A trace has been found.

Abbreviations
~X_1 = (~M_1,~M_2,~M_3) = choice[(attvid_4,attsk_4,cert(attvid_4,pk(attsk_4),cask_4)),(attvid_5,attsk_5,cert(attvid_5,pk(attsk_5),cask_5))]
~M_5 = choice[aenc((groupkey_request,nonce_21,sign(groupkey_request,vsk_9),cert(vid_21,pk(vsk_9),cask_4)),pk(cask_4)),aenc((groupkey_request,nonce_23,sign(groupkey_request,vsk_11),cert(vid_23,pk(vsk_11),cask_5)),pk(cask_5))]
~M_7 = choice[aenc((groupkey_request,nonce_20,sign(groupkey_request,vsk_8),cert(vid_20,pk(vsk_8),cask_4)),pk(cask_4)),aenc((groupkey_request,nonce_22,sign(groupkey_request,vsk_10),cert(vid_22,pk(vsk_10),cask_5)),pk(cask_5))]
~M_8 = choice[aenc(((groupkey_response,nonce_21,vid_21,gsk(vid_21,gmsk_4),gpk(gmsk_4)),sign((groupkey_response,nonce_21,vid_21,gsk(vid_21,gmsk_4),gpk(gmsk_4)),cask_4)),pk(vsk_9)),aenc(((groupkey_response,nonce_23,vid_23,gsk(vid_23,gmsk_5),gpk(gmsk_5)),sign((groupkey_response,nonce_23,vid_23,gsk(vid_23,gmsk_5),gpk(gmsk_5)),cask_5)),pk(vsk_11))]

Honest Process

{1}new gmsk_4
{2}new cask_4
{3}new vid_20
{4}new vsk_8
{5}new nonce_20
{6}new vid_21
{7}new vsk_9
{8}new nonce_21
{9}new attvid_4
{10}new attsk_4
{11}new gmsk_5
{12}new cask_5
{13}new vid_22
{14}new vsk_10
{15}new nonce_22
{16}new vid_23
{17}new vsk_11
{18}new nonce_23
{19}new attvid_5
{20}new attsk_5

Attacker

~M = pk(choice[cask_4,cask_5])

!

{489}event choice[AttackerGetsEnrollmentCertificate(attvid_4,pk(attsk_4)),AttackerGetsEnrollmentCertificate(attvid_5,pk(attsk_5))]

!

{494}event WaitingRequest

~X_1

~M_4 = choice[cert(vid_21,pk(vsk_9),cask_4),cert(vid_23,pk(vsk_11),cask_5)]

{261}event ValidGroupKeyRequestSent(choice[vid_21,vid_23])

~M_5

~M_6 = choice[cert(vid_20,pk(vsk_8),cask_4),cert(vid_22,pk(vsk_10),cask_5)]

{30}event ValidGroupKeyRequestSent(choice[vid_20,vid_22])

~M_7

~M_5

{507}event GroupKeyRequestReceived(choice[aenc((groupkey_request,nonce_21,sign(groupkey_request,vsk_9),cert(vid_21,pk(vsk_9),cask_4)),pk(cask_4)),aenc((groupkey_request,nonce_23,sign(groupkey_request,vsk_11),cert(vid_23,pk(vsk_11),cask_5)),pk(cask_5))])

{537}get v_234: table suchthat (if choice[true,false] then (success?(1-proj-revokedcerts(v_234)) && (choice[vid_21,caught-fail] =nf 1-proj-revokedcerts(v_234))) else (success?(1-proj-revokedcerts(v_234)) && (choice[caught-fail,vid_23] =nf 1-proj-revokedcerts(v_234)))): else branch taken

{522}event choice[ValidGroupKeyRequestReceived(cask_4,vid_21),ValidGroupKeyRequestReceived(cask_5,vid_23)]

{527}event choice[ValidGroupPrivateKeySent(vid_21,gsk(vid_21,gmsk_4),gpk(gmsk_4)),ValidGroupPrivateKeySent(vid_23,gsk(vid_23,gmsk_5),gpk(gmsk_5))]

~M_8

~M_8

{270}new vpseudosk_20
{271}new nonce_24
{272}new vpseudosk_21
{273}new m_32
{274}new nonce_25

{295}if choice[true,false]
This process performs a test that may succeed on one side and not on the other.