Abbreviations
~X_1 = (~M_1,~M_2,~M_3) = choice[(attvid_18,attsk_18, cert(attvid_18,pk(attsk_18),cask_18)),(attvid_19, attsk_19,cert(attvid_19,pk(attsk_19),cask_19))]
~M_5 = choice[aenc((groupkey_request,sign(groupkey_request, vsk_37),cert(vid_91,pk(vsk_37),cask_18)),pk(cask_18)), aenc((groupkey_request,sign(groupkey_request,vsk_38), cert(vid_92,pk(vsk_38),cask_19)),pk(cask_19))]
~M_7 = choice[aenc((groupkey_request,sign(groupkey_request, vsk_36),cert(vid_90,pk(vsk_36),cask_18)),pk(cask_18)), aenc((groupkey_request,sign(groupkey_request,vsk_39), cert(vid_93,pk(vsk_39),cask_19)),pk(cask_19))]
~M_8 = choice[aenc(((groupkey_response,vid_91, gsk(vid_91,gmsk_18),gpk(gmsk_18)),sign((groupkey_response, vid_91,gsk(vid_91,gmsk_18),gpk(gmsk_18)),cask_18)), pk(vsk_37)),aenc(((groupkey_response,vid_92,gsk(vid_92,gmsk_19),gpk(gmsk_19)),sign((groupkey_response, vid_92,gsk(vid_92,gmsk_19),gpk(gmsk_19)),cask_19)), pk(vsk_38))]

A trace has been found.

Honest Process

{1}new gmsk_18
{2}new cask_18
{3}new vid_90
{4}new vsk_36
{5}new vid_91
{6}new vsk_37
{7}new attvid_18
{8}new attsk_18
{9}new gmsk_19
{10}new cask_19
{11}new vid_92
{12}new vsk_38
{13}new vid_93
{14}new vsk_39
{15}new attvid_19
{16}new attsk_19

Attacker

~M = pk(choice[cask_18,cask_19])

!

{325}event choice[AttackerGetsEnrollmentCertificate(attvid_18,pk(attsk_18)),AttackerGetsEnrollmentCertificate(attvid_19,pk(attsk_19))]

!

~X_1

~M_4 = choice[cert(vid_91,pk(vsk_37),cask_18), cert(vid_92,pk(vsk_38),cask_19)]

{177}event ValidGroupKeyRequestSent(choice[vid_91, vid_92])

~M_5

~M_6 = choice[cert(vid_90,pk(vsk_36),cask_18), cert(vid_93,pk(vsk_39),cask_19)]

{26}event ValidGroupKeyRequestSent(choice[vid_90, vid_93])

~M_7

~M_5

{449}get v_1585: table suchthat (if choice[true, false] then (success?(1-proj-revokedcerts(v_1585)) && (choice[vid_91,caught-fail] =nf 1-proj-revokedcerts(v_1585))) else (success?(1-proj-revokedcerts(v_1585)) && (choice[caught-fail,vid_92] =nf 1-proj-revokedcerts(v_1585)))): else branch taken

{436}event choice[ValidGroupKeyRequestReceived(cask_18,vid_91),ValidGroupKeyRequestReceived(cask_19, vid_92)]

{441}event choice[ValidGroupPrivateKeySent(vid_91, gsk(vid_91,gmsk_18),gpk(gmsk_18)),ValidGroupPrivateKeySent(vid_92,gsk(vid_92,gmsk_19),gpk(gmsk_19))]

~M_8

~M_8

{186}new vpseudosk_120
{187}new vpseudosk_121
{188}new m_80

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