



ACOS5-64 v3.00

FIPS 140-2 Level 3-Certified



Advanced Card Systems Ltd.

Card & Reader Technologies

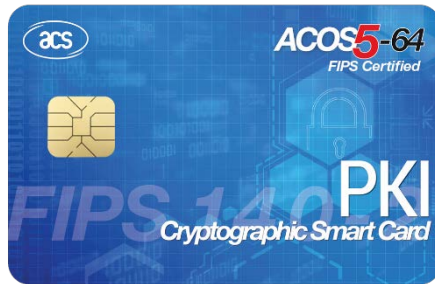
Units 2010-2013, 20th Floor
Chevalier Commercial Centre
8 Wang Hoi Road, Kowloon Bay, HK
Tel: +852-27967873 Fax: +852-27961286
info@acs.com.hk www.acs.com.hk

1. Product Overview
2. Product Features
3. Technical Specifications
4. Certifications/Compliance
5. Product Applications
6. Related Product

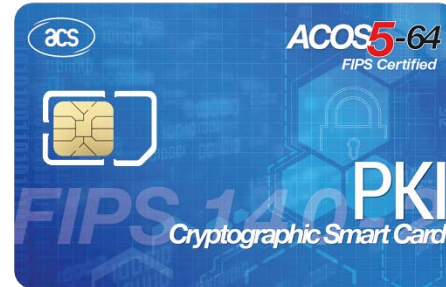
ACOS5-64 Card Operating System v3.00 Series



Module



Full-sized Card



SIM-sized Card



USB Token

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

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

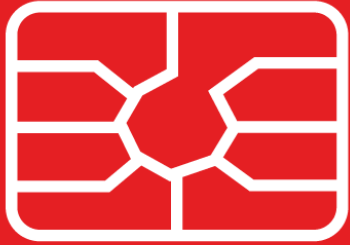
Security Functions

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

Category		ACOS5-64 OS v3.00
Product Code		ACOS5-C1AACSC3000 (Full-sized Card) ACOS5-C2AACSC3000 (SIM-sized Card)
Communication Speed		
Contact <i>(Smart Card)</i>	9,600 bps – 223,200 bps	✓
USB Full Speed		✓
User EEPROM Memory		
User Memory		64 KB
Endurance <i>(write/erase cycle)</i>		500,000
ISO Standards		
Contact	ISO 7816 – 1/2/3	✓
	ISO 7816 – 4	✓
	ISO 7816 – 8/9	✓

Category	ACOS5-64 OS v3.00
Cryptographic Capabilities	
3DES/3K3DES	✓
AES-128/192/256 bits	✓
RSA-512 to 4096 bits (in 256-bit step)	✓
SHA -1/SHA-256	✓
Secure Messaging	✓
Mutual Authentication	✓
Operating Conditions	
Temperature	0 °C – 50 °C
Humidity	Max. 90% (non-condensing)
MTBF	500,00 hrs





Product Applications



Advanced Card Systems Ltd.

Card & Reader Technologies

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



e-Government



Digital Signature



Network Security



Encryption



Windows Logon



Email Security

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



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



Employees stores the digital certificate in the ID



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



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

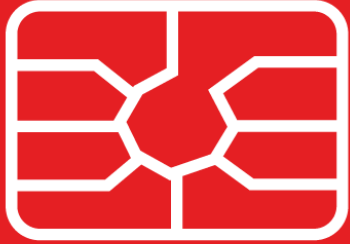


Citizen logs in to a secured website and submits the digitally signed and encrypted document to the government agency



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





Related Product



Advanced Card Systems Ltd.

Card & Reader Technologies

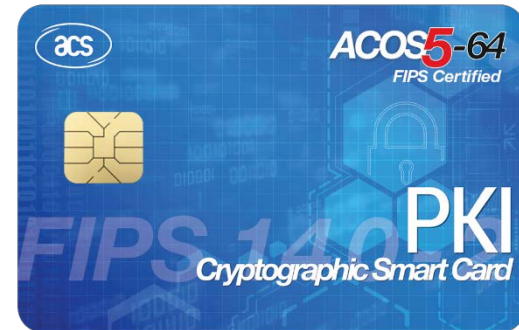
ACS provides the **ACOS5 Client Kit** to Certificate Authorities and other organizations who employ PKI solutions. It is a secure and easy-to-use software solution, ideal for managing, protecting, and using digital certificates.

ACOS5 and CryptoMate Nano securely stores all sensitive credentials and private keys. They ensure that sensitive pieces of information never leave the smart card and token, providing added security for your digital credentials.

The Client Kit contains two types of packages - Administrator Package and User Package. The Administrator Package is designed for Security Officers or Administrators in preparing the cards/tokens to be distributed for their end-users. The User Package can be distributed to end-users to manage their personal smart card/token with their digital credentials.

The Client Kit supports the following operating systems:

- Windows®
 - Windows 7 and later
- MAC OS®
 - 10.9, 10.10, 10.11 and 10.12
- Linux®
 - Debian-based
 - Debian
 - Ubuntu
 - openSUSE
 - Fedora



The Client Kit supports a number of security infrastructures and applications, including:

- Microsoft CryptoAPI, Microsoft® CNG and PKCS #11 Middleware
- Secure Online Certificate Generation
- Microsoft® Outlook, Windows® Mail, Microsoft® Outlook Express and Mozilla® Thunderbird® mail signing and encryption (S/MIME)
- Mozilla® Firefox®
- Internet Explorer®
- Windows® Smart Card Logon
- Microsoft® Office
- Open Office
- Adobe® Reader®

For more information please visit the ACS website: www.acs.com.hk



Thank You!

info@acs.com.hk

www.acs.com.hk



<http://twitter.com/SmartCardReader>



<http://www.facebook.com/AdvancedCardSystems>



<http://gplus.to/advancedcardsystems>



<http://www.youtube.com/user/AdvancedCardSystems>



Advanced Card Systems Ltd.

Card & Reader Technologies