Advanced Card Systems Ltd.
Card & Reader Technologies

CyptoMate64

Technical Specifications

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

Table of Contents

Figures

1.0. Introduction

CryptoMate64 is a lightweight USB token providing a strong authentication solution. With a weight of only 6 grams, it is the most secured and portable cryptographic USB token in the market.

CryptoMate64 enables one to perform digital signature, email encryption, online payments, Windows log-on and other Public Key Infrastructure (PKI) applications in one USB token. Moreover, Smart Card Minidriver is implemented, that of which enables plug-and-play feature for secure and efficient operations in both Windows and Linux environments.

The built-in ACOS5-64 chip (64 Kbytes EEPROM) complies with CC EAL5+, international standards ISO 7816 1~4, 8, 9 and it is FIPS140-2 compatible. Likewise, the casing is designed to provide tamper-evidence to against unauthorized physical access. CryptoMate64 protects all sensitive credentials and cryptographic keys with cryptographic operations such as RSA-4096, SHA-256, AES-256 and 3K 3DES performed inside the ACOS5-64-based Smart Card IC instead of the terminal. Sensitive information are protected from being hacked or sniffed. This allows ultimate security to be achieved.

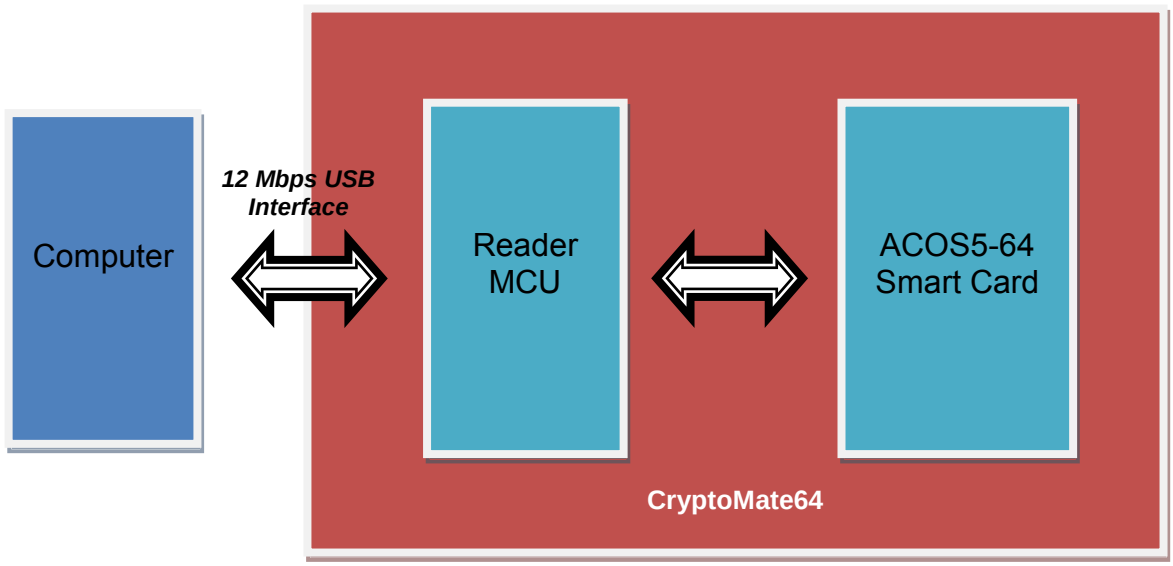


Figure 1: CryptoMate64 System Block Diagram

2.0. Features

2.1. Cryptographic Smart Card and Crypto-processor

- ACOS5-64 chip
- Configurable baud rates up to 233,200 bps
- High user memory: 64 Kbytes 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
- Water resistant IPX7 – IEC 529 (under evaluation)
- Supports ISO 7816 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: 3DES (ECB, CBC); MAC; SHA-1, SHA-256; AES-128, 192, 256; RSA-512, 1024, 2048, 3072 and 4096 bits
- 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 in PKCS #11 and CSP compliant softwares like Netscape, Mozilla, Internet Explorer and Microsoft Outlook
- CSP supports Microsoft smart card enrollment for Windows smart card user and smart card logon
- RoHS compliant
- Tamper-evidence

2.2. Host Interface

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

2.3. Token Form Factor

- Extremely lightweight: 6 grams
- Pocket size: 53.5 mm x 15.7 mm x 7.8 mm
- Keychain hole

2.4. Human Interface

- Blue status LED

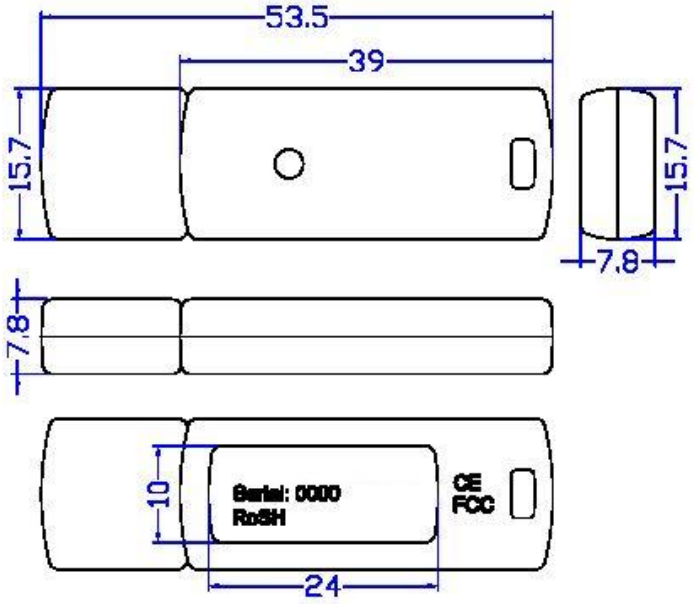
3.0. Typical Applications

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

4.0. Middleware

To use CryptoMate64 for applications like PKI with your own digital certificates, an applicable middleware is needed. ACS is providing CSP and minidriver for MS-CAPI applications, and PKCS #11 for all other applications (E.g. Mozilla and Netscape).

5.0. Technical Specifications



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 ..... 64 Kbytes
Endurance ..... 500,000 write/erase cycles
Data retention ..... 10 years

Case

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

Status LED

Color ..... Blue

Operating Conditions

Temperature ..... 0 – 50° C
Humidity ..... 40% - 80%

Compliance/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, Tamper-evidence

Operating System Support

Windows 98, ME, 2000, XP, 2003, Vista, 7, Linux

Middleware Support

PKCS#11, Microsoft Cryptographic Service Provider (CSP), Mini-Driver

Cryptographic Capability

3DES, MAC, AES-128, 192, 256 bits, RSA-512, 1024, 2048, 3072, 4096 bits and Secure Messaging

Hashing Capability

SHA-1, SHA-256

OEM

OEM-Logo possible, customer-specific colors and casing