



海思智能机顶盒 3 级安全方案 使用指南

文档版本 00B01
发布日期 2015-06-25

版权所有 © 深圳市海思半导体有限公司 2015。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HISILICON、海思和其他海思商标均为深圳市海思半导体有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受海思公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，海思公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

深圳市海思半导体有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： <http://www.hisilicon.com/cn/>

客户服务邮箱： support@hisilicon.com



前 言

概述

本文档主要介绍海思 3 级安全方案的使用方法。






读者对象

本文档（本指南）主要适用于以下工程师：

- 技术支持工程师
- 软件开发工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
 DANGER	表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
 WARNING	表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
 CAUTION	表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 TIP	表示能帮助您解决某个问题或节省您的时间。
 NOTE	表示是正文的附加信息，是对正文的强调和补充。



作者信息

章节号	章节名称	作者信息
全文	全文	W00269678

修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

修订日期	版本	修订说明
2015-06-25	00B01	第一次临时发布。



目 录

前 言.....	i
1 概述.....	1
1.1 安全方案 L3 介绍	1
1.2 安全方案 L3 分工	1
2 运营商使用指导.....	3
2.1 生成 Key 的步骤	3
2.2 签名 fastboot 步骤.....	5
2.2.1 环境准备	5
2.2.1 操作流程	5
2.3 签名 bootargs 分区	6
2.3.1 环境准备	6
2.3.2 操作流程	6
2.4 签名 recovery 分区	8
2.4.1 环境准备	8
2.4.2 操作流程	8
2.5 签名 kernel 分区.....	9
2.5.1 环境准备	9
2.5.2 操作流程	10
3 客户使用指导.....	13
3.1 编译.....	13
3.2 签名.....	13
3.3 修改制作 update.zip	13
3.4 USB 烧写	14
3.4.1 USB 裸片烧写.....	14
3.4.2 USB 非裸片烧写.....	14
3.5 烧片器烧写	15
3.6 HiTools 烧写	16



插图目录

图 2-1 CASignTool 生成 RSA Key	3
图 2-2 工具生成的 key 文件.....	4
图 2-3 签名 fastboot.....	5
图 2-4 生成文件	6
图 2-5 生成 FinalBoot.bin 文件.....	6
图 2-6 签名 bootargs.....	7
图 2-7 生成文件夹	7
图 2-8 生成 bootargs_Sign.img 文件	8
图 2-9 签名 recovery	9
图 2-10 生成文件夹	9
图 2-11 签名 kernel.....	10
图 2-12 生成文件夹	11
图 3-1 裸片烧写流程	15



1 概述

1.1 安全方案 L3 介绍

和安全方案 L2（见文档《海思智能机顶盒 2 级安全方案》）相比，厂商没有签名的 key，所以编译阶段无法生成带签名的 fastboot、bootargs、recovery、kernel 分区，需要把未签名的镜像给运营商签名，然后运营商再把签名好的镜像发给客户。当厂商得到签名后的镜像数据后烧写方法同安全方案 L2。



说明

本文以 Hi3798MV100 为例，其他支持的芯片类似处理。

1.2 安全方案 L3 分工

海思：

- 提供芯片和开发环境给机顶盒厂商；
- 提供给运营商 windows 签名工具，路径在：
device/hisilicon/bigfish/sdk/tools/windows/advca/CASignTool

运营商：

- 用签名工具生成两对 key 并对客户的分区镜像签名，步骤见 2.1 和 2.2 节；
- 提供给机顶盒厂商 root_rsa_pub.bin, roor_rsa_pub_crc.bin

机顶盒厂商：

- 编译出未签名的高安 fastboot 和其他分区镜像；
- 提供未签名的 fastboot, bootargs, recovery, kernel 给运营商，运营商对这些分区签名，再发给客户；
- 得到签名的镜像后，重新打包 update.zip



2 运营商使用指导

2.1 生成 Key 的步骤

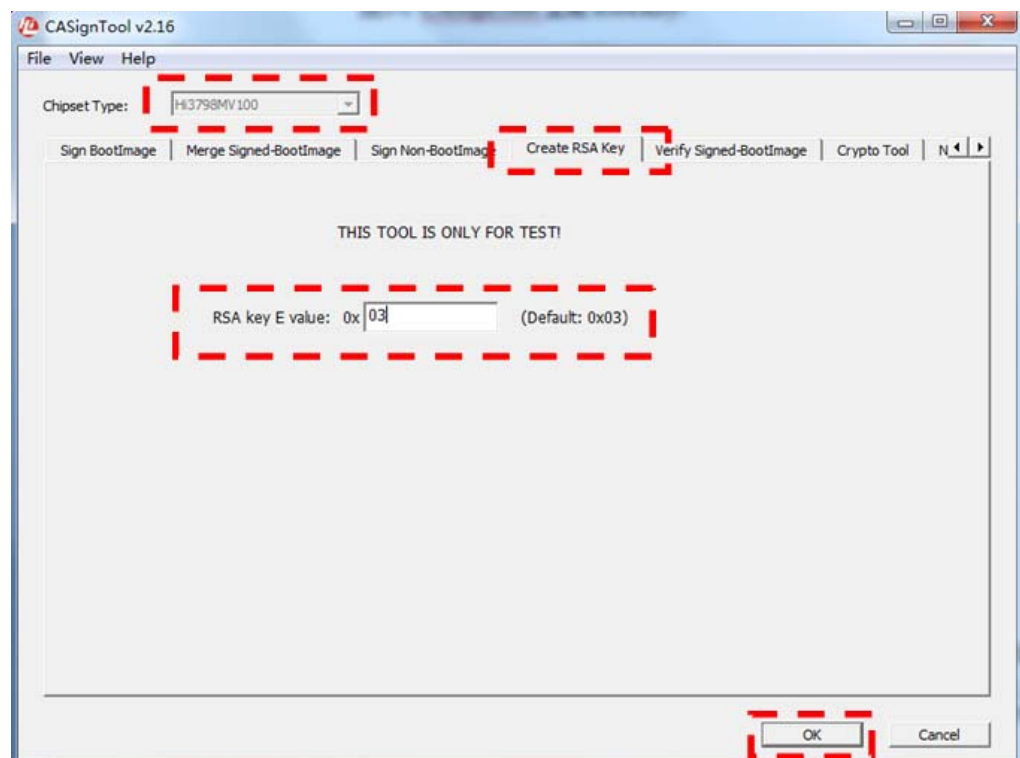
安全启动涉及到的镜像都需要使用密钥签名。一共有两对密钥：

- 一对用于对 fastboot 签名校验；
- 一对用于对除 fastboot 以外的其它镜像签名校验。

使用海思提供的工具生成两对密钥的步骤如下：

步骤 1 打开应用程序 CASignTool，切换至 Create RSA Key 页面，输入 RSA key E value 默认值：03，如图 2-1 所示。

图2-1 CASignTool 生成 RSA Key





注意

输入的 RSA key E value 默认值为 0x03，会用来生成 RSA Key 对。也可以输入其他 16 进制正整数，最大为 0xffffffff。不过改为其他值会大大增加生成密钥的计算量，推荐使用默认值 0x03。

- 步骤 2 点击 OK 键，工具会在其所在目录生成一个“RSA_XXXXXXX”的目录用于存放生成的 Key 文件，如图 2-2 所示。

图2-2 工具生成的 key 文件

rsa_priv.txt	2015/1/4 14:14
rsa_pub.bin	2015/1/4 14:14
rsa_pub.h	2015/1/4 14:14
rsa_pub.txt	2015/1/4 14:14
rsa_pub_crc.bin	2015/1/4 14:14

生成的第一对密钥，用于对 fastboot 的签名校验。

- 将 rsa_priv.txt 重命名为 root_rsa_priv.txt
- 将 rsa_pub.bin 重命名为 root_rsa_pub.bin
- 将 rsa_pub_crc.bin 重命名为 root_rsa_pub_crc.bin
- 其他文件用不到，可以删除

- 步骤 3 再次点击 OK，生成第二对密钥，用于 bootargs、recovery、kernel 等的签名校验。

- 将 rsa_pub.txt 重命名为 extern_rsa_pub.txt
- 将 rsa_priv.txt 重命名为 extern_rsa_priv.txt
- 其他文件用不到，可以删除

- 步骤 4 把 root_rsa_priv.txt，extern_rsa_pub.txt，extern_rsa_priv.txt，root_rsa_pub.bin，root_rsa_pub_crc.bin 五个文件保存到一个文件夹，不要泄露。

----结束



注意

运营商需要自己保留 root_rsa_priv.txt，extern_rsa_pub.txt，extern_rsa_priv.txt 三个 key 对 fastboot 签名；

运营商需要发送给厂商的是 root_rsa_pub.bin 和 root_rsa_pub_crc.bin。



2.2 签名 fastboot 步骤

2.2.1 环境准备

环境准备步骤如下：

步骤 1 配置密钥对。

- root 私钥——root_rsa_priv.txt
- external 公钥——external_rsa_pub.txt
- external 私钥——external_rsa_priv.txt

步骤 2 单板配置参数 cfg.bin（由客户提供）。

步骤 3 准备普通 boot（由客户提供）。

----结束

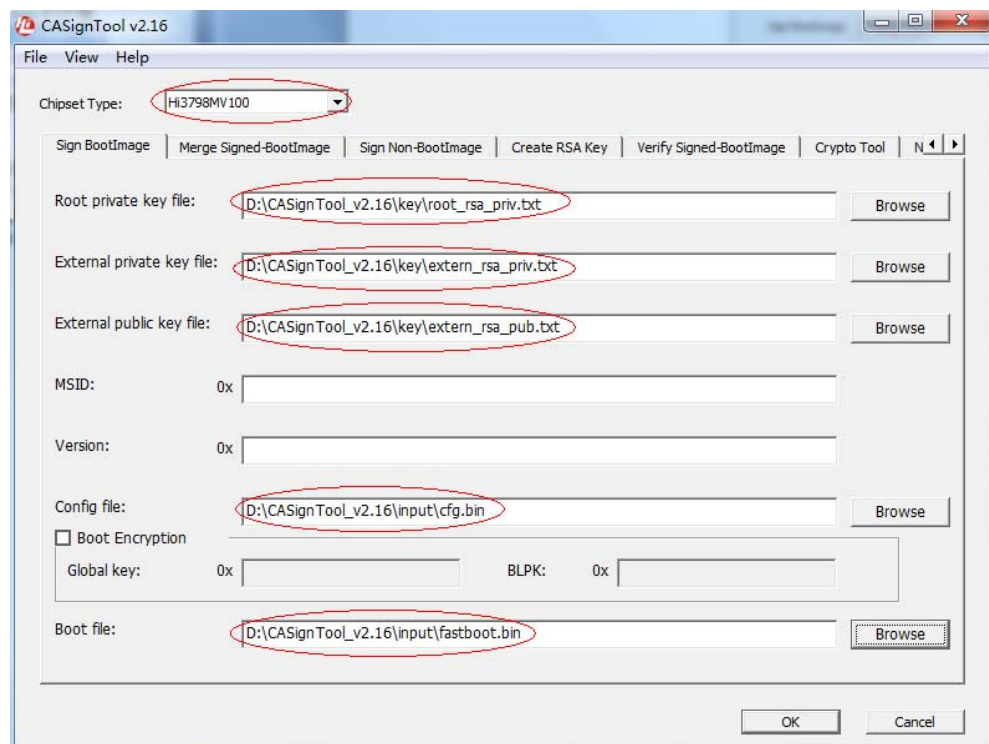
2.2.1 操作流程

操作流程如下：

步骤 1 打开应用程序 CASignTool。芯片类型选择 Hi3798MV100 为例。

步骤 2 切换至 Sign BootImage 页面，按照图 2-3 配置。

图2-3 签名 fastboot

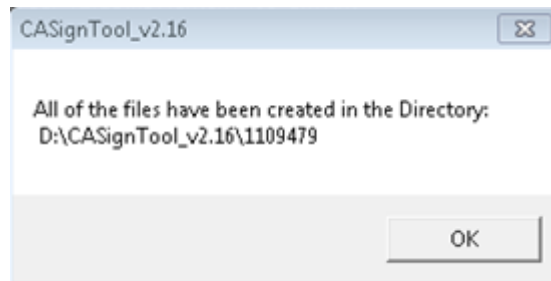


步骤 3 单击“ok”键。



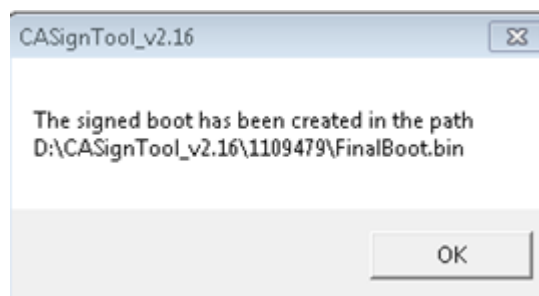
步骤 4 工具将会在工具所在的文件夹新建一个文件夹，生成文件放在这个文件夹下。

图2-4 生成文件



步骤 5 带签名的安全 boot 的名字为 FinalBoot.bin

图2-5 生成 FinalBoot.bin 文件



2.3 签名 bootargs 分区

2.3.1 环境准备

环境准备步骤如下：

步骤 1 配置密钥对。

- external 公钥——external_rsa_pub.txt
- external 私钥——external_rsa_priv.txt

步骤 2 准备未签名的 bootargs.bin——由客户提供。

----结束

2.3.2 操作流程

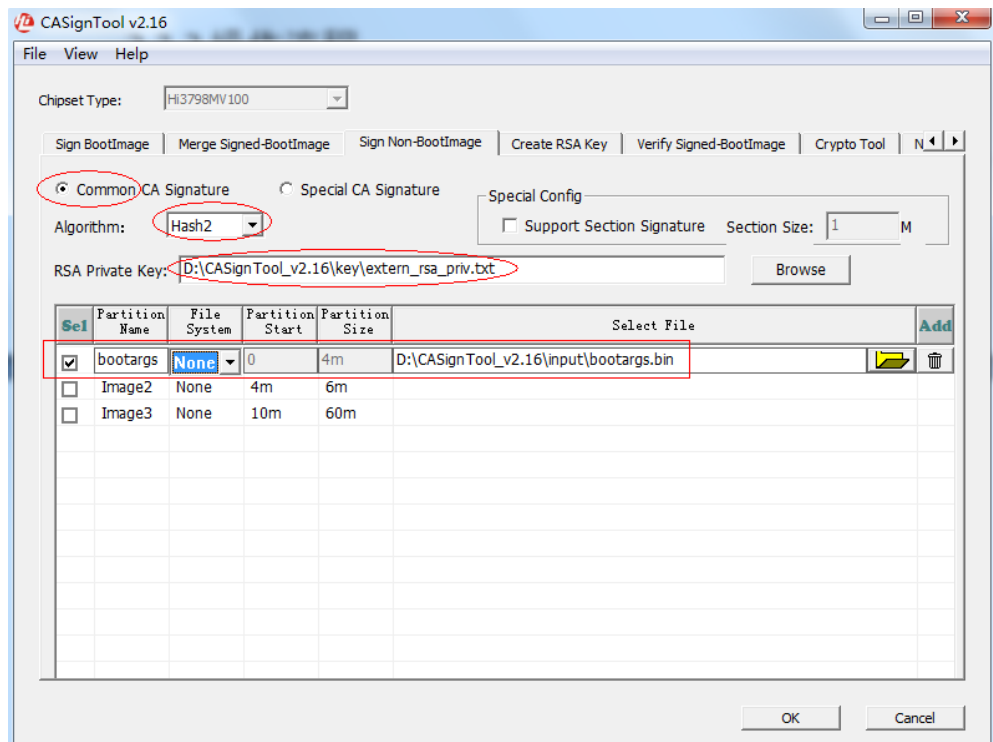
操作流程如下：

步骤 1 打开应用程序 CASignTool，切换至 Sign Non-BootImage 页面。

步骤 2 按照图 2-6 配置，签名方式选择 Common CA Signature。



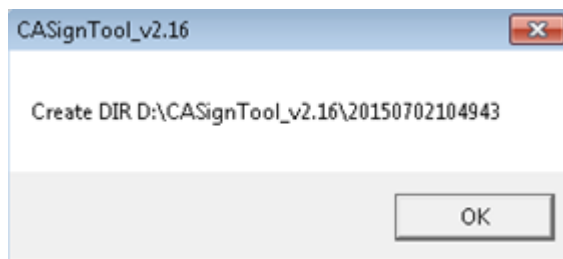
图2-6 签名 bootargs



步骤 3 单击“ok”键。

步骤 4 工具将会在工具所在的文件夹新建一个文件夹，生成文件放在这个文件夹下。

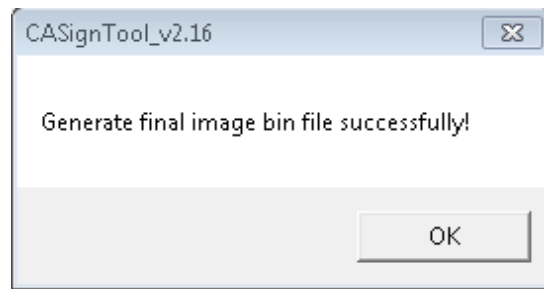
图2-7 生成文件夹



步骤 5 带签名的 bootargs 的名字为 bootargs_Sign.img



图2-8 生成 bootargs_Sign.img 文件



----结束

2.4 签名 recovery 分区

2.4.1 环境准备

环境准备步骤如下：

步骤 1 配置密钥对。

- external 公钥——external_rsa_pub.txt
- external 私钥——external_rsa_priv.txt

步骤 2 准备未签名的 recovery.img（由客户提供）。

----结束

2.4.2 操作流程

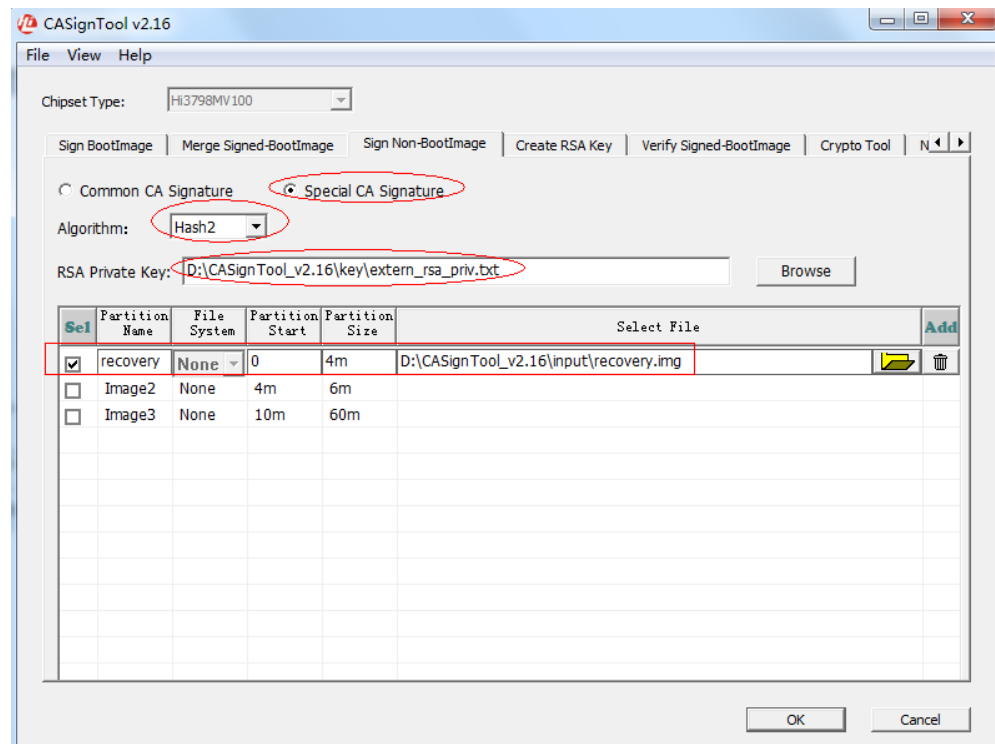
操作流程如下：

步骤 1 打开应用程序 CASignTool，切换至 Sign Non-BootImage 页面。

步骤 2 按照图 2-6，配置签名方式选择 Special CA Signature。



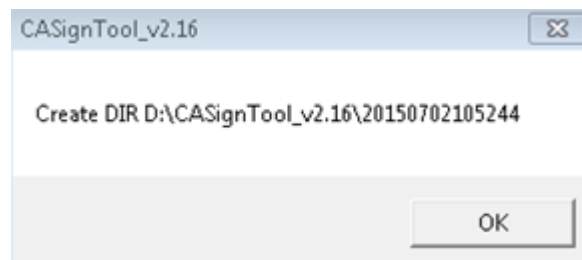
图2-9 签名 recovery



步骤 3 单击“ok”键。

步骤 4 工具将会在工具所在的文件夹新建一个文件夹，生成文件放在这个文件夹下。

图2-10 生成文件夹



步骤 5 带签名的 recovery 的名字为 FinalImage.bin，需要重命名为 recovery_Sign.img。

-----结束

2.5 签名 kernel 分区

2.5.1 环境准备

环境准备步骤如下：



步骤 1 配置密钥对。

- external 公钥——external_rsa_pub.txt
- external 私钥——external_rsa_priv.txt

步骤 2 准备未签名的 kernel.img（由客户提供）。

----结束

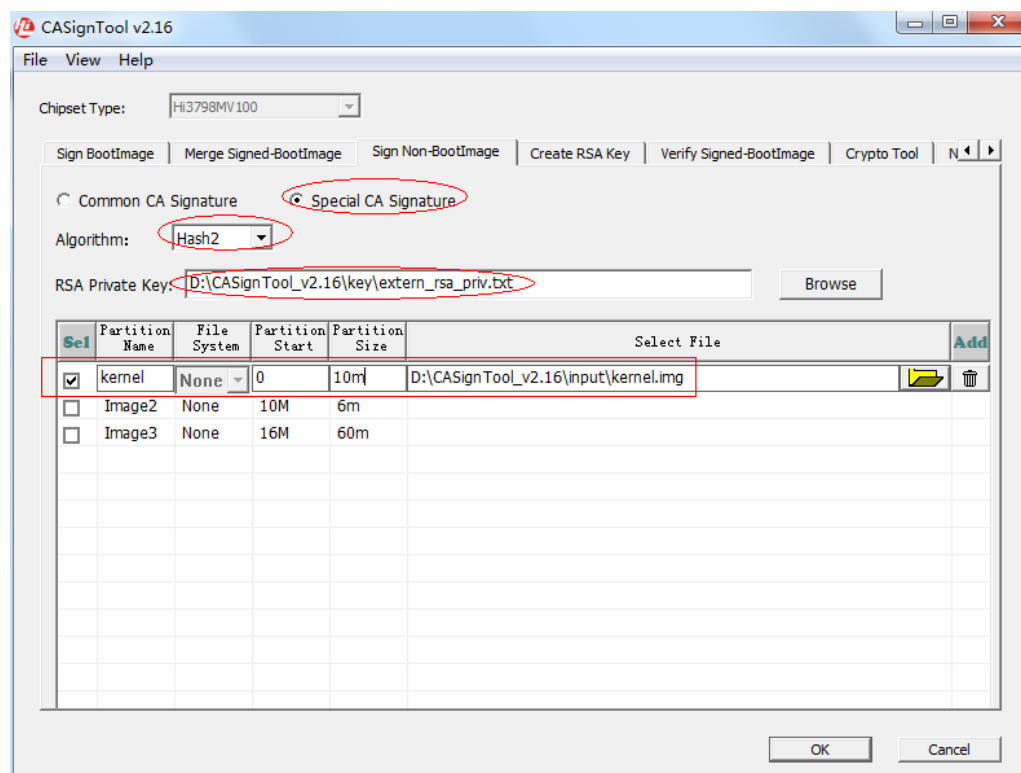
2.5.2 操作流程

操作流程如下：

步骤 1 打开应用程序 CASignTool，切换至 Sign Non-BootImage 页面。

步骤 2 按照图 2-11 配置，配置签名方式选择 Special CA Signature。

图2-11 签名 kernel

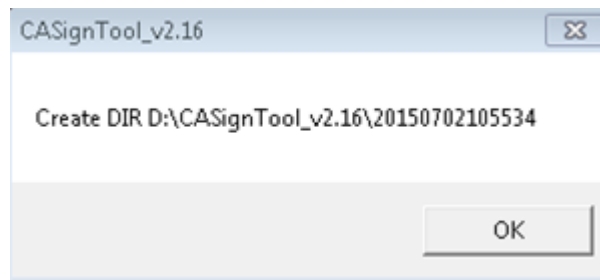


步骤 3 单击“ok”键。

步骤 4 工具将会在工具所在的文件夹新建一个文件夹，生成文件放在这个文件夹下。



图2-12 生成文件夹



步骤 5 带签名的 kernel 的名字为 FinalImage.bin，需要重命名为 kernel_Sign.img。

----结束

当所有的镜像签过名后，把带签名的分区镜像发送给机顶盒厂商。



3 客户使用指导

3.1 编译

在 device/hisilicon/Hi3798MV100/customer.mk 增加安全方案 L3 开关:

```
HISILICON_SECURITY_L3 := true
```

当打开开关后,能编译出未签名的安全 fastboot.bin 和其它未签名的各个分区镜像在如下目录:

```
out/target/product/Hi3798MV100/Emmc
```

3.2 签名

- 厂商编译出未签名的镜像后,提供如下文件给运营商签名:
 - 未签名的 fastboot.bin、bootargs.bin、recovery.img、kernel.img
 - 版本对应的 boot cfg 文件:
文件路径: device/hisilicon/bigfish/sdk/source/boot/sysreg
 - 镜像签名方式:
bootargs 用 common 方式签名;
recovery 和 kernel 通过 special 方式签名
- 运营商对这些分区签名,再发给厂商如下文件:
 - 签名后的分区镜像: Finalboot.bin、bootargs_Sign.img、recovery_Sign.img、kernel_Sign.img
 - 安全启动 otp root key: root_rsa_pub.bin、root_rsa_pub_crc.bin

3.3 修改制作 update.zip

用签名后的 Finalboot.bin、bootargs_Sign.img、recovery_Sign.img 和 kernel_Sign.img 替换 update.zip 中未签名的这几个分区,重新生成 update.zip。需要用到 HiUpdateEdit 工具,路径在:

```
device/hisilicon/bigfish/sdk/tools/windows/advca/HiUpdateEdit
```



使用方法见文档《HiUpdateEdit 工具使用指南》。



注意

使用 HiUpdateEdit 工具制作升级包时，需要拷贝源码包 device/hisilicon/Hi3798MV100/security 下的所有 key 到工具文件夹 HiUpdateEdit\Config\ 下，同时把 releasekey.pk8 和 releasekey.x509.pem 分别命名为 testkey.pk8 和 testkey.x509.pem。

3.4 USB 烧写

3.4.1 USB 裸片烧写

裸片烧写前需要准备如下：

- 未签名的 fastboot.bin、bootargs.bin、recovery.img 和重新生成的 update.zip
- 运营商提供的 key：root_rsa_pub_crc.bin
- FAT32 格式的 U 盘

USB 裸片烧写的步骤如下：

- 步骤 1 将 fastboot.bin、bootargs.bin、recovery.img、update.zip、root_rsa_pub_crc.bin 拷贝至 U 盘根目录。
- 步骤 2 将 U 盘插入 USB2.0 接口。
- 步骤 3 将单板上电，将自动进入烧写流程。烧写过程中指示灯会不断闪烁，烧写完成后，指示灯将常亮。

----结束

3.4.2 USB 非裸片烧写

经过 USB 裸片烧写，启动完成的单板，已经锁定为安全芯片。安全芯片再烧写，需使用 USB 非裸片烧写方式。

非裸片烧写需要准备：

- 运营商签过名的 FinalBoot.bin、bootargs_Sign.img、recovery_Sign.img 和重新生成的 update.zip
- FAT32 格式的 U 盘

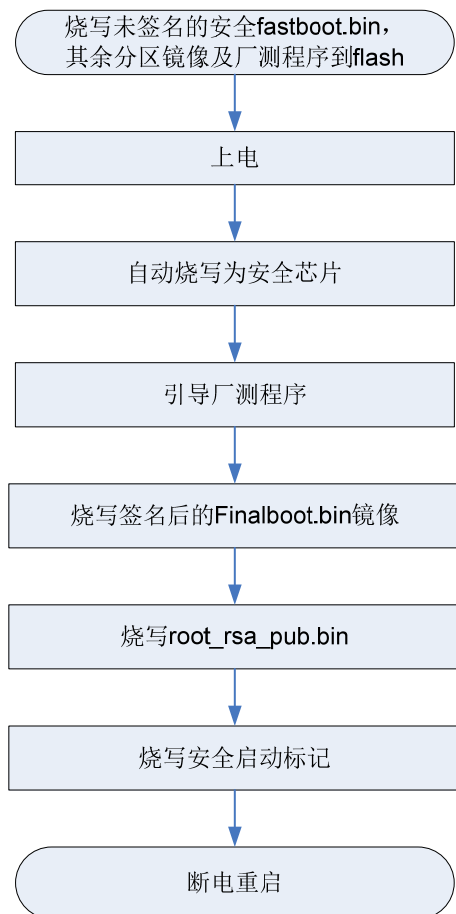
- 步骤 1 将 FinalBoot.bin、bootargs_Sign.img、recovery_Sign.img 分别重命名为 fastboot.bin、bootargs.bin、recovery.img，和重新生成的 update.zip 拷贝至 U 盘根目录。
- 步骤 2 将 U 盘插入 USB2.0 接口。
- 步骤 3 按住单板上的 USB 烧写按键上电，进入烧写流程。烧写过程中指示灯会不断闪烁，烧写完成后，指示灯将常亮。



----结束

3.5 烧片器烧写

图3-1 裸片烧写流程



烧片器烧写步骤如下：

- 步骤 1 用烧片器烧写未签名的 fastboot.bin 和签过名的 bootargs_Sign、recovery_Sign, kernel_Sign, 以及其他各分区。
- 步骤 2 单板上电, 此时 fastboot.bin 会把单板烧写成安全芯片, 并进入厂测程序。
- 步骤 3 通过厂测程序烧写运营商签过名的 Finalboot.bin, 烧写时需要从 flash 初始地址偏移 512 Byte 的地方烧写。
- 步骤 4 通过厂测程序烧写 OTP root key 和安全启动标志位。

----结束



3.6 HiTools 烧写

HiTools 裸片烧写步骤如下：

步骤 1 HiTools 烧写未签名 fastboot.bin。

- 选择芯片类型：Hi3798MV100
- 选择烧写未签名的 fastboot.bin
- 启动烧写，烧写完毕后上电，单板将被烧写成安全芯片

步骤 2 HiTools 烧写其他镜像。

- 选择芯片类型：Hi3798MV100_CA
- Programmer 文件选择：运营商签过名的 Finalboot.bin
- Fastboot、bootargs、recovery、kernel 选择签过名的分区镜像
- 其他分区镜像均未被签名，选择默认的
- 启动烧写

步骤 3 系统起来后通过命令行烧写 root_rsa_pub.bin 和安全启动标志位：

```
sample_ca_writeRSAkey /sdcard/root_rsa_pub.bin  
sample_ca_opensecboot emmc
```

----结束

对于非裸片，通过 HiTools 烧写只需从上面步骤 2 开始执行就可以。