可信执行环境(TEE)

根据GlobalPlatform和通用标准的标准评估和认证可信执行环境(TEE)的安全性、功能性和互操作性。

TEE是一种高附加值（支付、优质内容、eID）手机服务的安全解决方案。该解决方案为手机应用程序提供了一个安全且独立的执行环境，该环境保持足够的开放性，以便服务提供商能够访问和管理它们的数据。
TEE是一个安全的执行环境，它与设备的操作系统（如Android）并行运行，并且只有授权和可靠的应用程序（可信应用程序）才能在该环境下运行。TEE使用软硬件安全资源来保护在TEE中执行的应用程序。这提高了存储和处理可信应用程序管理的敏感数据的安全性。此外，TEE为安全应用程序提供了一组标准化的例程和函数(API)，以促进这些应用程序的研发。这一解决方案不仅适用于智能手机，也适用于其他设备，如平板电脑、智能电视、机顶盒等管理敏感数据并接入互联网（物联网）的产品。
TEE解决方案的标准化和认证是推动其在市场中被采用和扩展的关键因素，而在手机市场这样一个涉及许多参与者（原始设备制造商、移动网络运营商、服务提供商等）的复杂环境中，尤其如此。

解决方案

Applus+ Laboratories经认可对GlobalPlatform认证方案和可信执行环境(TEE)通用标准进行测试和安全评估。
GlobalPlatform (GP)： GP已经实现了专用接口(API)的标准化，这些接口允许在智能手机的操作系统(Rich OS)和安全应用程序之间、安全应用程序和TEE操作系统之间进行通信。使用**GlobalPlatform TEE认证方案**，带有TEE的设备供应商可以确保其产品符合GlobalPlatform标准中定义的安全性、功能性和互操作性要求。

- **GlobalPlatform TEE安全评估：**Applus+参与了GlobalPlatform TEE认证体系的创建和评估方法的研发。该方法侧重于对产品进行测试，根据手机市场产品研发和营销周期较短的特点，调整文件和程序要求。
- **GlobalPlatform TEE功能需求（初始TEE配置）：**Applus+经授权根据GP最初的TEE配置标准测试TEE的功能性和互操作性。

通用标准(CC)：保证TEE安全等级的另一种方法是根据通用标准对产品进行认证，这是一种在市场上得到广泛认可的安全标准。

- **TEE保护框架(EAL TEE)：**Applus+是通用标准安全测试实验室（ITSEF），能够进行所需的评估，以获得TEE的通用标准认证。此认证基于TEE保护框架。它可以与GlobalPlatform认证同时进行，这样制造商可以同时获得两份证书。

优势：

- 推动TEE技术的大规模采用，培养市场信心，并通过独立实验室实现功能的标准化和认证。
- Applus+是根据行业两个主要标准为获得TEE认证的一站式服务机构：GlobalPlatform和通用标准

注意：由于Applus+ Laboratories是经过多个评估和认证方案认证的第三方实验室，为了保证其公正性，Applus+工程师从未参与实际的产品研发或解决方案实施。