HIRSCH

SICHERHEITS-SCHLÜSSEL SECUREKEY

Passwortlose Authentifizierung

AUTHENTIFIZIERUNG



STARK & PASSWORTLOS

SecureKeys bieten starke, passwortlose Authentifizierung sowie die Standalone-Anmeldung unter Windows 10 – in Kombination mit dem SecureKey Manager.

Mit den SecureKeys von Hirsch können Privatpersonen, Unternehmen sowie Behörden und deren Auftragnehmer Passwörter durch Multi-Faktor-Authentifizierung (MFA) ersetzen – eine sichere, schnelle, skalierbare und kosteneffiziente Anmeldelösung.

Die Schlüssel funktionieren mit Smartphones, Tablets, Laptops und Desktop-PCs sowie mit allen Diensten (z. B. Gmail, Facebook, LinkedIn). Sie sind als USB-A- oder USB-C-Ausführung erhältlich und verfügen über Near Field Communication (NFC) für die kontaktlose Anmeldung.

DIE + PUNKTE

- **DAS PASSWORTPROBLEM LÖSEN** – Kein Passwort mehr erforderlich. Einsatz als zweiter Faktor oder Einbindung in eine Multi-Faktor-Authentifizierung (MFA).
- **INTELLIGENTE ARCHITEKTUR** – Einfache Aktivierung und Registrierung durch den Nutzer. Resistent gegen Phishing-Angriffe und Datenlecks.
- **SCHLÜSSELVERWALTUNG** – Authentifizierung an Standalone-Geräten mit Windows 10. Erhältlich im Paket mit der Software SecureKey Manager.
- **TAA-KONFORM**

SECUREKEY MANAGER

Mit der Software SecureKey Manager konfigurieren Sie unter Windows 10 die Funktionen FIDO2, Einmalpasswort (OTP) und Personal Identity Verification (PIV) Ihres SecureKey.

Mit dem Tool können Sie Typ und Firmware Ihres Sicherheitsschlüssels prüfen oder Seriennummern anzeigen, per OTP ein Shared Secret laden – wie es in der Kryptografie häufig zum Entschlüsseln von Informationen verwendet wird – sowie per PIV digitale Zertifikate laden, PIN/PUK festlegen oder Schlüssel setzen bzw. ändern.

ARTIKELNUMMERN

SecureKey, USB 2.0 und NFC

- **905601:**
  SecureKey USB-A – USB-Typ-A-Stecker
- **905602:**
  SecureKey USB-C – USB-Typ-C-Stecker

FIDO-ZERTIFIZIERTE SICHERHEIT

Alle SecureKeys von Hirsch sind von der FIDO Alliance zertifiziert. Das kryptografische Sicherheitsmodell der Geräte schließt das Risiko von Phishing, Passwortdiebstahl und Replay-Angriffen aus.

Die kryptografischen FIDO-Schlüssel werden auf dem Gerät gespeichert und sind für jede Website eindeutig. Nutzer können darüber also nicht websiteübergreifend verfolgt werden.



TECHNISCHE DATEN

	SECUREKEY	
Merkmal	**USB-A**	**USB-C**
Host-Schnittstelle	USB 2.0 und NFC	
Secure-Element-Schnittstelle	FIDO2, FIDO/U2F, HOTP, PIV	
Kontaktlose Funktionen	PIV für physischen Zutritt	
Unterstützte Betriebssysteme	Windows 10/11, macOS, Linux, ChromeOS, Android	
Abmessungen	52 x 20 x 5 mm	52 x 20 x 6 mm
Gewicht	3 g	4 g
Betriebstemperatur	0 °C bis +40 °C	
Lagertemperatur	-20 °C bis +85 °C	
Anschluss	USB-Typ-A-Stecker	USB-Typ-C-Stecker
Statusanzeige	Amberfarbene LED	
Unterstützte Browser	Chrome, Internet Explorer, Edge, Safari, Firefox	
Unterstützte Anwendungen	SecureKey Windows Login	
Garantie	12 Monate	
Herkunftsland	Kambodscha	
ZERTIFIZIERUNGEN		
Systeme/Normen	FIDO Universal 2nd Factor (U2F), FIDO2	
Regulatorisch/Umwelt	CE, FCC	
BESTELLINFORMATIONEN		
Artikelnummer	905601	905602

DIE SECURE-IDENTITY-REIHE		
SECUREPASS	**SECUREKEY**	SECUREKEY GOV
		

fpr_SECUREKEY - DE - 20/11/2026 - Unverbindliche Angaben, Änderungen vorbehalten.