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\_25), $\sim$ 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  $(\sim M_15,\sim M_16) = (VERSION,GET_DIGESTS)$ (VERSION,DIGESTS,a\_5)  $(\sim M_17, \sim M_18) = (VERSION, GET_CERTIFICATE)$ a\_6 a\_7 a\_8  $\sim$ M 19 = ACK a\_9  $\sim$ M 20 = ACK a\_10  $\sim$ M 21 = ACK a\_11  $\sim$ M 22 = ACK a\_12 a 13 (VERSION, GET\_DIGESTS)  $(\sim M_23,\sim M_24,\sim M_25) = (VERSION,DIGESTS,hash(cert($ IDPTx,spk(sskPTx),sign((IDPTx,spk(sskPTx)),sskCA\_1)))) (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)))  $\sim X_1$ {37} new nonce\_1  $(\sim M_31, \sim M_{32}, \sim M_{33}) = (VERSION, CHALLENGE, nonce_1)$ (VERSION,CHALLENGE,~M\_33) = (VERSION,CHALLENGE, nonce 1) {74} event sendResp(sskPTx) (~M 34,~M 35,~M 36,~M 37) ~X\_2 {43} event successAuth(spk(sskPTx))