

Operating System

kernel
file system
drivers
run-time trust
applications

TPM

initial image

Keys

EK^{-1} SRK^{-1}

NVRAM

SINIT Policy

PCRs

17 0IMLE

18 0ISINIT

19 0