HIRSCH

SecureKey GOV

Strong Authentication for Government Agencies

For government and regulated agencies, Hirsch's SecureKey GOV Security Keys meet FIPS 140-3 and NIST guidelines for high assurance strong authentication.

Hirsch's SecureKey GOV Security Keys are the perfect strong near field communication (NFC) authentication device, providing FIPS 140-3 validation and assurance level 3 (AAL3) of NIST SP800-63B guidance for regulatory compliance.

SecureKey GOV Security Keys are perfect for government employees and contractors, as well as for citizens accessing government services, public safety personnel, first responders, and emergency communications teams.
Our security keys are available in two form factors: USB-A and USB-C. Both models feature near field communication (NFC) functionality for contactless sign-on to applications.

Multi-protocol support for FIDO2, FIDO U2F, PIV, HOTP, and WebAuth enables strong multi-factor authentication and removes the necessity for passwords.

Based on public-key cryptography, the cryptographic security model of the devices eliminates the risk of phishing, password theft, and replay attacks. The FIDO cryptographic keys are stored on-device and are unique for each website, meaning they cannot be used to track users across sites.

High-Security Features

Simple and Secure

- No server-side shared secrets to steal
- Protects against phishing, man-in-the middle, and replay attacks
- FIDO Certified

Cost-Effective and User-Friendly

- Lower development and maintenance costs and little-to-no provisioning costs
- Faster time to market and future-proof

Multi-Protocol and Multiple Connectivity

- Supports both contact(USB A/C) and contactless (NFC) use cases
- Multi-protocol FIDO U2F, FIDO2, smart card (PIV), PGP and HOTP support

TAA Compliant

SecureKey GOV Security Keys

Parameter	SecureKey GOV USB-A	SecureKey GOV USB-C
Host Interface	USB 2.0 and NFC	
Secure Element Interface	FIDO2, FIDO/U2F, HOTP, PIV	
Contactless Functionality	FIDO, PGP, Physical Access PIV	
Supported Operating Systems	Windows 10/11, Windows Servers, macOS, Linux, ChromeOS, Android	
Dimensions	52 x 20 x 5 mm	52 x 20 x 6 mm
Weight	3 g	4 g
Operating Temperature Range	-10 °C to 75 °C (14 °F to 167 °F)	
Storage Temperature Range	-20 °C to 85 °C (-4 °F to 185 °F)	
Connector	USB Type A Connector	USB Type C Connector
Status Indicator	Amber LED (FIDO); Green LED (PC/SC) Only over USB	
Reading/Writing Cycles	10 years minimum - 500.000 cycles minimum	
API & Supported Standard	PKCS#11 v2.40, v3.0 PKCS#15 v1.1 Microsoft CSP (CryptoAPI) & KSP/CNG (Next Generation) Apple CTK (CryptoTokenKit) & TokenD X.509 v3, SSL v3, TLS1.3, IPSec	
Supported Signing/Encryption Schemes	PKCS#1 v1.5, v2.1, RSA-OAEP, RSASSA-PSS	
Secure Chip Management	PIN and PUK management	
Organizational Security Policies	SSCD: Secure Signature Creation Device CGA: Certificate Generation Application SCA: Signature Creation Application NR: Non Repudiation	
Supported Browsers	Chrome, Edge, Safari, Firefox	
Supported Applications	SecureKey Windows Login	
Warranty	12 Months	
Country of Origin	Cambodia	

SecureKey GOV Security Keys

Parameter	SecureKey GOV USB-A	SecureKey GOV USB-C
Secure Element		
Name	JCOP4.5 P71D600	
Standard	FIPS 140-3 Level 3	
Symmetric Block Cipher		
AES	supports 128, 192, 256 bits	
Asymmetric Block Cipher		
RSA Key Generation	generates up to 4096 bits	
RSA Signature, cipher/decipher	supports up to 4096 bits	
ECC Key Generation	generates up to 521 bits	
ECC Signature	supports up to 521 bits	
Hashing		
SHA (Hashing) / ECDSA SHA	SHA1, SHA-224, SHA-256, SHA-384, SHA-512	
Certifications		
IP Rating	IP68	
System/Standards	FIDO Universal 2nd Factor (U2F), FIDO2	
Regulatory/Environmental	FIPS 140-3, CE, FCC	
Ordering Information		
Product Part Number	905601-1	905602-1