



**Advanced Card Systems Ltd.**  
Card & Reader Technologies

# CryptoMate64 USB Cryptographic Token



Technical Specifications V1.06



## Table of Contents

- 1.0. Introduction ..... 3**
- 2.0. Features ..... 4**
  - 2.1. Cryptographic Smart Card and Crypto-processor Features ..... 4
  - 2.2. Token Features ..... 4
- 3.0. Typical Applications ..... 5**
- 4.0. Middleware ..... 6**
- 5.0. Technical Specifications ..... 7**

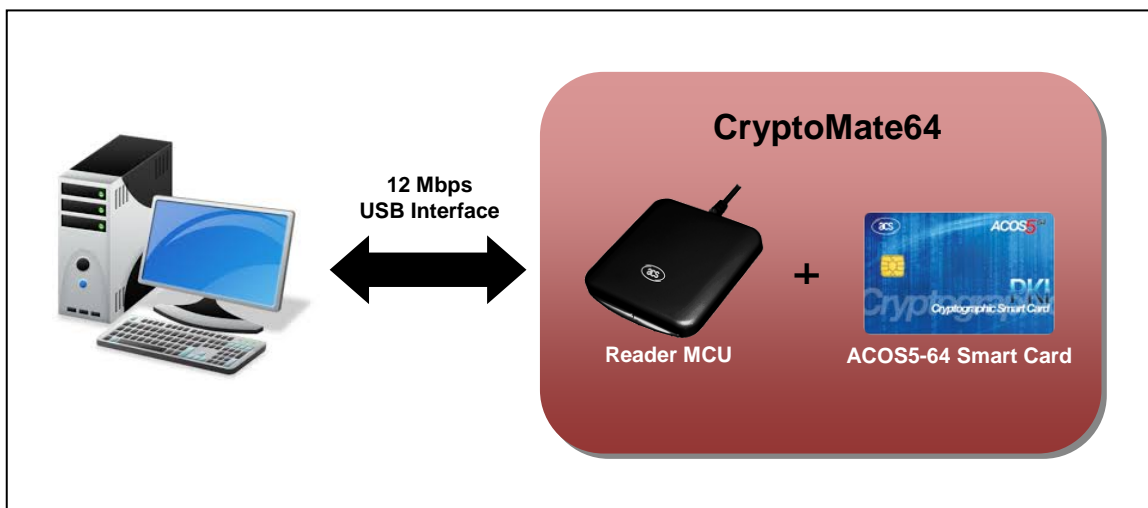
## List of Figures

- Figure 1 : CryptoMate64 System Block Diagram ..... 3**
- Figure 2 : Middleware Diagram ..... 6**

## 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 that complies with various international standards such as Common Criteria EAL5+, ISO 7816 (parts 1-4, 8, 9), and FIPS 140-2 (US Federal Information Processing Standards). 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 3K3DES 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

Furthermore, CryptoMate-64 supports a number of security infrastructures and applications, including:

- Microsoft® Crypto-API, Microsoft® CNG and PKCS #11 Middleware
- Secure Online Certificate Generation
- Microsoft® Outlook, Windows® Mail, Microsoft® Outlook Express and Mozilla® Thunderbird® mail signing and encryption (S/MIME)
- Mozilla® Firefox®
- Internet Explorer®
- Windows® Smart Card Log-on
- Microsoft® Office
- Libre Office
- Adobe® Reader®
- Lotus Notes®



## 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-compliant (parts 1, 2, 3, 4, 8, 9)
- FIPS 140-2-compliant
- Supports ISO 7816 Part 4 File Structures: Transparent, Linear Fixed, Linear Variable, Cyclic
- Cryptographic capabilities:
  - DES, 3DES and 3K3DES with 64/128/192 bit keys data encryption in ECB and CBC mode. AES 128/192/256-bit is also supported
  - Secure on-card RSA key pair generation with 512-bit to 4096-bit keys in 256-bit steps
  - RSA computation and verification with 512-bit to 4096-bit keys in 256-bit steps
  - Private and secret key file read access can be set to “Never”
  - Mutual authentication (terminal-to-card and card-to-terminal) using Triple DES with session key generation for encryption and MAC
  - SHA-1 and SHA-256 hashing algorithm
  - Secure Messaging function for confidential and authenticated data transfers
  - File access condition capability with ISO 7816-compliant Secure Attribute - Compact. File access is only allowed if the proper security conditions are met (e.g., PIN submission)
  - Command execution condition capability per Dedicated File (DF) with ISO 7816-compliant Secure Attribute - Extended. Commands are allowed only if the proper security conditions are met (e.g., PIN submission)
- Configurable baud rates
- Configurable ATR
- Customizable Key and PIN code
- ACS Middleware Support:
  - Ease of integration with various software applications such as Internet Explorer, Mozilla, Microsoft Office, and Adobe PDF Reader
  - Supports X.509 V3 Certificate Storage
  - SSL v3

### 2.2. Token Features

- Extremely lightweight: 6 g
- Pocket size: 53.5 mm x 15.7 mm x 7.8 mm
- Keychain hole
- Tamper-evident casing
- Blue Status LED
- Smart card power supply through USB port
- Supports Android™ 3.1 and later<sup>1</sup>
- USB 2.0 Full Speed Interface
- CCID-compliant (Plug and Play)
- NSH-1 (ICP-Brazil)-certified
- CE and FCC-certified
- RoHS 2-compliant
- REACH-certified
- Microsoft® WHQL-certified

---

<sup>1</sup>Uses an ACS-defined Android Library



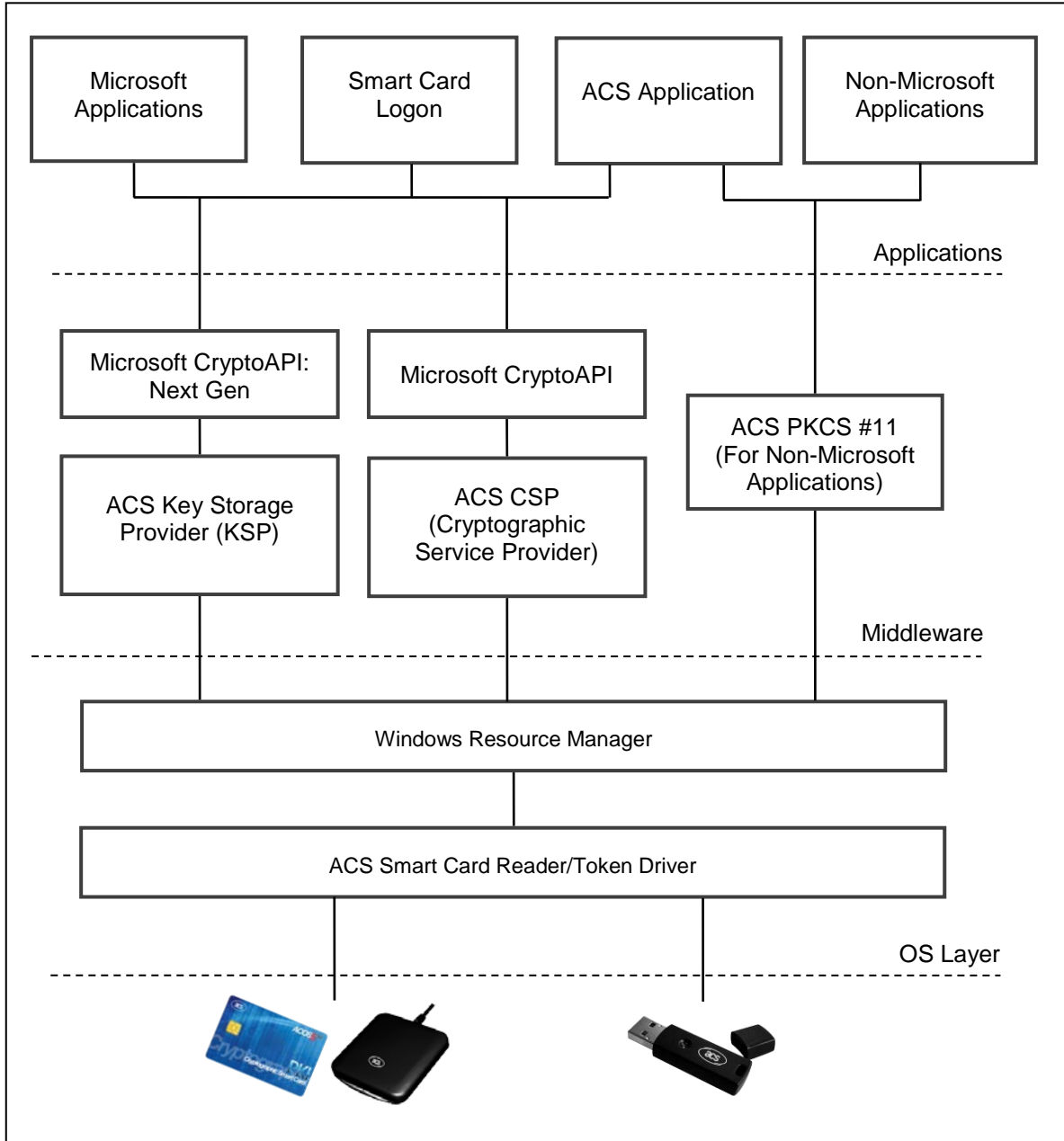
### **3.0. Typical Applications**

- e-Government
- Banking and Payment
- e-Healthcare
- Network Security
- Access Control
- Public Key Infrastructure
- Digital Signature



## 4.0. Middleware

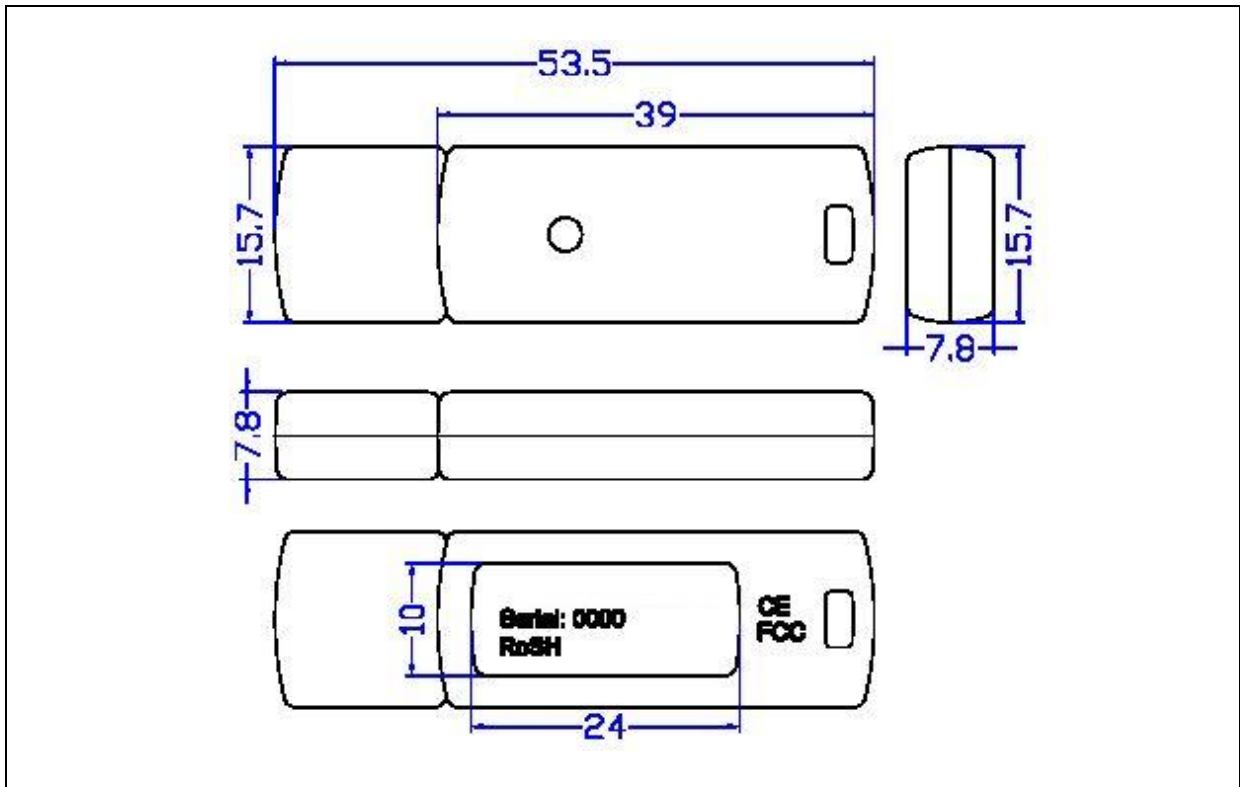
To use the CryptoMate64 for PKI applications with your own digital certificates, an applicable middleware is needed. ACS provides the ACS CSP and ACS KSP middleware for MS-CAPI applications, and the ACS PKCS #11 middleware for all other applications such as Mozilla Firefox as shown in the figure below:



**Figure 2: Middleware Diagram**

Please contact us at [info@acs.com.hk](mailto:info@acs.com.hk) for inquiries about the middleware support for the CryptoMate64 token.

## 5.0. Technical Specifications



### Physical Characteristics

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

### USB Host Interface

Protocol..... USB CCID  
Connector Type..... Standard Type A  
Power Source..... From USB port  
Speed..... USB Full Speed (12 Mbps)

### ACOS5 Cryptographic Smart Card Chip

Memory Size ..... 64 KB  
Endurance..... 500,000 write/erase cycles  
Data Retention ..... 10 years  
Cryptographic Capability ..... 3K3DES, 3DES (ECB, CBC), MAC, AES-128, AES-192, AES-256, RSA-512, 1024/2048/3072/4096 bits and Secure Messaging  
Hashing Capability ..... SHA-1, SHA-256  
Middleware Support ..... ACS PKCS #11, ACS CSP (based on Microsoft's CryptoAPI), ACS KSP (based on Microsoft's CNG), FIPS 140-2 (USA), X.509 V3 Certificate Storage, SSL v3

### Built-in Peripherals

LED ..... Blue  
Casing..... Tamper-evident  
Others ..... Keychain hole for portability

### Operating Conditions

Temperature..... 0 °C - 50 °C  
Humidity ..... Max. 90% (non-condensing)  
MTBF ..... 500,000 hrs

### Certifications/Compliance

ISO 7816, USB Full Speed, Common Criteria EAL5+ (Chip Level), PC/SC, CCID, CE, FCC, RoHS 2, REACH NSH-1 (ICP Brazil), FIPS 140-2 (USA), Microsoft® WHQL



**Device Driver Operating System Support**

Windows® XP, Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1, Windows® 10  
Windows® Server 2003, Windows® Server 2003 R2, Windows® Server 2008, Windows® Server 2008 R2,  
Windows® Server 2012, Windows® Server 2012 R2  
Linux®, Mac OS®, Android™ 3.1 and later



Adobe and Reader are registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.  
Android is a trademark of Google Inc.  
Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.  
Lotus Notes is a registered trademark of IBM Corporation.  
Mac OS is a trademark of Apple Inc., registered in the U.S. and other countries.  
Microsoft, Windows and Windows Vista are registered trademarks of Microsoft Corporation in the United States and/or other countries.  
Mozilla, Firefox, Thunderbird, Mozilla Firefox, and Mozilla Thunderbird are registered trademarks of Mozilla Corporation.