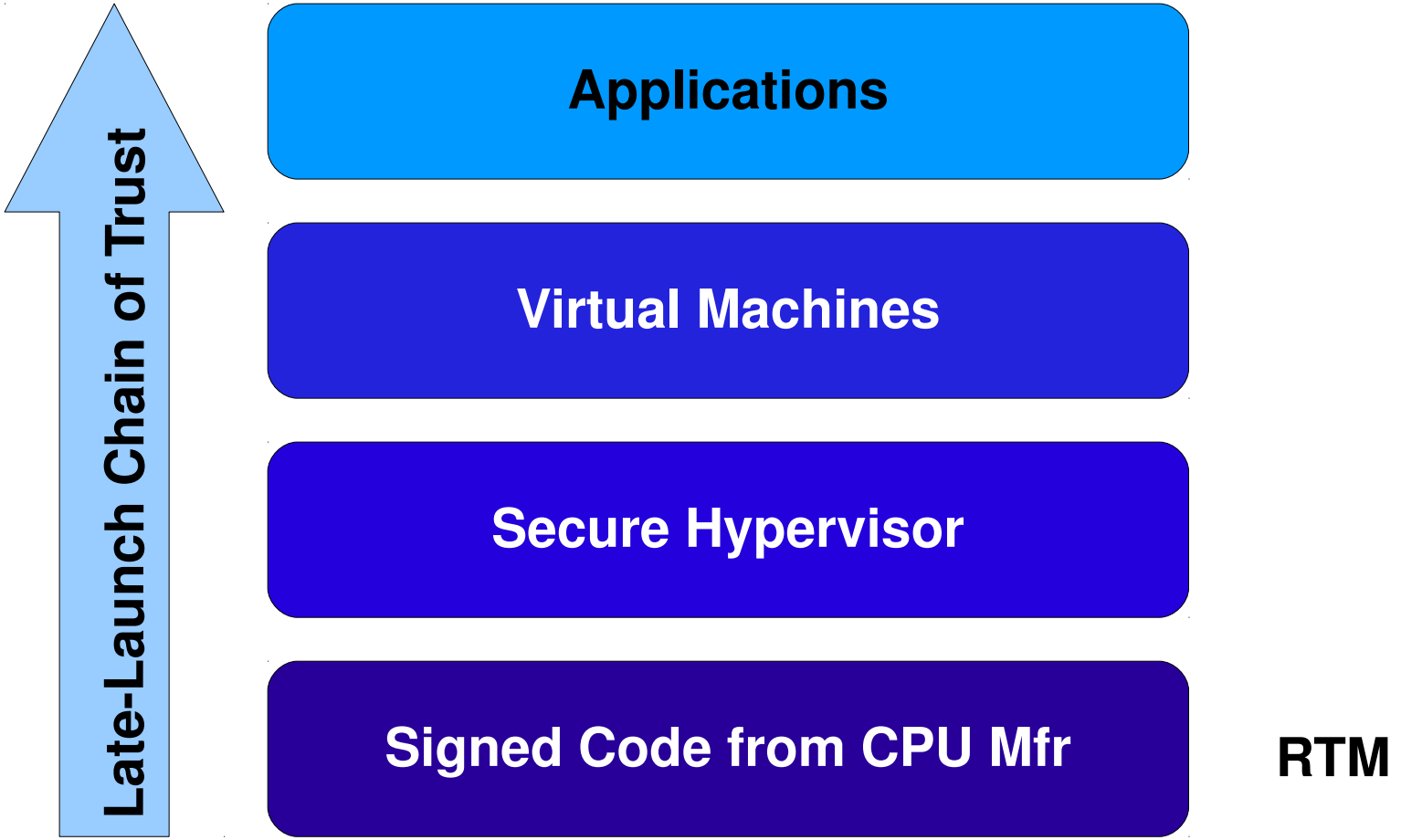
Late-Launch Chain of Trust
Applications
Virtual Machines
Secure Hypervisor
Signed Code from CPU Mfr
RTM