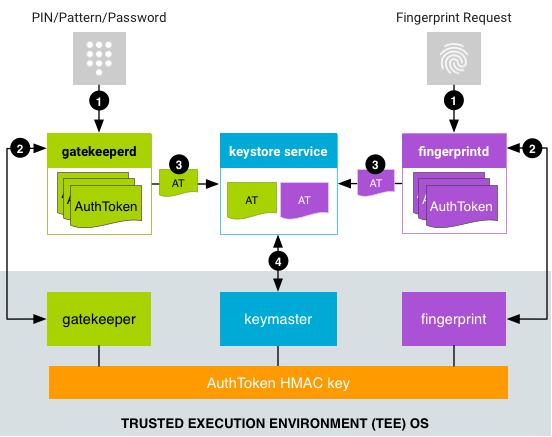


身份验证:

https://source.android.com/security/authentication?hl=zh-cn



<https://www.researchgate.net/figure/The-TEE-boot-and-root-of-trust-procedure_fig5_340615353>

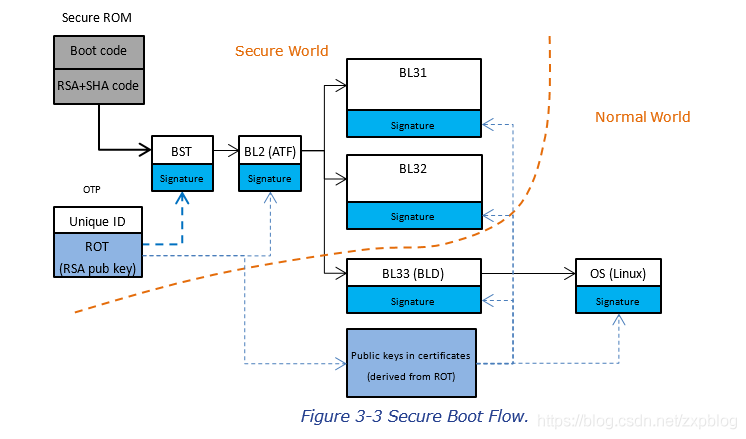
<https://baijiahao.baidu.com/s?id=1701986826964877586&wfr=spider&for=pc>

## root of trust

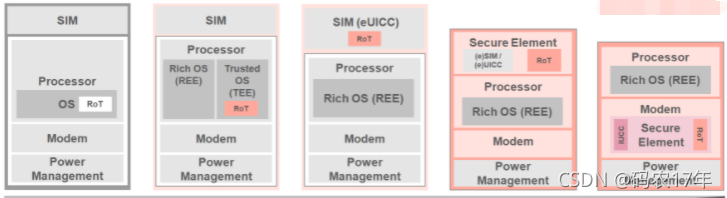
安全启动 root of trust

<https://blog.csdn.net/zxpblog/article/details/107410971>

chain of trust



https://blog.csdn.net/weixin\_49369227/article/details/120646358



ATF(Arm Trusted Firmware)/TF-A Chapter 03 Chain of Trust (CoT)

https://blog.csdn.net/puyoupuyou/article/details/105414174

## 使用OP-TEE进行可信软件开发

<http://taqini.space/2021/10/18/trusted-software-development-op-tee/>

TEE是如何实现的？

TEE 需要软件和硬件（内置于处理器中）支持。

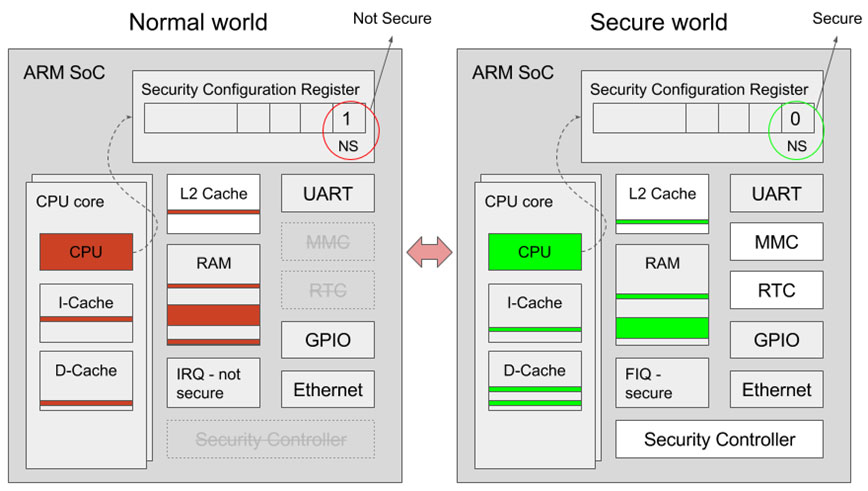
在硬件方面，基于ARM的处理器使用TrustZone技术实现TEE。TrustZone使单个物理处理器核心能够安全高效地执行来自正常世界（Linux/Android等丰富操作系统）和安全世界（OP-TEE等安全操作系统）的代码。这使得高性能安全软件能够在正常的操作环境下运行。TrustZone实现了基于“状态”的内存和IO保护。举个例子，当处理器在安全状态/上下文（安全世界）下运行时，它具有不同的系统视图，并且可以访问通常无法从非安全状态/上下文（正常世界）访问的内存/外围设备。更改当前运行的虚拟处理器时，两个虚拟处理器上下文通过监视器模式切换。

作者: TaQini

链接: http://taqini.space/2021/10/18/trusted-software-development-op-tee/

来源: TaQini

著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。



## 玩转OP-TEE

https://community.arm.com/cn/b/blog/posts/op-tee

https://www.cnblogs.com/jiangzhaowei/p/11057881.html

https://optee.readthedocs.io/en/latest/faq/faq.html#testing

https://optee.readthedocs.io/en/latest/

## 采用开源OP-TEE 的芯片厂商

https://cloud.tencent.com/developer/article/1079822

## linaro公司及其op-tee介绍

<https://mp.weixin.qq.com/s?__biz=MzI1Mjg2NjkwOQ==&mid=2247486299&idx=1&sn=d0d5dbf9b2719740a0e1e59e78e0c2f3&chksm=e9dc7369deabfa7f80aadbd1c98d89342a22116ef8c46a50f247b1d06790d7e4296bdf160506&scene=21#wechat_redirect>

2010年3月由ARM、NXP(飞思卡尔)、IBM、三星、ST-Ericsson和德州仪器，宣布共同出资组建Linaro公司。这家非营利性质的开放源代码软件工程公司将主要从事ARM平台开源软件的开发工作，帮助其他企业更快的推出基于Linux核心的设备ARM平台操作系统，包括Android、Ubuntu等。

不光是Linux内核,如下编译工具链是不是很熟悉？

arm-linux-gnueabihf

armv8l-linux-gnueabihf

aarch64-linux-gnu

arm-eabi

aarch64-elf

......

还有许多开源工程，比如TEE领域的OPTE。



OPTEE 是一个开源工程，完整的实现了一个可信执行环境。该项目最初由意法-爱立信所发起，是一个专门的解决方案，然后由ST半导体拥有和维护，2014年Linaro开始与意法半导体合作推出**将这个专有的TEE解决方案转换成一个开源的TEE解决方案。**

2015年9月，Linaro拥有了这个项目。今天它成为Linaro的一个关键的安全项目，Linaro的几个成员的支持和使用它。



关于op-tee使用的license问题：

1，大部分遵循BSD 2-条款。

2，TEE kernel 驱动遵循GPLv2。

3，测试套件，在TEE侧代码（TA）遵循BSD 2-条款，在REE侧代码（CA）遵循GPLv2。

再普及下开源协议知识：

BSD开源协议是一个给于使用者很大自由的协议。基本上使用者自由的使用，修改源代码，也可以将修改后的代码作为开源或者专有软件再发布。

BSD 代码鼓励代码共享，但需要尊重代码作者的著作权。BSD由于允许使用者修改和重新发布代码，也允许使用或在BSD代码上开发商业软件发布和销售。而很多的公司企业在选用开源产品的时候都首选BSD协议，因为可以完全控制这些第三方的代码，在必要的时候可以修改或者二次开发。

但是Linux就是采用的是GPL。GPL协议和BSD, Apache Licence等鼓励代码重用的许可很不一样。GPL的出发点是代码的开源/免费使用和引用/修改/衍生代码的开源/免费使用，但不允许修改后和衍生的代码做为闭源的商业软件发布和销售。

GPL协议的主要内容是开源和免费。这就是所谓的”传染性”。GPL协议的产品作为一个单独的产品使用没有任何问题，还可以享受免费的优势。

由于GPL严格要求使用了GPL类库的软件产品必须使用GPL协议，对于使用GPL协议的开源代码，商业软件或者对代码有保密要求的部门就不适合集成/采用作为类库和二次开发的基础。

现在就明白了吧。

国内许多企业也用了optee作为其TEE OS。

## keymaster

/\*\*

\* ITransport is an abstract interface with a set of virtual methods that allow communication between the keymaster

\* HAL and the secure element.

\*/

https://github.com/divegeek/JavaCardKeymaster