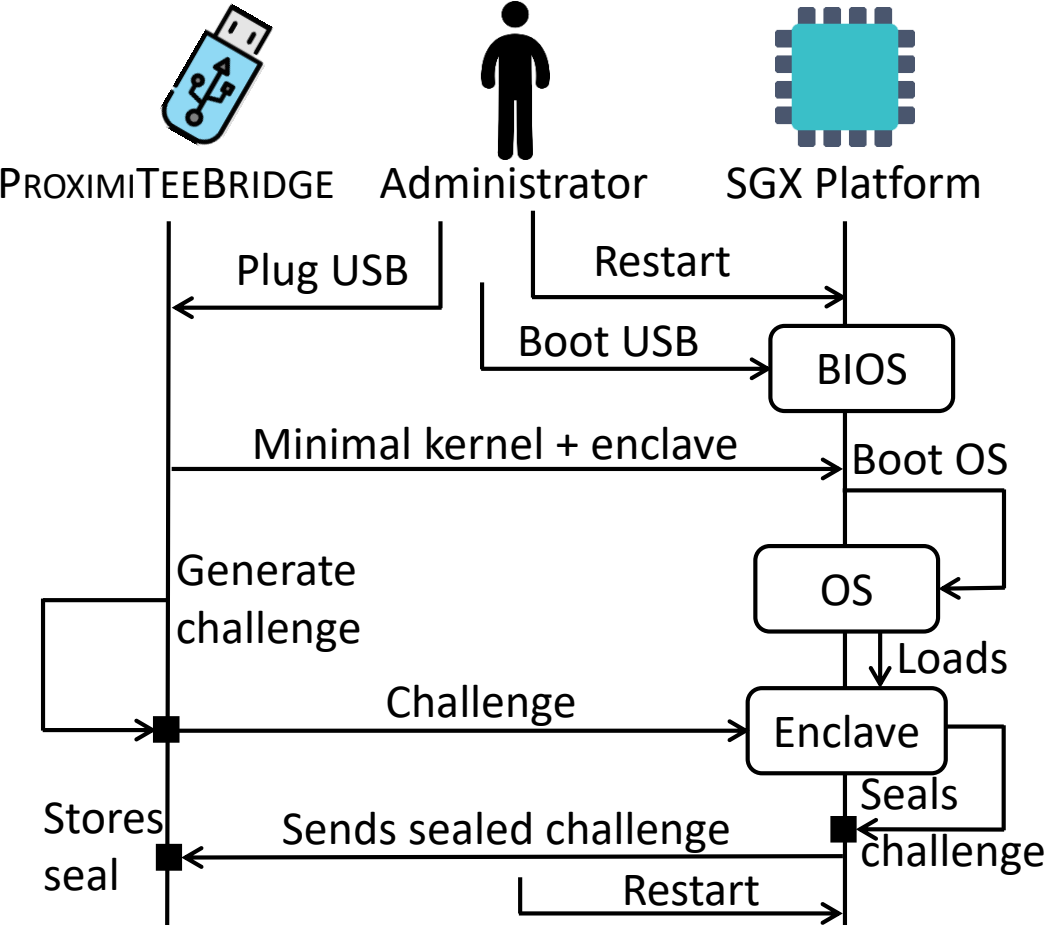
ProximiTEEBridge
Administrator
SGX Platform
Plug USB
Restart
Boot USB
BIOS
Minimal kernel + enclave
Boot OS
Generate challenge
OS
Loads
Challenge
Enclave
Seals challenge
Stores seal
Sends sealed challenge
Restart