Terminology

https://docs.google.com/document/d/1xZ6IX0w0jaWDbLMFNAybTF3FpLnQ5TJ98nzIWbsbFnY/edit

Confidential Library	a library (e.g., an ‘enclave’) that is executed inside a hardware-based TEE, and is used by an application outside the TEE
Confidential Process	a process (e.g., a “Trusted Application”) which is executed inside a hardware-based HW TEE
Confidential Container	an OCI-compliant container that is executed inside a hardware-based TEE
Confidential VM	a virtual machine that executes inside utilizing a hardware-based TEE, whereby code and data within the entire VM image is protected from the hypervisor and the host operating system.

Technology Contexts

- SGX
  - Lifetime of an instance of trusted code+data is tied to a single untrusted process in unencrypted space. All I/O is via this process.
  - Library binaries are loaded then encrypted, and initial local storage / threads are allocated in encrypted space.
  - During initial library loading, trusted Firmware does measurement of binaries. The encryption phase is not touchable by the OS.
  - System calls/high privilege operations are not allowed while TEE is being processed in CPU. TEE state is preserved during CPU interrupts.
  - IPCs and I/O out of the TEE are protectable by a mutually authenticated secure channel, as shared memory isn't allowed.
- SEV-SNP
  - Guest VMs and supplemental data are initialized then launched, with each load sequentially measured by Firmware.
  - Paging control is done by the Hypervisor so that the CPU will restrict writing only to the page owner.
  - A context page not readable by the Hypervisor is passed into the CPU to allow interpretation of each page's contents.
  - Any shared memory remains within the confines of the VM.
  - Any I/O beyond the VM is not protected by default. Mutually authenticated secure channel establishment would be needed.
- OP-TEE/TrustZone
  - A base of trustworthiness of the Firmware+ minimal Kernel is established based on verified signatures on the loaded code+data payload.
  - This TEE is not directly addressable by other TEEs or any other untrusted code, including host/guest OSes and VMM running on the same HW)
  - Firmware loads into a single TEE various bits of application libraries/interpretable code/data, each of which is measurable and attestable layer.
  - A set of standard APIs are exposed to the untrusted code for requesting services from the trusted side. This includes IPC services that can be invoked among TEEs.
  - I/O Peripheral code may also be verified, and message passing to/from the application is via the trustworthy base of the Firmware + minimal Kernel.

Confidential Compute – Packaging Options