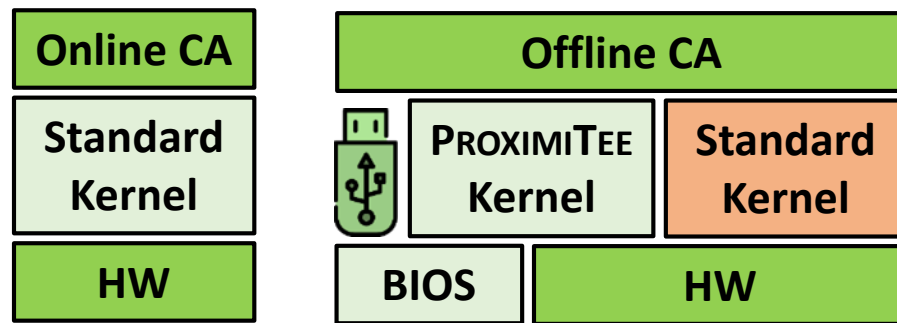


Strawman Solution (TOFU) **Boot-time Initialization + attestation**



 Untrusted  Trusted  Trust on first use