dsb
datenschutzbeauftragter
kanton zürich

Merkblatt

Passwortmanager

1 Einleitung

Für die sichere Verwendung von Online-Diensten ist für jedes Konto ein anderes und starkes Passwort erforderlich. In der Praxis führt diese Regel zu unzähligen Passwörtern, die man sich merken muss. Mit spezieller Software, sogenannten Passwortmanagern, lässt sich dieses Problem in den Griff bekommen. Sie erleichtern die Erstellung und Nutzung sicherer Passwörter, weil man sich nur noch wenige merken muss: diejenigen für die wirklich sensiblen Dienste sowie das Master-Passwort für den Passwortmanager.

Dieses Merkblatt enthält eine sicherheitstechnische Analyse sowie einen Vergleich der folgenden Passwortmanager und beschreibt, wie KeePass2, MiniKeePass und KeePass2Android installiert und konfiguriert werden können.

- 1Password
- Bitwarden
- KeePass2
- MiniKeePass
- KeePass2Android
- LastPass
- Schlüsselbundverwaltung / Keychain
- SecureSafe

2 Kriterien

Kriterien	Beschreibung
Betriebssystem	Beschreibt, auf welchen Betriebssystemen (Windows, MacOS, iOS, Linux oder Android) der Passwortmanager genutzt werden kann.
Quellcode verfügbar	Beschreibt, ob der Programcode öffentlich verfügbar ist. Dies ist sicherheitsrelevant, da ein öffentlich verfügbarer Quellcode (Open Source) besser auf Schwachstellen überprüft werden kann.
Brute-Force-Schutz	Beschreibt, welche Schutzmassnahme gegen Brute-Force-Angriffe (Durchprobieren aller möglichen Passwörter) existiert.
Keylogger-Schutz	Beschreibt, welche Schutzmassnahme gegen Keylogger-Angriffe (Aufzeichnen der Tastatureingaben) existiert.
Schutz Zwischenablage	Beschreibt, wie die Zwischenablage gegen Auslesen geschützt ist.
Automatische Sperre	Beschreibt, ob die Passwortdatenbank nach einer gewissen Zeitspanne automatisch gesperrt wird.
Authentifizierung	Beschreibt die Möglichkeiten zur Authentifizierung gegenüber dem Passwortmanager.
Automatische Passwortgenerierung	Gibt an, ob sich sichere Passwörter automatisch generieren lassen.
Ablageort Datenbank (DB)	Beschreibt, ob die Passwortdatenbank lokal oder auf einem externen Server abgelegt ist.
Verschlüsselung DB	Beschreibt, mit welchem Algorithmus und welcher Schlüssellänge die Passwortdatenbank verschlüsselt wird.
Passwortwiederherstellung	Beschreibt, ob und wie das Master-Passwort wiederhergestellt werden kann.
Synchronisation	Beschreibt, ob sich die Passwörter über verschiedene Systeme synchronisieren lassen. Eine automatische Synchronisation erhöht die Benutzerfreundlichkeit, aber auch die Risiken.
Portability (Export)	Beschreibt, in welchem Format die Passwörter zur weiteren Verwendung exportiert werden können.

3 Analyse und Vergleich

Produkte / Kriterien	KeePass-Datenbanken			1Password	Bitwarden	LastPass	Schlüsselbund-verwaltung	SecureSafe
	KeePass2	MiniKeePass	KeePass2 Android					
Unterstützte Betriebssysteme (Client)								
Windows	x				x	x		x
MacOS	x				x	x	x	x
Linux	x				x	Add-on		
Android			x		x	x		x
iOS		x			x	x	x	x
Schutzfunktionen Passwortmanager								
Brute-Force-Schutz	Schlüssel-transformation	Schlüssel-transformation	Schlüssel-transformation	PBKDF2	PBKDF2	PBKDF2	*Keine Informationen verfügbar*	PBKDF2
Keylogger-Schutz	TCATO / Secure Desktop (Master-Passwort)	Guter Schutz durch App-Rechte-management	Eigene Software-tastatur	*Keine Informationen verfügbar*	*Keine Informationen verfügbar*	Virtuelle Tastatur	*Keine Informationen verfügbar*	–
Schutz Zwischenablage	Automatische Löschung	Automatische Löschung	Eigene Software-tastatur	Automatische Löschung	*Keine Informationen verfügbar*	Automatische Löschung	*Keine Informationen verfügbar*	Automatische Löschung
Automatische Sperre	Ja	Ja	Ja, Quick-Unlock-Schlüssel	Ja	Konfigurierbar	Ja	Ja	Ja
Verschlüsselung DB	AES/Rijndael256	AES/Rijndael256	AES/Rijndael256	AES256	AES256	AES256	AES256	AES256

Produkte / Kriterien	KeePass-Datenbanken			1Password	Bitwarden	LastPass	Schlüsselbund-verwaltung	SecureSafe
	KeePass2	MiniKeePass	KeePass2 Android					
Authentifizierung	Passwort / Schlüsseldatei / OTP (OATH/HOTP), Yubikey, Google Authenticator usw.	Passwort / Schlüsseldatei	Passwort / Schlüsseldatei / OTP (OATH/HOTP) / Yubikey	Passwort	Benutzername / Passwort, Authy, Google Authenticator Kostenpflichtig: SMS, Yubiykey	Benutzername / Passwort, Yubikey, Google Authenticator, OTP, Fingerprint usw.	Passwort / iCloud 2-Faktor	Benutzername / Passwort / mTan (kostenpflichtig)
Passwortfunktionen und -speicherung								
Automatische Passwortgenerierung	Ja	Ja	Ja		Ja	Ja	Ja	Ja
Ablageort Datenbank (DB)	Lokal oder auf Server gespeichert	Lokal oder auf Server gespeichert	Lokal oder auf Server gespeichert		Lokal[1] oder in der Cloud gespeichert	In der Cloud gespeichert	Lokal oder in der iCloud	In der Cloud (CH) gespeichert
Synchronisation	Über Drittdienste (siehe Merkblatt Online-Speicherdienste)			Ja	Ja			
Passwort-wiederherstellung	–	–	–	Ja (Emergency Kit)	–	Passworthinweis, Back-up-Schlüssel und E-Mail	Nur bei iCloud Synchronisation	Wiederherstellungscode
Portability (Export)	CSV / HTML	CSV / HTML (über PC-Anwendung)	CSV / HTML	CSV	CSV	CSV		CSV

[1] Lokales Abspeichern der Bitwarden-Passwortdatenbank vor allem für Expertinnen oder Experten

Produkt- und Herstellerinformationen								
Hersteller	Dominik Reichl (DE) http://www.dominik-reichl.de	Flush Software, LLC (USA) http://minikeepass.github.io	Philipp Crocoll (DE) http://philipp.crocoll.net/donate.php	AgileBits, Inc. (CA) https://www.1password.com	8bit Solutions LLC https://bitwarden.com	Marvasol Inc. (USA) https://www.lastpass.com	Apple Inc. (USA) https://www.apple.com	DSwiss AG (CH) https://www.securesafe.com
Quellcode verfügbar	Quellcode verfügbar	Quellcode verfügbar	Quellcode verfügbar	Quellcode nicht verfügbar	Quellcode verfügbar	Quellcode nicht verfügbar	Quellcode teilweise verfügbar	Quellcode nicht verfügbar
Preis	kostenlos	kostenlos	kostenlos	Ab $3 pro Jahr	kostenlos / Premiumdienste ab $12 pro Jahr	24$ pro Jahr (eingeschränkt: kostenlos)	kostenlos	kostenlos (bis 50 Passwörter)
Bemerkungen	Sehr grosser Funktionsumfang				Benutzerfreundlich	Gute Dokumentation, sehr benutzerfreundlich		

	sehr sicher / sehr vertrauenswürdig		sicher / vertrauenswürdig		weniger sicher / weniger vertrauenswürdig

4 Tipp

KeePass2, KeePass2Android und MiniKeePass sind kostenlos verfügbare, sichere und ausgereifte Passwortmanager-Programme. LastPass oder SecureSafe bieten umfangreichere Synchronisationsoptionen, sind jedoch kostenpflichtig. Zudem werden bei diesen Produkten die Schlüssel extern abgespeichert, wodurch die Sicherheit der Daten nicht komplett gewährleistet ist.

5 Restrisiken

Beim Einsatz eines Passwortmanagers besteht das Risiko darin, dass alle Passwörter an einem Ort abgespeichert sind und durch einen Trojaner ausgelesen werden können. Um das Risiko eines Trojanerbefalls zu reduzieren, muss das Endgerät mit folgenden Massnahmen geschützt werden:

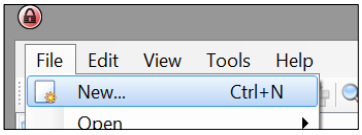
- Regelmässige Aktualisierung durchführen (Betriebssystem wie Windows, Programme wie Browser und Flash Player)
  - Weitere Informationen im Leitfaden Patch-Management des Bundesamts für Sicherheit in der Informationstechnik (BSI, Deutschland)
- Kritischer Umgang bei E-Mails und Downloads
  - Weitere Informationen im Merkblatt Sichere E-Mails
  - Informationen zu Schadsoftware auf Webseiten und Schadsoftware in E-Mails sowie Spam und Phishing von der Melde- und Analysestelle Informationssicherung (MELANI)
- Firewall aktivieren und Virenschutzsoftware installieren
  - Weitere Informationen in der Checkliste PC-Sicherheit
- Sicheres Master-Passwort verwenden
  - Weitere Informationen zu Passwörtern vom BSI
  - Weitere Informationen und Passwortcheck auf Passwortcheck.ch

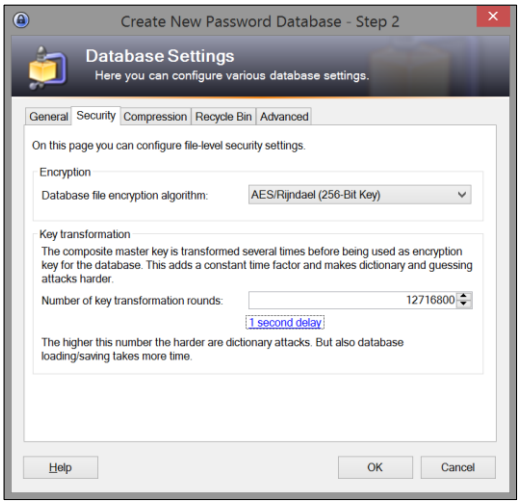
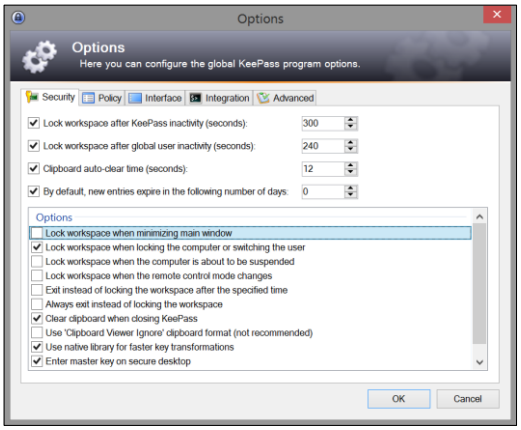
Trojaner bleiben trotz dieser technischen Massnahmen ein nicht vernachlässigbares Risiko. Passwörter für sensible Dienste (zum Beispiel E-Banking, Paypal oder E-Mail-Dienste) sollen deshalb auf keinem IT-System abgespeichert oder die Zugänge mit einer starken Authentifizierung (zum Beispiel SMS, Google Authenticator, Yubikey, RSA Token) geschützt sein.

6 Anleitungen

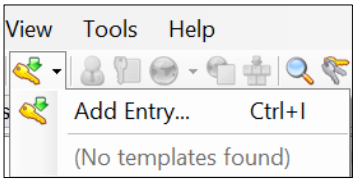
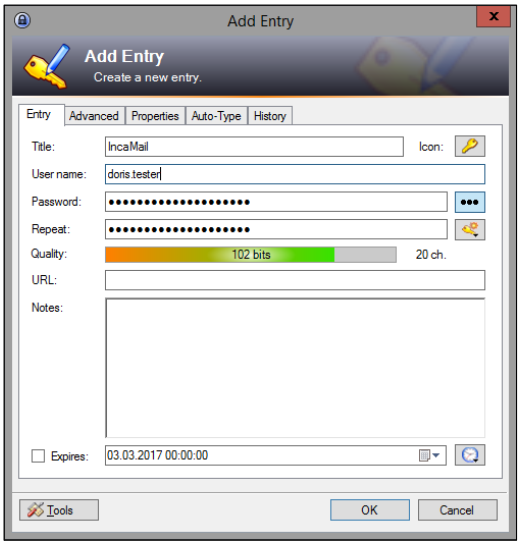
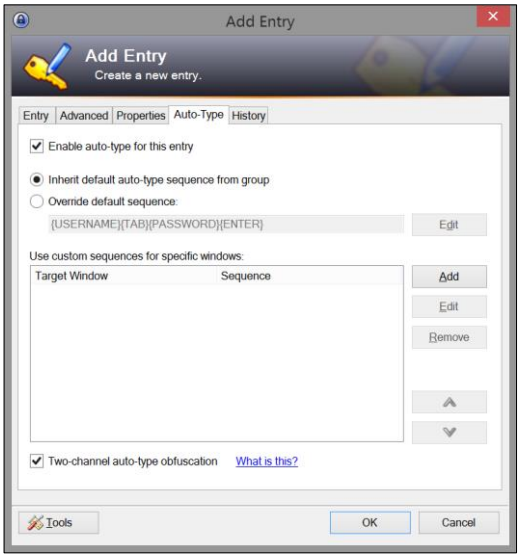
6.1 Anleitung KeePass2 für Windows

6.1.1 Passwort-Datenbank erstellen

1. KeePass2 herunterladen und installieren (https://keepass.info/download.html)	
2. KeePass2 starten	
3. Neue Datenbank erzeugen	
4. Pfad für die Passwort-Datenbank angeben (z.B. Dokumente\PW.kdbx)	
5. Starkes Master-Passwort wählen Als zusätzlicher Schutz der Passwortdatenbank kann eine Schlüsseldatei (Key File) erstellt werden. Die Schlüsseldatei ist entsprechend zu sichern und vor unbefugtem Zugriff zu schützen (z.B. auf einem USB-Stick).	

6. Tab Security → Number of key... → mehr als 500 000 eintragen	
7. OK klicken	
8. Tools → Options: Einstellungen anpassen	

6.1.2 Neue Einträge hinzufügen

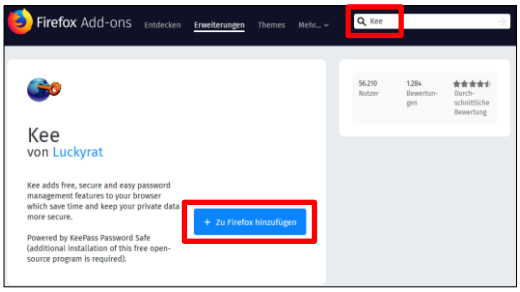
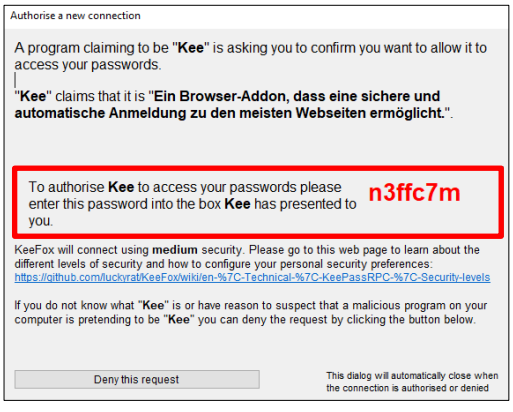
1. Eintrag hinzufügen (z.B. www.incamail.ch)	 
2. Auto-Type konfigurieren (sofern nötig)	
3. OK klicken	

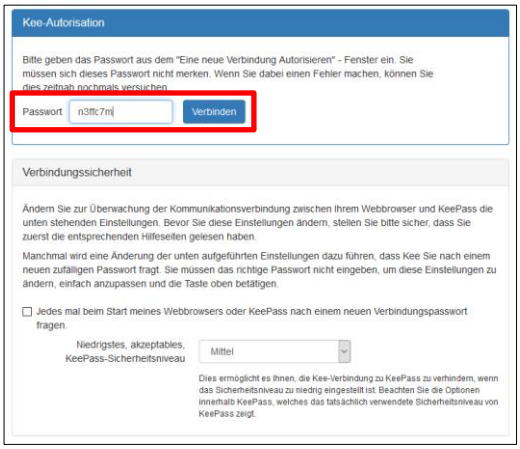
6.1.3 Webseiten aufrufen (Passwörter verwenden)

1. Gewünschte Webseite im Browser aufrufen (z.B. www.incamail.ch)
2. Tastaturkombination Ctrl + Alt + A klicken

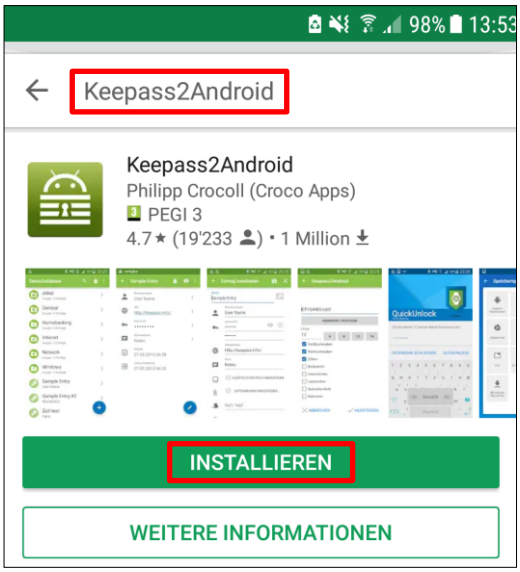
6.1.4 Firefox Add-on Kee installieren

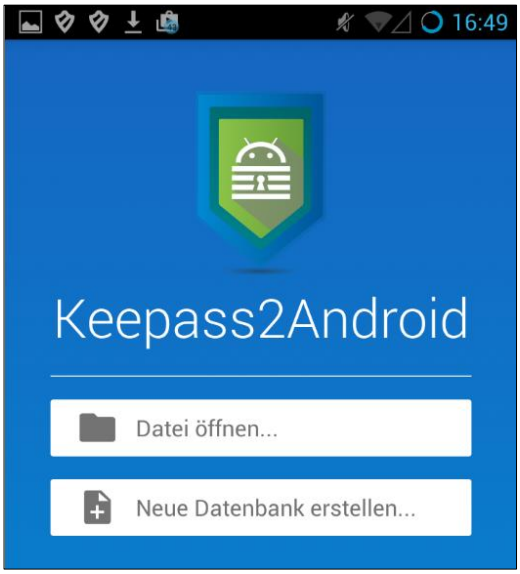
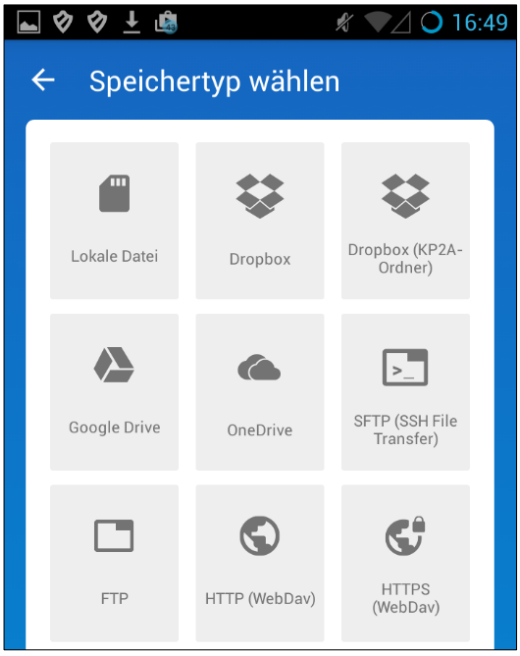
Die Installation des Firefox-Browser-Add-ons Kee macht die Benutzung von KeePass2 komfortabler. Internet-Passwörter können damit einfacher hinzugefügt und verwendet werden.

1. Herunterladen des Plugins KeePassRPC.plgx	
2. KeePassRPC.plgx in das Plugin-Verzeichnis (z.B. c:\Programme (X86)\KeePass Password Safe 2\plugins) kopieren	
3. Add-on Kee suchen und Installieren klicken	
4. KeePass2 starten und die Passwortdatenbank mit dem Master-Passwort entsperren	
5. Authorisierungscode auslesen	

6. Zum Firefox wechseln und Authorisierungscode eingeben	
7. Verbinden klicken	
8. Fertig	

6.2 Anleitung Keepass2Android

1. Vorhandene Schlüsseldatenbank (z.B. PW.kdbx) auf das mobile Geräte, die SD-Karte oder den Cloud-Speicher-Ordner kopieren	
2. Keepass2Android auf Google Play suchen	
3. Keepass2Android öffnen	

4. Datei öffnen… klicken	
5. Datei lokal oder in Cloud-Speicher-Ordner auswählen	

6.3 Anleitung MiniKeePass

Die Installation von MiniKeePass auf iOS erfolgt analog der Installation von Keepass2Android.

dsb

datenschutzbeauftragter
kanton zürich

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

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

www.datenschutz.ch
twitter.com/dsb_zh