Trusted Execution Environment (TEE)

Evaluierung und Zertifizierung von Sicherheit, Funktionalität und Interoperabilität des Trusted Execution Environment (TEE) nach GlobalPlatform- und Common Criteria-Standards.

TEE ist eine Sicherheitslösung für Handys, die eine sichere Umgebung für Dienstleistungen mit hohem Mehrwert (Bezahlsysteme, Premiuminhalte und eID) bietet und zugleich offen genug ist, damit Serviceanbieter auf ihre Daten zugreifen und sie verwalten können; und alles, ohne das Nutzererlebnis zu beeinträchtigen.
TEE ist ein parallel zum Betriebssystem des Gerätes (z.B. Android) laufendes, sicheres Betriebssystem, auf dem nur autorisierte und verlässliche Applikationen (trusted apps) ausgeführt werden. Es nutzt Sicherheitssoftware und -hardware, um die im TEE ausgeführten Applikationen zu schützen. Somit wird die Sicherheitsstufe für Speicherung und Verarbeitung der von den verlässlichen Applikationen verwalteten sensiblen Daten erhöht. Zusätzlich bietet das TEE den sicheren Applikationen ein standardisiertes System von Methoden und Funktionen (APIs), welches die Weiterentwicklung dieser Applikationen erleichtert.
Diese Lösung ist nicht nur auf Handys anwendbar, sondern auch auf anderen Geräten wie Tablets, Smart TVs, Decodern oder jedem anderen Produkt, das sensible Daten verwaltet und mit dem Internet verbunden ist (internet of things).
Die Standardisierung und Zertifizierung der TEE-Lösungen sind Schlüsselelemente zur Förderung ihrer Markteinführung und –verbreitung, besonders in einem so komplexen System wie dem Handy, mit seinen zahlreichen Akteuren (OEMs, MNOs, Service Providern, etc.).

Lösung

Applus+ Laboratories ist zugelassen, die Sicherheitsprüfungen und -bewertungen der Zertifizierungssysteme GlobalPlatform und Common Criteria für Trusted Execution Environments (TEE) durchzuführen.
GlobalPlatform (GP): GP hat die verschiedenen Interfaces (APIs) standardisiert, welche die Kommunikation zwischen dem Betriebssystem des Handys (Rich OS) und den

sicheren Applikationen sowie zwischen Letzteren und dem TEE-Betriebssystem erlauben. Das **Zertifizierungssystem GlobalPlatform TEE** ermöglicht es den Händlern zu gewährleisten, dass ihr Produkt die in den GlobalPlatform-Standards definierten Anforderungen an Sicherheit, Funktionalität und Interoperabilität erfüllt.

- **GlobalPlatform TEE Sicherheitsbewertung**: Applus+ war an der Einrichtung des GlobalPlatform-Zertifizierungssystems für TEE und der Entwicklung des Evaluierungsverfahrens beteiligt. Der Schwerpunkt dieses Verfahrens liegt auf der Durchführung von Produktprüfungen, deren Dokumentations- und Verfahrensanforderungen an die kurzen Entwicklungs- und Vermarktungszyklen des Handymarktes angepasst sind.
- **GlobalPlatform TEE Funktionalitätsanforderungen (Initial TEE Configuration)**: Applus+ ist für die Funktionalitäts-und Interoperabilitätsprüfung des TEE nach dem GP Initial TEE Configuration-Standard zugelassen.

Common Criteria (CC): Eine weitere Möglichkeit, das TEE-Sicherheitsniveau zu gewährleisten, ist die Produktzertifizierung nach Common Criteria, einem Sicherheitsstandard, der schon über eine breite Marktakzeptanz verfügt.

- **TEE-Schutzprofil (EAL TEE)**: Applus+ ist ein zugelassenes Sicherheitslabor für die Evaluierung nach Common Criteria, um die CC-Zertifizierung für TEE zu erlangen. Diese auf dem TEE-Schutzprofil basierende Zertifizierung kann parallel zur GlobalPlatform-Zertifizierung durchgeführt werden und ermöglicht somit den Herstellern, zeitgleich zwei Sicherheitszertifikate zu erhalten.

Vorteile:

- Förderung der Einführung der TEE-Technologie auf breiter Front durch die Stärkung des Marktvertrauens mit Hilfe der Standardisierung und Zertifizierung ihrer Funktionalitäten durch unabhängige Labors.
- Applus+, *One-Stop-Shop* für die Zertifizierung ihrer TEE gemäß den zwei wichtigsten Industriestandards: GlobalPlatform und Common Criteria.