

CPU

Trusted Execution

SENDER
SINIT

TPM

Keys

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

NVRAM

SINIT Policy

PCRs

17 -1

18 -1

19 -1