Task 1: Secure running environment

Max 300 words excluding sources.

A trusted platoform module (TPM) is a secure cryptoprocessor standardized under ISO/IEC 11889 since 2003. It is desinged to enchance platform security through hardware-based cryptographic functions. The TPM helps ensure that systems starts in a trusted state. Beginning from verified hardware and firmfare components. It includes a hardware random number generator that creates entropy-based random values for secure key generation. It using unique RSA based binding key derived from a storage root key.

https://en.wikipedia.org/wiki/Trusted_Platform_Module

Enclave is a secure enclave that could use information in security. It is one of out two forms of confidential computing environments. The other form is virtual machine. The most widely known and adopted secure is enclaves platform is intel.

Enclaves are used to create trusted execution environments. An enclave is an isolated region of code and data within the address space for an application. Only code that runs within the enclave can access data within the same enclave.

A Cryptographic Enclave or Secure Enclave is a hardware-level security isolation and memory encryption technique within a computing environment. In this computing environment, sensitive operations such as generating and managing cryptographic keys or other highly prudent actions occur with a high degree of integrity and confidentiality. It can isolate cryptographic codes and data from anyone with privileges.

https://www.edgeless.systems/wiki/what-is-confidential-computing/secure-enclaves

https://www.ve3.global/cryptographic-enclave-problems-common-hardware-enclaves-for-better-security/

https://en.wikipedia.org/wiki/Trusted_Platform_Module