

## Fact Sheet

## Password Managers

## 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

## 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.



Criteria \ Products	KeePass databases			1Password	Bitwarden	LastPass	Keychain Access	SecureSafe
	KeePass2	MiniKeePass	KeePass2 Android					
Authentication	Password/keyfile/OTP (OATH/HOTP), Yubikey, Google Authenticator etc.	Password/keyfile	Password/keyfile/OTP (OATH/HOTP)/ Yubikey	Password	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 password generation	Yes	Yes	Yes		Yes	Yes	Yes	Yes
Database storage location	Local	Local	Local	In the cloud standard, local supported <sup>11</sup>	Local <sup>22</sup> or stored in the cloud	Stored in the cloud	Local or in iCloud	Stored in the cloud (CH)
Syncing	Via third-party services (see <a href="#">Online Storage Services Fact Sheet</a> )			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/HTML (using PC app)	CSV/HTML	CSV	CSV	CSV		CSV

<sup>1</sup> Local storage in local folder (local folder/vault) possible

<sup>2</sup> Local storage in Bitwarden password database primarily for experts

Product and maker information								
Maker	Dominik Reichl (DE) <a href="http://www.dominik-reichl.de">http://www.dominik-reichl.de</a>	Flush Software, LLC (USA) <a href="http://minikee-pass.github.io">http://minikee-pass.github.io</a>	Philipp Crocoll (DE) <a href="http://philipp.crocoll.net/donate.php">http://philipp.crocoll.net/donate.php</a>	AgileBits, Inc. (CA) <a href="https://www.1password.com">https://www.1password.com</a>	8bit Solutions LLC <a href="https://bit-warden.com">https://bit-warden.com</a>	Marvasol Inc. (USA) <a href="https://www.lastpass.com">https://www.lastpass.com</a>	Apple Inc. (USA) <a href="https://www.apple.com">https://www.apple.com</a>	DSwiss AG (CH) <a href="https://www.securesafe.com">https://www.securesafe.com</a>
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	Free	From USD 3/month	Free/premium service from USD 12/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 friendly		
	Very secure/very reliable		Secure/reliable		Less secure/less reliable			

## 4 Tip

KeePass2, KeePass2Android and MiniKeePass 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 and Flash Player)
  - More information can be found in the [Patch Management Guide](#) (in German) released by the Federal Office for Information Security (BSI, Germany)
- 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).

dsb



datenschutzbeauftragte  
kanton zürich

Data protection authority  
of the Canton of Zurich  
8090 Zurich

Telefon 043 259 39 99  
datenschutz@dsb.zh.ch

[www.datenschutz.ch](http://www.datenschutz.ch)  
[twitter.com/dsb\\_zh](https://twitter.com/dsb_zh)

