IDProtect Key v2 with LASER — secure USB multi-factor authentication

Multi-Factor Authentication

As organisations continue to realise the benefit of the digital landscape it is increasing importance to ensure access to e-resources that are tightly controlled.

Athena's multi-factor authentication technology enables issuers to incorporate 'something the user knows', 'something the user has' and 'something the user is' within a secure package and deploy it seamlessly with existing systems.

Athena's IDProtect Key v2 loaded with LASER (Athena's on-card PKI application) provides a complete multi-factor authentication solution within a convenient USB form factor.

Making Multi-factor Authentication Truly Portable

Boasting a full speed USB 2.0 interface, single chip architecture, ISO IP58 and industry security certification, such as FIPS and CommonCriteria, means IDProtect Key v2 LASER is the ideal platform deploying truly portable digital security solutions.

MS CAPI/CNG, PKCS#11, PC/SC and ILM support - Ready for PKI

Each IDProtect Key is delivered with Athena's state of the art middleware—IDProtect Client—which in conjunction with IDProtect Key v2 provides PKCS#11, PC/SC, Microsoft CAPI/ CNG and optionally Microsoft ILM/FIM support.

Technology Options

IDProtect Key can also support the latest biometric Match-On-Card technologies and integrate with Microsoft ILM/FIM architectures.

Take advantage of IDProtect Key v2 multi-application architecture by loading other applications pre- or post-issuance. Either source your own Java Card application or use one of Athena's — the choice is yours. Through Java Card and GlobalPlatform compliance applications can be added securely to IDProtect Key v2 at any time. Athena can offer ICAO, IAS ECC, PIV and payment applications to expand the possible uses of the key.

Microsoft Support with IDProtect Client

With support for Microsoft's Cryptography API (CAPI) and Cryptography API: Next Generation (CNG) through the certified Athena Crypto Service Provider (CSP) or Minidriver, IDProtect Client seamlessly integrates the IDProtect Key v2 with Microsoft Windows applications including Outlook, Internet Explorer as well as Windows 7, Vista, XP, Server 2003/2008/2008 R2 Smart Card Logon, VPN, IPSec/IKE and Remote Terminal Services.

Athena supports:

LINUX and Mac Support

IDProtect Key v2 can also be supplied with PKCS#11 and TokenD middleware for LINUX and Mac OSX systems (including 10.5 and 10.6 TokenD for both Intel and PPC platforms).

Technical Highlights

- ISO IP58 certified
- FIPS 140-2
- ISO 7816
- Full speed USB 2.0 and USB 1.1
- Java Card 2.2.2
- Global Platform 2.1.1
- DES and 3DES
- RSA
- AES
- SHA-1
- SHA-256
- SHA-384
- SHA-512
- MS-CAPI/CNG
- PKCS# 1, 7, 10 and 11
- X. 509 version 3
- Windows, Linux and Mac
- Microsoft ILM/FIM (optional)
- Biometric Match-On-Card (optional)

athena Smartcard

IDProtect Key v2 LASER Technical Specification

Delivery form factor:

- Full speed USB 2.0 and USB 1.1
- ISO IP58 certified (Water Resistant)
  - Dust Protected
  - Continuous Immersion Water Resistant
  - Tamper Evident
- Secure single chip architecture
- Activity LED
- Dimensions: 3.65(L) x 1.70(W) x 0.70(H)
- Weight: 5g
- USB connector cap

Silicon Memory:

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

Silicon 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 Cryptographic Accelerator for Public Key Operations with GF(2n)

Silicon 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)

Silicon Certification:

- CC EAL4+
- VISA
- CAST

Operating system specification:

- ISO/IEC 7816
- Sun Microsystems Java Card 2.2.2
- Global Platform 2.1.1

Signal and Transmission protocols supported:

- ISO/IEC 7816-3 and ISO/IEC 7816-4
- T=0 (default) and T=1
- PPS speed enhancement
- Multiple Logical Channels (base + 3)

Global Platform functionality supported:

- Life cycle management
- Security domains (including DAP verification, Delegated Management and Supplementary Security Domains)
- Secure channel protocols (SCP 01, 02 and 03 supported)

Operating system security:

- 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 TDES
- RSA (key lengths: up to 2048 bits)
- RSA on-card key generation (key lengths: up to 2048 bits)
- ECC FP
  - JC API key lengths supported: 112, 128, 160, 192
  - Application key lengths supported: 256, 384, 521
- ECC FP key generation
  - JC API key lengths supported: 112, 128, 160, 192
  - Application key lengths supported: 256, 384, 521
- EC-DH key agreement
  - JC API key lengths supported: 112, 128, 160, 192
  - Key lengths supported: 256, 384 and 521
- SHA-1, -256, -384 and -512

Operating system certification:

- FIPS 140-2 validated
- CommonCriteria EAL4+

LASER supports (on key PKI application):

- Microsoft Crypto API: CAPI and Next Generation (CNG)
- Microsoft ILM (optional)
- PKCS# 1, 7, 10 and 11 (PKCS#15 optional)
- X.509 version 3
- PC/SC
- Ability to store certificate chains (limited only by silicon memory capacity)
- 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

IDProtect Key v2 LASER and IDProtect Client solution provides:

- Microsoft certified Cryptographic Service Provider (CSP) or Minidriver. Certified minidriver available through Windows Update.
- LINUX PKCS#11 library
- Mac OSX & PKCS#11 middleware (including 10.5 and 10.6 TokenD for both Intel and PPC platforms)
- Microsoft Outlook, Internet Explorer as well as Windows 7, Vista, XP, 2000/2003/2008/2008 R2 Server Smart Card Logon (x86 and x64 versions available)

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 PKI solution supports (partial list):

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

Asia
1-14-16, Motoyokoyama-cho
Hachioji-shi
Tokyo, 192-0063
Tel: +81-426-60-7555
Fax: +81-426-60-7106

North America
20380 Town Center Lane
Suite 240
Cupertino, CA 95014
Tel: +1 408 786 1028
Fax: +1 408 608 1818

LATAM & Iberia
CL. Padre Jesús Ordoñez,
5 1-B, 28002,
Madrid, Spain
Tel: +34 9 1564 4651
Fax: +34 9 1564 4651

EMEA & International
Westpoint
4 Redheughs Rigg
Edinburgh EH12 9DQ
Tel: +44 131 208 2102
Fax: +44 131 777 8150

Web: www.athena-scs.com — Email: sales@athena-scs.com

athena Smartcard