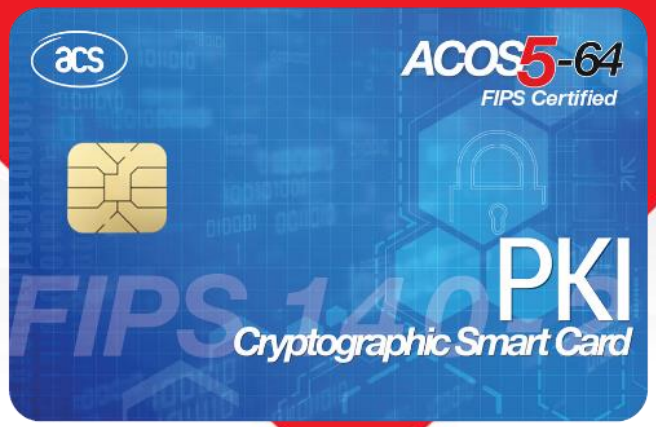
# ACOS5-64 v3.00

FIPS 140-2 Level 3–Certified

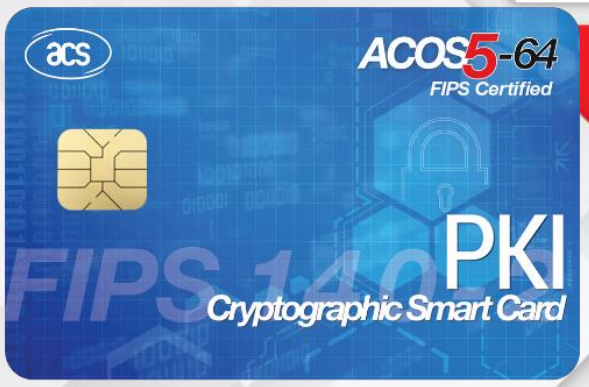



**Advanced Card Systems Ltd.**

Card & Reader Technologies

# Outline

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

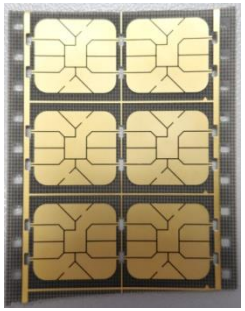



# Product Information

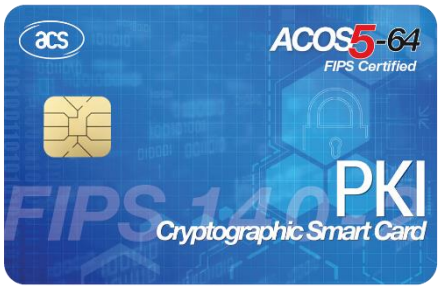
Advanced Card Systems Ltd.
Card & Reader Technologies

# Product Overview

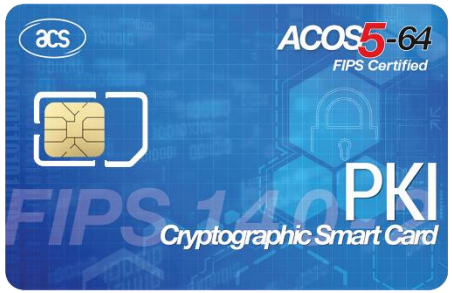
## ACOS5-64 v3.00 Series



Module




Full-sized Card




SIM-sized Card

CryptoMate Nano USB Token

# Key Features of ACOS5-64 v3.00

## Certifications and Compliance

- FIPS 140-2 Level 3–Certified
- Common Criteria EAL5+ (Chip Level)
- ISO 7816 Parts 1, 2, 3, 4, 8, and 9

## 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

- RSA – up to 4,096 bits
- AES – 128/192/256
- DES/3DES/3K3DES
- Supports SHA-1 and SHA-256
- On-board RSA processor for key generation, signature, and encryption

## Security Functions

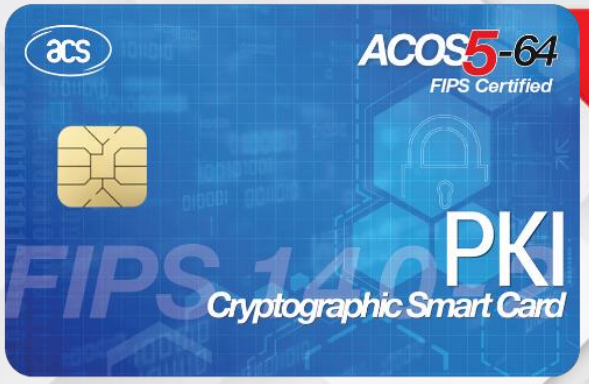
- Provides multi-level secured access hierarchy
- Supports Secure Message and MAC
- Supports Mutual Authentication and Session Key Generation

# Technical Specifications

| Category | | ACOS5-64 OS v3.00 |
|---|---|---|
| **Product Code** | | ACOS5-C1AACSA3003 (Full-sized Card)<br>ACOS5-C2AACSA3003 (SIM-sized Card) |
| **Communication Speed** | | |
| **Contact** *(Smart Card)* | 9,600 bps – 223,200 bps | ✓ |
| **USB Full Speed** | | ✓ |
| **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 | ✓ |

# Technical Specifications

| Category | ACOS5-64 OS v3.00 |
|---|---|
| **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 | ✓ |
| **Operating Conditions** | |
| Temperature | 0 °C – 50 °C |
| Humidity | Max. 90% (non-condensing) |
| MTBF | 500,000 hrs |




# Product Applications

Advanced Card Systems Ltd.
Card & Reader Technologies

# In what areas can the ACOS5-64 be used?

# In what areas can we apply ACOS5-64 V3.00?

Company provides their employees with an ID

Employees request for a digital certificate via the company website

Employee inserts the ACOS5 ID 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

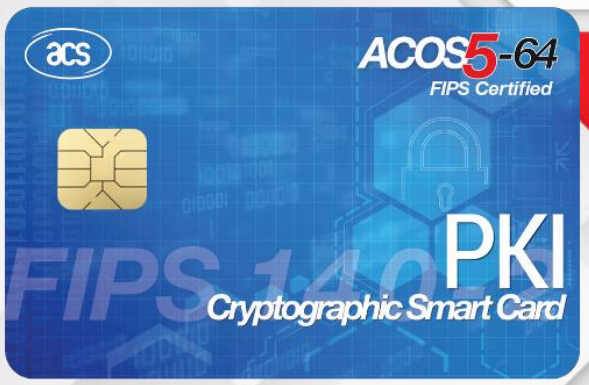
# In what areas can we apply ACOS5-64 V3.00?

**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

# 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 ACOS5-64/CryptoMate Nano 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 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 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**