Abbreviations
~X_1 = (~M_1,~M_2,~M_3) = choice[(attvid_6,attsk_6,cert(attvid_6,pk(attsk_6),cask_6)),(attvid_7,attsk_7,cert(attvid_7,pk(attsk_7),cask_7))]
~M_5 = choice[aenc((groupkey_request,sign(groupkey_request,vsk_13),cert(vid_31,pk(vsk_13),cask_6)),pk(cask_6)),aenc((groupkey_request,sign(groupkey_request,vsk_15),cert(vid_33,pk(vsk_15),cask_7)),pk(cask_7))]
~M_7 = choice[aenc((groupkey_request,sign(groupkey_request,vsk_12),cert(vid_30,pk(vsk_12),cask_6)),pk(cask_6)),aenc((groupkey_request,sign(groupkey_request,vsk_14),cert(vid_32,pk(vsk_14),cask_7)),pk(cask_7))]

A trace has been found.

Honest Process

Attacker

{1}new gmsk_6
{2}new cask_6
{3}new vid_30
{4}new vsk_12
{5}new vid_31
{6}new vsk_13
{7}new attvid_6
{8}new attsk_6
{9}new gmsk_7
{10}new cask_7
{11}new vid_32
{12}new vsk_14
{13}new vid_33
{14}new vsk_15
{15}new attvid_7
{16}new attsk_7

~M = pk(choice[cask_6,cask_7])

!

{325}event choice[AttackerGetsEnrollmentCertificate(attvid_6,pk(attsk_6)),AttackerGetsEnrollmentCertificate(attvid_7,pk(attsk_7))]

!

~X_1

~M_4 = choice[cert(vid_31,pk(vsk_13),cask_6),cert(vid_33,pk(vsk_15),cask_7)]

{177}event ValidGroupKeyRequestSent(choice[vid_31,vid_33])

~M_5

~M_6 = choice[cert(vid_30,pk(vsk_12),cask_6),cert(vid_32,pk(vsk_14),cask_7)]

{26}event ValidGroupKeyRequestSent(choice[vid_30,vid_32])

~M_7

~M_5

{400}get v_344: table suchthat (if choice[true,false] then (success?(1-proj-revokedcerts(v_344)) && (choice[vid_31,caught-fail] =nf 1-proj-revokedcerts(v_344))) else (success?(1-proj-revokedcerts(v_344)) && (choice[caught-fail,vid_33] =nf 1-proj-revokedcerts(v_344)))): else branch taken

{358}if (if choice[true,false] then not(choice[true,false]) else not((choice[false,true] && choice[caught-fail,false])))
This process performs a test that may succeed on one side and not on the other.