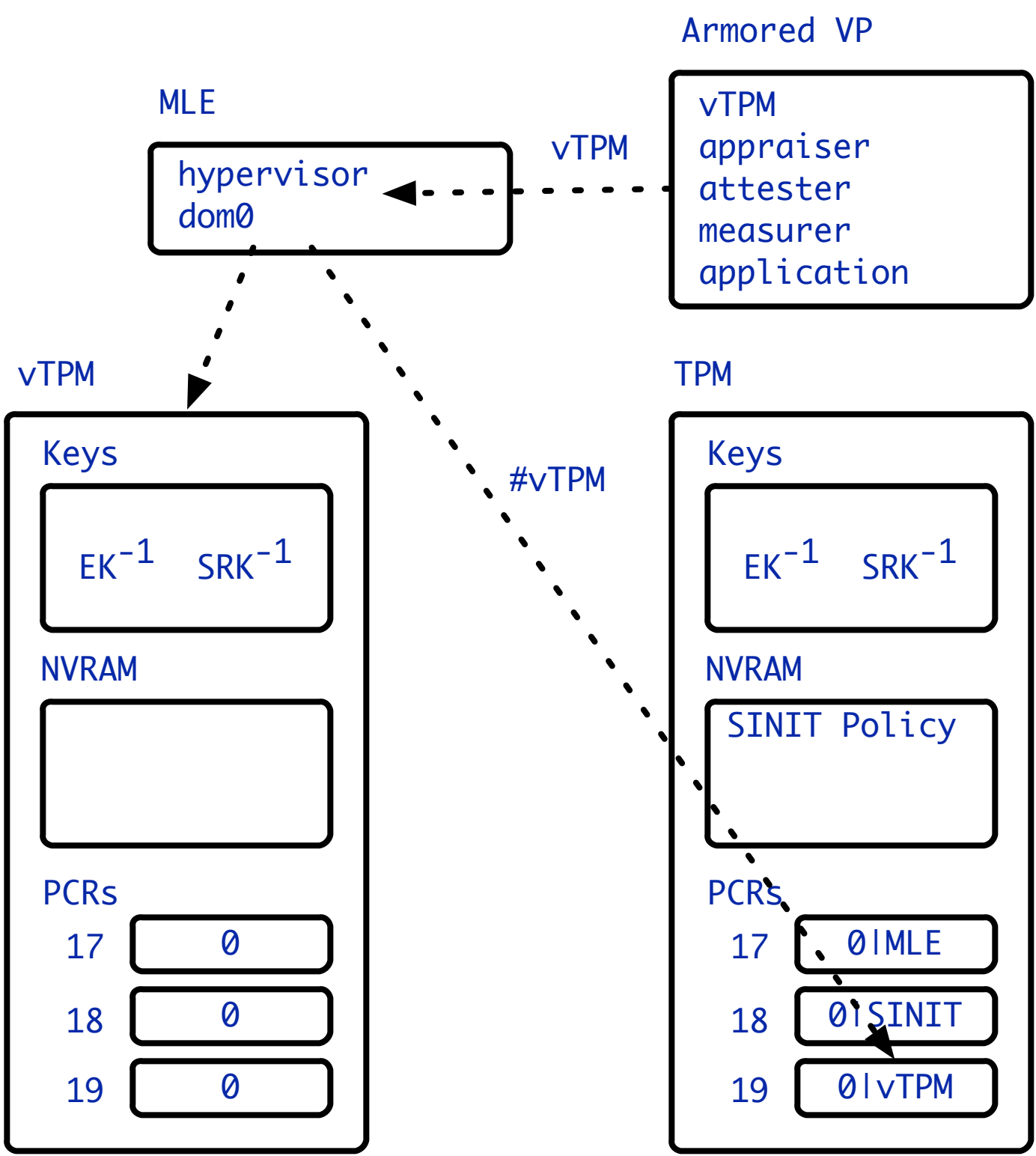
Armored VP
vTPM
appraiser
attester
measurer
application
MLE
hypervisor
dom0
vTPM
vTPM
Keys
EK-1 SRK-1
NVRAM
PCRs
17 0
18 0
19 0
#vTPM
TPM
Keys
EK-1 SRK-1
NVRAM
SINIT Policy
PCRs
17 0|MLE
18 0|SINIT
19 0|vTPM