

## #SecureBoot签名工具用户手册

发布版本: 1.0

作者邮箱: [liuyji@rock-chips.com](mailto:liuyji@rock-chips.com)

日期: 2020-04-20

文档密级: 公开资料

---

### 前言

#### 概述

SecureBoot签名工具主要是对固件中的各级启动代码进行签名。

#### 支持芯片

3308|3326|3399|3328|3228h|3229|3368|3228|3288|3128|3126|3188|3036|1808|px30

#### 读者对象

本文档（本指南）主要适用于以下工程师：

技术人员

#### 修订记录

日期	版本	作者	修改说明
2020-04-20	V1.0	刘翊	初稿
2020-05-08	v1.1	刘翊	增加签名ddr测试文件签名

---

#### 1. 签名前的准备工作

- 1.1 了解芯片与Key的关系
- 1.2 签名方案与芯片的关系
- 1.3 生成rsa key pair
- 1.4 key格式相互转换

#### 2. 固件签名

- 2.1 签名update.img
- 2.2 签名loader
- 2.3 签名DDR测试文件

#### 3. 常见问题分析和处理

- 3.1 解包update.img问题
- 3.2 签名boot.img问题

#### 5. 工具日志

---

## 1. 签名前的准备工作

### 1.1 了解芯片与Key的关系

芯片	Key
3188/3036	1024
3228h/3368/3228/3288/3229/3128/3126	2048
3399/3328/3308/3326/1808/px30	2048 Pem(Openssl兼容)

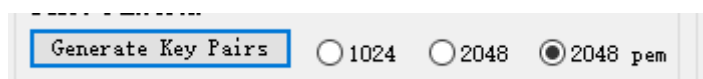
使用1024key的芯片内部没有加解密模块是采用软件进行计算，使用2048key的芯片内部是第一代加解密模块,使用2048 pem key的芯片是最新的加解密模块。

## 1.2 签名方案与芯片的关系

芯片	签名方案	安全级别
3228h/3368/3228/3288/3229/3128/3126	摘要:sha256 (big);签名:rsa 2048(不填充)	低
3399/3328	摘要:sha256;签名:rsa 2048(不填充)	中
3308/3326/1808/px30	摘要:sha256;签名:rsa 2048(Pss填充)	高

## 1.3 生成rsa key pair

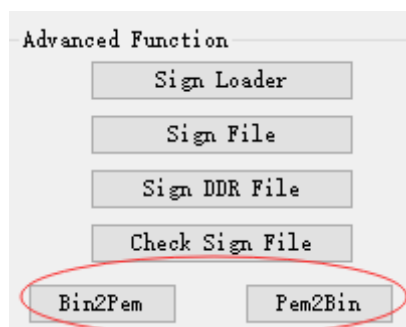
步骤1：选择key 类型,然后点击"Generate Key pairs"



## 1.4 key格式相互转换

secureboot签名工具支持两种格式的rsa key,一种是选择2048生成的bin格式key pair,另一种是选择2048 pem生成的pem格式的key pair,openssl工具可以直接使用。

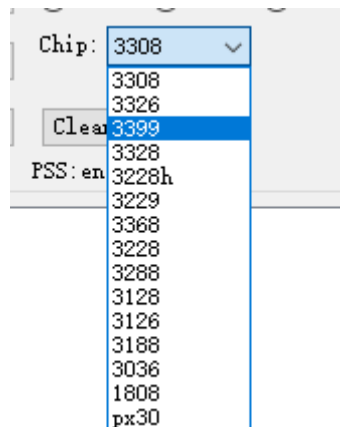
两种格式间的相互转换可以通过高级功能下的"Bin2Pem"和"Pem2Bin"来完成,激活高级功能通过按"Ctrl+RK"键



## 2. 固件签名

## 2.1 签名update.img

步骤1:选择芯片

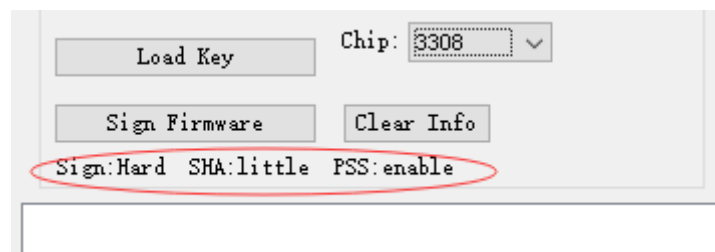


选择完芯片后会自动配置下面信息:

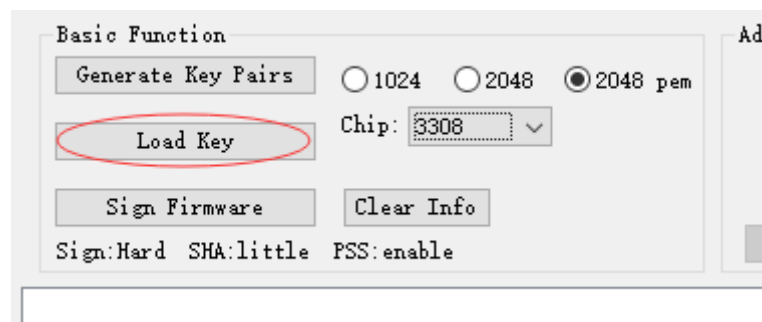
Sign:表示是硬件加解密还是软件, hard为硬件,soft为软件

SHA:表示采用的sha256摘要是大端还是小端,小端是标准sha256算法, 大端则需要先对明文进行4字节倒序后再云计算摘要

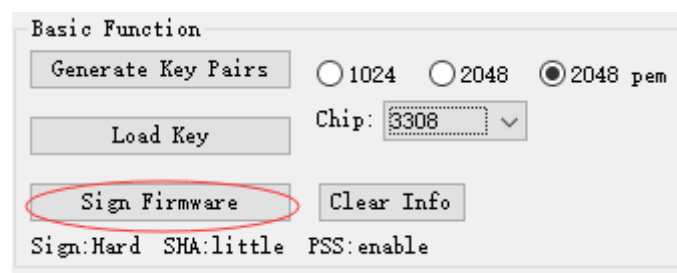
PSS:表示是否采用pss填充后再进行rsa 2048计算



步骤2:点击"Load Key"加载rsa key pair,先选择私钥再选择公钥



步骤3:点击"Sign Firmware",选择update.img后开始固件签名过程



## 2.2 签名loader

签名loader的步骤1,步骤2同上, 按"Ctrl+RK"键, 使能右边的高级功能, 点击"Sign Loader"



## 2.3 签名DDR测试文件

签名DDR的步骤1,步骤2同上, 按"Ctrl+RK"键, 使能右边的高级功能, 点击"Sign DDR File"



---

## 3. 常见问题分析和处理

### 3.1 解包update.img问题

问题:当碰到"No found firmware.img"或者"Unpack union firmware failed"

处理方法: 先检查update.img的头4个字节是不是RKFW, 如果多数原因是打包update.img的过程出问题, 请再确认打包过程是否有异常。

### 3.2 签名boot.img问题

问题:当碰到"sign boot.img failed"

处理方法: 先检查boot.img的头几个字节是不是ANDROID, 如果不是请在执行mk\_image.sh时带上ota参数, 因为secureboot的过程需要boot.img带上kernel代码

---

## 5. 工具日志

日志保存在工具的Log目录下, 名字为"Log日期.txt"格式, 如果碰到其他问题, 请将工具错误截图和当时的日志发给工程师分析。