



Advanced Card Systems Ltd.
Card & Reader Technologies

CryptoMate



Technical Specifications



Table of Contents

1.0.	Introduction	3
2.0.	Features	4
2.1.	Cryptographic Smart Card & Crypto-processor	4
2.2.	Host Interface.....	4
2.3.	Token form factor	4
2.4.	Human Interface.....	4
3.0.	Typical Applications	5
4.0.	Middleware.....	5
5.0.	Technical Specification.....	6



1.0. Introduction

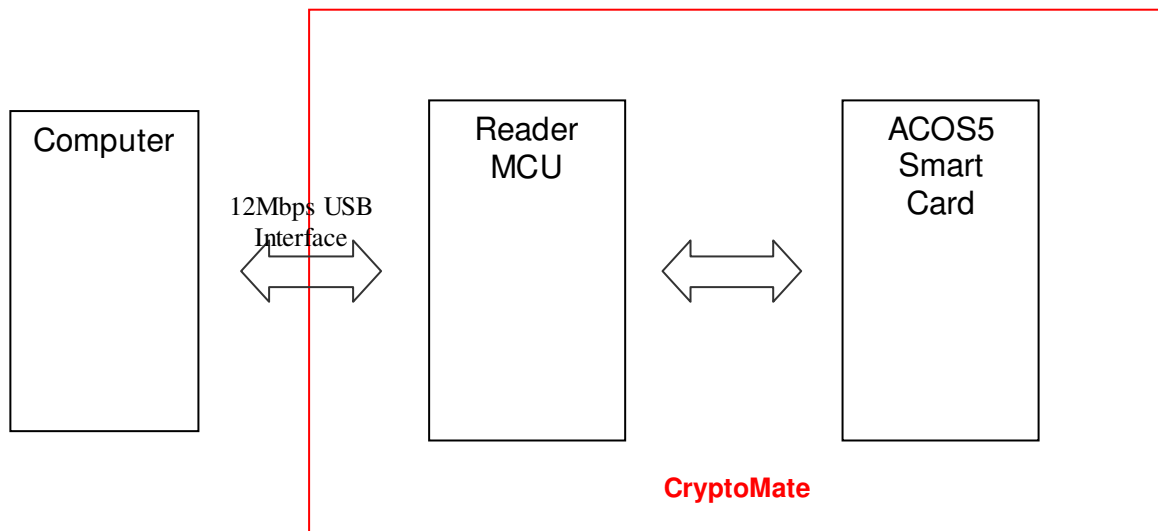


Frustrated by network breaches like Trojan program attack, credential/password leakage, legitimate session hijacking, or all of the above? It is time for a CryptoMate.

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 CC EAL5+ and the most stringent international standards, like ISO 7816 1-4, 8, 9, FIPS140-2 compatible and possesses the most reliable encrypting capabilities like DES, 3DES, AES, and RSA. Furthermore, the casing is designed to provide tamper-evidence to protect against unauthorized physical access. Though rich in features, it is merely 6 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



2.0. Features

2.1. Cryptographic Smart Card & Crypto-processor

- ◆ ACS ACOS 5
- ◆ Configurable baud rates up to 115,200bps
- ◆ High user memory: 32K Bytes of EEPROM
- ◆ Common Criteria EAL5+ (Chip level)
- ◆ Supports commands for cryptographic operations, authentication and access control, compliant with ISO 7816 1-4, 8, 9.
- ◆ FIPS140-2 (US Federal Information Processing Standards) compatible
- ◆ Under evaluation: Water resistant IPX7 – IEC 529
- ◆ 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, SHA-256*, SHA-512*, 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.
- ◆ RoHS – compliant
- ◆ Tamper-Evidence

2.2. Host Interface

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

2.3. Token form factor

- ◆ Extremely light weight :6g
- ◆ Pocket size: 53.5 mm x 15.7mm x 7.8mm
- ◆ Keychain hole

2.4. Human Interface

- ◆ Green status LED



3.0. Typical Applications

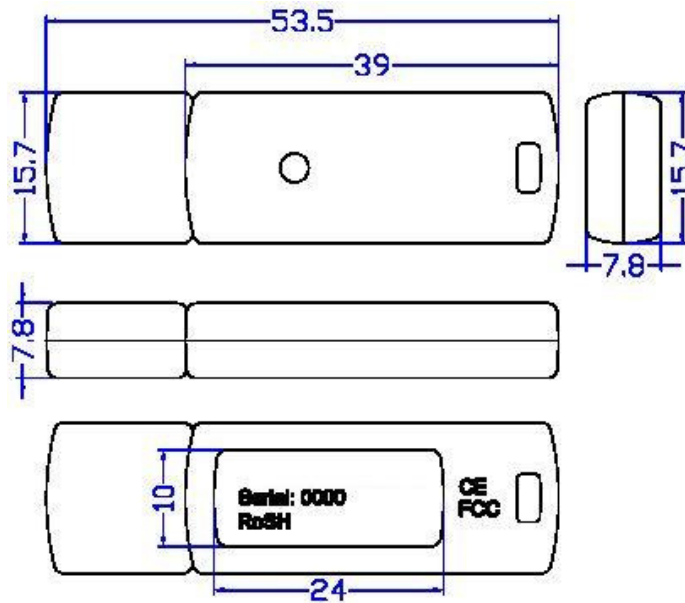
- ◆ E-Commerce
- ◆ Network Security
- ◆ Corporate Identity
- ◆ File and Disk Cryptography
- ◆ Physical/ Logical Access Control
- ◆ Microsoft Windows and Network Logon
- ◆ Public Key Infrastructure based Application
- ◆ PKCS#11- & CSP- compliant software applications

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.



5.0. Technical Specification



Universal Serial Bus Interface

Type.....USB full speed, four lines: +5V, GND, D+ and D-
 Power sourceFrom USB
 Speed.....12 Mbps (Full Speed)

ACOS5 Cryptographic Smart Card Chip

Memory32K bytes
 Endurance500,000 write/erase cycles
 Data retention10 years

Case

Dimensions.....53.5 mm (L) x 15.7mm (W) x 7.8mm (H)
 Color.....White
 Weight.....6 g

Status LED

Color.....Green

Operating Conditions

Temperature.....0 - 50° C
 Humidity40% - 80%

Standard/Certifications

USB Full Speed, ISO 7816 1-4, 8, 9, CC EAL5+ (Chip level), FIPS140-2 compatible, PC/SC, X.509 V3 certificate storage, CE, FCC, RoHS-compliant, Tamper-evidence



OS Support

Windows 98, ME, 2000, XP, 2003, Vista, 7(beta), Linux



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, SHA-256*, SHA-512*

OEM

OEM-Logo possible, customer-specific colors and casing