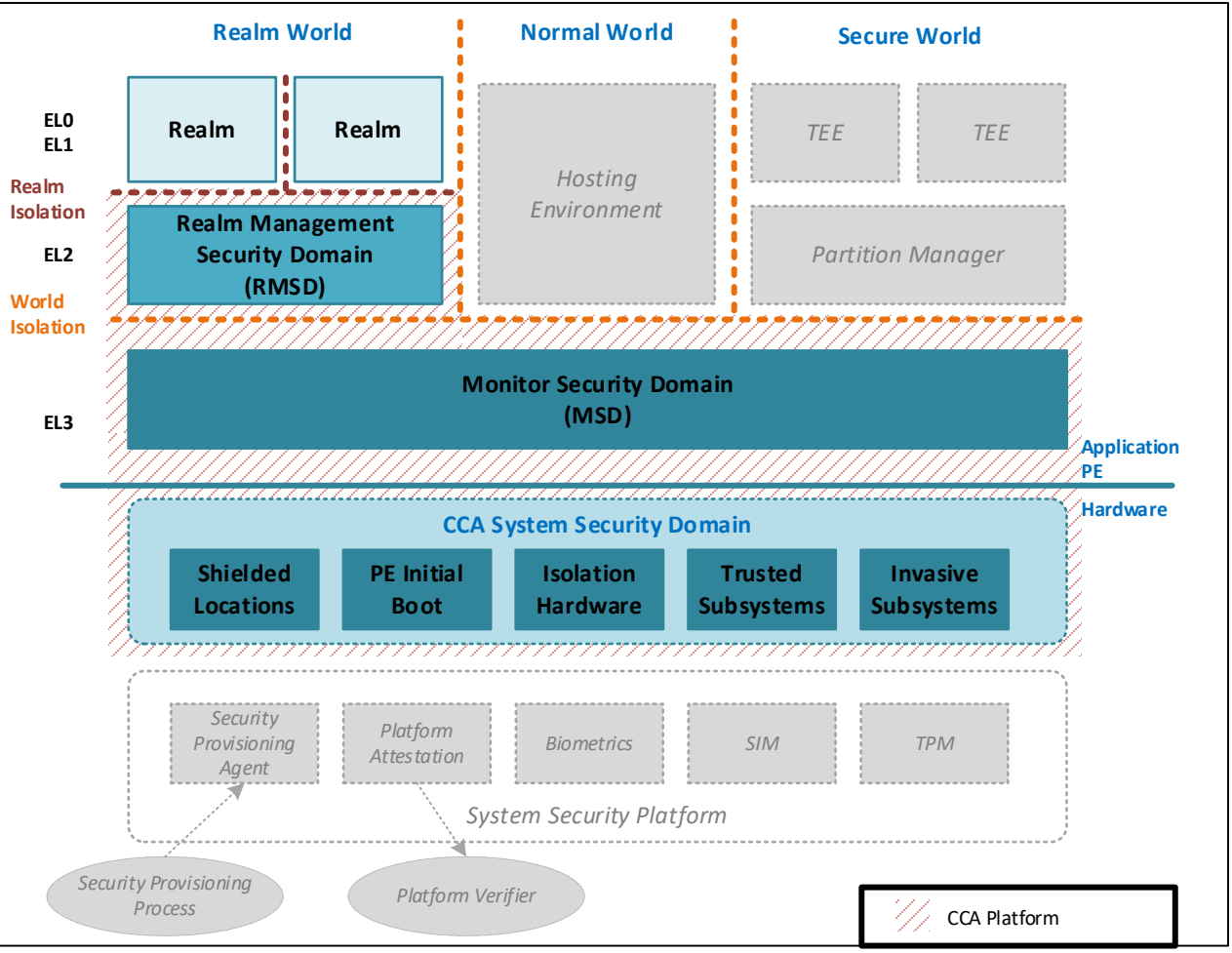
Realm World
Normal World
Secure World
EL0
EL1
Realm
Realm
Realm
Isolation
Hosting
Environment
TEE
TEE
EL2
Realm Management
Security Domain
(RMSD)
Partition Manager
World
Isolation
EL3
Monitor Security Domain
(MSD)
Application
PE
Hardware
CCA System Security Domain
Shielded
Locations
PE Initial
Boot
Isolation
Hardware
Trusted
Subsystems
Invasive
Subsystems
Security
Provisioning
Agent
Platform
Attestation
Biometrics
SIM
TPM
System Security Platform
Security Provisioning
Process
Platform Verifier
CCA Platform