FIDO2, Passkeys und Hardware-Sicherheitsschlüssel

Voraussetzungen und Installation (Debian)

Für FIDO2-gestützte SSH-Schlüssel sind ein geeigneter OpenSSH-Client und ein kompatibler Authenticator erforderlich.

```
sudo apt update
```

```
sudo apt install openssh-client libfido2-1
```

Version prüfen:

```
ssh -V
```

Zweck

FIDO2 ermöglicht phishingresistente Authentifizierung mit asymmetrischer Kryptografie. Passkeys sind Anmeldedaten, die auf FIDO-Technologien beruhen und auf Geräten oder in geeigneten Passwortmanagern gespeichert beziehungsweise synchronisiert werden können.

Prinzip

Bei der Registrierung wird ein Schlüsselpaar für den Dienst eingerichtet. Der Dienst speichert den öffentlichen Schlüssel; die private Schlüsselkomponente bleibt beim Authenticator. Bei der Anmeldung wird eine Herausforderung signiert.

Vorteile

- Kein wiederverwendbares Passwort muss an die Website übermittelt werden.
- Die Anmeldung ist an den legitimen Dienst gebunden und schützt dadurch wirksam vor vielen Phishing-Angriffen.
- Geräte-PIN oder Biometrie können den lokalen Zugriff auf den Authenticator schützen.

Hardware-Schlüssel

Ein Hardware-Sicherheitsschlüssel kann FIDO2-Anmeldungen bereitstellen. Einige Geräte unterstützen

zusätzlich andere Funktionen wie PIV oder OpenPGP; diese sind technisch getrennt von FIDO2.

SSH mit FIDO2

Aktuelle OpenSSH-Versionen unterstützen unter passenden Voraussetzungen hardwaregestützte Schlüsseltypen wie `ed25519-sk`. Die Verfügbarkeit hängt von OpenSSH, Betriebssystem und Authenticator ab.

```
ssh-keygen -t ed25519-sk -f ~/.ssh/id_ed25519_sk
```

Der Befehl benötigt einen kompatiblen Authenticator. Vor der Umstellung sicherstellen, dass ein alternativer Zugang verfügbar bleibt.

Wiederherstellung

Vor der ausschließlichen Verwendung von Passkeys müssen Ersatz-Authenticator, Synchronisierung und Wiederherstellungswege geklärt sein. Ein verlorener Sicherheitsschlüssel kann sonst den Zugang zu Konten verhindern.

Zurück zur Übersicht

From:
https://wiki.bluegnu.de/ - **wiki**

Permanent link:
https://wiki.bluegnu.de/doku.php/open:it:secure:fido2

Last update: **2026/11/15 16:36**