

ecurity Class: Top-Secret ( ) Secret ( ) Internal ( ) Public (  $\checkmark\,$  )

# **RK3399\_Efuse\_Operation\_Instructions**

(Technical Department, R & D Dept. II)

Status:	Version:	V1.00
[] Modifying	Author:	Wu Liangqing, Wei Jianxing
[] Released	Date:	2019-2-14
	Auditor:	
	Date:	

Fuzhou Rockchips Electronics Co., Ltd (All rights reserved)



## **Revision History**

Version no.	Author	Revision Date	Revision description	Remark
V1.00	Wu Liangqing,	2019-2-14	Initial version release	
	Wei Jianxing			



## Content

Pre	face	
1	Windov	vs tools signature step2
	1.1	Generate public keys and private keys2
	1.2	Signature firmware4
	1.3	Programme efuse7
	1.4	Burning signature firmware9
2	Linux t	ools signature step11
	2.1	Generate Key Pairs11
	2.2	Sign firmware11
	2.3	Sign loader
	2.4	Package update.img11
	2.5	Sign update.img md511
	2.6	RK3399 commands11
3	Make e	fuse ota update.zip12
4	Efuse p	oower up



## Preface

#### **Overview**

This document mainly describes Rockchip RK3399 efuse burning method and other related notices.

#### **Product version**

Chip name	Kernel version	Android version
RK3399	Linux4.4	

## Object

This document (guide) is mainly suitable for below engineers:

Field application engineers

Software development engineers



## 1 Windows tools signature step

## **1.1 Generate public keys and private keys**

1) Open tools "SecureBootTool v.1.85"

asic Functi	on		Advanced Func	tion
hip: <b>3125</b>	~	Generate Key Pairs		Sign Loader
norpyt:		Load Key		Sign File
0.6			1	and the second second second
LIATHEA	( roft	Sign Firmware		Check Sign File
() eruse	() soft	Sign Firmware	Clear Info	Check Sign File

2) Select chip: 3399

asic Function		Advanced Func	tion
hip: 3126	Generate Key Pairs		Sign Loader
3126 arrpy 3128	Load Key	1	Sign File
3228 0 ef 3288	Sign Firmware		Check Sign File
3328		Clear Info	
3399 others			



#### 3) Select "Encrpyt" type: efuse

	044		Advanced Func	tion
hip: 3399	~	Generate Key Pairs		Sign Loader
norpyt:	-	Load Key	1	Sign File
• efuse	Oroft	Sign Firmware		Check Sign File
Contraction of	0		Clear Info	

## 4) Select "Generate Key Pairs" to create key

				Sim Loadar
chip: 3399	~	Generate Key Fairs		pren manar
Incrpyt:		Load Key		Sign File
() ofneo	Oraft	Sign Firmware	I	Check Sign File
Gerase	Osore	organization de c	Clear Info	

5) Create successfully and save

lasic Function		Advanced Fun	otion
hip: 3399	Generate Key Pairs		Sign Loader
norpyt:	Load Key		Sign File
o.	0' P'		Check Sign File
PROMPT	Key pairs succeed,would you war	nt to save them?	×
PROMPT	Key pairs succeed,would you war 是(Y)	nt to save them? 否(N)	×
PROMPT	Key pairs succeed,would you war 是(Y)	nt to save them? 否(N)	×

#### 6) After saving the following key file

] privateKey.bin	2018/5/14 11:27	BIN 文件
publicKey.bin	2018/5/14 11:27	<b>BIN 文件</b>
The second secon		NAME AND ADDRESS OF

## 1.2 Signature firmware

Rockchip

瑞芯微申

1) Open tool SecureBootTool v.1.85, configure as create key

asio rancer			Advanced Func	
hip: 3399	~	Generate Key Pairs		Sign Loader
ncrpyt:		Load Key	1	Sign File
• efuse	Oraft	Sim Firmword		Check Sign File
the second se	1 1 N H L L			
):Start to g ):Start to i ):Generating ):Generate y	enerate rsa l nitialize ra g rsa key pair	vey pairs. ndom number. rs. ok Elenzed(3031)WS	Clear Info	



2) Click "Load Key" button to load key

Load Key		Sign File
Sign Firmware	Clear Info	Check Sign File
s. ok, Elapsed(3031)MS		
	Sign Firmware ey pairs. dom number. s. ok, Elapsed(3031)MS	Sign Firmware Clear Info ey pairs. dom number. s. ok, Elapsed(3031)MS

 Select the key files generated in the previous step, and the public and private keys need to be loaded twice.

-) - 🕈 📙 « RK33	99 > efuse > SecureBootToo	ol_v1.85 > out ∨	O 捜索"out"			م
iQ ▼ 新建文件夹						6
_ 此电脑	名称	修改日期	美型	大小		
3D 对象	privateKey.bin	2018/5/14 11:27	BIN 文件		2 KB	
△ WPS云文档	publicKey.bin	2018/5/14 11:27	BIN 文件		1 KB	
冒 视频						
副 圏片						
🔁 文档						
🕹 下載						
♪ 音乐						
重直 重面						
L OS (C:)						
🕳 本地磁盘 (D:)						
本地磁盘 (E:) v						
文件名(N	():		Key File(*.b	in)		~
				-	-	

 Click the "Sign Firmware" button to select the target firmware. For more details about the compilation and packaging of Firmware, please refer to section 2 of rockchip\_secure\_boot\_application\_note\_v1.2.1 \_20171128.pdf.



asic Function		Advanced Func	tion
hip: 3399 🗸	Generate Key Pairs		Sign Loader
Incrpyt:	Load Key	1	Sign File
●efuse ○soft	Sign Firmware		Check Sign File
O:Generating rsa key pai	irs.		

Rackchi

5) The firmware signing process takes about 10 minutes, and the signed firmware is under the out directory in the path where the tool is located, and its name is update\_signal.img

Basic Function		Advanced Func	tion
chip: 3399 ~	Generate Key Pairs		Sign Loader
Encrpyt:	Load Key	1	Sign File
●efuse ○soft	Sign Firmware		Check Sign File
Our Our			
70:Sign file succeed Elap: 70:Start to sign file(boo 70:Sign file succeed Elap: 70:Start to sign file(rec	sed(438)MS t. img). sed(391)MS overv.img)	Clear Info	
FO:Sign file succeed Elap: FO:Sign file succeed Elap: FO:Sign file succeed Elap: FO:Start to sign file(reco FO:Sign file succeed Elap: FO:Start to pack android i FO:pack android firmware ( FO:Start to pack union fir FO:pack union firmware (K	sed(438)MS t. ing). ted(391)MS overy. ing). sed(390)MS firmware. DK. rmware.	Clear Info	



×

## 1.3 Programme efuse

RK3399 board configuration: efuse power on, enter "masrom" mode

- EfuseI# v1.37 😽 8828 -> 🧼 🛯 🕸 总统 透出 固件质本: 面件: Loader 版本: 芯片信息: ID 失敗 设备列表 设备类型 1D 升级信息 1D 成功 🗅 👹 我的电脑 RootHub20 Port(1) Hub 3 + Port[1] - Port[2] + Port[3] + Port[4] + Port[5] ++ Port[6] + Port[2] RootHub20 Port[1] Hub 1 - Port[1] - Port[2] - Port[3] + Port[4] + Port[5] + Port[6] + Port[7] 友情提示: 00000 1. 第一次使用,标识USB端口方法,连接设备,工具显示设备后记录绑定ID,标识所有USB端口, 甫功: 2. 插入设备升级,要等到工具开始升级后两接入下一台。 00000 失败: 3.升级过程中,绿灯寒,接入设备,红灯寒,不要接插设备。 4. 升级结束, 病功以绿色背景显示, 失败以红色背景显示. 00000 总共: 5. 所有威功设备会在右侧表格中显示,所有失败设备会在左侧表格中显示,
- 1) Open tool: "Efuse 工具 v1.37"

2) Select the firmware signed in previous step



http://www.rock-chips.com/

14:	D件版本 Loader版本 芯片信息	] 固件版本 Loader版本 芯片信息							
ID 失敗	1.0	设备列表	设备类型	1D	升级信息		1D	iD 成功	Ţ
	e 👹	我的电脑				^			
	8	RootHub20							
		Port(1)	Hub	3		_			
		- Port[1]				- 11			
		Port[2]							
		Port[3]				- 11			
		- Portisi				_			
		Portifi				- 11			
		- Porti21							
	-	RootHub20							
	1.00	🗑 🎬 Port[1]	Hub	1					
		- Port[1]							
		- Port[2]							
		- Port[3]							
		+ Port[4]							
		-+++ Port[5]							
		+G Port[6]							
	- Cl.	Port[7]							
(情美示:									
1. 第一次使用, 标识USB端口方法; 连接设备, 工具整示设备后记录绑定ID, 标识所有USB端口,							成功:	00000	
2. 插入设备升级,要等到工具开始升级后两按入下一台。								1000000	
,升级讨程中,绿灯客,接)	设备, 红红寒,	不要接近设备。					失败:	00000	
and the state of the state of the state	E	and the second sec						20120324	

#### 3) After identifying the maskrom device, click start to write

214 V	/E40 Nefuse UK	refeotiool_vi. S5\out\update	sign ing		固件新本:6.0.0 Loader新本:1.1 芯片信息:RK330	11 09 IC		
ID 失敗	-	设备列表	设备类型	1D	升级信息	1D	成功	
		🕒 👹 我的电脑				^		
		B and RootHub20						
		Port[1]	Hub	3				
		- Port[1]			/			
		+ Port[2]						
		+ Port[3]		40	-	_		
		Port[4]	Maskrom	10		_		
		Port[5]				_		
		Port[2]						
		ReatHub30						
		ANR Port[1]	Hub	1				
		Port[1]	1.1.1.1			_		
		- Port[2]						
		- Port[3]						
		+ Port[4]				10		
		+ Port[5]						
		-++ Port[6]						
	×.	- +++ Port[7]				*		
****								
ALL DE ALL								
1. 第一次使用, 标识USB	捕口方法;	這接设备。工具显示设备后记录	绑定ID. 非识所有I	的演口。		雨和	ta: 000	PC应用:
2. 插入设备升级,要等3	[工具开始]	升级后再接入下一台。					223	
3. 升极过程中, 绿灯寒,	接入设备。	红灯亭, 不要接插设备,				失罪	g: 000	1
a Thenes III all the state	15 B m.=	计数目结合教育师学						
4.开始增速,所从现在	有意题不同	的现代证据非常现不可				94	± 000	



4) Burning successfully

	AUX DOMESTICS	Secondon (cd. r) (Souri optime			固件质本:6.0.01				
			Loader版本 1.09 芯片信息:RK330C	Loader版本:1.09 芯片信息:BX330C					
D	失敗	设备列表	设备类型	ID	升级信息		1D	成功	
	0.68602	🕞 👹 我的电脑				^	16	0.4	
		B RootHub20							
		Port(1)	Hub	3					
		- Port[1]							
		- Port[2]				- 11			
			Maskrom	16	華人成功				
		Port[5]				- 11			
		Port[6]				- 11			
		- Port[2]				- 11			
		RootHub20				- 11			
		Port[1]	Hub	1		- 11			
		Port[1]				- 11			
		- Port[2]				- 11			
		Port[3]				- 84			
		Port[4]				- 11			
		Port[5]				- 1			
		Port[0]							
		rout/				23			
情拠示:									
第二次中国:	地位的建立方法	- 注論込み 丁目県の込み后辺型(	ander in the second second	residers.			威功	00001	
and the state			PERSONAL PROPERTY IN CONTRACTOR OF CONTRACTO	NAME OF COLUMN			10.00		
插入设备升印	81、卖寺到工具升	雅井驳局再接入下一台。					a. 90	00005	
升级过程中,	绿灯亮。接入设计	h, 红灯亮, 不要披插设备,					1000	00000	
Then extended the set	******	子 计数时结束联系统学						00000	

## 1.4 Burning signature firmware

- TTIH v1.52 х ۲ 圆件 0.94 〇位度 10 透出 -团件质本 面件 Loader 版本: Depo 芯片信息; 设备列表 设备类型 1D 升级信息 成功 ID 失敗 ID 👹 我的电脑 RootHub20 Port(1) Hub 3 Port[1]
  Port[2]
  Port[3]
  Port[4] Maskrom 16 + Port[5] + Port[6] - Port[2] RootHub20 Port[1] Hub 1 - Port[1] Port[2]
  Port[3] Port[4]
  Port[5] + Port[6] + Port[7] 友情视示: 00000 甫功: 1. 第一次使用,标识USD端口方法:连接设备,工具显示设备后记录绑定ID. 标识所有USD端口. 2. 插入设备升级,要等到工具开始升级后再接入下一台。 00000 失败: 3.升级过程中,绿灯亮,接入设备,红灯亮,不要极适设备。 4. 升级结束, 病功以绿色背景显示, 失败以红色背景显示. 00000 9.# 5. 所有威功设备会在右侧表格中显示,所有失败设备会在左侧表格中显示,
- 1) Open tool: "FactoryTool\_v1.63"



Alt <sup>2</sup>						因件版本 Loader版本 芯片信息			
ID 失敗	-		设备列表	设备类型	ID	升级信息		ID	成功
		ء 👹 😑	幼的电脑				^		
	B St RootHub20								
		6	Port(1)	Hub	3		_		
			- Port[1]				_		
		-	- Port[2]				_		
		-	-+++ Port[3]				-		
			Port[4]	Maskrom	16		_		
			+++ Port[5]				- 11		
			Port[0]				- 11		
			Port[2]				_		
		10-2	KDOTHUD2U	14.6			_		
		-	Port[1]	PND			_		
		-	Port[7]				_		
		-	Port[2]				- 11		
		-	Port[4]				- 10		
			Port[5]				_		
		-	+ Portifi						
	- 9		- Port[7]				*		
**=									
11 (K) (P) (								100	
·第一次使用,标识USI	捕口方法	连接设备	,工具显示设备后记录	限绑定ID。将织所有I	DSDMAD.			盾功:	00000
插入设备升级,要等	加工具开始	升级后两	接入下一台。						
升级讨留中, 绿竹室	接入设备	4T 1T 18. 3	不算损损损益。					失败:	00000
al location and a second second	In Proc Ma	ALL ALL PROPERTY							
, 升砚结束, 病劝以躁)	的有景觀不	5. 失戦以1	1他有景观示。					여부	00000

## 2) Select the firmware signed in previous step

#### 3) Start to download

(\$. (\$ <b>M.D.T.M.1902)</b> Dato	durel Second col pri 1950 ad la galate			Loader版本: 1.09 芯片信息: BK330C				
ID 失敗	2 设备列表	化物质型	ID	升级信息	*			
	E ScotHub20							
	Port[1]	Hub	3					
	Port[1]				- 11			
	Port[2]							
	Portial	Loader	16	正在下数图体(2%)。				
	- Porti5i	coust		at the Processing Project open				
	- Port[6]							
	- Port[2]							
	B M RootHub20							
	👜 🏧 Port[1]	Hub	1					
	- Port[1]							
	- Port[2]							
	-49 Port[3]							
	- Port[4]							
	-+++ Port[5]							
	- +++ Port[6]							
	Port[7]				×1			
情後示:								
第一次使用,标识USB排	口方法:连接设备,工具显示设备后记录	·抑定ID. 存识所有	USDimical			成功:	00000	
插入设备升级,要等到3	[具开始升级后两接入下一台。							Po
升级过程中,绿灯车 接	λ设备,打打家,不算极适设备					失败:	00004	
the second se	A NAME OF TAXABLE STATES AND ADDRESS OF TAXABLE ADDRESS OF TAX							



## 2 Linux tools signature step

#### 2.1 Generate Key Pairs

SecureBootConsole -k|-kk SaveKeyDir //generate key -k(1024) -kk(2048)

#### 2.2 Sign firmware

trust.img uboot.img recovery.img boot.img

SecureBootConsole -si privatekey \_path image\_path

#### 2.3 Sign loader

//SignEx Loader (efuse 2048)

SecureBootConsole -slx privatekey\_path publickey \_pathl oader\_path

#### 2.4 Package update.img

Package the signed images such as Loader, trust.img, uboot.img, recovery.img and boot.img into update.img.

#### 2.5 Sign update.img md5

SecureBootConsole -sh privateKey \_path firmware\_path

#### 2.6 RK3399 commands

SecureBootConsole -kk SaveKeyDir

sudo ./SecureBootConsole -slx privateKey.bin publicKey.bin

Image/MiniLoaderAll.bin

sudo ./SecureBootConsole -si privateKey.bin Image/recovery.img

sudo ./SecureBootConsole -si privateKey.bin Image/boot.img



sudo ./SecureBootConsole -si privateKey.bin Image/trust.img

sudo ./SecureBootConsole -si privateKey.bin Image/uboot.img

./mkupdate.sh

sudo ./SecureBootConsole -sh privateKey.bin update.img

## 3 Make efuse ota update.zip

1) Make sure build/tools/ has "drmsigntool" sign tool, if it is already existing, no need

to add manually.





2) Copy key to build/target/product/security/

Need to sign loader, uboot and trust before making ota package and then put it into

SDK project to replace the original file.

3) Make ota package as normal

## 4 Efuse power up

1) Use the power supply method of reference design, as shown in below picture:



The above circuit is designed in the test fixture (recommend to use the LDO with voltage adjustable, then you can increase the LDO voltage in case there is voltage reduction on probe) to save cost. When flashing EFUSE, RK3399 (GPIO4\_D3) EFUSE\_VQPS\_EN\_H will output high to enable LDO to supply power for EFUSE\_VQPS. 2) Directly use the DC regulated power supply to supply power for EFUSE\_VQPS:



The two test points shown in above picture are designed in the main board. Directly



use the DC regulated power supply to supply 1.8V for the test fixture. Make sure the main board enters masrom, then supply 1.8V for EFUSE\_VQPS, and finally flash EFUSE.