ET299 U 盘锁产品白皮书

北京坚石诚信科技股份有限公司

2009-9-9

ET299 U 盘锁是在 ET299 加密锁的基础上，增加 U 盘功能的产品。U 盘空间可以分为光盘区和 U 盘区。光盘区的内容不能修改，开发商可以将软件放到该区中，废除软件安装光盘；U 盘区为最终用户提供 U 盘功能，存储数据信息。ET299 U 盘锁采用通过 EAL 4+和 IT SEC 认证的国外进口高性能智能卡硬件，安全可靠。同时 ET299 U 盘锁可以无缝集成 ET99 的各种应用，即如果您是 ET99 的用户，软件不需要做任何改动，插上 ET299 U 盘锁就可以使用，使系统从单片机升级到智能卡，并具有 U 盘功能。

产品特点：

- U 盘结合，应用软件/加密锁/U 盘三合一
- 进口高性能智能卡硬件核心，彻底杜绝复制风
- 通过国际权威安全机构检测和认证（EAL 4+和 IT SEC 认证）
- 完全符合 CE 和 FCC 标准
- 全系统兼容的高速 HID 无驱 USB 设备
- USB 通讯硬件级加密，有效保证了传输数据的安全性
- 完善易用的 API 接口调用
- 超强外壳保护工具
- 硬件内部支持 1024 位 RSA 非对称运算
- 硬件内部支持 3DES 对称运算
- 硬件内部支持 HMAC-MD5 运算
- 6K 字节安全存储空间，用户级别读写控制
- 8 个 32 字节 HMAC-MD5 密钥
- 8 个 16 字节 3DES 密钥
- 自定义 SN
- 安全远程升级
- Windows、Linux、Mac 跨平台支持

硬件参数:

核心芯片	国外进口高性能智能卡，通过国际权威安全机构检测和认证（EAL 4+和 IT SEC 认证），彻底杜绝硬件复制。
硬件序列号	全球唯一 64 位（bit）硬件序列号
自定义 SN	120 字节可自定义 SN
安全存储空间	6K 字节
非对称加解密算法	硬件内部支持 1024 位 RSA 非对称算法
对称加解密算法	硬件内部支持 3DES 对称算法
散列算法	硬件内完成 HMAC-MD5 运算
安全密钥存储区	8 个 32 字节的 HMAC-MD5 密钥存储区，硬件保证该存储区中的密钥只能在锁内参与 HMAC-MD5 运算，无法被读取或导出。
安全密钥存储区	8 个 16 字节 3DES 密钥存储区。
读次数	没有限制
写次数	至少 10 万次
USB 通讯	全系统兼容的 HID 无驱 USB 设备，USB1.1 标准设备，兼容 USB2.0 接口。硬件级通讯加密。

物理参数:

默认外壳	ABS 工程塑料，表面抛光处理
默认颜色	瓷白色
外壳尺寸	57×19×9（毫米）
重量	10 克
防水	防水浸泡 10 分钟
接口类型	USB A 类接头
工作温度	0℃～50℃
存放温度	－10℃～60℃
工作湿度	20%～80%
工作功率	250mW（最大）
工作电压	5V
工作电流	50mA（最大）

数据保存年限	至少 10 年
USB 接口号码	USB 接口上所刻的 11 位号码的前 5 位为生产日期，后 6 位为随机数。如：90822013459，表明 2009 年 8 月 22 日生产。该序列号只作为保修参考用，没有 API 接口可以得到，也不保证是唯一的。

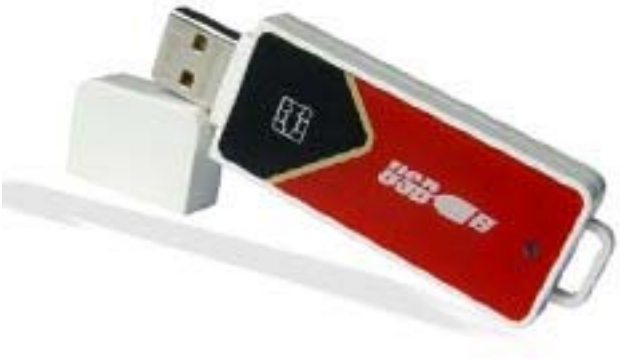
安全性：

硬件核心	国外进口高性能智能卡，通过国际权威安全机构检测和认证（EAL 4+和 IT SEC 认证），彻底杜绝硬件复制。
USB 通讯	硬件级通讯加密，有效防止 USB 端口数据劫持，保证了传输数据的安全性
非对称加解密算法	硬件内部支持 1024 位 RSA 非对称算法
对称加解密算法	硬件内部支持 3DES 对称算法
散列算法	硬件内完成 HMAC-MD5 运算
安全存储区	智能卡硬件保证锁内数据安全存储
安全密钥存储区	8 个 32 字节的 HMAC-MD5 密钥存储区，硬件保证该存储区中的密钥只能在锁内参与 HMAC-MD5 运算，无法被读取或导出。
安全密钥存储区	8 个 16 字节 3DES 密钥存储区。
外壳加密	高强度外壳保护
远程升级	建立在 RSA 算法体系上的安全远程升级
PID（Product IDentification）	产品 ID，用户自定义，出厂默认为 8 个 F，即“FFFFFFFF”，不区分大小写。
SO PIN（Super Officer Personal Identification Number）	管理员 PIN 码，用户自定义，出厂默认为 16 个 F，即“FFFFFFFFFFFFFFFF”，不区分大小写。
User PIN（User Personal Identification Number）	用户 PIN 码，用户自定义，出厂默认为 16 个 F，即“FFFFFFFFFFFFFFFF”，不区分大小写。
PIN 重试次数限制	SO PIN 和 User PIN 都有重试次数限制。最大重试次数可以设置为 1～15 次，当设置为 0 时，则表明 SO PIN 和 User PIN 将永远不被锁死。
全球唯一 ID	64 位（bit）
自定义 SN	120 字节可自定义 SN
超大用户空间	6K 字节，只有通过 User PIN 验证后才可以读写。

PIN 码:

PID（Product IDentification）	产品 ID,用户自定义,出厂默认为 8 个 F,即“FFFFFFFF”,不区分大小写。调用 et_FindToken 和 et_OpenToken 时输入的参数，开发商需要通过种子产生自己的 PID，以区分不同开发商之间的 ET299。种子机制的优势，种子是由开发商自己设定的一串数据,其他人即使得到 PID,但不知道产生该 PID 的种子，因此无法制作相同 PID 的 ET299。注意: 产生新的 PID 后，请保留好新产生的 PID 和种子。
SO PIN （Super Officer Personal Identification Number）	管理员 PIN 码，用户自定义，出厂默认为 16 个 F，即“FFFFFFFFFFFFFFFF”，不区分大小写。SO PIN 在产生 PID 和解锁 User PIN 时用到。SO PIN 同样使用种子机制产生。注意: 请保留好新产生的 SO PIN 和种子。
User PIN（User Personal Identification Number）	用户 PIN 码，用户自定义，出厂默认为 16 个 F，即“FFFFFFFFFFFFFFFF”，不区分大小写。User PIN 在读写数据，使用 HMAC-MD5 密钥进行计算等操作中用到。User PIN 的修改需要先验证旧的 PIN 码,再设置新的 PIN 码。注意: User PIN 码长度为 16 个十六进制字符，即 16 个 0～9 和 A～F 的字符组合。
PIN 重试次数限制	SO PIN 和 User PIN 都有重试次数限制。最大重试次数可以设置为 1～15 次，当设置为 0 时，则表明 SO PIN 和 User PIN 将永远不被锁死。如果开发商将 SO PIN 和 User PIN 的最大重试次数设为 1～15 时，那么当使用者连续输入错误的次数达到了最大限制次数，则多功能锁锁死，这时即使输入正确的 SO PIN 和 User PIN，也不能进行相应的操作。如果在最大限制次数内只要有一次输入正确，最大重试次数又恢复为开发商所设置的最大值。出厂默认为 SO PIN 不会锁死，User PIN3 次锁死。另外，可以通过 et_Verify 验证 PIN 码接口的错误返回值得到重试次数，调用该接口成功时返回 0，错误时返回 0xF*，*表明剩余的重试次数，如: 0xF2 表明还剩 2 次重试机会，0xF0 表明 PIN 码已被锁死，如果每次都返回 0xFF，表明没有重试次数限制。

产品外观：



定制外壳图片：

如需产品外壳定制，请联系相关销售人员