IDEMIA ID-ONE PIV® TECHNICAL SPECIFICATIONS

CERTIFICATIONS

- FIPS 140-2 Certification: Level 2 (CIV), and Level 3 (SPE)
- Common Criteria: EAL 5+

CRYPTOGRAPHIC ALGORITHMS

- ECDSA: Curve P-224, P-256, P-384, P-521
- ECDH: Curve P-224, P-256, P-384, P-521
- RSA: 2048-bit, 3072
- AES: 128, 192, 256 bit Keys (CBC and ECB)
- 3TDES: 3 Key (CBC and ECB) (Legacy only)

RETIRED KEYS

- Supports up to 20 on-card retired key management keys (aka archived decryption keys) with associated X509 certificates.

ON-CARD FINGERPRINT VERIFICATION

- Takes less than 100 milliseconds for a positive match.

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 secure channel modes "01," "03," and "33."

CUSTOM EXTENSIONS

- Supports additional data objects with custom access conditions as needed.

PROXIMITY SUPPORT (OPTIONAL)

- Optionally supports 125 KHz proximity technology on the PIV card, compatible with most widely-used proximity technologies and formats (HID®, CASI®, Indala®, Honeywell®)

MIFARE®, DESFire® SUPPORT (OPTIONAL)

- Options include MIFARE® Classic (1K, 4K), MIFARE® Plus (2K, 4K), DESFire® (2K, 4K, 8K, 16K, 24K, 32K)
- LEAF Standard or Custom on DESFire®.

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.

MINIDRIVER SUPPORT

- IDEMIA Minidriver available for download from Microsoft Update Catalog website.

COMMUNICATION PROTOCOLS

- T=1 (ISO/IEC 7816-3)
- T=CL (ISO/IEC 14 443 Type A)
- Supports extended length APDU for faster data exchange

COMMUNICATION SPEED

- Up to 625,000 bps over the contact interface with a 5MHz clock
- Up to 848,000 bps over the contactless interface

OPERATING VOLTAGE

- Class A (5V), Class B (3V), and Class C (1.8V)

CMS COMPATIBILITY

- Out-of-the-box support for most widely used commercial CMS products.

IDEMIA is certified
ISO 9001: 2008
ISO 14001: 2004