Abbreviations ~M_2 = choice[aenc((groupkey_request,sign(groupkey_request, vsk_13),cert(vid_43,pk(vsk_13),cask_10)),pk(cask_10)), aenc((groupkey_request,sign(groupkey_request,vsk_12), cert(vid_42,pk(vsk_12),cask_11)),pk(cask_11))] \sim X_1 = (\sim M_3, \sim M_4, \sim M_5) = choice[(attvid_11,attsk_11, cert(attvid_11,pk(attsk_11),cask_10)),(attvid_10, attsk_10,cert(attvid_10,pk(attsk_10),cask_11))] ~M_7 = choice[aenc((groupkey_request, sign(groupkey_request, vsk_15),cert(vid_45,pk(vsk_15),cask_10)),pk(cask_10)), aenc((groupkey_request, sign(groupkey_request, vsk_14), cert(vid_44,pk(vsk_14),cask_11)),pk(cask_11))] ~M_8 = choice[aenc(((groupkey_response,vid_43, gsk(vid_43,gmsk_10),gpk(gmsk_10)),sign((groupkey_response, vid_43,gsk(vid_43,gmsk_10),gpk(gmsk_10)),cask_10)), pk(vsk_13)),aenc(((groupkey_response,vid_42,gsk(vid_42,gmsk_11)),sign((groupkey_response, vid_42,gsk(vid_42,gmsk_11)),gpk(gmsk_11)),cask_11)), pk(vsk_12))] **Honest Process** Attacker {1}new gmsk_10 {2}new cask_10 {3}new gmsk_11 {4}new cask_11 \sim M = pk(choice[cask 10,cask 11]) {10} new vid_42 {11}new vsk_12 {12} new vid_43 {13}new vsk_13 \sim M_1 = choice[cert(vid_43,pk(vsk_13),cask_10), cert(vid_42,pk(vsk_12),cask_11)] [19] event ValidGroupKeyRequestSent(choice[vid_43, vid_42]) ~M 2 ~X 1 \sim M_6 = choice[cert(vid_45,pk(vsk_15),cask_10), cert(vid_44,pk(vsk_14),cask_11)] $\sim M \mid 2$ {364}get v_689: table suchthat (if choice[true, false] then (success?(1-proj-revokedcerts(v_689)) && (choice[vid_43,caught-fail] =nf 1-proj-revokedcerts(v_689))) else (success?(1-proj-revokedcerts(v_689)) && (choice[caught-fail,vid_42] =nf 1-proj-revokedcerts(v_689)))): else branch taken {351}event choice[ValidGroupKeyRequestReceived(cask_10,vid_43),ValidGroupKeyRequestReceived(cask_11,vid_42)] {356}event choice[ValidGroupPrivateKeySent(vid_43, gsk(vid_43,gmsk_10),gpk(gmsk_10)),ValidGroupPrivateKeySent(vid_42,gsk(vid_42,gmsk_11),gpk(gmsk_11))] ~M 8 ~M 8 {28} new vpseudosk_32 {29}new vpseudosk_33 {30} new m_28 [48] if choice[true,false]
This process performs a test that may succeed on one side and not on the other.

{10} new vid_44

{11} new vsk_14

{12}new vid_45

{13}new vsk_15

{234}new attvid_10

{235}new attsk_10

{236}new attvid_11

{237}new attsk_11

+M 7

{240}event choice[AttackerGetsEnrollmentCertificate(attvid_11,pk(attsk_11)),AttackerGetsEnrollmentCertificate(attvid_10,pk(attsk_10))]

{19} event ValidGroupKeyRequestSent(choice[vid_45, vid_44])

A trace has been found.