CryptoMate Nano

(ACOS5-64 Cryptographic USB Token)

Advanced Card Systems Ltd.
Card & Reader Technologies

Outline

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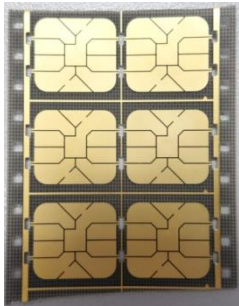3. Related Software Products
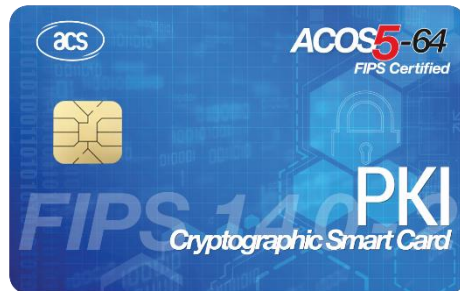
Product Information

Advanced Card Systems Ltd.
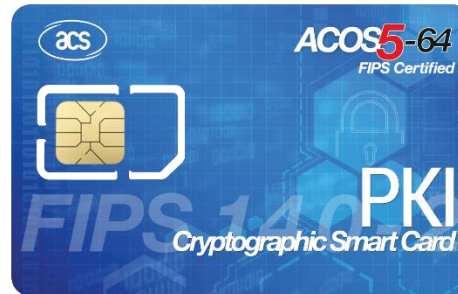Card & Reader Technologies

Product Overview

ACOS5-64 v3.00 Series

Module

Full-sized Card

SIM-sized Card

CryptoMate Nano USB Token

CRYPTOMATE NANO

ACOS5-64 Cryptographic USB Token

The CryptoMate Nano contains the FIPS 140-2 Level 3–certified ACOS5-64 v3.00 module, making it one of the most secured and portable cryptographic USB tokens in the market.
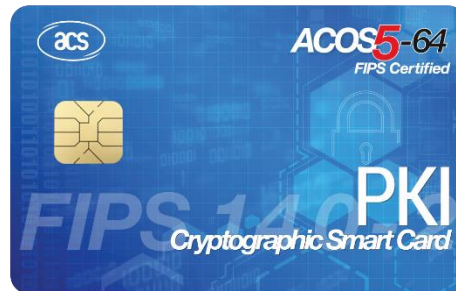
What is CryptoMate Nano?

Smart Card Reader + **ACOS5-64 Cryptographic Smart Card** = **CryptoMate Nano USB Token**
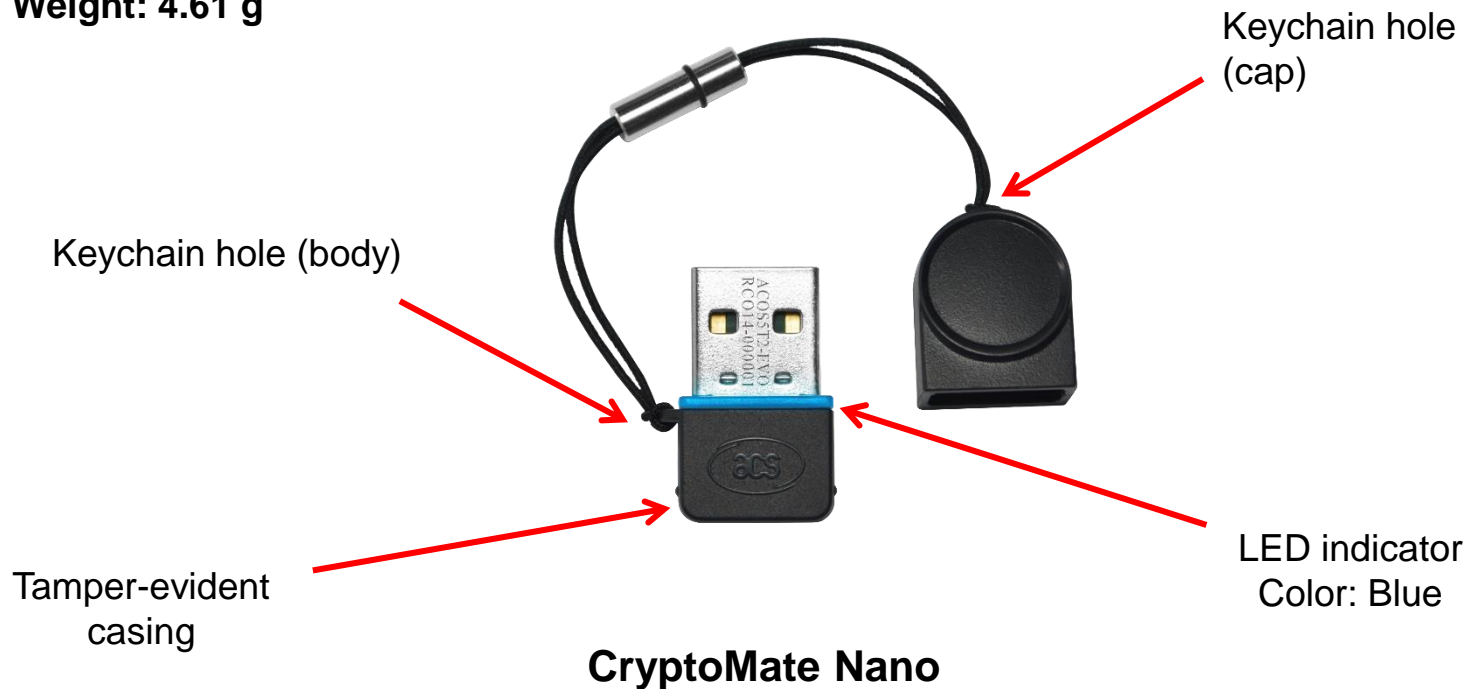
Product Overview

Physical Characteristics

Dimension:
29.25 mm (L) × 14.80 mm (W) × 10.28 mm (H)

Weight: 4.61 g

Keychain hole (cap)

Keychain hole (body)

LED indicator
Color: Blue

Tamper-evident casing

CryptoMate Nano

Key Features of CryptoMate Nano

Certifications and Compliance

- ISO 7816 Parts 1, 2, 3, 4, 8, and 9
- Common Criteria EAL5+ (Chip Level)
- X.509 V3 Certificate Storage, SSL v3
- FIPS 140-2 (US Federal Information Processing Standards) Level 3–Certified Module

Speed and Memory

- 64 KB EEPROM for Application Data
- High Speed Transmission (9,600 bps – 223,200 bps)
- Configurable ATR (Answer To Reset)
- Anti-tearing Function

Cryptographic Capabilities

- DES/3DES
- AES – 128/192/256
- RSA – up to 4,096 bits
- On-board RSA processor for key generation, signature, and encryption
- Supports SHA-1 and SHA-256

Security Functions

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

Technical Specifications

Category		CryptoMate Nano
Product Code		ACOS5T2-B100ACSA02
User EEPROM Memory		
User Memory		64 KB
Endurance *(write/erase cycle)*		500,000
ISO Standards		
Contact	ISO 7816 – 1/2/3	✓
	ISO 7816 – 4	✓
	ISO 7816 – 8/9	✓
Communication Speed and Protocol: Contact Interface		
Protocol	T=0	✓
Speed	9,600 bps – 446,400 bps	✓ TA = 96 (223,200 bps) Default
Operating Conditions		
Temperature		0 °C – 50 °C
Humidity		Max. 90% (non-condensing)

Technical Specifications

Category	CryptoMate Nano
Cryptographic Capabilities	
RSA	up to 4096 bits
DES/3DES	56/112/168-bits (ECB, CBC)
AES	128/192/256 bits (ECB, CBC)
Hash	SHA1, SHA256
MAC	CBC-MAC (DES/3DES)
Secure Messaging	✓
Mutual Authentication	✓

Certifications/Compliance

Product Applications

In what areas can we apply CryptoMate Nano?

Digital Signature

e-Government

Network Security

Windows Logon

Encryption

Email Security
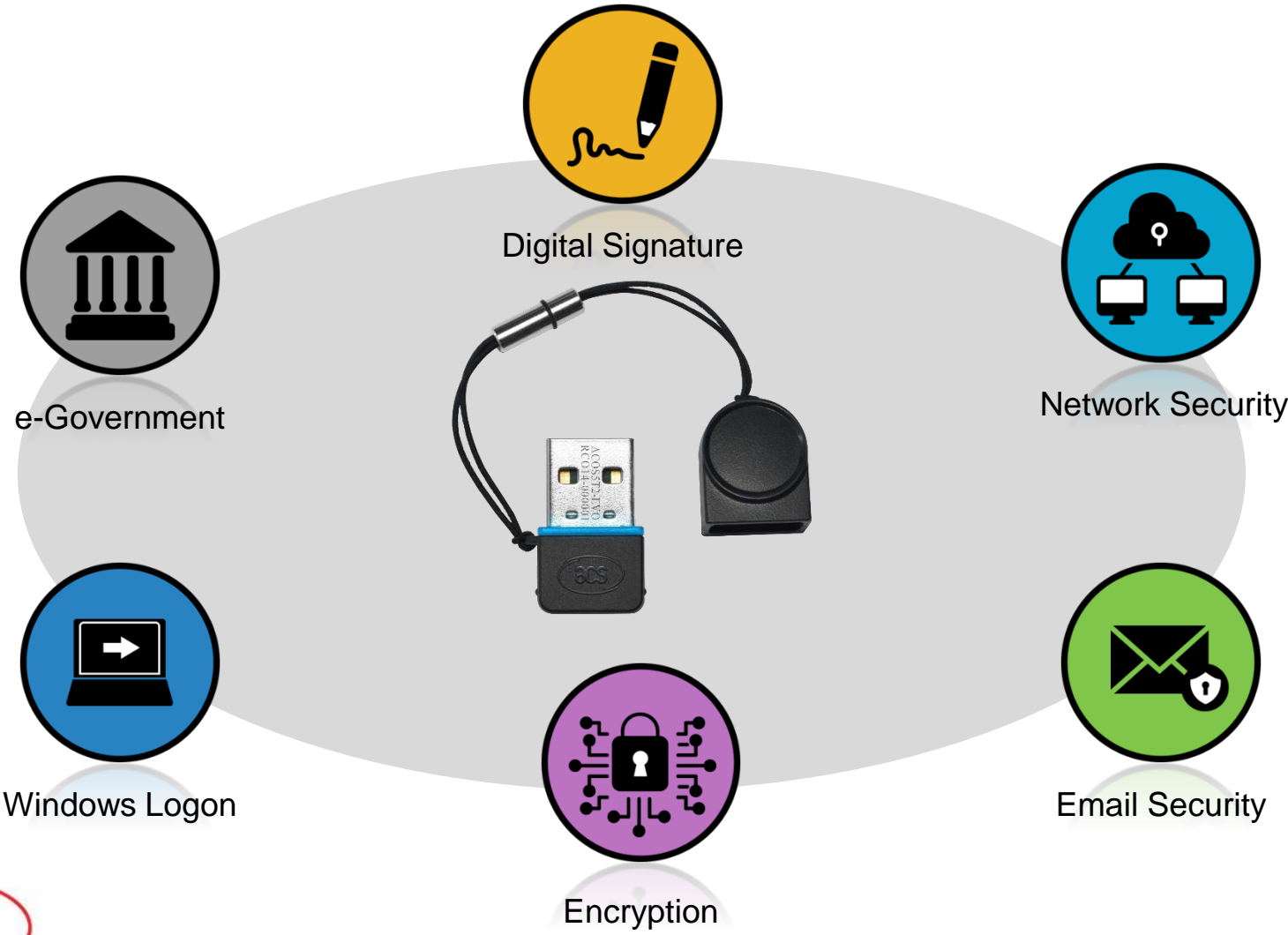
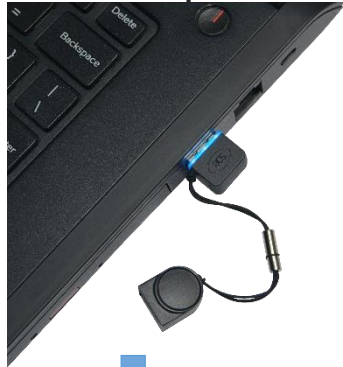# In what areas can we apply CryptoMate Nano?

Company provides the token to its employees

Employees request for a digital certificate via the company website

Employee plugs CryptoMate Nano into the computer

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

Employee stores the digital certificate in the token

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

In what areas can we apply CryptoMate Nano?

Citizens go to Registration Authorities to apply for a Digital Certificate

Certificate Authority provides the citizen with the digital certificate

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

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

Related Software Products

acs Advanced Card Systems Ltd.
Card & Reader Technologies

Client Kit

ACS offers the **ACOS5 Client Kit** to Certificate Authorities and other organizations who implement PKI solutions. It is a secure and easy-to-use software solution ideal for managing, protecting, and using digital certificates.

With the ACOS5/CryptoMate Client 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®

The Client Kit currently supports the following OS:
- Windows®
- MAC OS®
- Linux®

Contact your ACS sales representative or email us at info@acs.com.hk for more information.

ACOS5 Minidriver

For clients who want to use the ACOS5-64 v3.00 and CryptoMate Nano in Windows Environment only, ACS also provides the ACOS5 Minidriver.

The following Windows Application 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 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