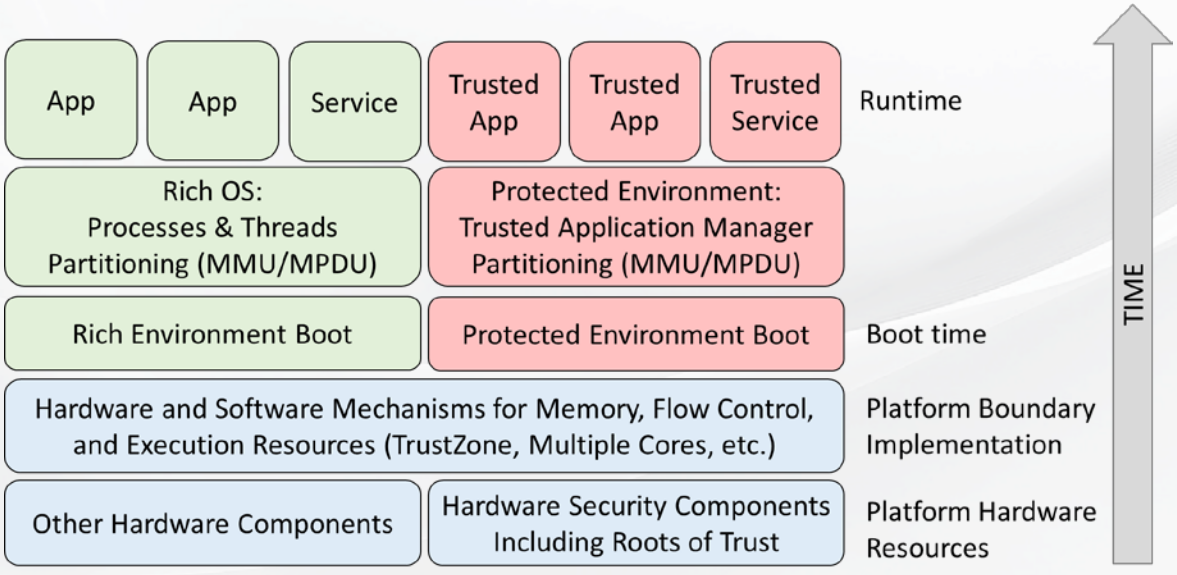
TCG Guidance on Mobile Reference Architecture (MRA)

People rely on their mobile platforms in their personal and professional lives. Trusted mobile platforms offer key benefits (e.g. device integrity and protection of secrets) for a variety of applications. Interoperable solutions can facilitate adoption of trusted mobile architectures and services.

MRA defines a framework for interoperable Protected Environments and Trusted Computing technologies in mobile systems. TCG Mobile Platform WG has collaborated with GlobalPlatform to align this framework with trusted computing technologies in mobile ecosystems (e.g. TCG TPM 2.0 and GlobalPlatform Trusted Execution Environment). MRA offers guidance to OEMs, system integrators, and application developers who are building mobile devices with strong security services.

MRA defines a Protected Environment as a functional element with its own execution and memory resources that are isolated from other components. A mobile system without hardware for Trusted Execution Environment Provisioning (TEEP) Architecture (RFC 9397) compliance can still establish a Protected Environment during Secure Boot. All Protected Environments and Trusted Applications are secured by underlying Roots-of-Trust (RoT), such as storage and measurement. The diagram below provides a notional depiction of the MRA.



Copyright © TCG 2025