Trusty 指纹 TA 开发指南

Document Number:		**Document Version:**	0.2
Owner:		**Date:**	2017/04/21
Document Type:			
NOTE:	ALL MATERIALS INCLUDED HEREIN ARE COPYRIGHTED AND CONFIDENTIAL UNLESS OTHERWISE INDICATED. The information is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination, or other use of or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited. This document is subject to change without notice. Please verify that your company has the most recent specification. Copyright © 2017 Spreadtrum Communications Inc.		

SPREADTRUM

www.spreadtrum.com

Revision History

Revision	Date	Author	Description
0.1	2017/03/20	Andrew.Ma Jinping.Wu	draft
0.2	2017/04/21	Aijun.Sun	1.更新 API 列表 2.完善 TA Demo 说明

Table of Contents

1. Trusty API

1.1. 原生 Trusty API

主要为 IPC 类 API，请参考 https://source.android.com/security/trusty/trusty-ref

1.2. 扩展 API

1.2.1. 安全存储

主要包括以下接口

```
storage_open_session
storage_open_file
storage_close_session
storage_close_file
storage_get_file_size
storage_read
storage_write
storage_delete_file
```

1.2.2. Keymaster

主要包括以下接口

```
keymaster_open
keymaster_close
keymaster_get_auth_token_key
```

1.2.3. SPI 驱动

主要包括以下接口

```
spi_setup
spi_sync
```

```
spi_read
spi_write
```

2. 设备驱动

由于 Trusty/LK 不支持统一的设备驱动框架，一般对设备驱动的实现无特别要求。但在指纹驱动的开发中，需注意在驱动程序中注册操作接口给用户空间使用。目前 Trusty 支持 ioctl, read, write 3 类操作。

3. 开发文档

请参考 Google Trusty 官网 https://source.android.com/security/trusty

4. TA 参考代码

4.1. 代码结构

```
├── cademo
│   ├── Android.mk
│   ├── cademo.cpp
│   ├── cademo.h
│   ├── cademo_ipc.c
│   └── cademo_ipc.h
├── readme
└── tademo
    ├── ipc
    │   ├── rules.mk
    │   ├── tademo_ipc.cpp
    │   └── tademo_ipc.h
    ├── LICENSE
    ├── manifest.c
    ├── rules.mk
    ├── trusty_tademo.cpp
    └── trusty_tademo.h
```

4.2. CA(Client Application)

CA 主要包含两个文件，cademo_ipc.c 和 cademo.cpp

cademo_ipc 实现了 IPC 部分代码，包括 trusty_cademo_call、trusty_cademo_connect、trusty_cademo_disconnect 单个函数供 cademo 调用，写自己的 ca 需要修改
cademo_ipc.h 中几个定义，其中 tademo_message 只需要改下名字，结构体本身不需要修改。

4.3. TA(Trusted Application)

tademo_ipc 实现了 TEE 侧 IPC 部分代码，除了名字修改外，针对具体业务，主要需要修改 handle_request 函数，in_buf 为 CA 传过来的数据，out_buf 为 TA 返回给 CA 的数据，这个函数需要把
CA 传过来的数据传到 TA 去处理，然后把 TA 返回的数据放到 out_buf 中返回给 CA

4.4. TA manifest

TA manifest 定义了 TA UUID, TA 所使用的 heap 和 stack 的内存大小。

```
trusty_app_manifest_t TRUSTY_APP_MANIFEST_ATTRS trusty_app_manifest =
{

   /* UUID : {4304bef6-36e5-4d90-94b0-1ea4cd51d40b} */
   { 0x4304bef6, 0x36e5, 0x4d90,
       { 0x94, 0xb0, 0x1e, 0xa4, 0xcd, 0x51, 0xd4, 0x0b } },

         /* optional configuration options here */
         {
                  TRUSTY_APP_CONFIG_MIN_HEAP_SIZE(2 * 4096),
                  TRUSTY_APP_CONFIG_MIN_STACK_SIZE(1 * 4096),
         },
};
```

4.5. 编译配置

CA 代码的编译配置可以参考 Android native 程序。
Trusty TA 使用的 makefile 文件为 rules.mk, 类似 Android.mk。有几个主要的 makefile 变量必须定义，如下。
MODULE： TA 在 Trusty 中的 module 名称

MODULE_SRCS：　　所有代码文件
MODULE_DEPS：　　依赖的模块或库
MODULE_INCLUDES：依赖的头文件