A trace has been found.

Abbreviations
~M_2 = choice[aenc((groupkey_request,sign(groupkey_request, vsk_7),cert(vid_19,pk(vsk_7),cask_4)),pk(cask_4)), aenc((groupkey_request,sign(groupkey_request,vsk_6), cert(vid_18,pk(vsk_6),cask_5)),pk(cask_5))]
~X_1 = (~M_3,~M_4,~M_5) = choice[(attvid_5,attsk_5,cert(attvid_5,pk(attsk_5),cask_4)),(attvid_4,attsk_4, cert(attvid_4,pk(attsk_4),cask_5))]
~M_7 = choice[aenc((groupkey_request,sign(groupkey_request, vsk_9),cert(vid_21,pk(vsk_9),cask_4)),pk(cask_4)), aenc((groupkey_request,sign(groupkey_request,vsk_8), cert(vid_20,pk(vsk_8),cask_5)),pk(cask_5))]
~M_8 = choice[aenc(((groupkey_response,vid_19, gsk(vid_19,gmsk_4),gpk(gmsk_4)),sign((groupkey_response, vid_19,gsk(vid_19,gmsk_4),gpk(gmsk_4)),cask_4)), pk(vsk_7)),aenc(((groupkey_response,vid_18,gsk(vid_18,gmsk_5),gpk(gmsk_5)),sign((groupkey_response, vid_18,gsk(vid_18,gmsk_5),gpk(gmsk_5)),cask_5)), pk(vsk_6))]

Honest Process

Attacker

{1}new gmsk_4

{2}new cask_4

{3}new gmsk_5

{4}new cask_5

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

!

{10}new vid_20

{11}new vsk_8

{12}new vid_21

{13}new vsk_9

{10}new vid_18

{11}new vsk_6

{12}new vid_19

{13}new vsk_7

!

~M_1 = choice[cert(vid_19,pk(vsk_7),cask_4),cert(vid_18,pk(vsk_6),cask_5)]

!

{234}new attvid_4

{235}new attsk_4

{236}new attvid_5

{237}new attsk_5

{19}event ValidGroupKeyRequestSent(choice[vid_19, vid_18])

!

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

~M_2

!

~X_1

~M_6 = choice[cert(vid_21,pk(vsk_9),cask_4),cert(vid_20,pk(vsk_8),cask_5)]

{19}event ValidGroupKeyRequestSent(choice[vid_21, vid_20])

~M_7

~M_2

{284}get v_121: table suchthat (if choice[true, false] then (success?(1-proj-revokedcerts(v_121)) && (choice[vid_19,caught-fail] =nf 1-proj-revokedcerts(v_121))) else (success?(1-proj-revokedcerts(v_121)) && (choice[caught-fail,vid_18] =nf 1-proj-revokedcerts(v_121)))): else branch taken

{271}event choice[ValidGroupKeyRequestReceived(cask_4,vid_19),ValidGroupKeyRequestReceived(cask_5, vid_18)]

{276}event choice[ValidGroupPrivateKeySent(vid_19, gsk(vid_19,gmsk_4),gpk(gmsk_4)),ValidGroupPrivateKeySent(vid_18,gsk(vid_18,gmsk_5),gpk(gmsk_5))]

~M_8

~M_8

{28}new vpseudosk_11

{29}new vpseudosk_12

{30}new m_16

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