RK3308 SecureBoot 开发工具指南

Version 1.0

2018/5/15

版本	日 期	描 述	作 者	审核
V1.0	2018-5-15	初始版本	王征增	

目录

1. 概述

该文档将介绍 RK3308 的安全启动功能。

安全启动功能旨在保护设备使用正确有效的固件，非签名固件或无效固件将无法启动。

2. 工具操作步骤

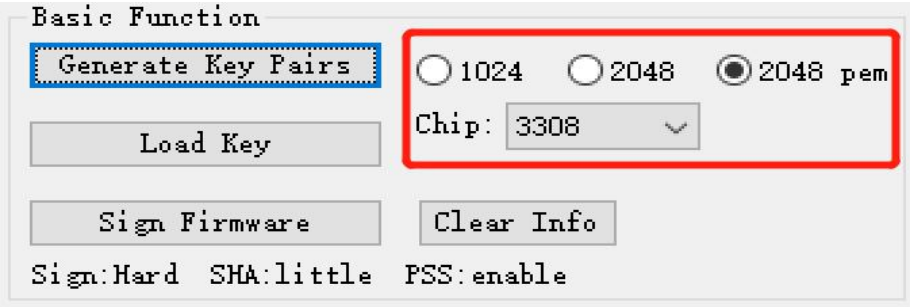
Windows 工具在工程根目录下 tools/windows/SecureBootTool_v1.89.zip

1. 修改配置：

   因为 RK3308 使用 OTP 存储公钥，修改工具根目录下的 config.ini 文件，将其中的 sign_flag=20。

2. 生成公私钥：

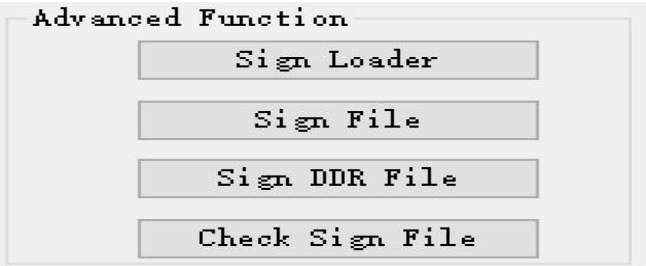
   选择 2048 pem 类型，chip->3308,点击 Generate Key Pairs，然后选择密钥的保存目录，生成 PrivteKey.pem 和 PublicKey.pem。（密钥随机生成，两次生成的密钥一定不同，所以请妥善保存这两个密钥，在安全功能启用后，如果丢失了这两个密钥，机子将无法刷机）



3. 签名：

   首先，我们需要载入密钥，选择 Load Key，根据提示，将公私钥载入。

   然后开始给固件签名，我们采用的是独立签名的方式，按 alt+ctrl+r+k 启用 Advanced function。



使用 Sign Loader，给 MiniloaderAll.bin 签名。

使用 Sign File 给 uboot.img 和 trust.img 签名。

3. 验证

1. 使用 AndroidTool(windows) 或 upgrade_tool(linux)下载分立固件。

   其中，第一次下载成功，重启后，loader 会自动将公钥写进 OTP 中，本次重启 SecureBoot 不启用。之后再次重启，OTP 中就有了公钥，SecureBoot 就会一直启用了。

2. 查看 log

```
107  GetParam
108  check parameter success
109  Unknow param: MACHINE_MODEL:rk3288!
110  Unknow param: MACHINE_ID:007!
111  Unknow param: MANUFACTURER:RK3288!
112  Unknow param: PWR_HLD: 0,0,A,0,1!
113  power key: bank-0 pin-5
114  can't find dts node for ricoh619
115  pmic:act8846
116  fg:cw201x
117  Secure Boot Mode: 0x1
118  SecureBootEn = 1, SecureBootLock = 1
119
```

   当 Uboot 中出现 SecureBootEn = 1, SecureBootLock=1，说明 SecureBoot 启用成功。

3. 使用未签名 loader

   SecureBoot 启用成功后，使用未签名 Loader 升级时，会出现 Loader 无法下载的情况。

4. 使用未签名 trust

   SecureBoot 启用成功后，使用未签名 trust.img，可以下载，但是固件起不来。

5. 使用未签名 uboot

   uSecureBoot 启用成功后，使用未签名 uboot.img，可以下载，但是固件起不来。