Trusted Execution Environment (TEE)

Return to Glossary

A **Trusted Execution Environment (TEE)** is a secure area of the main processor (i.e., Central Processing Unit (CPU). It guarantees code and data loaded inside to be protected with respect to confidentiality and integrity. A TEE as an isolated execution environment provides security features such as isolated execution, the integrity of applications executing with the TEE, along with confidentiality of their assets. In general terms, the TEE offers an execution space that provides a higher level of security for trusted applications running on the device than a rich Operating System (OS) and more functionality than a 'secure element' (SE).

Source: https://en.wikipedia.org/wiki/Trusted_execution_environment

From:
https://omgwiki.org/dido/ - **DIDO Wiki**

Permanent link:
https://omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a_glossary:t:tee&rev=1628875175

Last update: **2021/08/13 13:19**