$\sim$ M 27 = VERSION  $\sim$ M 28 = CHALLENGE AUTH ~M\_29 = extLSB(hash(cert(IDPTx,spk(sskPTx),sign(( IDPTx,spk(sskPTx)),sskCA\_1)))) ~M\_30 = 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))))), A trace has been found. sskPTx)  $\sim$ X\_1 = (VERSION,CHALLENGE\_AUTH,extLSB( $\sim$ M\_23), $\sim$ M\_30) (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 a 2  $\sim$ 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)))) {33} event notRevoked(spk(sskPTx)) {34} new nonce\_1  $(\sim M_24, \sim M_25, \sim M_26) = (VERSION, CHALLENGE, nonce 1)$ (VERSION, CHALLENGE, ~M\_26) = (VERSION, CHALLENGE, nonce 1) (67) event sendResp(sskPTx)  $(\sim M_27,\sim M_28,\sim M_29,\sim M_30)$ ~X 1

Abbreviations