Advanced Card Systems Ltd.
Card & Reader Technologies

CryptoMate Nano

(ACOS5-64 Cryptographic USB Token)

Technical Specifications V1.04

Table of Contents

List of Figures

1.0. Introduction

The CryptoMate Nano contains a built-in ACOS5-64 v3.00 module that is FIPS 140-2 (US Federal Information Processing Standards) Level 3–certified. It is a small and portable cryptographic USB token with 64 KB of EEPROM and complies with various international standards.

The CryptoMate Nano casing is designed to be tamper-evident so that any unauthorized physical access will be easily visible. It also protects sensitive credentials and cryptographic keys since cryptographic operations such as RSA, SHA, AES and 3K3DES are performed on the FIPS 140-2 Level 3–certified ACOS5-64 module inside the token. With this, important and sensitive information are protected from being hacked or sniffed, achieving a high level of security for applications.

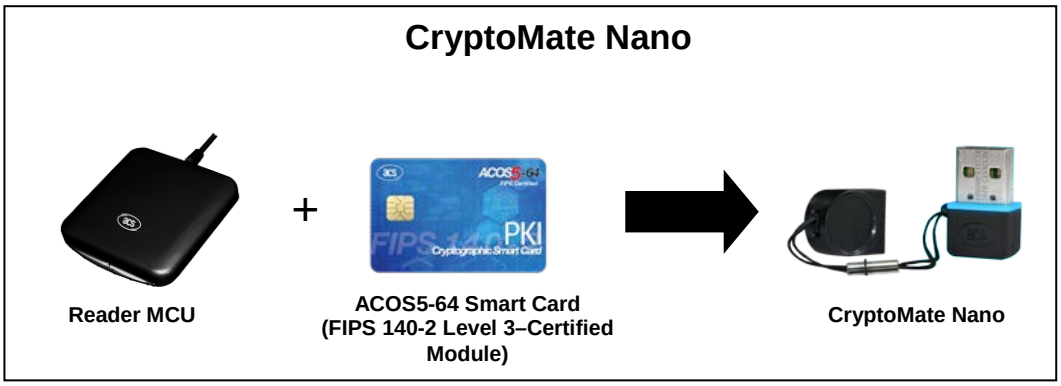


Figure 1: CryptoMate Nano System Block Diagram

For more information about the capabilities, protection and access rights of the ACOS5-64 v3.00 (FIPS 140-2 Level 3–Certified) Cryptographic Module, please check the ACOS5-64 FIPS 140-2 Level 3 Security Policy from the CMVP (Cryptographic Module Validation Program) webpage:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2664.pdf

2.0. Features

2.1. Cryptographic Smart Card Features

The CryptoMate Nano contains the ACOS5-64 v3.00 FIPS 140-2 Level 3 Certified Module which has the following features:

2.1.1. Communication Protocol

- T=0 with baud up to 223,200 bps

2.1.2. Memory

- Capacity: 64 KB
- EEPROM Endurance: 500,000 erase/write cycles
- Data Retention: 30 years

2.1.3. Cryptographic Capabilities

ACOS5-64 supports a number of cryptographic algorithms, including:

- 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, SHA256
- MAC: CBC-MAC (DES/3DES)

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 submission).
- 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) using Triple DES 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
- Certified with FIPS 140-2 Level 3
- Certified with Common Criteria EAL 5+ (Chip Level)

2.2. Token Features

2.2.1. Physical Characteristics

- Blue 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 the CryptoMate Nano for PKI applications with digital certificates, an applicable middleware is needed.

ACS offers software solutions such as the ACOS5 Minidriver and ACOS5 Client Kit so that the ACOS5-64 and CryptoMate Nano can be used with other third party applications as shown in the figure below:

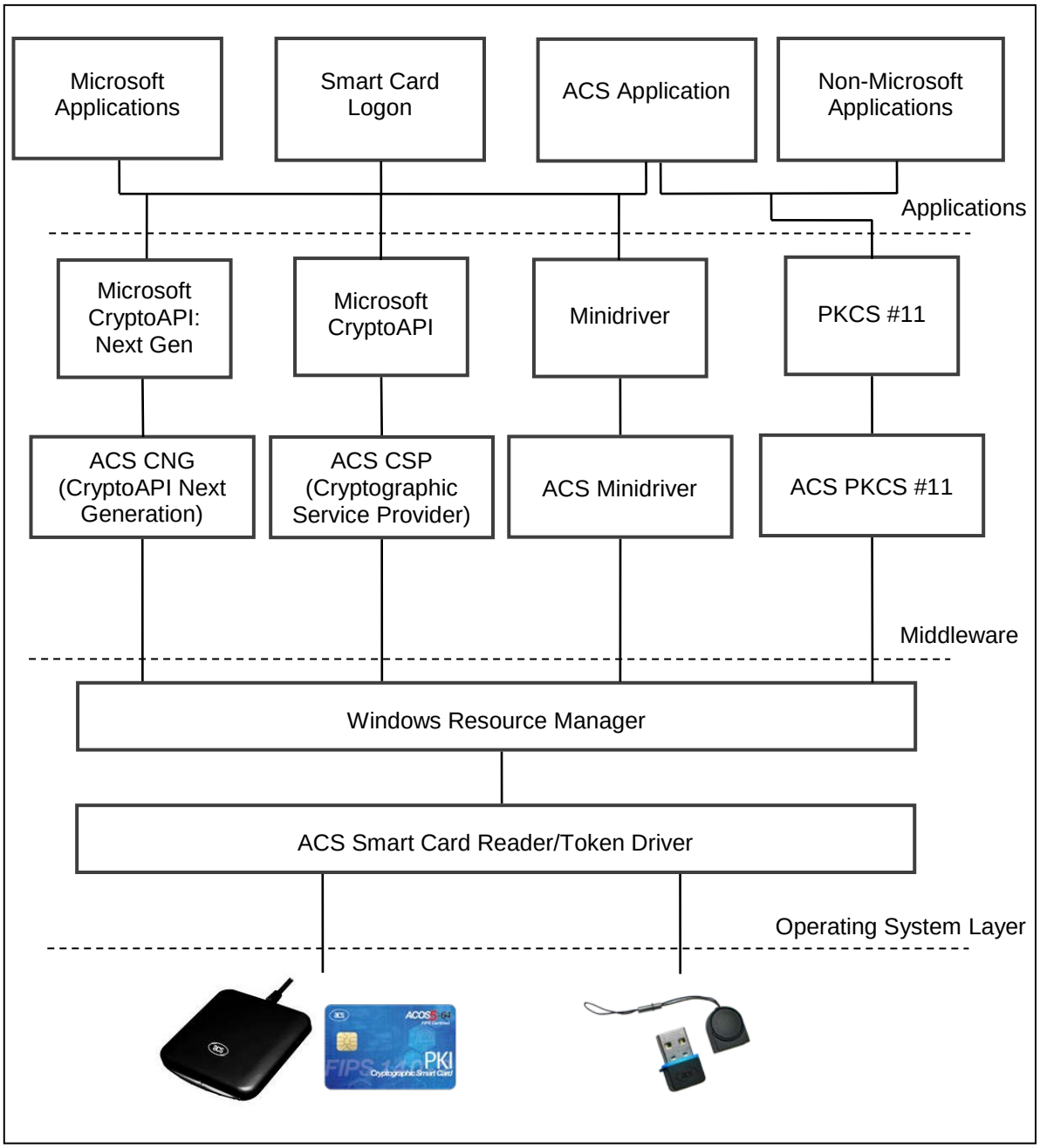
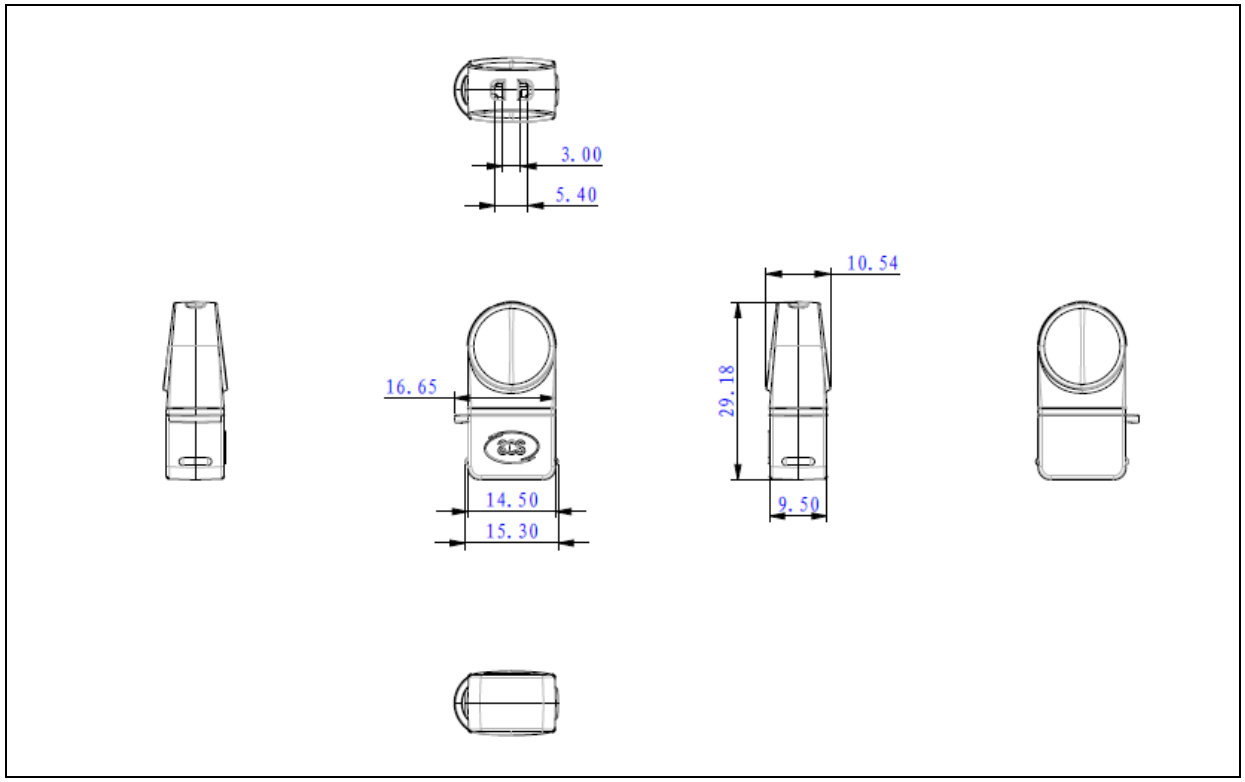


Figure 2: Middleware Diagram

Please contact us at info@acs.com.hk for inquiries about the middleware support for the CryptoMate Nano 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
ACOS5-64 Cryptographic Smart Card Module	
Memory Size	64 KB
Endurance	500,000 write/erase cycles
Data Retention	30 years
Cryptographic Capability	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)
Hashing Capability	SHA-1, SHA-256
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	Blue
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	

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