

# ET99 产品白皮书 (身份认证)

坚石诚信

北京坚石诚信科技股份有限公司

2009-9-9

ET99 是一款高速 HID 无驱并可以同时支持软件保护和身份认证应用的多功能 USB 设备。其采用国际流行的冲击响应认证方式，硬件内部完成 HMAC-MD5 运算，密钥不出锁，安全可靠。通过 ET99，就可以安全快速的完成登录的过程，不必再为密码被盗而担心，真正实现上网无忧。

#### 产品特点：

- 优惠的价格帮您最大限度节省购买成本
- 稳定的质量解决后顾之忧
- 全系统兼容的 HID 无驱 USB 设备
- 高速 USB 通讯模式
- 单个硬件多种功能
- 传统密码登录的冲击响应方式
- 硬件内部支持 HMAC-MD5 运算
- 全球唯一 64 位硬件序列号
- 1000 字节安全存储空间，用户级别读写控制
- 8 个 32 字节算法密钥
- 真硬件时钟芯片控制，提供高强度的时间授权保护
- Windows、Linux、Mac 跨平台支持
- 用户必须先输入 ET99 的 User PIN，验证通过后才能登录
- User PIN 有最大重试次数限制，连续输入错误会锁死。从而防止硬件丢失后，被不合法的持有者反复重试，暴力破解
- 硬件保证锁内密钥只能在锁内参与 HMAC-MD5 运算，无法被读取或导出
- 硬件和 User PIN 双重因子保护。必须同时具备 ET99 硬件和保护硬件的 User PIN 双重因子时才能登录。
- 网络传输的数据一次一密，有效防止黑客截获，重放攻击等盗用手段。

**硬件参数:**

核心芯片	8 位 CPU 芯片
硬件序列号	全球唯一 64 位 (bit) 硬件序列号
安全存储空间	1000 字节
硬件内置算法	HMAC-MD5
时钟芯片	真正硬件时钟芯片, 寿命 3~5 年
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

**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:**

全球唯一 ID	64 位 (bit)
硬件算法	硬件内完成 HMAC-MD5 运算
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。
S0 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	S0 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 S0 PIN 和 User PIN 将永远不被锁死。
安全存储区	1000 字节, 只有通过 User PIN 验证后才可以读写。
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。
外壳加密	高强度外壳保护
时钟模块	锁内真正硬件时钟芯片, 完全与计算机脱离, 使用寿命 3~5 年。提供高强度的时间授权保护。

PIN 码:

<p>PID (Product IDentification)</p>	<p>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。</p>
<p>SO PIN (Super Officer Personal Identification Number)</p>	<p>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。</p>
<p>User PIN (User Personal Identification Number)</p>	<p>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。</p>
<p>PIN 重试次数限制</p>	<p>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。</p>

产品外观:



定制外壳图片:

丝网印效果



激光刻字效果



如需产品外壳定制，请联系相关销售人员