Contact: info@appluslaboratories.com

Trusted Execution Environment (TEE) testing

Evaluate and certify the security, functionality and interoperability of the Trusted Execution Environment (TEE), in accordance with GlobalPlatform and Common Criteria standards.

The TEE is a security solution for mobile services with high added value (payment, Premium content, eID). This solution provides a secure and isolated execution environment for mobile apps, that remains open enough for service providers to be able to access and manage their data.

The TEE is a secure execution environment that runs in parallel with the operating system of the device (e.g. Android) and where only authorised and reliable applications are run (trusted apps). The TEE uses software and hardware security resources to protect the applications which are being executed in the TEE. This increases the security in the storage and processing of the sensitive data managed by the trusted applications. Furthermore, the TEE provides secure applications with a standardized set of routines and functions (APIs) that facilitate their development. This solution is applicable not only to smart phones but also to other devices such as tablets, Smart TV, set-boxes and other products that manage sensitive data and are connected to the Internet (Internet of things).

The standardization and certification of TEE solutions is a key element in promoting their adoption and expansion in the market, in particular in an environment as complex as that of mobile market which involves a number of actors (OEMs, MNOs, Service Providers, etc.). Applus+ Laboratories is accredited to carry out the testing and security evaluation of the certification schemes GlobalPlatform and Common Criteria for Trusted Execution Environments (TEE).

Contact: info@appluslaboratories.com

GlobalPlatform TEE Certification

GloblaPlatform (GP) has standardized the specific interfaces (API) that allow communication to take place between the smart phone's operating system (Rich OS) and secure applications, and between the secure applications and the TEE's operating system. With the **GlobalPlatform TEE certification scheme,** vendors of devices with a TEE may ensure that their product complies with the security, functionality and interoperability requirements defined in the GlobalPlatform standards.

- **GlobalPlatform TEE Security Evaluation**: Applus+ took part in the creation of the GlobalPlatform TEE certification scheme and in the development of the evaluation methodology. This methodology focuses on carrying out testing on the product, with documentary and procedural requirements adjusted to the short product development and marketing cycles of the mobile market.
- **GlobalPlatform TEE Functional requirements (Initial TEE Configuration)**: Applus+ is accredited to test the functionality and interoperability of the TEE according to the GP Initial TEE Configuration standard.

Common Criteria Certification of TEE

Another way to guarantee the security level of the TEE is to certify the product under Common Criteria (CC), a security standard with wide recognition in the market.

- **TEE Protection Profile (EAL TEE)**: Applus+ is a Common Criteria security testing laboratory (ITSEF) and is able to carry out the required evaluation in order to obtain the Common Criteria certification for the TEE. This certification is based on the TEE Protection Profile. It can be undertaken in parallel with the GlobalPlatform certification so that manufacturers may obtain two certificates at the same time.

Benefits:

- Promote the large-scale adoption of TEE technology fostering confidence in the market, by having your functionalities standardized and certified by independent laboratories.
- Applus+ is a one-stop-shop for obtaining certification for your TEE according to the two main standards of the industry: GlobalPlatform and Common Criteria

Note: Because Applus+ Laboratories is accredited as a third party laboratory by several evaluation and certification schemes, and in order to guarantee its impartiality, Applus+ engineers are never involved in actual product development or solutions implementation.