ACOS6-SAM

Secure Access Module Card (SAM)

Advanced Card Systems Ltd.
Card & Reader Technologies

Outline

1. Product Information
   - Product Overview
   - Product Features
   - Technical Specifications
2. Product Applications
3. Related Software Product

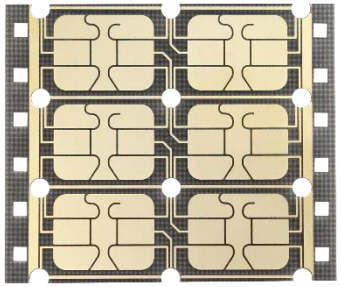
Product Information

Advanced Card Systems Ltd.
Card & Reader Technologies

Product Overview

ACOS6S-C (64 KB EEPROM)

Secure Access Module (SAM) Card



Module

SIM-sized card

Key Features of ACOS6S-C

Supports Various Client Cards

- ACOS3
- ACOS6
- ACOS7
- ACOS10
- MIFARE Ultralight® C
- MIFARE® DESFire®
- MIFARE® DESFire® EV1
- MIFARE® DESFire® EV2
- MIFARE® DESFire® Light
- MIFARE Plus®

Security Features

- DES, 2K3DES, 3K3DES (ECB, CBC)
- AES: 128/192 bits (ECB, CBC)
- FIPS 140-2 compliant hardware-based random number generator
- Session key based on random numbers
- Key pair for mutual authentication
- Secure Messaging function for confidential and authenticated data transfers
- Multilevel secured access hierarchy

Compliance to Standards

- ISO 7816 Parts 1, 2, 3, 4
- ISO 7816 Part 4 File Structures: Transparent, Linear-Fixed, Linear-Variable, Cyclic

Storage and other Features

- 64 KB EEPROM Size
- High Baud rate of up to 223 Kbps
- Anti-tearing capability

Technical Specifications

	ACOS6-SAM
Product Code	ACOS6S-C
User EEPROM Memory	
User Memory	64 KB
Compliance to ISO Standards	
ISO 7816 – 1/2/3	✓
ISO 7816 – 4	✓
Communication Speed and Protocol: Contact Interface	
Protocol	T=0
Speed	223.2 kbps
Operating Conditions	
Temperature	-25 °C to 85 °C

Technical Specifications

	ACOS6-SAM
File System	
Transparent (Binary File)	✓
Linear Fixed Record	✓
Linear Variable Record	✓
Cyclic File	✓
Cryptographic Capabilities	
DES/3DES	56/112/168 bits
AES	128/192 bits
Secure Messaging	✓
Mutual Authentication	✓
Random Number Generator	✓

Technical Specifications

	ACOS6-SAM
Secure Access Module Compatibility	
ACOS3	✓
ACOS6	✓
ACOS7	✓
ACOS10	✓
MIFARE Ultralight® C	✓
MIFARE® DESFire®	✓
MIFARE® DESFire® EV1	✓
MIFARE® DESFire® EV2	✓
MIFARE® DESFire® Light	✓
MIFARE Plus®	✓

Product Applications

Advanced Card Systems Ltd.
Card & Reader Technologies

In what areas can we apply ACOS6S-C?

How to use ACOS6S-C with Client Cards?

ACOS6S-C

+

Client Card

Mutual Authentication — Perform mutual authentication process and generate a session key

Key Diversification — Initialize client card (e.g., ACOS3/ ACOS6) with diversified keys based on the card's serial number

Secure Messaging — Perform secure messaging with client card (e.g., ACOS3/ACOS6)

Cryptographic Computation — Compute MAC for the PURSE

How to use ACOS6S-C with Client Cards?

e-Purse Application for a Merchant

Card Issuance and Card Usage

1. During the Card Issuance Stage, the ACOS6-SAM is used to store Diversified Keys when initializing client cards (ACOS3/ACOS6) for a Payment/e-Purse Application.

2. The customer receives the card, and tops up the card in a kiosk (e.g. an ACR900 device). The client card (ACOS3/ACOS6) is authenticated by the terminal and vice versa. This process is called mutual authentication, and is made possible by the ACOS6-SAM card inside the terminal.

3. Customer purchases items using the card and a merchant's PIN-pad terminal.

4. Mutual Authentication is once again performed and a session key is also generated as proof of the transaction. This is possible because of the ACOS6-SAM card stored in the PIN-pad terminal.

Related Software Products

Advanced Card Systems Ltd.
Card & Reader Technologies

Software Development Kits

ACOS6 Software Development Kit (SDK)

Develop your own smart card applications

For Developers

To develop multi-application and purse applications in:
- ACOS6 SAM card
- ACOS6 Smart Card
- ACOS3 Smart Card *

**You may also use the ACOS3 card as a client card when using the ACOS6-SAM.*

For further details about the SDK, please visit:
ACOS6 SDK: http://www.acs.com.hk/en/products/117/acos6-multi-application-purse-smart-card-software-development-kit/

Thank You!

Advanced Card Systems Ltd.
Card & Reader Technologies

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