Abbreviations
~M_13 = PRF(PRF(preMasterSecret_2,clientRandom_4, serverRandom_4),client_finished_label,hash((clientRandom_4, serverRandom_4,cert(subjectServer2_1,pk(skServer2_1), skCA_1),penc(preMasterSecret_2,pk(skServer2_1)))))
~M_14 = PRF(PRF(preMasterSecret_2,clientRandom_4, serverRandom_4),server_finished_label,hash(((clientRandom_4, serverRandom_4,cert(subjectServer2_1,pk(skServer2_1), skCA_1),penc(preMasterSecret_2,pk(skServer2_1))), PRF(PRF(preMasterSecret_2,clientRandom_4,serverRandom_4), client_finished_label,hash((clientRandom_4,serverRandom_4, cert(subjectServer2_1,pk(skServer2_1),skCA_1), penc(preMasterSecret_2,pk(skServer2_1)))))))
~M_15 = constructURL(subjectServer2_1,path_1)
~M_16 = HMAC(constructURL(subjectServer2_1,path_1), PRF(PRF(preMasterSecret_2,clientRandom_4,serverRandom_4), serverRandom_4,clientRandom_4))
~X_1 = (getURL(~M_8),~M_16) = (constructURL(subjectServer2_1, path_1),HMAC(constructURL(subjectServer2_1,path_1), PRF(PRF(preMasterSecret_2,clientRandom_4,serverRandom_4), serverRandom_4,clientRandom_4)))
~M_17 = sign(makeMUDfile(constructURL(subjectServer2_1, path_1),aclList_3),skServer2_1)
~M_18 = cert(subjectServer2_1,pk(skServer2_1),skCA_1)
~M_19 = HMAC((sign(makeMUDfile(constructURL(subjectServer2_1, path_1),aclList_3),skServer2_1),cert(subjectServer2_1, pk(skServer2_1),skCA_1)),PRF(PRF(preMasterSecret_2, clientRandom_4,serverRandom_4),serverRandom_4, clientRandom_4))
~M_4 = cert(subjectServer2_1,pk(skServer2_1),skCA_1)

A trace has been found.