

TEE 指南

本文翻译自 Global Platform 的白皮书“GlobalPlatform made simple guide: Trusted Execution Environment (TEE) Guide”

1. 什么是可信执行环境(Trusted Execution Environment - TEE)?

TEE 是存在于智能手机、平板电脑，或任意移动设备主处理器中的一个安全区域，确保各种敏感数据在一个可信环境中被存储、处理和受到保护。TEE 为授权安全软件，也称为“可信应用”提供一个安全的执行环境，通过实施保护、保密性、完整性和数据访问权限确保端到端的安全。

2. 它如何应用于目前以及未来的安全应用生态系统?

手机中的安全框架可由三种移动环境组成。每一个都有不同的任务：

- **丰富的操作系统 (Rich OS)：**针对多功能性和丰富性创建的环境，执行诸如安卓 (Android)、塞班 (Symbian) 和 Windows Phone 等设备应用。在设备生产以后向第三方开放下载。该环境下安全是其考虑因素，但并非最重要的因素。
- **可信执行环境 (TEE)：**TEE 由软件和硬件组成，针对在 Rich OS 环境中生成的软件攻击提供保护。它协助控制需要与 Rich OS 隔离的敏感性应用的访问权限和存储。例如，TEE 是内容提供商在限定的时间段内提供视频服务的理想环境，因为他们需要保证其重要内容（例如高清视频）的安全，使其无法被免费共享。
- **安全元件 (Secure Element- SE)：**SE 由软件和防篡改硬件组成，支持高级别的安全性，可以与 TEE 一起运行。对于需要最高安全级别的近距离支付相关应用或官方电子签名，SE 是强制的安全措施。TEE 也可以提供可信用户界面，用以安全地传输个人身份识别号码 (PIN)，进行大额交易。它还可以将直接存储在 SE 中的应用进行过滤访问。

TEE 是一个与 Rich OS 并行运行的独立环境，为多种环境提供安全服务。它比 Rich OS 更安全，但略逊于 SE，它足以为大量应用提供安全。因此，TEE 在高级别保护的 SE 和低级别保护的 Rich OS 之间提供了安全的“中间地带”。

TEE 现在是移动生态系统的重要组成部分。它为移动设备的所有方面—手机、Rich OS 和 SE 提供安全性和保护，可满足主要参与者的需求。

服务提供商、移动网络运营商操作系统和应用开发者、设备制造商、平台提供商和芯片供应商都是关键的利益相关者，因此，他们都愿意看到安全性成为被谨慎制定且记录在案的标准。

3. TEE 诞生的时间和源头?

手机制造商或芯片制造商在多年前开发了该技术，并且拥有众多版本，他们将其应用在设备中，作为专有解决方案的一部分。因此，应用开发者需要创建并安全评估每个应用的不同版本，以便符合不同的规范集和由各个专有解决方案拟订的安全级别，并要应对由此带来的复杂性。

由于 GlobalPlatform 与手持设备和 Rich OS 没有相关利益关系，有利于它推出一种方法，让 TEE 被所有供应商采用，并与每个 Rich OS 环境很好地共存。TEE 的标准化将增强功能性和安全性的互操作性。这将简化应用开发和所有相关部署。

4. 它创建的原因是什么？它满足了哪些业务和商业需求？

TEE 的存在有两个主要原因：

- 更多的移动业务不断涌现，需要更高的安全级别。
- 随着用户数量的增加，防御恶意软件/病毒的需求也相应增加。有些应用需要具有更高安全性，因为这些应用在受到攻击后会导致更严重的后果，因此它们不单单需要软件解决方案自身的保护，还需要更多的安全措施。

内容保护、企业环境、连接性和移动金融服务的兴起都需要安全级别的不断提高。TEE 隔离安全应用，并防止其受到可能无意间下载的恶意软件的攻击。这使 TEE 成为未来设备发展的主要环境。

在业务和商业收益方面，TEE 是主要参与方的核心要求。移动设备制造商需要提供一个 TEE 环境以便满足不同内容提供商的业务需求。移动网络运营商希望采用 TEE，因为它能使其为客户提供更多、更高价值的服务，来促进收入的增长。内容提供商希望采用 TEE 确保其产品的安全，并能够以一个通用方式部署在多个平台上。

此外，支付服务提供商不希望相同应用必须开发不同版本来满足不同的专属 TEE 环境的需求。例如，如果生态系统没有标准化，支付服务提供商就必须进行认证并支持不同的应用和流程。这非常耗时、昂贵，并且与创建应用程序的大规模市场部署这一目标背道而驰。

5. 为何涉及 GlobalPlatform？

GlobalPlatform 及其成员认识到开发标准需要与新生态系统的演进同步进行。这种双向开发扫除了因为互操作性问题而导致的障碍，从而提供更大的确定性，降低整个行业的发展成本。

GlobalPlatform 认识到 TEE 对于未来管理安全芯片技术应用的重要性。填补 Rich OS 和 SE 之间的空白，对于移动设备可信应用的未来安全非常重要。实施标准化还将增强市场信心。凭借在移动领域的十年经验和成员的专长，

GlobalPlatform 的工作位于市场的最前沿。GlobalPlatform 已经开始进行 SE 应用管理的标准化工作。且通过开发并于 2010 年 7 月颁布的 TEE Client API 1.0

规范，在 TEE 领域掌握丰富的经验。因此，继续实施标准化并扩展其专长是非常有意义的。

由于 GlobalPlatform 与成员无利益关系，因此它正在寻求使规范标准化的方法，以确保实现一个开放、可互操作的生态系统。GlobalPlatform 的目标是最终制定与 TEE 有关的标准，并推出一个支持该标准的计划，这样它就可以测试和认证 TEE 的功能层面，并坚持采用有效的 GlobalPlatform 测试套件，应用开发商、硬件制造商和软件开发商都将直接从中受益。另外，GlobalPlatform 还推出了一个安全认证计划，以便使指定的 TEE 实施合格的安全级别。这将为市场带来信心：TEE 的性能将表现的如其广告所说。在中期阶段，GlobalPlatform 将致力于构建一个生态系统，遵从 GlobalPlatform 是服务提供商和手机制造商协作的前提条件。该标准的长期目标是成为业界的事实标准，这是该实现市场全面普及的奠基之作。