电 信 终 端 产 业 协 会 标 准

TAF-WG4-AS0008-V1.0.0:2017

移动终端安全环境安全评估内容和方法

mobile terminal trusted environment evaluation content and method

2017-05-18 发布　　2017-05-30 实施

电信终端产业协会　　发 布

目 次

前　　言

本标准按照 GB/T 1.1-2009给出的规则起草。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院(工业和信息化部电信研究院)、深圳市纽创信安科技开发有限公司。

本标准主要起草人：国炜、樊俊锋、焦四辈、王宗岳、朱凯、刘峥。

引　　言

随着移动终端市场的日益成熟和发展，安全问题逐渐成为人们关注的焦点。 终端用户在他们的智能终端上装载了各种各样的应用，于是在开放环境下，安全需求激增。存储安全、连接安全、移动支付这些问题都引发了人们对安全的关注。近年来，以硬件和软件为依托提供的安全解决方案日益成为了行业内的焦点，如可信执行环境（TEE）是以终端硬件提供的安全能力为依托，基于微内核OS向应用提供各种安全服务。为了保证TEE平台具备可靠的安全能力， YD/T2844《移动终端可信环境技术要求》系列标准定义了可信执行环境（TEE）平台所应具备的安全功能和要求，为行业提供了有价值的安全解决方案参考作用。

本标准基于YD/T2844系列标准规定的安全功能要求制定其相应的安全评估方法。

移动终端安全环境安全评估内容和方法

1 范围

本文档规定了移动终端安全环境的评估方法，原则上仅在论坛内部使用，为论坛开展移动终端安全环境评估提供技术依据，安全评估分为两个步骤：脆弱性分析和渗透性测试。本文档是评估实验室进行脆弱性分析的指南，也可以供认证产品的生产商使用，以便厂商配合实验室进行评估。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 2844.1-2015 移动终端可信环境技术要求 第1部分：总体
YD/T 2844.2-2015 移动终端可信环境技术要求 第2部分：可信执行环境
YD/T 2844.3-2015 移动终端可信环境技术要求 第3部分：安全存储
YD/T 2844.4-2015 移动终端可信环境技术要求 第4部分：操作系统的安全保护
YD/T 2844.5-2016 移动终端可信环境技术要求 第5部分：与输入输出设备的安全交互

3 术语、定义和缩略语

3.1 缩略语

CA	Client Application	客户端应用
REE	Rich Execution Environment	富执行环境
RIC	Runtime Integrity Checking	运行时完整性校验
TA	Trusted Application	可信应用
TEE	Trusted Execution Environment	可信执行环境
TOE	Target of Evaluation	评估对象
ST	Security Target	安全目标

4 评估类型和范围

评估所针对的目标产品为内部搭载依托硬件和软件实现的安全解决方案的终端设备。评估的范围包括目标产品用来提供安全环境所必需的安全功能所有相关的硬件、固件和软件部分。所评估的目标产品的形态为SoC或移动终端设备。

5 安全评估内容

将依据以下行业标准所规范的TEE安全功能要求，对目标产品的安全环境进行安全评估。

YD/T 2844.1-2015 移动终端可信环境技术要求 第1部分：总体

YD/T 2844.2-2015 移动终端可信环境技术要求 第2部分：可信执行环境

YD/T 2844.3-2015 移动终端可信环境技术要求 第3部分：安全存储

YD/T 2844.4-2015 移动终端可信环境技术要求 第4部分：操作系统的安全保护

YD/T 2844.5-2016 移动终端可信环境技术要求 第5部分：与输入输出设备的安全交互

6 安全评估流程和方法

6.1 安全评估总体流程

评估移动终端安全环境将遵循以下流程对目标产品进行完整的安全评估。

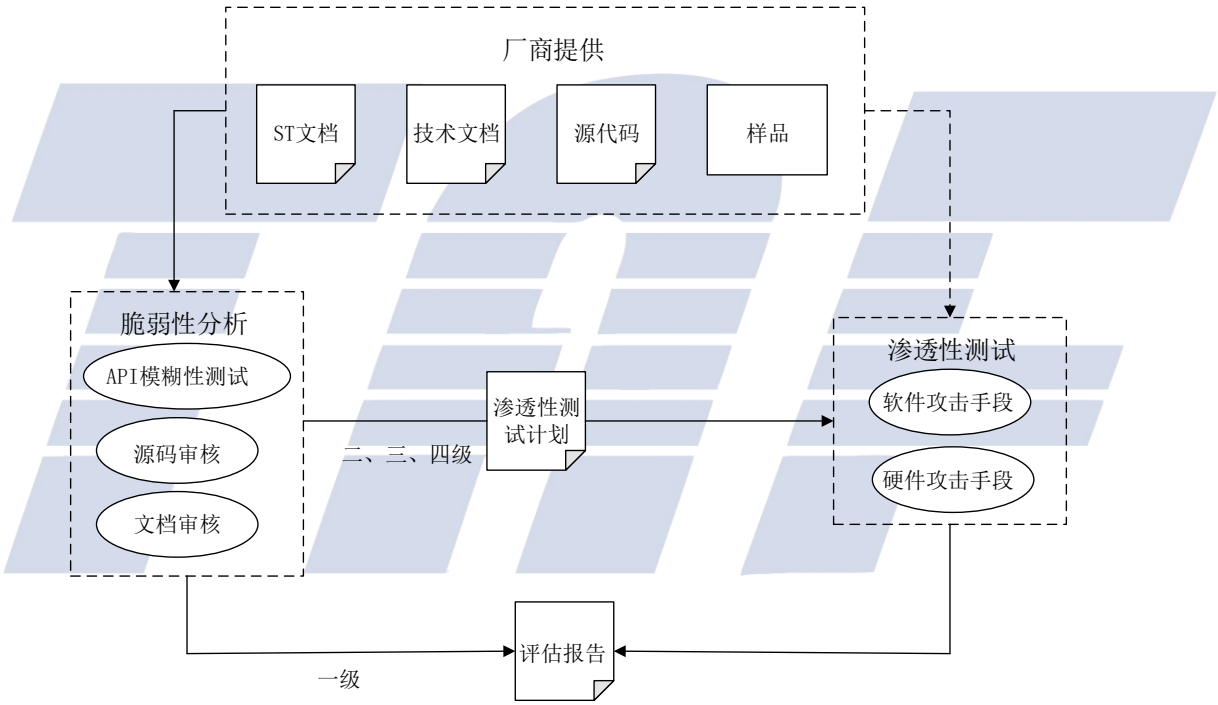

图1 安全评估流程

厂商提交的部分包括ST文档、技术文档、相关源代码和被测样品。具体的文档格式和要求分别详见附录D、E。

脆弱性分析的目标是实验室评估人员根据厂商提交的ST文档，并按照安全功能要求所规定的，对厂商提交的设计文档和相关源码进行初步的方案审核，发现可能的脆弱点和其影响，并由此定义后续渗透性测试的计划和测试例。脆弱性分析的输出作为最终评估报告的一部分。

渗透性测试是实验室根据前期所发现产品的脆弱性，在一定时间内开展对这些脆弱点进行攻击的测试。攻击的手段主要是使用软件攻击和硬件攻击，具体的软、硬件攻击手段详见附录C.

本标准将安全环境的评估等级划分为依次递增的四个安全等级，不同的安全等级将采用不同的安全评估手段并覆盖不同的安全功能要求，详见表一：

一级：依据一级安全功能要求，对厂商提供的文档和相关源码进行审核并结合API接口的模糊性测试分析产品安全漏洞，最终给出评估报告；

二级：依据二级安全功能要求，对厂商提供的文档和相关源码进行审核并结合API接口的模糊测试分析产品安全漏洞，根据安全漏洞设计渗透性测试攻击路径和测试例实施软、硬件的渗透性攻击，最终给出评估报告。

三级：依据三级安全功能要求，对厂商提供的文档和相关源码进行审核并结合API接口的模糊测试分析产品安全漏洞，根据安全漏洞设计渗透性测试攻击路径和测试例实施软、硬件的渗透性攻击，最终给出评估报告。

四级：依据二级安全功能要求，对厂商提供的文档和相关源码进行审核并结合API接口的模糊测试分析产品安全漏洞，根据安全漏洞设计渗透性测试攻击路径和测试例实施软、硬件的渗透性攻击，最终给出评估报告。

注1：软、硬件攻击手段详见附录C。

表 1 移动终端安全环境评级对照表

安全功能		一级	二级	三级	四级
密钥安全	根密钥机密性、完整性、可靠性	文档审阅 API 模糊性测试	文档审阅 API 模糊性测试 渗透性测试	文档审阅 API 模糊性测试 渗透性测试	文档审阅 API 模糊性测试 渗透性测试 基于物理隔离的安全芯片的实现
	公共密钥完整性、可靠性				
	对称密钥和私钥的机密性、完整性、可靠性				
安全启动	安全启动过程的可靠性、完整性	文档审阅 API 模糊性测试	文档审阅 API 模糊性测试 渗透性测试	文档审阅 API 模糊性测试 渗透性测试	文档审阅 API 模糊性测试 渗透性测试
	安全启动代码镜像更新的可靠性、完整性				
	异常处理				
安全存储	存储的机密性、可靠性、一致性、原子性	文档审阅 API 模糊性测试	文档审阅 API 模糊性测试 渗透性测试	文档审阅 API 模糊性测试 渗透性测试	文档审阅 API 模糊性测试 渗透性测试 基于物理隔离的安全芯片的实现
	存储的权限管理				
	存储密钥的生成机制及其机密性、完整性、一致性、原子性				
随机数发	基于硬件的随机数发生器，满足一	文档审阅 API 模糊性	文档审阅 API 模糊性测	文档审阅 API 模糊性测	文档审阅 API 模糊性测试

生器	定的熵值	测试	试 渗透性测试	试 渗透性测试	渗透性测试
TEE 隔离安全	TEE 与 REE 隔离 TEE 与 REE 的通信保护 TEE 与 REE 的通信异常处理	文档审阅 API 模糊性测试	文档审阅 API 模糊性测试 渗透性测试	文档审阅 API 模糊性测试 渗透性测试	文档审阅 API 模糊性测试 渗透性测试
TEE 状态保护	TEE 自身状态机的管理与保护			文档审阅 API 模糊性测试 渗透性测试	文档审阅 API 模糊性测试 渗透性测试
TA 安全管理	TA 的加载、运行、撤销 TA 安装、更新、卸载 TA 间隔离保护 可信用户接口运行时异常状态处理			文档审阅 API 模糊性测试 渗透性测试	文档审阅 API 模糊性测试 渗透性测试

6.2 脆弱性分析

实验室应基于以下内容进行独立的脆弱性分析：

- 通过厂家提供的资料对评估产品具有一定地了解，这一步包括对资料文档（ST文档、产品相关的设计文档或指南）的审核 ，除此之外还包括与厂家TEE开发团队的沟通；
- TEE相关的API接口的一致性和模糊测试；
- 如果厂商可以提供，需要执行对相关源码的审核；
- 在评估范围内，标识出可能存在的脆弱点；

脆弱性分析过程的输出结果作为制定渗透性测试计划的依据，即制定渗透性测试路径以及其测试例。除此之外，在最后的安全评估报告中应包括脆弱性分析，包括：

- 源码审核结论；
- 潜在的脆弱点以及脆弱点分析；
- 渗透性测试路径和测试例；

6.3 渗透性测试

实验室根据脆弱性分析的结果制定渗透性测试路径以及测试例并实施渗透性测试。在安全评估报告中，要提供实施渗透性测试的环境、产品目标的配置和每一个渗透性测试的结果，同时还要具体地描述实施过程中的步骤。

渗透性测试过程中的攻击手段包括软件和硬件攻击，详见附录C。

附 录 A
（资料性附录）
文档编写记录

修订时间	修订后版本号	修订内容
2016.11.29	V0.1	全文格式
2017.3.15	V1.0	重定义评估等级

附 录 B
（资料性附录）
TEE 安全功能要求

B.1 密钥安全要求

安全要求序列号	安全要求描述	对应的安全目标实体
TEE-1	可信执行环境应能根据预定义的密钥生成机制生成或衍生密钥和密钥对。	密码系统
TEE-2	可信执行环境应能根据预定义的密钥销毁机制销毁密钥或密钥对。	密码系统
TEE-3	可信执行环境应能够保证任何私密钥或者安全密钥的完整性。	密码系统
TEE-4	可信执行环境应能够保证任何根密钥存储的完整性和可靠性	密码系统
TEE-5	除非公共密钥被存储在被完整性保护的存储器中，否则在使用这些公共密钥前要验证其完整性和可靠性	密码系统
TEE-6	对私密钥和安全密钥的存储和操作应保护其机密性	密码系统
TEE-7	私密钥和安全密钥的机密性应一直维持到他们被消除。	密码系统
TEE-8	除非私密钥和安全密钥被存储在完整性保护存储器中，否则在使用私密钥和安全密钥前，应验证其完整性	密码系统
TEE-9	任何操作加密密钥的可信执行代码应具有完整性保护，或者在这些代码被授权接入到加密密钥之前应验证其完整性	密码系统

B.2 安全启动功能要求

安全要求序列号	安全要求描述	对应的安全目标实体
TEE-68	在执行其它的安全启动代码前应验证这些代码	初始化进程

	的可靠性和完整性。	
TEE-69	保证安全启动的初始化过程与设备的SoC绑定。	初始化进程
TEE-70	保证执行代码更新应用在安全环境内执行，并在执行前应验证该应用的可靠性和完整性。	初始化进程
TEE-71	应保证安全启动代码更新镜像和安全启动代码列表的完整性和可靠性。	初始化进程
TEE-72	在装载更新的安全启动代码前应验证代码更新镜像的完整性。	初始化进程
TEE-73	如果设备需要回滚到早些版本的安全启动代码更新镜像，那么这个回滚操作必须在当前版本的拥有者授权下才能发生。	初始化进程
TEE-74	如果代码更新镜像安装失败，则代码更新应用必须恢复到安装之前的版本。	初始化进程
TEE-75	在安全启动过程中，如果验证启动代码的完整性失败，则整个启动过程应中止。	初始化进程

B.3 安全存储功能要求

安全要求序列号	安全要求描述	对应的安全目标实体
TEE-55	敏感实体应存储在安全的存储器中； 或者对所保存的敏感实体进行加密存储； 或者将敏感实体保存在SE中。	可信存储
TEE-56	安全存储对敏感实体的操作处理应具有加密和完整性保护机制执行，甚至在敏感实体被转移的过程中还应保证这些	可信存储

	敏感实体的机密性、可靠性、一致性和原子性。	
TEE-57	任何被安全存储的应用级敏感实体应仅被下面用户访问： a) 应用资产管理者； b) 应用资产管理者授权的应用；	可信存储
TEE-58	应用通过调用安全存储来获得应用资产管理者提供的安全存储服务。	可信存储
TEE-59	安全存储的应用资产管理者数据仅仅由应用资产管理者访问。	可信存储
TEE-60	应用资产管理应与TEE应用具有一对一的绑定关系。	可信应用
TEE-61	安全存储的敏感实体由与这些敏感实体相绑定的应用访问。	可信应用
TEE-62	与这些敏感实体相绑定的应用授权其它的可信应用访问其安全存储的敏感实体。	可信应用
TEE-63	安全存储密钥管理机制应保证存储密钥的机密性和完整性。	可信存储
TEE-64	安全存储的密钥管理仅仅由应用资产管理者访问。	可信存储
TEE-65	安全存储中的密钥仅仅由密钥管理者访问和处理。	可信存储
TEE-66	安全存储密钥在被使用前应保证其完整性和可靠性。	可信存储
TEE-67	安全存储的密钥管理机制在对存储的密钥进行操作、存储和转移行为过程中应保证其机密性、完整性、一致性和	可信存储

	原子性。	

B.4 TEE隔离安全要求

安全要求序列号	安全要求描述	对应的安全目标实体
TEE-41	任何负责在TEE和其它EE之间转换或共享资产的机制都应被保护，以防来自管理这些资产的其它EE的攻击。	TEE分离
TEE-42	TEE代码、数据和密钥资产不应被TA所接入到，除非这种接入是根据策略被授权的TA。	TEE分离
TEE-43	在共享资产的情况下，如果资产被从一个TEE分配到另外的EE，那么保存在这些资产内的所有数据在资产被重分配之前进行数据的清除，或者数据以相同的等级继续被保存在TEE中，除非这些数据被转移到这个EE中，同时资产重分配是通过一个被授权的通道完成。	TEE分离
TEE-44	根据安全特性，TEE代码、数据和密钥资产不应被接入到其它EE中，除非这种接入是通过被授权的EE间通信信道。 注：被授权的EE间通信信道可以包含共享资源（如存储）的使用。	TEE分离
TEE-45	当存在通信应用的需求时，TEE应能够保护其内部应用间交换数据的加密和完整性。	TEE分离、TA分离
TEE-46	应可以在两个EE之间建立通信，并且至少其中一个EE是TEE，同时这种通信是被经过授权。 这个授权可以是设备生产商通过配置隐性提供。	执行过程机密性和完整性
TEE-47	运行在不同的EE内的两个对等应用之间的通信信道内，暴露于TEE的交换数据不应被除了这两个对等应用之外的应用所获取。 注：这个需求仅仅针对EE。	执行过程机密性和完整性

TEE-48	如果一个对等的EE或者TEE请求和一个TEE X通信，并且这个TEE X里关系到此通信的代码和/或数据完整性保护失败，这个TEE X应拒绝与对等EE或者TEE通信，如果有可能并通知RIC完整性失败错误处理。	执行过程机密性和完整性
TEE-49	如果一个TEE被通知任何一个敏感应用的代码或数据资产完整性失败，它会将此通知给请求安全通信信道的对等应用，或者拒绝接入到请求安全通信信道的对等应用。	执行过程机密性和完整性
TEE-50	当存在至少两个EE且至少其中一个EE是TEE，一个应用将可能从一个EE发布到对等的TEE内。	TEE分离、TEE数据保护
TEE-51	对于一个EE，除了通过被授权的TEE接口，不能通过任何其其他的机制通信或者操作一个TEE。	TEE数据保护、执行过程机密性和完整性
TEE-52	当存在至少两个EE且至少其中一个EE是TEE，将可能出发从TEE发布一个应用到对等的EE。	TEE分离、TEE数据保护
TEE-53	任何开放的TEE要能直接或者通过其它的EE与UICC通信。	TEE分离、TEE运行
TEE-54	任何TEE可以直接或者通过其它的EE与UICC通信。	TEE分离、TEE运行

B.5 TEE安全管理要求

安全要求序列号	安全要求描述	对应的安全目标实体
TEE-14	可信执行环境应能提供存储和恢复设备唯一标识的机制。	设备标识
TEE-15	TEE应能够针对来自REE或者TA引起的异常状态的保护机制。	回滚保护
TEE-16	TEE应能够检查并处理来自REE或者TA的可信服务请求。	TEE运行、TA身份识别、TEE分离、TA分离
TEE-17	TEE应能够管理它自己的状态机并能够拒绝在当前状态下不期望的操作。	TEE初始化进程、TEE运行
TEE-18	开放的可信执行环境应为应用提供接入一个GBA的能力。	TEE运行

	注：GBA详细架构说明参见YD/T XXXX-XXXX。	
TEE-19	TEE内随机数的产生应结合硬件机制	随机数发生器
TEE-35	需要完整性和可靠性的可信执行环境代码、数据和密钥在使用前应被验证，除非这些资产被存储在至少具有完整性和可靠性的存储器中。	初始化进程、执行过程机密性和完整性、TEE固件完整性
TEE-36	TEE应保证其永久数据的可靠性、一致性和机密性。	TEE数据保护
TEE-37	TEE应保护TEE固件不被非授权的修改。	TEE固件完整性
TEE-38	TEE应提供固件的安全升级策略，以便保证固件最新版本的使用。	TEE固件更新
TEE-39	TEE应针对TEE永久数据、TA数据、密钥和代码的存储提供回滚策略。	回滚保护
TEE-40	TEE应能检测到对回滚策略的任何破坏。	回滚保护

B.6 TEE保证TA安全执行要求

安全要求序列号	安全要求描述	对应的安全目标实体
TEE-20	如果可信执行环境能装载应用，那这个可信执行环境需要有一个应用装载策略，仅仅允许符合这个应用装载策略的应用进行安装。	TA分离、TA身份识别、TEE运行
TEE-21	如果可信执行环境能够装载应用，那这个可信执行环境应提供对应用撤销的机制。	TA分离、TA身份识别、TEE运行
TEE-22	可信执行环境应能在整个存储时期保护敏感应用代码的机密性。	可信存储
TEE-23	可信执行环境可以具有预置装载应用的能力。	TEE运行
TEE-24	开放的可信执行环境应有装载应用的能力	TEE运行
TEE-25	一个开放的可信执行环境应能通过空中接口装载应用。	TEE运行
TEE-26	TEE应保证每一个TA的标识具	TA身份识别、TA分离、TEE

	有唯一性，且每一个TA标识应与CA标识相区分。	分离
TEE-27	如果一个可信执行环境能够装载应用，这个可信执行环境在装载、更新、卸载应用的时候提供敏感应用代码和数据的机密性机制。	TEE数据保护、可信存储
TEE-28	在创建一个TA实例到这个TA实例被消除的生命周期内，TEE应提供TA实例时间，并保证这个时间在整个TA实例生命周期内的原子性。	TA实例时间
TEE-29	在TA实例生命周期内，TEE应保证TA实例时间不被低功耗状态迁移所影响。	TA实例时间
TEE-30	根据安全特性，属于一个可信执行环境应用的开放的可信执行环境应用代码、数据和密钥不能被可信执行环境内的其它应用获取，除非这个其它的应用被授权接入并且这个接入是通过一个被授权的通信信道完成。	TA分离
TEE-31	需要完整性和/或可靠性的可信执行环境代码在被执行前应被验证，如果验证失败，将不允许代码被执行。	初始化进程、执行过程机密性和完整性、TEE固件完整性
TEE-32	需要完整性和/或可靠性的可信执行环境数据和密钥在使用前应被验证，如果验证失败，将不允许被使用。	执行过程机密性和完整性
TEE-33	除了可信执行环境和这个可信执行环境里的其它应用，敏感的可信执行环境应用数据在被使用或者被修改时应被加密保护以防所有的组件进行潜在的偷听。	执行过程机密性和完整性
TEE-34	可信执行环境应能阻止任何非授权应用接入具有加密保护需求的应用代码。	执行过程机密性和完整性

B.7 TEE运行时安全能力要求

安全要求序列号	安全要求描述	对应的安全目标实体
TEE-76	TEE应对RIC相关的TEE和TA数据资产的安全属性严格地加以保护。	执行过程机密性
TEE-77	TEE应禁止将RIC相关的数据、随机数、密钥暴露给REE或者非授权的TA。	执行过程机密性
TEE-78	TEE应保证仅对授权的TA接入敏感数据、随机数和密钥。	执行过程机密性
TEE-79	TEE应保证无效的敏感资源不可用。	执行过程机密性
TEE-80	RIC过程所使用的任何数据和密钥在使用前应保证其完整性和可靠性。	执行过程完整性
TEE-81	RIC过程所使用的资产（包括数据和代码）应仅能通过安全启动过程进行修改。	执行过程完整性
TEE-82	RIC过程应使用完整性保证的参考测量来验证系统启动时存储内容的完整性。	执行过程完整性
TEE-83	RIC过程应使用完整性保证的参考测量来验证应用运行时存储内容的完整性。	执行过程完整性
TEE-84	RIC过程应能够识别对所检测存储空间的非授权修改并能将其上报给RIC的错误处理。	执行过程完整性
TEE-85	RIC的错误处理在收到系统级完整性失败报告后应使用相应的机制对系统进行重新启动。	执行过程完整性
TEE-86	RIC的错误处理在收到应用级的完整性失败报告后应采取相应的错误	执行过程完整性

	处理机制。	
TEE-87	TEE启动后必须执行RIC。	执行过程完整性
TEE-88	RIC应具有将RIC过程的日志存储在非易失的存储器中，并且对其写操作仅仅由安全启动或者RIC本身来执行。	执行过程机密性和完整性

B.8 TUI安全要求

安全要求序列号	安全要求描述	对应的安全目标实体
TEE-90	可信用户接口显示屏的显示顺序应具有原子性。	安全显示
TEE-91	可信用户接口显示屏由TA发起，每一个TA显示都是完全隔离。	安全显示
TEE-92	当可信用户接口显示屏处于显示状态时，REE不能对该显示屏进行读或写操作。	安全显示
TEE-93	对于已经开始一个可信用户接口显示请求但没有显示的行为，应有一个时间超期处理，处理结果为关闭该请求。	安全显示
TEE-94	当可信用户接口显示屏工作在显示状态时，TEE所提供的安全指示应处于有效状态。	安全显示
TEE-95	当发生以下情况时，应停止可信用户接口显示屏工作： — 终端设备重新启动； — 终端设备电源关闭； — 终端设备开启睡眠模式； — 终端设备关闭背光；	安全显示

TEE-96	使用键盘或虚拟键盘进行输入的时候，TEE所提供的安全指示应处于有效状态。	安全输入
TEE-97	当发生以下情况时，应停止可信用户输入接口工作： — 终端设备重新启动； — 终端设备电源关闭； — 终端设备开启睡眠模式； — 终端设备关闭背光；	安全输入
TEE-98	安全指示由TEE管理，与REE分离。	安全指示
TEE-99	安全指示应处于用户显而易见的位置。当工作域为 TEE 时，安全指示有效；当工作域为 REE 时，安全指示无效。	安全指示
TEE-100	安全指示的信息不应被REE获知。	安全指示
TEE-101	当发生以下情况时，应停止安全指示工作： — 终端设备重新启动； — 终端设备电源关闭； — 终端设备开启睡眠模式； — 终端设备关闭背光；	安全指示

附 录 C
（资料性附录）
渗透性攻击测试方法

C.1 基于硬件的攻击路径

- **侧信道攻击：**侧信道攻击的目的是恢复可信存储中的加密密钥。攻击的手段是在可信存储操作过程中，通过对获取到的 TEE 平台能量或电磁信号进行分析来恢复可信存储操作的密钥。
- **错误注入攻击：**这种攻击的目的是使用激光、电磁或者毛刺等物理手段作用于输入信号（如时钟、电源），来临时的改变 TEE 的某种行为。这种攻击行为可以改变代码的执行顺序或者改变对处理数据的解释，以便旁路那些 TEE 中执行的安全校验例如签名验证或者防回滚校验。

C.2 基于软件的攻击路径

- **缓存攻击：**这种攻击方法的前提条件是 TEE 和 REE 的共享内存机制、完全由软件实现的加解密以及加密算法依赖于对存储的接入，通过控制 REE 侧的内存来获取到分配给 TEE 的内存信息，进而测量 TEE 加密操作的次数以便统计出密钥信息。
- **API 接口的模糊测试：**这种攻击的目的是触发 TEE 的异常行为或者是 TEE 内部的一个异常状态以便挖掘出脆弱点。
- **存储隔离的破坏：**这种攻击方法是利用存储隔离的缺陷直接接入 TEE 存储并尝试修改里面的内容。
- **证书解析算法分析：**这种攻击方法是通过提供 TEE 一个错误的证书使攻击者在安全环境内注入一段伪代码。
- **已知 API 或者协议的脆弱性利用：**这种攻击方法是利用已被弃用或者未被文档化的接口向 TEE 中注入恶意代码或者从 TEE 中提取敏感数据，攻击向量例如是加密 API 调用了存有漏洞的算法库或者未即时更新安全补丁的 API。

附 录 D
（资料性附录）
厂商提交的产品清单

D.1 硬件资源

- 开发板
  - 数量:（根据级别 2/12/22）
  - 10 个样品去表层封装(高级)
  - 样品表面没有任何覆盖（如散热片）
  - 样品主芯片可由外部电源单独供电，尽量减少电源的滤波电容
  - 提供调试接口（如 JTAG、USB 等）
- 触发
  - 触发信号可以被测试程序控制
  - 触发信号可以以简单方式与示波器相连（如 I/O 引脚或 GPIO 引脚）
  - 触发信号触发与待测模块启动之间没有非必要的操作
- Reset
  - 提供样品的 reset 信号，并能从外部对其进行控制
  - Reset 跟冷启动过程等价
- 模块
  - 样品安全防护功能可以在测试过程中开启或关闭，包括软硬件
  - 与测试向量无关的模块可以被关闭（如显示屏，GPS，WIFI，蓝牙等）
  - 样品能通过通信接口与计算机相连并传输数据
  - 主芯片时钟信号可设置为由外部时钟输入
  - 密码算法底层输入输出可直接通过通信接口导出

D.2 软件资源

这里主要包含评测过程中需要的软件相关资源

- REE/TEE 应用开发环境
  - REE 应用开发环境（CA 开发 SDK）
  - TEE 应用开发环境（TA 开发 SDK）
  - 开发所使用的 IDE
- ToE Debug 实验环境
  - 针对 REE/TEE 进行 Debug 的工具列表，必要时提供列表中的工具
  - 针对 ToE 的 Debug 软件环境的搭建（例如 Debug 所需驱动、工具、软件，SDK 等）
- ToE 固件打包工具
  - 固件生成工具

- 固件签名工具
- 固件加密工具（必要时可能需要提供加密密钥）
- 固件烧录工具

- ToE 实现的加密算法源代码
  - 开源算法需要提供算法库名称、版本、许可证等
  - 闭源算法至少需要提供 API 以及相关介绍文档，必要时在 NDA 允许条件下需要提供关键部分代码
- TEE 密钥相关功能的所有实现源代码
  - 包括 TEE 密钥的生成、衍生、管理、存储、调用、销毁等过程的全部实现源代码
- TEE 安全监视器实现代码
  - TEE 与 REE 环境切换与通信信道的详细实现代码。对于基于 ARMv8-A 系列 SoC 的产品，主要是安全监视器（SMC）的详细实现代码，例如 ARM-Trusted Firmware 等。
- TEE 安全存储功能实现代码
  - 对 REE 中程序（CA）开放的接口以及实现代码
  - 对 TEE 中程序（TA）开放的接口以及实现代码
  - REE 与 TEE 进行数据传输的具体实现代码
  - TEE 对内部安全 OS 暴露的接口以及实现代码
  - TEE 对保护数据的处理实现代码（TEE 如何写入、读取、验证、鉴权等）
- TEE 安全启动的详细实现代码
  - 启动流程中所有一定会被执行的源代码
  - 启动流程中所有可能被执行的源代码
  - 启动流程中执行的安全验证部分源代码（包括可靠性、完整性、时间戳等验证）
  - 启动流程中安全冗余部分实现源代码（如果实现了）
  - 对于基于 ARMv8-A 系列 SoC 的产品，启动部分可能包含在 ARM-Trusted Firmware 中。
  - Etc.
- TEE 的运行时完整性安全功能实现代码
  - 运行时对 TEE/TA 安全资产的保护功能源代码
  - 运行时对 TEE/TA 密钥的保护功能源代码
  - 运行时对使用的敏感安全资产、密钥等的验证实现代码
  - 启动前、运行时对应用以及数据做的安全验证与防护功能实现的源代码
  - 运行时安全验证（完整性验证）失败的处理代码
  - 运行时安全处理日志的记录与处理代码
  - Etc..
- TEE 与输入输出设备的安全交互功能实现代码
  - TEE 与可信输入输出设备之间的通信实现源代码
  - TEE 与可信输入输出设备之间的安全保障部分源代码
  - Etc..

D.3 文档资源

这里主要包含评测过程中所需要的文档资源

- ToE 整体架构设计文档
  - 整个系统的硬件架构设计文档
  - 整个系统的软件架构设计文档
- ToE TEE 内存分配与隔离设计文档
  - TEE 硬件隔离机制
  - TEE 内存分配与共享机制
  - 内存页表的配置
  - MMU 的配置
  - REE 与 TEE 之间内存共享映射机制与保护机制
  - TEE 内存/FLASH 等存储介质的隔离机制
- ToE TEE 安全启动详细实现文档
  - 安全启动架构设计
  - 对启动代码的可靠性、完整性验证实现机制
  - 启动代码对硬件的硬件验证/绑定机制（如果实现了）
  - TEE 启动环境初始化详细流程
  - 样品系统完整启动流程（包括 TEE/REE 的完整启动过程、状态机）
  - 代码（固件/BootLoader）更新流程
  - 代码更新安全防护机制（例如防止回滚，固件验证等）
  - 启动/更新过程的异常处理机制
- TEE 的基础工作流程/状态机介绍文档
  - TEE 有哪些基本工作状态
  - TEE 有哪些异常状态
  - TEE 是如何在这些状态之间进行切换与保护的等信息。
- TEE 的异常恢复与保护机制实现文档
  - 存储和恢复设备唯一标识的实现机制
  - 针对 REE/TA 引起的异常保护机制
  - 针对其他异常的保护机制（例如断电、重启等）
  - 回滚验证与保护机制（时间回滚、版本回滚等）
- ToE 实现的公开 API 文档
  - 加密算法 API
  - 安全存储 API
  - Etc…
- TEE 的应用装载和应用使用策略应用接口文档
  - 文档应描述 TEE 在装载、更新、卸载应用时，代码所调用的应用接口。
- 可信执行环境应用装载和应用使用管理

- 文档应描述 TEE 中对于一个应用装载、撤销、存储的策略。包括对 TA 的识别和机密性保护以及低功耗状态时，保持 TA 实例时间不变的控制策略。
- 实现代码应展示 TEE 在装载、更新、卸载应用时，对敏感应用代码和数据的机密性机制，对 TA 标识的唯一性识别，以及对不同 TA 装载实现的逻辑隔离机制。

o TEE 的密钥管理相关文档
- 具体需要包括 TEE 密钥的生成、衍生、管理、存储、调用、销毁等过程的全部实现文档。

o TEE 所支持的所有公开加密标准密码算法的详细实现文档
- 需要提供 TEE 所支持的所有公开加密标准密码算法的详细实现文档。如果是使用的第三方加密算法库，则需要提供详细的开发库详细说明文档，包括 API 详细文档以及算法库的版本与使用许可证信息。

o TEE 内随机数发生器（RNG）的详细实现文档
- 需要提供 TEE 内随机数发生器（RNG）的详细实现文档，包括硬件实现、软件接口等。

o TEE 与 REE 环境切换与通信信道的详细实现文档
- 对于基于 ARMv8-A 系列 SoC 的产品，主要是安全监视器（SMC）的详细实现文档，主要包括环境切换与通信信道两个部分；对于基于 ARMv8-M 系列 SoC 的产品，这部分则主要是 TEE 与 REE 之间切换的硬件实现文档，以及 TEE 与 REE 之间的通信信道详细实现文档。

o TEE 安全存储的详细实现文档
- 安全存储器的实现机制（硬件实现与软件实现原理）
- 对安全存储器内数据的访问权限鉴别
- 对安全存储数据的访问、加解密、添加、修改删除等操作原理
- 对安全存储数据的读写、加解密操作等操作 API 详细介绍
- 安全存储的冗余保障实现
- 安全存储模块对异常的处理
- 安全存储的根密钥的写入、读取、保护机制
- 安全存储抗攻击的实现机制（如果实现了）
- 安全存储的实现与硬件的绑定机制（如果实现了）

o TEE 运行时完整性保护实现文档（可选）
- 运行时对 TEE/TA 安全资产的保护
- 运行时对 TEE/TA 密钥的保护
- 运行时对使用的敏感安全资产、密钥等的验证机制
- 启动前、运行时对应用以及数据做的安全验证与防护
- 运行时安全验证（完整性验证）失败的处理机制
- 运行时安全处理日志的记录与处理
- Etc..

o TEE 与输入输出设备间的安全交互实现文档（可选）
- TEE 与可信输入输出设备之间的通信架构设计

- TEE 与可信输入输出设备之间的安全保障
- TEE 与可信输入输出设备之间通信时的隔离实现（主要是与 REE 的隔离）
- Etc..
  - 安全显示功能描述
    - 文档应描述可信用户接口显示屏的显示顺序的原子性
    - 文档应描述保证可信显示由 TA 发起时 REE 隔离策略
    - 文档应描述保证可信显示接口显示屏出于现实状态时，REE 不能对该显示屏进行读或写操作
    - 文档应描述保证可信显示的超时处理机制
    - 文档应描述保证可信显示处于显示状态时，安全指示处于有效状态
    - 文档应描述在异常或低功耗情况下的安全显示的显示功能应停止工作
  - 安全输入功能描述
    - 文档应描述当时用键盘或虚拟键盘进行安全输入时，TEE 所提供的安全指示应处于有效状态，及遇到异常或低功耗时的安全输入终止策略。
  - 安全指示功能描述
    - 文档应描述安全指示功能的应用场景、与 REE 的逻辑隔离及遇到异常或低功耗时的安全指示终止策略。

- 产品硬件设计文档
  - 样品数据手册
  - 所有芯片的数据手册
  - 样品内部电源设计文档
  - 样品时钟设计文档
  - 样品电路图
  - 样品 PCB 版图
  - 样品 Gerber 文件
  - 样品序列号、样品 ID 说明文档
- 使用说明
  - Debug 工具的详细描述
  - 开发板使用说明
  - 样品使用说明
  - 测试环境搭建说明
  - 测试程序说明

附 录 E
（资料性附录）
厂商提交的 ST

E.1 密钥安全目标

E.1.1	根密钥机密性、完整性、可靠性保障	**是否支持：**	是/否
	如果有，请详细列出根密钥存储方式和使用策略	TEE-4	
详细描述：			

E.1.2	公共密钥完整性、可靠性保障	**是否支持：**	是/否
	如果有，请详细列出公共密钥存储方式和使用策略，例如安全启动过程中所使用的公共密钥	TEE-5	
详细描述：			

E.1.3	对称密钥和私钥的机密性、完整性、可靠性	**是否支持：**	是/否
	如果有，请详细列出对称密钥和私钥的存储和使用策略，如果密钥为衍生密钥，请详细列出密钥衍生和管理策略（包括生成、使用、销毁）	TEE-1 TEE-2 TEE-3 TEE-6 TEE-7 TEE-8 TEE-9	
详细描述：			

E.2 安全启动目标

E.2.1	安全启动过程的可靠性、完整性验证	**是否支持：**	是/否
	如果有，请详细列出安全启动整体流程，包括引导程序的安全保护策略、可信执行环境的安全保护策略，安全启动与设备硬件的绑定策略。	TEE-68 TEE-69	
详细描述：			

E.2.2	安全启动代码镜像更新过程的可靠性、完整性	**是否支持：**	是/否
	如果有，请详细列出安全启动代码镜像更新整体流程，包括引导程序的更新保护策略、可信执行环境的更新保护策略。	TEE-37 TEE-38 TEE-70 TEE-71 TEE-72	

详细描述：

E.2.3	安全启动过程的异常处理	**是否支持：**	是/否
	如果有，请详细列出安全启动过程的异常处理机制，包括回滚授权、安全启动失败、更新失败的异常处理机制。	TEE-73 TEE-74 TEE-75	
详细描述：			

E.3 安全存储目标

E.3.1	TEE 中敏感实体存储的机密性、可靠性、一致性、原子性保障以及可擦除机制	**是否支持：**	是/否
	如果有，请详细列出安全存储机制，包括存储位置以及机密性、完整性、原子性实现方式。	TEE-35 TEE-36 TEE-39 TEE-40 TEE-55 TEE-56	
详细描述：			

E.3.2	TEE 中敏感实体存储的权限管理	**是否支持：**	是/否
	如果有，请详细列出对敏感实体的权限管理机制，包括权限分配、权限撤销机制的具体实现方式。	TEE-57 TEE-58 TEE-59 TEE-60 TEE-61 TEE-62	
详细描述：			

E.3.3	TEE 中安全存储密钥的生成方式以及其机密性、完整性、一致性、原子性	**是否支持：**	是/否
	如果有，请详细列出 TEE 安全存储所使用的密钥的生成策略及具体实现方式，以及相关密钥的机密性、完整性、一致性、原子性的保护策略及具体实现方式。	TEE-39 TEE-40 TEE-63 TEE-64 TEE-65 TEE-66 TEE-67	

详细描述：

E.4 TEE隔离安全目标

E.4.1	TEE 与 REE 隔离机制	**是否支持：**	是/否
	如果有，请详细列出 TEE 与 REE 之间的隔离实现方式，包括存储介质（如 RAM、ROM）、CPU 和安全资产（如生物识别模块）的软、硬件隔离具体实现方式。	TEE-41	
详细描述：			

E.4.2	TEE 与其它运行环境的通信保护	**是否支持：**	是/否
	如果有，请详细列出 TEE 与其它运行环境之间通信的授权机制具体实现。	TEE-46 TEE-47	
详细描述：			

E.4.3	TEE 与其它运行环境的通信异常处理	**是否支持：**	是/否
	如果有，请详细列出 TEE 与其它运行环境之间通信发生异常情况下的处理机制，这些异常情况例如非授权 CA 重复访问 TA、访问的数据完整性验证失败等。	TEE-48 TEE-49	
详细描述：			

E.5 TEE状态保护目标

E.5.1	TEE 自身状态机的管理与保护	**是否支持：**	是/否

	如果有，请详细列出 TEE 自身状态机的架构设计，以及状态异常切换的检测及保护机制及具体实现。	TEE-17
详细描述：		

E.6 随机数发生器

E.6.1	基于硬件的随机数发生器	**是否支持：**	是/否
	如果有，请详细列出随机数产生的具体方式。	TEE-19	
详细描述：			

E.7 TA安全管理目标

E.7.1	TEE 加载/运行/撤销 TA 的安全策略	**是否支持：**	是/否
	如果有，请详细列出 TEE 在加载/运行/撤销 TA 时的安全策略，包括 TA 代码的存储位置和存储方式，TEE 加载时实现完整性、唯一性的具体方法，TA 运行时的原子性和相应的撤销机制及具体实现方法。	TEE-20 TEE-21 TEE-22 TEE-26 TEE-28 TEE-29	
详细描述：			

E.7.2	TEE 安装/更新/卸载 TA 的安全策略	**是否支持：**	是/否
	如果有，请详细列出 TEE 安装/更新/卸载 TA 的安全策略；如果是通过空中接口进行安装/更新，请详细列出其机密性、完整性保护策略及具体实现方式。	TEE-22 TEE-23 TEE-24 TEE-25 TEE-27	
详细描述：			

E.7.3	TA 间的隔离保护	**是否支持：**	是/否
	如果有，请详细列出 TA 运行时内存隔离机制以及实现方法。	TEE-30	
详细描述：			

E.8 TEE运行时的安全目标 （可选）

E.8.1	TEE 运行时完整性校验（RIC）	**是否支持：**	是/否
	如果有,请详细列出TEE运行时完整性校验机制包括完整性校验位置、保护对象、实现方式。	TEE-87 TEE-88	
详细描述：			

E.8.2	RIC 相关的敏感数据的保护	**是否支持：**	是/否
	如果有，请详细列出对 RIC 相关的敏感数据的安全保护机制，包括数据存储、使用时的完整性、可靠性；数据使用的管理机制。	TEE-76 TEE-77 TEE-78 TEE-80 TEE-81 TEE-82 TEE-83	
详细描述：			

E.8.3	RIC 相关的敏感数据的使用异常处理	**是否支持：**	是/否
	如果有，请详细列出对 RIC 相关的敏感数据的异常处理机制，包括数据完整性校验失败、非授权访问等。	TEE-84 TEE-85 TEE-86	
详细描述：			

E.9 可信用户接口目标 （可选）

E.9.1	可信用户接口运行时安全保护	**是否支持：**	是/否
	如果有，请详细列出可信用户接口（包含显示屏、键盘等）安全保护策略，包括可信接口的安全配置、原子性、隔离性、安全指示等具体实现方法。	TEE-90 TEE-91 TEE-92 TEE-94 TEE-96 TEE-98 TEE-99 TEE-100	
详细描述：			

E.9.2	可信用户接口运行时异常状态处理	**是否支持：**	是/否
	如果有，请详细列出可信用户接口（包含显示屏、键盘等）的异常状态处理机制安全保护策略及具体实现方法。	TEE-93 TEE-95 TEE-97 TEE-101	
详细描述：			