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))

A trace has been found.