



Highlights:

- Java Card 2.2.1
- Global Platform 2.1.1
- ISO/IEC 7816-1,2,3,4,5
- 67k user available EPPROM
- 8k RAM
- RSA Standard and CRT 1024-2048 bit with on-card key generation
- FIPS 186 certified Random Number Generator
- AES 256
- DES
- 3DES
- SHA-1
- SHA-256
- MD5
- CAPI
- PKI



Java Card™ is a trademark of Sun Microsystems, Inc. in the United States and other countries.

GlobalPlatform™ is a trademark of Global Platform Inc.

Athena OS755 (IDProtect) Overview



Java promises write once, run anywhere capability.

Athena OS755 - Java Card™ technology and GlobalPlatform™ operating system - fulfils that promise for the smart card industry.

Athena's OS755 (IDProtect) is built to give you flexibility and security in the way you work: a blank canvas on which to create smart card products for all market sectors. Central to Athena OS755 (IDProtect) is its compliance with the Java Card™ and GlobalPlatform™ standards; multiple compliant Java Card™ applets from any source will run securely on Athena OS755 (IDProtect) enabled Atmel AT90SC25672RCT silicon.

Applets can be securely loaded, disabled and deleted post issuance thanks to GlobalPlatform™ compliant Issuer Security Domain implementation.

From the outset OS755 (IDProtect) has been built with security in mind. It employs a range of measures to ensure the software and data integrity of the card, such as self tests, application firewall, velocity checking, masking cryptographic operations and storing keys securely.

Athena uses its RapidPort architecture to ease the process of porting the system to different silicon platforms, including contactless, meaning it is already available on various devices from leading manufacturers.

Technical Specifications - Operating System

| Feature | Sub-feature | Description |
|---------------|---|--|
| JavaCard™ | 2.2.1 (2.2.2) optional | Runtime Environment Specification for the Java Card™ Platform, Version 2.2.1 October, 2003; Application Programming Interface, Java Card™ Platform, Version 2.2.1 October, 2003; Virtual Machine Specification for the Java Card™ Platform, Version 2.2.1, October, 2003 |
| Communication | Physical | |
| | ISO/IEC 7816-1 | Identification Cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics |
| | ISO/IEC 7816-2 | Identification cards - Integrated circuit cards - Part 2: Cards with contacts - Dimensions and location of the contacts (Note: SMD form factor) |
| | Electrical | |
| | ISO/IEC 7816-3 | Information Technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols |
| | Inter-industry commands for interchange | |
| | ISO/IEC 7816-4 | Information Technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry commands for interchange |
| | Identification | |
| | ISO/IEC 7816-5 | Identification cards - Integrated circuit cards - Part 5: Registration of application providers |

Technical Specifications (Continue)

| Feature | Sub-feature | Description |
|--------------------------|--|---|
| Communication (Continue) | Protocol Support | |
| | T=0 | Protocol T=0 with PPS for speed enhancement |
| | T=1 | Protocol T=1 with PPS for speed enhancement with extended APDU length support |
| Card Manager | Generic term for the three card management entities of a GlobalPlatform™ card; the GlobalPlatform™ Environment, Issuer Security Domain and Cardholder Verification Method Service Provider | |
| | Global Platform™ 2.1.1 | Global Platform Card Specification v2.1.1 Version: 2.1.1 Published: March 2003 |
| | Atomic Package and Application Deletion | Memory recovered and is reusable |
| | Global PIN | A PIN that may be checked by all applets on a card, using CVM.verify(). Its value is usually set at personalization time |
| | Secure Channel Protocol 01 | SCP01 provides mutual authentication; integrity and data origin authentication; confidentiality |
| | Secure Channel Protocol 02 | Support for all SCP02 options |
| | Repeated application install failure | The OPEN may keep track of the number of unsuccessful consecutive attempts of the Card Content load and installation process by a particular Application and the total number of such attempts by all applications. Actions may include such defensive measures as the locking or termination of the card |
| | Applications boundary violations | The OPEN may also enable velocity checking against repeated failed attempts by an Application to allocate additional memory beyond its allowed limit as stored in the Open Platform Registry. The OPEN may choose to lock an Application which exhibits such behaviour |
| JCVM | Data type int | Fully supported by Athena OS755 (IDProtect) |
| Security Settings | Keys and PINs are stored encrypted | The OS does not store any Keys or PINs in plain text during computation |
| | On card key generation | RSA Standard and CRT keys can be generated on card up to 2048 bits in lengths |
| | FIPS 140-2 Level 3 | Federal Information Processing Standards Publication: Security Requirements for Cryptographic Modules FIPS PUB 140-2, issued May 25 2001 See NIST certificate number 749 - March 2007 |
| | FIPS approved secure and pseudo RNG | Athena OS755 (IDProtect) supports the secure and pseudo RNG specified in JC API and are FIPS approved (see NIST certificate numbers 75 and 209) |
| | FIPS 140-2 Self Tests | Power-up self tests are performed between the card power-up and the first execution of the related APDU command |
| | FIPS 140-2 KAT | Known Answer Tests performed at power up. The cryptographic function tests consist of computing from pre-recorded input data, and comparing the results with pre-recorded answers |
| | FIPS 140-2 Software Integrity | Checks that no FIPS application present in EEPROM (packages) is corrupted. The error detecting code is FIPS approved |
| Card integrity | Power loss | Transaction atomicity is fully supported ensuring EEPROM writes are protected from corruption due to power loss |
| | Termination | Fully supports GlobalPlatform life cycle states, including terminated. Once a card is locked or terminated further interaction is not permitted |
| PKI | Microsoft CryptoAPI (CAPI) | Support for all industry leading CAPI implementations |
| | PKCS# 11 | Support for all industry leading Cryptographic Token Interface (Cryptoki) implementations |

Technical Specifications (Continue)

| Feature | Sub-feature | Description |
|----------------------------|---------------------------------|---|
| Biometrics | Biometric Applet | Support for industry leading "match-on-card" biometric applet |
| JavaCard™ cryptography API | javacard.security.KeyBuilder | LENGTH_AES_128 LENGTH_AES_192 LENGTH_AES_256 LENGTH_DES LENGTH_DES3_2KEY LENGTH_DES3_3KEY LENGTH_RSA_2048 LENGTH_RSA_1024 LENGTH_RSA_768 LENGTH_RSA_512 Note: The KeyBuilder class supports the creation of RSA standard and CRT keys from 512- to 2048-bits in 32-bit increments |
| | javacard.security.KeyPair | ALG_RSA, ALG_RSA_CRT Standard and CRT key pairs from 512-2048-bits in increments of 32-bits may be generated. On Card 1024 bit RSA key generation – 10 seconds-typical |
| | javacard.security.MessageDigest | ALG_SHA ALG_SH256 |
| | javacard.security.RandomData | ALG_PSEUDO_RANDOM |
| | javacard.security.Signature | ALG_AES_MAC_128_NOPAD ALG_DES_MAC8_ISO9797_M1 ALG_DES_MAC8_ISO9797_M2 ALG_DES_MAC8_NOPAD |
| | javacardx.crypto.Cipher | ALG_AES_BLOCK_128_CBC_NOPAD ALG_AES_BLOCK_128_ECB_NOPAD ALG_DES_CBC_ISO9797_M1 ALG_DES_CBC_ISO9797_M2 ALG_DES_CBC_NOPAD ALG_DES_ECB_ISO9797_M1 |
| Delivery | Transport Key | Configurable Transport Key locks card for reading/writing during pre-issuance |

Athena developer IDE/SDK

To support users of OS755 (IDProtect) Athena also offers a streamlined Java Card™ Integrated Development Environment that is considered to be one of the most comprehensive smartcard development tools available.

This tool provides users with a robust and powerful visual environment to build, test and deploy compliant applications for Java Card™ technology-based smartcards on Athena's Java Card™ solutions.

An all-in-one solution

Athena developer provides a quick and easy to use visual development environment. You don't need to run different applications for writing and developing code, nor for debugging and writing the applet onto the Java Card™. Athena developer is an all-in-one solution, which is good news for developers with all levels of experience

Product Evaluation

To evaluate Athena OS755 (IDProtect) and its development environment please contact the Athena Sales Team

Contact Details

To contact Athena's sales team send an email to sales@athena-scs.com or contact one of the Athena offices.

Japan

Marutaya Building
6-9 Yokoyamacho, Hachioji
Tokyo 192-0081
Tel: +81-426-60-7555
Fax: +81-426-60-7106
sales@athena-scs.co.jp

USA

20380 Town Center Lane
Suite 240
Cupertino, CA 95014
Tel: +1 866 359 2273
Fax: +1 408 608 1818
sales@athena-scs.com

UK

10 Lochside Place
Edinburgh Park
Edinburgh EH12 9RG
Tel: +44 131 248 3785
Fax: +44 131 777 8150
sales@athena-scs.com



www.athena-scs.com