A trace
has been found.

Abbreviations
~M_8 = certDevice(subjectServer_1,constructURL(subjectServer_1, path_1),pk(skThingAttacker_1),skRogueCA_1)
~M_9 = skThingAttacker_1
~M_12 = certDevice(subjectServer_1,constructURL(subjectServer_1, path_1),pk(skThingAttacker_1),skRogueCA_1)
~M_13 = nonceS_3
~M_21 = PRF(PRF(preMasterSecret_2,clientRandom_4, serverRandom_4),client_finished_label,hash((clientRandom_4, serverRandom_4,cert(subjectServer_1,pk(skServer_3), skCA_1),penc(preMasterSecret_2,pk(skServer_3)))))
~M_22 = PRF(PRF(preMasterSecret_2,clientRandom_4, serverRandom_4),server_finished_label,hash(((clientRandom_4, serverRandom_4,cert(subjectServer_1,pk(skServer_3), skCA_1),penc(preMasterSecret_2,pk(skServer_3))), PRF(PRF(preMasterSecret_2,clientRandom_4,serverRandom_4), client_finished_label,hash((clientRandom_4,serverRandom_4, cert(subjectServer_1,pk(skServer_3),skCA_1),penc(preMasterSecret_2,pk(skServer_3))))))))
~M_23 = constructURL(subjectServer_1,path_1)
~M_24 = HMAC(constructURL(subjectServer_1,path_1), PRF(PRF(preMasterSecret_2,clientRandom_4,serverRandom_4), serverRandom_4,clientRandom_4))
~X_1 = (getURL(~M_8),~M_24) = (constructURL(subjectServer_1, path_1),HMAC(constructURL(subjectServer_1,path_1), PRF(PRF(preMasterSecret_2,clientRandom_4,serverRandom_4), serverRandom_4,clientRandom_4)))
~M_25 = sign(makeMUDfile(constructURL(subjectServer_1, path_1),aclList_3),skServer_3)
~M_26 = cert(subjectServer_1,pk(skServer_3),skCA_1)
~M_27 = HMAC((sign(makeMUDfile(constructURL(subjectServer_1, path_1),aclList_3),skServer_3),cert(subjectServer_1, pk(skServer_3),skCA_1)),PRF(PRF(preMasterSecret_2, clientRandom_4,serverRandom_4),serverRandom_4, clientRandom_4))
~M_3 = cert(subjectServer_1,pk(skServer_3),skCA_1)