Advanced Card Systems Ltd.
Card & Reader Technologies

CryptoMate64

加密令牌 (USB Key)

技术规格书 V1.04

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

目录

图目录

1.0. 简介

CryptoMate64 是一款轻量级的 USB Key。它为用户提供了功能强大的身份验证解决方案，符合 CCID 标准。这款轻便的 USB Key 的重量仅为 6 克，是市场上最安全、最便携的 USB Key 之一。它能够帮助用户实现数字签名、电子邮件加密、网上支付、Windows 登录以及其它多种公钥基础设施（PKI）的应用。

CryptoMate64 内置的 ACOS5-64 芯片（64 KB EEPROM）符合 CC EAL5+以及 ISO 7816 1-4、8、9 等多种国际标准。它的外壳专门设计为具有防窃启功能，可以很轻易地发现任何未经授权的访问。另外，它在内嵌的 ACOS5-64 智能卡 IC 中执行 RSA-4096、SHA-256、AES-256 和 3KDES 加密操作，这样就可以确保所有敏感的信任证书和密钥都受到保护，使敏感的重要信息不会被黑客窃取或监听，帮助应用实现了高级别的安全性。

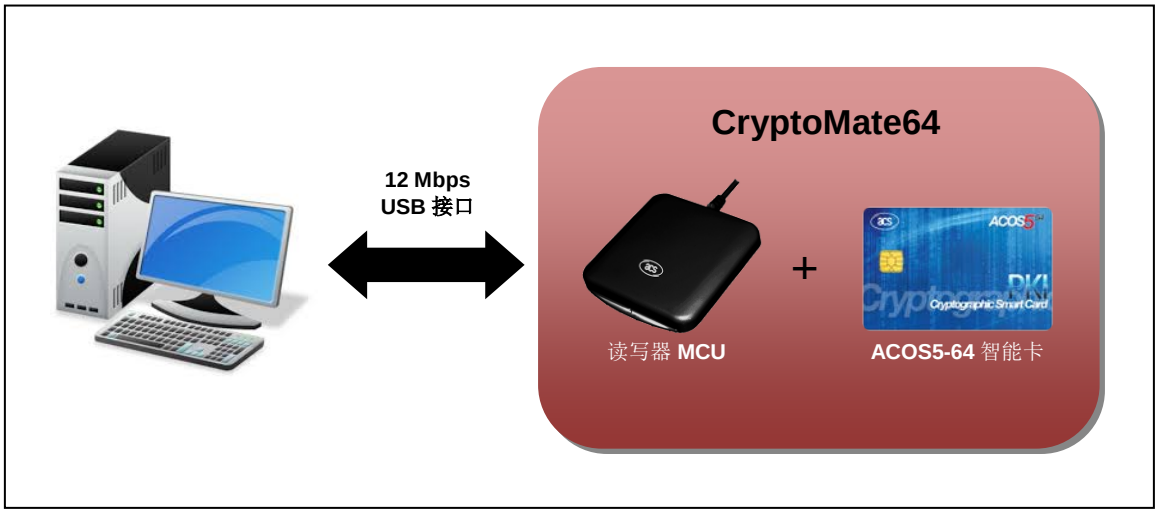


图1 ：CryptoMate64 系统框图

CryptomMate-64 支持多种安全基础设施和应用，其中包括：

- Microsoft® Crypto-API、Microsoft® CNG 以及 PKCS #11 中间件
- 安全的在线证书生成
- Microsotf® Outlook、Windows® Mail、Microsoft® Outlook Express 以及 Mozilla Thunderbird 邮件签名和加密(S/MIME)
- Mozilla Firefox
- Internet Explorer®
- Windows® 智能卡登录
- Microsoft® Office
- Open Office
- Adobe® Reader®
- Lotus Notes®

2.0. 特性

2.1. 加密智能卡和密码处理器

- 嵌入式 ACOS5-64 芯片
- 用户内存：64 KB 的 EEPROM
- 通用标准 EAL5+（芯片级）
- 符合 ISO 7816 第 1、2、3、4、8、9 部分
- 符合 FIPS 140-2（美国联邦信息处理标准）
- 支持 ISO 7816 第 4 部分规定的文件结构：透明、线性定长、线性变长、循环
- 加密功能：
  - 在 ECB 和 CBC 模式下采用 64/128/192 位密钥对数据进行 DES、3DES 和 3K3DES 加密。AES 还支持采用 128/192/256 位密钥
  - RSA 密钥对的智能卡内安全生成，采用 512 位至 4096 位长的密钥，步长为 256 位
  - RSA 运算和验证，采用 512 位至 4096 位长的密钥，步长为 256 位
  - 可设置为“永不”读取私钥和密钥文件
  - 采用 3DES 进行相互认证（终端对卡和卡对终端），生成过程密钥用于加密和 MAC
  - SHA-1 和 SHA-256 散列算法
  - 安全报文机制保证数据传输的机密性和安全性
  - 通过符合 ISO 7816 的安全属性（标准）来设置文件访问条件，访问文件前必须满足相应的安全条件（如：提交 PIN）。
  - 通过符合 ISO 7816 的安全属性（扩展）来设置各个专用文件（DF）的命令执行条件。执行命令前必须满足相应的安全条件（如：提交 PIN）。
- 能够通过 ACS 中间件与 Internet Explorer、Mozilla、Microsoft Office、以及 Adobe PDF Reader 等多种软件应用轻松集成
- 可配置波特率
- 可配置 ATR
- 可定制 KEY 与 PIN
- 支持 X.509 V3 证书存储以及 SSL v3

2.2. USB Key

- 重量轻：6 克
- 体积小：53.5 mm x 15.7 mm x 7.8 mm
- 带钥匙扣孔
- USB 2.0 全速接口
- 符合 CCID 标准（即插即用）
- 通过 USB 端口为智能卡供电
- 通过 NSH-1 (ICP-Brazil)认证
- 通过 CE 和 FCC 认证
- 通过 Microsoft® WHQL 认证
- 符合 RoHS 2
- 防窃启外壳
- 蓝色 LED 状态指示灯

3.0. 典型应用

- 电子政务
- 电子银行和电子支付
- 电子医疗
- 网络安全
- 逻辑访问控制
- 公钥基础设施
  - 数字签名
  - 安全电子邮件
  - Windows 智能卡登录

4.0. 中间件

要使用 CryptoMate64 加上您的个人数字证书用于 PKI 应用，需要一个合适的中间件。ACS 为 MS-CAPI 应用程序提供了 ACS CSP 和 ACS KSP 中间件，为所有其它应用程序（如 Mozilla Firefox）提供了 ACS PKCS #11 中间件，如下图所示：

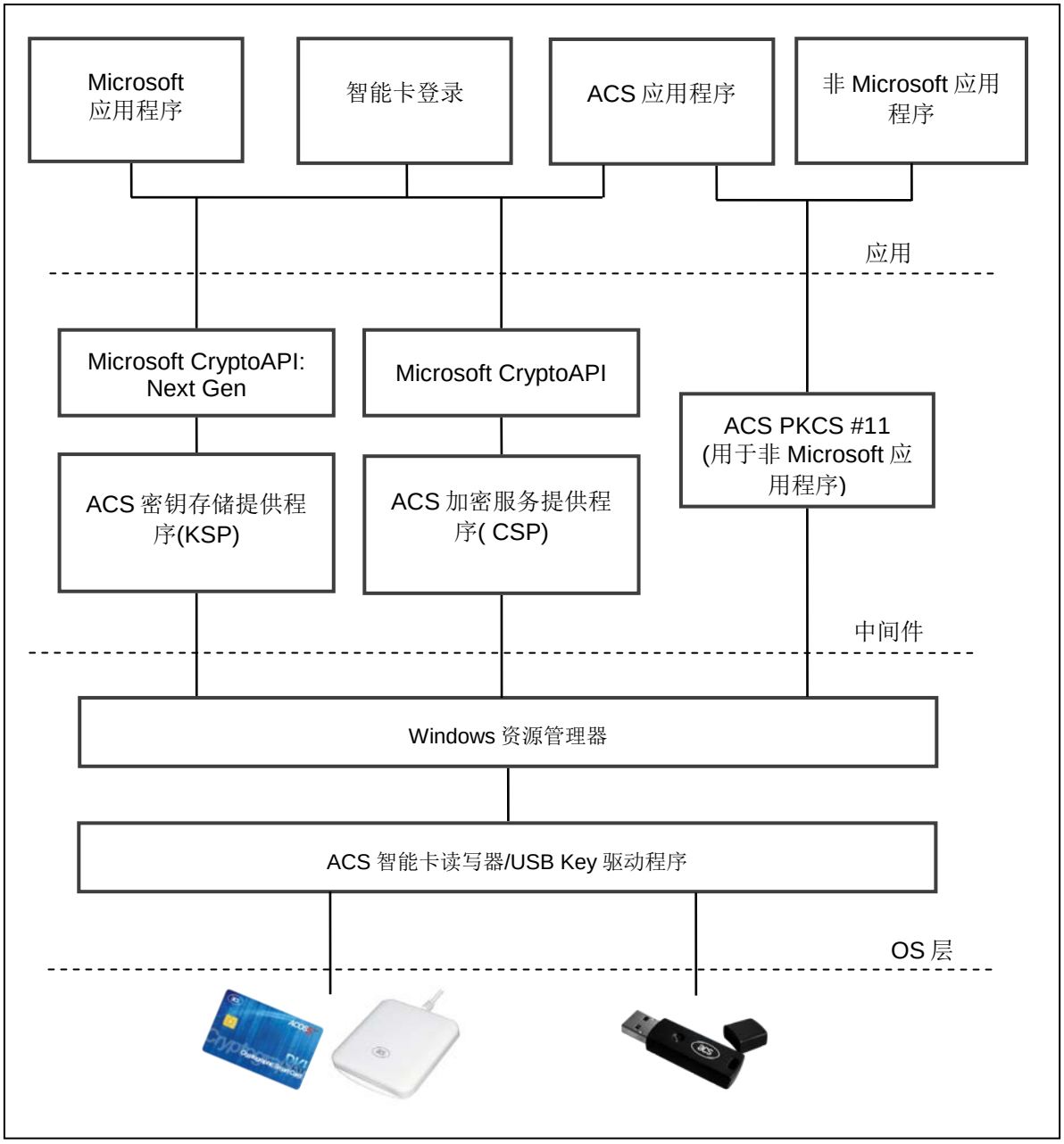
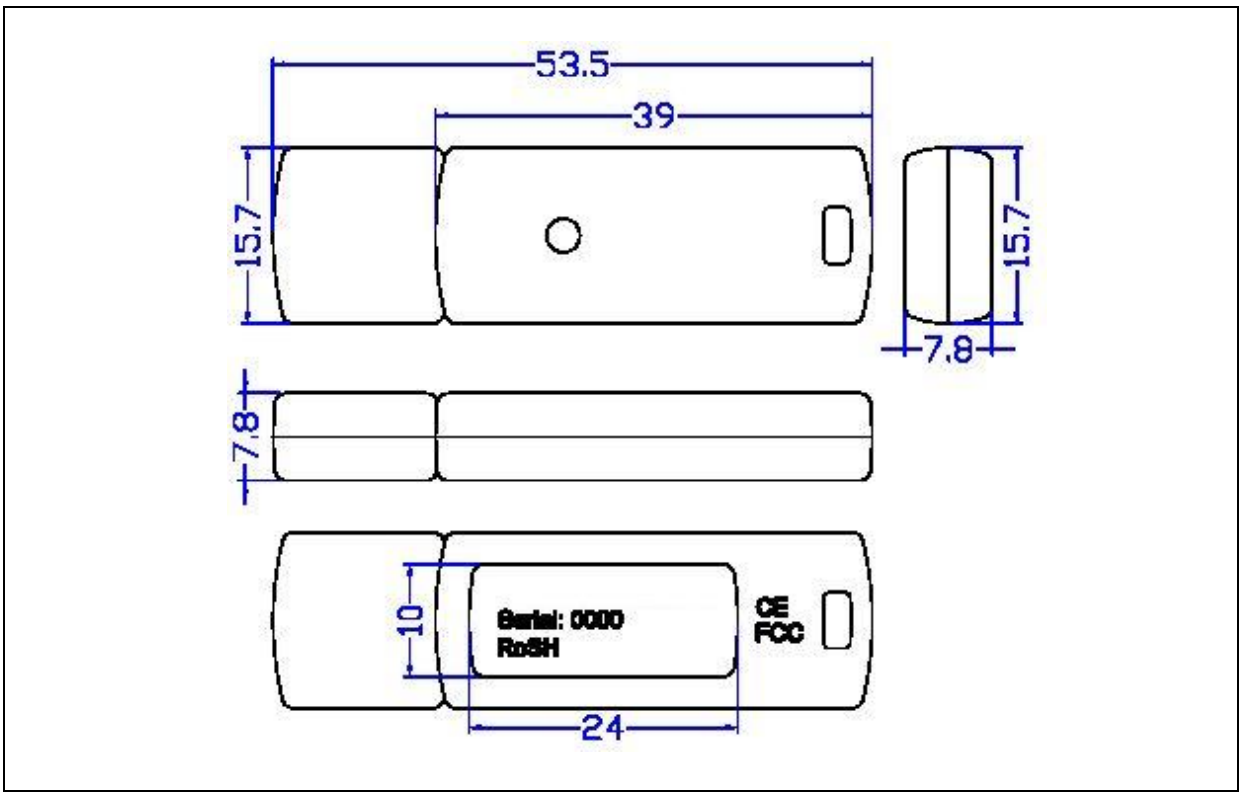


图2 ：中间件图

如需了解 CryptoMate64 USB Key 的中间件支持情况，请联系我们，邮箱地址 info@acs.com.hk。

5.0. 技术规格



USB 接口参数	
类型	USB 全速，四线：+5 V、GND、D+和 D-
电源	USB 取电
速度	12 Mbps（全速）
ACOS5 加密智能卡芯片参数	
内存	64 KB EEPROM
耐久性	50 万次擦写
数据保留期限	10 年
加密功能	3K3DES, 3DES (ECB, CBC), MAC, AES-128, AES-192, AES-256, RSA-512, 1024/2048/3072/4096 位以及安全报文发送
散列功能	SHA-1, SHA-256
中间件支持	ACS PKCS #11, ACS CSP (基于 Microsoft 的 CryptoAPI), ACS KSP (基于 Microsoft 的 CNG)
物理规格参数	
尺寸	53.5 mm (L) x 15.7 mm (W) x 7.8 mm (H)
颜色	黑色
重量	6 g
状态指示灯	蓝色
外壳	防窃启
其它	钥匙扣孔
工作条件	
温度	0 °C – 50 °C
湿度	最大 90%（无凝结）
MTBF	500,000 个小时

认证/标准

NSH-1 (ICP Brazil), FIPS 140-2 Compatible, Common Criteria EAL5+ (Chip Level), X.509 V3 Certificate Storage, SSL v3, CE, FCC, RoHS 2, PC/SC, USB Full Speed
Microsoft® WHQL for Windows® 2000, Windows® XP, Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1, Windows® Server 2008 R2, Windows® Server 2012, Windows® Server 2012 R2

设备驱动程序操作系统

Windows® XP, Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1, 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 及以上版本