Abbreviations
~X_1 = PRF(PRF(a_3,a_1,~M_8),client_finished_label,hash((a_1,~M_8,~M_3,penc(a_3,getPk(~M_3))))) = PRF(PRF(a_3,a_1,serverRandom_4),client_finished_label, hash((a_1,serverRandom_4,cert(subjectServer_1, pk(skServer_3),skCA_1),penc(a_3,pk(skServer_3)))))
~M_10 = PRF(PRF(a_3,a_1,serverRandom_4),server_finished_label, hash(((a_1,serverRandom_4,cert(subjectServer_1, pk(skServer_3),skCA_1),penc(a_3,pk(skServer_3))), PRF(PRF(a_3,a_1,serverRandom_4),client_finished_label, hash((a_1,serverRandom_4,cert(subjectServer_1, pk(skServer_3),skCA_1),penc(a_3,pk(skServer_3)))))))
~X_2 = (~M_7,HMAC(~M_7,PRF(PRF(a_3,a_1,~M_8),~M_8,a_1))) = (constructURL(subjectServer_1,path_1),HMAC(constructURL(subjectServer_1,path_1),PRF(PRF(a_3,a_1,serverRandom_4), serverRandom_4,a_1)))
~M_11 = sign(makeMUDfile(constructURL(subjectServer_1, path_1),aclList_2),skServer_3)
~M_12 = cert(subjectServer_1,pk(skServer_3),skCA_1)
~M_13 = HMAC((sign(makeMUDfile(constructURL(subjectServer_1, path_1),aclList_2),skServer_3),cert(subjectServer_1, pk(skServer_3),skCA_1)),PRF(PRF(a_3,a_1,serverRandom_4), serverRandom_4,a_1))

A trace has been found.