ASECard Crypto J Datasheet

ASECard Crypto J is Athena's state-of-the-art cryptographic Java Card. ASECard Crypto J is compliant with the Java Card™ and GlobalPlatform standards; multiple compliant Java Card™ applets can run securely on ASECard Crypto J. Applets can be securely loaded and deleted post issuance thanks to GlobalPlatform compliant Issuer Security Domain implementation. ASECard Crypto J includes the Athena PKI applet integrated with the industry leading ASECard Crypto Toolkit cryptographic middleware product for high-performance certificate based authentication and digital signatures.

ASECard Crypto J is designed to comply with FIPS 140-2 level 2 and 3 and Common Criteria EAL 4+ for SSCD Type 3 devices.

Specifications Supported

Java Card™ 2.2.1

GlobalPlatform 2.1.1

General Features

- Designed for CC EAL 4+ and FIPS 140-2 Level 3 requirements
- Available memory 72Kbyte
- T=0 and/or T=1 protocol
- Communication speed up to 153,600 bps through PPS.
- Option for USB Full Speed and 14443 Type B contactless interfaces.
- PKCS#11, PKCS#15, ISO 7816 1-5, 8-9

Security Features

- AES, DES, MD5, RSA, SHA-1,256, On-board RSA key generation 512- 2048 bit.
- Secure against side-channel analysis (SPA, DPA, SEMA and DEMA).
- PKCS#1 and ISO9796-2 padding schemes.
- Support for X.509 v3 certificates

Available Applets:

- Built-in Athena PKI.
- Native support for Precise Biometrics Match-on-Card Fingerprint Authentication.

ASECard Crypto J - Technical Specification

FEATURE	SUB FEATURE
JC API	Supported Cryptographic Functions
javacard.Security. Checksum	ALG_ISO3309.CRC16 ALG_ISO3309.CRC32
javacard.Security. keybuilder	JC 2.2.1 LENGTH_AES_128 LENGTH_DES TYPE_DES LENGTH_DES3_2KEY TYPE_AES_TRANSIENT_RESET LENGTH_DES3_3KEY TYPE_DES_TRANSIENT_DESELECT LENGTH_RSA_2048 TYPE_DES_TRANSIENT_RESET LENGTH_RSA_1024 TYPE_RSA_CRT_PRIVATE LENGTH_RSA_768 TYPE_RSA_PRIVATE LENGTH_RSA_512 TYPE_AES_TRANSIENT_DESELECT TYPE_AES TYPE_RSA_PUBLIC The key builder package supports the generation of DES, Triple DES and AES keys of 128 bits, as well as RSA 512, 768, 1024 and 2048.
javacard.Security. keybuilder	ALG_RSA ALG_RSA_CRT It is possible to generate RSA key pairs for key lengths 64, 80, 96, 112 and 128 bits. All odd public exponents greater than or equal to 3 are supported.
java.Security.KeyPair	ALG_RSA ALG_RSA_CRT It is possible to generate RSA key pairs for key lengths 64, 80, 96, 112 and 128 bytes. All odd public exponents greater than or equal to 3 are supported.
java.Security. MessageDigest	ALG_SHA ALG_MD5
javacard.Security. RandomData	ALG_PSEUDO_RANDOM ALG_SECURE_RANDOM

FEATURE	SUB FEATURE	
JC API	Supported Cryptographic Algorithms	
javacard.Security.Signature	ALG_DES_MAC8_ISO9797_M1 ALG_DES_MAC8_ISO9797_M2 ALG_DES_MAC8_NOPAD ALG_RSA_SHA_ISO9796	ALG_RSA_SHA_PKCS1 MODE_SIGN MODE_VERIFY
javacardx.crypto.Cipher	ALG_AES_MAC_128_NOPAD 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	ALG_DES_ECB_ISO9797_M2 ALG_DES_ECB_NOPAD ALG_RSA_NOPAD ALG_RSA_PKCS1 MODE_DECRYPT MODE_ENCRYPT

Data subject to change without notice. Please consult your Athena representative for the latest product specifications.

For further details contact:

USA & Canada
Athena Smartcard Inc.
225 Franklin Street, Suite 2600
Boston, Massachusetts 02110
Toll Free: 1-866-359-2273
Fax: 617-507-2689
e-mail: sales@athena-scs.com

International Office
11 Hamenofim St.
P.O. Box 12483
Herzliya 46733, Israel
Tel: +972 9 951 7550
Fax: +972 9 951 7551
e-mail: sales@athena-scs.com

Athena Japan
6F Marutaya Building
6-9 Yokoyama-Cho Hachioji
Tokyo 192-0081, Japan
Tel: +814 2 660 7555
Fax: +814 2 660 7106
e-mail: sales@athena-scs.co.jp