|  |
| --- |
| **设备加密系统** |
| **武汉普赛斯仪表有限公司** |
| **声明：本文件所有权和解释权归武汉普赛斯仪表有限公司所有，未经武汉普赛斯仪表有限公司书面许可，不得复制或向第三方公开。** |

修订历史记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **日期** | **AMD** | **修订者** | **说明** |
| V1.0.0 | 2022.11.1 | A | 赵兵 | 初始版本 |
| V1.0.1 | 2022.11.2 | M | 赵兵 | 将密钥生成算法改为示例算法 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

(A-添加，M-修改，D-删除)

目 录

[1 功能 4](#_Toc118303030)

[1.1 知识产权保护 4](#_Toc118303031)

[1.2 保存设备信息 4](#_Toc118303032)

[2 系统组成 5](#_Toc118303033)

[2.1 设备子板 5](#_Toc118303034)

[2.2 生产工具 5](#_Toc118303035)

[2.3 数据结构与协议算法 5](#_Toc118303036)

[3 数据结构 6](#_Toc118303037)

[4 访问协议(SCPI指令) 6](#_Toc118303038)

[4.1 \*PSS:FAC:INFO? 6](#_Toc118303039)

[4.2 \*PSS:FAC:INFO <item> 7](#_Toc118303040)

[4.3 \*PSS:FAC:INFO:SAVE 7](#_Toc118303041)

[5 密钥生成算法 8](#_Toc118303042)

[5.1 公式: K = D(I, R); 8](#_Toc118303043)

[5.2 加密算法D步骤(示例)： 8](#_Toc118303044)

[6 密钥生成软件 8](#_Toc118303045)

[7 配置工具软件 8](#_Toc118303046)

[7.1 配置文件 8](#_Toc118303047)

[7.2 界面状态显示 8](#_Toc118303048)

[7.3 界面可选择项 8](#_Toc118303049)

[7.4 界面编辑项 9](#_Toc118303050)

[7.5 界面操作项 9](#_Toc118303051)

# 功能

## 知识产权保护

1. 防止未经授权的访问或拷贝设备内部程序；
2. 防止使用非正常手段抄袭PCB，将产品的PCB完全复制；

## 保存设备信息

1. 公司信息：固定为 ”PSS\_INS” 字符串；
2. 产品系列：产品系列字符串，如 ”Sx00”、”Px00” 等；
3. 子板类型：PCB板类型字符串，如 “Angl”、”Pwr”、”Ctrl”、”Fnt”；
4. 生产时间：产品生产的时间字符串，如 “2022.07.28\_13:56:57”；
5. **产品型号**：产品型号字符串，如 “S100”、”S200”、”S300”；以便软件运行时动态加载相应功能模块。
6. BOM编码：物料管理系统BOM编码字符串，如 “46.20.000000189”；
7. **硬件版本**：PCB板版本字符串，如 “PSS\_SMU\_A\_HW\_V2.0.5[;AD5768]”，其中 [] 本身及其中内容为可选部分，以便软件运行时动态适配不同硬件。
8. 变更时间：最后修改数据的时间字符串，如 “2022.07.28\_13:56:57”；
9. SN码：产品SN字符串，如 “22140010”；
10. **定制信息**：用于标识不同定制版本的字符串，如 “”、“Huawei”；以便软件运行时动态加载相应功能模块。
11. 防抄板信息：保存部分机器指令，用于知识产权保护；
12. 自定义信息：扩展用途，由具体子板定义；

# 系统组成



图2.1 设备加密系统组成

设备加密系统由被保护的设备子板、生产工具、协议算法与数据结构三大部分组成，如图2.1所示。

## 设备子板

被保护的设备子板必须有CPU与加密芯片硬件，并且CPU上加载了加密系统固件程序；否则无法为该子板提供加密服务。

## 生产工具

1. 密钥生成软件：运行在服务器，通过TCP 9114端口访问，根据给定的密钥生成码生成与设备子板通信用SCPI密钥；
2. 配置工具软件：可运行在位于公司内网的任何电脑上，通过SCPI指令与密钥，读写设备子板加密系统数据；

## 数据结构与协议算法

1. 数据结构：定义保存到加密芯片的数据；
2. 协议：定义加密系统配置软件与设备子板间的通信协议；
3. 算法： 确保设备子板加密系统数据访问安全的密钥生成算法；

# 数据结构

typedef struct FACORY\_INFO\_TAG\_

{

  char company[8];    // 公司信息, 如 "PSS\_INST"             --- ATSHA204 OTP区

  char product[16];   // 产品信息, 如 "Ex00"                 --- ATSHA204 OTP区

  char brdType[8];    // 子板类型, 如 "Anlg"                 --- ATSHA204 OTP区

  char facTime[32];   // 生产时间, 如 "2022.07.28\_13:56:57"  --- ATSHA204 OTP区

  char subType[32];   // 产品型号, 如 "S100"、"S200"、"S300" --- ATSHA204 DATA区

  char bom[32];       // BOM 编码, 如 "46.20.000000189"     --- ATSHA204 DATA区

  char hwVer[32];     // 硬件版本, 如 "PSS\_SMU\_A\_HW\_V2.0.5"  --- ATSHA204 DATA区

  char mdyTime[32];   // 修改时间, 如 "2022.07.28\_13:56:57" --- ATSHA204 DATA区

  char SN[32];        // 设备 SN,  如 "22140010"            --- ATSHA204 DATA区

  char custInfo[32];  // 定制信息, 如 "Huawei"、"Accelink"   --- ATSHA204 DATA区

  char antiCopy[32];  // 防抄板信息, 保存部分机器指令         --- ATSHA204 DATA区

  char custom[32];    // 自定义信息, 由具体子板定义           --- ATSHA204 DATA区

} FACORY\_INFO\_T, \*FACORY\_INFO\_P;

# 访问协议(SCPI指令)

## \*PSS:FAC:INFO?

|  |  |
| --- | --- |
| **命令格式** | \*PSS:FAC:INFO? |
| **功能描述** | 获取 加密系统访问密钥生成数 |
| **返回值** | 1个8字节十六进制数，1个4字节十六进制数；  如：0x0102030405060708,0x12345678 |

## \*PSS:FAC:INFO <item>

|  |  |  |
| --- | --- | --- |
| **命令格式** | \*PSS:FAC:INFO <item>, <data>, <pwd>  \*PSS:FAC:INFO? <item>, <pwd> | |
| **功能描述** | **设置/查询**加密系统数据 | |
| **参数** | item | 加密系统数据条目  company : 公司信息，最长7字节字符串  product : 产品信息，最长15字节字符串  brdType : 子板类型，最长7字节字符串  facTime : 生产时间，最长31字节字符串  subtype : 产品型号，最长31字节字符串  bom : BOM 编码，最长31字节字符串  hwVer : 硬件版本，最长31字节字符串  mdyTime : 修改时间，最长31字节字符串  SN : 设备SN，最长31字节字符串  custInfo : 定制信息，最长31字节字符串  antiCopy : 防抄板信息，最长32字节二进制数据  custom : 自定义信息，最长31字节字符串 |
| data | 数据 |
| pwd | 加密系统访问密钥 |
| **返回值** | 字符串或二进制数据 | |

## \*PSS:FAC:INFO:SAVE

|  |  |  |
| --- | --- | --- |
| **命令格式** | \*PSS:FAC:INFO:SAVE <pwd>  \*PSS:FAC:INFO:SAVE? <pwd> | |
| **功能描述** | 保存加密系统数据  查询加密系统数据是否保存 | |
| **参数** | pwd | 加密系统访问密钥 |
| **返回值** | 0 | 未保存 |
| 1 | 已保存 |

# 密钥生成算法

## 公式: K = D(I, R);

I为8字节芯片ID信息 ，R为4字节随机数据

## 加密算法D步骤(示例)：

1. 逆序：分别将8字节芯片ID，以及4字节随机数据进行逆序操作；
2. 异或：逆序后将前4字节芯片ID数据与后4字节ID数据分别与随机数据进行异或。
3. 累加：将上述两者异或后的结果进行累加，输出为4字节长度的结果。
4. 逆序：将上述操作后的结果再次进行逆序操作，输出4字节密钥K。

# 密钥生成软件

1. 运行于服务器TCP 9114端口；
2. 接收以逗号分隔、’\n’为结束符的字符串；
3. 执行密钥生成算法;
4. 返回加密系统访问指令密钥；

例如：向服务器TCP 9114端口发送 0x0102030405060708,0x12345678\n ，服务器返回 0x87654321 。

# 配置工具软件

## 配置文件

1. 配置工具软件以配置文件为基础，每个配置文件对应一个产品。
2. 对于每个产品，由型号、子板、硬件、定制、BOM 5个配置项。

## 界面状态显示

## 界面可选择项

1. 产品：如 Sx00、Px00
2. 型号：如 S100、S200、S300
3. 子板：如 Angl、Pwr、Ctrl、Fnt
4. 硬件：如PSS\_SMU\_A\_HW\_V2.0.5; AD5768
5. 定制：可以为空或任意标识定制信息的字符串
6. BOM：如 46.20.000000189

## 界面编辑项

1. SN码：8位数字字符串，前4位表示年于周，后4位表示生产批号。

## 界面操作项

1. 烧录：必须是所有信息为空的设备子板才能操作；
2. 维修：必须是烧录后的设备子板才能操作，仅能修改硬件、定制信息；
3. 升配：必须是烧录后的设备子板才能操作，仅能修改型号、硬件、定制信息；