Abbreviations
~M_8 = certDevice(subjectServer_1,constructURL(subjectServer_1, path_1),pk(skThingAttacker_1),skRogueCA_1)
~M_9 = skThingAttacker_1
~X_1 = PRF(PRF(a_2,a,~M_10),client_finished_label,hash((a,~M_10,~M_3,penc(a_2,getPkServer(~M_3))))) = PRF(PRF(a_2,a,serverRandom_4),client_finished_label, hash((a,serverRandom_4,cert(subjectServer_1,pk(skServer_3),skCA_1),penc(a_2,pk(skServer_3)))))
~M_12 = PRF(PRF(a_2,a,serverRandom_4),server_finished_label, hash(((a,serverRandom_4,cert(subjectServer_1,pk(skServer_3),skCA_1),penc(a_2,pk(skServer_3))), PRF(PRF(a_2,a,serverRandom_4),client_finished_label, hash((a,serverRandom_4,cert(subjectServer_1,pk(skServer_3),skCA_1),penc(a_2,pk(skServer_3))))))))
~X_2 = (getURL(~M_8),HMAC(getURL(~M_8),PRF(PRF(a_2,a, ~M_10),~M_10,a))) = (constructURL(subjectServer_1, path_1),HMAC(constructURL(subjectServer_1,path_1), PRF(PRF(a_2,a,serverRandom_4),serverRandom_4,a)))
~M_13 = sign(makeMUDfile(constructURL(subjectServer_1, path_1),aclList_2),skServer_3)
~M_14 = cert(subjectServer_1,pk(skServer_3),skCA_1)
~M_15 = HMAC((sign(makeMUDfile(constructURL(subjectServer_1, path_1),aclList_2),skServer_3),cert(subjectServer_1, pk(skServer_3),skCA_1)),PRF(PRF(a_2,a,serverRandom_4), serverRandom_4,a))

A trace has been found.