密级状态： 绝密(　　) 秘密(　　) 内部资料(　　) 公开(√)

Security Class: Top-Secret (　　) Secret (　　) Internal (　　) Public (√)

Android 验证启动功能说明

Android_Verify_Boot_Function_Introduction

（第二系统产品部）

(Technical Department, R & D Dept. II）

文件状态： **Status:** [　] 草稿 [　] Draft [　] 正在修改 [　] Modifying [√] 正式发布 [√] Released	**文件标识：** **File No.:**	RK-SM-YF-205
	当前版本： **Current Version：**	V1.1
	作　　者： **Author:**	吴惊晨 Wu Jingchen
	完成日期： **Finish Date:**	2019-11-16
	审　　核： **Auditor:**	卞金晨 Bian Jinchen
	审核日期： **Finish Date:**	2019-11-16

福州瑞芯微电子股份有限公司

Fuzhou Rockchip Electronics Co., Ltd.

免责声明

本文档按“现状”提供，福州瑞芯微电子股份有限公司（“本公司”，下同）不对本文档的任何陈述、信息和内容的准确性、可靠性、完整性、适销性、特定目的性和非侵权性提供任何明示或暗示的声明或保证。本文档仅作为使用指导的参考。

由于产品版本升级或其他原因，本文档将可能在未经任何通知的情况下，不定期进行更新或修改。

Disclaimer

This document is provided “as is” and Fuzhou Rockchip Electronics Co. Ltd (“the company”) makes no express or implied statement or warranty as to the accuracy, reliability, completeness, merchantability, specific purpose and non-infringement of any statement, information and contents of the document. This document is for reference only.

This document may be updated without any notification due to product version upgrades or other reasons.

商标声明

“Rockchip”、“瑞芯微”、“瑞芯”均为本公司的注册商标，归本公司所有。

本文档可能提及的其他所有注册商标或商标，由其各自拥有者所有。

Brand Statement

Rockchip, Rockchip™ icon, Rockchip and other Rockchip trademarks are trademarks of Fuzhou Rockchip Electronics Co., Ltd., and are owned by Fuzhou Rockchip Electronics Co., Ltd.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

福州瑞芯微电子股份有限公司

Fuzhou Rockchip Electronics Co., Ltd.

地址： 福建省福州市铜盘路软件园 A 区 18 号

网址： www.rock-chips.com

客户服务电话： +86-4007-700-590

客户服务传真： +86-591-83951833

客户服务邮箱： fae@rock-chips.com

Fuzhou Rockchip Electronics Co., Ltd.

Address: No. 18 Building, A District, No.89,software Boulevard Fuzhou,Fujian,PRC
Website: www.rock-chips.com
Customer service tel.: +86-4007-700-590
Customer service fax: +86-591-83951833
Customer service e-mail: fae@rock-chips.com

版 本 历 史 Revision History

版本号 Version no.	作者 Author	修改日期 Revision Date	修改说明 Revision description	备注 Remark
v1.0	吴惊晨 Wu Jingchen	2018.11.12	创建初始版本 Initial version release	适用 8.1 及以上版本 Suitable for 8.1 and higher versions
v1.1	吴惊晨 Wu Jingchen	2019.11.16	Q 版本更新 Updated for Android Q	

目 录 Contents

1 概述 Overview

本文档对如何进行定制 Android 的 verity-boot 功能做详细的说明，用于支持固件的验证启动功能，**默认开启**。如果启用此功能，在刷写未进行哈希树签名运算的系统镜像或被篡改过的系统镜像时，系统会重启到 fastboot，不允许继续挂载和启动 Android 系统。

This document describes how to customize Android verity-boot function in details, which is used to support image verify boot function and **enabled by default**. If this function is enabled, when flashing the system mirror not signed by hash tree algorithm or tampered, the system will reboot to fastboot, and fail to continue loading and starting Android system.

主要用于系统调试，或进行 VTS 认证，烧写谷歌 AOSP 的 system 镜像时，关闭 verity-boot 后，GSI 固件方可正常启动。

It is mainly used for system debugging, or VTS certificate. When flashing Google AOSP system mirror, GSI image can boot up normally only after verity-boot is disabled.

verity-boot 1.0 加解锁方式：通过使用**瑞芯微写号工具**可以进行加解锁。

The lock/unlock method of verity-boot 1.0: use **Rockchip WriteSN tool** can lock/unlock.

verity-boot 2.0 加解锁方式：通过使用 fastboot 解锁。

The lock/unlock method of verity-boot 2.0: use fastboot to unlock.

快速使用只需参看 ---> 2 快速使用方法

Please refer to chapter 2 for quick usage.

2 快速使用方法开启与关闭 Quick enable and disable

2.1 判断verity-boot 版本号 Judge verity-boot version number

进入 adb shell 模式 getprop | grep avb

Enter adb shell mode getprop | grep avb

如果有[ro.boot.avb_version]则代表是 verity-boot 2.0，请查看 2.3 小节；

If there is [ro.boot.avb_version], it is verity-boot 2.0. Please refer to chapter 2.3.

否则为 verity-boot 1.0，请查看 2.2 小节。

Otherwise it is verity-boot 1.0, please refer to chapter 2.2.

2.2 verity-boot 1.0 加解锁方式 Lock/unlock method of verity-boot 1.0

在 Android 中默认开启了验证启动，如果需要调试或进行 VTS 认证时需要解锁，需要进行如下操作：

Android enables verity-boot by default. If need to debug or do VTS certificate, need to unlock it through the following steps:

1、重启设备进入 bootloader 模式；

Reboot the device to enter bootloader mode.

2、以文本编辑工具打开写号工具的安装目录（例如：D:\Program Files (x86)\瑞芯微电子\写号工具 ）中的 config.ini，**更改 OEMUNLOCK=0 为 OEMUNLOCK=1**，并保存配置文件，如图 1：

Use txt editing tool to open config.ini in the install directory of the WriteSN tool (such as: D:\Program Files (x86)\瑞芯微电子\写号工具), modify **OEMUNLOCK=0 to OEMUNLOCK=1**, and save the configuration file, shown as picture 1:

图 1：更改配置文件示例

Picture 1: Modify the configuration file

3、打开写号工具，点击写入，下方会显示是否成功写入，如图 2：

Open the WriteSN tool, click Write, and it will display whether write successfully in the bottom, shown as picture 2:

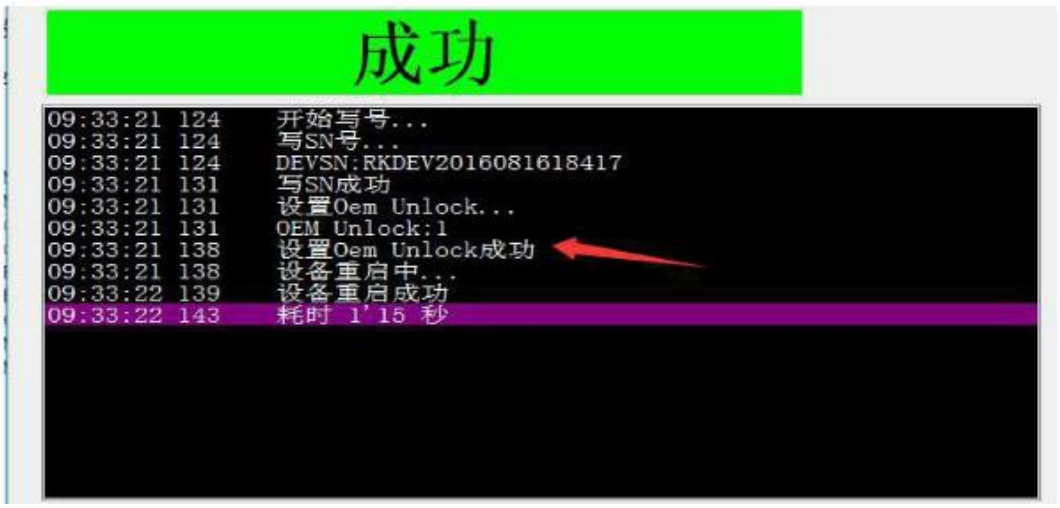

图 2：写入成功

Picture 2: Write successfully

4、如需重新锁定，请设置 config.ini 文件中的值为 0，保存该文件后重新打开写号工具进行写入。

If need to lock again, please set the value in the config.ini file as 0, save the file and reopen the WriteSN tool to write.

2.3 verity-boot 1.1 加解锁方式 Lock/unlock method of verity-boot 1.1

1：adb reboot fastboot 进入 fastboot 模式（Q 版本用 adb reboot bootloader）

adb reboot fastboot to enter fastboot mode (use adb reboot bootloader for Android Q).

2：输入 fastboot oem at-unlock-vboot 解锁机器

Input fastboot oem at-unlock-vboot to unlock the device.

3：fastboot reboot 重启机器

fastboot reboot to reboot the device.

注：可以用 fastboot oem at-lock-vboot 命令锁住机器

Note: you can use fastboot oem at-lock-vboot command to lock the device.

2.4 烧写 GSI 方式 Method of flashing GSI

1：verity-boot 1.0 烧写 Google 的 GSI 的 system.img

For verity-boot 1.0, flash system.img of Google GSI

2：verity-boot 1.1 烧写 Google 的 GSI 的 system.img ， 和 vbmeta.img

For verity-boot 1.1, flash system.img and vbmeta.img of Google GSI