Abbreviations
~X_1 = (VERSION,CERTIFICATE,cert(IDPTx,~M_1,~M_25)) = (VERSION,CERTIFICATE,cert(IDPTx,spk(sskPTx),sign((IDPTx,spk(sskPTx)),sskCA_1)))
~M_29 = VERSION
~M_30 = CHALLENGE_AUTH
~M_31 = extLSB(hash(cert(IDPTx,spk(sskPTx),sign((IDPTx,spk(sskPTx)),sskCA_1))))
~M_32 = 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(hash(cert(IDPTx,~M_1,~M_25))),~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))

A trace has been found.