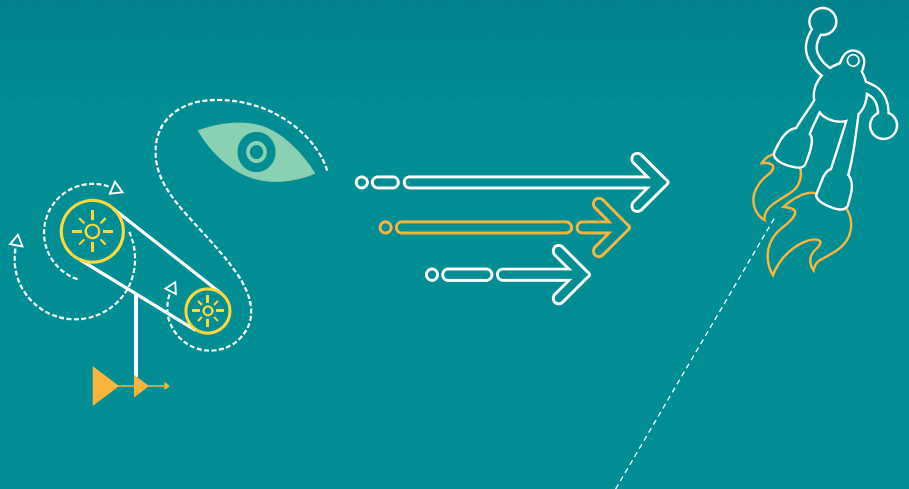
SDM670 TrustZone 与安全概述

Qualcomm Technologies, Inc.



80-PD126-3SC 版本 B

机密和专有信息 – Qualcomm Technologies, Inc.

禁止公开披露：如若发现本文档在公共服务器或网站上发布，请报告至：DocCtrlAgent@qualcomm.com。

未经 Qualcomm Technologies, Inc. 的明确书面许可，不得使用、复印、复制或修改其全部或部分内容，或以任何方式向其他人泄露其内容。

Qualcomm Trusted Execution Environment、Malware Detection、Qualcomm Snapdragon、Qualcomm Kryo、MSM、Qualcomm Spectra 和 Qualcomm Processor Security 是 Qualcomm Technologies, Inc. 的产品。本文中提到的其他 Qualcomm 产品是 Qualcomm Technologies, Inc. 或其子公司的产品。

Qualcomm、Snapdragon、Kryo 和 MSM 是 Qualcomm Incorporated 在美国及其他国家/地区所注册的商标。其他产品和品牌名称可能是其各自所有者的商标或注册商标。

本技术资料可能受美国和国际出口、再出口或转让（统称“出口”）法律的约束。严禁违反美国和国际法律。

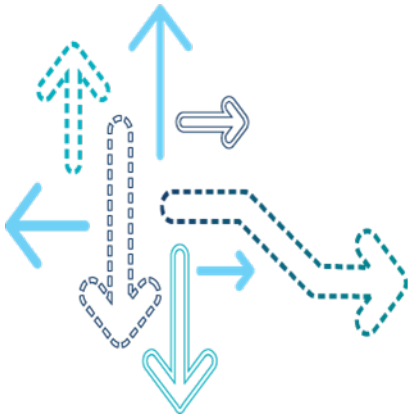
Qualcomm Technologies, Inc.
5775 Morehouse Drive
San Diego, CA 92121
U.S.A.

修订记录

版本	日期	说明
A	2017 年 8 月	初始版本
B	2017 年 9 月	更新了幻灯片 10 中对虹膜安全摄像头的说明

目录

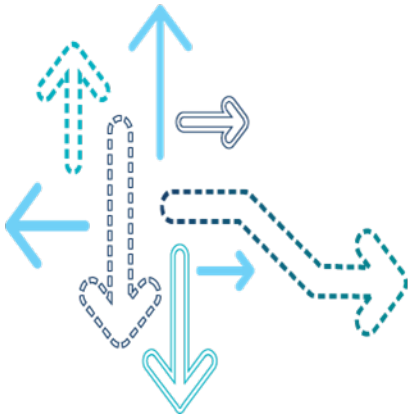
目标



目标

- 本文档可作为帮助 OEM 了解安全架构以及项目规划信息的切入点。
- 提供关于新功能、产品改进的信息，并帮助理解：
  - 芯片组和 MSM 芯片组级硬件架构
  - 软件架构
  - 硬件和软件迁移的详细信息，以帮助用户进行规划和开发工作
  - 高级软件设计
  - 提供更多详细信息的参考文档

产品特性



SDM670 安全摘要

软件功能	说明
安全启动	三种证书链模型： ▪ 通过 RSA-PSS 填充方案进行 SHA256 和 SHA384 签名 ▪ OEM 可定制的根密钥哈希 ▪ 用于安全访问控制设置的 Xbl_sec 启动加载程序映像
Qualcomm® 受信任执行环境 (QTEE) （以前称为 Qualcomm 安全执行环境 (QSEE)）	在基于 ARMv8-A 硬件的 TrustZone (TZ) 安全环境中运行的安全 OS
受信任应用程序 (TA)	在 QTEE 上运行的可动态加载的安全应用程序
伪 IMEM (pIMEM)	用于执行 TZ 安全 OS 和受信任应用程序的加密 DDR 区域
Keymaster (KM)	支持公钥和私钥生成、管理、签名和验证的 Keystore 服务
安全文件系统 (SFS)	TZ 和 Modem 的加密文件存储
访问控制	▪ 对寄存器地址（固定或动态）存储区域的从侧访问控制 ▪ 通过第 2 阶段存储器管理单元 (MMU) 实现主侧访问控制
调试安全 （以前称为安全调试）	在熔丝已熔断的设备上再次启用调试
内容保护	PlayReady、Widevine、HDCP 2.x 和 ISDB-T 全频段

SDM670 安全摘要（续）

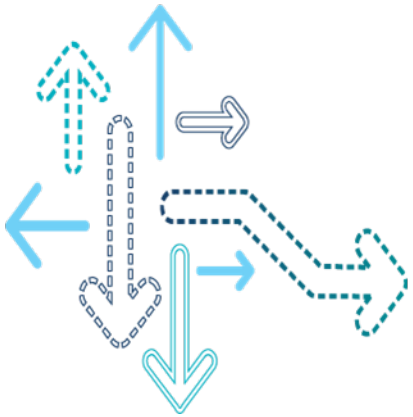
软件功能	说明
设备加密	全磁盘加密、基于文件的加密
鉴权框架	▪ 受信任 UI（以前称为安全 UI） ▪ 安全支付 ▪ 摄像头安全（以前称为安全摄像头） ▪ Qualcomm® 恶意软件检测（以前称为 Qualcomm Snapdragon 智能保护）
Android 验证启动	高级操作系统 (HLOS) 映像的加密鉴权

硬件功能	说明
加密核心	在设备硬件中执行 AES、三重 DES、SHA 加密算法
内嵌加密引擎 (ICE)	存储设备的硬件加密
熔丝存储器	▪ 一次性可编程 QFPROM 熔丝存储器 ▪ 通过安全分区自动编程

SDM670 安全迁移指南

更改	说明	迁移	影响
密钥管理： Keymaster 3.0	Keymaster 3.0 的格式变更	▪ 通过 Keymaster v1.5 或 v2 生成的密钥与 Keymaster v3 不兼容 ▪ 升级时必须擦除用户数据	高
TZ： 受信任应用程序改进	▪ 改进了与 Commonlib 的动态链接 ▪ 增加了保护页以进行堆和堆栈溢出检查	受信任应用程序必须使用 SDM670 TZ 编译文件重新编译	高
生物特征识别： 虹膜安全摄像头	支持 Qualcomm Spectra™ ISP 硬件的端到端安全摄像头解决方案	▪ 利用少量更改实现并测试此功能 ▪ 提供移植指南	低

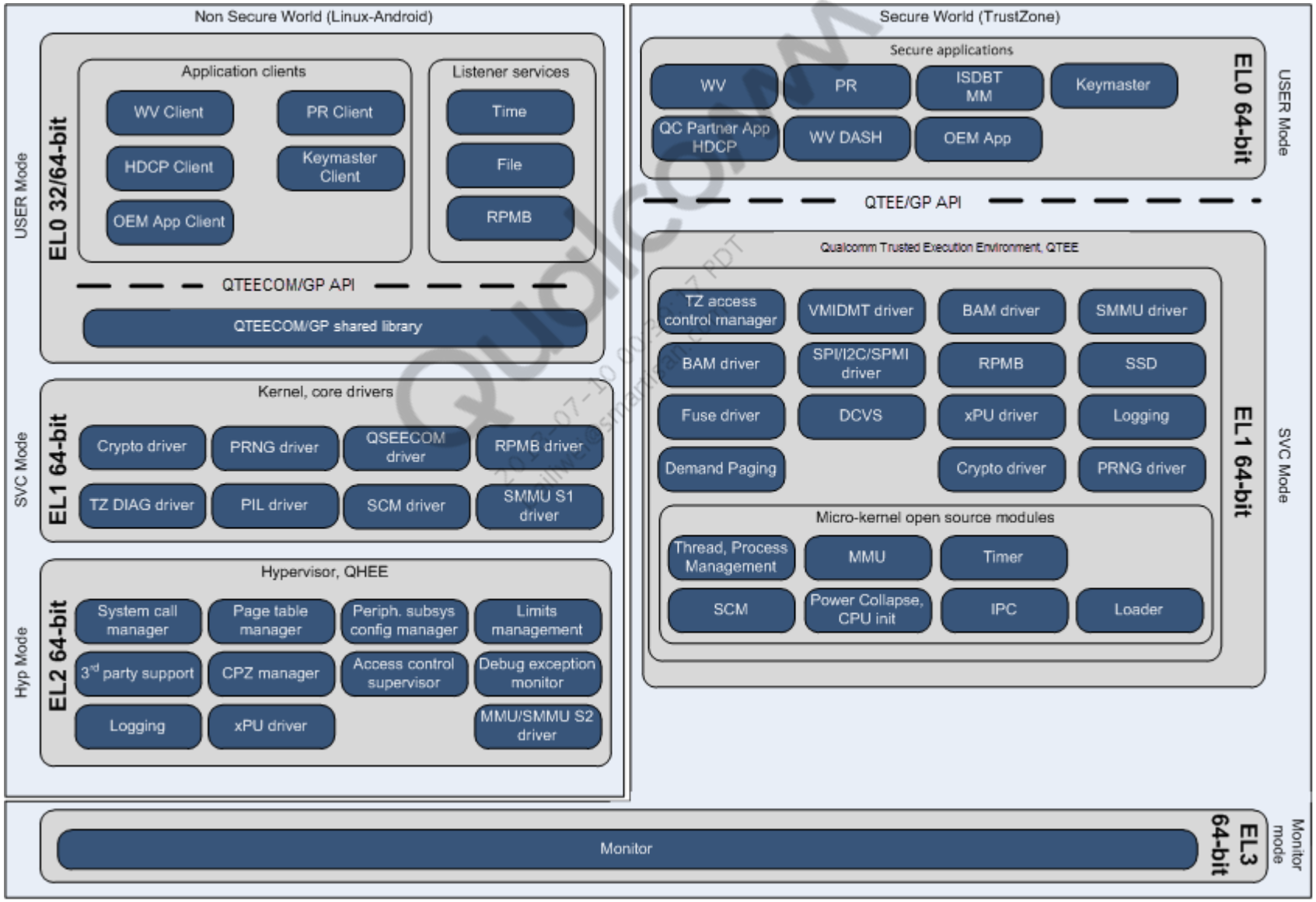
TrustZone



TrustZone 概述

- SDM670 芯片组提供 64 位 ARMv8-A 处理器系统，包括具有硬件虚拟化功能的 Qualcomm® Kryo™ CPU
- TZ 是一种基于硬件的安全环境，通过 ARM 处理器安全模式实现
  - 操作系统在非安全 EL1 模式下运行
  - 通过安全监视器模式由非安全模式过渡到安全模式
- TZ 软件由 TZ 板支持包 (TZBSP) 和 QTEE 组件构成
  - TZBSP
    - 为芯片组安全提供软件支持
    - 公开芯片组安全函数的硬件抽象层 (HAL) API，如加密、熔丝模块、PRNG 等
    - 在启动以及从深度休眠模式唤醒过程中，针对软件和硬件的系统安全环境进行初始化
    - 在运行过程中，保护存储器和其他子系统并提供服务
  - QTEE
    - 提供安全服务，如映像加载、鉴权、缓存管理、加密、日志记录和 QFPROM 至 TZ 安全应用程序
- TZ 软件映像在初始设备启动过程中通过 XBL 加载程序进行加载，并由 XBL SEC 鉴权
- 伪 IMEM (PIMEM) 提供 64 MB 加密双倍数据速率 (DDR) 区域，用于执行 TZ 和受信任应用程序

QTEE 框架框图



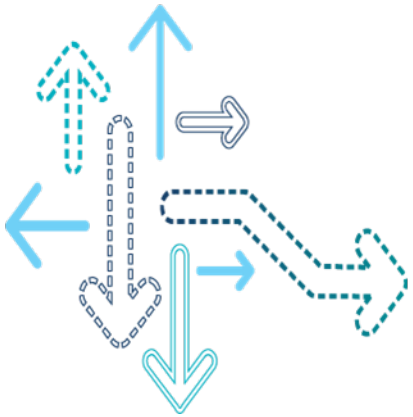
受信任应用程序

- 支持在安全环境 EL0 中运行的受信任应用程序
- 在非安全 HLOS 侧提供客户端使用的服务
- 在 SDM670 芯片组中，QTEE 创建保护页以进行堆和堆栈溢出检查
- 作为开发新受信任应用程序的模板和参考，提供的 sampleapp：
  - 用于配置 RPMB 和测试 QTEE API
  - 由其 HLOS 对应的 qseecom_sample_client 调用
  - 若要使用编译 sampleapp：
    - cd trustzone_images/build/ms
    - python build_all.py -b TZ.XF.5.0 CHIPSET=sdm670 --cbt=sampleapp
  - RPMB 密钥配置示例：qseecom_sample_client v smplap64 14 1
- 提供的 smplserv 和 smplcert 受信任应用程序作为 QTEE IPC 机制的参考
- smplcert 受信任应用程序使用 smplserv 提供的服务

安全文件系统概述

- 提供的安全文件系统 (SFS) 用于存储密钥、生物特征识别数据等敏感信息
- 提供两种独立的 SFS，一个位于 TZ 中，另一个位于 Modem 中
- 设备启用安全启动后，两安全文件系统使用不同硬件加密引擎进行文件数据加密和解密，因此两个文件彼此之间具有安全性
- 默认启用 SFS 防回滚保护功能
- 防回滚保护通过 eMMC/UFS 存储的 RPMB 硬件支持以及 TZ 中的 RPMB 驱动程序实现
- 在开发过程中，OEM 必须使用 sampleapp TrustZone 应用程序将其设备配置为使用测试 RPMB 密钥
- 在商用设备中，产品 RPMB 密钥由 TZ 在检测到安全启动且 JTAG 禁用电子熔丝后自动提供
- 为了确保 SFS 的安全，设备的 RPMB 密钥仅可提供一次；因此，如果为设备提供测试密钥，则无法再为其提供产品密钥
- OEM 必须谨慎规划开发设备，以满足上述限制条件
- OME 可在 XML 配置文件 trustzone_images/core/securemsm/trustzone/qsee/mink/oem/config/common/cmnlib_oem_config.xml 中启用或禁用基于 RPMB 的 SFS 防回滚保护

Qualcomm 访问控制



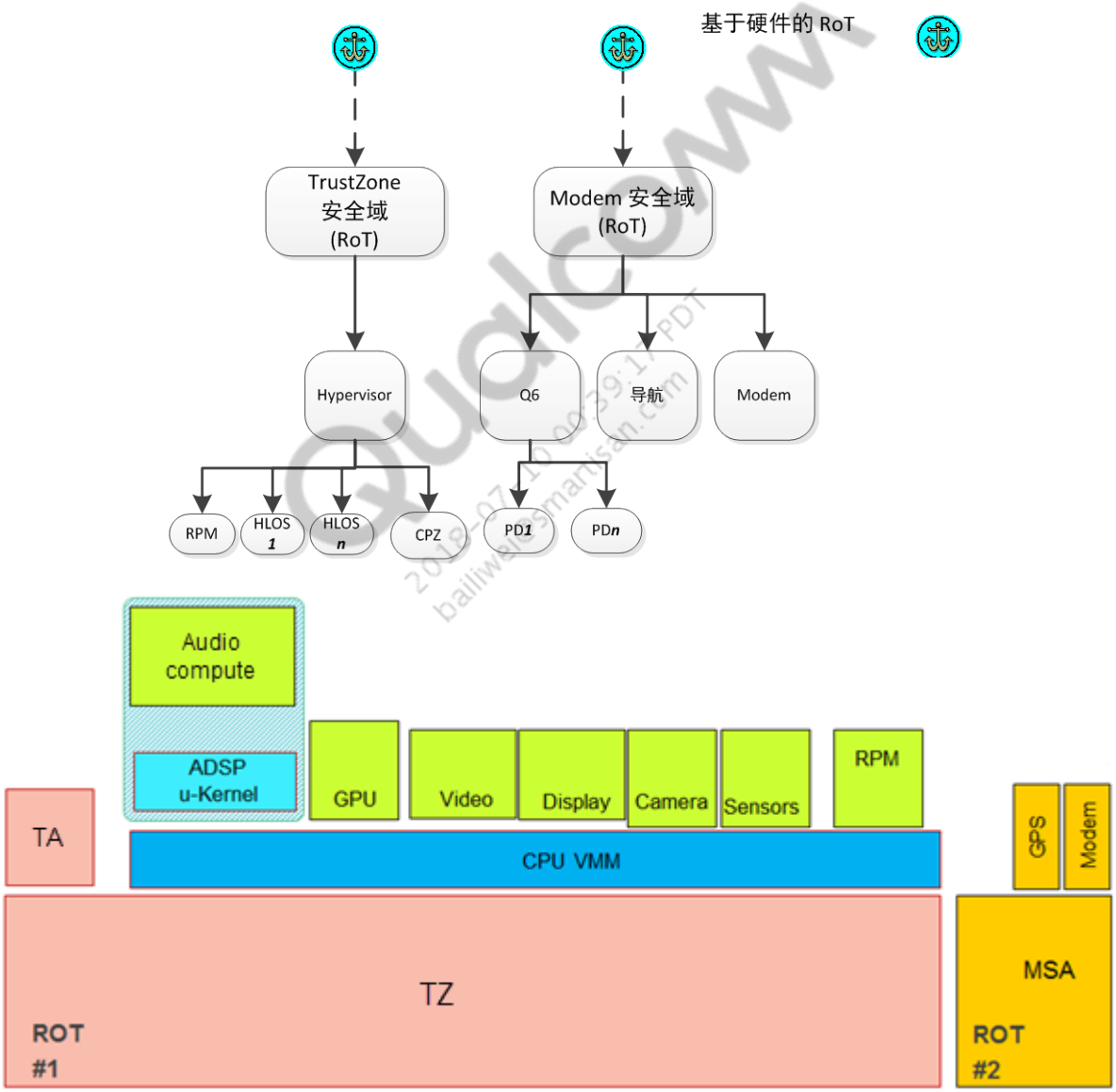
Qualcomm 访问控制概述

- TZ 和 MSA (Modem) 的信任模型相互独立。TZ 和 Modem 管理 xPU，强制实施访问控制策略以管理 Modem 和 TZ 资源
- 持久的安全和访问控制配置
- xPU 提供对寄存器/固定地址/动态存储区域的从侧访问控制
- 通过主侧访问控制实现内容保护的用例
- 对安全域的存储器管理仅限域所有者或信任层级中的创建者来执行
- 在安全域和执行环境中实现动态存储器共享

访问控制域

- 所有权分为三个层级：
  - TZ 管理 TZ 域
  - MSA 管理 MSA Modem 域
  - Hypervisor (EL2) 管理传统非安全域，包括内容保护区 (CPZ)
- TZ 和 MSA 通过 xPU 提供从侧访问控制
- Hypervisor 通过 MMU 在第 2 阶段页表中配置主侧访问控制
- 需要将系统资源拆分为通用的 4 KB 大小

访问控制 – 信任层级和安全域

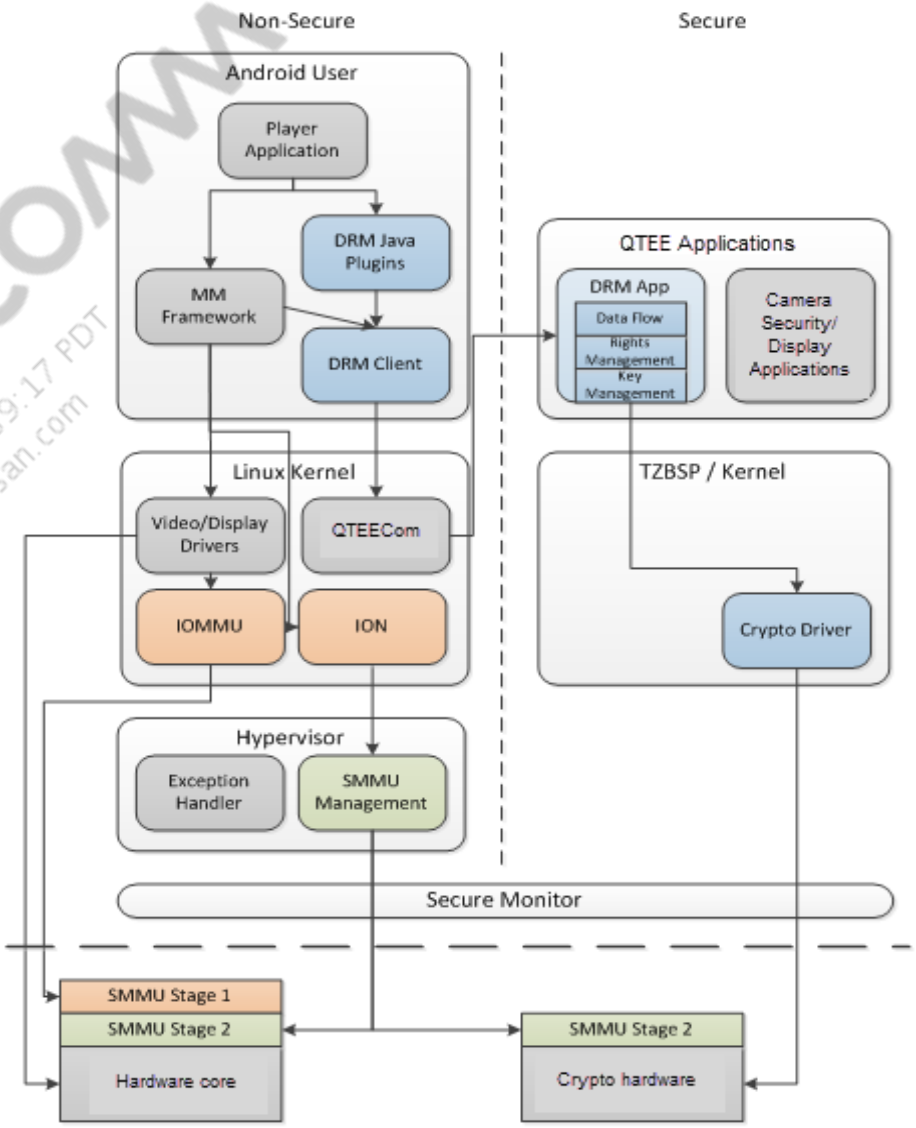


系统 MMU

- Hypervisor 管理第 2 阶段 MMU 和系统存储器管理单元 (SMMU)，以强制执行保护虚拟机 (VM) 中资源的策略
- HLOS 内核管理第 1 阶段 MMU 和 SMMU，以强制执行保护以用户权限层级运行的应用程序中资源的策略

访问控制 – CPZ

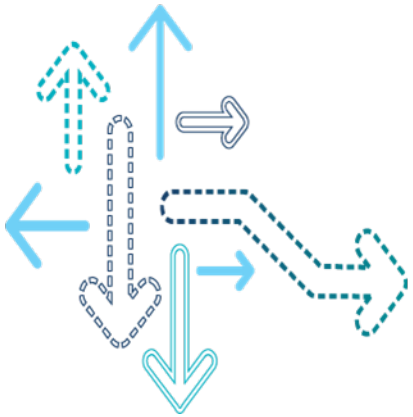
- 主侧内容保护功能
  - 基于主侧访问控制构建
  - 使用 MMU 第 2 阶段控制对受保护缓冲区的访问
  - 驱动程序仍在 HLOS 中
  - MMU 管理在 Hypervisor 中
  - DRM 仍在 TZ 中
- 主要优势
  - 动态分配缓冲区，缓冲区都不是预先分配好的
  - 调整为较大的存储器大小



安全外设映像加载

- 启动过程中，Hypervisor 会保护子系统起始地址、重新映射寄存器并复位控制
- 在 HLOS 内核中实现的 PIL 驱动程序会将映像加载到 DDR 中并调用到 Hypervisor 中
- 安全 PIL 调用会在 Hypervisor 中捕获，并会转发到 TZ 进行映像鉴权
- Hypervisor 更新 MMU 第 2 阶段以保护映像，HLOS 不再可访问映像
- Modem PIL 由 Modem 启动鉴权程序 (MBA) 映像处理

pIMEM

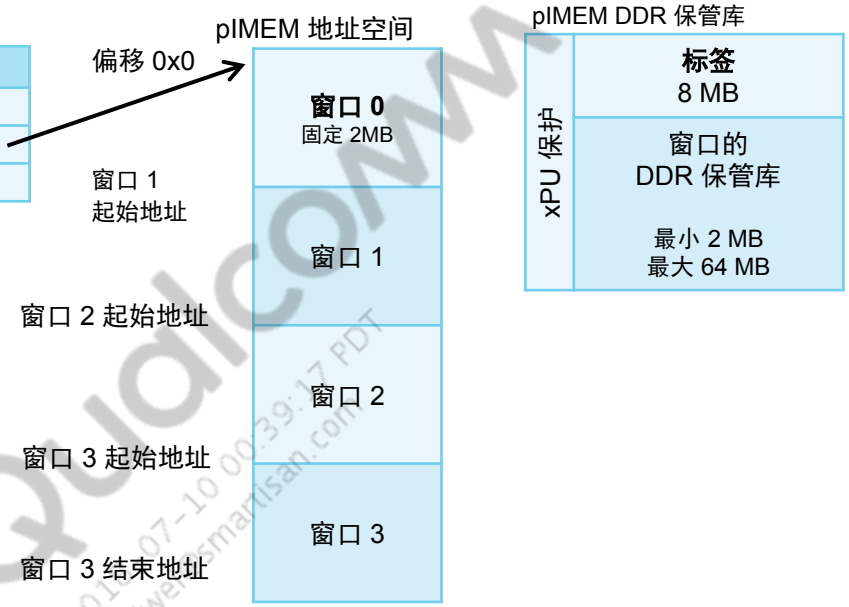


pIMEM DDR 保管库

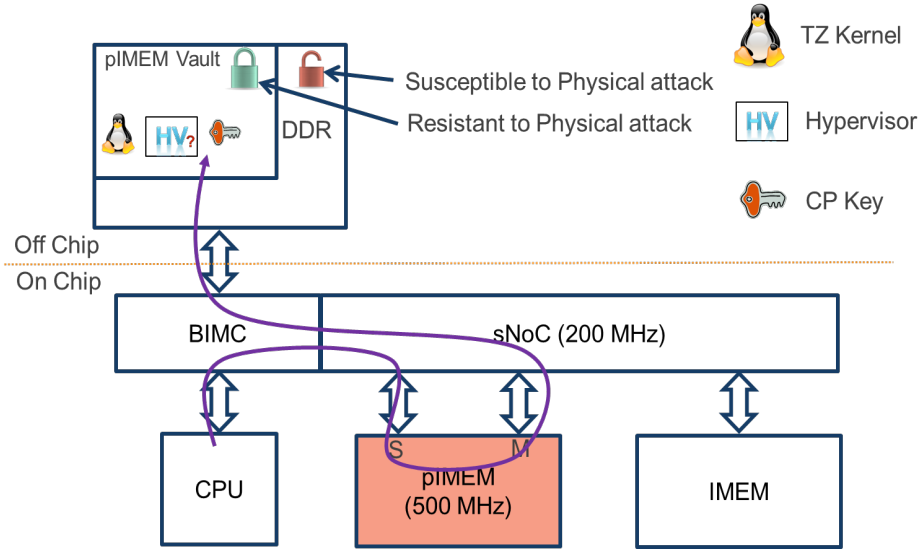
- pIMEM 即伪 IMEM，由 DDR 中的安全区域提供支持
- 读取/写入操作通过加密硬件完成
- 发展动因
  - 因进行 64 位迁移而增大 TZ 内核映像的大小
  - 提供额外存储区实现 OEM 专属功能
  - 在防御物理攻击的存储器中运行 TZ 应用程序（例如 DRM）
  - DDR 易受物理攻击

pIMEM – 架构

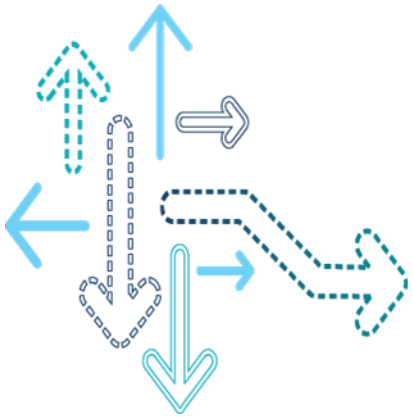
起始地址	结束地址	大小	备注
180000000	27FFFFFFF	4 GB	DDR
80000000	17FFFFFFF	4 GB	DDR
1C000000	1FFFFFFF	64 MB	pIMEM



- 与 pIMEM 相关的加密操作在硬件模块中执行
- pIMEM 通过 QSB 主端口和从端口连接至系统 NoC



加密



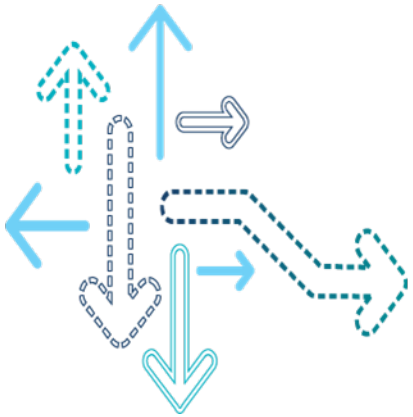
加密实现

- QTI 加密核心提供在设备硬件中实现的加密算法
  - 提供基于寄存器的访问
  - 包括：AES、三重 DES 和 SHA
  - 通过 Linux 内核加密驱动程序 (qcrypto) 提供对硬件加密的访问
  - QTEE 向受信任应用程序提供加密 API (qsee_SW_Cipher_*)
- ARMv8-A 加密扩展指令通过 HLOS 内核配置启用
- PRNG 和加密硬件模块已通过联邦信息处理标准 (FIPS) 140-2 认证

内嵌加密引擎

- 内嵌加密引擎 3.0 (ICE 3.0) 旨在对存储数据进行高吞吐量加密
- 支持 AES 128/256 ECB/XTS
- 支持多个加密流，可满足高吞吐量要求
- 每个加密流对应多个 AES 核心
- 32 个软件可配置密钥
- 非对称和对称运算

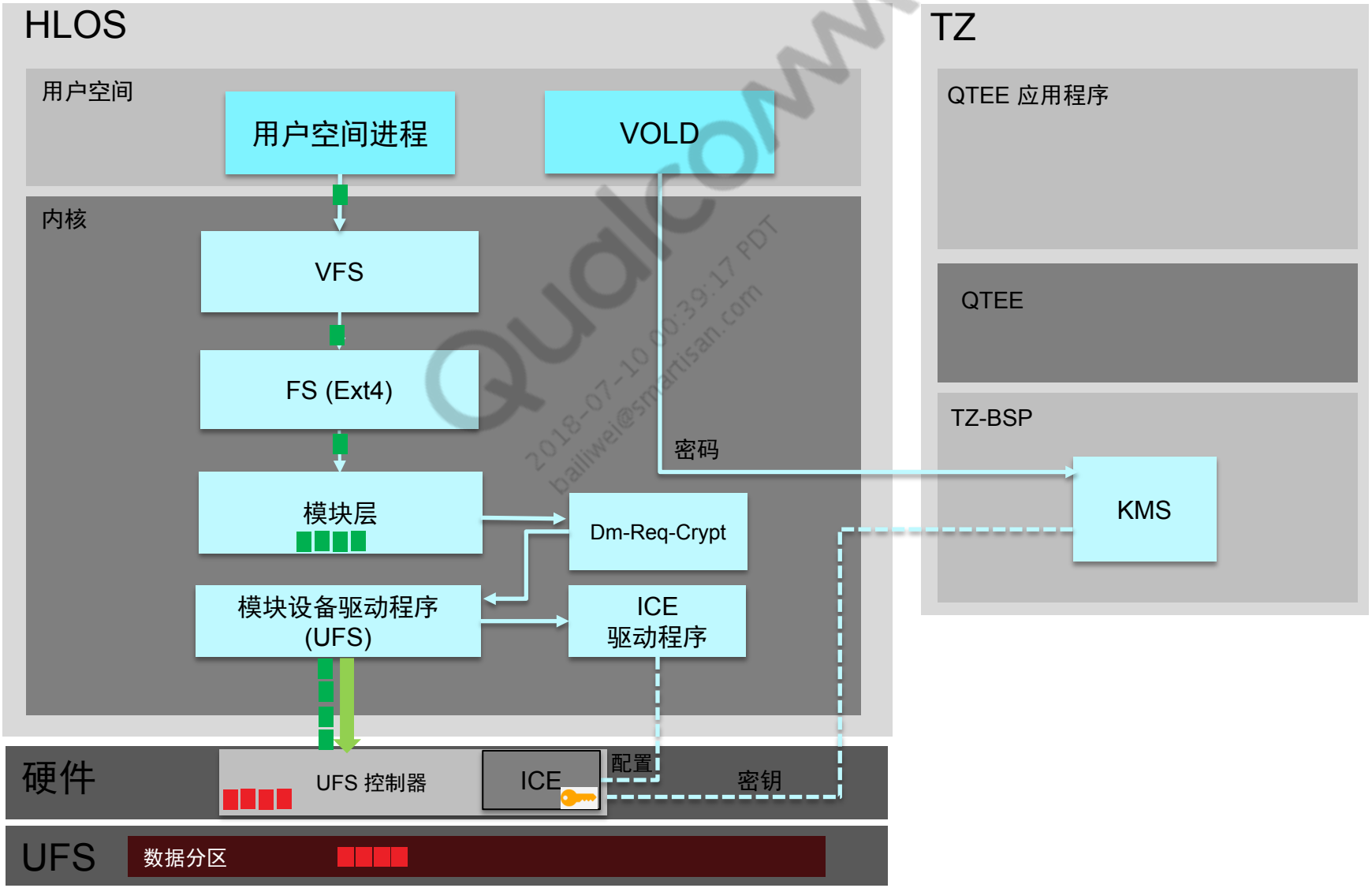
HLOS 安全



ICE – 全磁盘加密

- Android 提供基于软件的机制，通过磁盘加密保护用户数据
- 目前支持加密用户数据分区以及任何不可插拔 SD 卡，不对任何其他分区提供加密功能
- Android 磁盘加密基于 dm-crypt linux 内核模块
- 它使用内核的映射设备功能，在模块层级工作
- QTI 开发的 ICE 可显著提升加密吞吐量
- 凭借基于硬件的解决方案，ICE 具有以下优势：
  - 性能更佳
  - 通过硬件加密降低功耗
  - 由于加密密钥并不存储于 RAM 中，因此黑客无法进行转储，从而提升了安全性
- Android 支持新增的无 PIN 码和强制加密功能

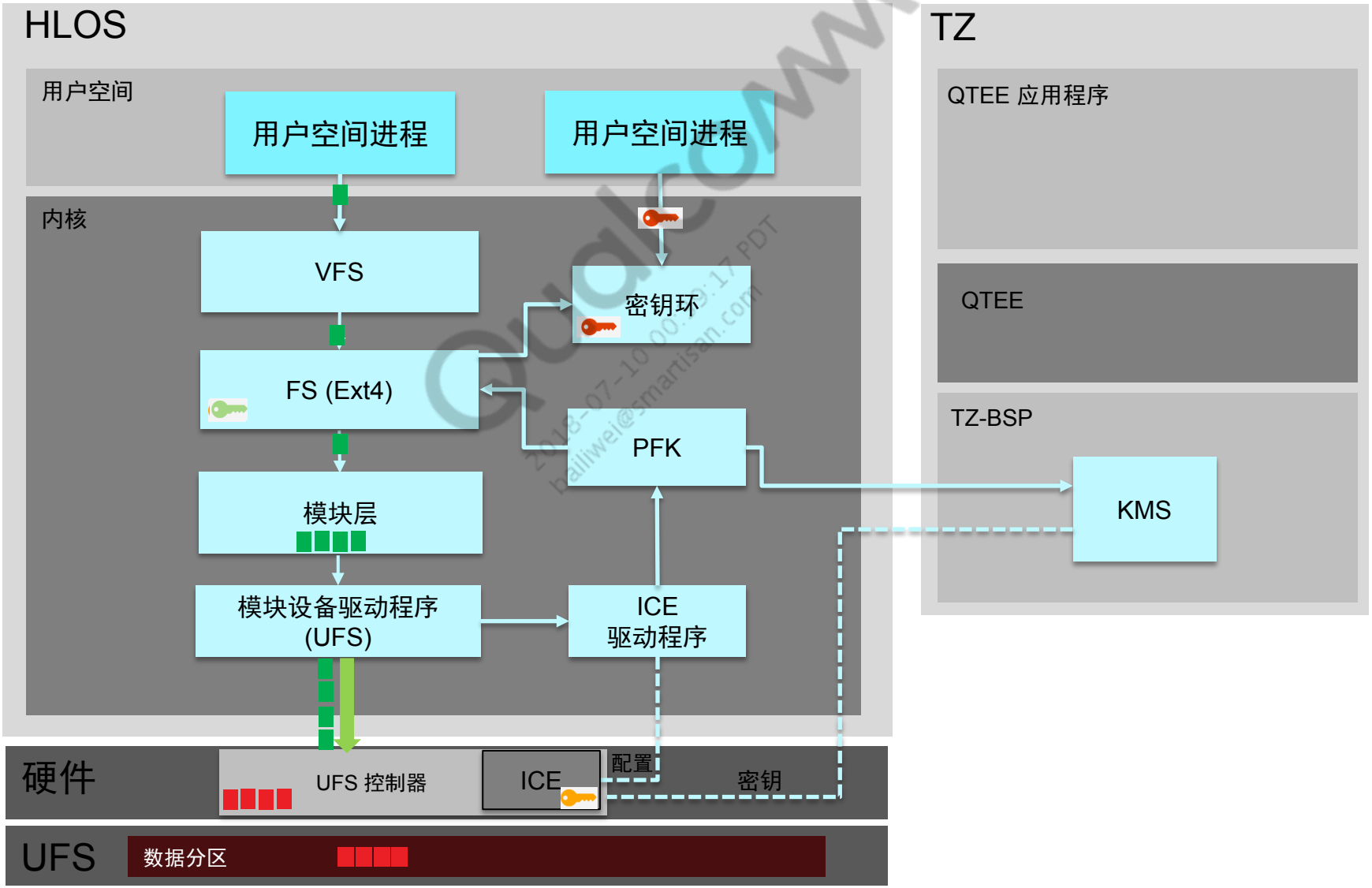
基于硬件的 FDE 解决方案



ICE – 文件级加密

- 文件级加密 (FBE/ext4Crypt)
  - 每个文件都采用不同密钥进行加密
  - 能够以更高的粒度进行区分 – 用户/组/文件
- 每个文件都有唯一的加密密钥
- ext4 级 FBE – ext4Crypt
- 文件名称加密
- FEK 存储在 xattr 中
- 主密钥
  - 与用户凭据一同使用
  - 加密 FEK
  - 存储在密钥环中

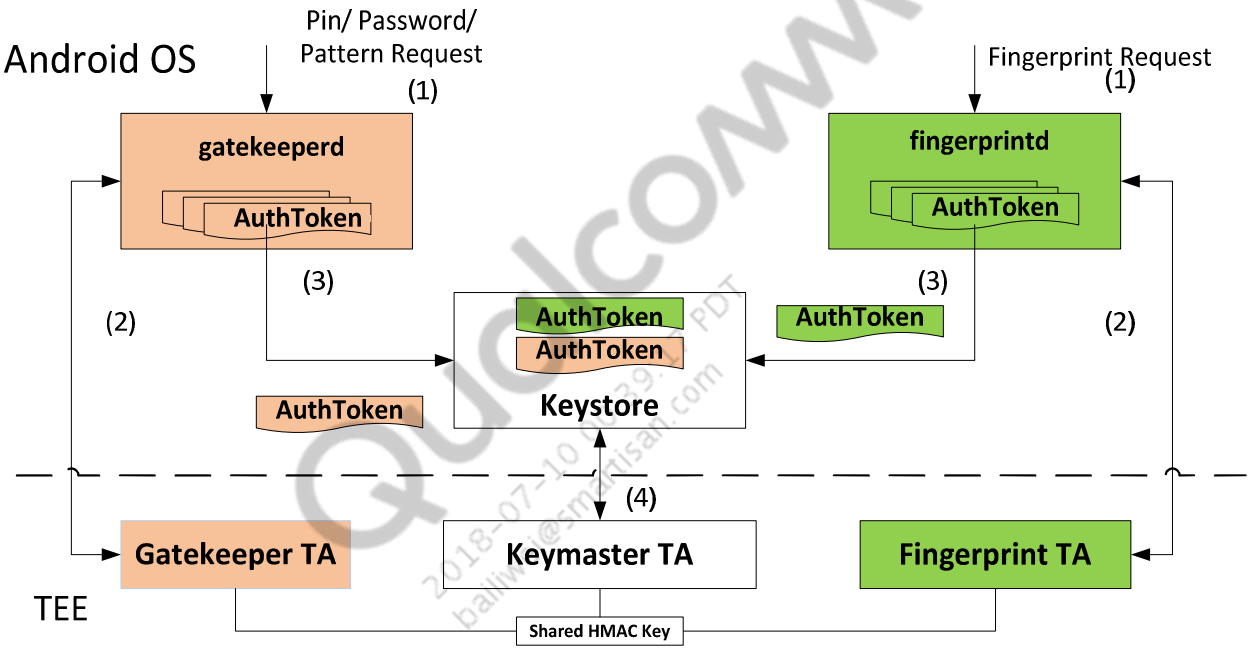
基于硬件的 FBE 解决方案



基于硬件的 Keymaster 和 Keystore

- 使用 TZ 应用程序 API，确保存储的密钥数据不可通过 HLOS 进行访问
- 目前仅支持 RSA 密钥类型
- 生成的 keyblob 通过仅可由 TZ 访问的密钥进行加密并存储于 HLOS 端的文件系统 (FS) 中
- HLOS 组件包括实现 keymaster.h 中定义的 Keymaster API：
  - generate_keypair
  - import_keypair
  - get_keypair_public
  - delete_keypair
  - delete_all
  - sign_data
  - verify_data
- 每个 API 都会调用到 TZ 中处理请求
- TZ 组件包括 keymaster T 应用程序，该应用程序会实现 API，并在 TX 映像编译中以分离二进制映像的形式生成
- OEM 可确定 tzbsp_keystore_enable_rpmb() API 更新后是否对 keystore 使用 RPMB 防回滚支持

Keymaster、Gatekeeper 和 Fingerprint 进程



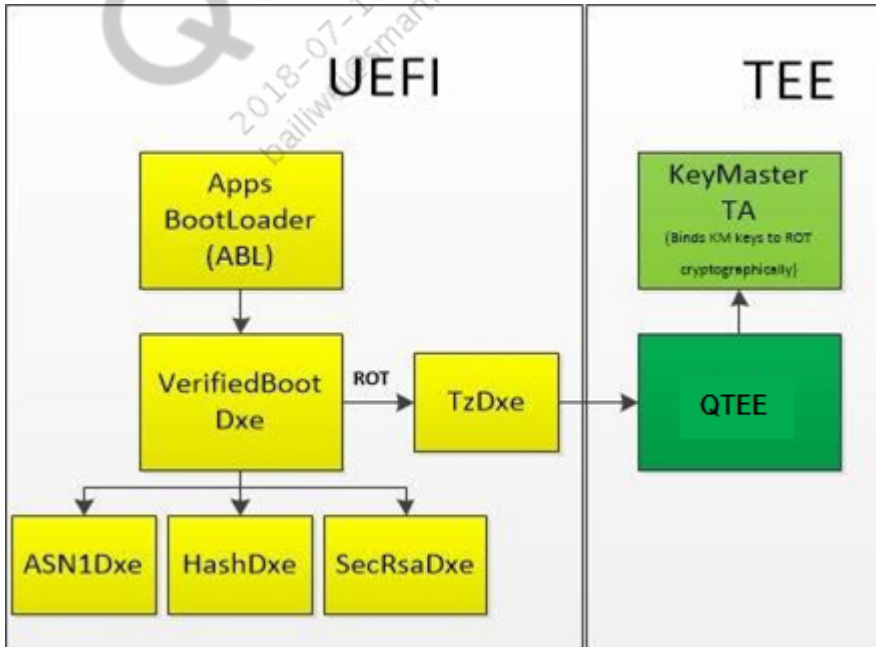
- 通过鉴权的令牌在针对用户进行鉴权时由 Gatekeeper 创建
- 共享（Keymaster、Gatekeeper 或 Fingerprint 受信任应用程序）哈希消息验证码 (HMAC) 密钥用于对 AuthToken 签名

Keymaster 3.0

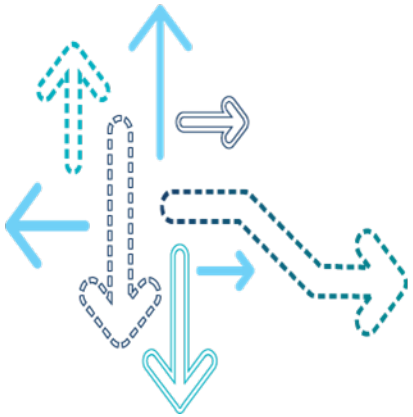
- 符合新的 HIDL HAL
- 新增证明和设备 ID 证明功能
- 设备 ID 证明：TEE 可通过以下隐私限制证明序列号、IMEI、MEID、品牌、设备、产品、制造商或型号：
  - 调用者必须提供正确值才能获得证明
  - 该功能可由用户永久禁用
  - 调用者无法区分用户禁用与数值错误
  - 功能仅供有权限的应用程序访问
- CDD 要求
  - Android O 中强制为新设备启用具有证明功能的 KM 3.0
  - 可选择设备 ID 扩展
- 升级
  - 可继续使用 KM 1.5 或 2.0
  - 如果集成 KM 3.0，需要对使用 KM 1.5 或 2.0 的设备上配置的证明密钥进行重新配置
  - OEM 应计划擦除用户数据

验证启动

- 基于 UEFI 的实现
- 包括 ABL 和 XBL 代码
- 在 ABL 中，BootLib 调用在 XBL 中实现的 API（VerifiedBootDxe 驱动程序）来执行映像验证
- EFIVerifiedBoot.h 头文件提供可供 ABL 使用的 API 原型
- 验证启动状态存储在 RPMB 中

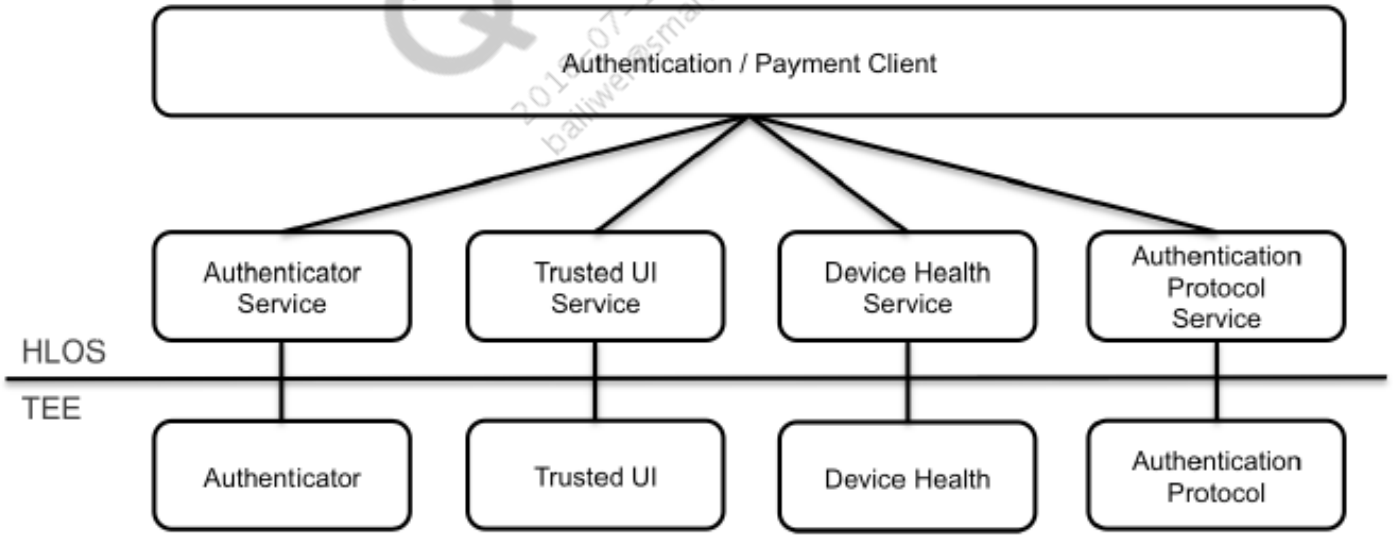


鉴权框架



鉴权框架概述

- 受信任 UI
- 安全支付
- 摄像头安全
- Qualcomm 恶意软件检测



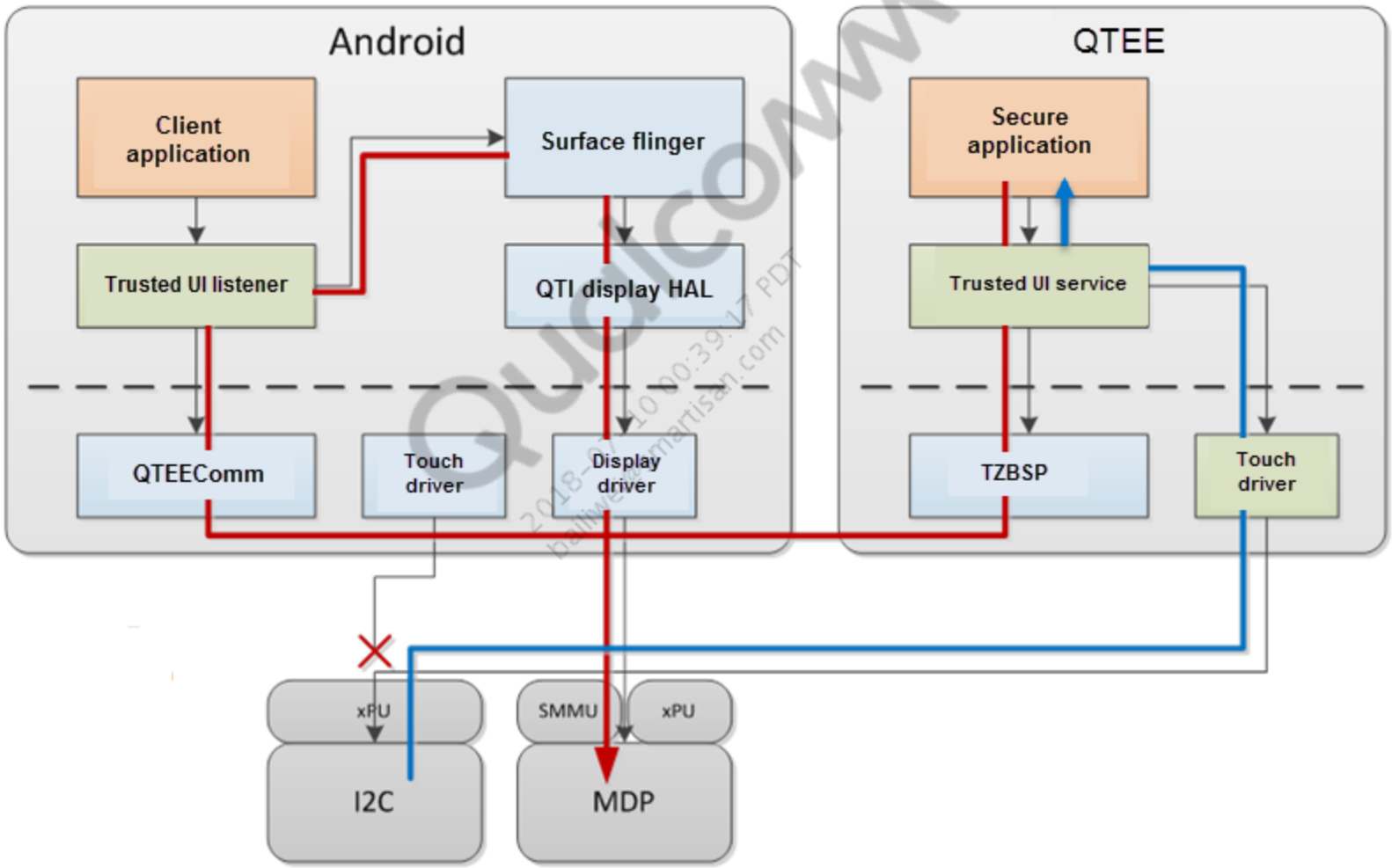
鉴权框架软件架构

- 鉴权框架由对 Android 操作系统 Java 层开放的多项服务组成
- 已通过鉴权的受信任 UI 和补充数据服务
  - IAuthenticator 服务 – 通用鉴权程序接口，支持通过 HLOS 用户验证令牌 (UVT) 路由进行用户验证
  - IAuthenticator2 服务 – 通用鉴权程序接口，支持通过 TEE UVT 路由进行用户验证
  - 受信任 UI 服务 – 用于交易确认的受信任用户接口服务
  - 设备健康服务 – 补充数据服务，用于报告设备健康指标
- 鉴权协议服务
  - FIDOCrypto 服务 – 支持线上快速身份验证 (FIDO) 通用鉴权框架 (UAF) 1.0 加密协议
  - FIDOCryptov2 服务 – 支持 FIDO UAF 1.0 加密协议、支持补充数据和受信任位置、支持使用受信任 UI 的交易确认

受信任 UI

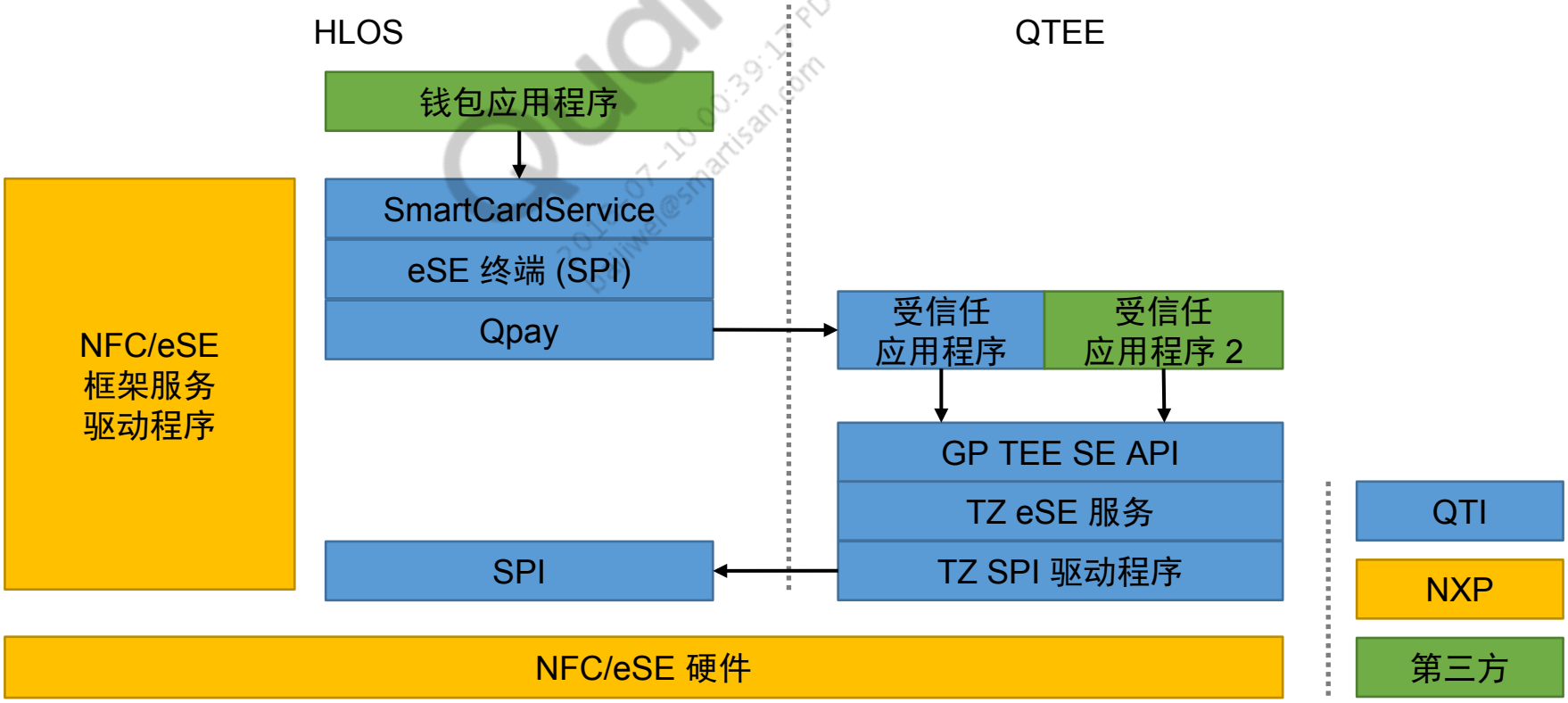
- 受信任 UI 系统功能允许 QTEE 安全应用程序向终端用户显示安全用户接口
- 显示内容和触控输入不受操作系统干扰
- 典型用例包括银行和安全密码输入、存储及验证
- 无法与安全摄像头同时使用

受信任 UI 框图



安全支付

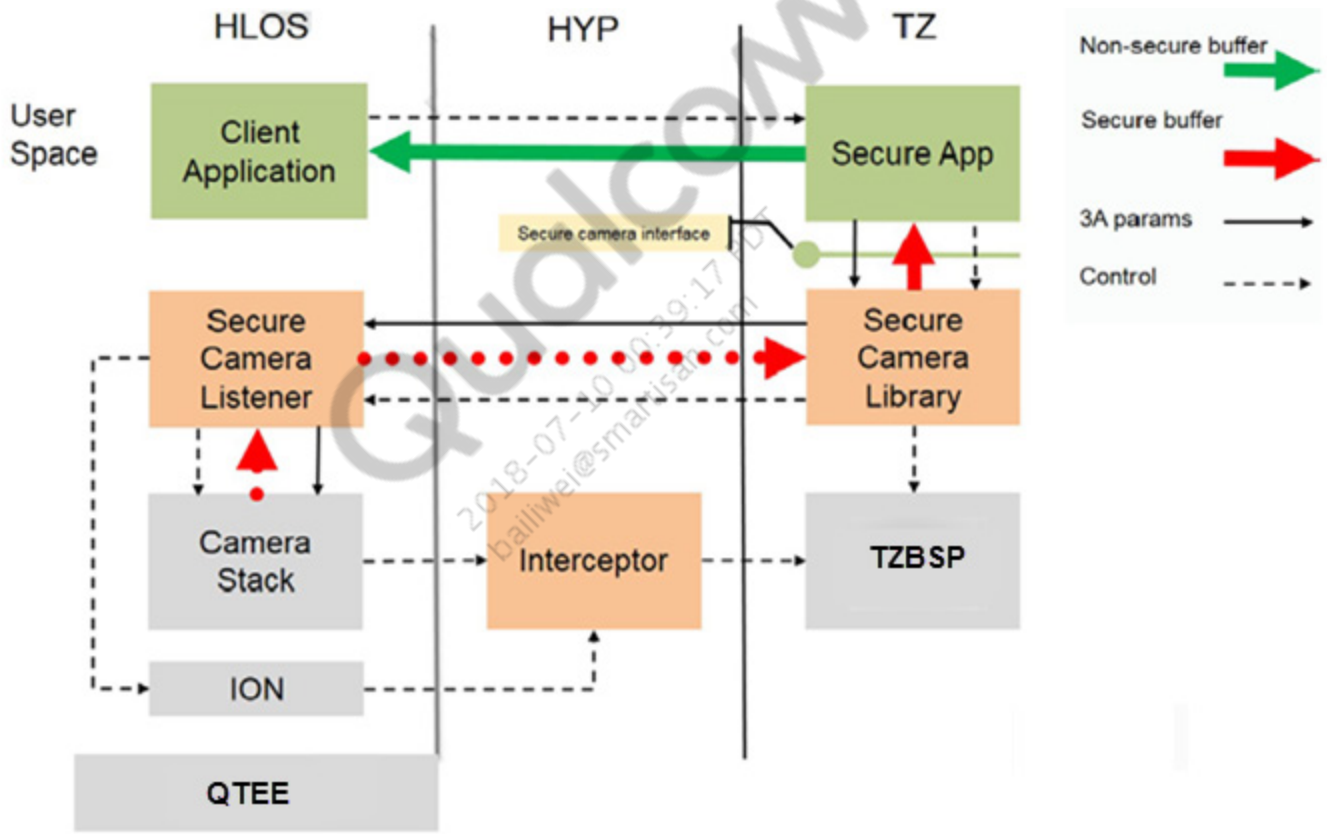
- 安全支付 (Qpay) 这一交易服务可通过 NFC 功能为几乎所有收款人或服务提供商提供功能强大的支付处理解决方案
- 集成 NFC/eSE 解决方案 NQxxx
- 具有 NFC 功能的手机包含以下组件：



摄像头安全

- 基于硬件的鉴权功能可利用基于摄像头的生物特征防止映像数据遭到恶意软件攻击
- 基于人眼的鉴权可使用安全摄像头提供强大的安全功能，专为保护摄像头与处理器之间的链接而设计
- 生物特征鉴权的安全级别仅与用于采集生物特征数据的物理输入和传感器的安全级别一样高
- 将接收到的数据与摄像头隔离，并将数据安全地存储在硬件中，防止不可信应用程序和进程访问
- 设计为仅允许相应人员访问设备安全信息，帮助通过受保护的鉴权方法进行支付及执行安全交易

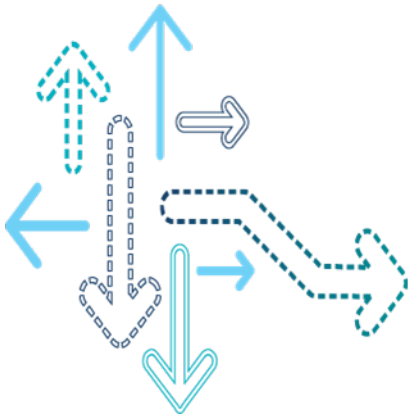
摄像头安全框图



Qualcomm 恶意软件检测

- 利用高级机器学习和物理存储器扫描来识别零延迟过渡型恶意软件和隐藏程序的智能恶意软件检测
- 恶意软件检测占用最少的 CPU 负荷在设备上执行实时监测，以针对已知和未知恶意软件变型提供通过实践验证的极佳检测结果
- 设备提供的恶意软件保护基于应用程序行为来监测设备健康状况并发出警告
- 分析是由在软件 OS 之外运行的安全应用程序来执行
- 设备健康 dhsecapp 受信任应用程序

内容保护



内容保护概述

- 内容保护是保护收费视频内容的解决方案
- 利用 Qualcomm® Processor Security（以前称为 SecureMSM）技术在硬件中提供的强大安全基础
- 获得主要内容工作室批准
- 多 DRM 支持业内使用最为广泛的内容保护解决方案，包括 PlayReady、Widevine、HDCP 2.x 和 ISDB-T 全频段
- 端对端保护
  - 所有视频流（压缩和未压缩格式）均受到保护
  - DRM 协议栈在安全执行环境中运行
  - DRM 密钥受到硬件安全存储的保护
- 预集成
  - 在 Qualcomm® 嵌入式平台芯片组上预先集成完善的解决方案
- 自主安全
  - 不依赖于 HLOS 安全
  - 不受 HLOS 超级用户权限或攻击影响
  - 不受用户所安装恶意软件的影响

参考资料

标题	文档号
Qualcomm Technologies, Inc.	
Security Software Master Document	80-PA692-1
TZ.XF.5.0 TrustZone Architecture Overview	80-P9301-28
Qualcomm Android Security Features	80-NU861-1
QSSP Device Health Overview	80-P3992-1
Qualcomm Secure Execution Environment Version 2.4 SFS Application Note	80-NM249-1
Authentication Framework Overview	80-NU395-1
QPAY Integration Overview	80-P7202-15
Secure FIDO 2 Authenticator Overview	80-P4935-1
Secure Camera Library API	80-P2888-1

参考资料（续）

缩略词或术语	定义
EL	ARM 异常等级 (ARM Exception Level)
FIPS	联邦信息处理标准 (Federal Information Processing Standards)
HAL	硬件抽象层 (Hardware Abstraction Layer)
HLOS	高级操作系统 (High-Level Operating System)
ICE	内嵌加密引擎 (Inline Crypto Engine)
KM	Keymaster
PBL	主启动加载程序 (Primary Boot Loader)
QSEE	Qualcomm 安全执行环境 (Qualcomm Secure Execution Environment)
QTEE	Qualcomm 受信任执行环境 (Qualcomm Trusted Execution Environment)
RoT	信任根 (Root of Trust)
RPMB	回放保护内存模块 (Replay Protected Memory Block)
SFS	安全文件系统 (Secure file system)
TA	受信任应用程序 (Trusted Application)
TZ	ARM TrustZone
TZBSP	TrustZone 板支持包 (TrustZone board support package)
XBL	启动加载程序 (Boot Loader)

问题？

https://createpoint.qti.qualcomm.com