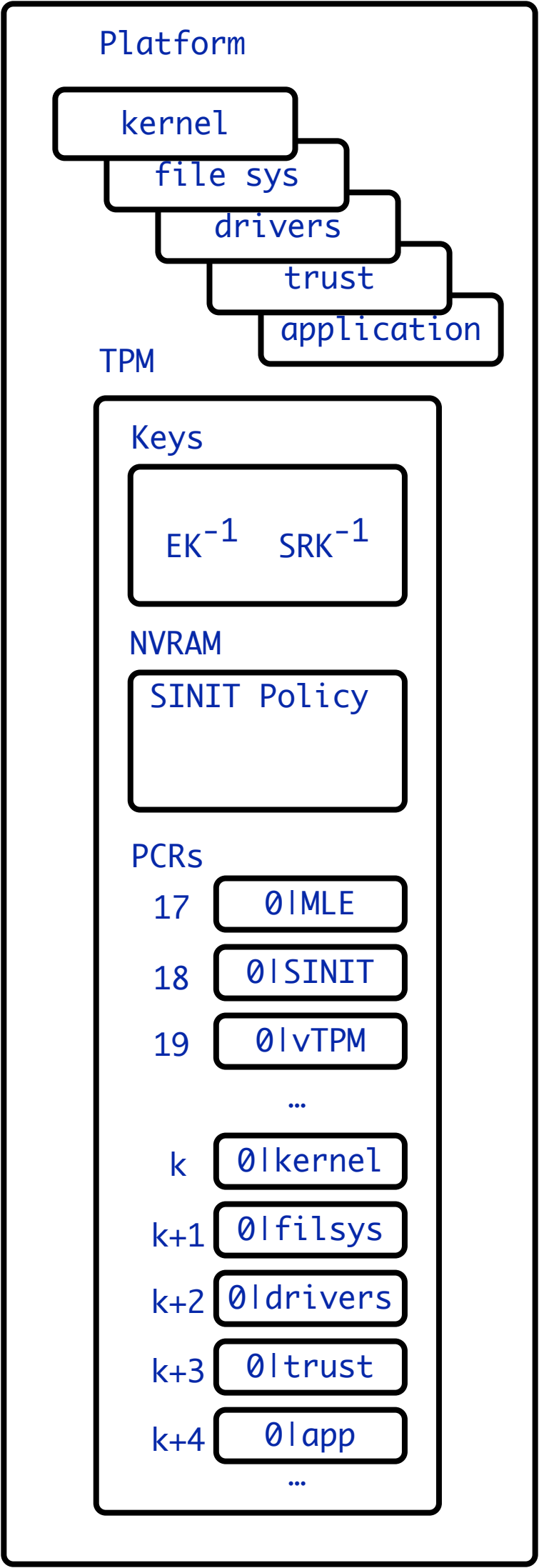
Platform
kernel
file sys
drivers
trust
application
TPM
Keys
EK-1 SRK-1
NVRAM
SINIT Policy
PCRs
17 0|MLE
18 0|SINIT
19 0|vTPM
…
k 0|kernel
k+1 0|filsys
k+2 0|drivers
k+3 0|trust
k+4 0|app
…