

# 二级密钥使用说明

## V1.2

珠海市杰理科技股份有限公司

**Zhuhai Jieli Technologyco.,LTD**

版权所有，未经许可，禁止外传

2022 年 08 月

## 目录

概述.....	1
一、 SDK 修改点 .....	2
1. 公司 A 打包库设置秘钥.....	2
2. 公司 B 下载脚本修改点 .....	2
二、 获取 KEY0 文件和 KEY1 文件方法 .....	2
三、 生成 MKEY 文件方法 .....	3
四、 工厂量产 FW 文件生成方法 .....	4

## 概述

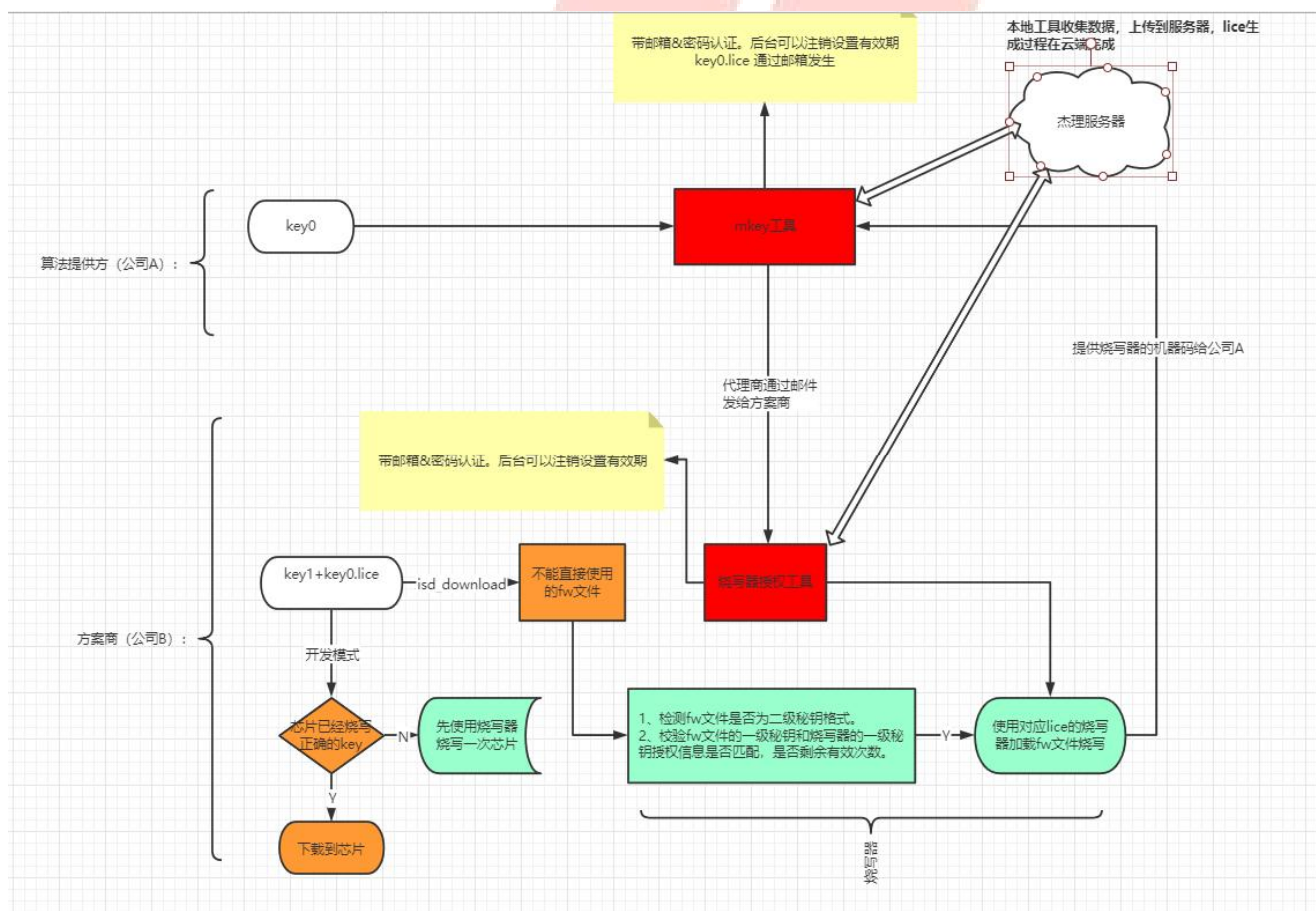
使用场景：

1. 公司 A 出售芯片给公司 B。
2. 公司 A 开发一个 SDK 提供给公司 B 做二次开发。

双向保护机制：

1. 公司 A 在自己的核心库里面配置好密钥后，可保护公司 A 的 SDK 不外泄。在没有获得授权的情况下 SDK 无法正常运行，可避免公司 B 从其他渠道购买芯片运行公司 A 所开发的 SDK。
2. 公司 A 没有公司 B 的 key1 文件，公司 A 拿到 fw 文件之后也无法生产，从而保护了公司 B 二次开发之后新 SDK 的权益。

整体框图如下：



## 一、SDK 修改点

### 1. 公司 A 打包库设置秘钥

注：设置秘钥放在需要保护的库里面, 里面有互斥操作，不能在中断函数调用。建议放在初始化函数里面。

```
{
    u32 sdk_mkey_lock(const u8 * pin_code);

    const char *pin_code = "\xFE\x23\xA8\xB1\x28\xD4\xB4\x29\xB6\x6D\xE8\x79\x2F\xB5\x49\x92\xB4\x54\xB4\x4E\x82\x04\x29";

    u32 crc = sdk_mkey_lock(pin_code);

    if (crc != CRC16(pin_code, 32)) {
        printf("mkey version error\n");
        while (1);
    }
}
```

检查返回值，确认秘钥设置成功。

### 2. 公司 B 下载脚本修改点

download.bat 修改点：

```
26
27
28 isd_download.exe -tonorflash -dev br23 -boot 0x12000 -div8 -wait 300 -uboot uboot.boot -app app.bin cfg_tool.bin
29 -res tone.cfg -key1 128_AC69XX_b0c8.key1 -mkey 128-AC69XX-[机器码CRC-c4ae]-ffa2.mkey
30 :: -format all
31 --reboot 2500
```

## 二、获取 KEY0 文件和 KEY1 文件方法

通过向杰理申请获取 KEY0 文件（key0.hex）和 KEY1 文件。

KEY0 文件由公司 A 向杰理申请，KEY1 文件由公司 B 向杰理申请。

名称	修改日期	类型	大小
128_AC69XX_ce6f.key0	2020/10/27 20:13	KEY0 文件	1 KB
128_AC69XX_ce6f.key0.hex	2020/10/27 20:13	UltraEdit Docum...	1 KB
128_AC69XX_d0e1.key1	2020/10/30 11:53	KEY1 文件	1 KB

128\_AC69XX\_ce6f.key0.hex - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

\xDD\x44\x66\x2D\x0A\x07\xF1\xA3\x6C\x1B\x0E\x87\x88\xFB\xF4\xC9\x97\xC9\xA0\x0B\x05\x2B\x56\x8D\xDA\xCB\x57\xF0\xC3\x07\x41\xBD

KEY0 和 KEY1 文件需要发送邮件至 [weiyushu@zh-jieli.com](mailto:weiyushu@zh-jieli.com) 申请，格式如下：

邮件主题：【二级密钥】-公司 A 名称-key0

邮件内容：

公司 A 名称：xxx

申请 key 类型：key0

芯片系列: xxx

对接人邮箱: xxx

对应公司 B 名称: xxx (首次申请 KEY0 时需要)

对接人邮箱: xxx (首次申请 KEY0 时需要)

注: 第一次申请 KEY0 的公司需要填写公司 B 的相关资料, 同时请公司 B 发申请 KEY1 的邮件过来;  
已申请过 KEY0 的公司 A, 可直接请公司 B 发申请 KEY1 的邮件。

邮件主题: 【二级密钥】-公司 B 名称-key1

邮件内容:

公司 B 名称: xxx

申请 key 类型: key1

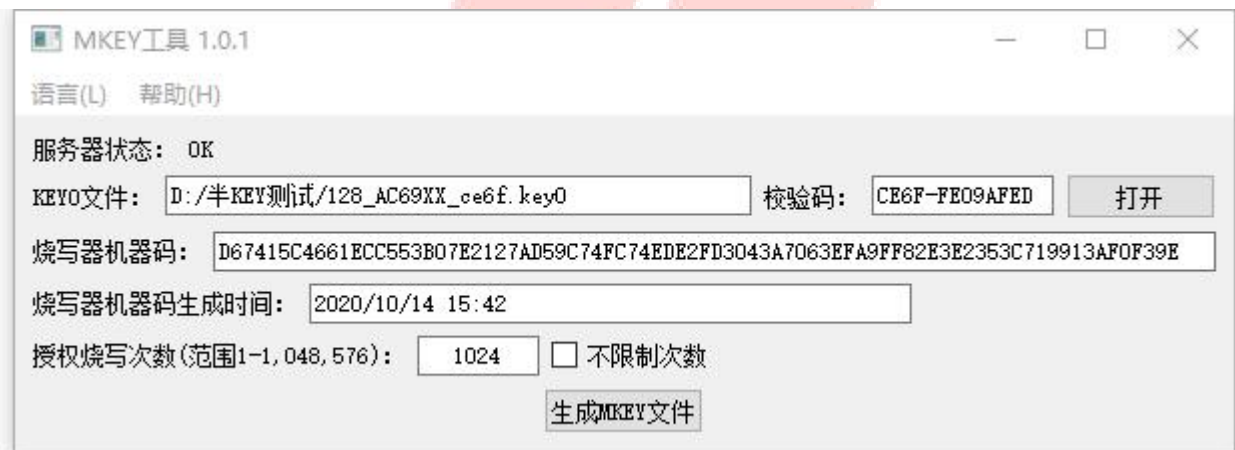
对接人邮箱: xxx

对应公司 A 名称: xxx

回复邮件内容包括: 用户名、密码、二级密钥相关资料。

### 三、生成 MKEY 文件方法

通过 MKEY 工具生成 MKEY 文件。工具界面如下:



**注: 此工具需要访问杰理服务器才能正常使用, 请保持网络可以正常访问杰理服务器。  
此工具发给公司 A, 同时公司 A 需要保护自己的 key0, 以及账号不要泄露。**

使用方法:

1. 登录账号
2. 公司 A 选择向杰理申请到的 KEY0 文件。
3. 公司 B 提供烧写器的机器码给 A, 设置授权烧写次数 (芯片购买量+损耗)
4. 公司 A 点击 “生成 MKEY 文件” 按钮保存 KEY 文件
5. 公司 A 发送 mkey 文件给公司 B。
6. 公司 B 按照第一点 SDK 修改点操作, 生成 fw 文件。

## 四、工厂量产 FW 文件生成方法

使用“固件授权信息合并工具”将 MKEY 中的授权信息合并到 FW 文件中，固件授权信息合并工具如下：



使用方法：

1. 登录账号
2. 选择 FW 文件
3. 选择 KEY1 文件（向杰理申请）
4. 授权方提供的 MKEY 文件
5. 点击“授权”，保存新的 FW 文件

**注：此工具需要访问杰理服务器才能正常使用，请保持网络可以正常访问杰理服务器。**

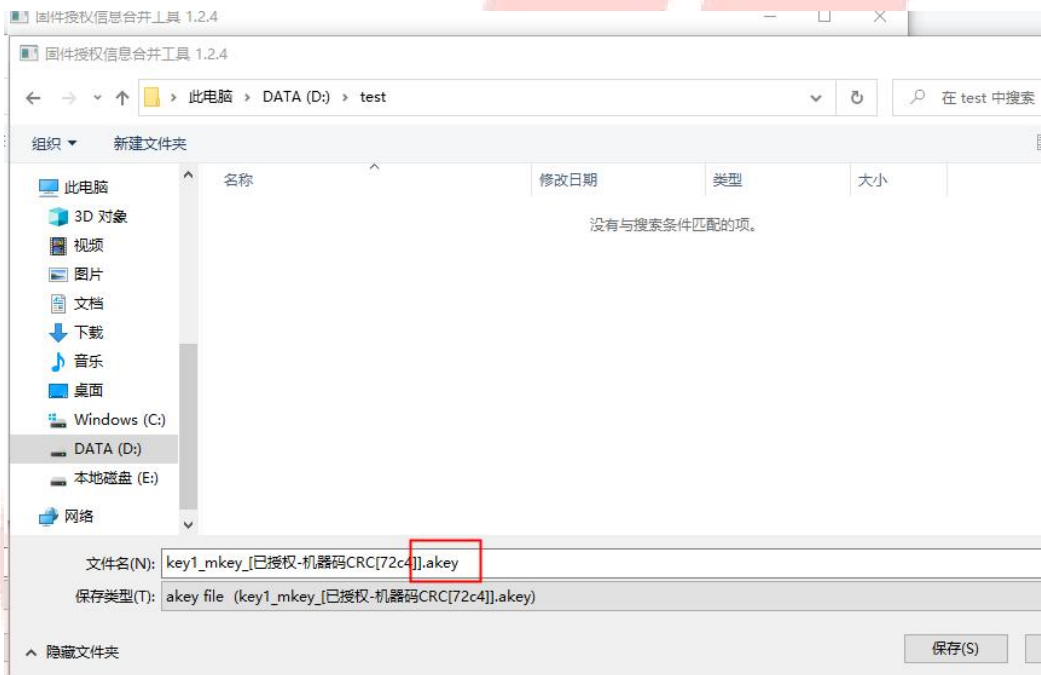
**特别说明：烧写器下单时需要备注“二级密钥”！**

## 五、A0 芯片量产方法

因为 A0 芯片没有内封 FLASH，所以不能用上一章节介绍的步骤生成的 FW 文件进行量产。A0 芯片的量产步骤如下：

1. 更新“固件授权信息合并工具”到 1.2.4 或之后版本。

2. 先选择 key1 文件，然后再选择 mkey 文件，点击生成 akey,文件.(不要选择 fw 文件)， 如下图：



3. 更新一拖二烧写器到 2.26.6 或之后的版本， 选择芯片型号后，部署 akey 文件到烧写器。  
4. 按正常烧写步骤烧写。