Abbreviations
~M_22 = VERSION
~M_23 = CHALLENGE_AUTH
~M_24 = extLSB(hash(cert(IDPTx,spk(sskPTx),sign((IDPTx,spk(sskPTx)),sskCA_1))))
~M_25 = 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_1 = (VERSION,CHALLENGE_AUTH,~M_24,~M_25) = (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))
~M_28 = VERSION
~M_29 = CERTIFICATE
~M_30 = IDPTx
~M_31 = spk(sskPTx)
~M_32 = IDPTx
~M_33 = spk(sskPTx)
~M_34 = sign((IDPTx,spk(sskPTx)),sskCA_1)
~X_2 = (VERSION,CERTIFICATE,cert(IDPTx,~M_1,~M_34)) = (VERSION,CERTIFICATE,cert(IDPTx,spk(sskPTx),sign((IDPTx,spk(sskPTx)),sskCA_1)))

A trace has been found.