HIRSCH

SMARTCARD SECUREPASS ONE

FIPS 140-3 Inside · Dual-Interface-Ausweiskarte

IDENTITÄT



STARK & PASSWORTLOS

Diese einfache, starke Authentifizierung macht Passwörter überflüssig.

Mit den SecurePass ONE Karten von Hirsch können Privatpersonen, Unternehmen sowie Behörden und deren Auftragnehmer Passwörter durch eine sichere, schnelle, skalierbare und kosteneffiziente Anmeldelösung ersetzen. SecurePass ONE Karten 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.

DIE ⊕ PUNKTE

- **KOMFORTABEL** – Passt wie eine Kreditkarte in jede Geldbörse.
- **STARKE MFA** – PIV und FIDO2 bieten starke Authentifizierung und verhindern die Übernahme von Konten.
- **PLATTFORMÜBERGREIFEND** – Funktioniert mit alltäglichen Geräten wie Smartphones, Tablets, Laptops und Desktop-PCs.
- **EINFACHE AUTHENTIFIZIERUNG** – Authentifizierung bei allen Diensten (z. B. Gmail, Facebook, Salesforce, LinkedIn).

FIPS 140-3 INSIDE

Das Secure Element der SecurePass ONE (NXP JCOP4.5 P71) erfüllt FIPS 140-3 Level 3 Inside.

SecurePass ONE basiert auf dem NXP P71D600, der über das FIPS 140-3 Validierungszertifikat #4679 verfügt. Neben FIDO2 stehen PIV- und PGP-Applets zur Verfügung.

ARTIKELNUMMERN

SecurePass ONE, ISO 7816 und NFC

- **905622-1:**
  SecurePass ONE Karte – FIPS 140-3 Dual-Interface-Ausweiskarte

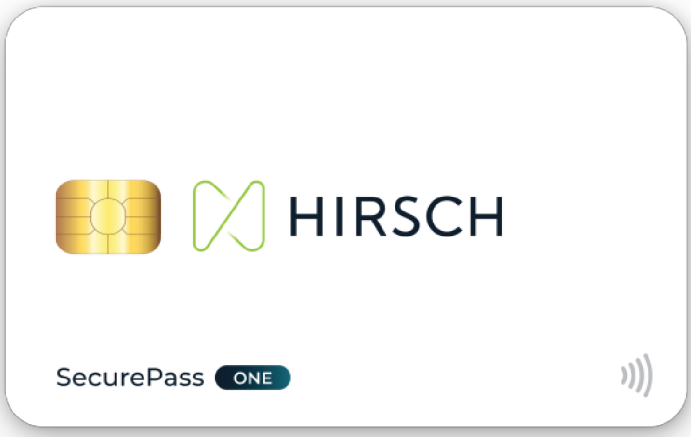
NFC & GERÄTEKOMPATIBILITÄT

SecurePass ONE Karten verfügen über Near Field Communication (NFC) für die kontaktlose Anmeldung an Anwendungen. Sie werden einfach an einen Smartcard-Leser oder an die Rückseite Ihres Smartphones bzw. Tablets* gehalten.

Die Karten funktionieren mit alltäglichen Geräten wie Smartphones*, Tablets*, Laptops** und Desktop-PCs** sowie mit allen Diensten (z. B. Gmail, Facebook, Salesforce, LinkedIn).

* Die Unterstützung hängt von der Antennengröße des Geräts ab; funktioniert ggf. nicht mit allen Smartphones und Tablets.

** Ggf. ist ein Smartcard-Leser erforderlich.



TECHNISCHE DATEN

	SECUREPASS ONE KARTE
Merkmal	**Angabe**
Host-Schnittstelle	ISO 7816 und NFC
Secure-Element-Schnittstelle	FIDO2 (CTAP 2.1), FIDO/U2F, weitere
Algorithmen	SHA256, AES, HMAC, ECDH, ECDSA, RSA
Unterstützte Betriebssysteme	Windows, macOS, iOS, Linux, ChromeOS, Android
Abmessungen	85,6 x 54 mm (Scheckkartenformat ID-1)
Gewicht	5 g
Betriebstemperatur	0 °C bis +50 °C
Lagertemperatur	-20 °C bis +85 °C
Betriebsfrequenz	13,56 MHz
HF-Schnittstelle	ISO 14443 A, Teile 1–4
Typische maximale Lesereichweite	Bis zu 6 cm
Kontaktlose Datenrate	Aktivierung mit 106 kbit/s; Datenübertragung mit bis zu 848 kbit/s
Schreibzyklen	Mindestens 100.000 Zyklen
Datenerhalt	Mindestens 10 Jahre
Material und Oberfläche	PVC weiß/weiß, glänzend, oder PVC-Polyester-Verbundwerkstoff
FIDO-APPLET	
Applet-Eigenschaften	Standards U2F v2, FIDO 2.0 und FIDO 2.1 Kontaktlose Schnittstelle NFC ISO 14443 und kontaktbehaftete Schnittstelle ISO 7816 Digitale EC-Signatur (ECDSA) mit NIST-P256-Parametern (256R1) 32-Bit-Signaturzähler, wird beim Zurücksetzen des Authenticators auf 0 gesetzt Mehrere Konten pro Relying Party Residente Schlüssel (64 Credential-Slots) CredManagement-Befehle
Applet-Optionen	HmacSecret; CredProtect; CredBlob für residente Schlüssel minPinLength: speichert bis zu 4 autorisierte RPs
PIV-APPLET	
Applet-Eigenschaften	Konform zu NIST SP 800-73-4; unterstützt RSA 2048 und 3072 Bit, ECC P-256 und P-384 sowie AES-128, AES-192 und AES-256
Applet-Optionen	Unterstützt die Zertifikate 9C und 9D; unterstützt bis zu 20 ausgemusterte (Retired) Zertifikate

WEITERE APPLETS & SECURE ELEMENT

	SECUREPASS ONE KARTE
Merkmal	**Angabe**
PGP-APPLET	
Applet-Eigenschaften	Konform zur OpenPGP Card Specification 3.4.1; unterstützt RSA 2048, 3072 und 4096 Bit sowie ECC P-256, P-384 und P-521
Applet-Optionen	Unterstützt optionale Datenobjekte (DOs)
SECURE ELEMENT	
Bezeichnung	JCOP4.5 P71
Standard	FIPS 140-3 Level 3 Inside
Beschreibung	NXP Semiconductors bietet mit JCOP ein sicheres Java-Card-Betriebssystem. JCOP4 P71 gewährleistet eine weitreichende Interoperabilität mit Anbietern von Drittanbieter-Applets, Kartenausgebern und allen bestehenden Smartcard-Infrastrukturen.
ZERTIFIZIERUNGEN	
Systeme/Normen	FIDO Universal 2nd Factor (U2F), FIDO2
BESTELLINFORMATIONEN	
Artikelnummer	905622-1

SecurePass ONE basiert auf dem NXP P71D600, der über das FIPS 140-3 Validierungszertifikat #4679 verfügt.

DIE SECURE-IDENTITY-REIHE		
SECUREPASS	SECUREKEY	SECUREKEY GOV
		

HIRSCH
Eisenstraße 2-4, Haus 3
65428 Rüsselsheim
+49 6142 4811950
@ info@hirschsecure.de
hirschsecure.com