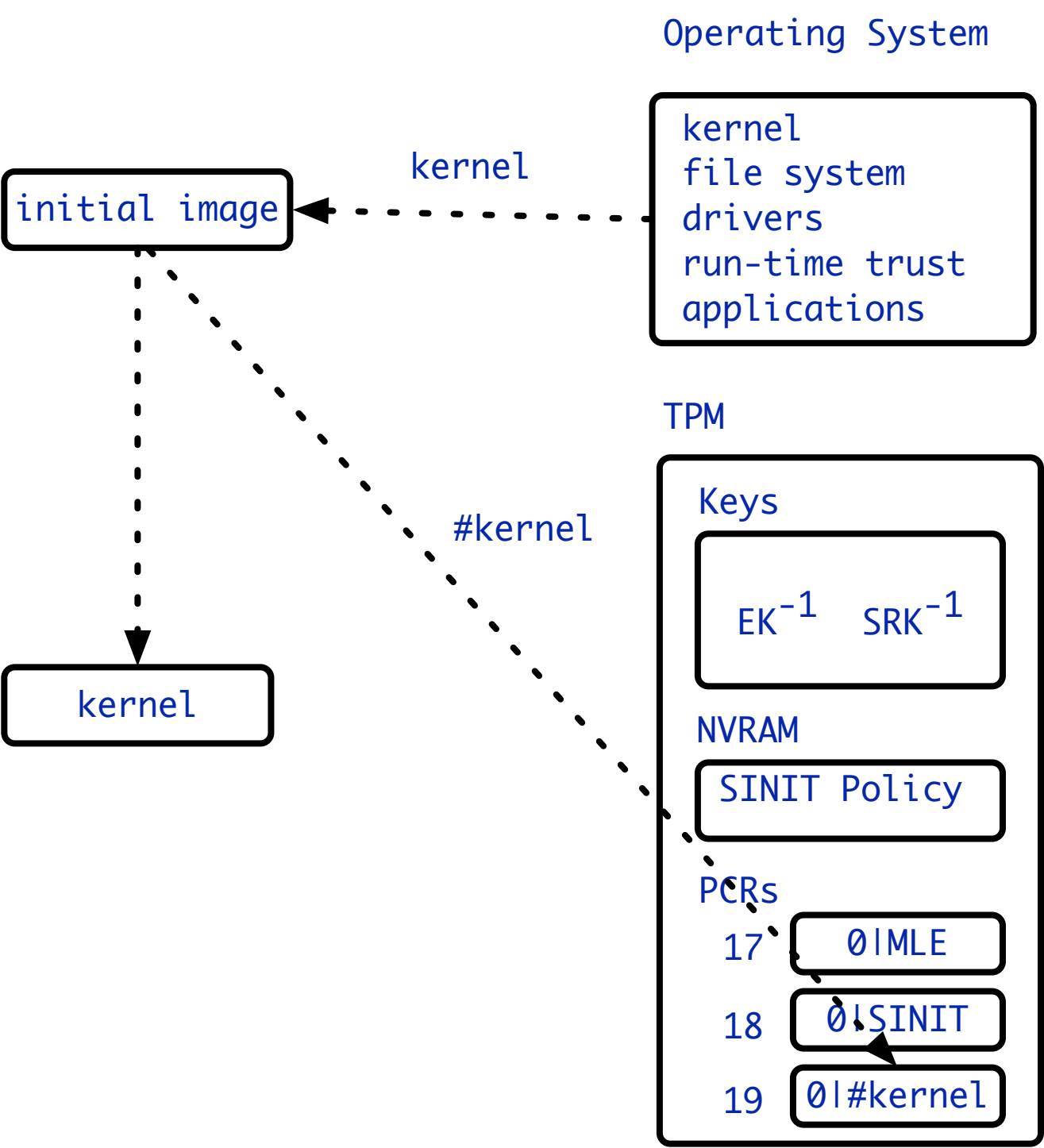
Operating System
kernel
file system
drivers
run-time trust
applications
kernel
initial image
kernel
TPM
Keys
EK-1 SRK-1
#kernel
NVRAM
SINIT Policy
PCRs
17
0|MLE
18
0|SINIT
19
0|#kernel