Abbreviations ~M_2 = choice[aenc((groupkey_request,sign(groupkey_request, vsk_27),cert(vid_99,pk(vsk_27),cask_24)),pk(cask_24)), aenc((groupkey_request,sign(groupkey_request,vsk_26), cert(vid_98,pk(vsk_26),cask_25)),pk(cask_25))] \sim X_1 = (\sim M_3, \sim M_4, \sim M_5) = choice[(attvid_25,attsk_25, cert(attvid_25,pk(attsk_25),cask_24)),(attvid_24, attsk_24,cert(attvid_24,pk(attsk_24),cask_25))] ~M_7 = choice[aenc((groupkey_request,sign(groupkey_request, vsk_29),cert(vid_101,pk(vsk_29),cask_24)),pk(cask_24)), aenc((groupkey_request,sign(groupkey_request,vsk_28), cert(vid_100,pk(vsk_28),cask_25)),pk(cask_25))] ~M_8 = choice[aenc(((groupkey_response,vid_99, gsk(vid_99,gmsk_24),gpk(gmsk_24)),sign((groupkey_response, vid_99,gsk(vid_99,gmsk_24),gpk(gmsk_24)),cask_24)), pk(vsk_27)),aenc(((groupkey_response,vid_98,gsk(vid_98,gmsk_25)),sign((groupkey_response,vid_98,gsk(vid_98,gmsk_25)),sign((gmsk_25)),cask_25)), pk(vsk_26))] **Honest Process** Attacker {1}new gmsk_24 {2}new cask_24 {3}new gmsk_25 {4}new cask_25 \sim M = pk(choice[cask_24,cask_25]) {10} new vid_100 {10} new vid_98 {11}new vsk_28 {11}new vsk_26 {12} new vid_99 {12} new vid_101 {13}new vsk_29 {13}new vsk_27 \sim M_1 = choice[cert(vid_99,pk(vsk_27),cask_24), cert(vid_98,pk(vsk_26),cask_25)] {314}new attvid_24 {315}new attsk 24 {19} event ValidGroupKeyRequestSent(choice[vid_99, vid_98]) {316}new attvid 25 {317}new attsk_25 {320}event choice[AttackerGetsEnrollmentCertificate(attvid_25,pk(attsk_25)),AttackerGetsEnrollmentCertificate(attvid_25,pk(attsk_24))] \sim M₂ ~X_1 \sim M_6 = choice[cert(vid_101,pk(vsk_29),cask_24), cert(vid_100,pk(vsk_28),cask_25)] {19} event ValidGroupKeyRequestSent(choice[vid_101, vid_100]) ~M 7 {364}get v_1907: table suchthat (if choice[true, false] then (success?(1-proj-revokedcerts(v_1907)) && (choice[vid_99,caught-fail] =nf 1-proj-revokedcerts(v_1907))) else (success?(1-proj-revokedcerts(v_1907)) && (choice[caught-fail,vid_98] =nf 1-proj-revokedcerts(v_1907)))): else branch taken {351}event choice[ValidGroupKeyRequestReceived(cask_24,vid_99),ValidGroupKeyRequestReceived(cask_25, vid_98)] {356}event choice[ValidGroupPrivateKeySent(vid_99, gsk(vid_99,gmsk_24),gpk(gmsk_24)),ValidGroupPrivateKeySent(vid_98,gsk(vid_98,gmsk_25),gpk(gmsk_25))] ~M 8 ~M 8 {28} new vpseudosk_81 {29}new vpseudosk_82 {30}new m_56 [48] if choice[true,false]
This process performs a test that may succeed on one side and not on the other.

A trace has been found.