Abbreviations  $\sim$ X\_1 = (VERSION,CERTIFICATE,cert(IDPTx, $\sim$ M\_1, $\sim$ M\_25)) (VERSION, CERTIFICATE, cert(IDPTx, spk(sskPTx), sign( (IDPTx,spk(sskPTx)),sskCA 1)))  $\sim$ M 29 = VERSION  $\sim$ M\_30 = CHALLENGE\_AUTH  $\sim$ M\_31 = extLSB(hash(cert(IDPTx,spk(sskPTx),sign(( IDPTx,spk(sskPTx)),sskCA 1))))  $\sim$ M\_32 = 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) ~X\_2 = (VERSION, CHALLENGE\_AUTH, extLSB(hash(cert(IDPTx,  $\sim$ M\_1, $\sim$ M\_25))), $\sim$ M\_32) = (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  $(\sim M_15, \sim M_16) = (VERSION, GET_CERTIFICATE)$ 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\_CERTIFICATE)  $(\sim M_21, \sim M_22, cert(\sim M_23, \sim M_24, \sim M_25)) = (VERSION,$ CERTIFICATE,cert(IDPTx,spk(sskPTx),sign((IDPTx, spk(sskPTx)),sskCA\_1))) ~X 1 {32} new nonce\_1  $(\sim M_26, \sim M_27, \sim M_28) = (VERSION, CHALLENGE, nonce_1)$ (VERSION,CHALLENGE,~M\_28) = (VERSION,CHALLENGE, nonce\_1) {65} event sendResp(sskPTx)  $(\sim M_29, \sim M_30, \sim M_31, \sim M_32)$ 

 $\sim X_2$