Athena IDProtect v3

Cryptographic Java Card™ Platform for Identity Management

Athena, with its extensive experience of smart card standards, has released IDProtect v3 for identity projects based on its Java Card™ Operating System.

Benefiting from the unique modular and portable design of its OS755 Java Card™ Platform, Athena has tailored IDProtect v3 for the identity market, incorporating the latest specifications from Java Card™ and GlobalPlatform™ and making available a range of accompanying applications.

The products benefit from Athena' expertise and could be used in any cross market implementation (ID and Finance, Finance and Loyalty, Mobile and Finance).

Additional applications

By loading additional applications - pre or post issuance - Card Issuers can instantly change the services offered by IDProtect v3. Athena has a range of optimised applications providing ICAO, IAS-ECC, PIV, PKI and Biometric functionality. Alternatively a Card Issuer can develop their own Java Card application and load it using the features offered by Java Card and GlobalPlatform open standards.

ICAO: Athena ICAO provides support for ICAO Doc 9303, Machine Readable Travel Documents specification and implements both Basic Access Control (BAC), Extended Access Control (EAC), Active Authentication (AA) and Logical Data Structures (LDS).

IAS-ECC: Athena IAS-ECC provides support for ICAO Doc 9303, SIS-CEN/TS 15480-1:2007, SIS-CEN/TS 15480-2:2007 and IAS ECC Identification Authentication Signature European Citizen Card Revision: 1.0.1

PIV: Athena PIV card application and middleware provides NIST certified support for Federal Information Processing Standard (FIPS) 201 and implements PIV optional data objects; Card Holder Facial Image, Card Holder Printed Information, X.509 Certificate for Digital Signature, X.509 Certificate for PIV Key Management and X.509 Certificate for Card Authentication

PKI: Laser, Athena's PKI card application, and its associated middleware provides PKCS#11 and Microsoft CAPI support and can be easily integrated with leading PKI and network security solutions. Available as either a Crypto Service Provider (CSP) or Minidriver Athena Laser and its middleware seamlessly integrates with Microsoft Windows applications including Outlook, Internet Explorer as well as Windows Vista, XP, 2000/2003/2008/2008 R2 Smart Card Logon, VPN, Remote Terminal Services and many other smart card aware software packages. LINUX library and Mac installation options are also available (10.5 and 10.6 TokenD for both Intel and PPC platforms)

Athena Laser supports:

Precise Biometrics BioMatch™: BioMatch adds finger print matching at issuance or post issuance and is compliant with the Java Card Forum Biometry API. The finger print template size is <1000 bytes/fingerprint with a False Acceptance Rate (FAR) of 1:1,000,000 and False Rejection Rate (FRR) of 1:100.

IDProtect v3 Highlights	
ISO 7816	•
Java Card™ 2.2.2	•
GlobalPlatform™ 2.1.1	•
FIPS 140-2	•
Security Domain support	•
Memory management	•
Transmission Protocols	T=0 (default) and T=1
DES	•
TDES	•
RSA	•
AES	•
ECC	•
SHA-1	•
SHA-256	•
ICAO	Optional
IAS-ECC	Optional
PIV applet	Optional
PKI applet	•
Precise Biometrics BioMatch™ API	Optional

athena Smartcard

IDProtect v3 Technical Specification

Silicon General:
- Low Power Idle and Power-down Modes
- Bond Pad Locations Conforming to ISO 7816-2
- ESD Protection to ± 6000V
- Operating Ranges: 2.7 to 5.5V

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

Silicon Peripherals:
- ISO 7816 Controller (compliant with T=0 and T=1 protocol)
- Programmable Internal Oscillator (Up to 30 MHz for AdvX and 30 Mhz for internal CPU Clock)
- Random Number Generator (RNG)
- Hardware DES and Triple DES DPA/DEMA Resistant
- Checksum Accelerator
- 32-Bit Cryptographic Accelerator (AdvX for Public Key Operations)

Silicon Security:
- Dedicated Hardware for Protection Against SPA/DPA/SEMA/DEMA Attacks
- Advanced Protection Against Physical Attack, Including Active Shield, EPO, CStack Checker, Slope Detector, Parity Errors
- Environmental Protection Systems
- Voltage Monitor
- Frequency Monitor
- Temperature Monitor
- Light Protection
- Secure Memory Management/Access Protection (Supervisor Mode)

Silicon Certification:
- CC EAL 5+
- 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
- T=1
- 3 Supplementary Logical Channels
- PPS speed enhancement

GlobalPlatform Functionality Supported:
- 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:
- 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 Functions:
- 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
- SHA-256

Operating System Certification
- FIPS 140-2 Level 3

Application Options:
- ICAO (BAC+EAC+AA+LDS)
- IAS-ECC
- PIV + middleware
- Precise Biometrics BioMatch API

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