ACOS5-EVO

Advanced Card Systems Ltd.
Card & Reader Technologies

Outline

1. Product Information
   - Product Overview
   - Product Features
   - Technical Specifications
   - Certifications/Compliance
2. Product Applications
3. Related Software Products

Product Information

Advanced Card Systems Ltd.
Card & Reader Technologies

Product Overview

ACOS5-EVO Series

PN: ACOS5-K1A
ACOS5-EVO
(Contact)

PN: ACOS5-K1K
ACOS5-EVO
(Combi)

PN: ACOS5-K1L
ACOS5-EVO
(Contactless)

PN: ACOS5T2-B1E1
CryptoMate EVO

Key Features of ACOS5-EVO

Cryptographic Algorithms

- ECC: Curves P-224/P-256/P-384/P-521
- RSA: up to 4096 bits
- AES: 128/192/256-bits (ECB, CBC)
- DES/3DES: 56/112/168-bits (ECB, CBC)
- Hash: SHA1, SHA224, SHA256, SHA384, SHA512
- MAC: CBC-MAC (DES/3DES, AES), CMAC (3DES, AES)
- Random Number Generator

Speed and Memory

- 192 KB Memory
- Configurable ATR (Answer To Reset)
- Anti-tearing Function

Certifications and Compliance

- Common Criteria EAL5+ (Chip Level)
- ISO 7816 Parts 1, 2, 3, 4, 8, and 9
- ISO 14443 Parts 1-4, Type A
- FIPS 140-2 Level 3 Compliant

Security Functions

- Provides multi-level secured access hierarchy
- Supports Secure Messaging
- Supports Mutual Authentication and Session Key Generation

Technical Specifications

Category		ACOS5-EVO
Product Code		ACOS5-K1AACSA4200 (Contact) ACOS5-K1KACSA4200 (Combi) ACOS5-K1LACSA4200 (Contactless)
User EEPROM Memory		
User Memory		192 KB
Endurance *(write/erase cycle)*		500,000
Compliance to ISO Standards		
Contact	ISO 7816 – 1/2/3/4	✓
	ISO 7816 – 4	✓
	ISO 7816 – 8/9	✓
Contactless	ISO 14443 - 1/2/3/4	✓
	Type A	✓

Technical Specifications

Category		ACOS5-EVO
Communication Speed and Protocol: Contact Interface		
Protocol	T=0	✓
	T=1	✓ (Default)
Speed	9,600 bps – 446,400 bps	✓ TA = 96 (223,200 bps) Default
Communication Speed and Protocol: Contactless Interface		
Protocol	T=CL	✓
Speed	106,000 – 424,000 kbps	✓
Operating Conditions		
Temperature		0 °C – 50 °C
Humidity		Max. 90% (non-condensing)

Technical Specifications

Category	ACOS5-EVO
Cryptographic Capabilities	
ECC	P-224/P-256/P-384/P-521
RSA	up to 4096 bits
DES/3DES	56/112/168-bits (ECB, CBC)
AES	128/192/256 bits (ECB, CBC)
Hash	SHA1, SHA224, SHA256, SHA384, SHA512
MAC	CBC-MAC (DES/3DES, AES), CMAC (3DES, AES)
Secure Messaging	✓
Mutual Authentication	✓

Product Applications

Advanced Card Systems Ltd.
Card & Reader Technologies

In what areas can we apply ACOS5-EVO?

In what areas can ACOS5-EVO be used?

Company provides their employees with an ID

Employees request for a digital certificate via the company website

Employee inserts the ACOS5-EVO in the ACR38U PocketMate

Administrator checks the credentials and provides the employee with the link to download and store the certificate in the ID

Employees stores the digital certificate in the ID

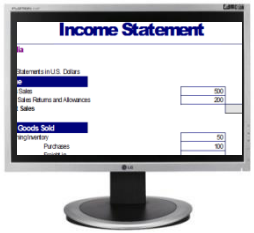
Employee uses his/her digital certificate to sign and encrypt the email

In what areas can ACOS5-EVO be used?

Citizens go to Registration Authorities to apply for a Digital Certificate

Certificate Authority provides the citizen with the digital certificate

Citizen digitally signs and encrypts his Income Tax Statement using the digital certificate stored in the card



Citizen logs in to a secured website and submits the digitally signed and encrypted document to the government agency

Related Software Products

Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS5-EVO PKI KIT

ACS offers the **ACOS5-EVO PKI KIT** to Certificate Authorities and other organizations who are interested in deploying **PKI Solutions with ECC Support.**

With the ACOS5-EVO/CryptoMate EVO PKI Kit, the following are supported:

- Secure Online Certificate Generation
- Microsoft® Outlook and Mozilla® Thunderbird® mail signing and encryption (S/MIME)
- Windows® Smart Card Logon
- Microsoft® Office
- Adobe® Reader®

Contact your ACS sales representative, visit our website at http://www.acs.com.hk or email us at info@acs.com.hk for more information.

ACOS5 Minidriver

For clients who want to use the ACOS5-EVO and CryptoMate EVO in Windows Environment only, ACS also provides the ACOS5 Minidriver.

The following Windows applications are supported:

- Windows® Smart Card Logon
- Microsoft® Office
- Microsoft® Outlook mail signing and encryption (S/MIME)

Once the token has been initialized with the ACOS5 Minidriver, it can only be used with Windows OS and will not be compatible with other ACS middleware.

Contact your ACS sales representative, visit our website at http://www.acs.com.hk or email us at info@acs.com.hk for more information.

Thank You!

Advanced Card Systems Ltd.
Card & Reader Technologies

info@acs.com.hk
www.acs.com.hk