# ET199 SD 产品白皮书



北京坚石诚信科技股份有限公司

**2010-3-5**

ET199 SD 将智能卡与 Micro SD 存储卡统一结合，同时具有智能卡加密锁和 SD 存储多种功能。智能卡采用 16 位国外进口高性能芯片，提供 64K 用户存储空间，硬件支持 512/1024/2048 位 RSA、DES/3DES、SHA1、HMAC、MD5 算法。Micro SD 存储卡默认 1G 存储空间，存取速度大于 10MB/S。

ET199 SD 外观精巧，是目前最小的智能卡加密锁和储存卡设备。ET199 SD 为手机应用软件提供高端智能保护。插入 SD 卡套后，就可以作为标准 SD 卡应用于数码相机、手机、摄像机等多种领域。另外，插入 SD 读卡器后，与计算机 USB 端口连接，就成为带 U 盘的 ET199 加密锁。

**产品特点:**

- 16 位进口高性能智能卡硬件核心，彻底杜绝复制风险
- 默认 1G 存储空间（可订制），Micro SD/TF 精巧封装
- 同类智能卡产品价格最低，最大限度节省购买成本
- 插入 SD 读卡器后为全系统兼容的高速 USB 无驱设备
- 兼容 ET199 的应用程序。只需要将 ET199 SD 的 API 库替换 ET199 的 API 库，您的应用就可以使用 ET199 SD 了
- USB 通讯硬件级加密，有效防止 USB 端口数据劫持，保证了传输数据的安全性
- 单个硬件多种功能
- 世界领先的锁内编程技术，使用成熟的 C51 语言开发
- 高强度外壳保护
- VS.Net 程序外壳保护
- 硬件内部支持 512/1024/2048 位 RSA 非对称算法
- 硬件内部支持 DES/3DES 对称算法
- 硬件内部支持 MD5、SHA1 散列算法
- 硬件内部支持单/双精度浮点运算
- 64K 超大安全存储空间
- 安全远程升级
- 支持网络锁功能
- Windows、Linux、Mac 跨平台支持

## 硬件参数:

| | |
|---|---|
| 核心芯片 | 16 位进口高性能智能卡 |
| Micro SD | 默认 1G 存储空间（可订制） |
| Micro SD 存取速度 | 大于 10M/S |
| 硬件序列号 | 全球唯一 64 位（bit）硬件序列号 |
| 安全存储空间 | 64K 字节 |
| 硬件内置非对称算法 | 512/1024/2048 位 RSA 算法 |
| 硬件内置对称算法 | DES/3DES |
| 硬件内置散列算法 | MD5、SHA1 散列算法 |
| 复杂数学运算 | 硬件内部支持单/双精度浮点运算 |
| 读次数 | 没有限制 |
| 写次数 | 至少 10 万次 |
| USB 通讯 | 全系统兼容的高速 USB 无驱设备。通讯硬件级加密。 |

## 物理参数:

| | |
|---|---|
| 默认外观 | Micro SD/TF 规范封装 |
| 默认颜色 | 黑色 |
| 外壳尺寸 | 11×15×1（毫米） |
| 重量 | 小于 1 克 |
| 接口类型 | 插入 SD 卡套后，为标准 SD 设备 |
| 接口类型 | 插入 SD 读卡器后，为高速 USB 无驱设备 |
| 工作温度 | 0℃～60℃ |
| 存放温度 | －25℃～80℃ |
| 工作湿度 | 20%～80% |
| 工作功率 | 0.5W（最大） |
| 工作电压 | 5V |
| 工作电流 | 100mA（最大） |
| 数据保存年限 | 至少 10 年 |

## 安全性:

| | |
|---|---|
| 硬件核心 | 16 位国外进口高性能智能卡，彻底杜绝硬件复制 |
| 锁内硬件可编程 | 可使用成熟的 C51 语言开发锁内程序 |
| 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 |
| 文件存储 | 可执行文件、密钥文件等机密文件不可导出，杜绝锁内算法泄漏 |
| 安全数据存储 | 智能卡硬件保证锁内数据安全存储 |
| 非对称加解密算法 | 硬件内部支持 512/1024/2048 位 RSA 非对称算法 |
| 对称加解密算法 | 硬件内部支持 DES/3DES 对称算法 |
| 散列算法 | 硬件内部支持 MD5、SHA1 散列算法 |
| 复杂数学运算 | 硬件内部支持单/双精度浮点运算 |
| 外壳加密 | 高强度外壳保护 |
| VS.Net 外壳加密 | 提供针对 VS.Net 程序的高强度外壳保护 |
| 远程升级 | 建立在 RSA 算法体系上的安全远程升级 |
| 全球唯一 ID | 64 位（bit） |
| 超大用户空间 | 64K |

## 相关信息:

| | |
|---|---|
| 开发商口令（24 字节） | 开发商在进行软件保护开发时使用到的，用于对 ET199 进行设置，如：创建文件/目录，删除文件/目录，设置客户号，设置 ATR 等。初始值为：“123456781234567812345678”。 |
| 用户口令（8 字节） | 在程序中调用 ET199 中的可执行文件前，需要验证用户口令。初始值为：“12345678”。 |
| 口令权限和重试次数 | ET199 中每个目录都有各自的开发商口令和用户口令。重试次数可以设置为 1～254 次，当设置为 0 或者 255 时表明没有重试次数限制。注意：当根目录开发商口令锁死后，没有任何办法能恢复，只能退回来重新生产。 |
| 客户号（4 字节） | 通过种子机制产生，设置前需要验证根目录开发商口令。种子机制的优势：种子是由开发商自己设定的一串数据，其他人即使得到客户号，但不知道产生该客户号的种子，因此无法制作相同客户号的 ET199。 |
| ATR（16 字节） | 设置 ATR，设置前需要验证根目录开发商口令。 |
| 可执行文件 | 可执行文件是由 C51 语言编写的，在加密锁内部运行的文件。通过开发商口令验证后，在锁内创建，该文件不能被读取。杜绝锁内算法泄漏。 |

| | |
|---|---|
| 内部数据文件 | 存放数据信息的文件。该文件在开发商口令验证后，可以通过 API 接口写入。或者通过锁内可执行文件来读取和写入。 |
| 密钥文件 | 存储 RSA 密钥对（公钥和私钥）的文件。写入时需要验证开发商口令，公钥可以读取，私钥文件不能读取。杜绝锁内私钥泄漏。 |

**产品外观:**