安全快速入门

启用安全功能时需要考虑以下因素：

- 安全启动
- 平台安全（Qualcomm 受信任执行环境 (QTEE)、TrustZone 安全应用程序及 Hypervisor）
- HLOS 安全（SELinux、FDE/FBE、Keymaster、验证启动）
- 内容保护（PlayReady、Widevine、DRM 及 HDCP）
- 生物特征识别（指纹、安全摄像头）

主要工作

- ❑ 审核安全功能
- ❑ 配置和熔断安全熔丝
- ❑ 为映像签名
- ❑ 调试安全设备
- ❑ 映射安全外设
- ❑ 配置密钥
- ❑ 开发/集成安全应用
- ❑ 配置 HLOS 安全
- ❑ 运行认证测试集

工作	工作子项	资源	产品阶段							
			评估	设计	编译	系统调通	集成	验证	认证	制造
审核安全功能	审核安全功能和发布计划	安全概述* 软件发布计划*	•							
	审核功能定义和性能指标	80-P9301-70 Design Review Questionnaire	•							
配置和熔断安全熔丝	评估熔丝配置	熔丝配置* 启用安全启动*	•	•						
	熔断工程机和量产机上的熔丝	80-NM248-3 Fuse Blowing				•				•
为映像签名	创建本地密钥对进行签名，或使用 QTI 根	启用安全启动*			•	•				
	验证签名工具	80-NM248-1 Image Signing			•	•				
	为生产映像签名					•	•			•
调试安全设备	在工程机上启用调试策略	80-NV396-72 Debug Policy Overview				•	•			
	验证安全调试	80-NM248-6 Debug Policy Tool						•		
映射安全外设	为 SPI、UART、I2C 设备配置模式和所有权	外设概述*				•				
配置密钥	配置存储密钥 (RPMB)	80-P8327-1 RPMB Security				•				•
	配置 DRM 密钥（Widevine、PlayReady、HDCP）	80-P1824-1 Provisioning Encryption Tool 80-N9124-1 DRM Key Provisioning 80-NM248-5 Encryption Key Provisioning 80-N3279-1 PlayReady DRM User Guide 80-N9340-1 Widevine DRM								•
	配置 HLOS 密钥（Keymaster、Verity）	80-NU861-1 Android Security Features								•
开发/集成安全应用	审核 QTEE API、编译环境和安全应用指南	QTEE 用户指南*		•	•					
	指纹	80-NV103-1 3rd Party Fingerprint Integration		•	•	•	•	•		
	安全摄像头	80-P2888-5 Secure Camera User Guide		•	•	•	•	•		
	支付	80-P7202-15 QPay Integration		•	•	•	•	•		
	DRM（Widevine，PlayReady）	80-N9340-1 Widevine DRM 80-N3279-1 PlayReady DRM User Guide		•	•	•	•	•		
配置 HLOS 安全	FDE、FBE、SELinux 策略	80-NU861-1 Android Security Features		•	•	•	•	•		
运行测试集	运行 CAVP、FIPS、GTS、CTS、VTS 认证测试	80-NR875-6 FIPS Compliant Modules						•	•	

* 参见芯片特定的文档

芯片特定的文档

	SDM630/ SDM660	SDM636	SDM670/ SDM710	SDM845	SM6150	SM8150
安全概述	80-P2484-65	80-P2484-65	80-PD126-3	80-P9301-27	80-PG596-40	80-PF777-12
软件发布计划/功能规范	80-P8754-61	80-PD860-1	80-PD126-29	80-P9301-87	80-PG596-1	80-PF777-2
熔丝配置（QFPROM 编程参考指南）	80-P7865-97 80-P7747-97	80-PD860-97	80-PB873-97	80-P6348-97	80-PG427-97	80-PD867-97
启用安全启动	80-P8754-68	80-P8754-68	80-PD126-20	80-P9301-4	80-PG596-42	80-PF777-9
外设概述	80-P8754-4	80-P8754-4	80-PD126-5	80-P9301-19	80-PG596-21	80-PF777-6
QTEE 用户指南	80-NH537-2	80-NH537-2	80-NH537-4	80-NH537-4	80-NH537-4	80-NH537-4

工具

工具	用途	资源
SecImage	提供用于映像签名的服务	Sectools：SecImage Tool User Guide (80-NM248-1)
FuseBlowing	用于配置和生成熔丝熔断数据	Sectools：FuseBlower Tool User Guide (80-NM248-3)
DebugPolicy	在安全设备上启用调试	Sectools：Debug Policy User Guide (80-NM248-6)
KeyProvision	提供安全服务，用于启用和配置加密密钥	Sectools：KeyProvision Tool User Guide (80-NM248-5)
CASS	在线签名系统	CASS 用户指南 •Windows (80-N7185-3) •Linux (80-N7185-4)

提示

- 使用三种证书进行映像鉴权和签名 – 根 CA、证明 CA 和证明
- RSAPSS、SHA256/Exp 65537 是为映像签名的首选方法。不再支持 PKCS
- sampleapp 源代码示例非常适合作为开发定制安全应用的出发点
- 在 QTEE 5 中，通过应用元数据文件配置用于安全应用的堆和堆栈内存大小
- 内联加密引擎为 Android 全磁盘加密和基于文件的加密提供优化性能
- 独立安全处理器子系统 (SPU) 为 Keymaster 操作提供增强安全功能

请求支持

1. **在 Salesforce 用例管理系统中创建支持请求：**https://createpoint.qti.qualcomm.com。
2. **为安全相关问题选择以下问题区域 (PA) 代码：**
   - 问题区域 1 (PA1) – BSP/HLOS
   - 问题区域 2 (PA2) – 安全
3. **提供关于问题的详细说明。**务必包含以下信息：
   - 转储及与转储匹配的符号文件（vmlinux、TrustZone 和 ELF 文件）
   - 测试场景、问题的出现频率，以及是否能够复现
   - 首次上报问题时的软件编译信息

联系我们

欢迎访问网站 https://createpoint.qti.qualcomm.com。

如对本文档存在任何问题或建议，可通过电子邮件发送至：DocFeedback@qti.qualcomm.com。

Qualcomm Technologies, Inc.