Advanced Card Systems Ltd.
Card & Reader Technologies

CryptoMate Nano USB Cryptographic Token

Technical Specifications V1.02

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

Table of Contents

List of Figures

1.0. Introduction

CryptoMate Nano is an extremely small USB PKI token that provides users with strong authentication solutions. CryptoMate Nano has a built-in ACOS5-64 v3.00 module that is FIPS 140-2 (US Federal Information Processing Standards) Level 3–certified. It uses the ACR39 Core that is also FIPS 201–certified.

The CryptoMate Nano has 64 KB of EEPROM and complies with various international standards. Its 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 is protected from being hacked or sniffed, achieving a high level of security for applications.

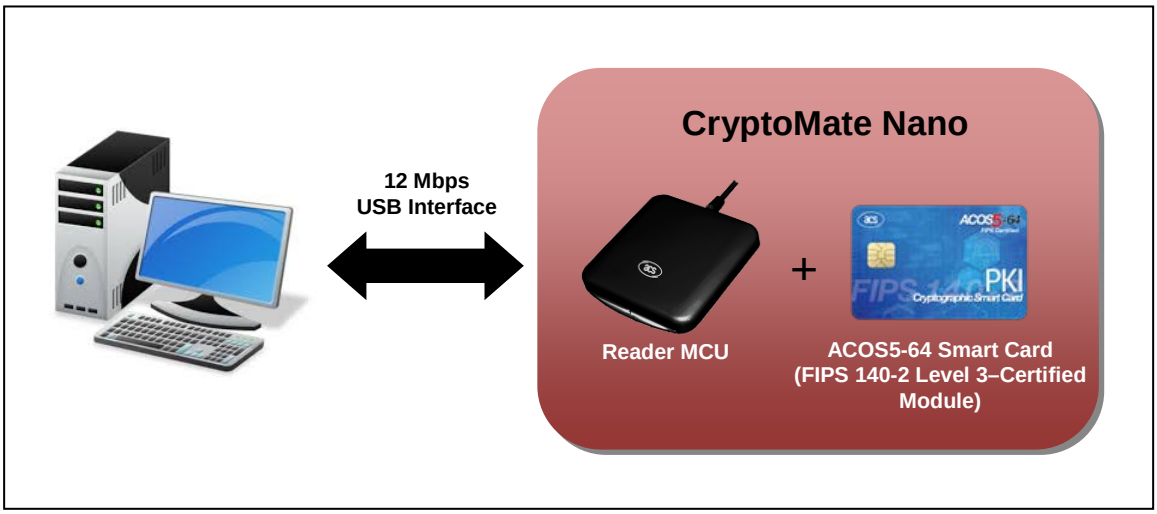


Figure 1: CryptoMate Nano System Block Diagram

2.0. Features

2.1. Cryptographic Smart Card and Crypto-processor Features

The CryptoMate Nano has an embedded ACOS5-64 v3.00 chip which has the following features:

- User memory: 64 KB of EEPROM
- Common Criteria EAL5+ (Chip Level)
- ISO 7816–compliant (parts 1, 2, 3, 4, 8, 9)
- FIPS 140-2 Level 3–certified Cryptographic Module
- Supports ISO 7816 Part 4 File Structures: Transparent, Linear-Fixed, Linear-Variable, Cyclic
- Cryptographic capabilities:
  - DES, 3DES and 3K3DES with 64/128/192 bit keys data encryption in ECB and CBC mode. AES 128/192/256-bit is also supported.
  - Secure on-card RSA key pair generation with 512-bit to 4096-bit keys in 256-bit steps
  - RSA signature computation and verification with 512-bit to 4096-bit keys in 256-bit steps
  - Private and secret key file read access can be set to “Never”
  - Mutual authentication (terminal-to-card and card-to-terminal) using Triple DES with session key generation for encryption and MAC
  - SHA-1 and SHA-256 hashing algorithm
  - Secure Messaging function for confidential and authenticated data transfers
  - 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).
  - Deterministic random number generation
- Configurable baud rates
- Configurable ATR (Answer To Reset)
- Customizable Key and PIN code
- ACS Middleware Support:
  - PKCS #11
  - Windows® Minidriver
  - Windows® CryptoAPI
  - Windows® CryptoAPI Next Generation
  - Supports X.509 V3 Certificate Storage
  - Supports SSL/TLS Certificates
  - Ease of integration with various software applications such as Internet Explorer®, Mozilla®, Microsoft® Office, and Adobe PDF Reader

For more information about ACOS5-64 (FIPS 140-2 Level 3–Certified) Cryptographic Smart Card, check the ACOS5-64 Functional Specifications in:
http://www.acs.com.hk/en/products/308/acos5-64-cryptographic-card-contact/

For more information about capabilities, protection and access rights of the ACOS5-64 v3.00 (FIPS 140-2 Level 3–Certified) Cryptographic Module, 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

2.2. Token Features

- Lightweight: 4.61 g
- Extremely small: 29.25 mm × 14.80 mm × 10.28 mm
- Keychain hole
- Smart card power supply through USB port
- Tamper-evident casing
- Blue Status LED
- Supports Android™ 3.1 and later[1]
- USB Full Speed Interface
- CCID-compliant (Plug and Play)
- CE and FCC–certified
- RoHS 2–compliant
- REACH-certified
- Microsoft® WHQL–certified

[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 Nano for PKI applications with your own digital certificates, an applicable middleware is needed. ACS provides the ACS CSP, ACS CNG and ACS Minidriver middleware for Microsoft® applications, and the ACS PKCS #11 middleware for all other applications such as Mozilla® Firefox® as shown in the figure below:

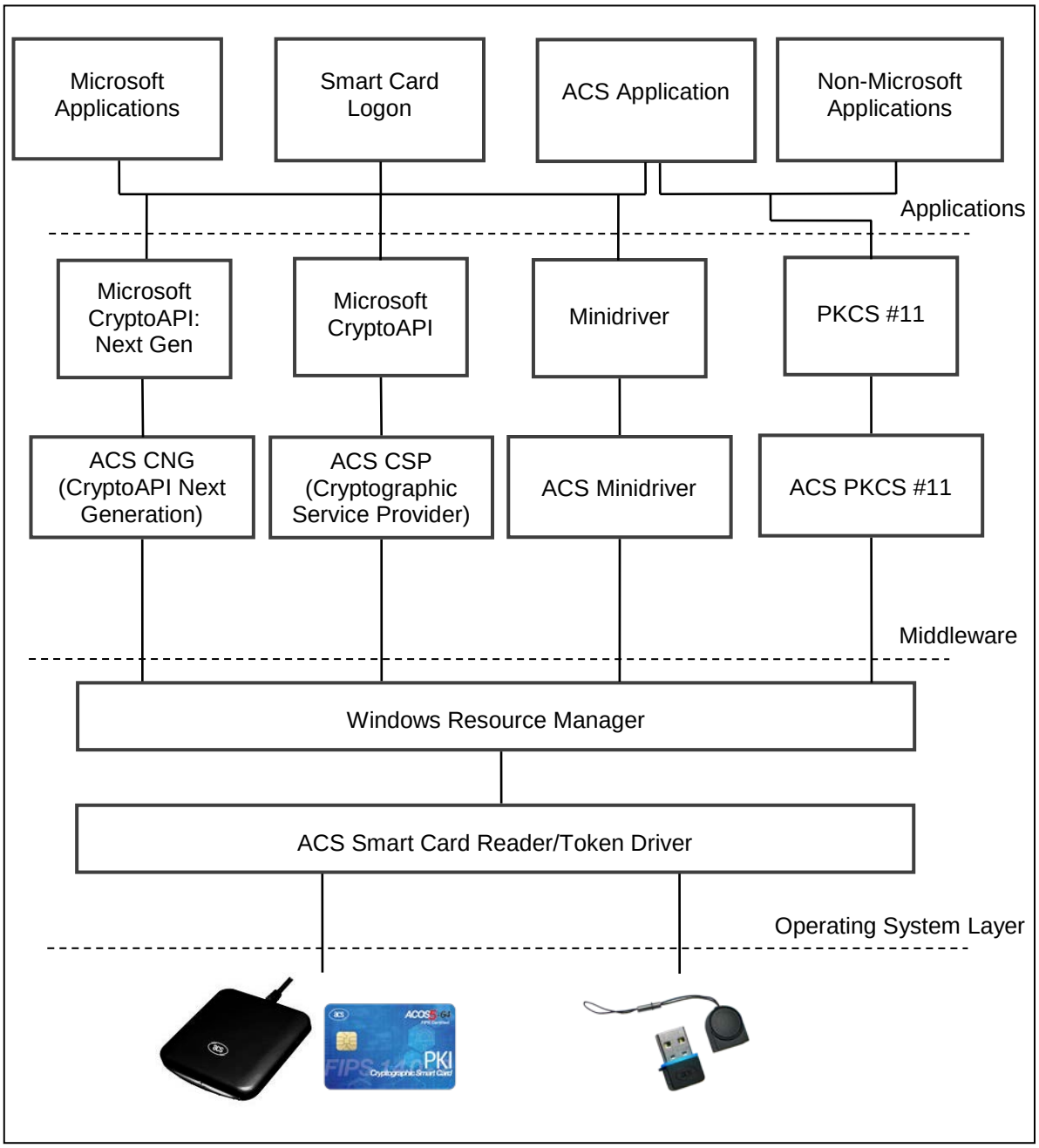
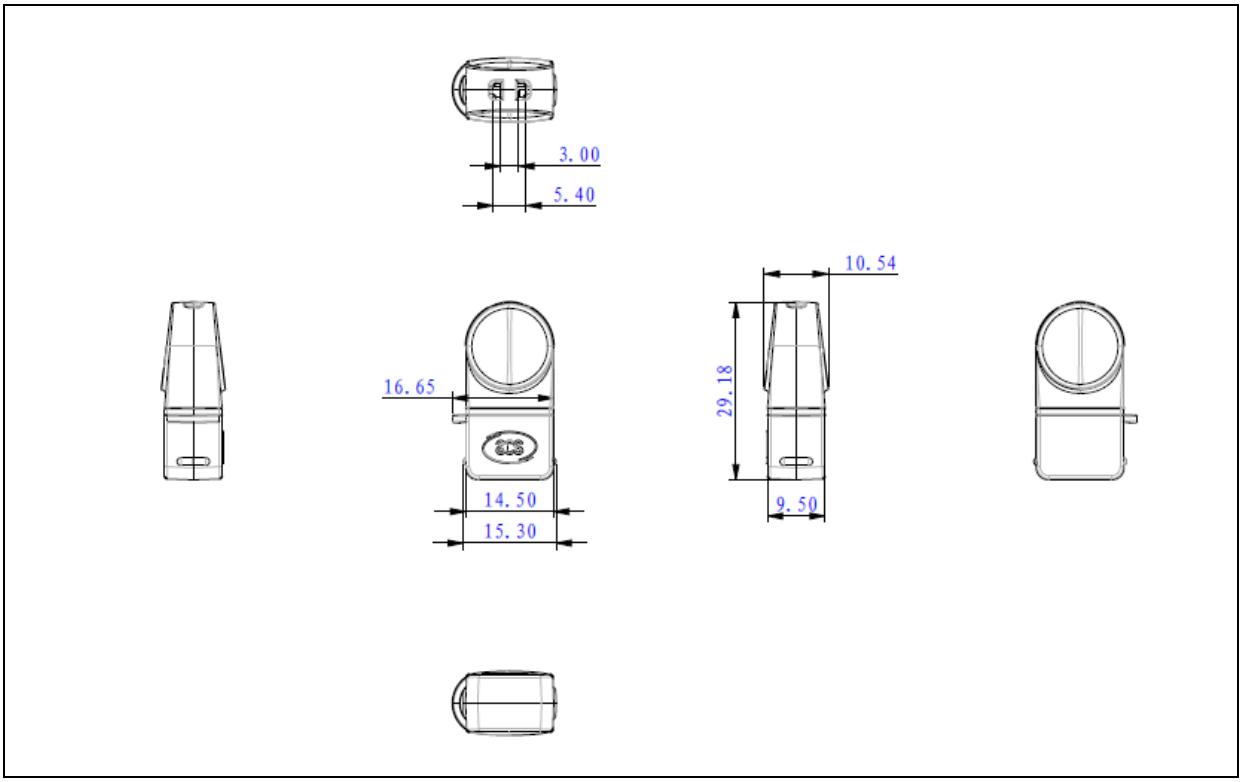


Figure 2: Middleware Diagram

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 Cryptographic Smart Card Chip	
Memory Size	64 KB
Endurance	500,000 write/erase cycles
Data Retention	10 years
Cryptographic Capability	3K3DES, 3DES (ECB, CBC), MAC, AES-128, AES-192, AES-256, RSA-512, 1024/2048/3072/4096 bits and Secure Messaging
Hashing Capability	SHA-1, SHA-256
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, SSL/TLS Certificates
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 2, REACH
FIPS 140-2 Level 3 (USA), Microsoft® WHQL

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
Linux®, Mac OS®, Android™ 3.1 and later