IDEMIA
PUBLIC SECURITY

Smart Credentials

Smart solutions for securing facilities,
communications, systems, and data

SMART CREDENTIALS BY IDEMIA

A range of solutions for securing both facilities and critical digital assets, including hardware tokens for phishing-resistant multifactor authentication and identity and credentialing access management.

Despite investing extensively in cybersecurity solutions and best practices, hackers and cyber criminals are stealing employees' access credentials with ever more sophisticated—and frequent—phishing attacks.

Phishing deceives employees into sharing their credentials through emails, text messages, or voice messages that pretend to be from a legitimate source. And the damage can be significant, with large organizations standing to **lose up to $15 million per year** to phishing attacks—not to mention the reputational damage and loss of trust that result from a breach.

Certificate-based authentication based on PIV and FIDO2 passkeys offer robust solutions to these human factor vulnerabilities, forming the cornerstone of any **Zero Trust security framework.** Hardware security tokens remain the gold standard for phishing-resistant multifactor authentication (MFA) since the user must have possession of the token in order to use a set of credentials, while FIDO2 passkeys do away with the need for passwords altogether, enhancing user experience while reducing the vulnerabilities associated with password theft.

WHY IDEMIA?

A pioneer in meeting the FIPS 201 standard for personal identity verification (PIV) laid out in Homeland Security Presidential Directive 12 (HSPD-12), **IDEMIA has been a leading provider of PIV and CAC cards** to the U.S. federal government and large enterprise customers for over 20 years. While multiple vendors claim to support the FIPS 201 (PIV) standard, only two have secure modules listed with active certification on the GSA's **Approved Products List** (APL)—and one of them is IDEMIA.

IDEMIA offers U.S.-based manufacturing and centralized print bureau services for personalization and fulfillment of PIV cards, delivering over **70 million cards to date.**

WHY PIV CARDS?

These versatile cards offer a robust solution for:

- Secure photo ID
- Building access (Prox, DESFire®, MIFARE, and LEAF supported)
- Tap-and-Go Mobile Authentication via NFC
- Workstation and Network Access
- Email and Document Signing
- Email and File Encryption
- FIDO2 Authentication

ID-ONE PIV® TECHNICAL DATA

Certifications	FIPS 140-3 validated: Certificate #5024 (Level 2) and Certificate #5027 (Level 3)	**Minidriver Support**	IDEMIA Minidriver available for download from Microsoft Update Catalog website.
Cryptographic Algorithms	ECDSA: Curve P-224, P-256, P-384, P-521 ECDH: Curve P-224, P-256, P-384, P-521 RSA: 1024 and 2048-bit, 3072 AES: 128, 192, 256 bit Keys (CBC and ECB) OATH (TOTP and HOTP) 3TDES: 3 Key (CBC and ECB) (Legacy only)	**Card Body**	Long-life composite PET-F/PVC plastic meeting physical and durability requirements specified in the FIPS 201 standard. Supports variety of security features up to Level 3 (forensic), and laser engraving options.
Retired Keys	Supports 20+ on-card retired key management keys (aka archived decryption keys) with associated X509 certificates.	**Communication Protocols**	T=1 (ISO/IEC 7816-3) T=CL (ISO/IEC 14443 Type A) Supports extended length APDU for faster data exchange
On-card Fingerprint Verification	Takes less than 70 milliseconds for a positive match.	**Operating Voltage (contact)**	Class A (5V), Class B (3V), and Class C (1.8V)
Secure Channel	PIV secure messaging ECC P-256, P-384, P-521 with VCI (Virtual Contact Interface) for mobile device interfacing. Global Platform SCP-03 with confidentiality and integrity of both incoming and outgoing data (secure channel mode 33).	**Communication Speed**	Up to 625,000 bps over the contact interface with a 5MHz clock Up to 848,000 bps over the contactless interface
Custom Extensions	Supports additional data objects with custom access conditions as needed.	**CMS Compatibility**	Out-of-the-box support for most widely used commercial CMS products.
Proximity Support (Optional)	Optionally supports 125 KHz proximity technology on the CIV (Commercial Identity Verification) card, compatible with most widely-used proximity technologies and formats (HID®, CASI®, Indala®, Honeywell®)	**MIFARE®, DESFire® Support (Optional)**	Options (for CIV cards only) include MIFARE® Classic (1K, 4K), MIFARE® Plus (2K, 4K), DESFire® (2K, 4K, 8K, 16K, 24K, 32K) LEAF Standard or Custom on DESFire®.

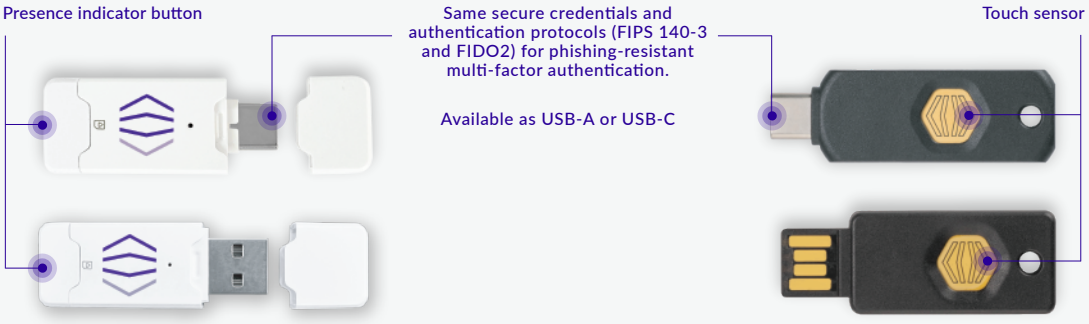
IDEMIA is certified
ISO 9001: 2008
ISO 14001: 2004

FIND YOUR FORMAT: USB SECURITY KEYS

While the bedrock of FIPS 201-compliant (PIV) authenticators remains the PIV card, there is an increasing demand for USB security keys because of their "plug-and-play" versatility for logical access.

IDEMIA now offers the ID-One Key™ range to make increasing your cybersecurity posture as convenient as possible.

Both the function-rich ID-One Key™ Bolt and the budget-friendly ID-One Key™ Go have PIV-certified cryptographic modules, while the ID-One Key™ Bolt is also FIDO2-certified, with both able to hold up to 120 FIDO2 passkeys.



ID-ONE KEY™ GO

Cost-effective solution for strengthening cybersecurity posture.

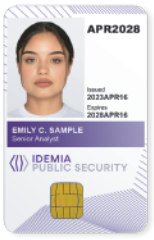
- Integrated chip reader does away with need for a PIV card reader.
- Uses button press to confirm user presence.

ID-ONE KEY™ BOLT

Feature-rich version with sleek form factor.

- Solid-state processor
- Waterproof and dust-resistant
- NFC-capable
- Uses touch sensor to detect user presence.

FEATURE COMPARISON WITH ID-ONE PIV CARDS

	CREDENTIALS	NFC?	PRESENCE DETECTION
 ID-One PIV® Card	LOGICAL ACCESS PIV (PKI) credential + FIDO Passkey(s) PHYSICAL ACCESS 125 KHz Prox® DESfire® Ev3 LEAF MIFARE®	Yes	N/A
 ID-One Key™ Bolt	PIV (PKI) credential + FIDO Passkey(s)	Yes	Touch sensor
 ID-One Key™ Go	PIV (PKI) credential + FIDO Passkey(s)	No	Button press

ID-ONE KEY™ TECHNICAL DATA

certified
ISO 9001: 2008
ISO 14001: 2004

	ID-One Key™ Go 	ID-One Key™ Bolt 
Interfaces	USB Type-A, USB Type-C	USB Type-A, USB Type-C Contactless (NFC)
OS Compatibility	Microsoft Windows® 10 (32 & 64 bits) Microsoft Windows 11 (64bits) Microsoft Windows 11 (ARM64-based PC) Microsoft Windows® Server 2022, 2025 Linux® Ubuntu (20.04 LTS, 22.04 LTS, 24.04 LTS) macOS (version 12 to 14) iOS 16+ Android 13+	Microsoft Windows® 10 (32 & 64 bits) Microsoft Windows 11 (64bits) Microsoft Windows 11 (ARM64-based PC) Microsoft Windows® Server 2022, 2025 Linux® Ubuntu (20.04 LTS, 22.04 LTS, 24.04 LTS) macOS (version 12 to 14) iOS 16+ Android 13+
Minidriver	Windows mini driver currently on the Microsoft Update Catalog IDEMIA – SmartCard Driver	Windows mini driver currently on the Microsoft Update Catalog IDEMIA – SmartCard Driver
Certifications	FIPS 201 Certification FIPS 140-3 Certification (pending) FIDO 2.1 Certification CTAP 2.1 (Level 2) and U2F (Level 2) CE, FCC	FIPS 201 Certification FIPS 140-3 Certification (pending) FIDO 2.1 Certification CTAP 2.1 (Level 2) and U2F (Level 2) IP68 certified (dust proof, waterproof) CE, FCC and NFC Forum
Cryptographic Algorithms: PIV applet	ECDSA: Curve P-224, P-256, P-384, P-521 ECDH: Curve P-224, P-256, P-384, P-521 RSA: 2048-bit, 3072 , 4096 AES: 128, 192, 256-bit Keys (CBC and ECB) 3TDES: 3 Key (CBC and ECB) (Legacy only)	ECDSA: Curve P-224, P-256, P-384, P-521 ECDH: Curve P-224, P-256, P-384, P-521 RSA: 2048-bit, 3072 , 4096 AES: 128, 192, 256-bit Keys (CBC and ECB) 3TDES: 3 Key (CBC and ECB) (Legacy only)
FIDO applet	ECC P256, 284 AND 521.	ECC P256, 284 AND 521.
Dimensions	USB-A: 49.5mm × 17.7mm × 8.0mm USB-C: 45.9mm × 17.7mm × 8.0mm	USB-A: 48.2mm x 18.3mm x 4.1mm USB-C: 50.4mm x 16.4mm x 5mm
Weight	USB-A: 8.1 g ± 1.0 g USB-C: 6.2 g ± 1.0 g	USB-A: 4g USB-C: 5g
Operating Temp.	0 - 65°C (32°F ~ 149°F)	0°C - 40°C (32°F ~ 104°F)
PIN Length	Support for numeric PIN and Alphanumeric passphrase up to 16 characters	Support for numeric PIN and Alphanumeric passphrase up to 16 characters
Credential Capacity	Dependent on ECC key encryption strength and PIV/CIV applet personalization	Up to 295 FIDO Credentials Dependent on ECC key encryption strength and PIV/CIV applet personalization