密级状态：绝密(　　)　秘密(　　)　内部资料(　　)　公开(√)

Rockchip Provision Tool 说明手册

(软件创新中心)

文件状态： ［　］草稿 ［√］正式发布 ［　］正在修改	文件标识：	Rockchip Provision Tool 说明手册
	当前版本：	1.1
	作　　者：	韦敦
	完成日期：	2017-11-2

版 本 历 史

版本号	作者	修改日期	修改说明
V1.0	张志杰	2017-5-10	初始版本
V1.1	韦敦	2017-11-2	keybox 烧写会用到 vendor ID 8

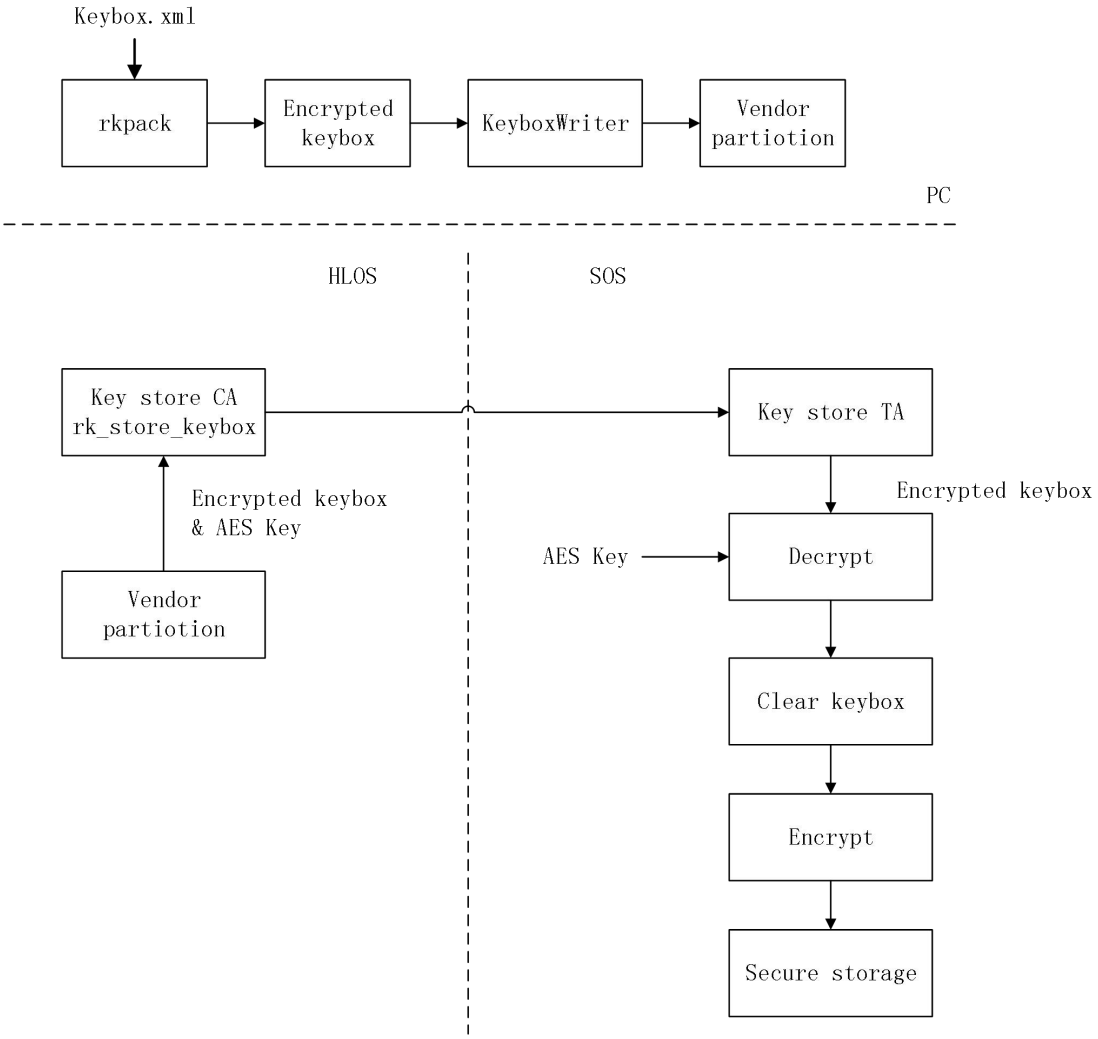
目 录

1 概述

Rockchip 提供了烧写安全相关信息到 secure storage 的方案。可实现将需要保密的重要安全信息安全高效地烧写到安全世界才能访问的安全存储区间中。

本文档以烧写 Widevine Keybox 为例进行方案说明.

整套烧写方案框图如下：



由以下几个部分实现：

1) rkpacker：keybox 加密打包工具；
2) KeyboxWriter：解析 keybox 密文包并将数据写入 vendor 区的工具；
3) rk_store_keybox：读取 vendor 中的 keybox 数据并将数据传到 Secure World 的 CA(Client Application)；

4) <uuid>.ta：Secure World 的应用程序，接收 keybox 数据，解密后将 keybox 明文再次进行加密，加密后存入 Secure Storage。

2 烧写步骤说明

2.1 PC 端工具加密 KEYBOX

OEM 厂商使用 RK 提供的 PC 端工具 rkpacker 加密 KEYBOX, 该工具只能运行在基于的 Linux 操作系统。

执行 rkpacker -h 可以查看操作说明

例如：rkpacker keybox.xml [...] [-o result.kdb]

如果要打包很多文件，可以使用 rkpacker *.xml 通配符。

2.2 PC 端工具烧写 vendor 区

OEM 厂商使用 RK 提供的 PC 端工具 KeyboxWriter 把加密后的 KEYBOX 以及密钥写入到 vendor 区，KeyboxWriter 需要以管理员权限打开。

KeyboxWriter 使用说明如下：

1）配置 config.ini NEW_VENDOR_SOLUTION，开启需要烧写的机器，通过 ADB 或者串口查看是否存在/dev/vendor_storage，存在则设置为 1，不存在则设置为 0。

1) 执行 KeyboxWriter.exe，点击“密钥文件”选取 rkpacker 生成的文件；

2) 设备进入 loader 模式，此时可在“端口”处看到设备信息；

3) 点击"开始"，开始写入 keybox，“提示信息”处可看到执行结果。

注意：如果设备存在/dev/vendor_storage， keybox 烧写会用到 vendor ID 8，如果项目还有自行开发工具用到 vendor 区，请从 ID 9 开始用。

2.3 CA/TA 自动烧写 Secure Storage

写入 vendor 区成功后，系统自动重启，然后通过 TEE 的 CA/TA 自动把 KEYBOX 烧写到 Secure

Storage，EMMC secure storage 目前用的是 RPMB。

3 环境需求与配置

本方案依赖于 TEE 环境，请确保系统的 TEE 环境正常。

4 注意事项

4.1 烧写出错排查

1) 向供应商确认使用的EMMC是否支持RPMB。
2) keybox烧写工具是否有以管理员权限打开。
3) 确认TEE环境是否正常，tee-supplicant 、rk_store_keybox是否开机运行。
4) 以上都确认没问题了，如果还是报错，请提供串口打印的log以及logcat。