

FIPS-201 Compliant Java Card™ PKI Smart Card



IDProtect Duo PIV

Athena, with its extensive smart card experience, has released a dual interface (contact and contactless) solution for identity projects requiring a FIPS 201 and 140-2 certified, multi-application platform.

Benefiting from the unique modular and portable design of its OS755 Java Card™ Platform, Athena has tailored IDProtect Duo PIV to incorporate the latest specifications from Java Card™, GlobalPlatform™, NIST and GSA. IDProtect Duo PIV is delivered with a FIPS 201 PIV application pre-loaded.

IDProtect Duo PIV benefits from Athena's expertise and could be used in any cross market implementation (ID and Finance, Finance and Loyalty, Mobile and Finance).

Independence

Athena's Java Card technology operating system is highly flexible and already available on multiple silicon platforms. It is the perfect solution for Smart Card manufacturers wishing to retain their independence and address all segments of the market. IDProtect Duo has been designed for Card Issuers wishing to use a single platform that can be ported to multiple silicon platforms to realise the benefits of efficient smart card manufacturing and personalisation for individual customer projects.

Specification Support

IDProtect Duo PIV complies with characteristics as described in:

- ISO/IEC 7810 - Identification cards -- Physical characteristics
- ISO/IEC 7816 - Identification cards -- Integrated circuit cards
- ISO/IEC 10373 - Identification cards -- Test methods
- ISO/IEC 14443— Identification cards -- Contactless integrated circuit cards
- GlobalPlatform™ 2.1.1
- Java Card™ 2.2.2

PIV Solution

The Athena PIV Card and Middleware solution is validated to Federal Information Processing Standard (FIPS) 201, is GSA approved, 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

IDProtect Duo PIV Highlights	
ISO 7810	•
ISO 7816	•
ISO 10373	•
ISO 14443	Type B
GlobalPlatform™ 2.1.1	•
Java Card™ 2.2.2	•
FIPS 140-2	•
FIPS 201	•
Supplementary Security Domain support	•
Memory Management	•
Transmission Protocols	T=0, T=1, T=CL
PIV applet	•
TDES	•
AES	•
RSA	•
RSA-CRT	•
SHA-1	•
SHA-256	•

IDProtect Duo PIV Technical Specification

Silicon general

- ESD Protection to $\pm 6000V$ on contact pins, $\pm 2000V$ on RF pins
- Operating Ranges: 2.7V to 5.5V
- Power-saving Wait and Very Low-power Stop Modes
- Power-up Detection

Silicon contactless mode

- Contactless Interface Controller (CIC) with Full Support for ISO/IEC 14443 Type B Protocol
- Reader-to-card:
 - ISO/IEC Type B: 10% ASK Modulation and NRZ Bit Coding
 - Baud Rates: 106Kbps, 212Kbps and 424Kbps
- Card-to-reader:
 - ISO/IEC Type B: Modulation of Incoming RF Carrier by Resistive Load Switching / Generation of 847.5KHz Subcarrier with BPSK Modulation / NRZ data Encoding
 - Baud Rates: 106Kbps, 212Kbps, 424Kbps and 848Kbps

Silicon memory

- 128k ROM
- 72k EEPROM
- 5k RAM
- Endurance: 500,000 Write/Erase Cycles at 25°C
- 10 Years Data Retention

Silicon Security

- Dedicated Hardware for Protection Against SPA/DPA Attacks
- Advanced Protection Against Physical Attack, Including Active Shield
- Voltage Monitor
- Frequency Monitor
- Temperature Monitor
- Light Protection

Silicon Security Certification Targeted:

- Common Criteria EAL5+
- VISA
- CAST

Operating system complies with characteristics as described in:

- ISO/IEC 7810
- ISO/IEC 10373
- ISO/IEC 7816
- ISO 14443
- GlobalPlatform™ 2.1.1

- Sun Microsystems™ Java Card 2.2.2

Signal and Transmission protocols supported:

- ISO/IEC 7816-3 and ISO/IEC 7816-4
- T=0 and T=1
- T=CL
- PPS speed enhancement

Global Platform functionality supported:

- Life cycle management
- Security domains (including DAP verification, Delegated Management and Supplementary Security Domains)
- Secure channel protocol SCP 01 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 and Memory compaction

Supported cryptography functions:

- TDES (112- and 168-bit)
- AES (128-, 192- and 256-bit)
- RSA (up to 2048 bit)
- RSA-CRT (up to 2048 bit)
- On card RSA key generation (up to 2048 bit)
- SHA-1
- SHA-256

Solution certification

- FIPS 140-2 (Certificate #991)
- FIPS 201 (Certificate #12)

Agency approval

- GSA (APL #380)

FIPS 201 PIV application implements:

- Card Holder Facial Image
- Card Holder Printed Information
- X.509 Certificate for Digital Signature
- X.509 Certificate for PIV Key Management
- X.509 Certificate for Card Authentication

USA

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

Japan

1-14-16, Motoyokoyama-cho
Hachioji-shi
Tokyo, 192-0063
Tel: +81-426-60-7555
Fax: +81-426-60-7106
sales@athena-scs.co.jp
www.athena-scs.co.jp

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

International

10 Abba Eban Blvd.
P.O. Box 12483
Herzliya 46733, Israel
Tel: +972 9 951 7550
Fax: +972 9 951 7551
sales@athena-scs.com
www.athena-scs.com