



IDProtect Key v1—LASER Technical Brief

Delivery Form Factor:

- Full speed USB 2.0
- Activity LED
- Dimensions: 3.65(L) x 1.70(W) x 0.70(H)
- Weight: 5g
- Water resistant
- Tamper proof

Key Memory:

- 72K EEPROM
- Typically More than 500,000 Write/Erase Cycles at a Temperature of 25°C
- 10 Years Data Retention

Microcontroller Peripherals:

- ISO 7816 Controller (compliant with T=0 or T=1 protocol)
- Programmable Internal Oscillator (Up to 40 MHz for CPU and Crypto Accelerator)
- Random Number Generator (RNG)
- Hardware DES and Triple DES DPA/DEMA Resistant
- Checksum Accelerator
- 32-bit AdvX™ Cryptographic Accelerator for Public Key Operations with GF (2n)

Microcontroller Security:

- Dedicated Hardware for Protection Against SPA/DPA Attacks
- Advanced Protection Against Physical Attack, Including Active Shield
- Environmental Protection Systems
- Voltage Monitor
- Frequency Monitor
- Light Protection
- Temperature Monitor
- Secure Memory Management/Access Protection (Supervisor Mode)

Microcontroller Security Certification:

- CC EAL4+
- VISA
- CAST

Operating System Specification:

- ISO/IEC 7816
- PC/SC architecture compliant
- Sun Microsystems Java Card 2.2.2
- Global Platform 2.1.1

Supported Signal and Transmission Protocols:

- ISO/IEC 7816-3 and ISO/IEC 7816-4
- T=0 (default) / T=1
- PPS speed enhancement

GlobalPlatform Functionality Supported by Operating System:

- Life cycle management
- Security domains (including DAP verification, Delegated Management and Supplementary Security Domains)
- Secure channel protocols (SCP 01 and 02 supported)

Operating System Security Features:

- Key and PIN value encryption in stored memory
- Key and PIN object integrity check in stored memory
- Key and PIN erasure on card termination

Operating System Memory Management:

- Garbage collection
- Memory compaction

Java Card Cryptography API:

- AES (Key lengths: 128, 192, 256 bits)
- DES and 3DES
- RSA (up to 2048 bit key lengths)
- RSA—CRT
- RSA on-board key generation (Key length: 512 to 2048 bits in 32 bit increments)
- SHA-1 and SHA-256
- MD-5

Operating System Certification:

- Validated FIPS 140-2
- Designed in accordance with Common Criteria principles

LASER supports (on key PKI application):

- Microsoft Crypto API (CAPI)
- Microsoft Crypto API : Next Generation (CNG)
- Microsoft ILM (optional)
- PKCS# 1, 7, 10 and 11 (PKCS#15 optional)
- X.509 version 3
- Ability to store certificate chains
- USER and Admin PIN (Admin PIN, Admin card and remote unlock capabilities configurable)
- PIN counters, policies, history and complexity rules stored on-key not host

Operating System:

- Windows 7, Vista, XP, 2000/2003/2008/2008 R2 Server Smart Card Logon (x86 and x64 versions available)
- Microsoft certified Cryptographic Service Provider (CSP) or Minidriver. Certified minidriver available through Windows Update.
- LINUX PKCS#11 library, Mac OSX PKCS#11 middleware available (OSX >10.4)

IDProtect Client highlights:

- Certificate formats supported: PFX, P12, P7B and CER
- VPN and Remote Terminal Services support
- Encrypted communication between middleware and USB key
- Secure key injection supported
- Biometric match-on-card support—Precise Biometrics BioMtach (optional)

Athena solution supports (partial list):

- Windows Smart Card Logon, Windows Mail, Microsoft Outlook and Outlook Express, mail signing and encryption (S/MIME), Internet Explorer, Netscape, Mozilla Firefox, Mozilla Thunderbird, IIS SSL, OpenSSL, IPSec/IKE, Run as Microsoft CA root certificate storage, Adobe Acrobat, Microsoft VPN, Checkpoint VPN, Cisco VPN, Citrix, Lotus Notes, Novell, PGP, SSH,