vTPM Architecture

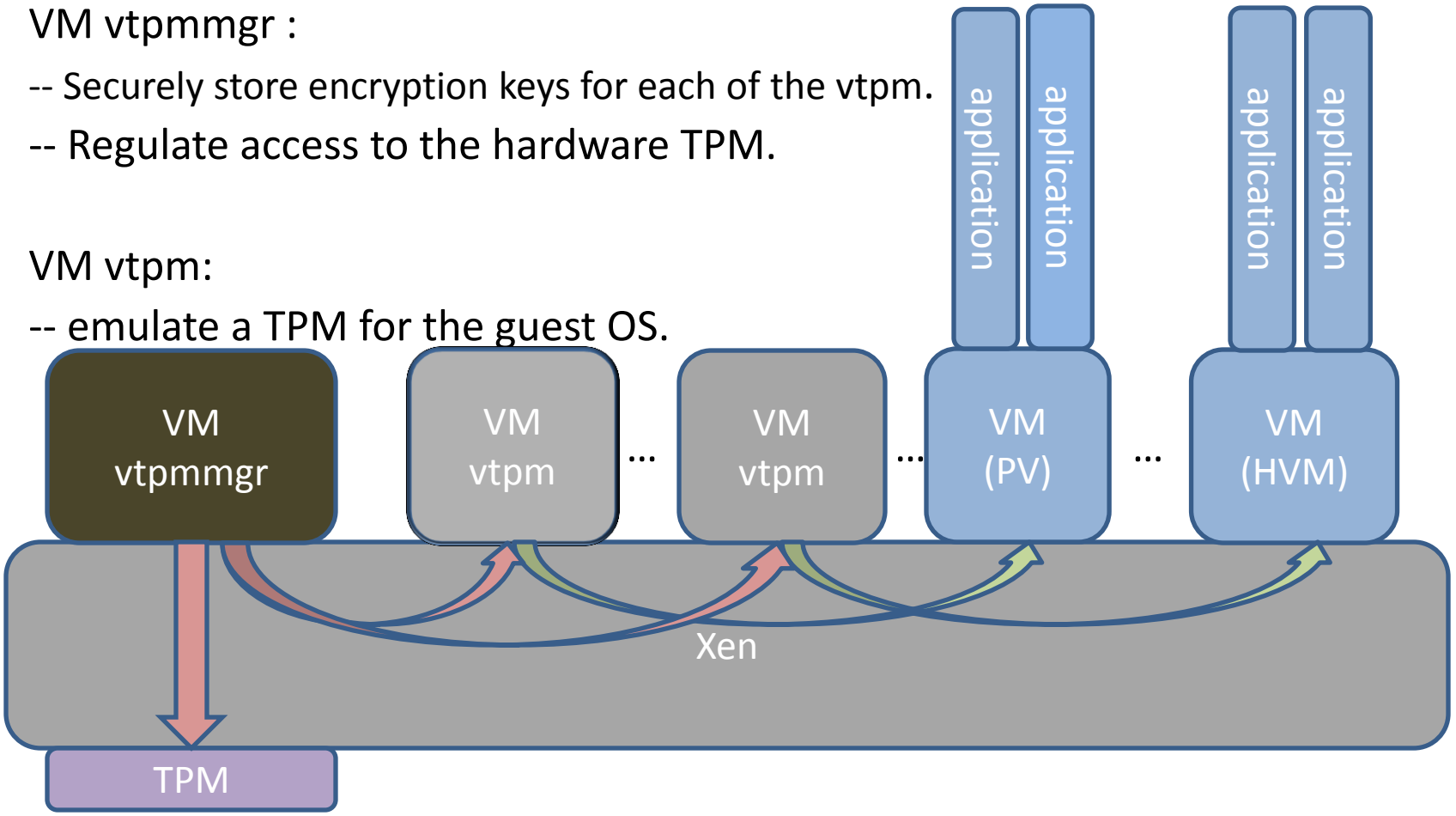
VM vtpmmgr :

-- Securely store encryption keys for each of the vtpm.

-- Regulate access to the hardware TPM.

VM vtpm:

-- emulate a TPM for the guest OS.



vTPM for HVM virtual machine .

- Qemu frontend
- Hvmloader/seabios

  --0xfed40000~0xfed45fff / ACPI