Passkeys

Inhaltsverzeichnis

- 1 Funktionsweise
- 2 Typische Einsatzbereiche
- 3 Wichtige Hinweise
- 4 Fazit

Passkeys sind eine phishing-resistente Anmeldemethode auf Basis von FIDO2/WebAuthn. Statt Passwörtern wird ein kryptografisches Schlüsselpaar genutzt, das an die Website (Origin) gebunden ist und gerätegebunden oder synchronisiert vorliegen kann.

1 Funktionsweise

Bei der Registrierung entsteht ein Schlüsselpaar: Der private Schlüssel bleibt auf dem Gerät oder in einem Password-Manager, der öffentliche Schlüssel liegt beim Dienst. Die Anmeldung erfolgt per kryptografischer Challenge statt Passworteingabe.

- **Phishing-Resistenz:** Schlüssel greifen nur für die echte Domain
- **Gerätebindung / Sync:** lokal oder über Ökosysteme synchronisiert
- **Biometrie/PIN:** Freigabe auf dem Gerät

2 Typische Einsatzbereiche

- Login bei Webdiensten und Unternehmens-SSO
- Ersatz oder Ergänzung von Passwort + MFA
- Absicherung privilegierter Konten

3 Wichtige Hinweise

- Recovery und Geräteverlust brauchen klare Fallback-Prozesse.
- Nicht jeder Dienst unterstützt Passkeys bereits vollständig.
- Shared Accounts und alte Apps können Übergangsregeln erfordern.

4 Fazit

Passkeys reduzieren Passwort-Risiken spürbar und gelten als einer der stärksten praxisnahen Wege zu sicherer, benutzerfreundlicher Authentifizierung.