HDMI_HDCP 密钥

烧写指南

版本号: 1.3
发布日期: 2023.10.18

版本历史

版本号	日期	制/修订人	内容描述
1.0	2021.4.01	AWA0962	1. 创建该文档
1.1	2023.3.03	AWA1977	1. 增加配置说明 2. 补充烧录步骤
1.2	2023.7.04	AWA2130	1. 整合以前的烧录说明文档 2. 补充烧录步骤
1.3	2023.10.18	AWA2130	1. 修改部分描述 2. 补充烧录过程的说明

目　录

插　图

1 概述

1.1 编写目的

本使用指南目的在于说明如何烧录 HDMI HDCP 的密钥，希望通过该文档能让开发人员以及客户快速上手 HDCP 功能。

1.2 适用范围

适用于使用 HDMI 2.0 版本驱动的平台

1.3 相关人员

显示项目组成员，客户。

1.4 名词解析

名词	解释
HDCPLoad	用于切割从 DCP 组织购买的原始密钥的工具（仅限用于 HDCP 1.4）
DragonSN	烧写软件
hdcp_1.bin	HDCP 1.4 的密钥
hdcp2pkf.bin	用来加密 esm 固件的密钥
HDCP2_TX_KEY.bin	从 DCP 组织购买的 HDCP 2.2 原始密钥
esm.fex	经过加密的 esm 的固件

2 准备工作

⚠ 注意

使用 HDMI 的 HDCP 加密功能需要用安全固件！机器一旦烧录了安全固件就不能烧回非安全的固件，烧录前请慎重考虑！

2.1 系统配置

2.1.1 HDCP 1.4

- menuconfig

```
CONFIG_HDMI2_HDCP_SUNXI=y
```

- board.dts

```
hdmi_hdcp_enable = 1;
```

2.1.2 HDCP 2.2

说明

配置文件开启了 HDCP 1.4 和 HDCP 2.2 功能，默认会先尝试使用 HDCP 2.2。若 HDMI 接收设备不支持 HDCP 2.2，则会尝试使用 HDCP 1.4。

- menuconfig

```
CONFIG_HDMI2_HDCP_SUNXI=y
CONFIG_HDMI2_HDCP22_SUNXI=y
```

- board.dts

```
hdmi_hdcp_enable = 1;
hdmi_hdcp22_enable = 1;
```

3 HDCP 1.4

3.1 生成 hdcp_1.bin

3.1.1 原始密钥的来源

DCP 官方给到客户的 HDCP 密钥文件是一个二进制文件，该二进制文件会包含多个 HDCP 密钥，原始密钥 **不能**在密钥烧录工具上 **直接使用**，需要我们先分割为能被密钥烧录工具支持的格式。

> 原始密钥需客户自行联系 DCP 组织购买，使用 HDCP 1.4 的 **每台机器**都需要烧录 **不同**的密钥。

以往经验：

首先需要缴纳年会员费，加入会员组织，然后根据购买 Key 的数量，签订不同单价的合同，DCP 组织会不定期地抽查设备和商务合同来进行监管。

3.1.2 原始密钥的组成

Key File	Byte	Segment
Order Format	4	Head
Key0	8	Key0 KSV
	280	Key0 Device Keys
	20	Key0 Hash
Key1	8	Key1 KSV
	280	Key1 Device Keys
	20	Key1 Hash
Key2	8	Key2 KSV
	280	Key2 Device Keys
	20	Key2 Hash
.....		
Key(n)	8	Key(n) KSV
	280	Key(n) Device Keys
	20	Key(n) Hash

图 3-1: hdcp1.4 原始 key 组成

3.1.3 密钥切割工具

HDCPLoad：HDCP 1.4 原始密钥的切割工具。

使用方法：

1. 显示子密钥的数量；

```
HDCPLoad.exe -v14 -count <原始密钥的文件路径>
```

2. 分割密钥；

- 直接切割：

```
HDCPLoad.exe -v14 <原始密钥的文件路径> <输出路径>
```

- 指定输出文件名和切割范围

```
HDCPLoad.exe -v14 -prefix hdcp1p4 -range 1 2 <原始密钥的文件路径> <输出路径>
```

参数解析：

参数	含义
count	显示原始密钥中包含的子密钥个数
prefix	指定输出文件名，例如：hdcp1p4 ，就会生成为：hdcp1p4_1.bin ，hdcp1p4_2.bin 等
range	指定分割范围，例如：1 2 ，范围：[1, 2]，意思是会分割出第 1 个和第 2 个的原始密钥。

分割后的密钥：

单个大小为 **368** byte，具体组成如下图所示：

Field Name	Size	Description
Magic Number	4	Magic number, Value is 0x5aa5a55a
Version	4	Version of the structure
Length	4	Data length from start,but not include CRC
RAK	16	Random 128 bit AES CBC key in big-endian
HDCP key	308	Encrypted HDCP key
Padding	12	Padding HDCP key length to 16 bytes align
MD5	16	MD5 hash value of raw HDCP Key
CRC	4	CRC32 value of the above data

图 3-2: 368bytes 的密钥组成

3.2 烧录 hdcp_1.bin

3.2.1 配置 DragonSN 软件

1. 打开 **DragonSN**，点击左下角的 **配置 key**；

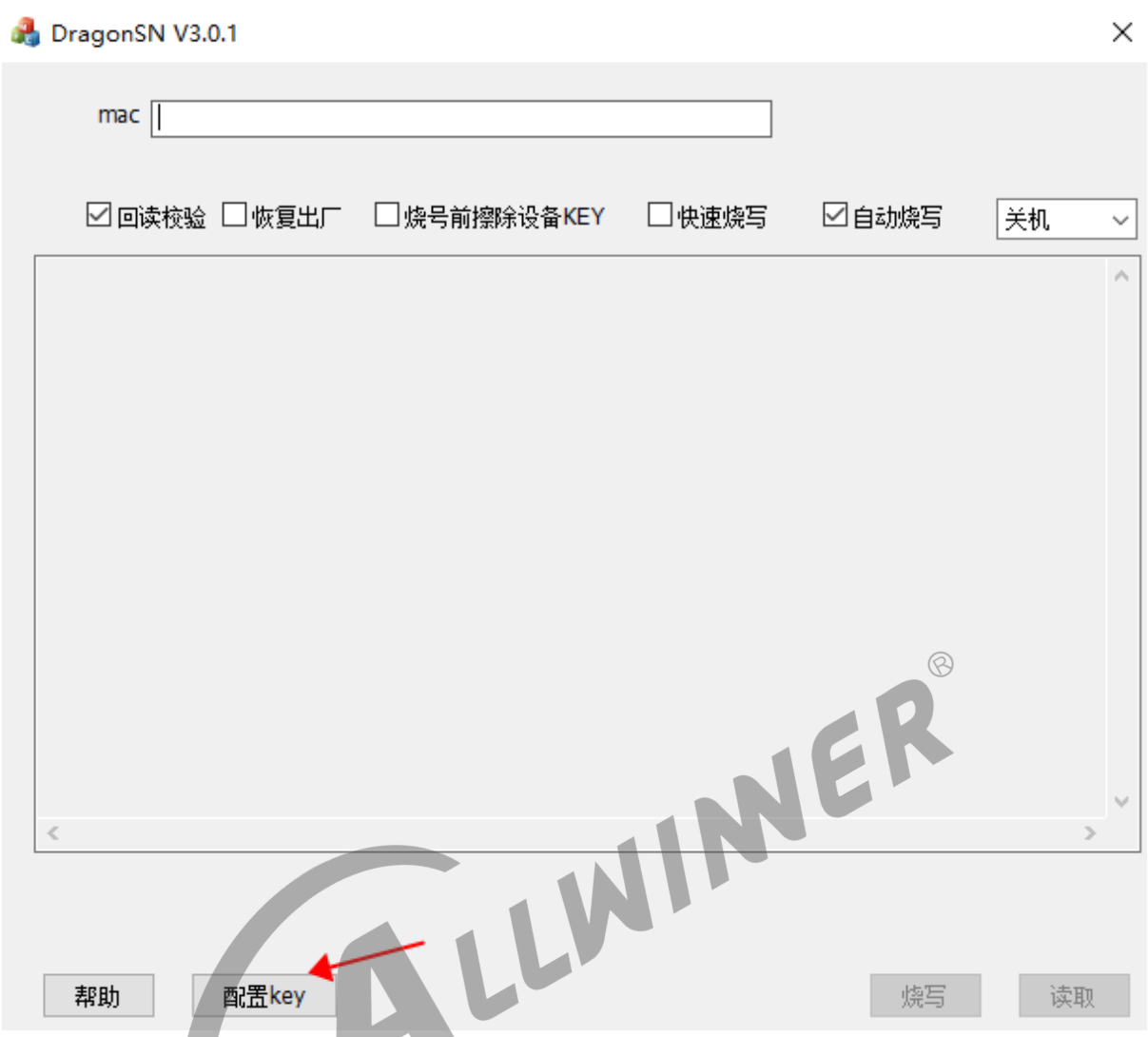

图 3-3: 配置 Key 入口

2. 如果当前配置有其他的配置项，请先**全部删除**，避免互相影响，**右击**，**删除**；

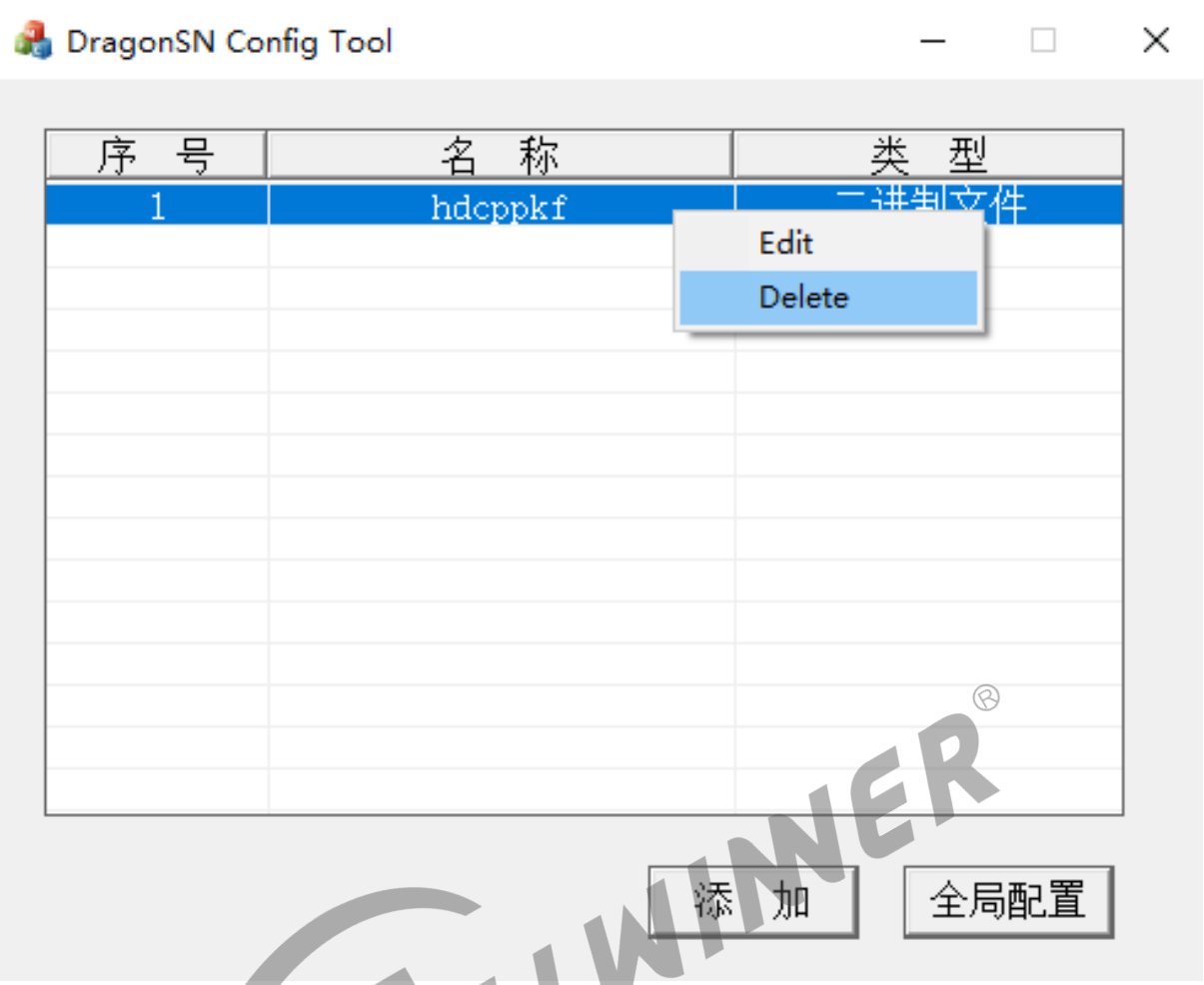

图 3-4: 删除 hdcppkf

3. 点击下方的**添加**，按下图所示配置，配置完成点击**保存**；

图 3-5: 配置 hdcpkey

关于 **烧完后**配置的解释：

1. 保留，一直烧同一个 key。
2. 移到 _used 目录，每烧完一个 key 就会将该文件移到同路径下的 _used 后缀文件夹中，即：依次烧不同的 key。

DCP 组织要求使用 HDCP 1.4 的每台设备都要烧录**不同的** key，所以应该选择第 2 种烧录方式。

4. 点击 Config Tool 界面右上角的 X ，退出到 DragonSN 软件界面。

3.2.2 开始烧录

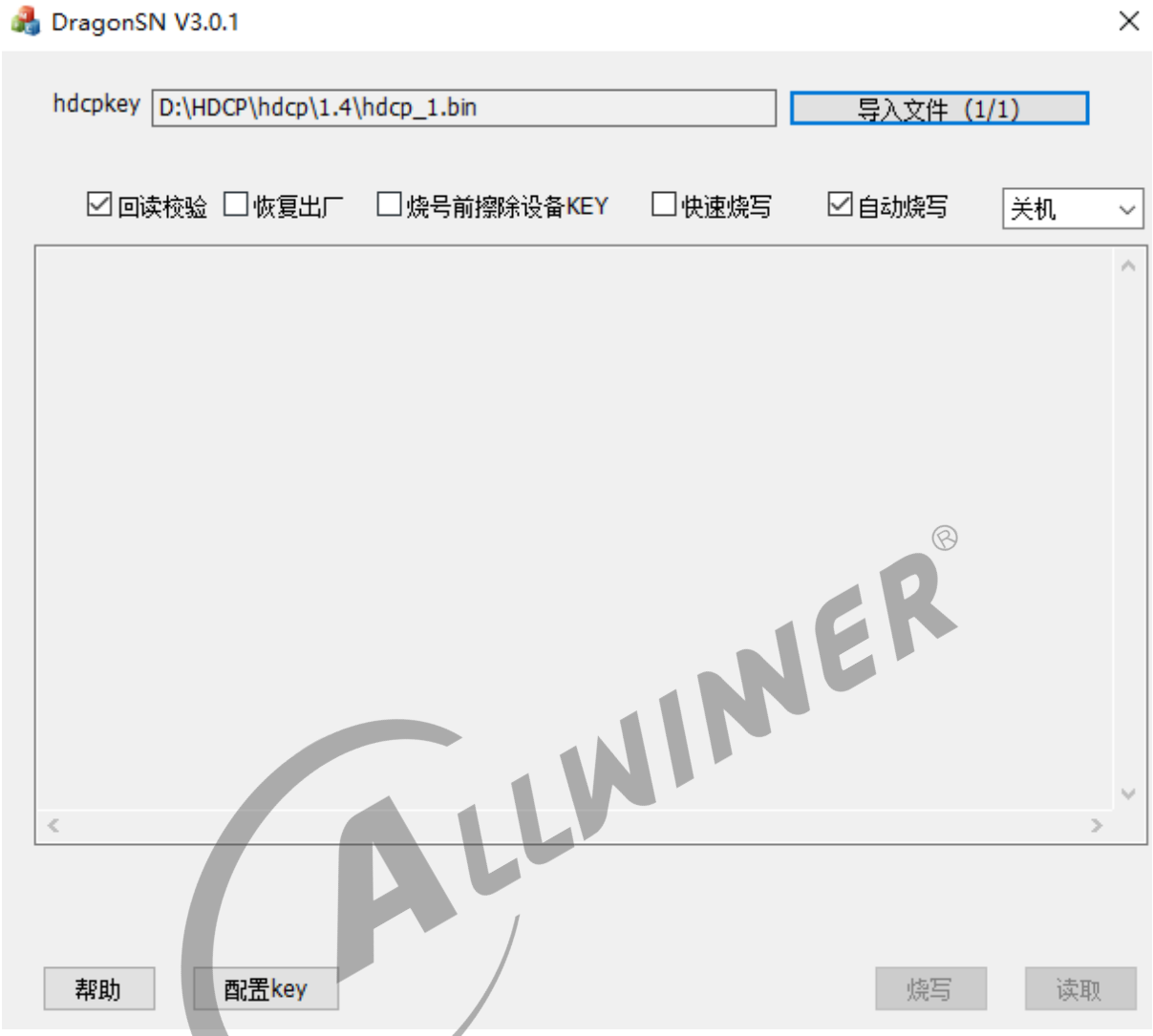

图 3-6: DragonSN_ 软件截图

1. 点击导入文件，选择要烧录的 **hdcp_1.bin** 所在的文件夹（尽量避免中文路径）；
2. **勾选**自动烧写，**取消勾选**快速烧写，选择烧写结束后 **关机**；
3. 确认开发板与 PC 已用 USB 线连接；
4. 重启开发板，工具会自动烧录；
5. 烧录完成后，可点击 **读取**确认烧录成功；

> 这里用单个机器烧录的流程做说明，多个机器烧录不同的 key，则参考上一章节，把烧录后的配置设为：移到 _used 目录。
> 只要当前选择的目录下还有 key 文件，烧录完成后拔掉，插上另一台机器即可，无需重复配置。

3.3 功能验证

> 功能验证的前提：HDMI RX 端（例如：电视）需要支持 HDCP 1.4 功能，否则会开启失败！

- 驱动层面使能 HDCP 开启认证

```
echo 1 > /sys/class/hdmi/hdmi/attr/hdcp_enable
```

- 串口获取 HDCP 状态

```
busybox hexdump /sys/class/hdmi/hdmi/attr/hdcp_status

0000000 0003
# AW_HDCP_DISABLE 0
# AW_HDCP_ING 1
# AW_HDCP_FAILED 2
# AW_HDCP_SUCCESS 3
```

- 认证失败的解决方法

1. 重新确认密钥生成和烧录过程是否正确；
2. 如果有条件，使用协议分析仪查看 aksv 的序列号是否一致，可以找以前用的开发板进行对比。
3. 确认烧录无误仍无法开启 HDCP，请联系全志 HDMI 工程师协助解决；

4 HDCP 2.2

4.1 相关介绍

HDCP 2.2 是通过 HDMI 的 esm 模块来实现加密的，该模块的运行需要加载固件，固件需要通过用户自定义的 pkf 文件来加密，避免泄露被破解，下图是对整个流程的介绍。

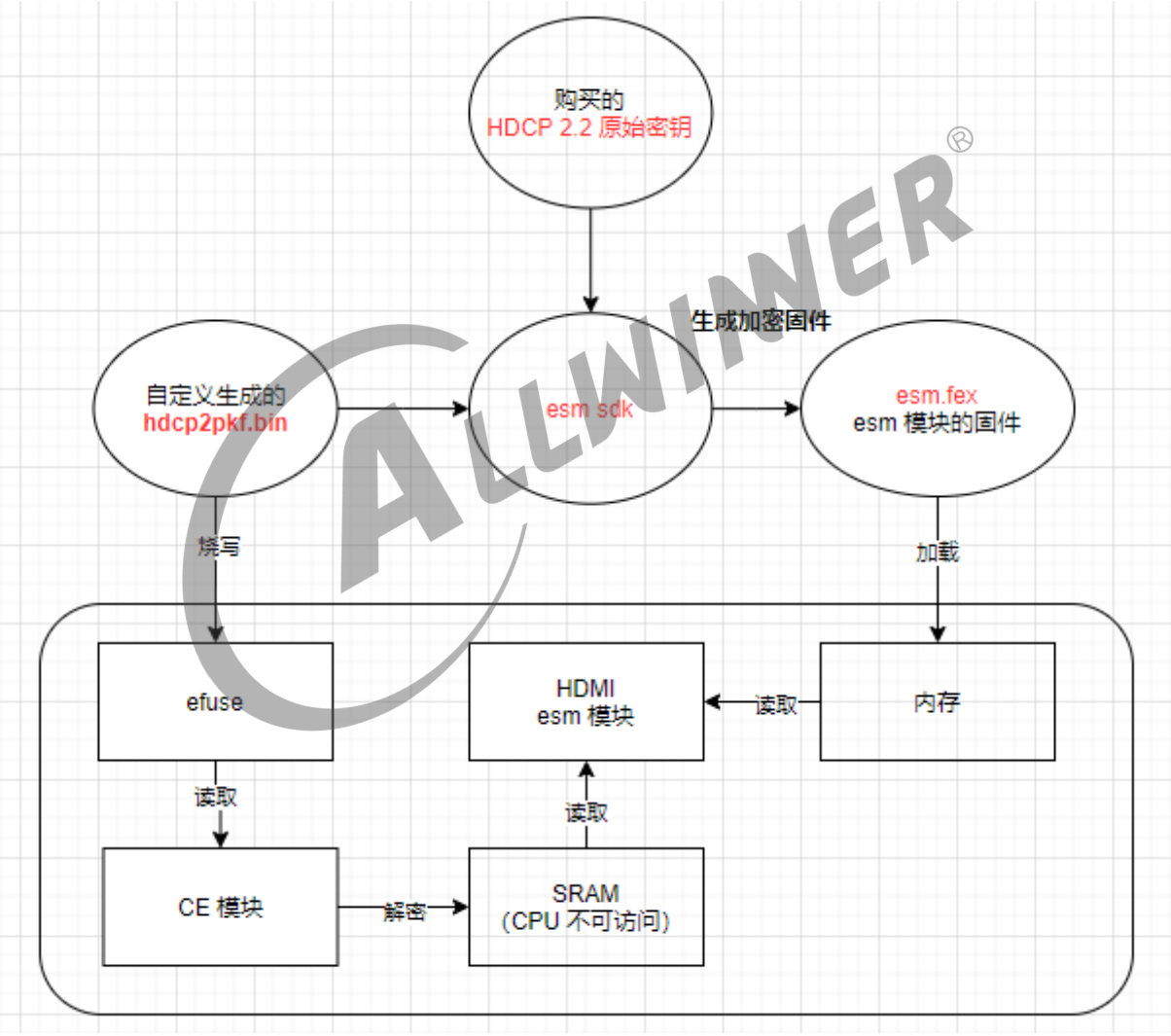

图 4-1: HDCP22 流程图

4.2 生成 hdcp2pkf.bin

hdcp2pkf.bin：是一串长度为 16 bytes 的随机数，这个值可按照自己需要去生成，但一旦确定下来要注意**一定要保存好**！

这里提供一个简单生成随机数的命令，用户也可自定义。

```
dd if=/dev/random of=hdcp2pkf.bin bs=16 count=1
```

4.3 生成 esm.fex

4.3.1 原始密钥的来源

DCP 官方给到客户的 HDCP 2.2 密钥文件是一个 **445 字节**的二进制文件，密钥文件 **无需切割**。

> 原始密钥需客户自行联系 DCP 组织购买，使用 HDCP 2.2 的 **每台机器**可以加载 **同一个**的原始密钥所生成的 esm 固件，**但是单个密钥能烧录多少台，则需要根据与 DCP 组织的合同来约定！**

以往经验：

首先需要缴纳年会员费，加入会员组织，然后根据需要烧录的数量，签订相应的合同，DCP 组织会不定期地抽查设备和商务合同来进行监管。

4.3.2 运行脚本

将上述步骤生成的 **hdcp2pkf.bin** 和客户自行购买到的**原始密钥**放到 esm sdk 的 vendor 目录下，然后执行 **build.sh** 脚本，最终会生成出 esm.fex 。

> 若 vendor 下的文件名称有变化，需要修改 build.sh 脚本里面对应的名称！

```
package_to_custome:
├──── build.sh      ---编译脚本
├──── esm.fex    ---最终生成的文件
├──── esmtool
├──── firmware
│    ├──── esm_config.i
│    └──── firmware.rom
├──── README.md
├──── utils
│    ├──── aictool
│    ├──── esm_swap
│    ├──── hdcpkeys
│    └──── sample.aic
└──── vendor
   ├──── hdcp2pkf.bin       ---生成方式查看上一章节
```

```
├── HDCP2_TX_KEY.bin    ---HDCP 2.2 原始密钥
└── hdcp_keys.le        ---(脚本执行过程中生成，无需关注)
```

4.4 烧录 hdcp2pkf.bin

4.4.1 配置 DragonSN 软件

1. 打开 **DragonSN**，点击左下角的 **配置 key**；

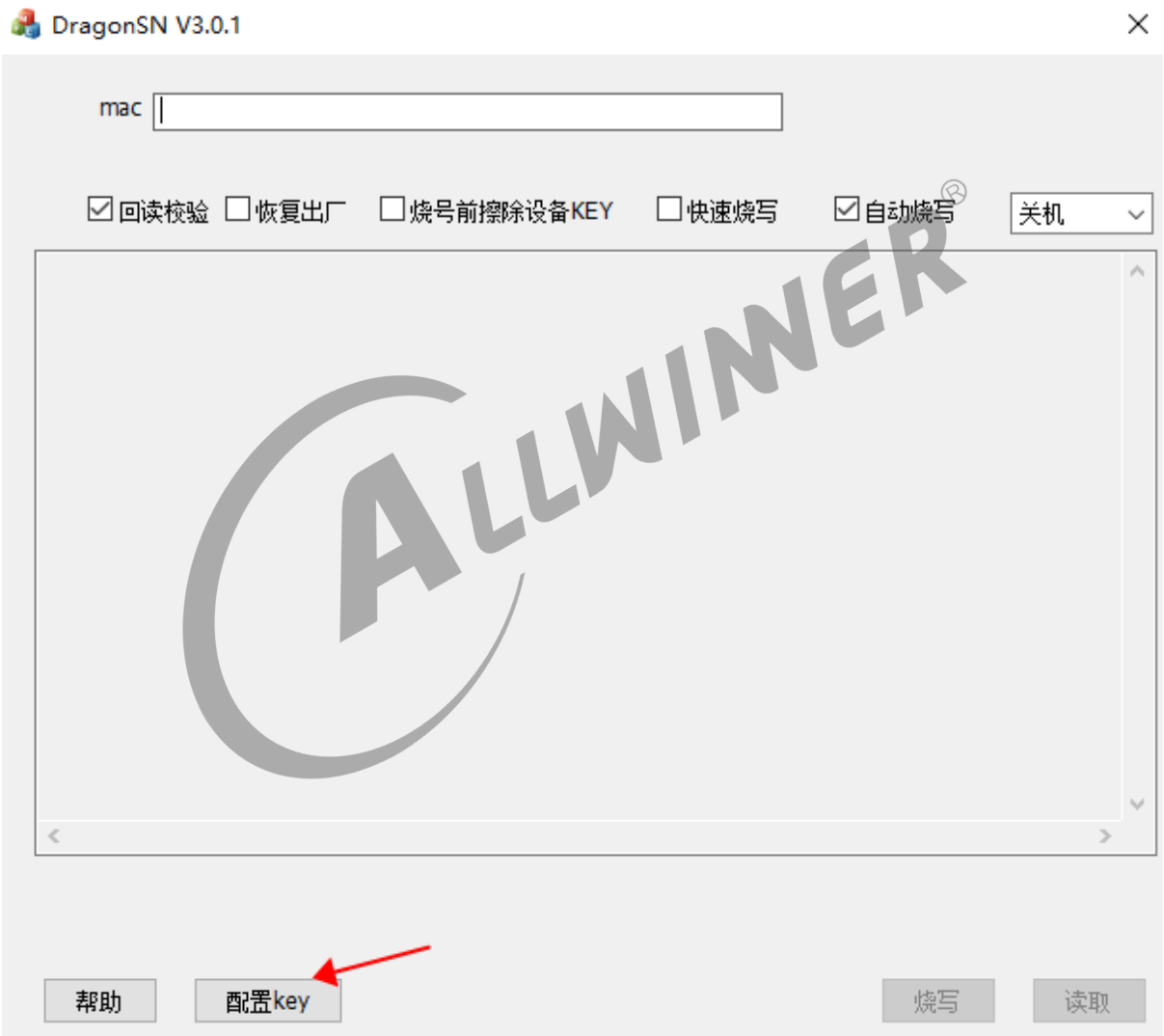

图 4-2: 配置 Key 入口

2. 如果当前配置有其他的配置项，请先**全部删除**，避免互相影响，右击，删除；

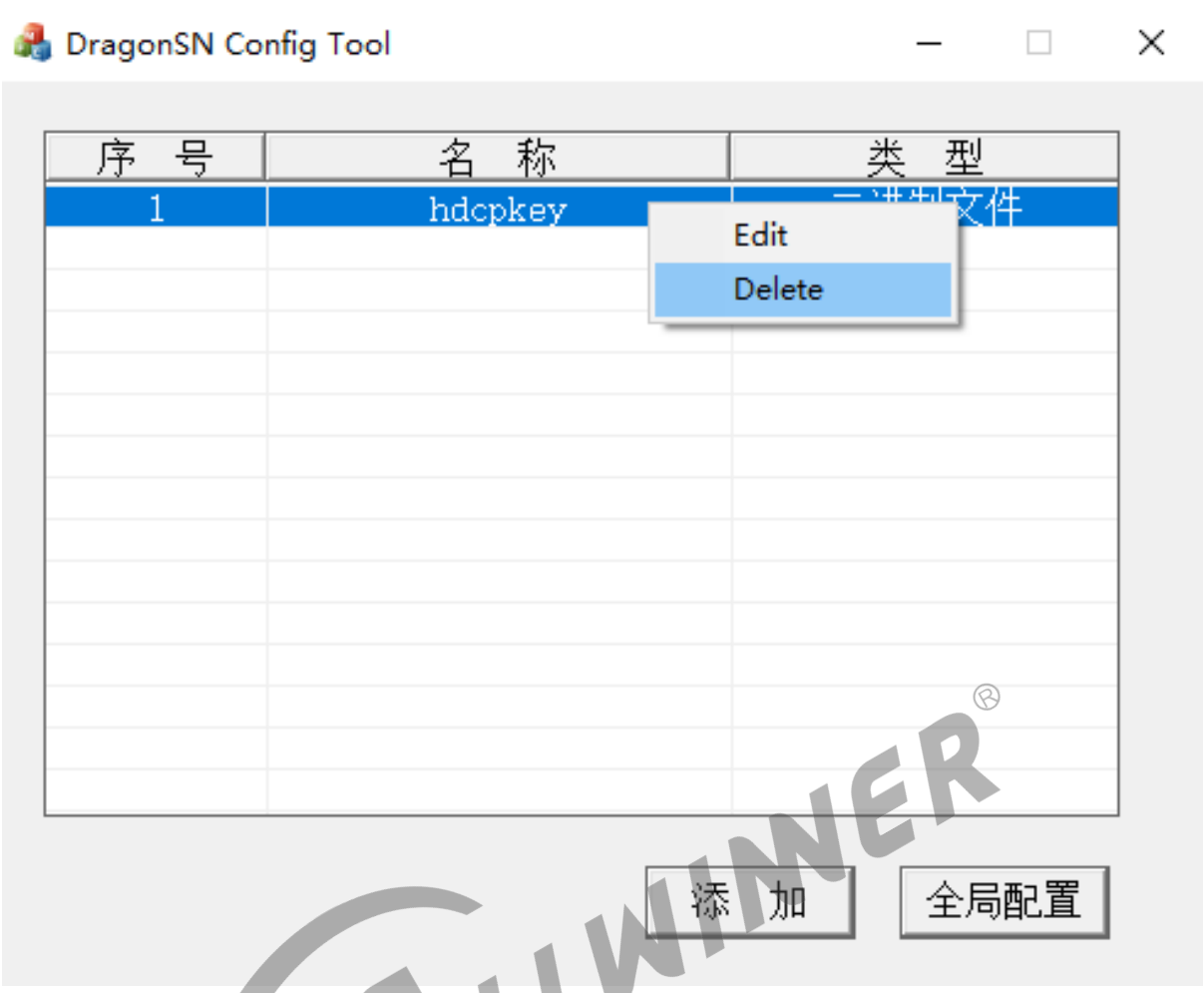

图 4-3: 删除 hdcpkey

3. 点击下方的添加，按下图所示配置，配置完成点击保存；

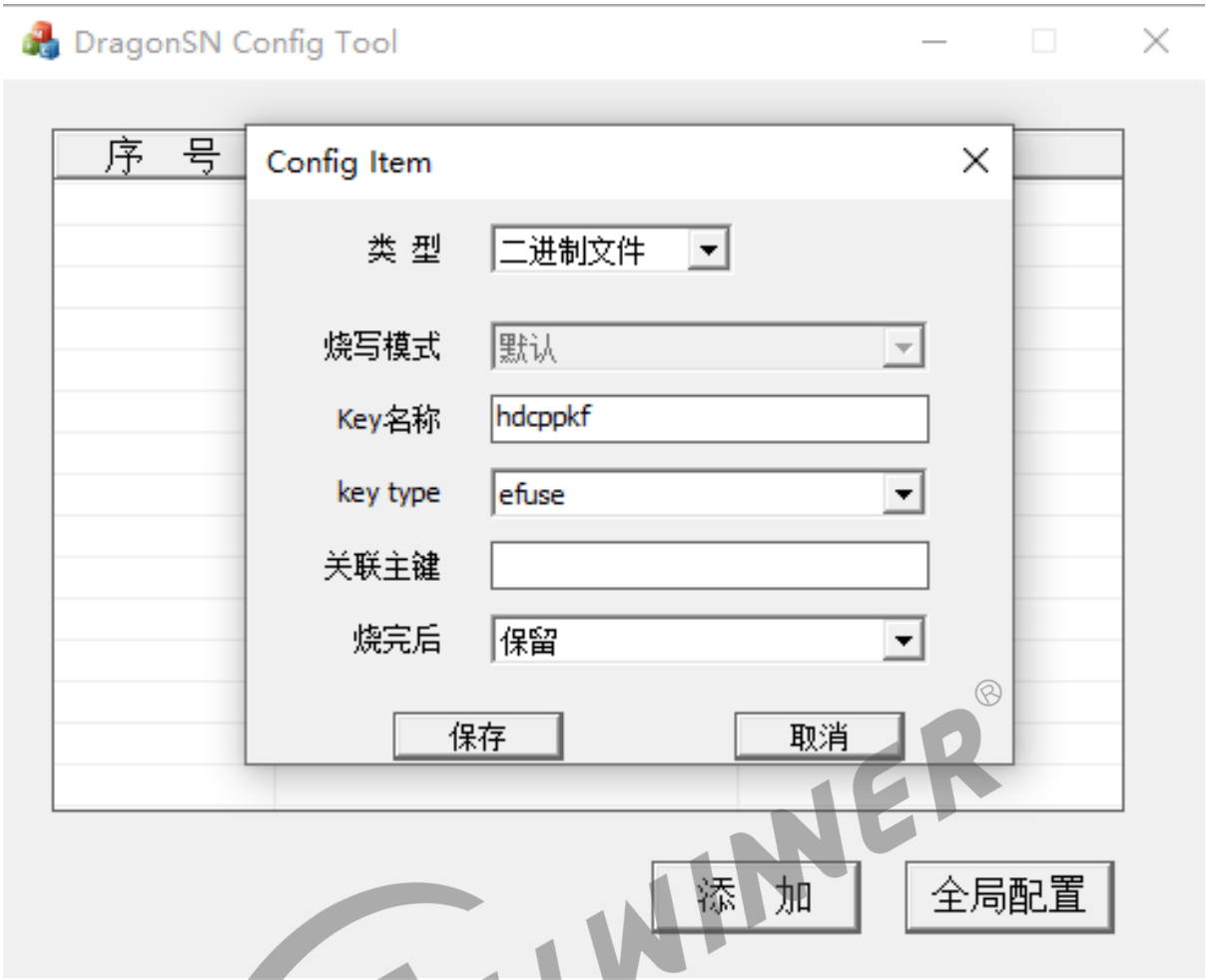

图 4-4: 配置 hdcppkf

关于 **烧完后**配置的解释：

1. 保留，一直烧同一个 key。
2. 移到 _used 目录，每烧完一个 key 就会将该文件移到同路径下的 _used 后缀文件夹中，即：依次烧不同的 key。

由于 HDCP 2.2 可以多个机器共用同一个 key，而且需要烧录的 pkf 也可以多台共用，所以选择 **保留**即可。

4. 点击 Config Tool 界面右上角的 X ，退出到 DragonSN 软件界面。

4.4.2 开始烧录

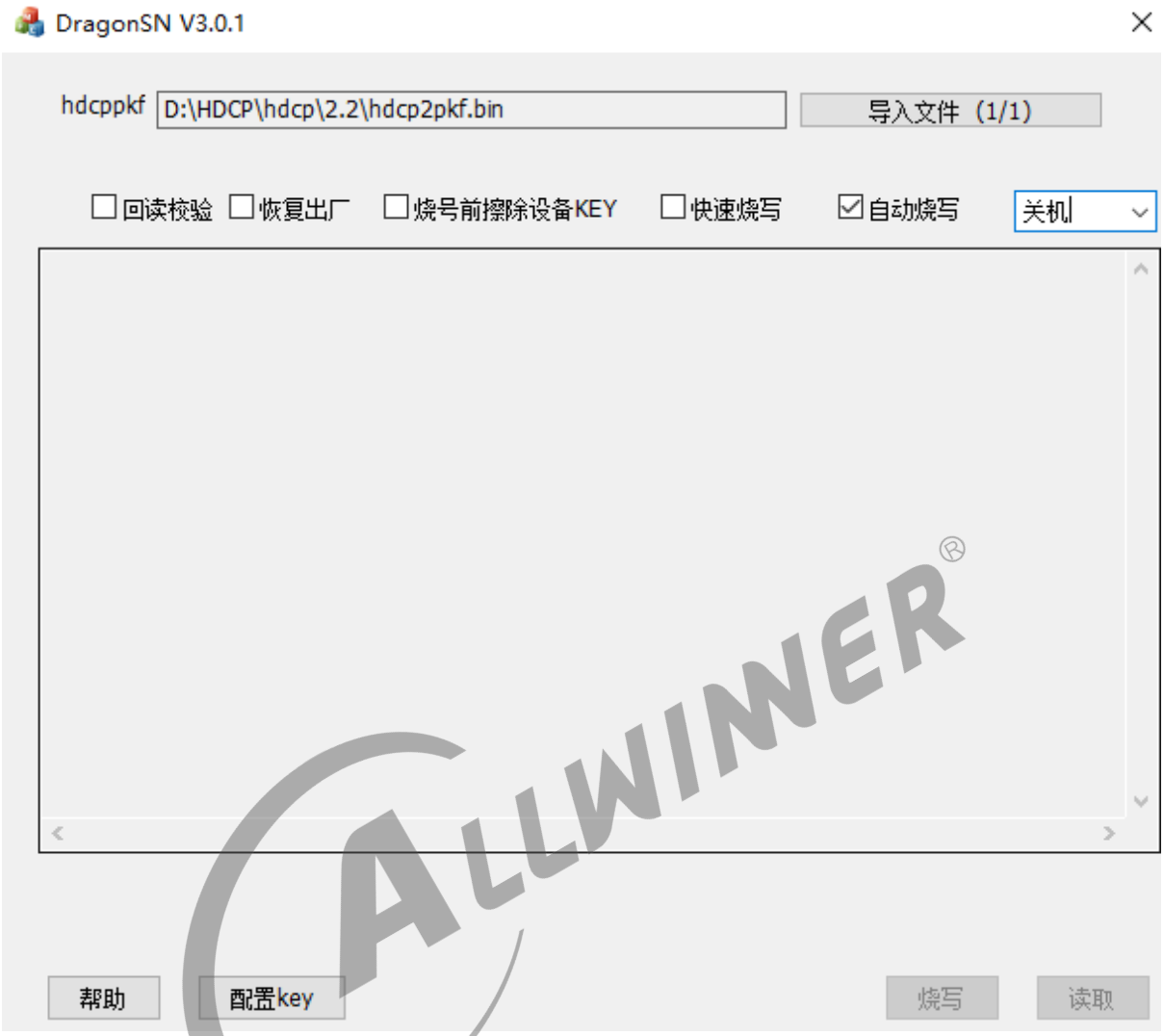

图 4-5: DragonSN_ 软件截图 2

1. 点击导入文件，选择要烧录的 **hdcp2pkf.bin** 所在文件夹（尽量避免中文路径）；
2. **勾选**自动烧写，**取消勾选**快速烧写，选择烧写结束后 **关机**；
3. 确认开发板与 PC 已用 USB 线连接；
4. 重启开发板，工具会自动烧录；
5. 烧录完成后，可点击 **读取**确认烧录成功；

> 这里是单台机器烧写的流程，如果是多台机器，烧录完成拔掉，插上另一台机器即可，无需重复配置。

4.5 加载 esm.fex

当前驱动提供了 2 种方法加载 ESM 固件：

1. 通过节点加载

```
cat /sys/class/hdmi/hdmi/attr/esm_dump
cat esm.fex > /sys/class/hdmi/hdmi/attr/esm_dump
```

2. 通过 ioctl 加载

```
CMD：
HDCP22_LOAD_FIRMWARE

PROTOTYPE：
int ioctl(int handle, unsigned int cmd,unsigned int *arg);

ARGUMENTS：
handle
  hdmi 驱动句柄；
cmd
  HDCP22_LOAD_FIRMWARE
arg
  arg[0]为 esm.fex 固件路径；
  arg[1]为 esm.fex 文件长度；

RETURNS：
  如果成功，返回0，否则，返回失败号；
```

4.6 功能验证

> 功能验证的前提：HDMI RX 端（例如：电视）需要支持 HDCP 2.2 功能，否则会开启失败！

- 驱动层面使能 HDCP 开启认证

```
echo 1 > /sys/class/hdmi/hdmi/attr/hdcp_enable
```

- 串口获取 HDCP 状态

```
busybox hexdump /sys/class/hdmi/hdmi/attr/hdcp_status

0000000 0003
# AW_HDCP_DISABLE 0
# AW_HDCP_ING 1
# AW_HDCP_FAILED 2
```

```
# AW_HDCP_SUCCESS 3
```

- 如果有下列打印，则证明 esm.fex 有异常或加载顺序有问题，需要重新检查烧录流程。

```
The HDMI RX support hdcp2.2
Wait for mailbox message timeout.
Failed to set FW_VLD bit (no response)
esm init mem failed!
[esm-error]:esm boots fail!
```

- 认证失败的解决方法

1. 重新确认密钥生成和烧录过程是否正确；
2. 确认烧录无误仍无法开启 HDCP，请联系全志 HDMI 工程师协助解决；

5 小结

因为 HDCP 1.4 和 2.2 存在较大差异，所以烧录密钥的过程也有许多不同，需要客户仔细完成每个步骤。

若对本文档有疑问或者改进建议，请联系对接的 AE 同事进行反馈。

6 Q&A

1. 如何确认当前开发板支持哪些版本的 HDCP?

```
cat /sys/class/hdmi/hdmi/attr/hdcp_dump
```

```
Tx use hdcp 1.4
Tx use hdcp 2.2
Enable HDCP
HDMI MODE: HDMI
esm firmware addr:0xa6080000  size:0x40000
esm data addr:0xa6060000  size:0x20000

Lowlevel Part:
Tx use hdcp 1.4
Tx use hdcp 2.2
Enable HDCP
HDCP  hardware has been Enable
HDMI MODE: DVI
```

2. 如何确定当前的 HDCP 状态?

```
busybox hexdump /sys/class/hdmi/hdmi/attr/hdcp_status
```

```
0000000 0003
# AW_HDCP_DISABLE 0
# AW_HDCP_ING 1
# AW_HDCP_FAILED 2
# AW_HDCP_SUCCESS 3
```

3. 如何确定当前使用的 HDCP 类型?

```
busybox hexdump /sys/class/hdmi/hdmi/attr/hdcp_type
```

```
0000000 0001
# DW_HDCP_TYPE_NULL -1
# DW_HDCP_TYPE_HDCP14 0
# DW_HDCP_TYPE_HDCP22 1
```

4. 开启 HDCP 时，出现 “esm set capability fail, maybe remote Rx is not 2.2 capable!” 如何解决?

> 可先尝试再次 echo 1 > /sys/class/hdmi/hdmi/attr/hdcp_enable，可能是 esm 启动异常。

著作权声明

商标声明

免责声明