Abbreviations
~X_1 = (~M_1,~M_2,~M_3) = choice[(attvid_8,attsk_8,cert(attvid_8,pk(attsk_8),cask_8)),(attvid_9,attsk_9,cert(attvid_9,pk(attsk_9),cask_9))]
~M_5 = choice[aenc((groupkey_request,nonce_37,sign(groupkey_request,vsk_17),cert(vid_41,pk(vsk_17),cask_8)),pk(cask_8)),aenc((groupkey_request,nonce_38,sign(groupkey_request,vsk_18),cert(vid_42,pk(vsk_18),cask_9)),pk(cask_9))]
~M_7 = choice[aenc((groupkey_request,nonce_36,sign(groupkey_request,vsk_16),cert(vid_40,pk(vsk_16),cask_8)),pk(cask_8)),aenc((groupkey_request,nonce_39,sign(groupkey_request,vsk_19),cert(vid_43,pk(vsk_19),cask_9)),pk(cask_9))]
~M_8 = choice[aenc(((groupkey_response,nonce_37,vid_41,gsk(vid_41,gmsk_8),gpk(gmsk_8)),sign((groupkey_response,nonce_37,vid_41,gsk(vid_41,gmsk_8),gpk(gmsk_8)),cask_8)),pk(vsk_17)),aenc(((groupkey_response,nonce_38,vid_42,gsk(vid_42,gmsk_9),gpk(gmsk_9)),sign((groupkey_response,nonce_38,vid_42,gsk(vid_42,gmsk_9),gpk(gmsk_9)),cask_9)),pk(vsk_18))]

A trace has been found.

Honest Process

{1}new gmsk_8
{2}new cask_8
{3}new vid_40
{4}new vsk_16
{5}new nonce_36
{6}new vid_41
{7}new vsk_17
{8}new nonce_37
{9}new attvid_8
{10}new attsk_8
{11}new gmsk_9
{12}new cask_9
{13}new vid_42
{14}new vsk_18
{15}new nonce_38
{16}new vid_43
{17}new vsk_19
{18}new nonce_39
{19}new attvid_9
{20}new attsk_9

Attacker

~M = pk(choice[cask_8,cask_9])

!

{489}event choice[AttackerGetsEnrollmentCertificate(attvid_8,pk(attsk_8)),AttackerGetsEnrollmentCertificate(attvid_9,pk(attsk_9))]

!

{494}event WaitingRequest

~X_1

~M_4 = choice[cert(vid_41,pk(vsk_17),cask_8),cert(vid_42,pk(vsk_18),cask_9)]

{261}event ValidGroupKeyRequestSent(choice[vid_41,vid_42])

~M_5

~M_6 = choice[cert(vid_40,pk(vsk_16),cask_8),cert(vid_43,pk(vsk_19),cask_9)]

{30}event ValidGroupKeyRequestSent(choice[vid_40,vid_43])

~M_7

~M_5

{507}event GroupKeyRequestReceived(choice[aenc((groupkey_request,nonce_37,sign(groupkey_request,vsk_17),cert(vid_41,pk(vsk_17),cask_8)),pk(cask_8)),aenc((groupkey_request,nonce_38,sign(groupkey_request,vsk_18),cert(vid_42,pk(vsk_18),cask_9)),pk(cask_9))])

{537}get v_816: table suchthat (if choice[true,false] then (success?(1-proj-revokedcerts(v_816)) && (choice[vid_41,caught-fail] =nf 1-proj-revokedcerts(v_816))) else (success?(1-proj-revokedcerts(v_816)) && (choice[caught-fail,vid_42] =nf 1-proj-revokedcerts(v_816)))): else branch taken

{522}event choice[ValidGroupKeyRequestReceived(cask_8,vid_41),ValidGroupKeyRequestReceived(cask_9,vid_42)]

{527}event choice[ValidGroupPrivateKeySent(vid_41,gsk(vid_41,gmsk_8),gpk(gmsk_8)),ValidGroupPrivateKeySent(vid_42,gsk(vid_42,gmsk_9),gpk(gmsk_9))]

~M_8

~M_8

{270}new vpseudosk_44
{271}new nonce_40
{272}new vpseudosk_45
{273}new m_48
{274}new nonce_41

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