

## **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



## 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 database	es					
Products Criteria	KeePass2	Strongbox	KeePass2 Android	1Password	Bitwarden	LastPass	Keychain Access	SecureSafe
Windows	Х			Х	Х	Х		Х
MacOS	Х	Х		Х	Х	Х	Х	Х
Linux	Х			Х	Х	Add-on		
Android			Х	Х	Х	Х		Х
iOS		Х		Х	Х	Х	Х	Х
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 informatio available		-
Clipboard protection	Automatic deletion	Automatic deletion	Built-in software keypad	Automatic deletion	Automatic deletion	Automatic deletion	Automatic No information available	
Automatic lock	Yes	Yes	Yes, with quick- unlock key	Yes	Configurable	Yes Yes		Yes
Database encryption	AES256	AES256	AES256	AES256	AES256	AES256	AES256	AES256



	I	KeePass databases	5					
Products 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 <sup>1</sup> or stored in the cloud	Stored in the cloud	Local or in iCloud	Stored in cloud (CH)
Syncing	Via third-party services (see <u>Online Storage Services</u> <u>Fact Sheet</u> )			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

<sup>&</sup>lt;sup>1</sup> Local storage in Bitwarden password database primarily for experts

Product and maker information									
Maker	Dominik Reichl (DE) https://keepass.i nfo/	Phoebe Code Limited (UK) <u>https://strongboxsafe.</u> <u>com</u>	Philipp Crocoll (DE) <u>https://github.com/PhilippC/keepass2</u> <u>android</u>	AgileBits, Inc. (CA) https://ww w.1 password.c om	8bit Solutions LLC <u>https://bit</u> <u>war</u> <u>den.com/</u>	Marcasol Inc. (USA) <u>https://www.l</u> <u>ast</u> pass.com	Apple Inc. (USA) https://www. app le.com	DSwiss AG (CH) <u>https://www</u> <u>.se</u> <u>curesafe.co</u> <u>m</u>	
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	Free	Free	Free	
Commen ts	Extensive range of functions				User- friendly	Good documentatio n, very user frindly			
Very secure/very reliable			Secure/reliable			Less secure/less	s reliable		



## 4 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 <u>Secure E-mails Fact Sheet</u> (in German)
  - Information on the website of the Swiss National Cyber Security Centre NCSC on <u>malware on</u> websites and <u>handling e-mails securely</u>, spam and <u>phishing</u>
- Enable firewall and install antivirus software
  - More information in the <u>PC Security Checklist</u> (in German)
- Use a secure master password
  - More information about <u>passwords</u> (in German) from the Federal Office for Information Security (BSI, Germany)
  - More information about <u>passwords</u> 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 Authenticator-Apps, Yubikey, RSA Token).

Translation of Merkblatt Passwortmanager V 3.6 / September 2024

