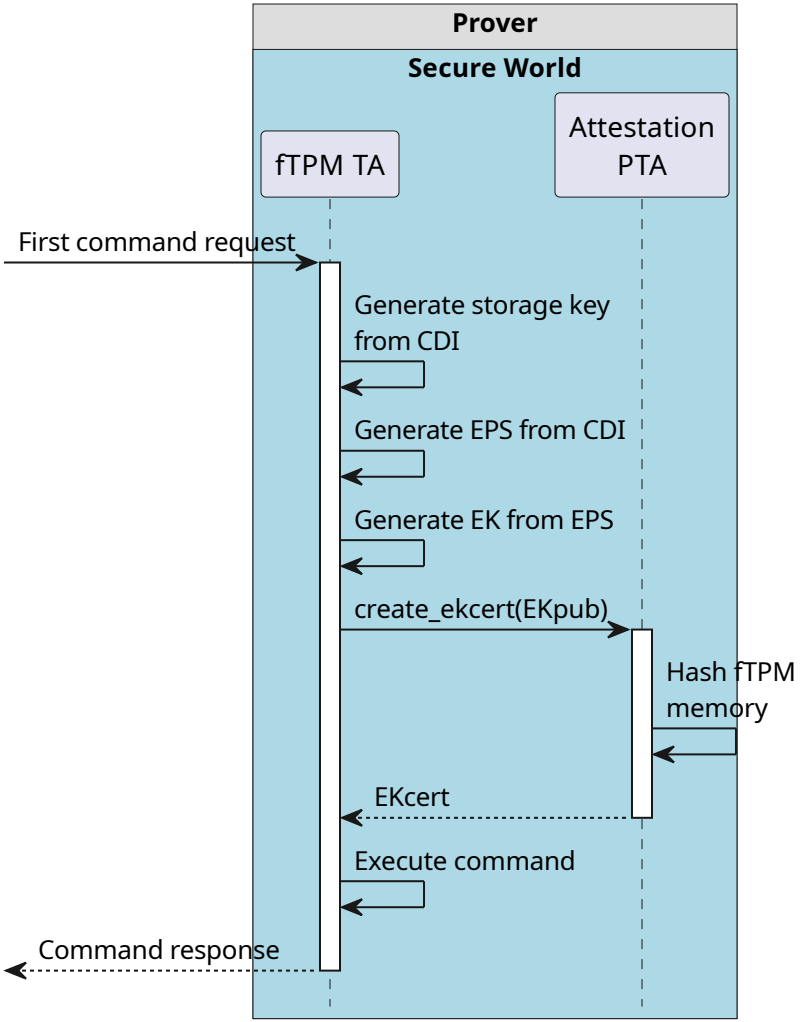
Prover
Secure World
fTPM TA
Attestation PTA
First command request
Generate storage key from CDI
Generate EPS from CDI
Generate EK from EPS
create_ekcert(EKpub)
Hash fTPM memory
EKcert
Execute command
Command response