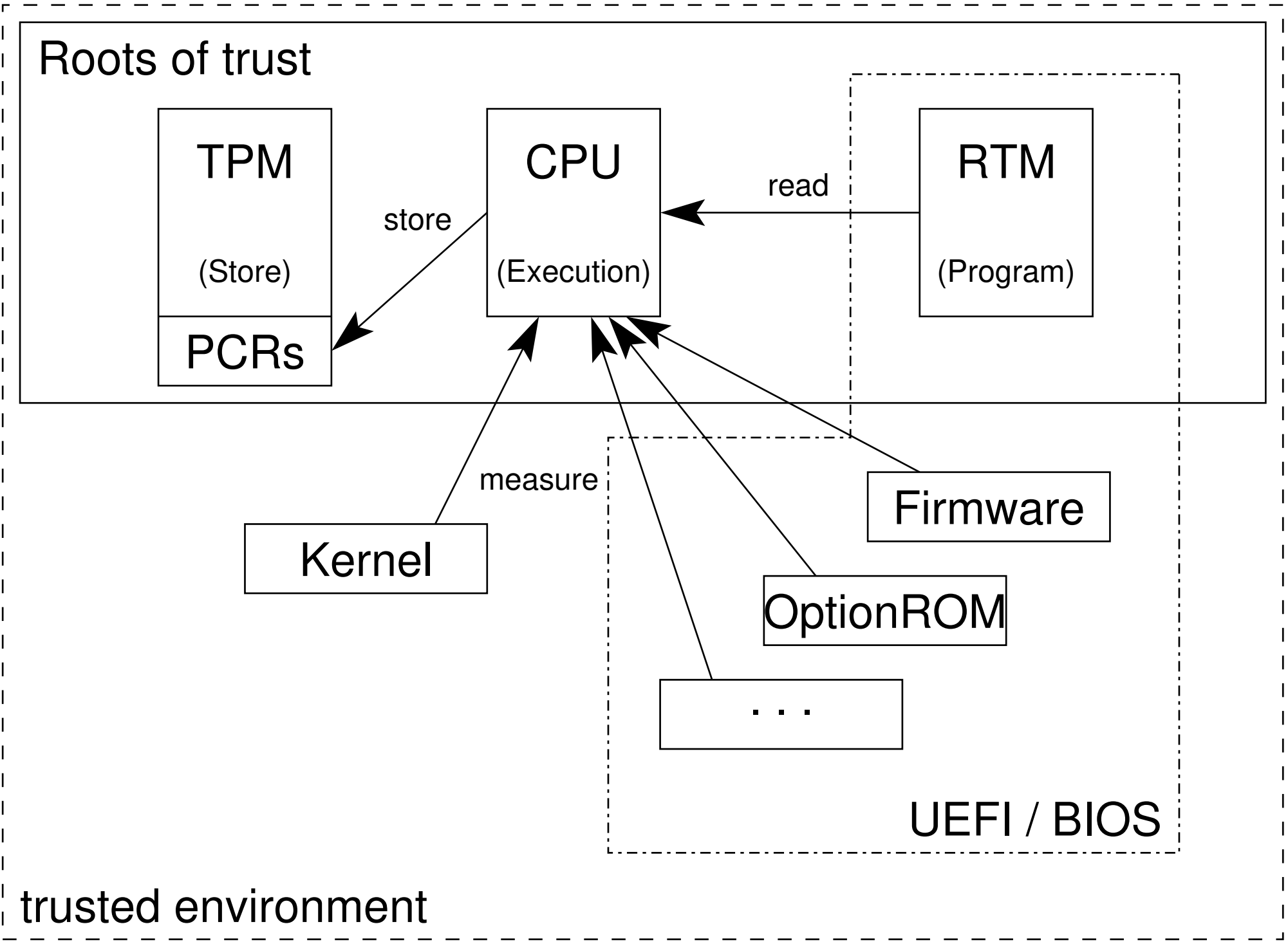
Roots of trust
TPM
(Store)
PCRs
CPU
(Execution)
RTM
(Program)
read
store
measure
Kernel
Firmware
OptionROM
. . .
UEFI / BIOS
trusted environment