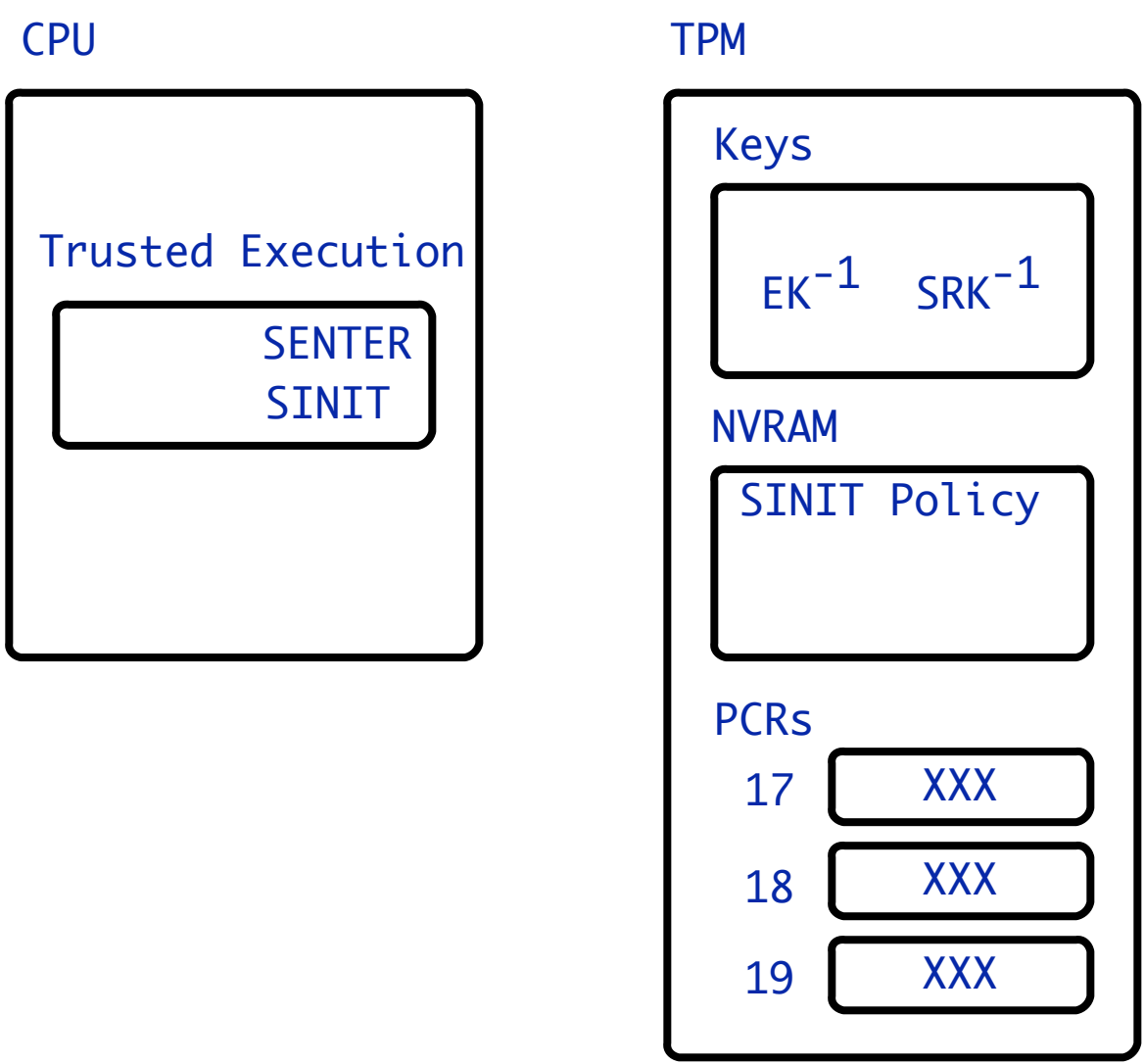
CPU
Trusted Execution
SENTER
SINIT
TPM
Keys
EK-1 SRK-1
NVRAM
SINIT Policy
PCRs
17 XXX
18 XXX
19 XXX