AG35-QuecOpen

安全架构介绍

LTE 系列

版本：AG35-QuecOpen_安全架构_V1.0

日期：2017-11-15

状态：临时文件

上海移远通信技术股份有限公司始终以为客户提供最及时、最全面的服务为宗旨。如需任何帮助，请随时联系我司上海总部，联系方式如下：

上海移远通信技术股份有限公司
上海市徐汇区虹梅路 1801 号宏业大厦 7 楼　　邮编：200233
电话：+86 21 51086236　　邮箱：info@quectel.com

或联系我司当地办事处，详情请登录：
http://quectel.com/cn/support/sales.htm

如需技术支持或反馈我司技术文档中的问题，可随时登陆如下网址：
http://quectel.com/cn/support/technical.htm
或发送邮件至：support@quectel.com

前言

上海移远通信技术股份有限公司提供该文档内容用以支持其客户的产品设计。客户须按照文档中提供的规范、参数来设计其产品。由于客户操作不当而造成的人身伤害或财产损失，本公司不承担任何责任。在未声明前，上海移远通信技术股份有限公司有权对该文档进行更新。

版权申明

文档历史

修订记录

版本	日期	作者	变更表述
1.0	2017-11-15	钱润生	初始版本

目录

表格索引

图片索引

1 AG35 安全介绍

Quectel 推出的 AG35 模块是基于 Qualcomm 推出的专业车载无线蜂窝数据基带芯片 MDM9628 而设计，有着非常高的**安全性**和**稳定性**。针对车载电子产品特殊的安全应用特点和要求，Quectel 给出了从下而上的全方位安全机制来保证客户的各种信息安全。

针对车载产品对于**启动安全、平台运行安全、通信安全**三个主要领域有着特殊很高的要求，为此 Quectel 结合了 Qualcomm 给出的 secureboot、QSEE/TrustZone 安全机制以及 Linux 系统的 DM-verity、SELinux 和 openSSL 等组合方式，实现从启动到客户进程的安全稳定运行，防止出现窃取、篡改客户信息和文件等重要信息，图 1 展示了 AG35 的安全架构。

图 1 安全框架

2 启动安全

2.1. 启动流程

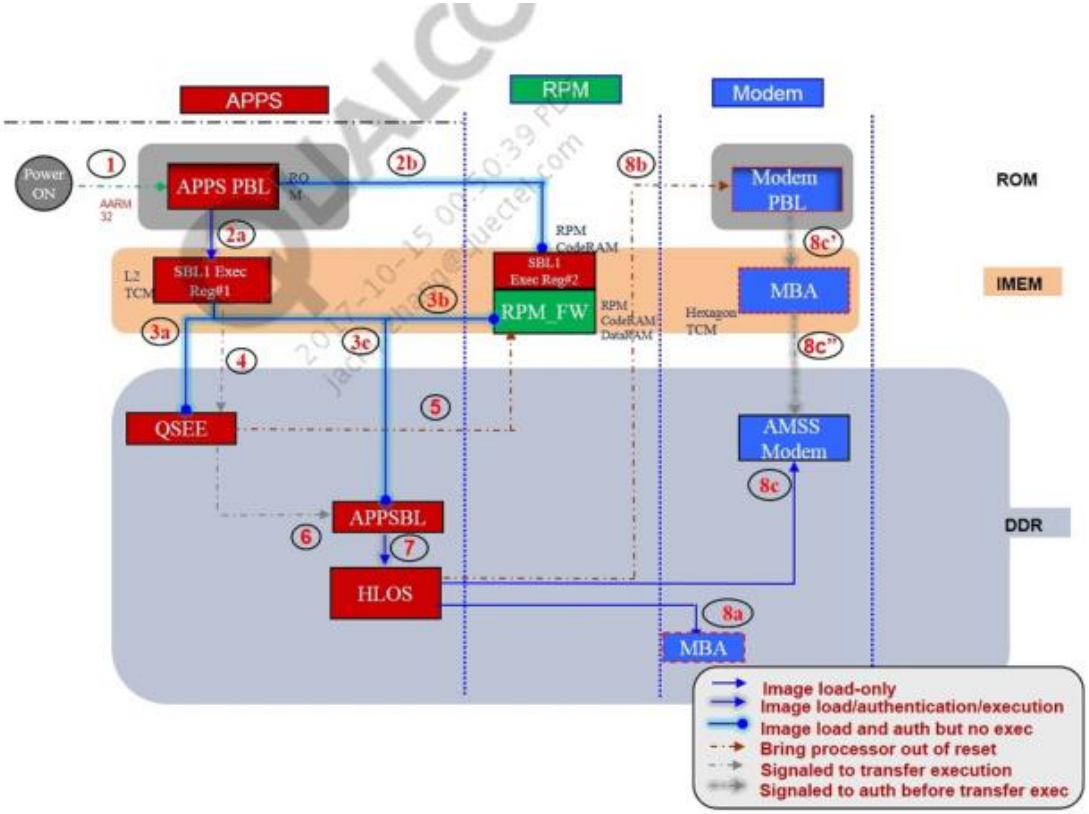

图 2 AG35 固件启动流程

2.2. DM-verity

QUCETL 实现基于 DM-Verity 机制实现对文件系统的安全检查，使用的基本步骤如下：

- 生成文件系统 image.
- 生成文件系统 image 的 hash 树.
- 构建 此 hash 树的 dm-verity 表.
- 对 dm-verity 表签名.
- 绑定 dm-verity 表和签名到元数据 metadata.
- 连接 image、verity metadata 和 hash 树.

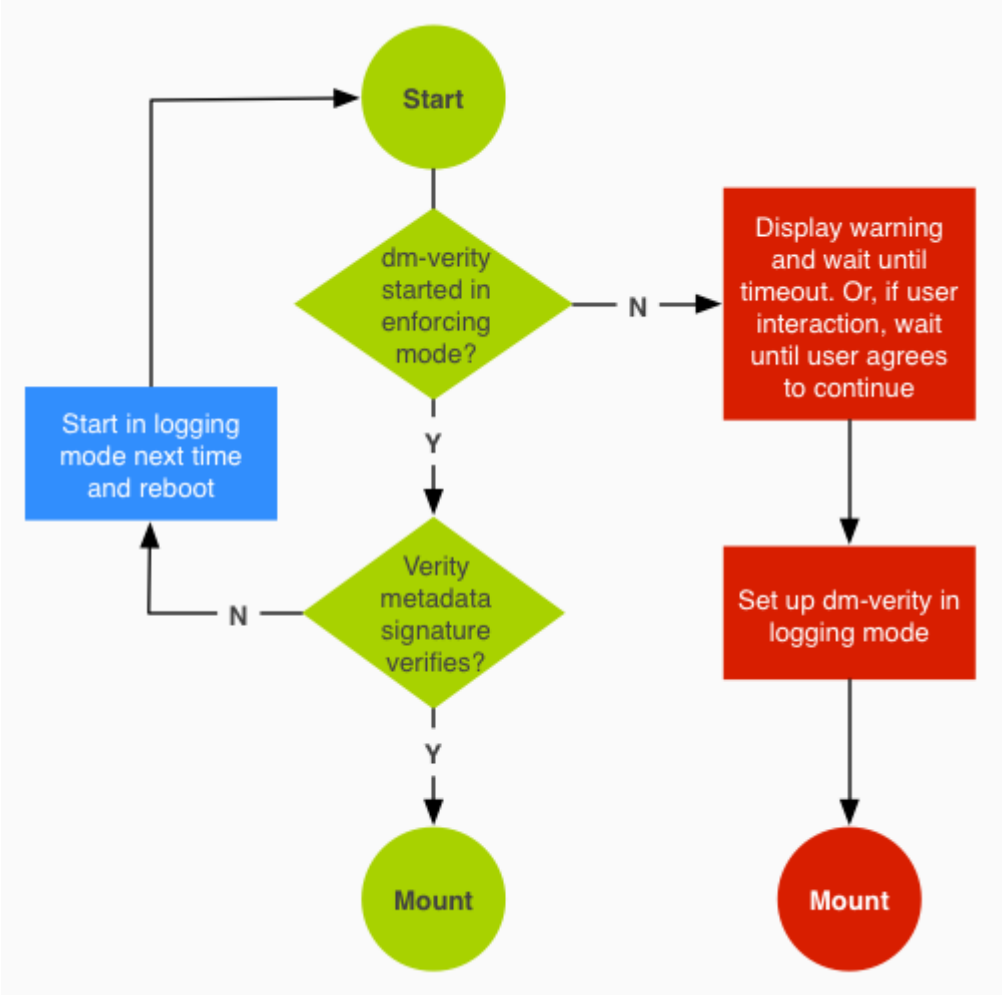

图 3 DM-Verity 工作机制

2.3. 使用步骤

（1）用户使用 OpenSSL 产生公私钥对和证书；

（2）用户使用该证书对 image 进行签名；

（3）用户使用工具产生 sec.dat 进行 eFuse 的配置使能，比如 JTAG Disable、secureboot 功能的使能；证书的 HASH 也存在 secdata 中。

（4） 用户在产线下载签名后的 image 以及 sec.dat；（需要重启）

（5）对只读文件系统采用 DM verify 方式签名验证(从 Android 移植 DM Verify)

3 平台安全

3.1. SELinux

Quectel 会提供该功能的开关功能，针对进程服务、文件的增加安全权限策略提供方案技术。SELinux 的工作过程如下图所示：

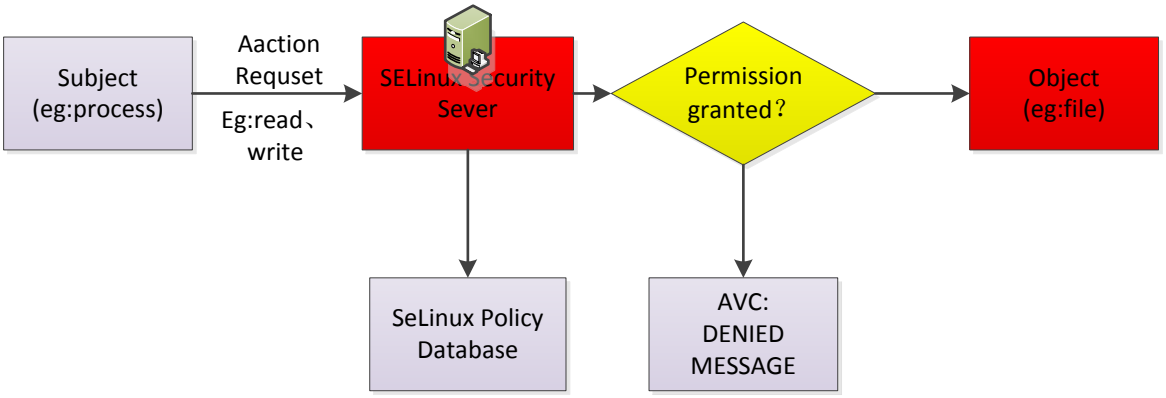

图 4 SELinux 工作过程

当一个主体 subject(如: 一个应用)试图访问一个客体 object(如：一个文件)，Kernel 中的策略执行服务器将检查 AVC (Access Vector Cache), 在 AVC 中，subject 和 object 的权限被缓存(cached)。如果基于 AVC 中的数据不能做出决定，则请求安全服务器，安全服务器在一个矩阵中查找“应用+文件”的安全环境。然后根据查询结果允许或拒绝访问，拒绝消息细节位于/var/log/messages 中。

使用步骤简要如下：

开启 SELinux 功能

为资源（文件）设定标签

针对特殊的 subject 和 object 建立 policy 并添加到 policy 数据库

策略文件可以单独存放于一个分区中，便于单独升级策略。

3.2. TrustZone 加密

TrustZone 提供一个可信程序执行环境(TEE)(包括内存安全、外设访问安全等)，保证你的代码运行时不能被别人窥探到。

其运行流程主要如下 3 个步骤:

1. 代码被编译成小程序(Trustlets).
2. 通过高通安全执行环境（QSEE）(表现为内核里的一个驱动)被载入到 TrustZone 中运行。
3. Linux 驱动再通过系统调用 smc_call() 调用你的 Trustlets 提供的服务。

Quectel 提供 Crypto Trustlet，提供加解密功能：

对称加解密(AES)： 生成秘钥、导入秘钥、加密、解密

非对称加解密（RSA）： 生成钥对、导入钥对、签名、校验、导出公钥

3.3. 固件保护

（1） 根文件系统采用只读模式
（2） 备份还原机制
（3） 可定制化分区

3.4. 调试接口保护

（1）可关闭 adb
（2）可关闭 fastboot
（3）可关闭 jtag
（4）可关闭串口，USB 口

3.5. 通信安全

3.5.1. Iptable

Quectel 针对客户特定的应用场景实现各种复杂安全路由策略。

3.5.2. OpenSSL

Quectel 提供标准的开源执行库和 API 接口头文件，定时完善安全漏洞，协助客户开发。