No.18 Building, A District, No.89,
software Boulevard Fuzhou,Fujian, PRC
Tel: 0591-83991906-8006
Email:zyf@rock-chips.com

Rockchip Secure Boot Specification

Revision 1.1

2013/12/05

Revision History

Revision	Date	Description	Author
1.0	2012-5-24	初版.	ZYF
1.1	2013-12-05	增加 Lock 功能	ZYF

目录：

1. 基础信息

为满足 DRM 等应用需求，Rockchip 提供通用 Secure Boot 解决方案。

Rockchip Secure Boot 有以下特性：

1.1 使用 SHA1 做 HASH

1.2 使用 1024 bits 长度的 RSA KEY 做签名

1.3 存储和校验 RSA Public Key

1.4 自动根据固件是否签名来 Enable 和 Disable Secure Boot

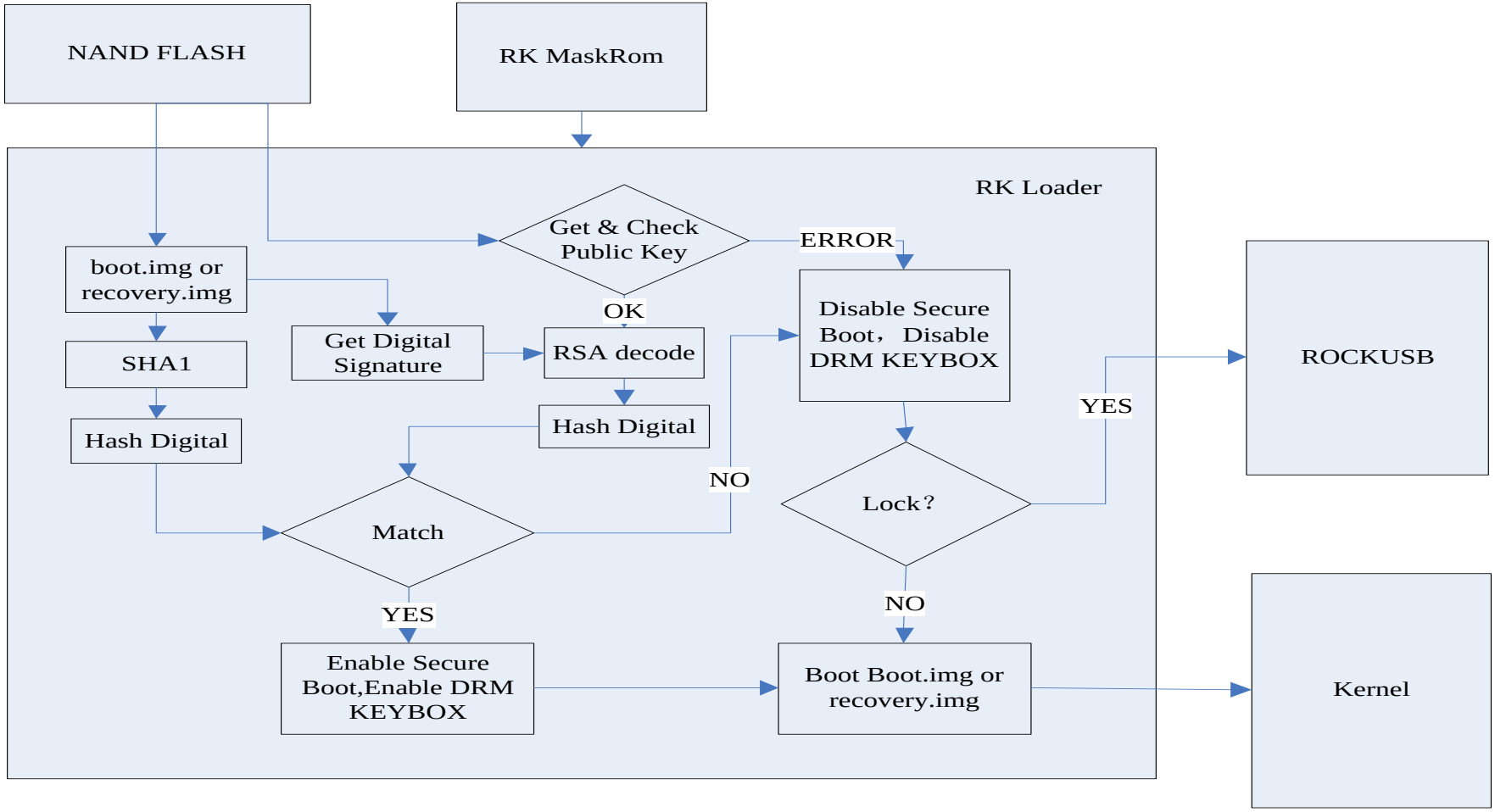
1.5 Secure Boot Disable 时会同步删除 DRM KEY 并禁用 DRM KEY BOX

1.6 在 Secure Boot Eanble 的情况下支持 Rockchip Loader Rockusb 升级模式

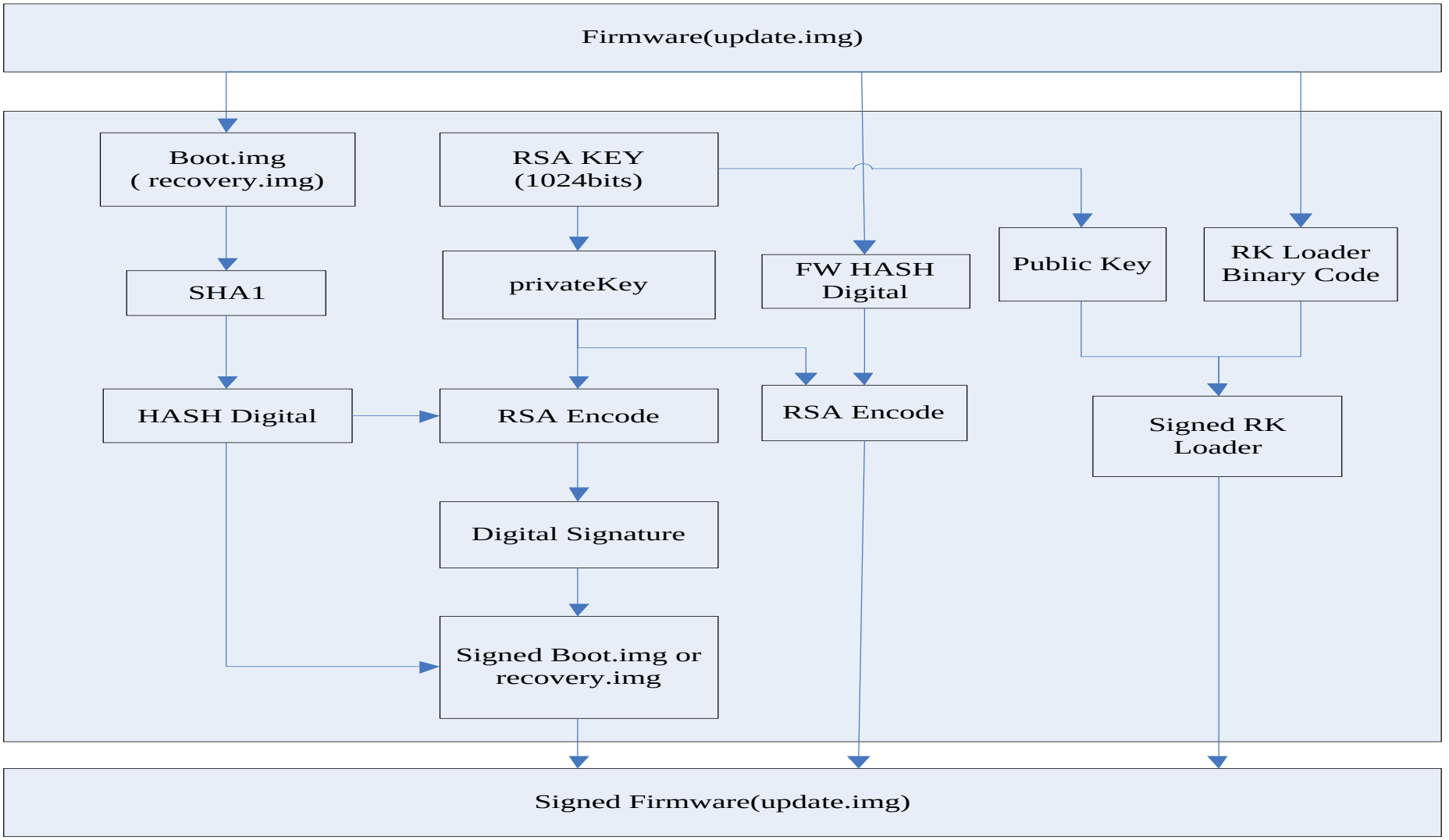
1.7 在 Lock 模式下，loader 升级模式只能升级匹配签名的固件，不能进行其他操作，比如更改 SN 序列号等。

2. 流程图

2.1 开机流程图



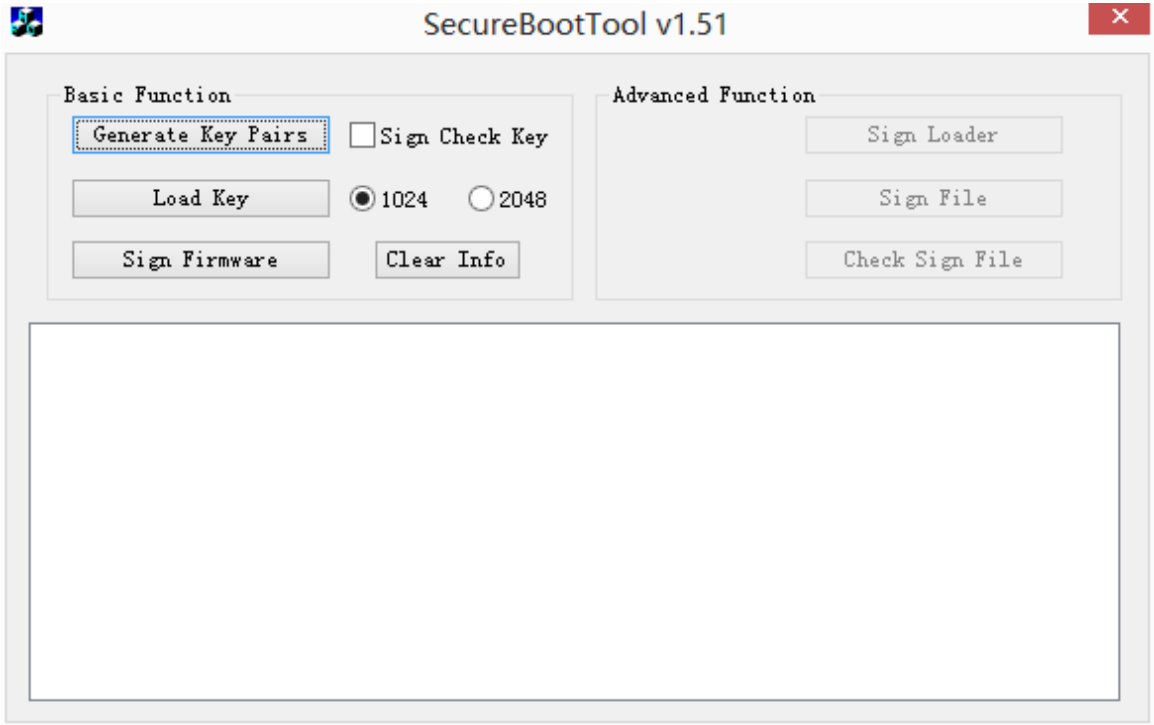
2.2 固件签名流程


Firmware(update.img)
Boot.img
(recovery.img)
RSA KEY
(1024bits)
SHA1
privateKey
FW HASH
Digital
Public Key
RK Loader
Binary Code
HASH Digital
RSA Encode
RSA Encode
Signed RK
Loader
Digital Signature
Signed Boot.img or
recovery.img
Signed Firmware(update.img)

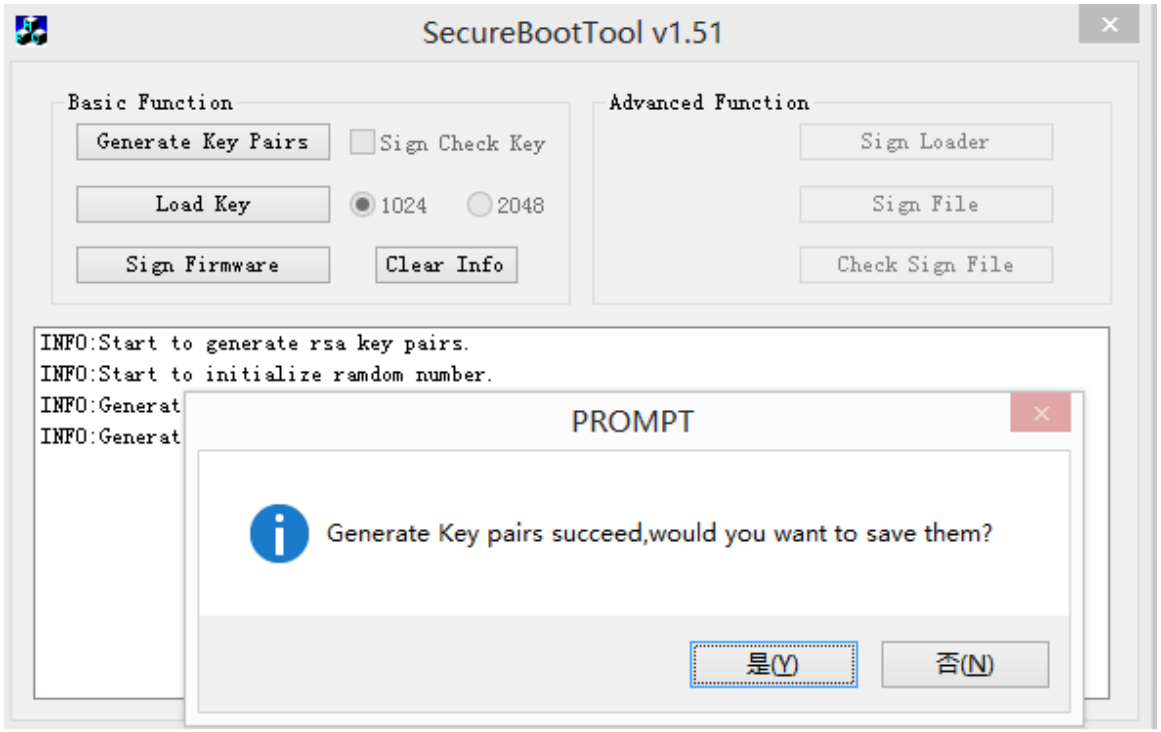
3. 固件签名

这个是 WIN 平台下的说明，LINUX 下的参考工具自带文档。

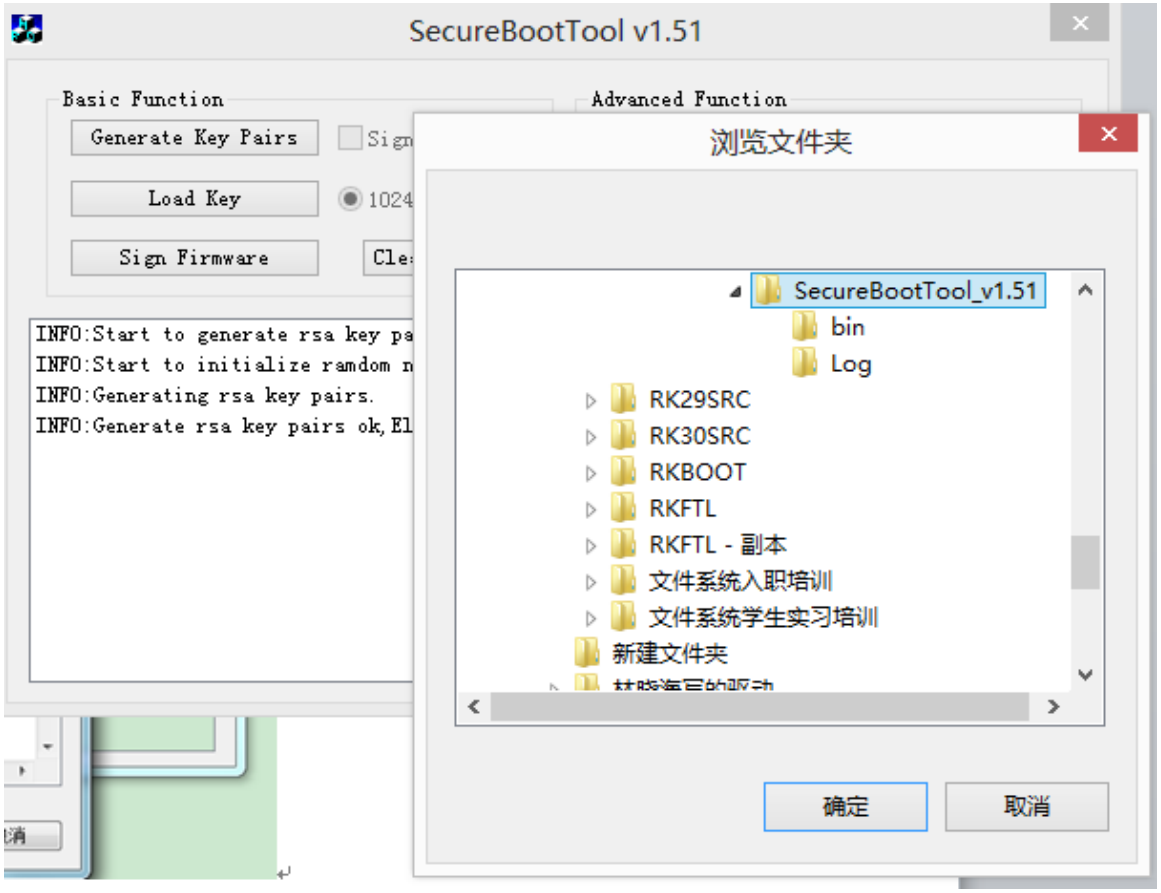
3.1 签名工具界面



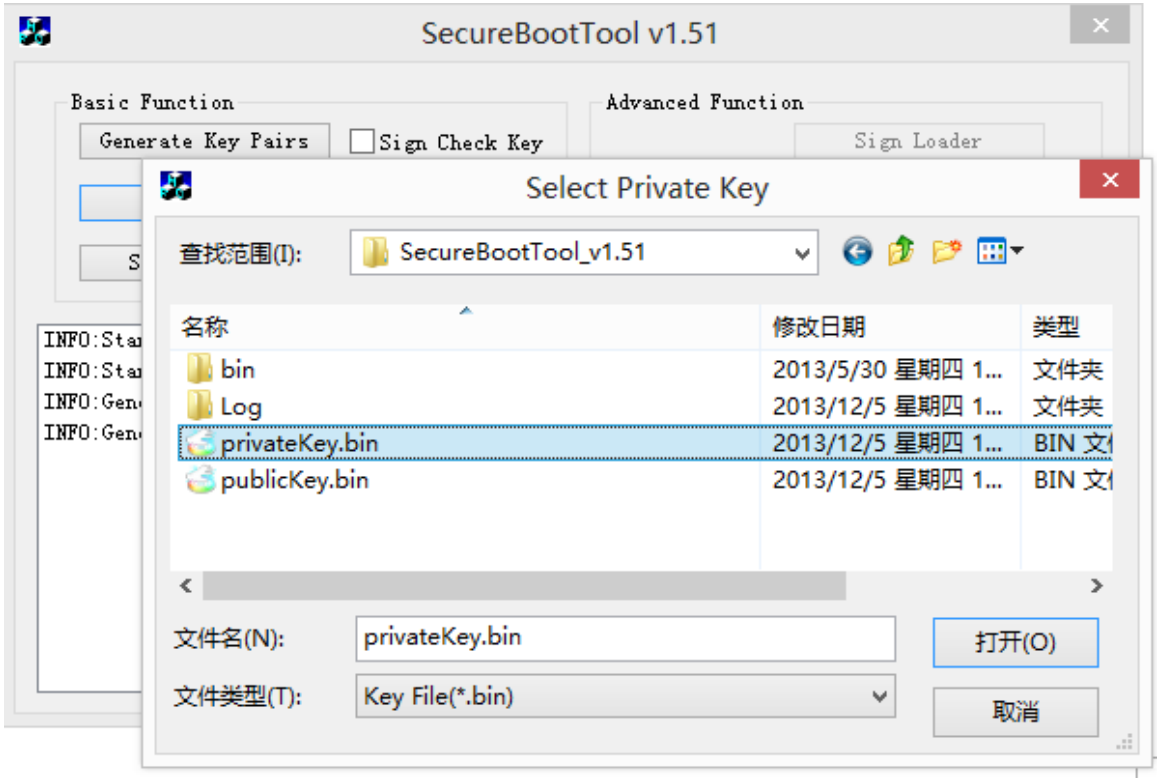
3.2 生成 RSA KEY，每款机器只生成一次。

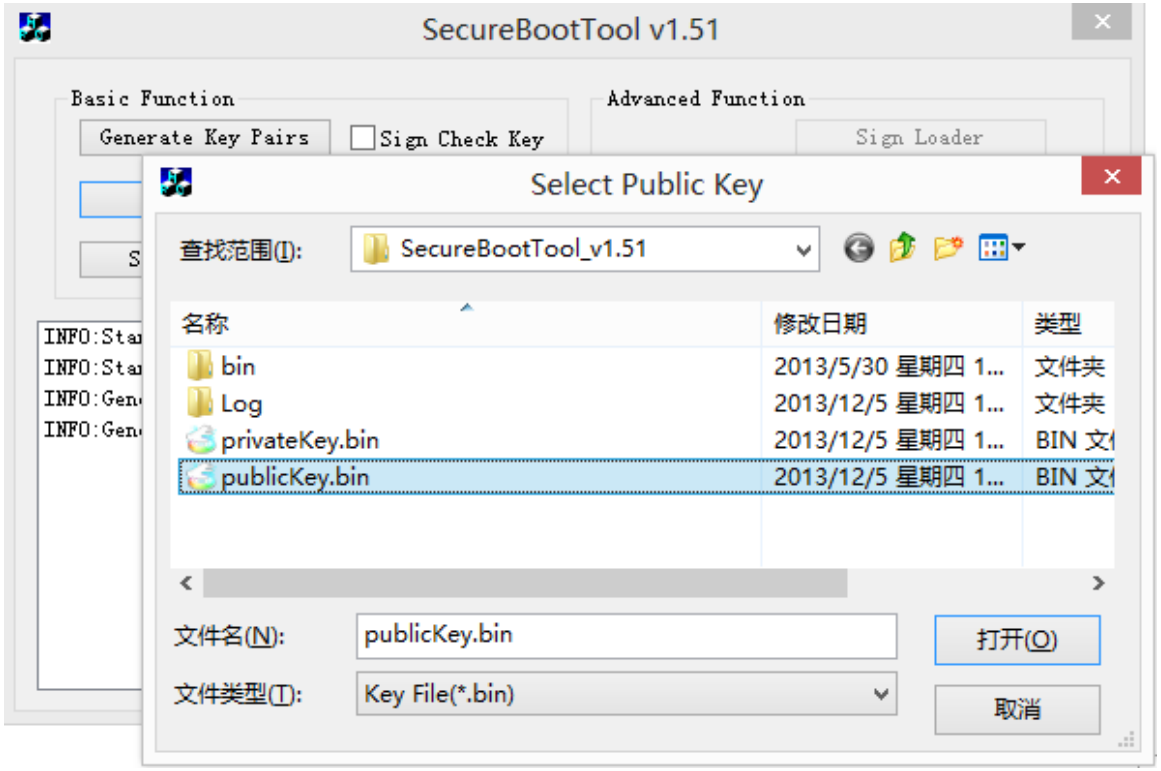


3.3 保存 RSA KEY，以后签名都只用这对 KEY。



3.4 加载 RSA KEY

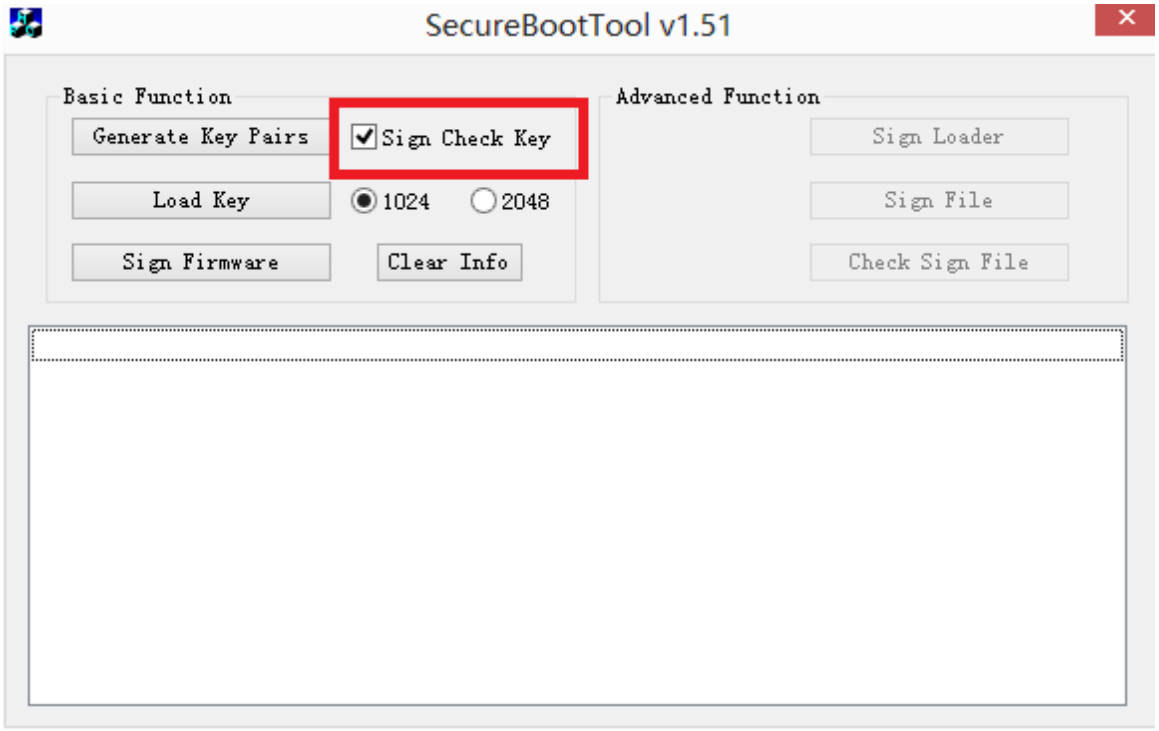

SecureBootTool v1.51
Basic Function
Generate Key Pairs
Sign Check Key
Advanced Function
Sign Loader
Select Private Key
查找范围(I):
SecureBootTool_v1.51
名称
修改日期
类型
bin
2013/5/30 星期四 1...
文件夹
Log
2013/12/5 星期四 1...
文件夹
privateKey.bin
2013/12/5 星期四 1...
publicKey.bin
2013/12/5 星期四 1...
文件名(N):
privateKey.bin
打开(O)
文件类型(T):
Key File(*.bin)
取消

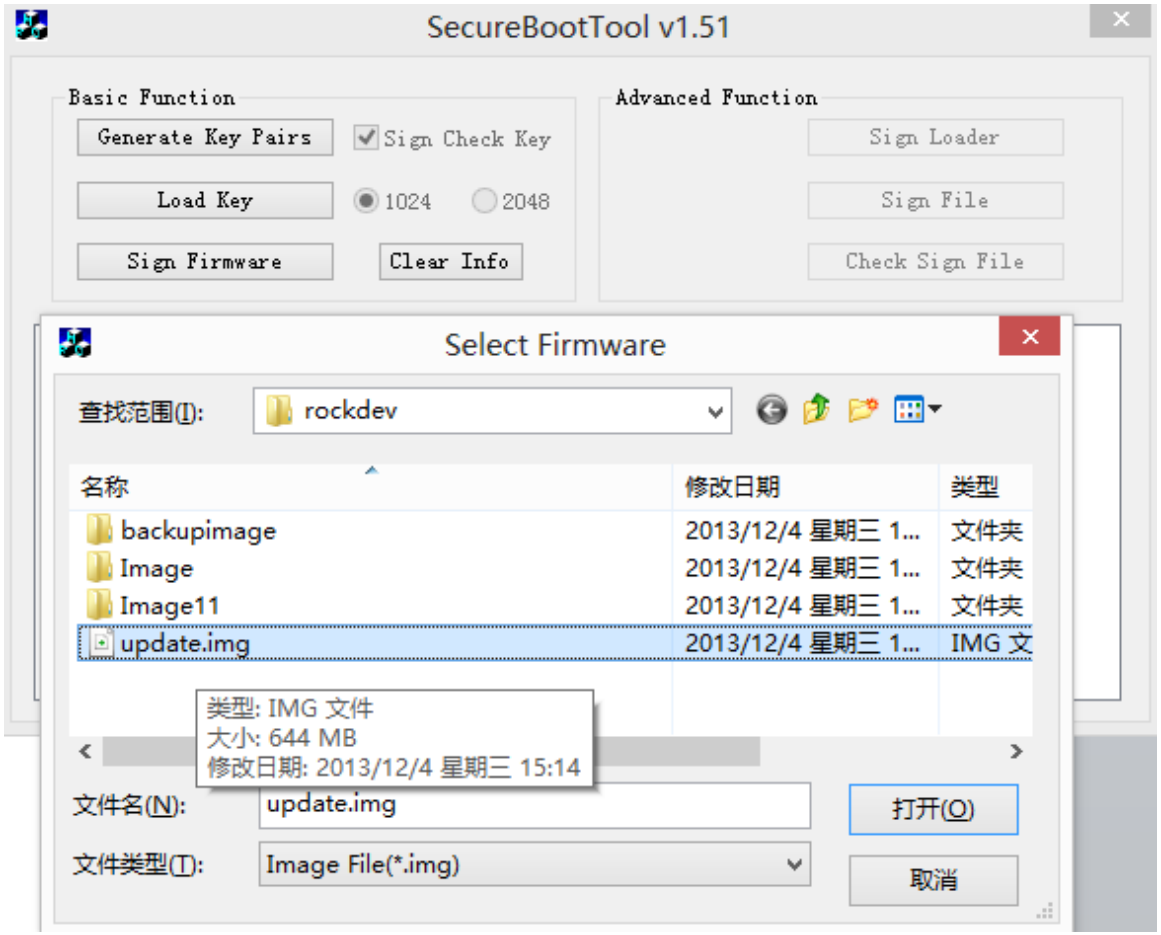

SecureBootTool v1.51
Basic Function
Generate Key Pairs
Sign Check Key
Advanced Function
Sign Loader
INFO:Star
INFO:Star
INFO:Gene
INFO:Gene
Select Public Key
查找范围(I):
SecureBootTool_v1.51
名称
修改日期
类型
bin
2013/5/30 星期四 1...
文件夹
Log
2013/12/5 星期四 1...
文件夹
privateKey.bin
2013/12/5 星期四 1...
BIN 文
publicKey.bin
2013/12/5 星期四 1...
BIN 文
文件名(N):
publicKey.bin
打开(O)
文件类型(T):
Key File(*.bin)
取消

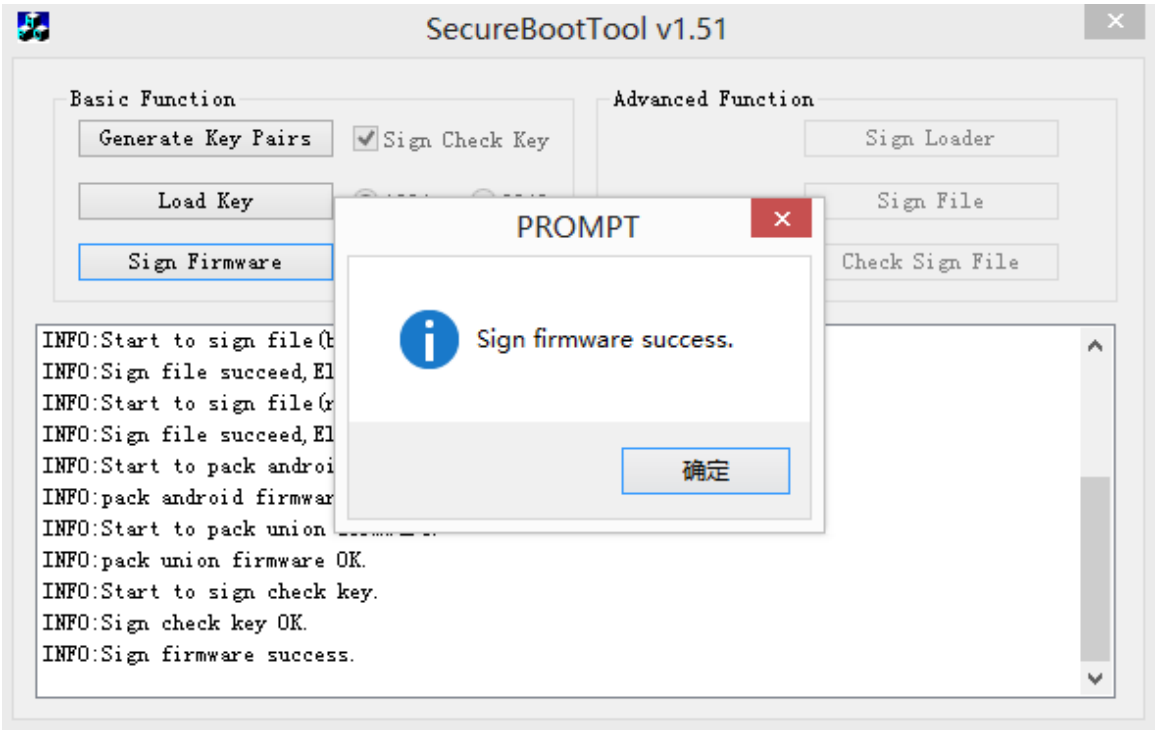
3.5 签名固件

固件要求 **boot.img** 和 **recovery.img** 都需要包含 **kernel**。

如果机器需要 **lock**，那么签名固件时需要选择 



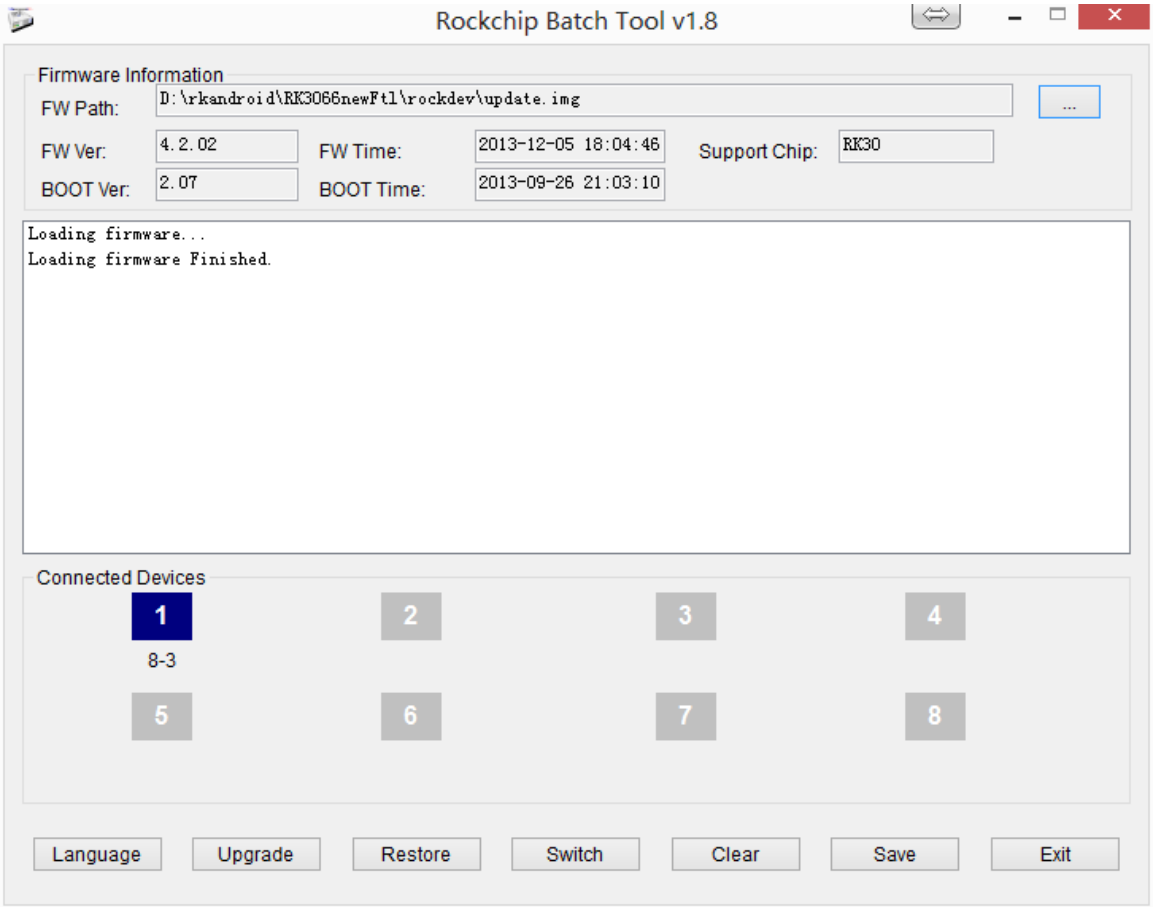

SecureBootTool v1.51
Basic Function
Generate Key Pairs
Sign Check Key
Load Key
1024
2048
Sign Firmware
Clear Info
Advanced Function
Sign Loader
Sign File
Check Sign File
Select Firmware
查找范围(I):
rockdev
名称
修改日期
类型
backupimage
2013/12/4 星期三 1...
文件夹
Image
2013/12/4 星期三 1...
文件夹
Image11
2013/12/4 星期三 1...
文件夹
update.img
2013/12/4 星期三 1...
IMG 文
类型: IMG 文件
大小: 644 MB
修改日期: 2013/12/4 星期三 15:14
文件名(N):
update.img
打开(O)
文件类型(T):
Image File(*.img)
取消


SecureBootTool v1.51
Basic Function
Generate Key Pairs
Sign Check Key
Load Key
Sign Firmware
Advanced Function
Sign Loader
Sign File
Check Sign File
PROMPT
Sign firmware success.
确定
INFO:Start to sign file(b
INFO:Sign file succeed, El
INFO:Start to sign file(r
INFO:Sign file succeed, El
INFO:Start to pack androi
INFO:pack android firmwar
INFO:Start to pack union
INFO:pack union firmware OK.
INFO:Start to sign check key.
INFO:Sign check key OK.
INFO:Sign firmware success.

4. 测试

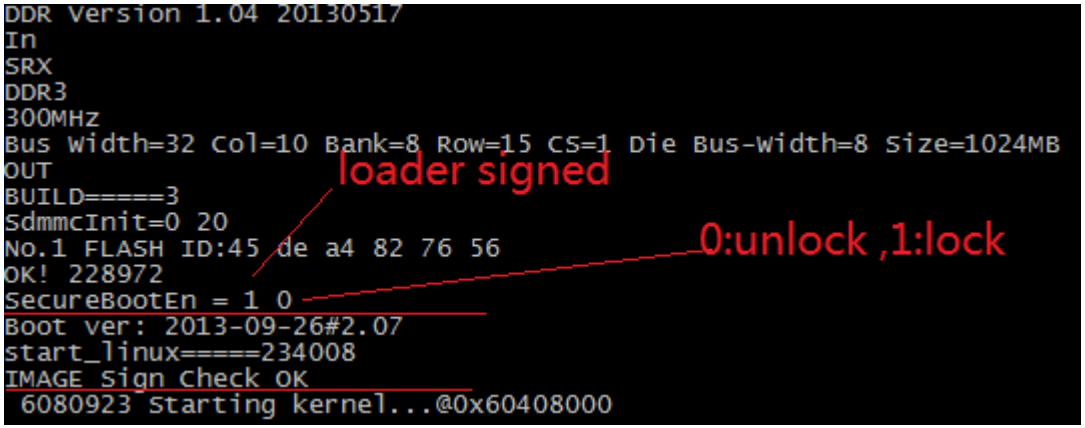
4.1 用最新的量产工具升级签名过的固件

已经 **lock** 的机器再次升级固件，量产工具需要 **1.8** 以上版本，第一次升级没有限制。

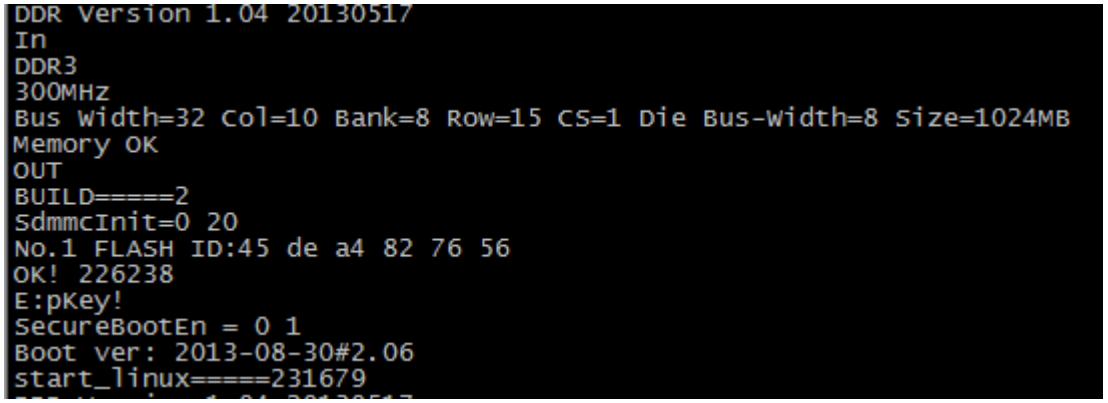


4.2 连接串口检查 secure boot 是否正常

4.2.1 签名正常，secure boot 引导正常



4.2.2 如果 public key 更新了，那么 log 就会打印“E:pkey!”



4.2.3 如果机器是 lock 的，public key 更新了或者固件没有签名，那么会打印出错，并进入 rockusb 升级模式：

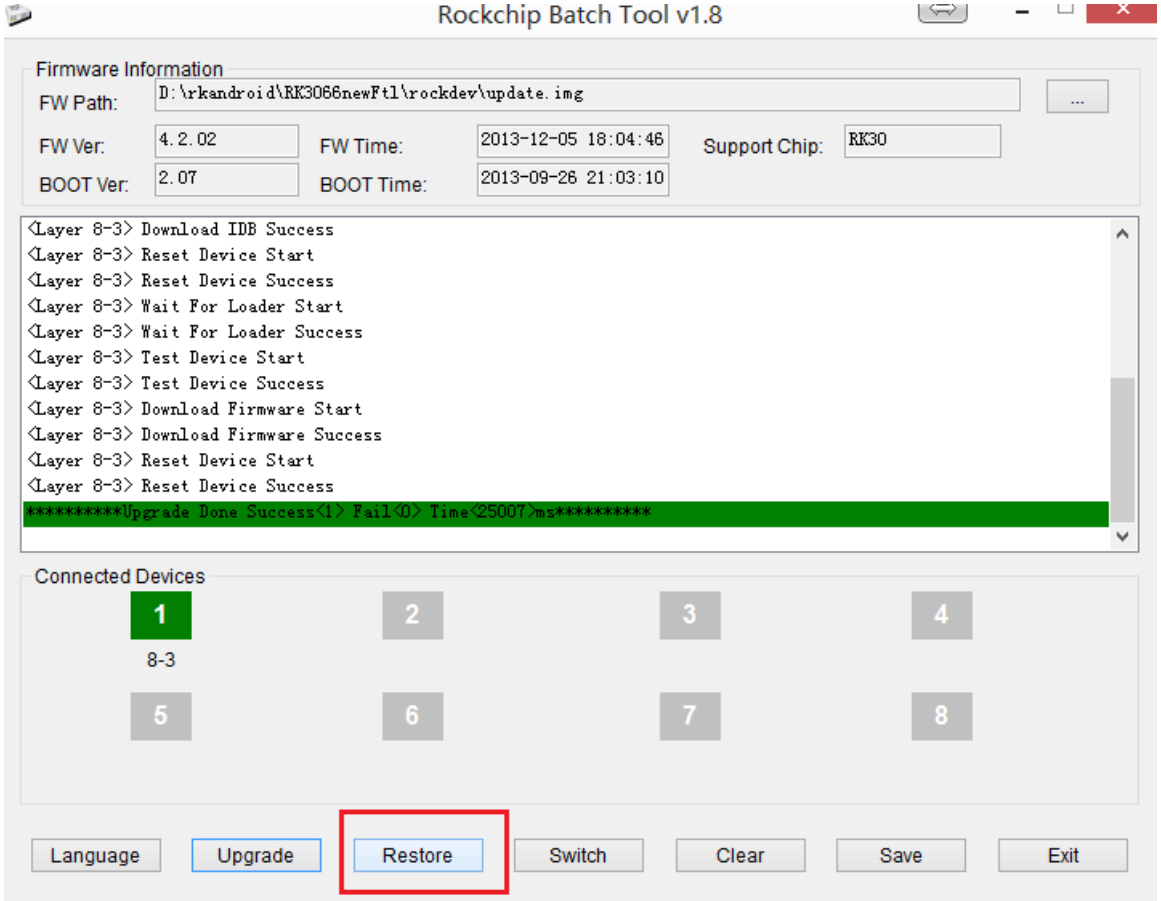
```
DDR Version 1.04 20130517
In
DDR3
300MHz
Bus Width=32 Col=10 Bank=8 Row=15 CS=1 Die Bus-Width=8 Size=1024MB
Memory OK
OUT
BUILD=====2
SdmmcInit=0 20
No.1 FLASH ID:45 de a4 82 76 56
OK! 226216
E:pKey!
SecureBootEn = 0 1
Boot ver: 2013-08-30#2.06
start_linux=====231657
FW unsigned!
Load failed!
FW unsigned!
Load failed!
UsbBoot 8145611
UsbHook ...8799515
powerOn 8799543
 8970237 UsbConnected
 9097166 UsbConnected
```

5. 常见问题处理

5.1 已经升级过不支持 secure boot 的旧机器怎么测试 secureboot？

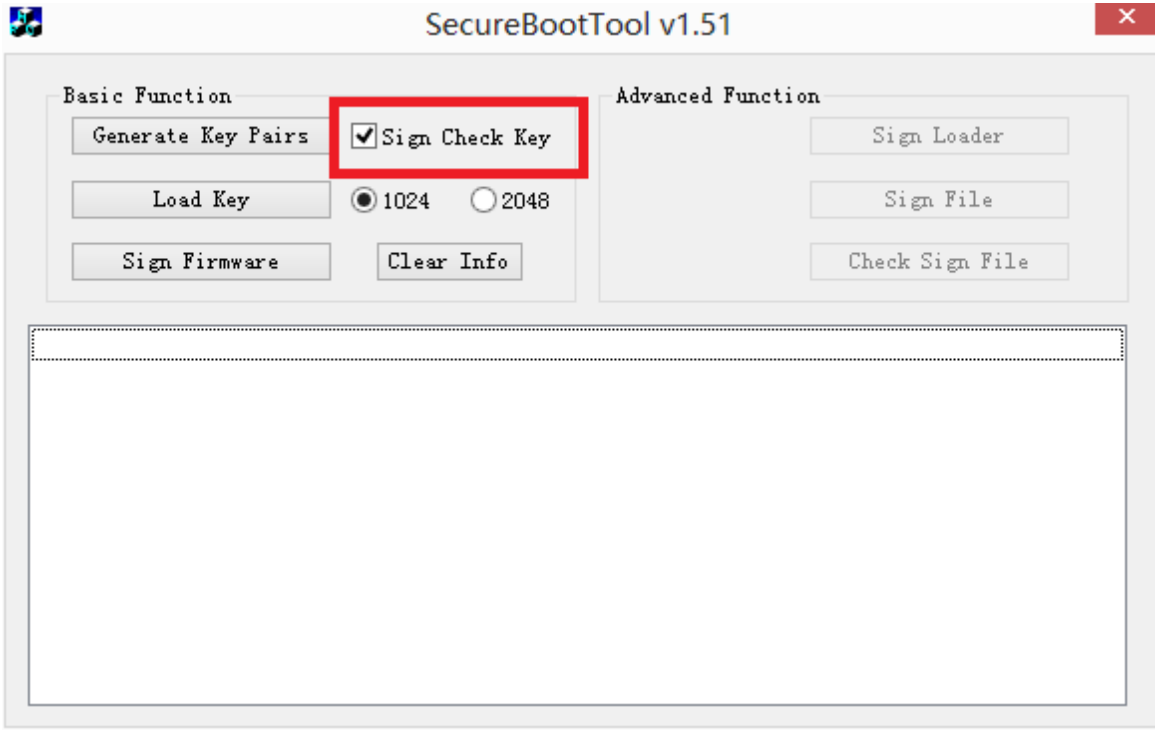
比较老的 loader 版本，不会打印“SecureBootEn”，不支持 secure boot 功能。

使用量产工具“**restore**”方式升级两次支持 **Secure Boot** 的固件即可。



5.2 已经 lock 的机器，签名的固件不能升级？

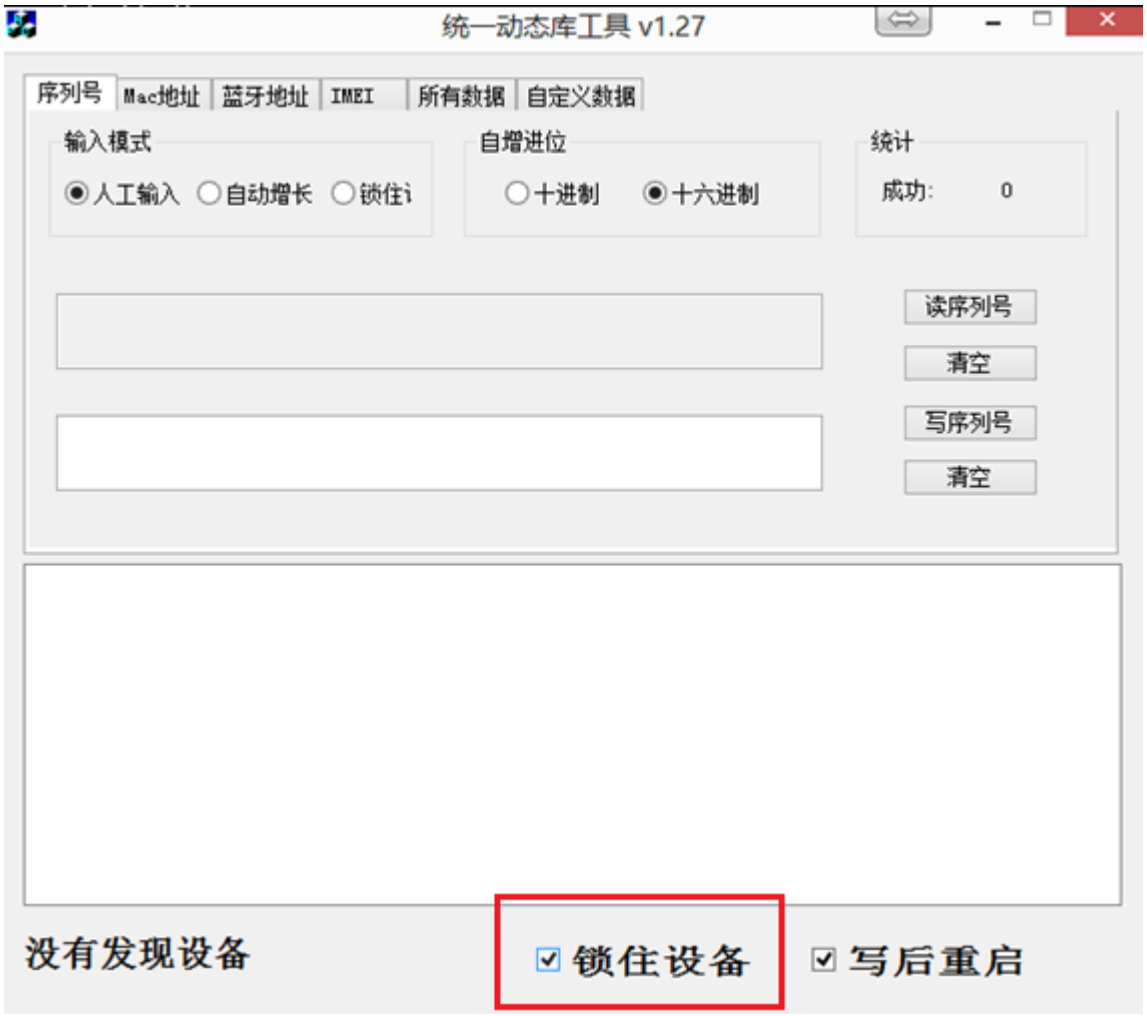
签名固件时没有选择 Sign Check Key 或者签名的的 RSA KEY 和机器第一次升级的 KEY 不一样。



5.3 怎么 lock 机器

1、选择带 lock 标记的 loader

2、使用 UpgradeDllTool 工具，写 SN 的同时 lock 机器



3、参考 nand 补丁包的 democode.c 中的代码，在 init（或者有 root 或者 system 权限的代码）里面 lock 机器

5.4 怎么 unlock 机器

参考 nand 补丁包的 democode.c 中的代码，在 init（或者有 root 或者 system 权限的代码）里面 unlock 机器