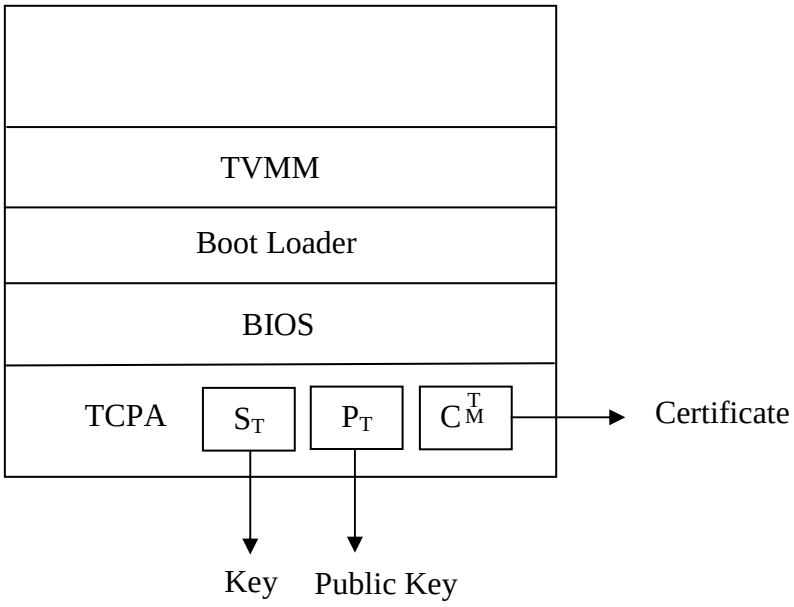
Terra TVMM Continuation 4/12

Terra Goals

-root secure
-remote attestation

Remote Attestation

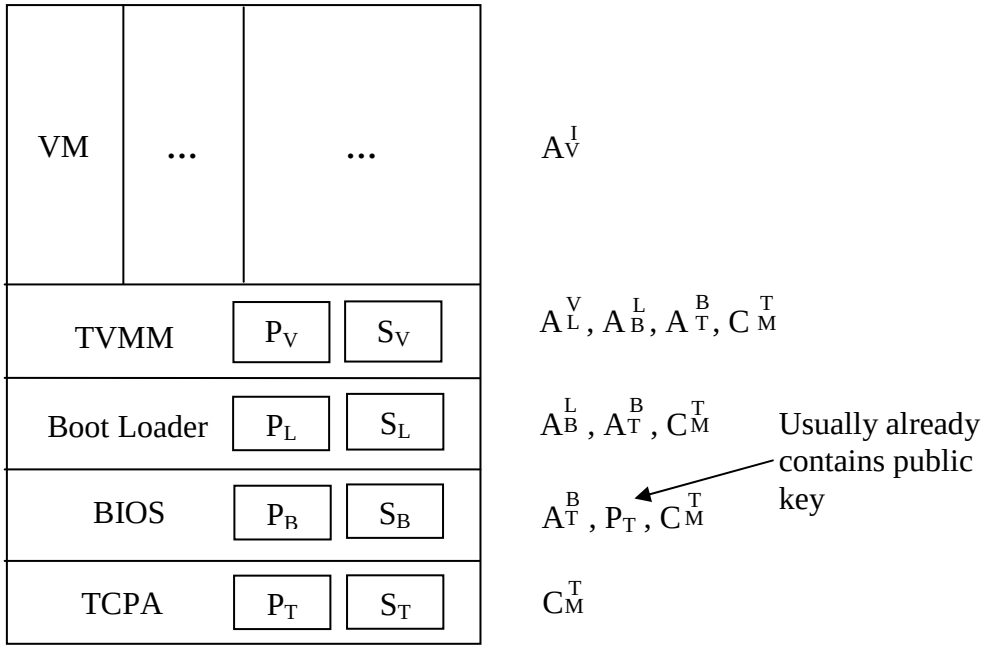
-Act of proving to remote party what software you are running.
=> add special tamper-proof hardware to machine



Identify of Bios = hash (BIOS machine Code)

$A_T^B = Sig (S_T , P_B \| h (B))$

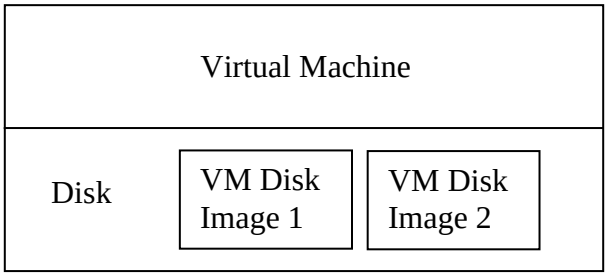
Attestation generated by T for B

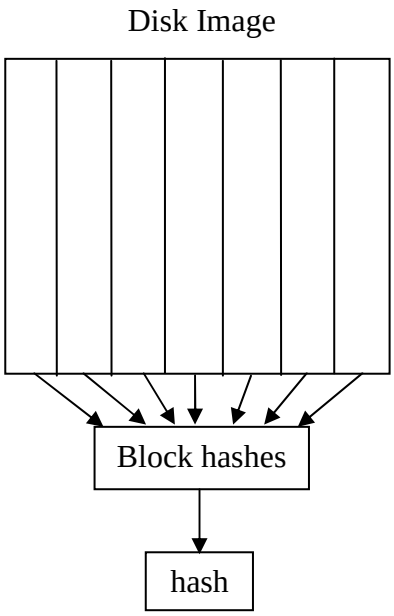


=> must not hash mutable parts of BIOS
=> sign binary image and then run

An idea would be to have OS separate mutable from immutable image, but, good OS have difficult time doing this.

Attesting to Large Disk Images





1. Load hash table and master hash
2. verify master hash against hash table

On Page Load

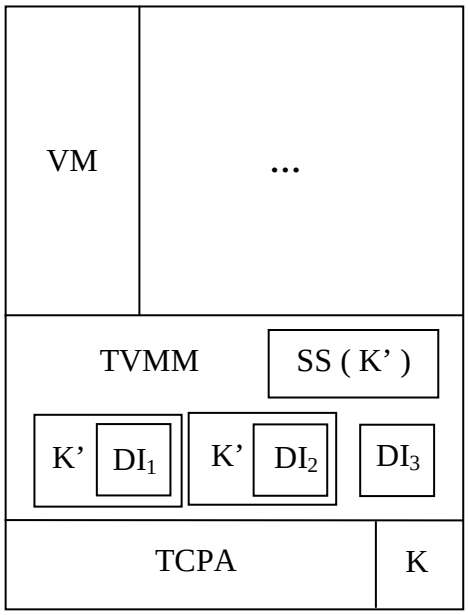
Compare hash of page to entry in table.

Remote Attestation

-requires trusting
  -TCPA hardware security
  -entire software stack
  -software security of entire stack
  -hardware manufacturer
  -other hardware hacks

Root Secure

-encrypt disk images to prevent owner from seeing contents
-cannot store key on disk (unencrypted)
-May also prevent tampering of disk using MACs



Sealed Storage

SS (M) = E_{KT} (h (requestor) || M)

message