip Authentication (Boot Manager)

Enter password: _

Titkosított fájl tároló

VeraCrypt

Kötetek Rendszer Kedvencek Eszközök Beállítások Segítség Weboldal...

Me... Kötet Méret Kódolási algoritmus Típus

Rendszermeghajtó

A:
B:
D:
E:
F:
G:
H:
I:
J:
L:

Kötet Létrehozása

Kötet

VeraCrypt

Soha ne mentse az előzmé

CSATOL Eszközök Auto-csatolása Mindent Lecsatol Kijépés

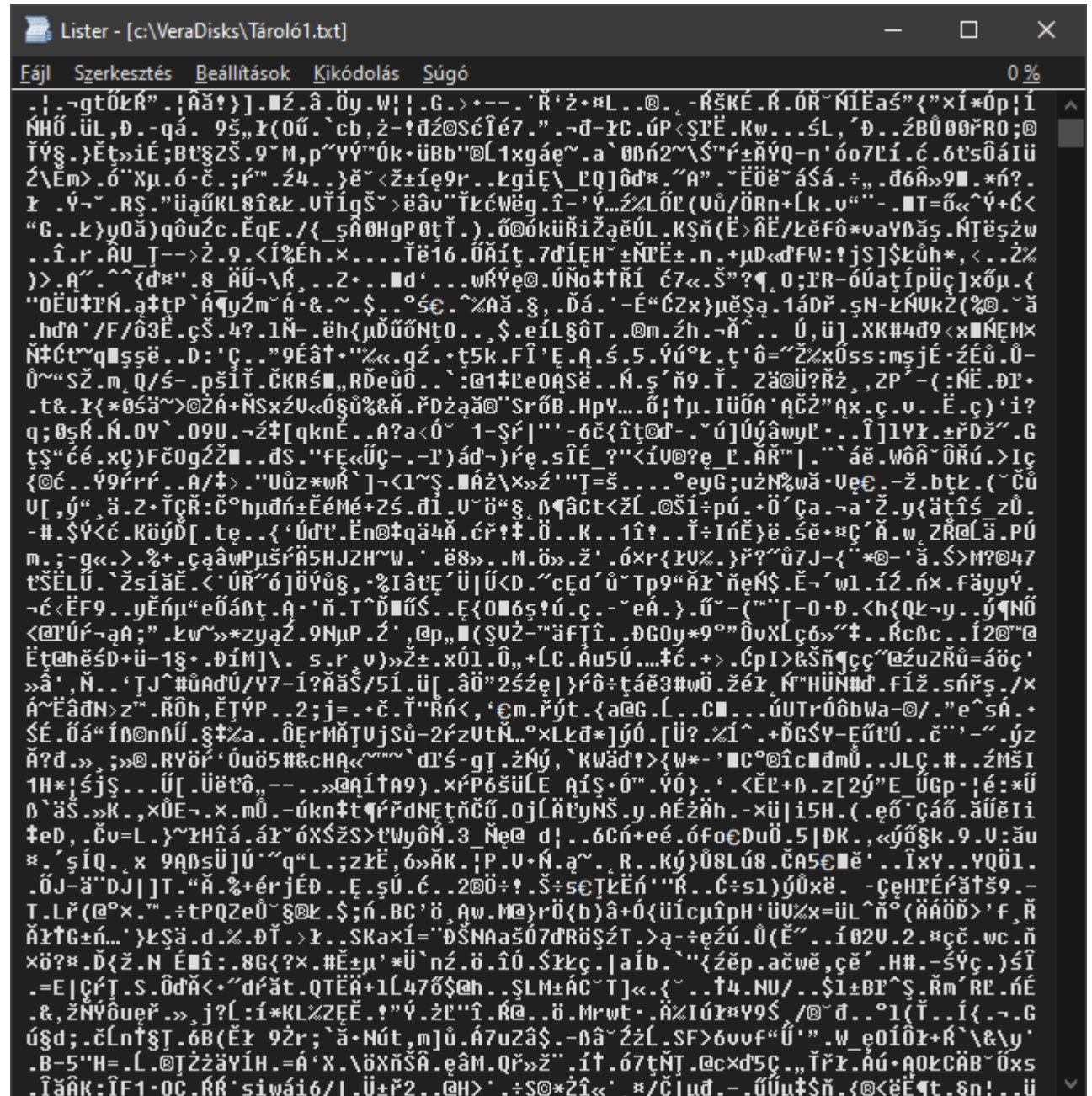
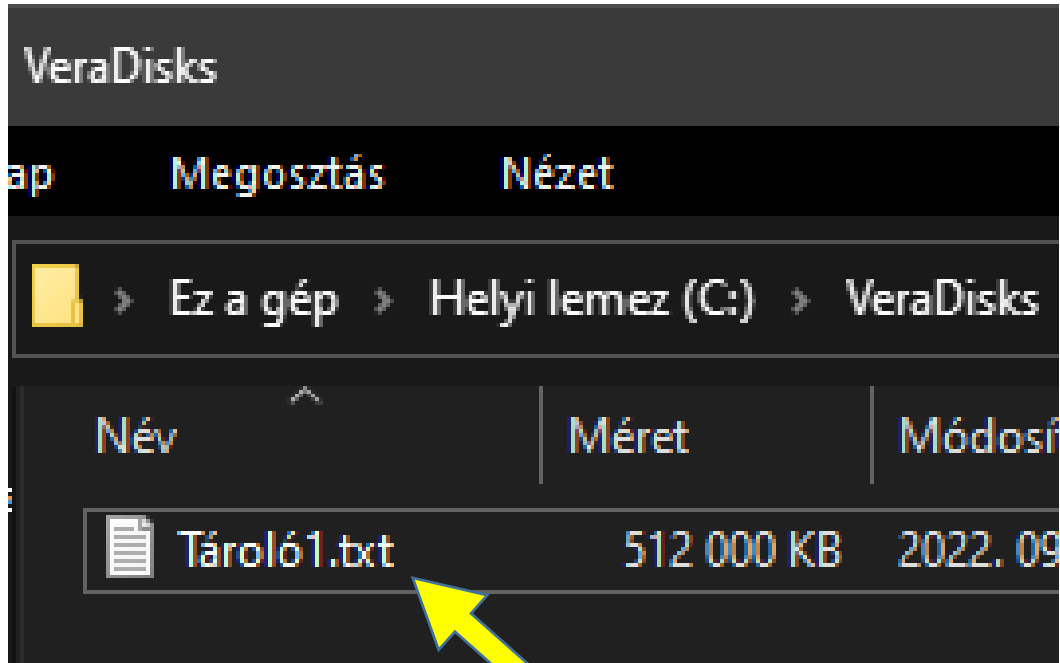
VeraCrypt Kötet Létrehozó Varázsló

VeraCrypt kötetkészítő varázsló

- Készíts egy kódolt fájl-tárolót**
Egy fájlon belül hoz létre kódolt lemezt. (Tapasztalatlan felhasználóknak ezt javasoljuk választani.)
[További információ](#)
- Nem-rendszer partíció/meghajtó Lekódolása**
Bármely belső vagy külső meghajtó egészében Lekódolható (Pl. pendrájv).
Opcionálisan rejtett is lehet.
- Kódold le a rendszer-partíciót/teljes rendszer-lemezt**
Titkosítja azt a partíciót/meghajtót, amelyre a Windows telepítve van. Bárki, aki hozzáférést szeretne kapni a rendszerhez, fájlokat kíván olvasni és írni, stb., a Windows indítása előtt minden alkalommal meg kell adnia a helyes jelszót. Opcionálisan rejtett rendszert hoz létre.
[További információ a rendszer-kódolásról](#)

Súgó < Vissza **Következő >** Mégsem

Titkosított fájl tároló



Titkosított fájl tároló

VeraCrypt

Kötetek Rendszer Kedvencek Eszközök Beállítások Segítség Weboldal...

| Me... | Kötet | Méret | Kódolási algoritmus | Típus |
|-------|---------------------------|--------|---------------------|--------|
| A: | | | | |
| B: | | | | |
| D: | | | | |
| E: | | | | |
| F: | C:\VeraDisks\Tároló 1.txt | 499 MB | AES | Normál |
| G: | | | | |
| H: | | | | |
| I: | | | | |
| J: | | | | |
| L: | | | | |
| M: | | | | |

Kötet Létrehozása Kötet Tulajdonságok...

Kötet

VeraCrypt

C:\VeraDisks\Tároló 1.txt Fáj kiválasztása...

Soha ne mentse az előzményeket Kötet Eszközök... Eszköz kiválasztása...

Leválaszt Eszközök Auto-csatolása Mindent Leccsatol Kijáráás

Ez a gép

Keresés: Ez a gép

Eszközök és meghajtók

Helyi lemez (C:) 11,1 GB szabad, méret: 111 GB

Helyi lemez (F:) 483 MB szabad, méret: 499 MB

Foglaljuk össze

Biztonságosan és titkosan ...



- ... tudunk bejelentkezni **hardverkulcs** segítségével nagyobb szolgáltatókhoz

- ... kezelhetjük a jelszavainkat egyetlen fájlban (**Jelszavak.kdbx**)

- ... tárolhatjuk a fájljainkat konténerben (**Tároló1.txt**)



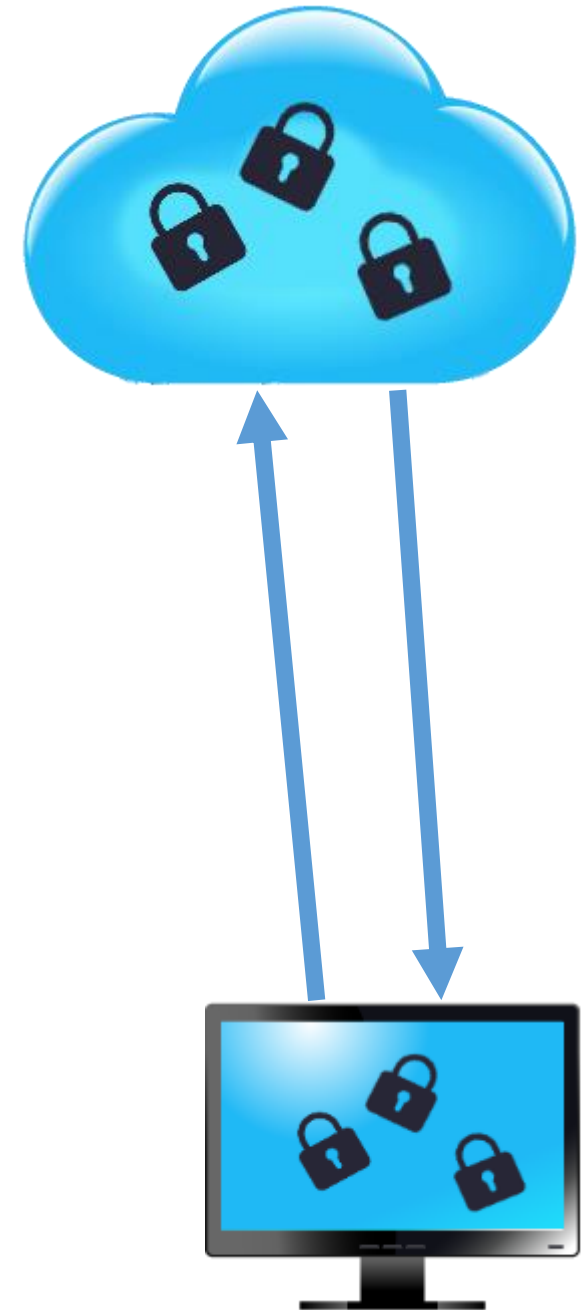
VeraCrypt

KeePassXC



Felhőtárhely használata ezek ismeretében

- Manapság mindenkinek van valamennyi felhőtárhelye (G Drive, MS Onedrive, stb.)
- Ezekbe való belépéshez használjuk a hardverkulcsunkat
- A felhő tároló tartalmát leszinkronizálhatjuk a számítógépre
- Belemozgatjuk a KeePassXC-vel létrehozott jelszófájlt és a VeraCrypt-tel létrehozott fájl tárolókat
- A számítógépen használjuk ezeket a mindennapi élethez.
 - A változások (Titkosított fájl szinten) felszinkronizálódnak a felhőbe.
 - Ha több gépen dolgozunk, a többi gépen leszinkronizálódik a változás.



Köszönöm.