

Armored VP

vTPM
appraiser
attester
measurer
application

TPM

hypervisor

dom0

Keys

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

NVRAM

SINIT Policy

PCRs

17 0IMLE

18 0ISINIT

19 0