Rockchip

Android Pie 安全启动方案使用指南

发布版本:**1.00**

日期:**2018.12**

前言

概述

本文档主要介绍基于 Rockchip Android 9.0 的 Box 平台，所配套的完整安全启动方案(RK secure boot +AVB)工作原理，流程以及配置使用方法。

产品版本

芯片名称	内核版本	**Uboot** 版本
RK3128H	4.4	next-dev
RK3229	4.4	next-dev
RK3328	4.4	next-dev

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

修订记录

日期	版本	作者	修改说明
2018.12.24	V1.00	huangjc	初始版本

目录

插图目录

1 安全启动方案说明

1.1 概述

Rockchip 安全启动方案基于 RK 芯片提供的硬件保护机制，对机顶盒的引导程序 loader, uboot, trust 镜像以及 Android 系统（boot(含 kernel), recovery、system、vendor、oem 等镜像）提供可靠的安全保护。对于机顶盒产品可用于保护机顶盒系统安全，防止机顶盒被刷机或业务相关应用被篡改等。

具体开发指导细节，请参考《Rockchip Secure Boot Application Note》和《Rockchip Android Pie AVB HOWTO》。

RK 安全启动方案的特性：

- 支持 Secure Boot Rom
- 支持 SHA256 或者 SHA160
- 支持 RSA2048 或者 RSA 1024
- 支持 efuse/OTP 验证 RSA Public Key
- 支持 Secure Boot Rockusb 升级固件
- 支持 Google AVB 2.0

1.2 安全启动

1.2.1 基本原理

名词介绍：

- BL1：Bootloader 1
- OBM code：需要被保护的代码，如 Bootloader，Uboot
- OTP：one time program 器件，芯片内存储器件，只允许写一次，RK 部分芯片使用 EFUSE 实现
- SHA256：Secure Hash Algorithm,结果为 256bit 的哈希值
- RSA2048：一种非对称算法，秘钥长度为 2048bit
- Data storge：只用于存储 boot 数据的 memory，如 flash，EMMC 等
- Data generate：数据的产生过程
- Data process in Bootrom：Bootrom 程序对安全数据的校验过程
- AVB：android verify boot，android 9.0 上支持的启动校验功能，主要用来验证各分区数据的完整性。

RK Android 9.0 平台上安全启动主要有两个部分组成：引导程序（uboot）的安全启动和 AVB；在安全启动开启后，Boot ROM 作只读代码 BL1，是可信的，BL1 会验签 loader，loader 会验签 uboot 和 trust，后续采用逐级验签的方式验证加载的每个字节是否篡改。

基本流程框图如下：

Non-A/B system：

AVB 2.0

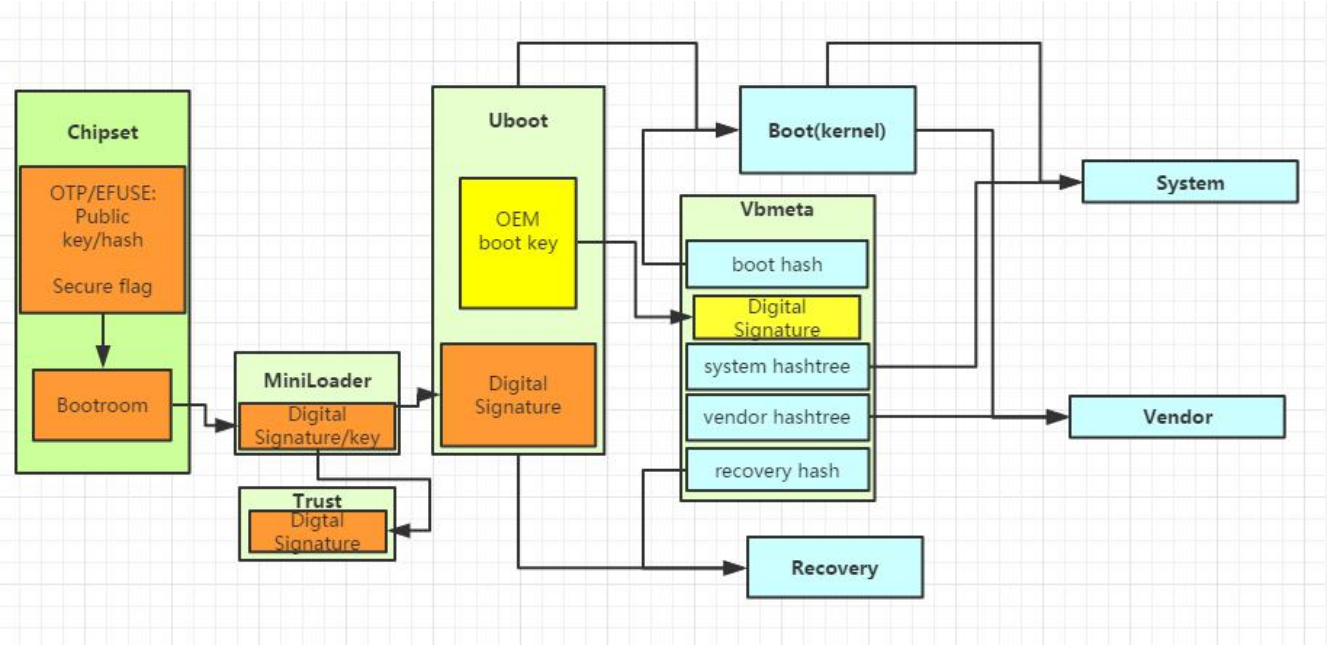


图 1-1 安全启动流程

步骤 1：

芯片上电后，片内 Boot ROM 判断 OTP 中的高安启动标志是否打开，若打开使用 OTP 中的 pubkey 对 Flash 中 Miniloader 内存储的签名进校验；

步骤 2：

若校验通过，Miniloader 开始加载并校验 Uboot 和 trust 镜像及签名，如果校验通过则执行下一步操作，否则系统复位；

步骤 3：

Uboot 校验通过后，开始执行 Vbmeta 元数据分区的校验，Vbmeta 校验通过后，Uboot 开始加载并对比 Vbmeata 中对应元数据分别校验 Boot、recovery 镜像分区，如果校验通过则执行下一步操作，否则系统复位；

步骤 4：

Boot 校验完成后，内核启动挂载 system 分区，开始对比 Vbmeata 中对应元数据分别校验 system 分区和 vendor 分区数据是否完整，若检测到不完整，系统复位。

----结束

1.2.2 引导程序的安全启动

引导程序的安全启动由 Rockchip Secure Boot Application 方案保证，基于 RK 芯片提供的硬件保护机制（OTP），基本原理如下图，细节可参考**《Rockchip Secure Boot Application Note》**。

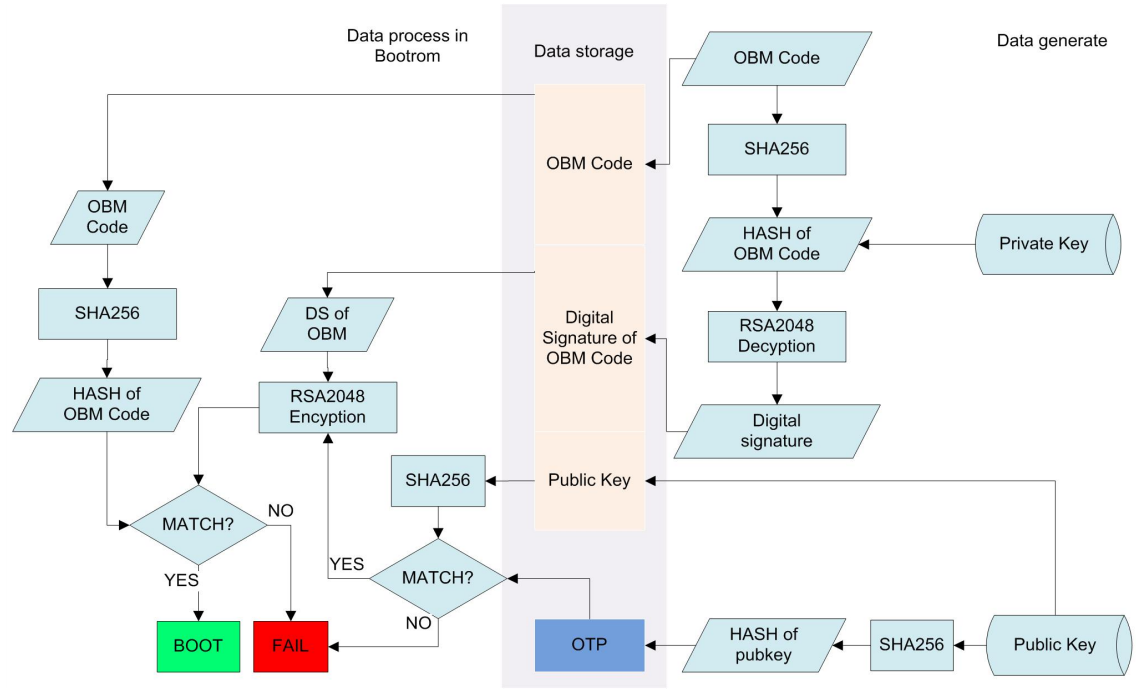


图 1-2Rockchip Secure Boot Application 流程

1.2.3 Android Verify Boot 2.0

AVB2.0(Android Verified Boot2.0)是 google 新设计的 verified boot 流程用于保护 boot/recovery/system/vendor 等一些受保护分区的完整性的功能。完整性相关的元数据放在 vbmeta 分区，只有验证了 vbmeta 的签名，AVB 才是有效的，vbmeta 签名验证在 U-Boot 中。

具体细节请参考**《Rockchip Android Pie AVB HOWTO》**和谷歌开发官网：

https://source.android.google.cn/security/verifiedboot/verified-boot

2 配置方法

2.1 概述

本节主要说明 Rockchip 安全启动方案使用与配置方式，方便客户快速集成。

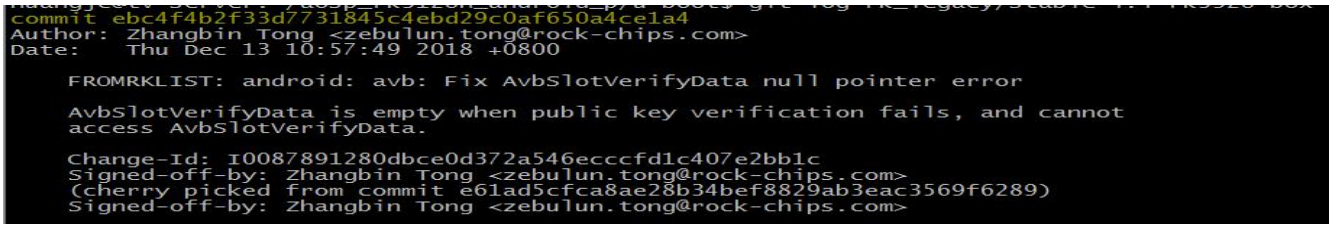
2.2 AVB 2.0 配置

AVB 2.0 功能开关只需要在源码对应产品目录下将宏 BOARD_AVB_ENABLE 开启重新编译即可，如 rk3328 box 产品平台下：

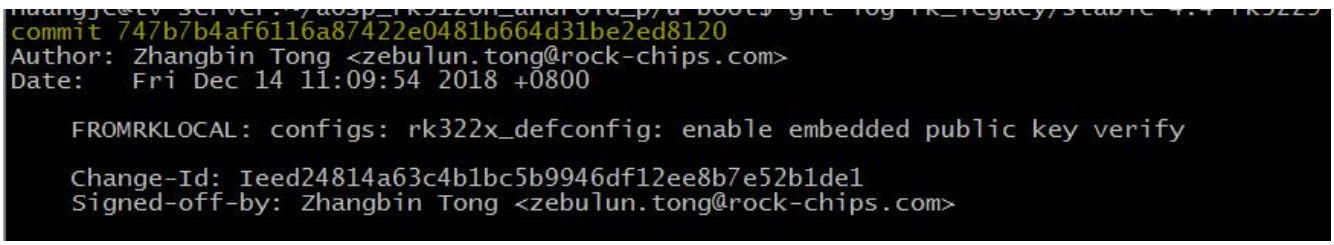
```
huangjc@tv-server:~/aosp_rk3328_android_p/device/rockchip/rk3328$ git diff .
diff --git a/rk3328_box/BoardConfig.mk b/rk3328_box/BoardConfig.mk
index 1425e95..5d242b5 100755
--- a/rk3328_box/BoardConfig.mk
+++ b/rk3328_box/BoardConfig.mk
@@ -36,7 +36,7 @@ TARGET_2ND_CPU_VARIANT := cortex-a53
 TARGET_PREBUILT_KERNEL := kernel/arch/arm64/boot/Image

 BOARD_CACHEIMAGE_FILE_SYSTEM_TYPE := ext4
-BOARD_AVB_ENABLE := false
+BOARD_AVB_ENABLE := true
 ifneq ($(filter true, $(BOARD_AVB_ENABLE)), )
 BOARD_KERNEL_CMDLINE := console=ttyFIQ0 androidboot.baseband=N/A
androidboot.selinux=permissive androidboot.wificountrycode=US
androidboot.hardware=rk30board androidboot.console=ttyFIQ0
firmware_class.path=/vendor/etc/firmware init=/init rootwait ro init=/init
 else
```

其它如 OEM boot key 生成、替换、fastboot 设备锁定等配置方法，请参考文档《Rockchip Android Pie AVB HOWTO》。

注意，要支持 AVB 2.0 相关功能，需要确认代码是否已更新如下提交：
rk3328 u-boot 目录：



rk3229 u-boot 目录：



Rk3128h u-boot 目录：

```
commit 9458472eba2d525c88c6d6a30785472c0996131b
Author: Zhangbin Tong <zebulun.tong@rock-chips.com>
Date:   Mon Dec 24 13:45:00 2018 +0800

    FROMRKLOCAL: configs: rk3128x_defconfig: enable embedded public key verify

    Change-Id: If9635bc69d2cfa13d54ab8281c8c6e7f74a18fea
    Signed-off-by: Zhangbin Tong <zebulun.tong@rock-chips.com>
```

2.3 Rockchip Secure Boot 配置

Rockchip Secure Boot 使用基本流程如下：

- 打包完整固件镜像 update.img
- 使用签名工具 SecureBootTool 签名固件（需要客户先生成自己的公私钥）
- 烧写 EFUSE
- 烧写签名后固件
- 验证安全启动开启

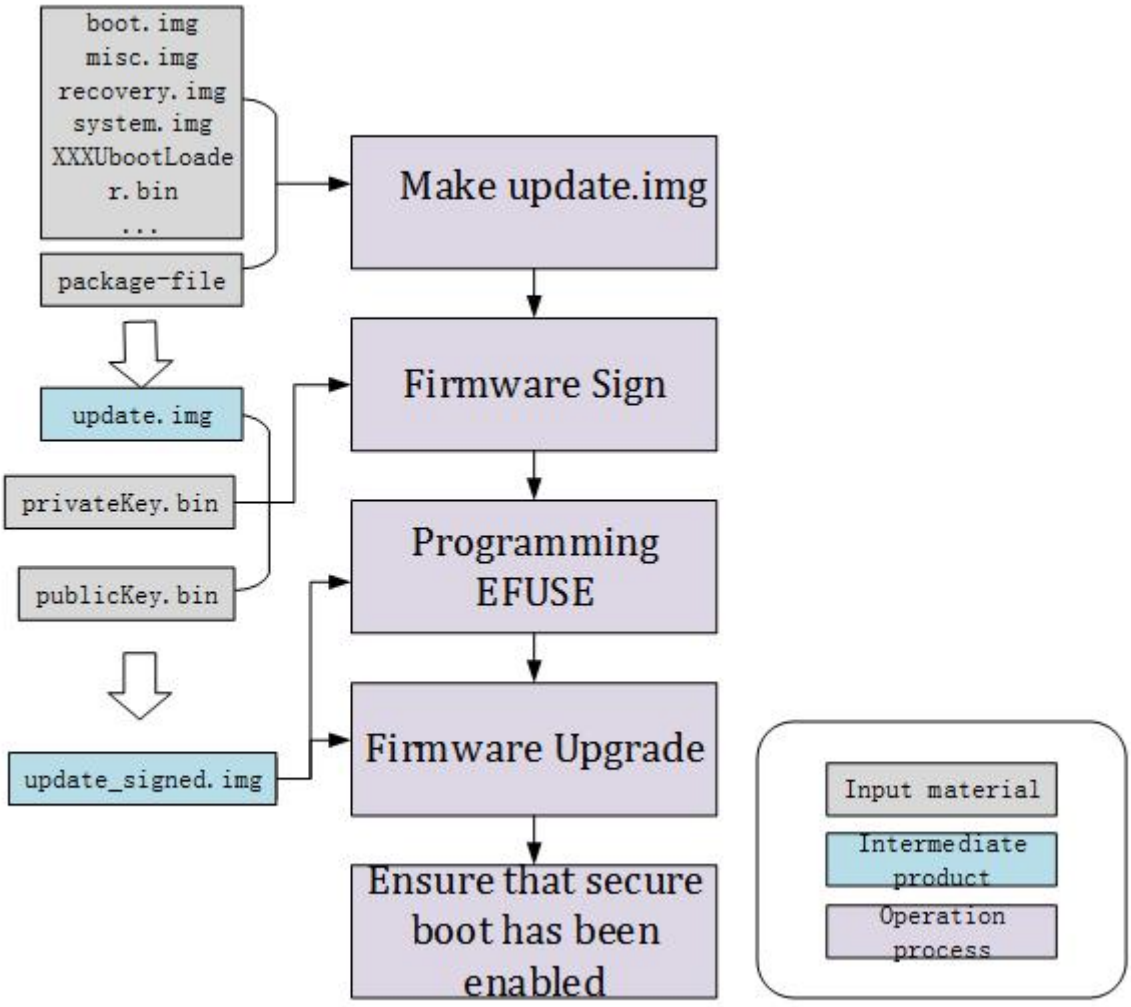


图 2-1 Rockchip Secure Boot 使用流程

详细请参考《Rockchip Secure Boot Application Note》文档中 4、5、6、7、8 章节中内容。

需要关注：

1. 若芯片平台只支持 efuse，需要确认机器硬件是否已支持 EFUSE 烧写，检查 efuse 供电等；
2. 若支持 OTP，目前是在签名固件烧写阶段自动烧写 OTP，无需额外 efuse 烧写步骤；
3. 若进行 OTA 包升级，在执行 make otapackage 生成对应 ota 包前，需要先对 u-boot 目录下编译生成的 loader、uboot、trust 镜像使用签名工具签名替换，否则升级会校验失败.

相关工具获取路径：**SDK 源码根目录下 RKTools 目录中获取。**

固件签名工具：**SecureBootTool**

工厂烧写工具：**FactoryTool**

Efuse 烧写工具：efuse_v1.xx.zip