Abbreviations \sim X_1 = (VERSION,CERTIFICATE,cert(IDPTx, \sim M_1, \sim M_30)) (VERSION, CERTIFICATE, cert(IDPTx, spk(sskPTx), sign((IDPTx,spk(sskPTx)),sskCA_1))) \sim M 34 = VERSION \sim M_35 = CHALLENGE_AUTH ~M_36 = extLSB(hash(cert(IDPTx,spk(sskPTx),sign((IDPTx,spk(sskPTx)),sskCA_1)))) \sim M_37 = sign((hash(cert(IDPTx,spk(sskPTx),sign((IDPTx, spk(sskPTx)),sskCA 1))),VERSION,CHALLENGE,nonce 1, A trace has been found. VERSION, CHALLENGE_AUTH, extLSB (hash(cert(IDPTx, spk(sskPTx),sign((IDPTx,spk(sskPTx)),sskCA_1))))), sskPTx) \sim X_2 = (VERSION,CHALLENGE_AUTH,extLSB(\sim M_23), \sim M_37) (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, extLSB (hash(cert(IDPTx, spk(sskPTx),sign((IDPTx,spk(sskPTx)),sskCA_1))))), sskPTx)) **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) Beginning of process PRx Beginning of process PTx \sim M_3 = DigitalPing a \sim M 4 = SIG $ID(\sim M_5,\sim M_6,\sim M_7,\sim M_8) = ID(MajorVer,MinorVer,$ MC,BDID) \sim M 9 = CFG a 1 \sim M 10 = FOD \sim M_11 = SRQ a 3 \sim M_12 = SRQen a 4 \sim M 13 = CE \sim M 14 = RP $(\sim M | 15, \sim M | 16) = (VERSION, GET DIGESTS)$ a 5 a_6 a 7 \sim M 17 = ACK a 8 \sim M 18 = ACK a 9 \sim M 19 = ACK a 10 \sim M 20 = ACK a 11 a 12 (VERSION, GET DIGESTS) $(\sim M_21,\sim M_22,\sim M_23) = (VERSION,DIGESTS,hash(cert($ IDPTx,spk(sskPTx),sign((IDPTx,spk(sskPTx)),sskCA_1)))) $(VERSION]DIGESTS,\sim M_23) = (VERSION,DIGESTS,hash($ cert(IDPTx,spk(sskPTx),sign((IDPTx,spk(sskPTx)), sskCA 1)))) $(\sim M_24,\sim M_25) = (VERSION,GET_CERTIFICATE)$ (VERSION, GET CERTIFICATE) $(\sim M_26, \sim M_27, cert(\sim M_28, \sim M_29, \sim M_30)) = (VERSION,$ CERTIFICATE,cert(IDPTx,spk(sskPTx),sign((IDPTx, spk(sskPTx)),sskCA_1))) $\sim X_1$ {39} event notRevoked(spk(sskPTx)) {40} new nonce_1 $(\sim M_31, \sim M_{32}, \sim M_{33}) = (VERSION, CHALLENGE, nonce_1)$ (VERSION, CHALLENGE, ~M_33) = (VERSION, CHALLENGE, nonce 1) {77} event sendResp(sskPTx) (~M 34,~M 35,~M 36,~M 37) ~X_2