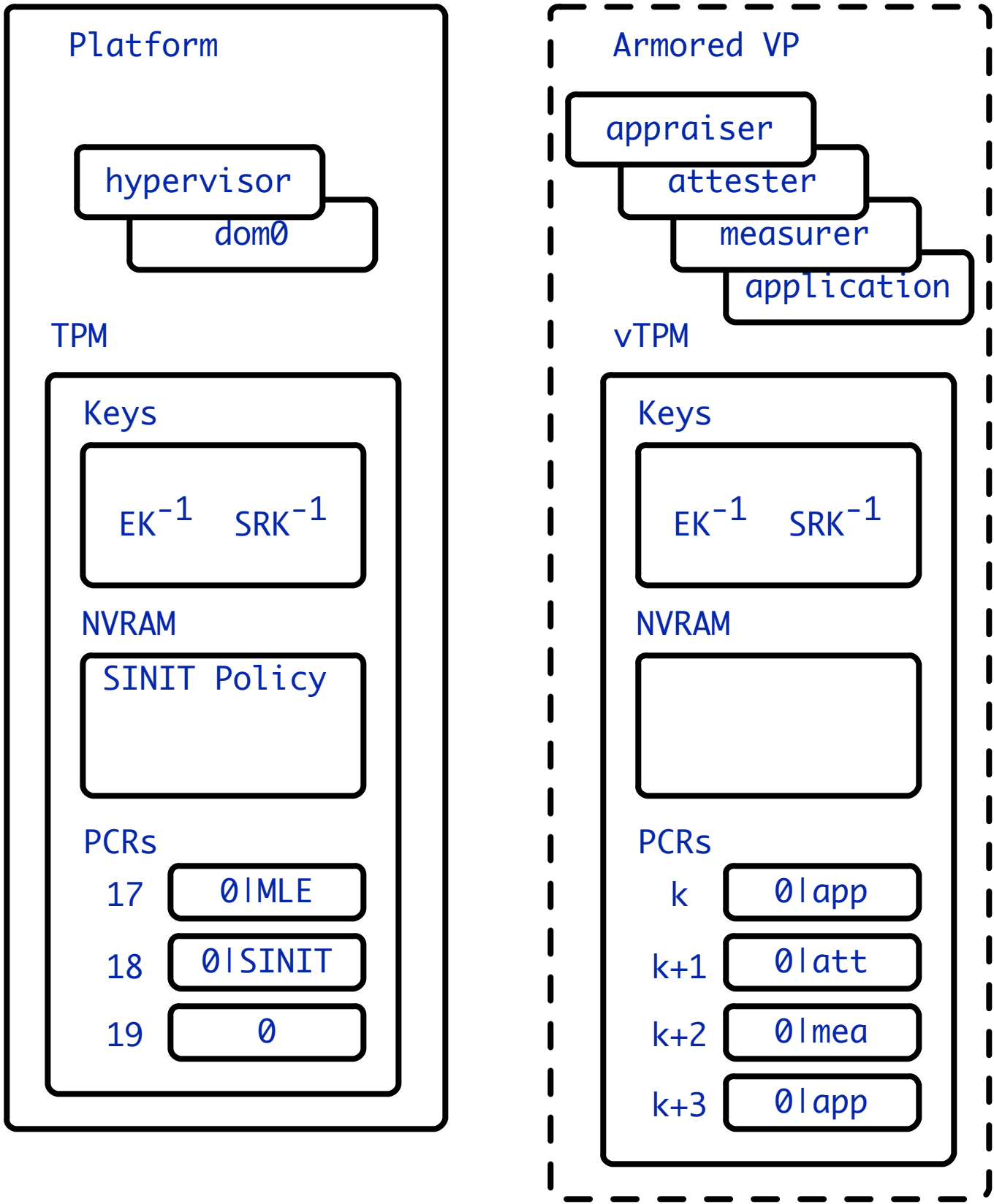
Platform
hypervisor
dom0
TPM
Keys
EK-1 SRK-1
NVRAM
SINIT Policy
PCRs
17 0|MLE
18 0|SINIT
19 0
Armored VP
appraiser
attester
measurer
application
vTPM
Keys
EK-1 SRK-1
NVRAM
PCRs
k 0|app
k+1 0|att
k+2 0|mea
k+3 0|app