HTNICE 加密芯片使用手册

GT-150505-V1.0

文 件 更 改 履 历 表				
编号	日期	版本	说明	备注
1.	2015-05-05	V1.0	初始讨论稿	
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				

目　录

警告：

1、加密芯片与用户相关的出厂熔丝都为芯片原厂出厂初始状态，开放给用户的密码保护权限为最高权限，我公司不保留控制权，机器出厂后因不当操作引起的用户熔丝或密码认证锁死问题，我公司也将无法解除，所以一旦出厂后出现锁死问题概不在保修范围内。加密芯片锁死后，只能通过更换加密芯片来解决锁死问题（锁死问题更换加密芯片为有偿服务）。

2、所有的加密手段都有被破解风险，用户在进行应用程序加密绑定时，需要综合考虑被破解的可能性。加密的安全性取决于芯片自身与用户应用程序的加密机制。本公司只提供给用户一个加密手段，不承担任何因用户应用程序被反向工程破解引起的损失；

用户使用了加密芯片功能，视同已经仔细阅读上述条款并接受可能存在的风险！

一、 加密芯片概述

注意：由于加密芯片的特殊性,如果连续多次错误操作,将造成加密芯片的永久损坏。锁定用户密钥后将不可再更改密钥，如出现密钥的误设定，只能通过返厂更换加密芯片的方式进行维修，我司将收取一定的维修费用。用户如需使用加密芯片，调试程序时务必小心谨慎。

板载加密芯片在出厂时，我们已经为每个加密芯片设定好一个唯一的 ID 号，此 ID 号不可更改。提供用户 16 字节的自定义产品信息存储空间，8 个字节自定义密钥以及 64 个字节加密的数据存储空间。

为了用户能简单快速的使用加密芯片，我司已经将加密芯片的操作进行了封装，以库文件的方式提供给用户使用，库文件的存放路径为光盘目录下 \编程示例\加密芯片相关\库文件。库文件为 libht98sc.so 和 libhtsc.a，其中 libht98sc.so 为加密芯片底层操作的动态库文件，已经集成在默认的文件系统中，是 libhtsc.a 所依赖的动态库文件。libhtsc.a 为提供给用户调用的加密芯片上层接口的静态库文件，为提高安全性，此接口只提供静态库，不再提供动态库文件。

此手册只适用于我司出品的 Linux 系统下带有加密芯片的嵌入式计算机。

二、 加密芯片上层应用接口说明

加密芯片上层应用接口定义在 libhtsc.h 头文件中，以下将对各个函数加以说明。

1) int HTSC_Open(void);

功能：打开加密芯片。
输入参数：无
返回参数：0-成功，其他-失败
说明：在对加密芯片进行操作之前，必须先打开加密芯片

2) int HTSC_Close(void);

功能：关闭加密芯片。
输入参数：无
返回参数：0-成功，其他-失败
说明：在完成对加密芯片进行操作后，调用此函数关闭加密芯片

3) HTSC_ReadID(unsigned char *pID, unsigned char *pCMC);

功能：读取预设的 ID 号及我司自定义信息
输入参数：7 字节的 pID 指针，4 字节的 pCMC 指针

返回参数：0-成功，其他-失败
说明：函数执行成功后，将 7 字节的 ID 数据拷贝到 pID 指针所指地址，将 4 字节的我司自定义信息数据拷贝到 pCMC 指针所指地址。其中，ID 号为唯一不重复数据，我司自定义信息数据不保证唯一性。

4) int HTSC_SetPER(unsigned char *pIssuserID,unsigned char *pAuthKey);

功能：设置用户自定义密钥及自定义产品信息
输入参数：16 字节的 pIssuserID 指针，8 字节的 pAuthKey 指针
返回参数：0-成功，其他-失败
说明：pIssuserID 为用户自定义产品信息数据存放指针，pAuthKey 为用户密钥存放指针。注意，在锁定用户密钥之前，即调用 HTSC_BurnPerFuse(void)函数执前，可重复调用此函数进行设定。锁定之后将不能进行修改，调用此函数将返回失败。

5) int HTSC_UserAuth(unsigned char *pAuthKey);

功能：用户密钥验证
输入参数： 8 字节的 pAuthKey 指针
返回参数：0-成功，其他-失败
说明：pAuthKey 为用户密钥存放指针。此函数验证密钥的合法性，验证成功后才能读写用户区数据。注意，为防止暴力破解，在连续 4 次认证失败后，加密芯片将自行报废。

6) int HTSC_ReadIssuserID(unsigned char *pIssuserID);

功能：读取用户自定义产品信息
输入参数： 16 字节的 pIssuserID 指针
返回参数：0-成功，其他-失败
说明：函数执行成功后，将 16 字节的用户自定义产品信息数据拷贝到 pIssuserID 指针所指地址，此用户自定义产品信息可通过 HTSC_SetPER(unsigned char *pIssuserID,unsigned char *pAuthKey)函数写入。

7) int HTSC_WriteUserData(unsigned int addr, unsigned char *pWR, unsigned int len);

功能：往用户数据存储区写入数据
输入参数： addr 为存储区开始写入地址，范围 0-63。
pWR 为准备写入数据所在的内存地址指针
len 为数据写入长度，范围 1-64
返回参数：0-成功，其他-失败
说明：必须在调用 HTSC_UserAuth(unsigned char *pAuthKey)函数成功后才能执行此函数。函数执行成功后，将 pWR 指针所指的数据，按 addr 开始的地址，往加密芯片的用户存储空间写入 len 个字节。由于用户总存储空间地址为 0-63，所以 addr+len 不能超过 64。

8) int HTSC_ReadUserData(unsigned int addr , unsigned char *pRD, unsigned int len);

功能：从用户数据存储区读出数据
输入参数： addr 为存储区开始读数据地址，范围 0-63。
pRD 为读出数据后存放的内存地址指针
len 为数据读出长度，范围 1-64
返回参数：0-成功，其他-失败
说明：必须在调用 HTSC_UserAuth(unsigned char *pAuthKey)函数成功后才能执行此函数。函数执行成功后，按 addr 开始的地址，从加密芯片的用户存储空间读出 len 个字节，拷贝至 pRD 指针所指地址。由于用户总存储空间地址为 0-63，所以 addr+len 不能超过 64。

9) int HTSC_BurnPerFuse(void);

功能：锁定用户密钥及用户自定义产品信息数据
输入参数： 无
返回参数：0-成功，其他-失败
说明：设定用户密钥后，在硬件出厂前必须调用此函数锁定密钥，否则无法起到加密保护程序的作用。密钥锁定后将无法更改，建议调试程序时暂不要调用此函数。

三、 加密芯片应用说明

根据编程方法从简单到复杂程度，加密芯片的使用方法可分为以下三种，同时安全性也从低到高依次增加。

1. 将应用程序与加密芯片内预先设定的 ID 号进行绑定

此方法最为简单，程序中只需要读出加密芯片的 ID 号来判断当前硬件是否合法，但此法安全级别较低。

读取加密芯片 ID 号的示例代码所在位置为光盘目录下\编程示例\加密芯片相关\读 ID 号\htscid。

2. 设置密钥并在应用程序中进行密钥验证

此方法要分两步执行，首先要设定用户密钥，然后才能在程序里进行密钥的验证，只有通过验证才能判断为合法硬件。此方法安全级别较高，但硬件出厂前必须锁定用户密钥，否则起不到任何加密保护作用。

设定用户密钥的示例代码所在位置为光盘目录下\编程示例\加密芯片相关\密钥设定与验证\ htscset。
用户密钥验证的示例代码所在位置为光盘目录下\编程示例\加密芯片相关\密钥设定与验证\ htscauth。

3. 将应用程序的关键数据存储到加密芯片中

此方法最为复杂，但同时也是安全级别最高的一种。用户在出厂前先将应用程序的关键数据存储于加密芯片中，程序运行时再从加密芯片中读出使用。由于在对用户数据存储区进行操作前要先通过密钥验证，所以在这之前要根据上一种方法进行密钥的设置。此方法同样需要在硬件出厂前必须锁定用户密钥，否则起不到任何加密保护作用。

用户数据存储区读写的示例代码所在位置为光盘目录下\编程示例\加密芯片相关\用户数据读写\ htscdata。

深圳市恒天智信科技有限公司
地址：深圳市龙华新区油松路106号天汇大厦D栋616
电话：（086）755-82792766
传真：（086）755-82550036
http://www.htnice.com