Trusted Execution Environment (TEE)

- protection during the boot process
- each device has a hardware key
- Trusted Computing Base
  - ↳ entire OS
  - ↳ for boot

- Runtime Protection
  - someone planted a backdoor to Guest OS using x2
  - complicated system → will have bugs or hacks
  - hypervisor (EL2) → not compromised if guest OS is compromised

Virtual Processor

- separate processor
- indep. of main processor
  - ↳ own kernel, drivers, etc.

ARM TrustZone

- normal v. secure world
- EL3 for secure monitor
  - ↳ secure world
- secure world is isolated
- switch done by secure monitor
  - ↳ certain space of memory is reserved

- encryption done to prevent copyright problems