athena Smartcard Solutions

SECURE > FAST > RELIABLE

ASECard Crypto

High performance Cryptographic Smart Card with RSA dedicated processor.

- ISO7816-3 4 ,8 and 9 compliant
- High performance RISC architecture and cryptographic processor
- RSA up to 2048 bits, Triple-DES, SHA-1, MD5 and ECC support
- On-card fast RSA key pair generation
- On-card Digital Signature generation and verification
- Secure Messaging support
- Tamper resistant and tamper proof
- Up to 72KB EEPROM
- CAPI and PKCS#11 support
- Professional SDK available

ASECard Crypto is a contact smart card which fully complies with ISO7816 - 3, 4, 8 and 9. It is designed for improving security and performance for RSA public key cryptographic operations which are essential in PKI, Digital Signature and various security requirements in networked environments. ASECard Crypto provides up to 72KB EEPROM of secure data storage.

Network Security and Public Key Cryptography

As more business activities migrate to on-line systems, the risk of unauthorized access, breach of confidentiality and user authentication is growing. Public key cryptography (PKI) is the preferred technology for reducing these risks. Public key cryptography uses a pair of strong cryptographic keys. With public key cryptography, the private key is always kept in a secure location, while its counterpart, the public key, may be published. Security is maintained as long as the private key is kept secure. Today's state-of-the-art Internet security techniques such as SSL, Digital Signature are all based on public key cryptography. ASECard Crypto improves the security and performance of such public key cryptography based mechanisms by providing secure storage for private keys and accelerating cryptographic operations.

CAPI and PKCS#11 support - Ready for PKI

As a modern cryptographic smart card, ASECard Crypto is supported by middleware for PKCS#11 and Microsoft CAPI and can be easily integrated within leading PKI and network security solutions. With its Crypto Service Provider (CSP), ASECard Crypto can be seamlessly integrated with Microsoft Windows applications including Outlook, Internet Explorer as well as Windows 2000/2003 Smart Card Logon, VPN, and Remote Terminal Services.

ASECard Crypto is also supported by a comprehensive SDK package. It helps developers build their own solutions by fully utilizing ASECard Crypto's advanced features which reduce the development cycle.

High Performance Cryptographic Smart Card

ASECard Crypto is a cryptographic contact smart card with state-of-the-art security features. Its cryptographic processor accelerates computationally intensive RSA operations and generates RSA key pairs and digital signatures on card. This ensures the ultimate security of the RSA private keys. ASECard Crypto also supports symmetric cryptographic algorithm such as Triple-DES, DES as well as standard hashing like SHA-1, MD5 and ECC.

ASECard Crypto

High performance Cryptographic Smart Card with RSA dedicated processor.

Comprehensive Software Development Kit

The ASECard Crypto SDK is available for developing applications that utilize the ASECard Crypto card. The APDU library provides high level programming interface while supporting all of the ASECard Crypto functionalities. Developers can also develop applications over PKCS#11 or CAPI. ASECardViewer is Athena's unique tool, which enables intuitive access to the ASECard Crypto functionality through an Explorer-like GUI. ASECard Edit is a utility that allows interactive access to the ASECard Crypto file system and command set. Sample programs help the programmer understand both basic concepts of smart cards and advanced features of ASECard Crypto. It supports Windows, Linux, Windows CE & MAC.

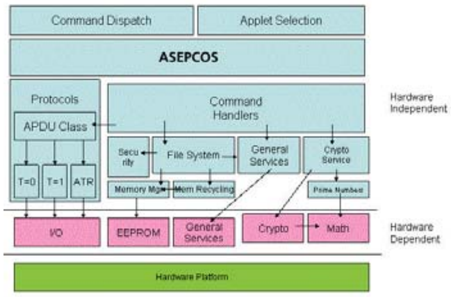
ASECard Crypto SDK

ASEPCOS - Smart card operating systems

ASECard Crypto is based on ASEPCOS, Athena's most advanced smart card operating system. ASEPCOS is designed with the maximum level of security in mind. Its built-in security features, smart memory management, and large user memory, make it the perfect platform for PKI, Authentication, and Digital Signature solutions.

ASECard Crypto Specifications

Architecture	CMOS RISC security controller with RSA processor
EEPROM	up to 72KB
External clock	1-5MHz
Supported standards	ISO7816-3, 4, 8, 9
Cryptographic algorithm support	RSA 1024/2048bits, Triple-DES, DES, ECC, AES
Hashing algorithm	SHA-1, MD5
Middleware support	CAPI (CSP), PKCS#11
External voltage	2.7 - 5.5V



ASEPCOS Diagram

athena
Smartcard Solutions

www.athena-scs.com

JAPAN
Athena Smartcard Solutions Inc.
6-9 Yokoyama-Cho Hachioji
Tokyo 192-0081, Japan
Tel: +81.426.60.7555
Fax: +81.426.60.7106
www.athena-scs.co.jp

USA
Athena Smartcard Inc.
225 Franklin Street, Suite 2600
Boston, Massachusetts 02110
Toll Free: 1.866.359.CARD (2273)
Fax: 1.617.507.2689
www.athena-scs.com

INTERNATIONAL
Athena Smartcard Solutions Ltd.
11 Hamenofim St.
Herzliya, 46733 Israel
Tel: +972.9.951.7550
Fax: +972.9.951.7551
www.athena-scs.com