



Advanced Card Systems Ltd.
Card & Reader Technologies



ACS5-32

CRYPTOGRAPHIC CARD

A Product Presentation



Rundown



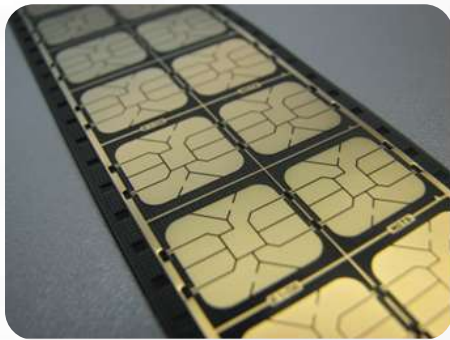
1. Product Overview
2. Product Feature
3. Product Value
4. Comparison Chart
5. Product Application
6. Product Roadmap
7. Q & A



Product Overview

ACOS5 Series (32KB EEPROM)

Cryptographic Smart Card and Token



Module



Full-Sized Card



SIM-Sized Card



CryptoMate USB
Token



Product Features

What are the Key Features of ACOS5?



High User Memory – 32KB !

International Standard Compliance
—ISO 7816-1/2/3/4/8/9

Protocol T=0

File Structure: Supports Linear
fixed record + Linear variable
record + Cyclic file + Transparent
file



ISO-7816 8 - contact module

Strong Cryptographic Capabilities:
DES + 3DES + MAC + AES-128bits +
RSA-512,1024,2048 bits + Secure
Messaging

Fast communication speed: 9,600
– 115,200 bps (switchable)

Configurable ATR +
Mutual Authentication w/
Session Key Generation



Product Value



What are the Key Features of ACOS5?

Time-to-market

Mask chip: shortens development & lead time

Unrivaled Security

Complies with ISO standards

Perfect medium for PKI applications

safeguarding your Certificate private & public keys.

High Portability

Can be used on different machines without compromising your security.

Ease of integration

Can be quickly used with PKCS-& CSP-compliant software like Netscape, Mozilla, Internet Explorer and Outlook Express

High-speed card

- 1.) Baud rate up to 115K bps
- 2.) Cryptographic processor

Meet the growing need for high security smart card application

Strong Performance

- 1.) RSA-512 signature:
62.5 ms (w/ CRT), 123.4 ms (w/o CRT)
- 2.) RSA-1024 signature:
193.9ms sec (w/CRT), 604.8ms (w/o CRT)
- 3.) RSA-2048 signature:
1081.2 ms (w/CRT)



Comparison Chart

Comparison Chart

Category	ACOS3		ACOS6-SAM	ACOS5
Product Code	ACOS3-16	ACOS3-24/64	ACOS6-16	ACOS5-32
Modules				
ISO 7816 compliant 6-contact module	✓			
ISO 7816 compliant 8-contact module		✓	✓	✓
Communication Speed				
9,600 bps (default)	✓	✓	✓	✓
14,400 bps	✓	✓	✓	
28,800 bps	✓	✓	✓	✓
115,200 bps	✓	✓	✓	
223,200 bps	✓	✓	✓	



Comparison Chart

Category	ACOS3		ACOS6-SAM	ACOS5
Product Code	ACOS3-16	ACOS3-24/64	ACOS6-16	ACOS5-32
EEPROM				
User Memory (byte)	16K	24K/64K	16K	32K
Configuration				
Configurable ATR	✓	✓	✓	✓
Configurable Baud Rate	✓	✓	✓	✓
Protocol				
T=0	✓	✓	✓	✓
Standard				
ISO 7816 - 1/2/3	✓	✓	✓	✓
ISO 7816 - 4			✓	✓
ISO 7816 - 8/9				✓



Comparison Chart



Category	ACOS3		ACOS6-SAM	ACOS5
Product Code	ACOS3-16	ACOS3-24/64	ACOS6-16	ACOS5-32
File Systems				
Directory File			✓	✓
Transparent (Binary) File		✓	✓	✓
Linear Fixed Record	✓	✓	✓	✓
Linear variable Record			✓	✓
Cyclic File			✓	✓
Security Keys				
User, Admin & Application Specified PIN Support	✓	✓		
DES/3DES key x2	✓	✓		
Customizable PIN & Key Codes			✓	✓



Comparison Chart



Category	ACOS3		ACOS6-SAM	ACOS5
Product Code	ACOS3-16	ACOS3-24/64	ACOS6-16	ACOS5-32
Cryptographic Capabilities				
DES	✓	✓	✓	✓
3DES	✓	✓	✓	✓
MAC	✓	✓	✓	✓
AES-128 bits				✓
RSA-512, 1024, 2048 bits				✓
Secure Messaging		✓	✓	✓
EEPROM Endurance				
100,000 write/erase cycles	✓	✓	✓	
500,000 write/erase cycles				✓
Data Retention				
10 years	✓	✓	✓	✓



Comparison Chart



Category	ACOS3		ACOS6-SAM	ACOS5
Product Code	ACOS3-16	ACOS3-24/64	ACOS6-16	ACOS5-32
Applications				
Customer Loyalty	✓	✓		✓
Payment System	✓	✓		✓
E-Purse	✓	✓		
Network Security	✓	✓		✓
Corporate Identity	✓	✓		✓
Microsoft Windows Logon	Custom	Custom		✓
PKI Application				✓
Cryptographic Middleware Layers CSP & PKCS#11				✓
Security Access Module (SAM)			✓	



Product Application



In what areas can we apply ACOS5?



Network Security



PKI
Application



Corporate Security/
Identification



Payment system /
e-Purse



Secure Email



Windows Logon
(Custom)



Physical Access
Control





Related Products

ACOS5 Related Products

for End Customers
(Enterprise Use)



CryptoMate Client Kit

For Developers



ACOS5 SDK

ACOS5 Related Products

CryptoMate Client Kit CD Contents

- CSP middleware
enabling your ACOS5 card and reader work with Microsoft browsers and email clients
- PKCS middleware
enabling your ACOS5 card and reader work with Netscape browsers and email clients.
- Smart Card Certificate Manager
allowing you to manage your electronic Certificates in your ACOS5 Cryptographic smart card
- Client Kit Manuals



ACOS5 SDK CD Contents

- CSP middleware
enabling your ACOS5 card and reader work with Microsoft browsers and email clients
- PKCS middleware
enabling your ACOS5 card and reader work with Netscape browsers and email clients.
- Smart Card Certificate Manager
allowing you to manage your electronic Certificates in your ACOS5 Cryptographic smart card
- ACS Card Tool
allowing you to send commands directly to your any PCSC-compliant smart card reader and cards including ACOS5 cards.
- ACR38 PC/SC drivers
- Reference Manual
for ACOS5 Cryptographic card & ACR38 smart card readers





Product Roadmap



Product Roadmap and Schedule



Apr 06 Jun 06 Sep 06

ACOS3-16

ACOS5-32

ACOS5-SDK

Jan 08 Jun 08

ACOS3-24

ACOS3-64

2006

2007

2008

2009

ACOS5-USB
Token
(CryptoMate)

ACOS5-CTM
EVK

ACOS5-64

Q2 09



Mar 07

Ordering Information



Ordering Information

Products	Description
ACOS5-32-GP	ACOS 32K bytes cryptographic card (glossy PVC)
ACOS5-32-SIM-GP	ACOS 32K bytes cryptographic SIM card (glossy PVC)
SDK-ACOS5	ACOS5 Software Development Kit
ACOS5-CTM-R	CryptoMate USB Token, RoHS -compliant
EVK-ACOS5-CTM	CryptoMate Client Kit



Thank You!!!

More information on:

<http://www.acs.com.hk/acos5.php>

