PHYTIUM 飞腾

腾锐 D2000 安全 CPU

Tboot 使用说明

v1.0

飞腾信息技术有限公司

2021 年 6 月

更新记录

版本号	发布部门	作者	发布日期	备　注
1.0	飞腾通用软件部	邓强	2021-06-10	初稿

目录

1 概述

由于 trust-os（optee 或者其他 TEE 环境运行的 OS）调试的特殊性，需要将 trust-os 和固件打包并烧写到硬件中。如果 trust-os 需要反复修改，调试时，烧写硬件将成为一种反复的，并消耗大量开发时间的重复劳动。T-boot 的功能可以解决该问题。

2 名词解释

T-OS1：飞腾提供默认打包到固件中的 trust-os，仅有功能为提供接口将真正的 trust-os 加载到固定地址运行。

T-OS2：真正的 trust-os，可用通过任意方式加载到内存后，调用 T-OS1 提供接口即可开始运行。

3 T-Boot 原理

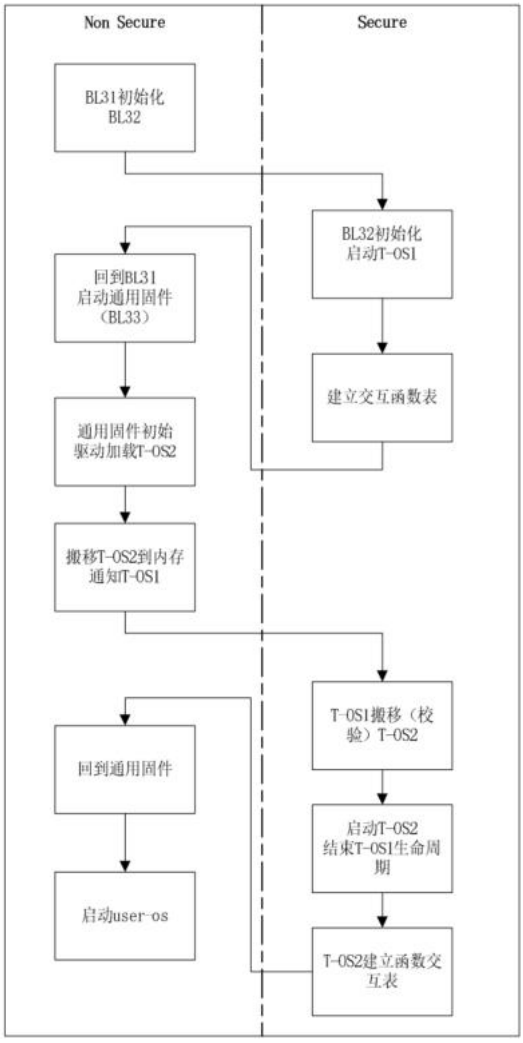

图 3.1 Tboot 交互原理图

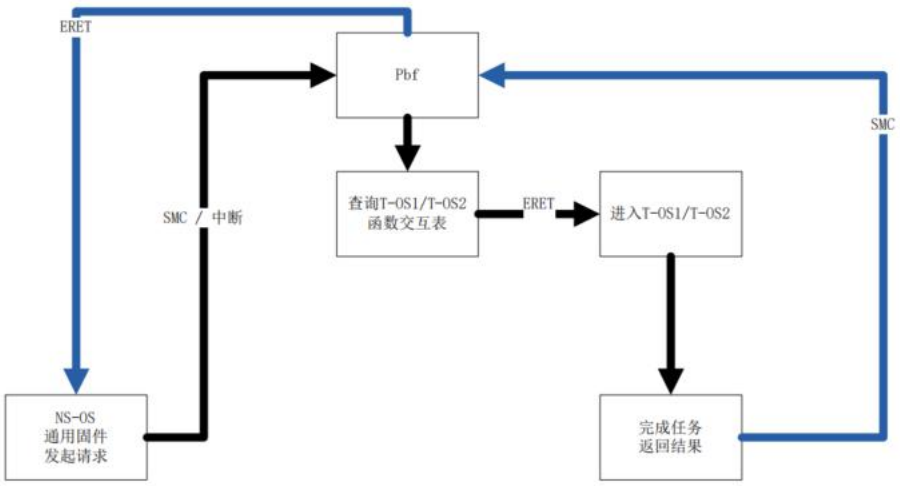

图 3.2 Tboot 调用关系图

4 Tboot 使用流程

1 更新 SDK 中打包工具 image_fix 中 build 目录为支持 T-boot 的 build 目录。

2 打包成 fip-all.bin，并烧录到硬件中。注意，这时候打包不要把 T-OS2 的映像打包进去。

3 启动系统，进入 uboot 或 uefi 命令行界面。

4 通过 U 盘/硬盘/网络加载等各种方式，加载 T-OS2 映像到内存。

比如预先将 T-OS2 映像保存在硬盘中，再在 uboot/uefi 下使用相关命令将 T-OS2 映像拷贝到内存的某个位置暂存。

5 通过调用 smc 指令，load T-OS2 映像进入系统。

smc 指令的调用可以使用系统自带接口，或者自定义的调用接口，只要符合 ARM smc 指令的调用规范。T-boot 功能的使用需要 smc 输入四个功能参数，定义如下：

表 4.1 Tboot 参数表

参数号	参数名	说明
0	操作码	T-boot 调用的操作码。 固定是 0xb2002006。
1	映像地址	暂存 T-OS2 映像的内存首地址。
2	映像大小	T-OS2 映像加载的大小。 必须大于等于 T-OS2 映像的实际大小。

3	保留	保留
4~7	保留	保留，AArch64 专用

接下来调试和 T-OS2 的普通调试保持一致。如果 T-OS2 需要修改，只需要重复 3,4,5 步骤即可，不需要重新烧写硬件。

5 注意事项:

1) T-OS2 编译地址应为：0xfc000000 ，可用空间：0xfc000000~0xff000000。
2) 此方案作为调测试补充手段，安全性不保证，不建议作为正式使用的 optee 启动加载方式。