HIRSCH

SMARTCARD SECUREPASS DUO

Konvergenter Zugang · Dual-Interface-Karte · MIFARE / DESFire

IDENTITÄT



KONVERGENT & PASSWORTLOS

Diese einfache, starke Authentifizierung macht Passwörter überflüssig.

Die SecurePass DUO Karten von Hirsch bieten ein einziges konvergentes Identifikationsmittel für den physischen und logischen Zugang. Durch die Kombination von passwortloser FIDO2-Authentifizierung mit DESFire-Technologie ermöglicht SecurePass DUO den sicheren Zugang zu Gebäuden, Arbeitsplätzen, Anwendungen und digitalen Diensten – mit nur einer Karte.

Die von der FIDO Alliance zertifizierte SecurePass DUO ersetzt Passwörter durch eine schnelle, skalierbare und kosteneffiziente Authentifizierungslösung. Ihr kryptografisches Sicherheitsmodell hilft, Phishing, Passwortdiebstahl und Replay-Angriffe auszuschließen, und speichert eindeutige FIDO-Anmeldeinformationen sicher auf der Karte.

DIE + PUNKTE

- **KOMFORTABEL** – Passt wie eine Kreditkarte in jede Geldbörse.
- **STARKE MFA** – PIV, PGP 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).

EIN IDENTIFIKATIONSMITTEL FÜR ALLES

Indem SecurePass DUO physischen Zugang, logischen Zugang und moderne Authentifizierung in einem einzigen Identifikationsmittel vereint, vereinfacht sie die Verwaltung von Identifikationsmitteln, erhöht den Komfort für die Nutzer und stärkt die Sicherheit insgesamt.

ARTIKELNUMMERN

SecurePass DUO, ISO 7816 und NFC

- **905622-2:**
  SecurePass DUO Karte – Dual-Interface-Ausweiskarte für konvergenten Zugang

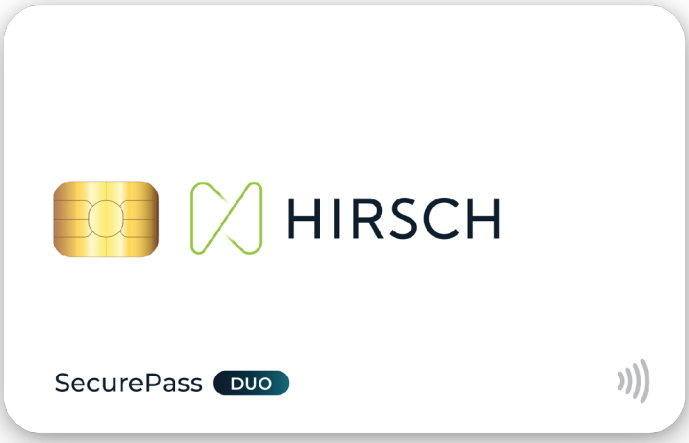
NFC & GERÄTEKOMPATIBILITÄT

SecurePass DUO 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 DUO 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 DUO 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)
DESFIRE-APPLET	
Speichertyp	EEPROM, 8 KByte
Speicherstruktur	Bis zu 28 Anwendungen mit jeweils bis zu 32 Dateien
SECURE ELEMENT	
Bezeichnung	JCOP4.5 P71
Beschreibung	NXP Semiconductors bietet mit JCOP ein sicheres Java-Card-Betriebssystem, das auf mehreren unabhängigen Spezifikationen Dritter basiert, etwa den Java-Card-3.0.4-Spezifikationen, den GlobalPlatform-Kartenspezifikationen, Normen der Internationalen Organisation für Normung (z. B. ISO 7816), EMV (Europay, Mastercard und VISA) und weiteren. Durch die Einhaltung dieser Standards gewährleistet JCOP4 P71 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	905622-2

DIE SECURE-IDENTITY-REIHE		
SECUREPASS	SECUREKEY	SECUREKEY GOV
		

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