Abbreviations
~X_1 = (~M_1,~M_2,~M_3) = choice[(attvid_12,attsk_12, cert(attvid_12,pk(attsk_12),cask_12)),(attvid_13, attsk_13,cert(attvid_13,pk(attsk_13),cask_13))]
~M_5 = choice[aenc((groupkey_request,sign(groupkey_request, vsk_25),cert(vid_61,pk(vsk_25),cask_12)),pk(cask_12)), aenc((groupkey_request,sign(groupkey_request,vsk_26), cert(vid_62,pk(vsk_26),cask_13)),pk(cask_13))]
~M_7 = choice[aenc((groupkey_request,sign(groupkey_request, vsk_24),cert(vid_60,pk(vsk_24),cask_12)),pk(cask_12)), aenc((groupkey_request,sign(groupkey_request,vsk_27), cert(vid_63,pk(vsk_27),cask_13)),pk(cask_13))]
~M_8 = choice[aenc(((groupkey_response,vid_61, gsk(vid_61,gmsk_12),gpk(gmsk_12)),sign((groupkey_response, vid_61,gsk(vid_61,gmsk_12),gpk(gmsk_12)),cask_12)), pk(vsk_25)),aenc(((groupkey_response,vid_62,gsk(vid_62,gmsk_13),gpk(gmsk_13)),sign((groupkey_response, vid_62,gsk(vid_62,gmsk_13),gpk(gmsk_13)),cask_13)), pk(vsk_26))]

A trace has been found.

Honest Process

{1}new gmsk_12
{2}new cask_12
{3}new vid_60
{4}new vsk_24
{5}new vid_61
{6}new vsk_25
{7}new attvid_12
{8}new attsk_12
{9}new gmsk_13
{10}new cask_13
{11}new vid_62
{12}new vsk_26
{13}new vid_63
{14}new vsk_27
{15}new attvid_13
{16}new attsk_13

Attacker

~M = pk(choice[cask_12,cask_13])

{325}event choice[AttackerGetsEnrollmentCertificate(attvid_12,pk(attsk_12)),AttackerGetsEnrollmentCertificate(attvid_13,pk(attsk_13))]

!

!

~X_1

~M_4 = choice[cert(vid_61,pk(vsk_25),cask_12), cert(vid_62,pk(vsk_26),cask_13)]

{177}event ValidGroupKeyRequestSent(choice[vid_61, vid_62])

~M_5

~M_6 = choice[cert(vid_60,pk(vsk_24),cask_12), cert(vid_63,pk(vsk_27),cask_13)]

{26}event ValidGroupKeyRequestSent(choice[vid_60, vid_63])

~M_7

~M_7

~M_5

{369}get v_942: table suchthat (if choice[true, false] then (success?(1-proj-revokedcerts(v_942)) && (choice[vid_61,caught-fail] =nf 1-proj-revokedcerts(v_942))) else (success?(1-proj-revokedcerts(v_942)) && (choice[caught-fail,vid_62] =nf 1-proj-revokedcerts(v_942)))): else branch taken

{356}event choice[ValidGroupKeyRequestReceived(cask_12,vid_61),ValidGroupKeyRequestReceived(cask_13, vid_62)]

{361}event choice[ValidGroupPrivateKeySent(vid_61, gsk(vid_61,gmsk_12),gpk(gmsk_12)),ValidGroupPrivateKeySent(vid_62,gsk(vid_62,gmsk_13),gpk(gmsk_13))]

~M_8

~M_8

{186}new vpseudosk_78
{187}new vpseudosk_79
{188}new m_56

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