

TrustFA Agent

App (Legacy OS)

Remote Server

2. Boot

1. $E_{K_{\text{public}}}(\text{nonce})$

SSL Session

3. Load private key

4. Data (D) collection

5. Data processing

7. $E_{K_{\text{private}}}(\text{D}, \text{nonce})$

SSL Session

6. $E_{K_{\text{private}}}(\text{D}, \text{nonce})$

8. Verification