Abbreviations
~X_1 = (~M_1,~M_2,~M_3) = choice[(attvid_10,attsk_10, cert(attvid_10,pk(attsk_10),cask_10)),(attvid_11, attsk_11,cert(attvid_11,pk(attsk_11),cask_11))]
~M_5 = choice[aenc((groupkey_request,sign(groupkey_request, vsk_21),cert(vid_51,pk(vsk_21),cask_10)),pk(cask_10)), aenc((groupkey_request,sign(groupkey_request,vsk_23), cert(vid_53,pk(vsk_23),cask_11)),pk(cask_11))]
~M_7 = choice[aenc((groupkey_request,sign(groupkey_request, vsk_20),cert(vid_50,pk(vsk_20),cask_10)),pk(cask_10)), aenc((groupkey_request,sign(groupkey_request,vsk_22), cert(vid_52,pk(vsk_22),cask_11)),pk(cask_11))]
~M_8 = choice[aenc(((groupkey_response,vid_51, gsk(vid_51,gmsk_10),gpk(gmsk_10)),sign((groupkey_response, vid_51,gsk(vid_51,gmsk_10),gpk(gmsk_10)),cask_10)), pk(vsk_21)),aenc(((groupkey_response,vid_53,gsk(vid_53,gmsk_11),gpk(gmsk_11)),sign((groupkey_response, vid_53,gsk(vid_53,gmsk_11),gpk(gmsk_11)),cask_11)), pk(vsk_23))]

A trace has been found.

Honest Process

{1}new gmsk_10
{2}new cask_10
{3}new vid_50
{4}new vsk_20
{5}new vid_51
{6}new vsk_21
{7}new attvid_10
{8}new attsk_10
{9}new gmsk_11
{10}new cask_11
{11}new vid_52
{12}new vsk_22
{13}new vid_53
{14}new vsk_23
{15}new attvid_11
{16}new attsk_11

Attacker

~M = pk(choice[cask_10,cask_11])

!

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

!

~X_1

~M_4 = choice[cert(vid_51,pk(vsk_21),cask_10), cert(vid_53,pk(vsk_23),cask_11)]

{177}event ValidGroupKeyRequestSent(choice[vid_51, vid_53])

~M_5

~M_6 = choice[cert(vid_50,pk(vsk_20),cask_10), cert(vid_52,pk(vsk_22),cask_11)]

{26}event ValidGroupKeyRequestSent(choice[vid_50, vid_52])

~M_7

~M_5

{449}get v_789: table suchthat (if choice[true, false] then (success?(1-proj-revokedcerts(v_789)) && (choice[vid_51,caught-fail] =nf 1-proj-revokedcerts(v_789))) else (success?(1-proj-revokedcerts(v_789)) && (choice[caught-fail,vid_53] =nf 1-proj-revokedcerts(v_789)))): else branch taken

{436}event choice[ValidGroupKeyRequestReceived(cask_10,vid_51),ValidGroupKeyRequestReceived(cask_11, vid_53)]

{441}event choice[ValidGroupPrivateKeySent(vid_51, gsk(vid_51,gmsk_10),gpk(gmsk_10)),ValidGroupPrivateKeySent(vid_53,gsk(vid_53,gmsk_11),gpk(gmsk_11))]

~M_8

~M_8

{186}new vpseudosk_64
{187}new vpseudosk_65
{188}new m_48

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