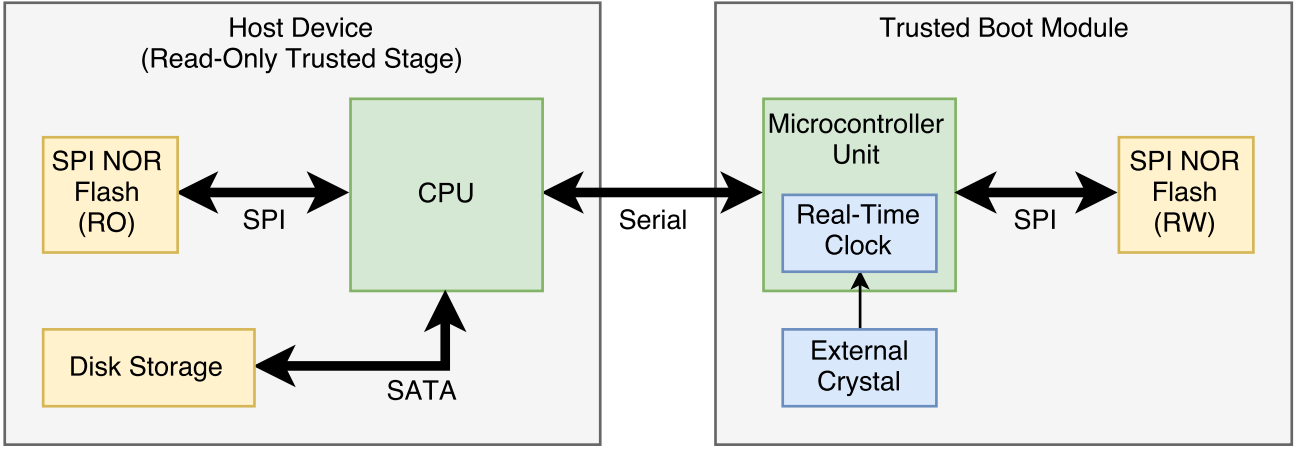
Host Device
(Read-Only Trusted Stage)
SPI NOR
Flash
(RO)
SPI
CPU
Disk Storage
SATA
Serial
Trusted Boot Module
Microcontroller
Unit
Real-Time
Clock
External
Crystal
SPI
SPI NOR
Flash
(RW)