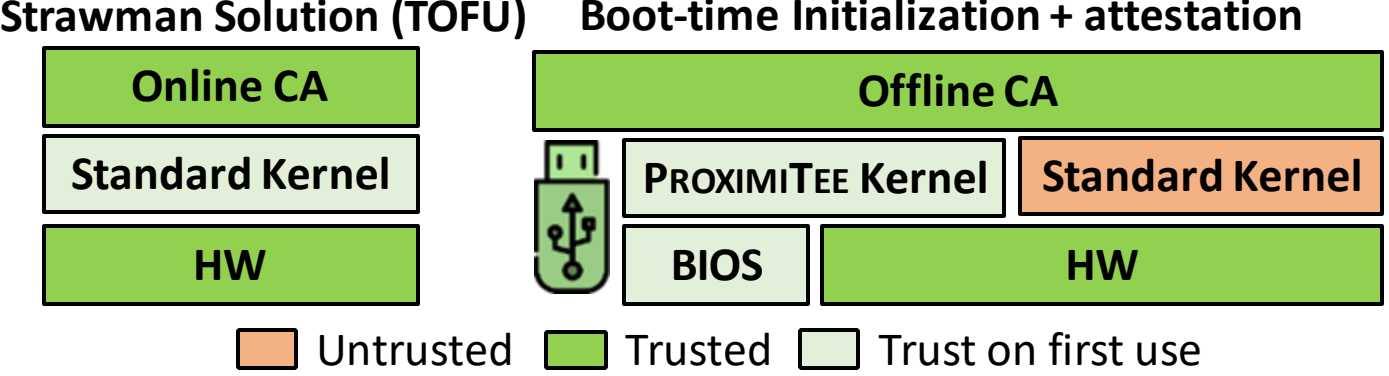
Strawman Solution (TOFU)
Online CA
Standard Kernel
HW
Boot-time Initialization + attestation
Offline CA
ProximiTee Kernel
Standard Kernel
BIOS
HW
Untrusted
Trusted
Trust on first use