Ensayos de Trusted Execution Environment (TEE)

Evaluar y certificar la seguridad, la funcionalidad y la interoperabilidad de Trusted Execution Environment (TEE) según los estándares de GlobalPlatform y Common Criteria.

El TEE es una solución de seguridad para móviles que provee un entorno seguro para servicios de alto valor añadido (pago, contenidos premium, eID) y, al mismo tiempo, suficientemente abierto para que los proveedores de servicios puedan acceder y gestionar sus datos. Todo ello sin perjudicar la experiencia de usuario.
El TEE es un entorno de ejecución seguro que funciona en paralelo al sistema operativo del dispositivo (Ej.- Android), donde solamente se ejecutan aplicaciones autorizadas y consideradas confiables (trusted apps). El TEE utiliza recursos de seguridad software y hardware para proteger las aplicaciones que están siendo ejecutadas en el TEE. De este modo refuerza el nivel de seguridad del almacenaje y procesado de los datos sensibles que gestionan las aplicaciones confiables. Adicionalmente, el TEE proporciona a las aplicaciones seguras un conjunto estandarizado de métodos y funciones (APIs) que facilitan el desarrollo de estas aplicaciones.
Esta solución es aplicable no solo a los teléfonos móviles sino también a otros dispositivos como tablets, Smart TV, decodificadores o cualquier producto que gestione datos sensibles y esté conectado a internet (internet of things).
La estandarización y certificación de las soluciones TEE es un elemento clave para fomentar su adopción y expansión en el mercado, especialmente en un ecosistema tan complejo como el móvil, con muchos actores implicados (OEMs, MNOs, Service Providers, etc.)

Solución

Applus+ Laboratories está acreditado para realizar ensayos y evaluaciones de seguridad de los esquemas de certificación GlobalPlatform y Common Criteria para Trusted Execution Environments (TEE).

GlobalPlatform (GP): GP ha estandarizado las distintos interfaces (API) que permiten la comunicación entre el sistema operativo del móvil (Rich OS) y las aplicaciones seguras, y entre las aplicaciones seguras y el sistema operativo del TEE. El **esquema de certificación GlobalPlatform TEE** permite a los *vendors* de dispositivos con TEE asegurar que su producto cumple con los requisitos de seguridad, funcionalidad e interoperabilidad definidos en los estándares GlobalPlatform.

- **GlobalPlatform TEE Security Evaluation**: Applus+ ha participado en la creación del esquema de certificación GlobalPlatform para TEE y en el desarrollo de la metodología de evaluación. Esta metodología está centrada en la realización de pruebas en el producto, con unos requisitos documentales y de procedimiento adaptados a los cortos ciclos de desarrollo y comercialización del mercado móvil.
- **GlobalPlatform TEE Functional requirements (Initial TEE Configuration)**: Applus+ está acreditado para ensayar la funcionalidad y la interoperabilidad del TEE según este estándar GP Initial TEE Configuration.

Common Criteria (CC): Otra opción para garantizar el nivel de seguridad del TEE es certificar el producto bajo Common Criteria, un estándar de seguridad que cuenta ya con un amplio reconocimiento en el mercado.

- **TEE Protection Profile (EAL TEE)**: Applus+ es un laboratorio de seguridad para Common Criteria (ITSERF) y puede realizar las evaluaciones necesarias para obtener la certificación Common Criteria para TEE. Esta certificación está basada en el Perfil de Protección de TEE. Esta certificación puede realizarse en paralelo con la certificación GlobalPlatform permitiendo a los fabricantes obtener dos certificados a la vez.

Beneficios:

- Promover la adopción a gran escala de la tecnología TEE fomentado la confianza en el mercado, mediante su estandarización y la certificación de sus funcionalidades por laboratorios independientes.
- Applus+, one-stop-shop para realizar la certificación de su TEE bajo los dos principales estándares de la industria, GlobalPlatform y Common Criteria

Nota: Dado que Applus+ Laboratories está acreditado como laboratorio independiente por varios esquemas de certificación, los ingenieros de Applus+ nunca participan en el desarrollo de producto o la implementación de soluciones, garantizando así su imparcialidad.