

Intel TDX module uses Secure EPT and MKTME to enforce the access control
btw. TDs, as well as TDs and legacy VMs

