Advanced Card Systems Ltd.
Card & Reader Technologies

CryptoMate64

Technical Specifications V1.01

Subject to change without prior notice

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

Table of Contents

List of Figures

1.0. Introduction

CryptoMate64 is a lightweight USB token that provides users with strong authentication solutions and the CCID compliant version of the CryptoMate token. Similarly, it is a lightweight token, weighing only 6 grams, making it one of the most portable and most secured cryptographic USB token in the market. It enables users to perform digital signature, email encryption, online payments, Windows log-on and other Public Key Infrastructure (PKI) applications.

CryptoMate64 has a built-in ACOS5-64 chip which has 64 KB of EEPROM complies with various international standards such as with CC EAL5+, ISO 7816 1-4, 8, 9. CryptoMate64's casing is designed to be tamper evident so that any unauthorized physical access will be easily visible. Aside from this, it also protects sensitive credentials and cryptographic keys since cryptographic operations such as RSA-4096, SHA-256, AES-256 and 3K 3DES are performed inside the ACOS5-64-based Smart Card IC inside the token. With this, important and sensitive information is protected from being hacked or sniffed achieving a high level of security for applications.

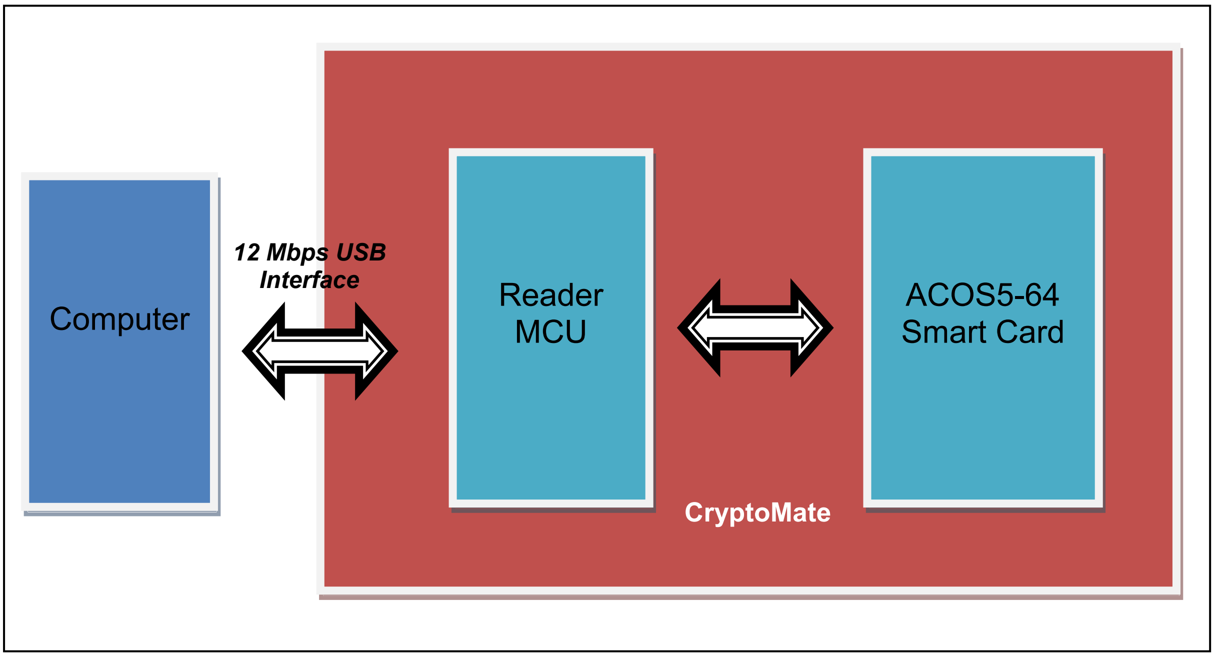


Figure 1: CryptoMate64 System Block Diagram

2.0. Features

2.1. Cryptographic Smart Card and Crypto-processor Features

- Embedded ACOS5-64 chip
- User memory: 64 KB of EEPROM
- Common Criteria EAL5+ (Chip Level)
- ISO 7816 Parts 1, 2, 3, 4, 8, 9 Compliant
- FIPS 140-2 (US Federal Information Processing Standards) compatible
- Supports ISO 7816 Part 4 File Structures: Transparent, Linear Fixed, Linear Variable, Cyclic
- Supports commands for cryptographic operations, authentication, and access control
- Supports Mutual Authentication with Session Key Generation
- Secure Messaging function that ensures confidentiality between the token and the application
- 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 that supports fast key generation, signature and encryption
- Ease of integration: can be quickly used with PKCS #11 and CSP compliant software like Netscape, Mozilla, Internet Explorer and Microsoft Outlook. Also supports Microsoft smart card enrollment for Windows smart card user and smart card logon when using CSP.
- CCID Compliant
- Supports Minidriver for Windows Operating System
- Configurable baud rates
- Configurable ATR
- Customizable Key and PIN code

2.2. Token Features

- Extremely lightweight: 6 grams
- Pocket size: 53.5 mm x 15.7 mm x 7.8 mm
- Keychain hole
- USB 2.0 Full Speed Interface
- Plug and Play
- Smart card power supply through USB port
- CE and FCC Certified
- Microsoft® WHQL Certified
- RoHS Compliance
- Tamper-evident casing
- Blue Status LED

3.0. Typical Applications

- e-Government
- e-Banking and e-Payment
- e-Healthcare
- Network Security
- Access Control
- Loyalty Program
- Public Key Infrastructure
- File and Disk Cryptography
- Microsoft Windows and Network Logon

4.0. Middleware

To use the CryptoMate64 for PKI applications with your own digital certificates, an applicable middleware is needed. ACS provides the CSP and minidriver for MS-CAPI applications, and PKCS #11 for all other applications such as Mozilla Firefox as shown in the figure below:

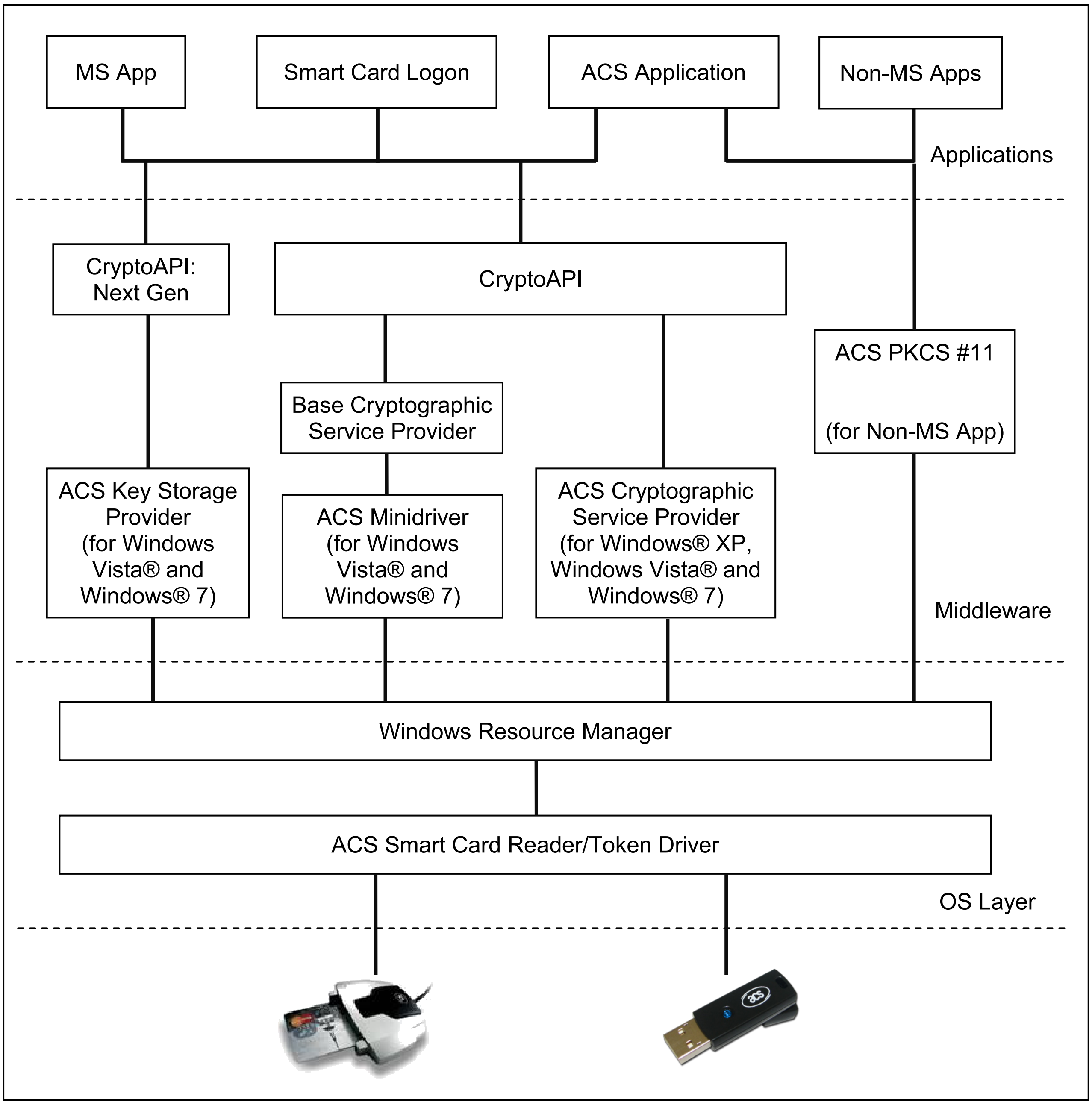
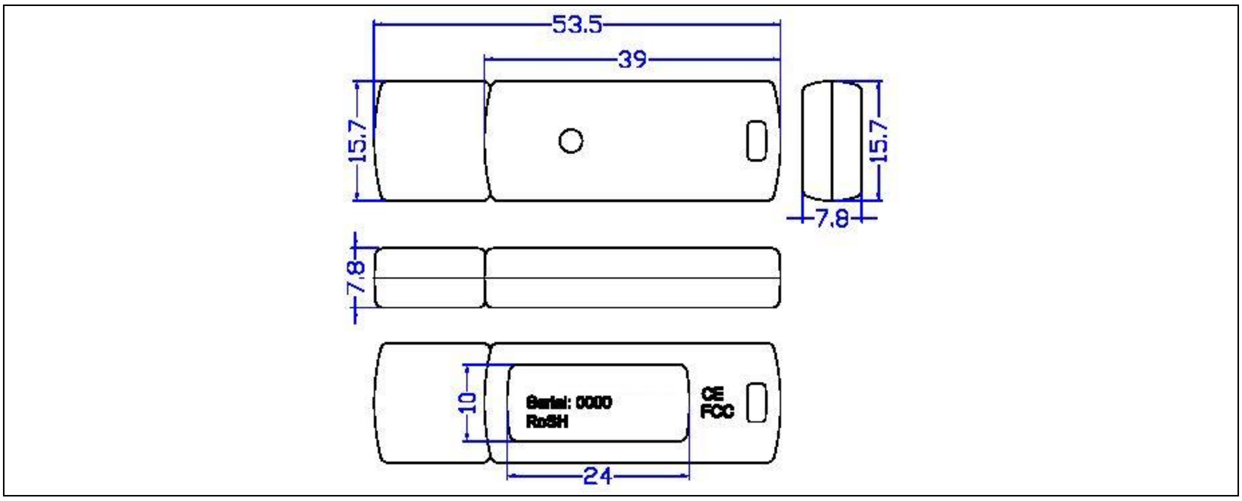

MS App
Smart Card Logon
ACS Application
Non-MS Apps
Applications
CryptoAPI: Next Gen
CryptoAPI
ACS PKCS #11 (for Non-MS App)
Base Cryptographic Service Provider
ACS Key Storage Provider (for Windows Vista® and Windows® 7)
ACS Minidriver (for Windows Vista® and Windows® 7)
ACS Cryptographic Service Provider (for Windows® XP, Windows Vista® and Windows® 7)
Middleware
Windows Resource Manager
ACS Smart Card Reader/Token Driver
OS Layer

Figure 2: Middleware Diagram

Kindly contact us at: info@acs.com.hk for inquiries about the middleware support for the CryptoMate64 token.

5.0. Technical Specifications



Universal Serial Bus Interface

Type	USB Full Speed, four lines: +5 V, GND, D+ and D-
Power Source	From USB
Speed	12 Mbps (Full Speed)

ACOS5 Cryptographic Smart Card Chip

Memory	64 KB of EEPROM
Endurance	500,000 write/erase cycles
Data Retention	10 years
Cryptographic Capability	3DES (ECB, CBC), MAC, AES-128, AES-192, AES-256, RSA-512, 1024, 2048, 3072 and 4096 bits and Secure Messaging
Hashing Capability	SHA-1, SHA-256
Middleware Support	PKCS #11, Microsoft Cryptographic Service Provider (CSP), Minidriver

Physical Specifications

Dimensions	53.5 mm (L) x 15.7 mm (W) x 7.8 mm (H)
Color	Black
Weight	6 g
Status LED	Blue Color
Casing	Tamper-evident
Others	Keychain hole for portability

Operating Conditions

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

Certifications/Compliance

ISO 7816, Common Criteria EAL5+ (Chip level), FIPS 140-2, PC/SC, CE, FCC, RoHS, USB Full Speed
Microsoft® WHQL Windows® 2000, Windows® XP, Windows Vista®, Windows® 7, Windows® 8, Windows® Server 2012

Device Driver Operating System Support

Windows® 2000, Windows® XP, Windows Vista®, Windows® 7, Windows® 8, Windows® Server 2012
Linux®, Mac

Minidriver Support

Windows® Vista, Windows® 7

OEM

OEM-Logo possible, customer-specific colors and casing