全志科技
Allwinner Technology

Tina

Secure 说明文档 v1.1

文档履历

版本号	日期	制/修订人	制/修订记录
V1.0	2017/10/27		初始版本
V1.1	2018/04/10		新增 AW 签名，新增量产工具

目　录

1. 概述

1.1. 编写目的

本文主要介绍了 Allwinner 安全方案的组成与功能。安全完整的方案基于 normal 方案扩展，覆盖 Secure Hardware、Secure Boot、Secure OS、Secure Application、量产工具等各个方面。除了 Secure Boot 是必选之外，其他功能都是可选的。

1.2. 适用范围

Allwinner 软件平台 Tina
Allwinner R18/R30 智能硬件平台

1.3. 相关人员

适用 Tina 平台的广大客户和相关技术人员。

2. 安全系统基础

2.1. 安全系统介绍

安全系统是基于硬件配合软件的安全解决方案。其主要目的是保障系统资源的完整性、保密性、可用性，从而为系统提供一个可信的运行环境。

2.2. 安全基础介绍

2.2.1. 内容保护

DRM：数字版权内容保护技术，用以强化保护数字化的音视频节目内容。
HDCP：高宽带数字内容保护技术，用于防止高清视频信号被非法录制。

2.2.2. 数据加密模型

（1）明文 P。准备加密的文本，称为明文。
（2）密文 Y。加密后的文本，称为密文。
（3）加解密算法 E(D)。用于实现从明文到密文或从密文到明文的一种转换关系。
（4）密钥 K。密钥是加密和解密算法中的关键参数。

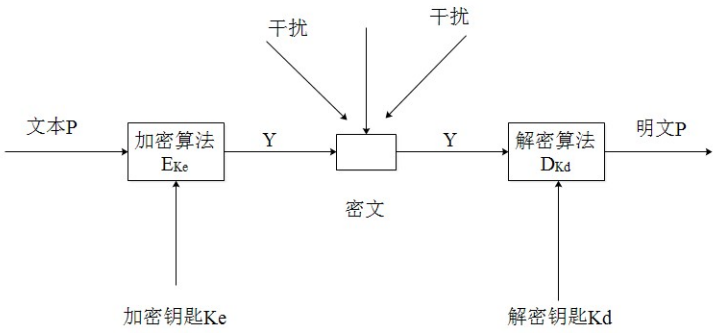

图 2-1 数据加密模型

2.2.3. 加密算法

对称加密算法：加密、解密用的是同一个密钥。比如 AES 算法。

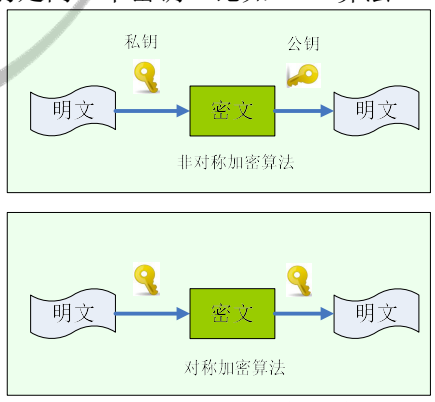

图 2-2 对称/非对称加密算法

非对称加密算法：加密、解密用的是不同的密钥，一个密钥“公开”，即公钥，另一个密钥持有，即私钥。其中一把用于加密，另一把用于解密。比如 RSA 算法。

散列（hash）算法：一种摘要算法，把一笔任意长度的数据通过计算得到固定长度的输出，但不能通过这个输出得到原始计算的数据。

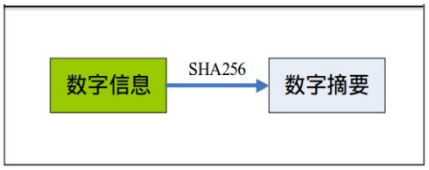

图 2-3 SHA256 算法

2.2.4. 签名与证书

数字签名：数字签名是非对称密钥加密技术与数字摘要技术的应用。数字签名保证信息是由签名者自己签名发送的，签名者不能否认或难以否认；可保证信息自签发后到收到为止未曾作过任何修改，签发的文件是真实文件。

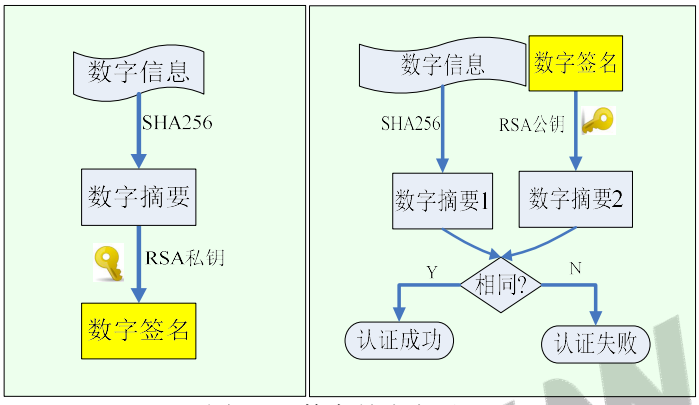

图 2-4 数字签名与认证

数字证书：是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件，是一种权威性的电子文档。

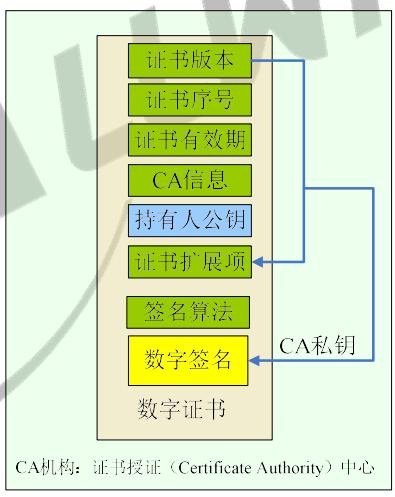

图 2-5 数字证书

2.2.5. efuse

efuse：一次性可编程熔丝技术。有些 SoC 集成了一个 efuse 电编程熔丝作为 OTP（One-Time Programmable，一次性可编程）存储器。efuse 内部数据只能从 0 变成 1，不能从 1 变成 0，只能写入一次。

2.3. TrustZone

TrustZone 是 ARM 提出的安全解决方案，旨在提供独立的安全操作系统及硬件虚拟化技术，提供可信的执行环境（Trust Execution Environment）。TrustZone 系统模型如图 2-6 所示。

TrustZone 技术将软硬件资源隔离成两个环境，分别为安全世界（Secure World）和非安全世界（Normal World），所有需要保密的操作在安全世界执行，其余操作在非安全世界执行，安全世界与非安全世界通过 monitor mode 来进行切换。具体可参考《trustzone security whitepaper.pdf》。

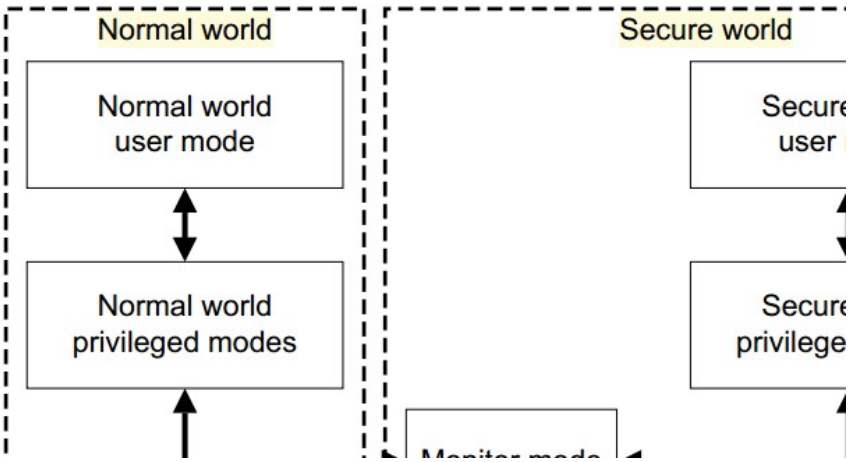

图 2-6 TrustZone 模型

2.3.1. OP-TEE

很多公司基于 TrustZone 推出了自己的安全操作系统，各自有各自的实现方式，但是基本都会遵循 GP（GlobalPlatform）标准。GlobalPlatform 是一个跨行业的国际标准组织，致力于开发、制定并发布安全芯片的技术标准，以促进多应用产业环境的管理及其安全、可互操作的业务部署。

OP-TEE 是 Linaro 联合其他几个公司一起合作开发的基于 ARM TrustZone 技术实现的 TEE 方案，遵循 GP 标准，主要由三部分组成：

① OP-TEE client (optee_client)： 运行在非安全世界用户空间的客户端 API。

② OP-TEE Linux Kernel device driver (optee_linuxdriver)： 用以控制非安全世界用户空间和安全世界通信的设备驱动。此部分代码在 Linux-4.4 mainline 上已经包含。

③ OP-TEE Trusted OS (optee_os)： 运行在安全世界的可信操作系统。

2.3.2. ATF

ARM Trusted Firmware(以下简称 ATF)是 ARM 推出的基于 AArch64 的启动系统架构。在 ATF 中，将启动划分成五个阶段：

- Boot Loader stage 1 (BL1) AP Trusted ROM
- Boot Loader stage 2 (BL2) Trusted Boot Firmware
- Boot Loader stage 3-1 (BL31) EL3 Runtime Software
- Boot Loader stage 3-2 (BL32) Secure-EL1 Payload (optional)
- Boot Loader stage 3-3 (BL33) Non-trusted Firmware

2.4. 相关术语

- SMC：Secure Monitor Call，ARM 给出的一条指令，可以让 CPU 从 Linux（非安全）直接跳转到 Monitor（安全）模式执行。
- RPC：Remote Procedure Control Protocol。optee 中，用于操作 Linux 下资源的一种机制。比如，optee 中不能读写文件，就通过 RPC 调用 Linux 下的文件系统来完成。
- REE：Rich Execution Environment。顾名思义，是资源丰富的执行环境，比如常见的 Linux，Android 系统等。
- TEE：Trusted Execution Environment。可信执行环境，即安全执行环境，在这个区域内，所有的代码，资源都是用户可以信任的。
- TA：Trusted Apps，在 TEE 下执行的应用程序，完成用户需要保护的任务，比如对密码的保护。
- NA：Normal Apps，在 REE 下执行的应用程序，完成普通的，不需要保护的任务，比如看普通视频。
- UUID：Universally Unique Identifier，通用唯一识别码。由当前日期和时间，时钟序列，机器识别码（如 MAC）组成。

3. Secure Boot

安全启动，即 Secure Boot，是一个安全系统必不可少的组成部分。Secure Boot 从 brom 执行开始，到 Linux 启动结束。Secure Boot 主要设计目的：

- 建立完整的安全信任链，确保启动阶段加载的各种镜像是可信的。
- 相关 key 的烧写。
- 固件版本管理。
- 设置安全的硬件环境，加载并运行 Secure OS 等。

3.1. 安全启动原理

Tina 安全方案基于私钥签名—公钥验签的业界公认非对称算法实现完整的安全启动方案，具体来说，对于 R18/R30，选择的是 RSA2048-SHA256。通过使用私钥给固件进行签名生成安全固件，再将公钥的 hash 值即 rotpk.bin 烧写至芯片的 efuse 区域。启动时，固化在芯片的 BROM 程序首先会读取 efuse 中的 hash 值确保根证书中公钥的可信任。然后会使用 flash 中存储的证书链中的一系列公钥来对各个子固件进行逐级安全校验。验证顺序为芯片的 brom->sboot->uboot->boot.img。efuse 的不可更改性确保了证书链的可信任，整个流程的设计确保了整个 Linux 方案的安全启动。

3.2. 如何生成安全固件

Tina SDK 已经将安全固件制作流程中密钥的生成和必要的签名过程集成在打包脚本内部，所以安全固件的编译及打包流程与非安全固件的几乎一致，只是在最后的打包的时候有差异。非安全固件的打包可参考用户《XXX Quick Start Guide.doc》文档，安全固件的打包步骤如下：

```
$ source build/envsetup.sh
      ==> 设置环境变量
$ lunch
      ==> 选择方案，R18 开发方案对应的是 tulip_*，R30 对应 koto_*
$ make [-jN]
      ==> 编译，-jN  参数选择并行编译进程数量
$ cd scripts/
$ ./createkeys
$ cd ../
      ==> 创建密钥，会在 out/<board>/keys/目录下生成所需的密钥。
$ pack -s [-d]
      ==> 打包，-s  表示制作安全固件。-d 参数使生成的固件包串口信息转到
tf 卡座输出。
```

编译完成后，系统镜像会打包在 out/<board>/目录下。

客户拿到 SDK 后，必须创建自己的密钥并妥善保存。请至少运行一次./createkeys 命令。同时执行下面操作：

- 拷贝 out/<board>/keys/目录下的 rotpk.bin , Trustkey.bin 和 Trustkey.pem 三个文件到自己私有的目录。
- 其中的 rotpk.bin 保存 Root rsa public key 的 hash 值，需要借助烧 key 工具烧写到芯片里。
- 另外两个文件都是 Root rsa private key，是非常重要的隐私数据，不能泄漏和丢失。丢失 Root rsa private key 会导致 SDK 生成的固件无法在芯片上启动，泄漏 Root rsa private key 可能会失去防刷机功能。

4. Secure OS

ARM 利用 CPU 分时复用的思路，设计了 SMC 指令切换到另外一个特殊状态再结合 SOC 级别的硬件 IP 构建了被称为 ARM TrustZone 的安全技术。

Tina 上的部分方案（如 R18/R30 等）从 SOC 层面支持 ARM Trustzone，但要设计满足 Linux 系统安全标准和需求的安全方案除了实现 ARM TrustZone SOC 还必须有一套软件可信执行环境 TEE。Tina 采用的 OP-TEE 便是一种特定安全系统实现，它严格遵循 ARM Trust-Zone 和 TEE/GP 等产业标准。

4.1. optee 总体框架

optee 系统，是由运行在 TEE 环境下的 optee os、TA、以及运行在 REE 环境下的 client、driver、NA 组成，一共五个部分。optee 总体架构如下图所示：

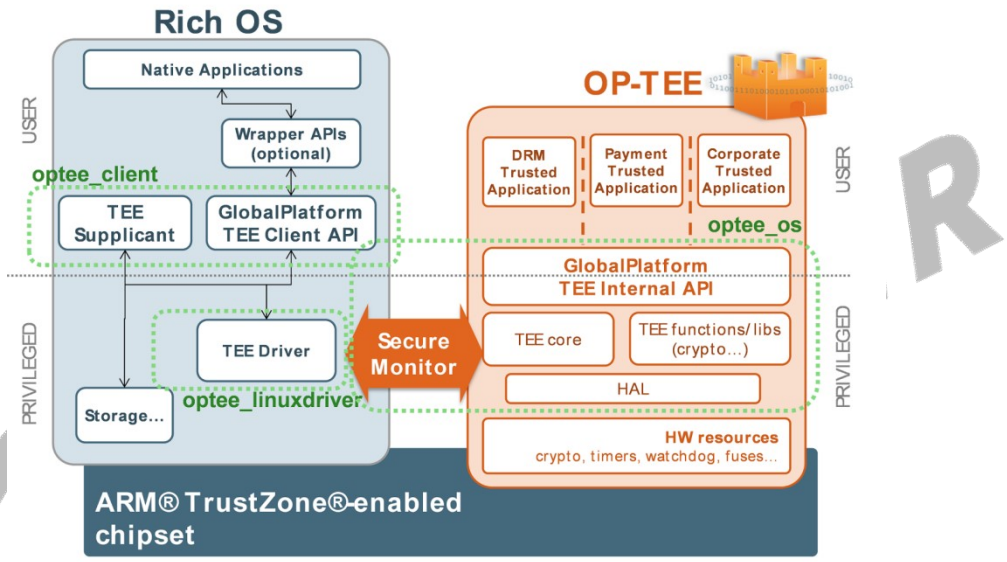

图 4-1 optee 总体架构

4.2. 如何开启 Secure OS

Tina 安全固件在打包时加入 -s 选项，就会自动把 optee 打包到安全固件中。

除此之外，还需要在内核中使能 optee 驱动，执行 make kernel_menuconfig，选中如下几项：

```
Device Drivers  --->
    <*> Trusted Execution Environment support
        TEE drivers  --->
            <*> OP-TEE
```

5. 量产工具

从整个安全系统的角度看，需要一整套工具来配合完成对应的工作。

5.1. RSA 密钥对生成工具

目前，有公开的密钥对生成工具 openssl，可以生成足够长度的密钥对。

Tina 开发平台 scripts 下提供了一个生成密钥对的脚本 createkeys，该脚本调用 dragonsecboot 工具，解析 dragon_toc*.cfg 中[key_rsa]字段，并基于字段的内容生成对应名字的密钥对。

5.2. 安全固件版本管理

安全固件打包时会解析 target/allwinner/generic/version/version_base.mk 文件，并基于其中的内容生成对应版本的固件。

在 efuse 中会有一块区域用来记录固件版本。烧写时，会将固件中的版本写入 efuse 中对应区域。

当启动时，会将 efuse 中记录的版本号同固件中的版本号比较，如果固件中的版本较低，则不能继续启动。可防止固件版本回退。

5.3. 数据封包工具

Tina 开发平台中提供固件封包工具 dragonsecboot，在安全固件打包过程中会对相关的镜像文件（sboot、uboot、kernel 等）进行签名，并生成证书以及相关信息，以便启动时对这些镜像文件进行校验，验证完整性。

5.4. 烧 key 工具

烧 key 工具用来将 rotpk.bin 烧写到设备的 efuse 中，efuse 位于 IC 内部，由于 efuse 中内容一旦写入便不可更改，所以从根源上保证了根证书公钥 hash 的安全性。

可用的烧 key 工具包含 DragonKey 或者 DragonSN，工具的使用说明位于工具包中。

6. 参考资料

6.1. TrustZone

【1】 PRD29-GENC-009492C_trustzone_security_whitepaper.pdf

6.2. GlobalPlatform

【1】 GPD_TEE_SystemArch_v1.1.pdf
【2】 GPD_TEE_Client_API_v1.0_EP_v1.0.pdf
【3】 GPD_TEE_Internal_Core_API_Specification_v1.1.pdf
【4】 GPD_TEE_TA_Debug_Spec_v1.0.pdf

6.3. OP-TEE

【1】 https://www.op-tee.org/documentation/

7. Declaration

This document is the original work and copyrighted property of Allwinner Technology (“Allwinner”). Reproduction in whole or in part must obtain the written approval of Allwinner and give clear acknowledgment to the copyright owner.

The information furnished by Allwinner is believed to be accurate and reliable. Allwinner reserves the right to make changes in circuit design and/or specifications at any time without notice. Allwinner does not assume any responsibility and liability for its use. Nor for any infringements of patents or other rights of the third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of Allwinner. This datasheet neither states nor implies warranty of any kind, including fitness for any particular application.