

iDash2023 Track 3 FAQ

Q1: How TCB is measured? Are dynamically linked libraries (e.g., libstdc++.so) included in TCB? If so, it is easy to exceed the 1MB threshold.

A: The TCB size is measured by executable size. It should include the (dynamic) libraries if any, but not the OS and its associated standard libraries.

Q2: Are the two SEV VMs on different machines or the same machine? If they are on the same machine, can we use shared memory to communicate instead of networking?

A: They should be on the same type of VMs, but can be guaranteed on the same machine (as in the cloud environment like Azure).

Q3: Is it allowed to modify the SEV hypervisor?

A: We will not allow to modify the hypervisor to simulate the execution in the cloud environment..

Q4: When using SEV, the host is responsible for creating SEV VMs. Is the input file placed in SEV VMs or the host?

A: In SEV VMs.

Q5: Can the program only run in user mode, or can it also run in kernel mode?

A: We do not have limitations on this.