dsb
datenschutzbeauftragte
des kantons zürich

Fact Sheet

# Password Manager

## 1 Introduction

A strong and unique password for every account is necessary to safely use online services. In practice, this creates far too many passwords to remember. Special software, or password managers, helps you manage this problem. Password managers make it easier to create and use secure passwords because you only have to remember a few of them: those for truly sensitive services and one master password for the password manager itself.

This fact sheet contains a security analysis and a comparison of the password managers below.

- 1Password
- Bitwarden
- KeePass2
- MiniKeePass
- KeePass2Android
- LastPass
- Keychain Access
- SecureSafe

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch, twitter: @dsb_zh

## 2 Criteria

| Criteria | Description |
|---|---|
| Operating system | Describes which operating systems (Windows, MacOS, iOS, Linux or Android) support the password managers. |
| Source code available | Describes whether the source code is publicly available. This is relevant to security because publicly available source code (open source) can be checked for vulnerabilities more easily. |
| Brute-force protection | Refers to methods that protect against brute-force attacks (trying all possible passwords). |
| Keylogger protection | Refers to methods that protect against keylogger attacks (recording keystrokes on the keyboard). |
| Clipboard protection | Describes how the clipboard is protected against being read. |
| Automatic lock | Describes whether the password database is automatically locked after a certain period of time. |
| Authentication | Describes authentication options for the password manager. |
| Automatic password generation | Specifies whether secure passwords can be generated automatically. |
| Database storage location | Describes where the password database is stored. |
| Database encryption | Describes what algorithms and key size are used to encrypt the password database. |
| Password recovery | Describes whether and how the master password can be recovered. |
| Syncing | Describes whether passwords can be synced across multiple systems. Automatic sync is more user-friendly but also riskier. |
| Portability (export) | Describes the format in which passwords can be exported for further use. |

## 3 Analysis an comparison

| | KeePass databases | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Products**<br>**Criteria** | **KeePass2** | **Strongbox** | **KeePass2 Android** | **1Password** | **Bitwarden** | **LastPass** | **Keychain Access** | **SecureSafe** |
| Windows | X | | | X | X | X | | X |
| MacOS | X | X | | X | X | X | X | X |
| Linux | X | | | X | X | Add-on | | |
| Android | | | X | X | X | X | | X |
| iOS | | X | | X | X | X | X | X |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Brute-force protection | Key transformation | Key transformation | Key transformation | PBKDF2 | PBKDF2 | PBKDF2 | No information available | PBKDF2 |
| Keylogger protection | TCATO/Secure Desktop (master password) | No information available | Built-in software keypad | No information available | No information available | Virtual keypad | No information available | - |
| Clipboard protection | Automatic deletion | Automatic deletion | Built-in software keypad | Automatic deletion | Automatic deletion | Automatic deletion | No information available | Automatic deletion |
| Automatic lock | Yes | Yes | Yes, with quick-unlock key | Yes | Configurable | Yes | Yes | Yes |
| Database encryption | AES256 | AES256 | AES256 | AES256 | AES256 | AES256 | AES256 | AES256 |

| | KeePass databases | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Products**<br>**Criteria** | **KeePass2** | **Strongbox** | **KeePass2 Android** | **1Password** | **Bitwarden** | **LastPass** | **Keychain Access** | **SecureSafe** |
| Authentication | Passwort/keyfile/ OTP (OATH/ HOTP), Yubikey, Google-Authenti-cator etc. | Passwort / TOTP, Premium: Yubikey, Face ID, Touch ID, Pin Code | Passwort/keyfile/ OTP (OATH/ HOTP), Yubikey | Password, Authy, Google Authenticator, Microsoft Authenticator etc. | User name/ password, Authy, Google Authenticator Paid :SMS, Yubikey | User name/ password, Yubikey, Google Authenticator, OTP, fingerprint, etc. | Password/iCloud two-factor | User name/password/ mTAN (paid) |
| Automatic pass-word generation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Database storage location | Local | Local or stored in the cloud | Local | Stored in the cloud | Local[1] or stored in the cloud | Stored in the cloud | Local or in iCloud | Stored in cloud (CH) |
| Syncing | Via third-party services (see Online Storage Services Fact Sheet) | | | Yes | Yes | Yes | Yes | |
| Password recovery | -- | -- | -- | Yes (Emergency Kit) | -- | Password hint, backup key and e-mail | Only with iCloud sync | Recovery code |
| Portability (export) | CSV/HTML | CSV | CSV/HTML | CSV | CSC | CSV | | CSV |

[1] Local storage in Bitwarden password database primarily for experts

| **Product and maker information** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Maker | Dominik Reichl (DE) https://keepass.info/ | Phoebe Code Limited (UK) https://strongboxsafe.com/about/ | Philipp Crocoll (DE) http://philipp.crocoll.net/donate.php | AgileBits, Inc. (CA) https://www.1password.com | 8bit Solutions LLC https://bitwarden.com/ | Marcasol Inc. (USA) https://www.lastpass.com | Apple Inc. (USA) https://www.apple.com | DSwiss AG (CH) https://www.securesafe.com |
| Source code available | Source code available | Source code available | Source code available | Source code not available | Source code available | Source code not available | Source code partially available | Source code not available |
| Price | Free | Free/premium service from USD 3/month | Free | From USD 3/month | Free/premium service from USD 10/year | From USD 3/month (limited version : free) | Free | From CHF 1.50/month (limited version free) |
| Comments | Extensive range of functions | | | | User-friendly | Good documentation, very user frindly | | |

**Very secure/very reliable** **Secure/reliable** **Less secure/less reliable**

## 4 Tip

KeePass2, KeePass2Android and Strongbox are free, secure and mature password managers. 1Password, LastPass and SecureSafe offer more extensive syncing options but are paid services. These products also store keys in the cloud, which means the security of the data cannot always be guaranteed.

## 5 Remaining risks

Because all passwords are stored in one place, using a password manager poses a risk that all passwords can be read by a trojan. To reduce the risk of trojan attacks, the end device must be protected by taking the following precautions:

- Regularly install updates (operating systems like Windows, programs like browsers)
- Judicious handling of e-mails and downloads
  - More information in the Secure E-mails Fact Sheet (in German)
  - Information on the website of the Swiss National Cyber Security Centre NCSC on malware on websites and handling e-mails securely, spam and phishing
- Enable firewall and install antivirus software
  - More information in the PC Security Checklist (in German)
- Use a secure master password
  - More information about passwords (in German) from the Federal Office for Information Security (BSI, Germany)
  - More information about passwords from iBarry.ch
  - More information on two-factor authentication from iBarry.ch
  - More information and password check at passwortcheck.ch

Despite these technical precautions, trojans remain a considerable risk. Passwords for sensitive services (such as online banking, PayPal, and e-mail services) should not be stored on any IT system, or access should be protected using strong authentication methods (such as SMS, Google Authenticator, Yubikey, RSA Token).

Translation of Merkblatt Passwortmanager V 3.4 / Juli 2022