Advanced Card Systems Ltd.
Card & Reader Technologies

CryptoMate EVO

(ACOS5-EVO Cryptographic USB Token)

Technical Specifications V1.01

Table of Contents

List of Figures

1.0. Introduction

The CryptoMate EVO contains an ACOS5-EVO cryptographic smart card module. The ACOS5-EVO cryptographic smart card module offers advanced asymmetric and symmetric cryptographic algorithms such as ECC and RSA, and is compliant with international standards for PKI smart cards such as FIPS 140-2 (US Federal Information Processing Standards) Level 3 and CC EAL 5+ (chip level).

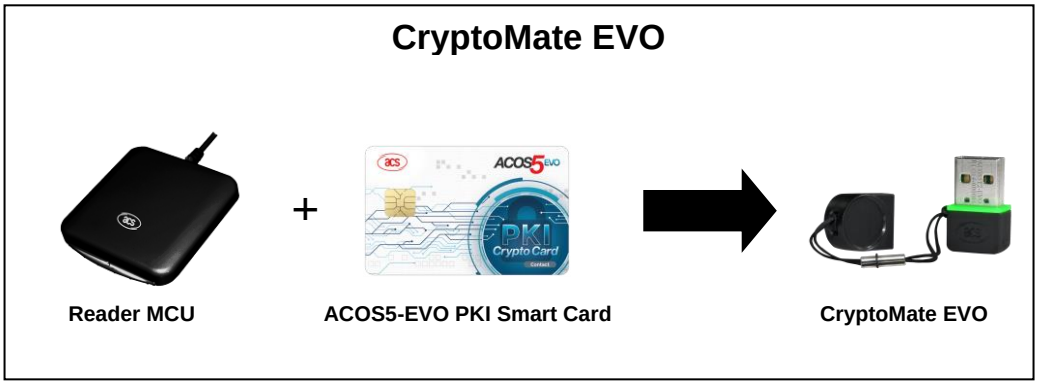


Figure 1: CryptoMate EVO System Block Diagram

The CryptoMate EVO is similar in appearance to the CryptoMate Nano, but it can be easily distinguished when plugged in the PC with its Green LED. PC applications will recognize it through its PCSC and Driver Name: ACS CryptoMate EVO. It also offers higher memory and more advanced cryptographic functionalities compared to the CryptoMate Nano.

2.0. Features

2.1. Cryptographic Smart Card Features

The CryptoMate EVO contains the ACOS5-EVO cryptographic smart card module, which has the following features:

2.1.1. Communication Protocols

- T=0, T=1 with baud up to 446,400 bps

2.1.2. Memory

- Capacity: 192Kb
- EEPROM Endurance: 500,000 erase/write cycles
- Data Retention: 30 years

2.1.3. Cryptographic Capabilities

The ACOS5-EVO supports a number of cryptographic algorithms, including:

- ECC: Curves P-224/P-256/P-384/P-521
- RSA: 512 – 4096 bits in 256 bits increments
- 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)

2.1.4. Random Number Generation

- Deterministic RNG according to FIPS 140-2
- Non-deterministic RNG compliant to AIS-31

2.1.5. File Security

- Private and secret key file read access can be set to “Never”
- File access condition capability with ISO 7816–compliant Secure Attribute-Compact. File access is only allowed if the proper security conditions are met (e.g. PIN submissions).
- Command execution condition capability per Dedicated File (DF) with ISO 7816–compliant Secure Attribute-Extended. Commands are allowed only if the proper security conditions are met (e.g. PIN submission).
- Secure Messaging function for confidential and authenticated data transfers
- Mutual authentication (terminal-to-card and card-to-terminal) with session key generation for encryption and MAC
- Anti-tearing Function Support

2.1.6. Compliance to Standards

- Compliance with ISO 7816 Parts 1, 2, 3, 4, 8, and 9
- Compliance with FIPS 140-2 Level 3
- Certified with Common Criteria EAL 5+ (Chip Level)

2.2. Token Features

2.2.1. Physical Characteristics

- Green Status LED
- Lightweight: 4.61 g
- Extremely small: 29.25 mm × 14.80 mm × 10.28 mm
- Keychain hole
- Tamper-evident casing
- Smart card power supply through USB port

2.2.2. Compliance to Standards

- USB Full Speed Interface
- CCID-compliant (Plug and Play)
- CE and FCC–certified
- RoHS–compliant
- REACH-certified
- Microsoft® WHQL–certified
- Supports Android™ 3.1 and later[1]

[1] *Uses an ACS-defined Android Library*

3.0. Typical Applications

- e-Government
- e-Healthcare
- Banking and Payment
- Network Security
- Access Control
- Public Key Infrastructure
- Digital Signature

4.0. Middleware

To use CryptoMate EVO for PKI applications with digital certificates, an applicable middleware is needed.

ACS offers software solutions such as the ACOS5 Minidriver and ACOS5-EVO PKI Kit so that the ACOS5-EVO and the CryptoMate EVO can be used with other third party applications as shown in the figure below:

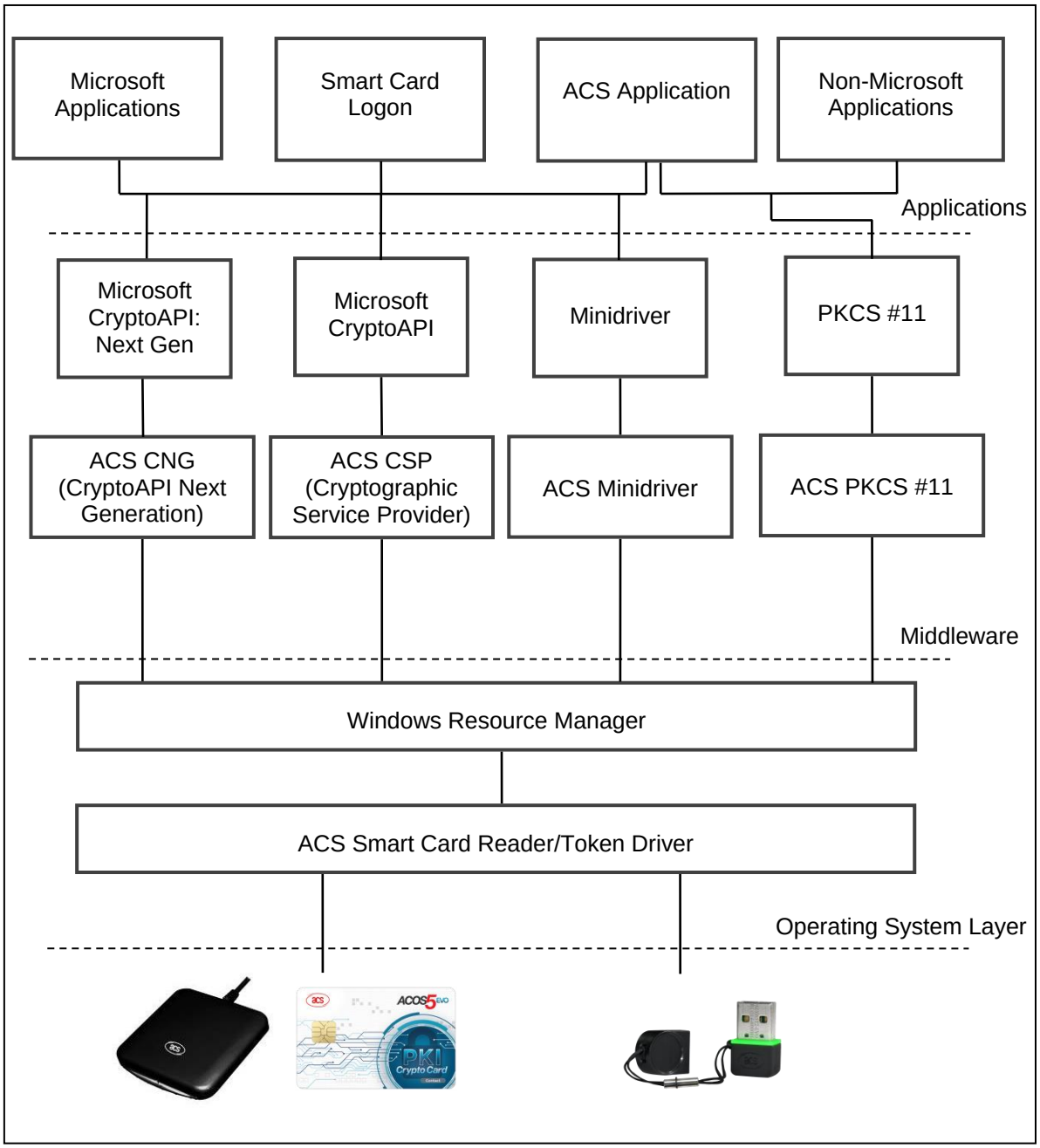
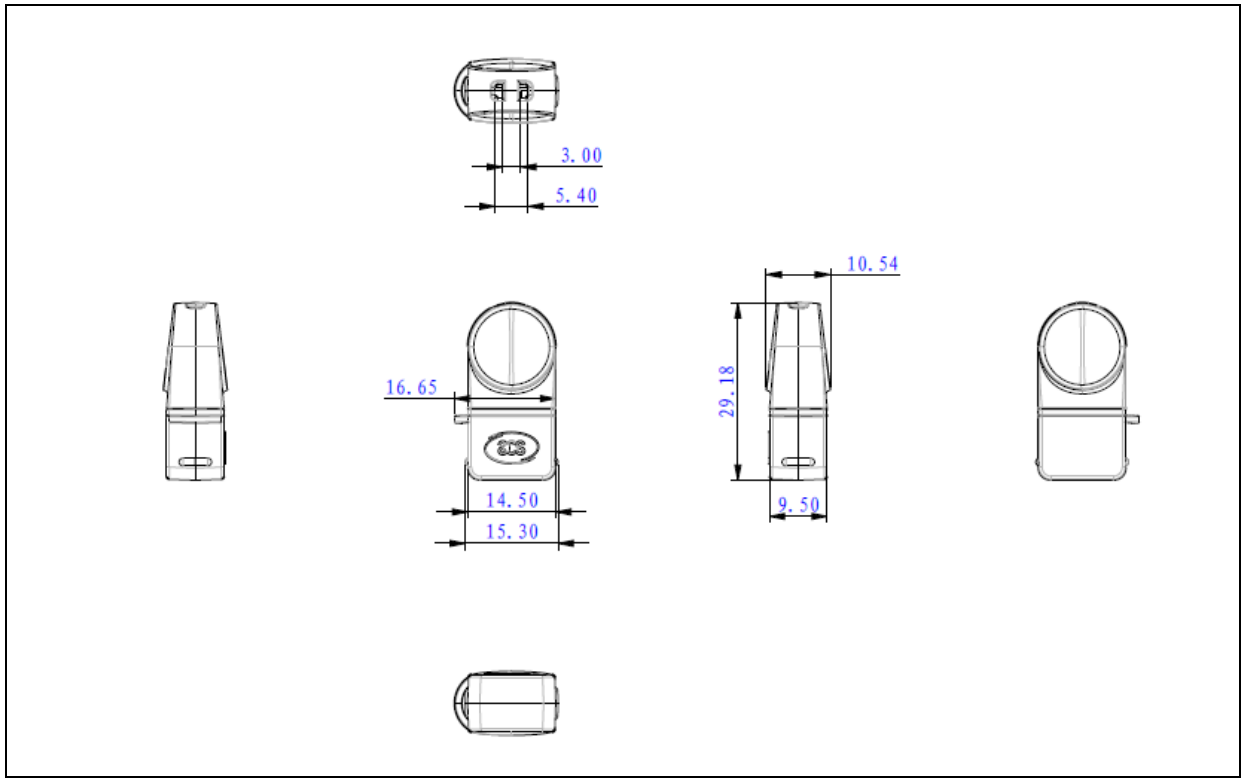


Figure 2: Middleware Diagram

Please contact us at info@acs.com.hk for inquiries about the middleware support for the CryptoMate EVO token.

5.0. Technical Specifications



Physical Characteristics	
Dimensions	29.18 mm (L) × 14.50 mm (W) × 10.54 mm (H)
Weight	4.61 g
Color	Black
ACOS5-EVO Cryptographic Smart Card Module	
Memory Size	192 KB
Endurance	500,000 write/erase cycles
Data Retention	30 years
Cryptographic Capability	ECC: Curves P-224/P-256/P-384/P-521
	RSA: 512 – 4096 bits in 256 bits increments
	AES: 128/192/256-bits (ECB, CBC)
	DES/3DES: 56/112/168-bits (ECB, CBC)
	MAC: CBC-MAC (DES/3DES, AES), CMAC (3DES, AES)
Hashing Capability	SHA1, SHA224, SHA256, SHA384, SHA512
USB Host Interface	
Protocol	USB CCID
Connector Type	Standard Type A
Power Source	From USB port
Speed	USB Full Speed (12 Mbps)
Built-in Peripherals	
LED	Green
Casing	Tamper-evident
Others	Keychain hole for portability
Operating Conditions	
Temperature	0 °C – 50 °C
Humidity	Max. 90% (non-condensing)
MTBF	500,000 hrs

Certifications/Compliance

ISO 7816, USB Full Speed, Common Criteria EAL5+ (Chip Level), PC/SC, CCID, CE, FCC, RoHS, REACH
FIPS 140-2 Level 3 (USA), Microsoft® WHQL

Middleware Support

ACS PKCS #11, ACS CSP (based on Microsoft's CryptoAPI), ACS CNG (based on Microsoft's CNG)
ACS Minidriver
X.509 v3 Certificate Storage (can store more than 10 Key Pairs)

Device Driver Operating System Support

Windows® 7, Windows® 8, Windows® 8.1, Windows® 10
Windows® Server 2008, Windows® Server 2008 R2, Windows® Server 2012, Windows® Server 2012 R2, Windows® Server 2016
Linux®, Mac OS®, Android™ 3.1 and later