IDProtect LASER

Athena, with its extensive experience of smart card standards, has released the IDProtect LASER range for Identity projects requiring a secure silicon platform with up to 80k EEPROM and PKI support.

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

As a modern cryptographic smart card, IDProtect LASER is supported by middleware for PKCS#11, Microsoft CAPI/CNG and optionally Microsoft ILM allowing easy integration with leading PKI and security solutions.

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 LASER can seamlessly integrate with Microsoft Windows applications including Outlook, Internet Explorer as well as Windows 7, Vista, XP, Server 2003/2008/2008 R2 Smart Card Logon, VPN, and Remote Terminal Services.

IDProtect LASER can 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).

IDProtect LASER can be used 'off the shelf' or loaded with other applications to satisfy the requirements of the most demanding projects.

Technology Options

IDProtect LASER also optionally supports the latest biometric Match-On-Card technologies and Microsoft ILM/FIM architectures. IDProtect LASER is available in contact, contactless or dual interface form factors.

Take advantage IDProtect LASER's multi-application architecture by securely loading applications pre– or post-issuance using widely available load tools.

IDProtect LASER platforms also offer IDL (ISO 18013), ICAO, IAS ECC applications on board if required. Additionally NIST PIV and payment applications could be added to further expand the possible uses of the card.

Technical Highlights

- Multiple silicon vendors
- Up to 80k EEPROM
- ISO 7816
- ISO 14443 Type B (platform dependent)
- Java Card™ 2.2.2
- GlobalPlatform™ 2.1.1
- FIPS 140-2 certified
- Common Criteria SSCD
- Security Domain support
- Memory management
- Multiple Transmission Protocols
- DES and 3DES
- RSA
- ECDSA FP
- DH (ECDH and DH)
- AES
- SHA-1
- SHA-224 (EC_FP)
- SHA-256, 384 and 512
- PKI on-card application (PKCS#11 and MS-CAPI)
- Athena middleware (MS Windows, LINUX and Mac OSX)
- Additionally ICAO Doc 9303, IDL (ISO 18013) and IAS ECC also on card
- NIST PIV and Payment (Optional)
- Biometric Match-On-Card Application (Optional)

Silicon Hardware features

- Enhanced 8/16-bit CPU cores
- Up to 80 Kbytes of User EEPROM
- Up to 30-year data retention at 25°C
- Enhanced crypto-processor for public key cryptography
- Hardware security enhanced DES accelerator
- 2.7 V to 5.5 V supply voltage ranges
- Power-saving Standby state
- Contact assignment compatible with ISO/IEC 7816-3 standards

Silicon Contactless features (platform dependent)

- Complies with ISO/IEC 14443 type B standards
- RFUART (RF universal asynchronous receiver transmitter) up to 848 Kbits/s

Silicon Security features

- Active shield
- Monitoring of environmental parameters
- Protection mechanisms against faults
- True random number generator (TRNG)
- ISO 3309 CRC calculation block
- Memory protection unit (MPU)
- Unique serial number on each die

Silicon Certification

- Up to CommonCriteria EAL 6+
- EMVCo approved
- ZKA
- FIPS 140-2

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
- PC/SC architecture compliant
- T=0 (default)
- T=1
- T=CL (platform dependent)
- PPS speed enhancement

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)
- Supplementary Logical Channels

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

Supported Cryptography

- AES (Key lengths: 128, 192, 256 bits)
- DES and 3DES (2 and 3 Keys)
- RSA
  - JC 2.2 key lengths: up to 2048
  - JC 3.0 key lengths: 3072, 4096
- Elliptic Curves (EC_FP)
  - JC 2.2 key lengths: 160, 192
  - JC 3.0 key lengths: 224, 256, 384
  - Proprietary key lengths: 521
- On-card key generation
  - RSA
  - EC_FP
- Key Agreement
  - DH
  - ECDH
- Hash Computation
  - SHA-1
  - SHA-224 (EC_FP)
  - SHA-256
  - SHA-384
  - SHA-512

Operating system certification

- FIPS 140-2
- CommonCriteria SSCD-PP in progress

PKI support

- Microsoft Crypto API (CAPI)
- Microsoft Crypto API : Next Generation (CNG)
- Microsoft ILM/FIM (optional)
- PKCS# 1, 7, 10 and 11 (2.20)
- PKCS#15 optional
- X.509 version 3

PKI Middleware support (IDProtect Client)

- Microsoft certified Cryptographic Service Provider (CSP) or Minidriver. Certified minidriver available through Windows Update.
- LINUX and Mac OSX PKCS#11 libraries available (OSX > 10.4)
- Microsoft Outlook, Internet Explorer as well as Windows 7, Vista, XP, 2000/2003/2008/2008 R2 Server Smart Card Logon
- VPN
- Remote Terminal Services
- Biometric match-on-card support (optional)

Support Applications (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, SSH

On-card applications

- PKI
- IDL (ISO 18013 compliant)
- ICAO
- IAS ECC

Optional Biometric application

- Biometric match-on-card algorithms available

Optional applications

- NIST PIV
- Payment

Asia
1-14-16,
Motoyokoyama-cho
Tokyo, 192-0063
Tel: +81 426 607 555
Fax: +81 426 607 106

North America
20380 Town Center Lane
Suite 240
Cupertino, CA 95014
Tel: +1 866 359 2273
Fax: +1 408 608 1818

LATAM & Iberia
CL. Padre Jesús Ordoñez
5 1-B, 28002,
Madrid, Spain
Tel: +34 915 644 651
Fax: +34 915 644 651

EMEA & International
Alba Centre Livingston.
EH54 7EG. UK.

Tel: +44 131 208 1202
Fax: +44 131 777 8150

Poland & Central Europe
ul. Kasprowicza 8a/4
31-523, Kraków, Poland
Tel: +48 602 315 641
Fax: +48 123 414322

www.athena-scs.com
sales@athena-scs.com