| 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,nonce_29,sign(groupkey_request,vsk_13),cert(vid_31,pk(vsk_13),cask_6)),pk(cask_6)),aenc((groupkey_request,nonce_31,sign(groupkey_request,vsk_15),cert(vid_33,pk(vsk_15),cask_7)),pk(cask_7))] |
| ~M_7 = choice[aenc((groupkey_request,nonce_28,sign(groupkey_request,vsk_12),cert(vid_30,pk(vsk_12),cask_6)),pk(cask_6)),aenc((groupkey_request,nonce_30,sign(groupkey_request,vsk_14),cert(vid_32,pk(vsk_14),cask_7)),pk(cask_7))] |
| ~M_8 = choice[aenc(((groupkey_response,nonce_29,vid_31,gsk(vid_31,gmsk_6),gpk(gmsk_6)),sign((groupkey_response,nonce_29,vid_31,gsk(vid_31,gmsk_6),gpk(gmsk_6)),cask_6)),pk(vsk_13)),aenc(((groupkey_response,nonce_31,vid_33,gsk(vid_33,gmsk_7),gpk(gmsk_7)),sign((groupkey_response,nonce_31,vid_33,gsk(vid_33,gmsk_7),gpk(gmsk_7)),cask_7)),pk(vsk_15))] |

A trace has been found.

Honest Process

{1}new gmsk_6
{2}new cask_6
{3}new vid_30
{4}new vsk_12
{5}new nonce_28
{6}new vid_31
{7}new vsk_13
{8}new nonce_29
{9}new attvid_6
{10}new attsk_6
{11}new gmsk_7
{12}new cask_7
{13}new vid_32
{14}new vsk_14
{15}new nonce_30
{16}new vid_33
{17}new vsk_15
{18}new nonce_31
{19}new attvid_7
{20}new attsk_7

Attacker

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

!

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

!

{576}event WaitingRequest

~X_1

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

{261}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)]

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

~M_7

~M_5

{589}event GroupKeyRequestReceived(choice[aenc((groupkey_request,nonce_29,sign(groupkey_request,vsk_13),cert(vid_31,pk(vsk_13),cask_6)),pk(cask_6)),aenc((groupkey_request,nonce_31,sign(groupkey_request,vsk_15),cert(vid_33,pk(vsk_15),cask_7)),pk(cask_7))])

{619}get v_573: table suchthat (if choice[true,false] then (success?(1-proj-revokedcerts(v_573)) && (choice[vid_31,caught-fail] =nf 1-proj-revokedcerts(v_573))) else (success?(1-proj-revokedcerts(v_573)) && (choice[caught-fail,vid_33] =nf 1-proj-revokedcerts(v_573)))): else branch taken

{604}event choice[ValidGroupKeyRequestReceived(cask_6,vid_31),ValidGroupKeyRequestReceived(cask_7,vid_33)]

{609}event choice[ValidGroupPrivateKeySent(vid_31,gsk(vid_31,gmsk_6),gpk(gmsk_6)),ValidGroupPrivateKeySent(vid_33,gsk(vid_33,gmsk_7),gpk(gmsk_7))]

~M_8

~M_8

{270}new vpseudosk_32
{271}new nonce_32
{272}new vpseudosk_33
{273}new m_40
{274}new nonce_33

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