Advanced Card Systems Ltd.

ACOS5-CTM
CryptoMate USB Token

Unit 1008, 10th Floor, Hongkong International Trade and Exhibition Centre
1 Trademart Drive, Kowloon Bay, Hong Kong
Tel: +852 2796 7873 Fax: +852 2796 1286 Email: info@acs.com.hk Website: www.acs.com.hk

CryptoMate USB Token

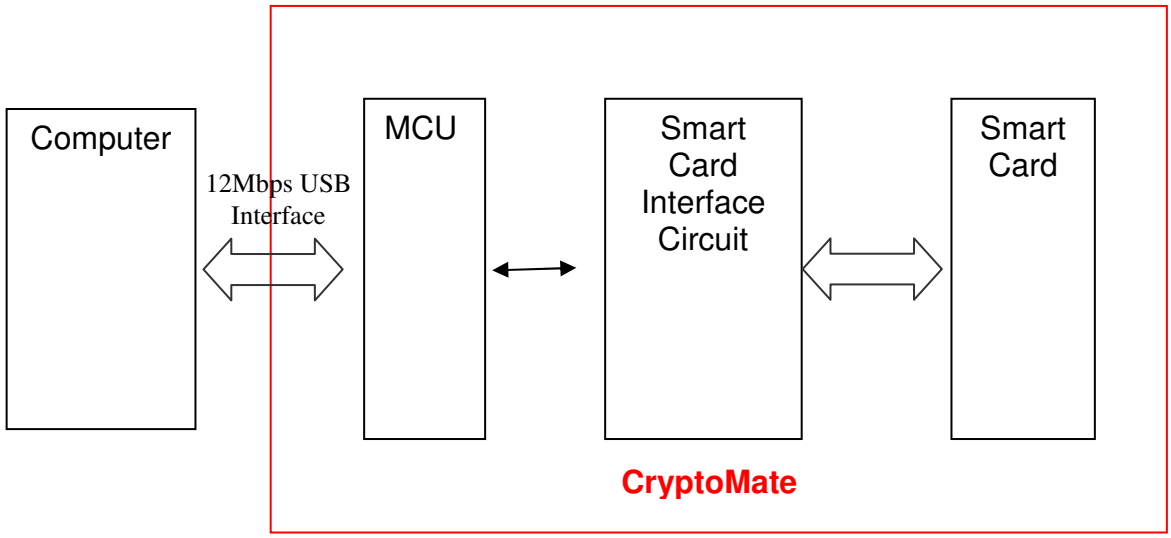
1.0 Introduction

Frustrated by network breaches like Trojan program attack, credential/password leakage, legitimate session hijacking, or all of the above? It is time for a CryptoMate.

The CryptoMate (ACOS5-CTM) is a 2-in-1 USB token, combining seamlessly the security of a cryptographic smart card chip and the convenience of a USB connector. It is always ready to be plugged into the USB port of any workstations, either for logon window or pay online. Everything is well prepared for you. You will never get into the trouble of seeking inter-operable smart card and smart card reader!

The CryptoMate is among the securest and lightest cryptographic USB tokens in the world. The built-in ACOS5 chip (32K bytes EEPROM) complies with the most stringent international standards, like ISO 7816 -3,-4-8,-9 and possess the most reliable encrypting capabilities like DES, 3DES, AES, and RSA. Though rich in features, it is merely 10 grams in weight, which is even lighter than a coin. You can pocket and use it conveniently anywhere you like.

Moreover, the CryptoMate is specially designed for PKI-based (Public Key Infrastructure) applications. Obviously, smart card technology combines with public key security system does provide a greater level of protection against hackers than a standalone public key system. All sensitive credentials and private keys are stored inside the smart card but not the vulnerable computer. As they never leave the token, ultimate security is reached.



CryptoMate System Block Diagram

Advanced Card Systems Ltd.
Unit 1008, 10th Floor
Hongkong International Trade and Exhibition Centre
1 Trademart Drive, Kowloon Bay, Hong Kong

Tel: +852 2796 7873
Website: www.acs.com.hk

Fax: +852 2796 1286
Email: info@acs.com.hk

2.0 Features

Cryptographic Smart Card & Crypto-processor

- ACS ACOS 5
- Configurable baud rates up to 115,200bps
- High user memory: 32K Bytes of EEPROM
- Supports commands for cryptographic operations, authentication and access control, compliant with ISO 7816 -4, -8, and 9.
- Supports ISO7816 part 4 file structures: transparent, linear fixed, linear variable, cyclic.
- Configurable ATR
- Customizable key and PIN code
- Supports mutual authentication with session key generation
- Cryptographic algorithm support : DES (ECB, CBC), 3DES (ECB, CBC), MAC, SHA-1, AES-128, RSA-512, 1024, and 2048
- On-board RSA processor supports fast key generation, signature and encryption.
- Secure messaging ensures confidentiality between the token and the application.
- Ease of integration: can be quickly used with PKCS#11- & CSP- compliant software like Netscape, Mozilla, Internet Explorer and Outlook
- Cryptographic service provider (CSP)supports Microsoft smart card enrollment for windows smart card user and smart card logon.

Host Interface

- Plug & Play USB full speed (12Mbps)
- Power supply through USB port

Token form factor

- Extremely light weight :10g
- Pocket size: 53.5 mm x 15.7mm x 7.8mm
- Keychain hole

Human Interface

- Green status LED

3.0 Typical Applications

- E-Commerce
- Network Security
- Corporate Identity
- File and Disk Cryptography
- Physical Access Control
- Microsoft Windows and Network Logon
- Public Key Infrastructure based Application
- PKCS#11- & CSP- compliant software applications

4.0 Middleware

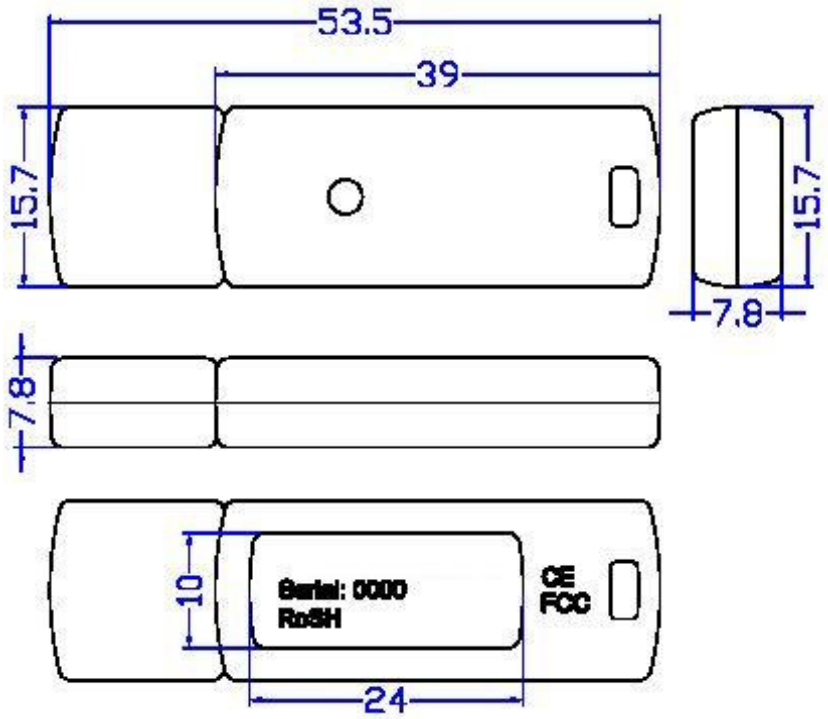
If you want to use CryptoMate for applications like PKI with your own certificates, then you need an applicable middleware for the card. For MS-CAPI applications you need a cryptographic service provider (CSP), for all other applications (Mozilla, Netscape) you need a PKCS#11. ACS is offering these two types of middleware.

Advanced Card Systems Ltd.
Unit 1008, 10th Floor
Hongkong International Trade and Exhibition Centre
1 Trademart Drive, Kowloon Bay, Hong Kong

Tel: +852 2796 7873
Website: www.acs.com.hk

Fax: +852 2796 1286
Email: info@acs.com.hk

5.0 Technical Specification



Universal Serial Bus Interface	
Type	USB full speed, four lines: +5V, GND, D+ and D-
Power source	From USB
Speed	12 Mbps (Full Speed)
ACOS5 Cryptographic Smart Card Chip	
Memory	32K bytes
Endurance	500,000 write/erase cycles
Data retention	10 years
Case	
Dimensions	53.5 mm (L) x 15.7mm (W) x 7.8mm (H)
Color	White
Weight	10 g
Status LED	
Color	Green
Operating Conditions	
Temperature	0 - 50° C
Humidity	40% - 80%

Advanced Card Systems Ltd.
Unit 1008, 10th Floor
Hongkong International Trade and Exhibition Centre
1 Trademart Drive, Kowloon Bay, Hong Kong

Tel: +852 2796 7873
Website: www.acs.com.hk

Fax: +852 2796 1286
Email: info@acs.com.hk

Standard/Certifications

USB Full Speed, ISO-7816-3, 4, 8, 9, PC/SC, X.509 V3 certificate storage, CE, FCC

OS Support

Windows 2K, XP, 2K3 Server

Middleware Support

PKCS#11, Microsoft Cryptographic Service Provider (CSP)

Cryptographic Capability

DES, 3DES, MAC, AES-128 bits, RSA-512, 1024, 2048 bits and Secure Messaging

Hashing Capability

SHA-1

OEM

OEM-Logo possible, customer-specific colors and casing

Advanced Card Systems Ltd.
Unit 1008, 10th Floor
Hongkong International Trade and Exhibition Centre
1 Trademart Drive, Kowloon Bay, Hong Kong

Tel: +852 2796 7873
Website: www.acs.com.hk

Fax: +852 2796 1286
Email: info@acs.com.hk