Abbreviations
~X_1 = (VERSION,CERTIFICATE,cert(IDPTx,~M_1,~M_30)) = (VERSION,CERTIFICATE,cert(IDPTx,spk(sskPTx),sign((IDPTx,spk(sskPTx)),sskCA_1)))
~M_34 = VERSION
~M_35 = CHALLENGE_AUTH
~M_36 = extLSB(hash(cert(IDPTx,spk(sskPTx),sign((IDPTx,spk(sskPTx)),sskCA_1))))
~M_37 = 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)
~X_2 = (VERSION,CHALLENGE_AUTH,extLSB(~M_23),~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))

A trace has been found.