

Log in – mit Sicherheit !?

Passwörter nerven, Passkeys zu kompliziert, sind
Hardware-Schlüssel die Lösung?

Einleitung

- Sichere Anmeldung an Webseiten
- zweiter Faktor für Anmeldungen
- sicherer weiterer Faktor für Passwortmanager

Geschichte

- 2007 Yubico
- 2015 Nitrokey
- 2016 Onlykey
- ca. 2019 Solokey

Übersicht Hardware Schlüssel

Hersteller	Top-Produkt	FIDO2	FIDO U2F	OTP	GPG	SSH	PIV	Preis
Nitrokey	Nitrokey 5C NFC	x	x	HOTP, TOTP	x	x	x	30-65
OnlyKey	OnlyKey	x	x	TOTP	x	x		50
SoloKeys	Solo 2C+ NFC	x	x		x	x	x	35-45
Yubico	YubiKey 5C NFC	x	x	TOTP, HOTP, Yubico OTP	x	x	x	30-60

Eigenschaften

Hersteller	Ursprungsland	Firmware	Aktualisierbar	Hardware	Besonderheiten
Nitrokey	Deutschland	Open Source	ja	Open Source	
OnlyKey	USA	Open Source	ja		Selbstzerstörung, 24 Accounts, Backup
SoloKeys	Italien	Open Source	ja	Open Source	
Yubico	Schweden + USA	Closed Source	nein	Closed Source	

Verbindungsarten

- USB A
- USB C
- NFC (nicht OnlyKey)
- Lightning (nur YubiKey)

Verwaltung

- Nitrokey App 2*
- OnlyKey App
- Solo2 CLI (GUI in Vorbereitung)
- Yubico Authenticator

* in Debian 13 Repository vorhanden

Unterschied FIDO, OTP, statisches Password

- OTP: sichere Einmalpasswörter
- FIDO U2F: Hardware Schlüssel nur als zweiter Faktor
- FIDO2: Anmelden mittels Hardware Schlüssel
- Statisches Passwort: möglichst lang und komplex

FIDO U2F

- Nur zweiter Faktor (zusätzlich zu Passwort)
- Proprietärer FIDO-Standard
- Keine Biometrieunterstützung
- Benötigt Hardware (z.B. USB-Schlüssel)

FIDO2

- steht für Fast Identity Online
- offener Authentifizierungsstandard
- besteht technisch aus den Komponenten WebAuthn (W3C-Standard) und CTAP2 (Client to Authenticator Protocol)
- ermöglicht passwortlose Authentifizierung oder Zwei-Faktor-Authentifizierung

FIDO2

- USB-Schlüssel, NFC-Chips, Bluetooth-Geräte
- biometrische Authentifizierung (Fingerabdruck auf Smartphone, Face ID auf Laptop usw.)
- Discoverable Credentials (komplette Anmeldedaten auf Key gespeichert)

Passkey

- Passkey erweitert den FIDO2-Standard
- In Cloud speicherbar/synchronisierbar
- Oder gespeichert auf Sicherheitsschlüssel
- Phishing resistant

Zusammenfassung

- Drei Arten der Anmeldung
 - Login + Password + Sicherheitsschlüssel als 2ter Faktor (U2F oder FIDO2)
 - Login + Sicherheitsschlüssel (FIDO2)
 - Nur Sicherheitsschlüssel (FIDO2 Discoverable Credentials)

Anwendungsfälle

- Passwortmanager z.B. KeepassXC
 - als einziger/zusätzlicher Faktor

Webseiten

- Nextcloud
 - FIDO Anmeldung ohne Passwort
 - MFA:Passwort + Schlüssel
- Discord
 - MFA:Passwort + Schlüssel
- GitLab
 - Nur Schlüssel

Weiteres

- Linux lokales Login
 - FIDO2 PAM
- SSH
 - FIDO2
- GnuPG
 - GPG Schlüssel

Links

- <https://support.discord.com/hc/en-us/articles/219576828-Setting-up-Multi-Factor-Authentication>
- <https://developers.yubico.com/SSH/>
- <https://2fa.directory/de/>
- <https://www.yubico.com/works-with-yubikey/catalog/?sort=popular>
- <https://www.yubico.com/works-with-yubikey/catalog/linux/>
- <https://www.ipg-group.com/blog/expertenberichte/fido2-passkey-passwordless>
- <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Passkeys/Kryptografie-hinter-Passkey/kryptografie-hinter-passkey.html>
- <https://misteruber.github.io/YubiKeyWiki/docs/OpenPGP/mailverschluesselung>
- <https://developers.yubico.com/pam-u2f/>
- https://developers.yubico.com/PGP/PGP_Walk-Through.html