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_11,sign(groupkey_request,vsk_9),cert(vid_13,pk(vsk_9),cask_4)),pk(cask_4)),aenc((groupkey_request,nonce_13,sign(groupkey_request,vsk_11),cert(vid_15,pk(vsk_11),cask_5)),pk(cask_5))]
~M_7 = choice[aenc((groupkey_request,nonce_10,sign(groupkey_request,vsk_8),cert(vid_12,pk(vsk_8),cask_4)),pk(cask_4)),aenc((groupkey_request,nonce_12,sign(groupkey_request,vsk_10),cert(vid_14,pk(vsk_10),cask_5)),pk(cask_5))]
~M_8 = choice[aenc(((groupkey_response,nonce_11,vid_13,gsk(vid_13,gmsk_4),gpk(gmsk_4)),sign((groupkey_response,nonce_11,vid_13,gsk(vid_13,gmsk_4),gpk(gmsk_4)),cask_4)),pk(vsk_9)),aenc(((groupkey_response,nonce_13,vid_15,gsk(vid_15,gmsk_5),gpk(gmsk_5)),sign((groupkey_response,nonce_13,vid_15,gsk(vid_15,gmsk_5),gpk(gmsk_5)),cask_5)),pk(vsk_11))]

Honest Process

{1}new gmsk_4
{2}new cask_4
{3}new vid_12
{4}new vsk_8
{5}new nonce_10
{6}new vid_13
{7}new vsk_9
{8}new nonce_11
{9}new attvid_4
{10}new attsk_4
{11}new gmsk_5
{12}new cask_5
{13}new vid_14
{14}new vsk_10
{15}new nonce_12
{16}new vid_15
{17}new vsk_11
{18}new nonce_13
{19}new attvid_5
{20}new attsk_5

Attacker

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

!

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

{192}event WaitingRequest

~X_1

~M_4 = choice[cert(vid_13,pk(vsk_9),cask_4),cert(vid_15,pk(vsk_11),cask_5)]

{110}event ValidGroupKeyRequestSent(choice[vid_13,vid_15])

~M_5

~M_6 = choice[cert(vid_12,pk(vsk_8),cask_4),cert(vid_14,pk(vsk_10),cask_5)]

{30}event ValidGroupKeyRequestSent(choice[vid_12,vid_14])

~M_7

~M_5

{219}event GroupKeyRequestReceived(choice[aenc((groupkey_request,nonce_11,sign(groupkey_request,vsk_9),cert(vid_13,pk(vsk_9),cask_4)),pk(cask_4)),aenc((groupkey_request,nonce_13,sign(groupkey_request,vsk_11),cert(vid_15,pk(vsk_11),cask_5)),pk(cask_5))])

{220}event choice[ValidGroupKeyRequestReceived(cask_4,vid_13),ValidGroupKeyRequestReceived(cask_5,vid_15)]

{225}event choice[ValidGroupPrivateKeySent(vid_13,gsk(vid_13,gmsk_4),gpk(gmsk_4)),ValidGroupPrivateKeySent(vid_15,gsk(vid_15,gmsk_5),gpk(gmsk_5))]

~M_8

~M_8

{119}new vpseudosk_10
{120}new vpseudosk_11
{121}new m_12

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