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_19,pk(vsk_13),cask_6)),pk(cask_6)),aenc((groupkey_request,sign(groupkey_request,vsk_14),cert(vid_20,pk(vsk_14),cask_7)),pk(cask_7))]
~M_7 = choice[aenc((groupkey_request,sign(groupkey_request,vsk_12),cert(vid_18,pk(vsk_12),cask_6)),pk(cask_6)),aenc((groupkey_request,sign(groupkey_request,vsk_15),cert(vid_21,pk(vsk_15),cask_7)),pk(cask_7))]
~M_8 = choice[aenc(((groupkey_response,vid_19,gsk(vid_19,gmsk_6),gpk(gmsk_6)),sign((groupkey_response,vid_19,gsk(vid_19,gmsk_6),gpk(gmsk_6)),cask_6)),pk(vsk_13)),aenc(((groupkey_response,vid_20,gsk(vid_20,gmsk_7),gpk(gmsk_7)),sign((groupkey_response,vid_20,gsk(vid_20,gmsk_7),gpk(gmsk_7)),cask_7)),pk(vsk_14))]

A trace has been found.

Honest Process

Attacker

{1}new gmsk_6

{2}new cask_6

{3}new vid_18

{4}new vsk_12

{5}new vid_19

{6}new vsk_13

{7}new attvid_6

{8}new attsk_6

{9}new gmsk_7

{10}new cask_7

{11}new vid_20

{12}new vsk_14

{13}new vid_21

{14}new vsk_15

{15}new attvid_7

{16}new attsk_7

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

!

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

~X_1

~M_4 = choice[cert(vid_19,pk(vsk_13),cask_6),cert(vid_20,pk(vsk_14),cask_7)]

{101}event ValidGroupKeyRequestSent(choice[vid_19,vid_20])

~M_5

~M_6 = choice[cert(vid_18,pk(vsk_12),cask_6),cert(vid_21,pk(vsk_15),cask_7)]

{26}event ValidGroupKeyRequestSent(choice[vid_18,vid_21])

~M_7

~M_7

~M_5

{217}get v_171: table suchthat (if choice[true,false] then (success?(1-proj-revokedcerts(v_171)) && (choice[vid_19,caught-fail] =nf 1-proj-revokedcerts(v_171))) else (success?(1-proj-revokedcerts(v_171)) && (choice[caught-fail,vid_20] =nf 1-proj-revokedcerts(v_171)))): else branch taken

{204}event choice[ValidGroupKeyRequestReceived(cask_6,vid_19),ValidGroupKeyRequestReceived(cask_7,vid_20)]

{209}event choice[ValidGroupPrivateKeySent(vid_19,gsk(vid_19,gmsk_6),gpk(gmsk_6)),ValidGroupPrivateKeySent(vid_20,gsk(vid_20,gmsk_7),gpk(gmsk_7))]

~M_8

~M_8

{110}new vpseudosk_16

{111}new vpseudosk_17

{112}new m_16

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