Abbreviations \sim M_22 = VERSION \sim M_23 = CHALLENGE_AUTH ~M_24 = extLSB(hash(cert(IDPTx,spk(sskPTx),sign((IDPTx,spk(sskPTx)),sskCA 1)))) \sim M_25 = sign((hash(cert(IDPTx,spk(sskPTx),sign((IDPTx, spk(sskPTx)),sskCA_1))),VERSION,CHALLENGE,nonce_1, VERSION, CHALLENGE_AUTH, extLSB(hash(cert(IDPTx, spk(sskPTx),sign((IDPTx,spk(sskPTx)),sskCA_1))))), sskPTx) \sim X_1 = (VERSION,CHALLENGE_AUTH, \sim M_24, \sim M_25) = (VERSION, CHALLENGE_AUTH,extLSB(hash(cert(IDPTx,spk(sskPTx), sign((IDPTx,spk(sskPTx)),sskCA_1)))),sign((hash(cert(IDPTx,spk(sskPTx),sign((IDPTx,spk(sskPTx)), sskCA_1))),VERSION,CHALLENGE,nonce_1,VERSION,CHALLENGE_AUTH, A trace has been found. extLSB(hash(cert(IDPTx,spk(sskPTx),sign((IDPTx, spk(sskPTx)),sskCA_1))))),sskPTx)) \sim M_28 = VERSION \sim M_29 = CERTIFICATE \sim M_30 = IDPTx \sim M_31 = spk(sskPTx) \sim M_32 = IDPTx \sim M_33 = spk(sskPTx) \sim M_34 = sign((IDPTx,spk(sskPTx)),sskCA_1) \sim X_2 = (VERSION,CERTIFICATE,cert(IDPTx, \sim M_1, \sim M_34)) (VERSION, CERTIFICATE, cert(IDPTx, spk(sskPTx), sign((IDPTx,spk(sskPTx)),sskCA_1))) **Honest Process** Attacker {1}new sskCA_1 \sim M = spk(sskCA_1) \sim M_1 = spk(sskPTx) {7}new dummyIDPTx_1 {8}new dummySskPTx_1 \sim M_2 = spk(dummySskPTx_1)

