



Highlights:

- Java Card™ 2.2.1
- Global Platform 2.1.1
- 72k EEPROM
- FIPS 140-2 Certified
- RSA Standard and CRT 2048 bit
- RSA Standard and CRT 2048 bit key generation
- AES 256
- DES
- TDES
- SHA-1
- SHA-256
- MD5
- Precise Biometrics™ BioMatch J Applet (optional)



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

GlobalPlatform™ is a trademark of Global Platform Inc.

IDProtect Overview



Java promises write once, run anywhere capability. Athena IDProtect - Athena Java Card™ technology and GlobalPlatform™ operating system - fulfils that promise for the smart card industry.

Athena's IDProtect is built to give you flexibility in the way you work: a blank canvas on which to create smart card products for all market sectors. Central to Athena IDProtect is its compliance with the Java Card™ and GlobalPlatform™ standards; multiple compliant Java Card™ applets from any source will run securely on Athena IDProtect enabled silicon. Applets can be securely loaded and deleted post issuance thanks to GlobalPlatform™ compliant Issuer Security Domain implementation. 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

Feature	Sub-feature	Description
JavaCard™	2.2.1	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
	ISO/IEC 7816-4	Information Technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry commands for interchange
	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
Contactless (optional)	Full support for ISO/IEC 14443 Type B protocol	

Technical Specifications (Continue)

Feature	Sub-feature	Description
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
	GlobalPlatform™2.1.1	Information Technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry commands for interchange
	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	Optionally supported in the JCVM but is supported in 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 keys indicated in the Key Pair list may be generated on the card
	FIPS 140-2 Level 3	Federal Information Processing Standards Publication: Security Requirements for Cryptographic Modules FIPS PUB 140-2, issued May 25 2001
	FIPS approved secure and pseudo RNG	IDProtect supports the secure and pseudo RNG specified in JC API and are FIPS approved
	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

Product Evaluation

Evaluation cards are available for this product from 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

%d !(* z A chcmc_cmlJa UI Vkc
<UWx]c?l'g\]
Hc_mc %- &! \$ \$ *
HY. 'Z , %d (&*! * \$! +))
: UI . 'Z , %d (&*! * \$! + % \$ *
gUYg4 UH\ YbUI! gVg"Vt" d
k k k "UH\ YbUI! gVg"Vt" d

USA

&\$' , \$ 'Hck b'7YbhYf'@UbY
Gi]hY' &(\$
7i dYfh]bcz'75' -) \$%(
HY: 'Z % , * * ') - ' &&+
: UI . 'Z % (\$, * * \$, % %
gUYg4 UH\ YbUI! gVg"Vt" a
k k k "UH\ YbUI! gVg"Vt" a

UK

%'@cWg]XY'DUW
9X]bVi f[\ 'DUf_
9X]bVi f[\ '9<%&' - F;
HY: 'Z ((' % % &(, ' ' + ,)
: UI . 'Z ((' % % + + + , %) \$
gUYg4 UH\ YbUI! gVg"Vt" a
k k k "UH\ YbUI! gVg"Vt" a



www.athena-scs.com