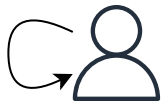


5. Verify report



Verifier

4. Attestation report

6. Open secure channel to CVM

CVM

2. Request report with
user data: Hash(pubkey)

1. create new key pair

3. Attestation report

TEE Hardware

