CryptoMate EVO

(ACOS5-EVO加密USB令牌)

Advanced Card Systems Ltd.

Card & Reader Technologies

目录

1. 产品信息
   - 产品概览
   - 产品特性
   - 技术规格
   - 认证/标准
2. 产品应用
3. 相关软件产品

产品信息

Advanced Card Systems Ltd.
Card & Reader Technologies

产品概览

ACOS5-EVO系列

PN: ACOS5-K1A
ACOS5-EVO
（接触式）

PN: ACOS5-K1K
ACOS5-EVO
（双界面）

PN: ACOS5-K1L
ACOS5-EVO
（非接触式）

PN: ACOS5T2-B1E1
CryptoMate EVO

产品概览

CRYPTOMATE EVO

ACOS5-EVO加密USB令牌

CryptoMate EVO是CryptoMate令牌系列的最新成员。

产品内置ACOS5-EVO模块，支持ECC和RSA密钥。

产品概览

CryptoMate EVO是什么？

智能卡读写器

+

ACOS5-EVO PKI智能卡

=

CryptoMate EVO

产品概览

物理规格参数

外壳尺寸：
29.25 mm (长) × 14.80 mm (宽) × 10.28 mm (高)

重量：4.61 g

CryptoMate EVO

CryptoMate EVO的主要特性

智能卡芯片特性

- ACOS5-EVO芯片（192KB内存）
- T=0, T=1（默认）
- 可配置ATR
- 防拔插

认证和标准

- 通用标准EAL5+（芯片级）
- ISO 7816第1、2、3、4、8和9部分
- 符合FIPS 140-2 Level 3规定
- CE、FCC
- RoHS、REACH
- Microsoft WHQL

加密算法

- ECC：曲线P-224/P-256/P-384/P-521
- RSA：最高4096位
- AES：128/192/256位（ECB、CBC）
- DES/3DES：56/112/168位（ECB、CBC）
- Hash：SHA1、SHA224、SHA256、SHA384、SHA512
- MAC：CBC-MAC (DES/3DES、AES)、CMAC (3DES、AES)
- 随机数生成器

技术规格

类别		CryptoMate EVO
产品代码		ACOS5T2-B1E1ACSA03
用户EEPROM容量		
用户内存		192 KB
耐久性（擦/写次数）		50万
符合ISO标准		
接触式	ISO 7816 – 1/2/3	✓
	ISO 7816 – 4	✓
	ISO 7816 – 8/9	✓
通讯速率和协议：接触式接口		
协议	T=0	✓
	T=1	✓ （默认）
速率	9,600 bps – 446,400 bps	✓ TA = 96（223,200 bps） 默认
工作条件		
温度		0 °C – 50 °C
湿度		最大90%（无冷凝）

技术规格

类别	CryptoMate EVO
加密功能	
ECC	P-224/P-256/P-384/P-521
RSA	最高4096位
DES/3DES	56/112/168位（ECB, CBC）
AES	128/192/256位（ECB、CBC）
Hash	SHA1、SHA224、SHA256、SHA384、SHA512
MAC	CBC-MAC（DES/3DES、AES）、CMAC（3DES、AES）
安全报文	✓
相互认证	✓

认证/标准


RoHS
COMPLIANT
REACH
COMPLIANT
Compatible with
Windows 7
Windows 8
Compatible
Windows 10
Compatible
CERTIFIED FOR
Windows
Server 2008
CERTIFIED FOR
Windows
Server 2008 R2
Windows
Server 2012
Certified
Windows
Server 2012 R2
Certified
Windows
Server
2016
Certified

产品应用

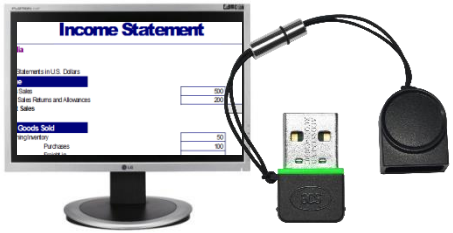
ACOS5-EVO的应用领域

CryptoMate EVO的使用场景

公民前往登记机关
申请数字证书

发证机关为
公民提供数字证书

公民使用CryptoMate EVO令牌中的数字证书对
其所得税申报表进行数字签署和加密



公民登陆安全网站，提交经过数字签署和加密
的文件给政府机关

CryptoMate EVO的使用场景

公司为员工
提供令牌

员工通过公司网站申请
数字证书

员工将CryptoMate EVO插入计算机

管理员检查信任凭证。
若一切正常则为员工提供下载链接，
以便将证书存储在ID里

员工将数字证书存储在令牌里

员工使用数字证书
签发和加密电子邮件

相关软件产品

Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS5-EVO PKI工具包

如果认证中心或其他机构有兴趣部署**支持ECC的PKI解决方案**，ACS可提供**ACOS5-EVO PKI工具包**。

通过ACOS5-EVO/CryptoMate EVO PKI工具包，可以实现：

- 安全的在线证书生成
- Microsoft® Outlook和Mozilla® Thunderbird®邮件签名和加密（S/MIME）
- Windows®智能卡登录
- Microsoft® Office
- Adobe® Reader®

如需了解更多信息，请联系ACS销售代表，访问ACS网站 http://www.acs.com.hk，或者发送电子邮件至 info@acs.com.hk 。

ACOS5微型驱动

对于只需将ACOS5-EVO和CryptoMate EVO用于Windows环境的客户，ACS还会提供ACOS5微型驱动。

支持下列Windows应用：

- Windows®智能卡登录
- Microsoft® Office
- Microsoft® Outlook邮件签名和加密（S/MIME）

通过ACOS5微型驱动初始化之后，令牌只能用于Windows操作系统，不再兼容其它ACS中间件。

如需了解更多信息，请联系ACS销售代表，访问ACS网站 http://www.acs.com.hk，或者发送电子邮件至info@acs.com.hk 。

谢谢!

Advanced Card Systems Ltd.
Card & Reader Technologies

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