

1a.Verifier	: Generate nonce
2a.Verifier→Attestor	: Attestation Request (nonce, PCRno)
3a.Attestor	: Loadkey(AIKkey)
4a.Attestor→TPM	: Execute TPM Quote Operation
5a.TPM	: Quote=sig{PCR,nonce}AIKpriv
6a.TPM→Attestor	: Quote
7a.Attestor	: Generate (SML)
8a.Attestor→Verifier	: Quote, SML and cert(AIKpub)
9a.Verifier	: validate cert(AIKpub)
9b.Verifier	: validate sig{PCR,nonce}AIKpriv
9c.Verifier	: validate SML using PCR