A trace has been found.

| Abbreviations |
| --- |
| ~X_1 = (~M_1,~M_2,~M_3) = choice[(attvid_4,attsk_4,cert(attvid_4,pk(attsk_4),cask_4)),(attvid_5,attsk_5,cert(attvid_5,pk(attsk_5),cask_5))] |
| ~M_5 = choice[aenc((groupkey_request,nonce,sign(groupkey_request,vsk_9),cert(vid_13,pk(vsk_9),cask_4)),pk(cask_4)),aenc((groupkey_request,nonce,sign(groupkey_request,vsk_11),cert(vid_15,pk(vsk_11),cask_5)),pk(cask_5))] |
| ~M_7 = choice[aenc((groupkey_request,nonce,sign(groupkey_request,vsk_8),cert(vid_12,pk(vsk_8),cask_4)),pk(cask_4)),aenc((groupkey_request,nonce,sign(groupkey_request,vsk_10),cert(vid_14,pk(vsk_10),cask_5)),pk(cask_5))] |
| ~M_8 = choice[aenc(((groupkey_response,vid_13,gsk(vid_13,gmsk_4),gpk(gmsk_4)),sign((groupkey_response,vid_13,gsk(vid_13,gmsk_4),gpk(gmsk_4)),cask_4)),pk(vsk_9)),aenc(((groupkey_response,vid_15,gsk(vid_15,gmsk_5),gpk(gmsk_5)),sign((groupkey_response,vid_15,gsk(vid_15,gmsk_5),gpk(gmsk_5)),cask_5)),pk(vsk_11))] |

Honest Process

{1}new gmsk_4
{2}new cask_4
{3}new vid_12
{4}new vsk_8
{5}new vid_13
{6}new vsk_9
{7}new attvid_4
{8}new attsk_4
{9}new gmsk_5
{10}new cask_5
{11}new vid_14
{12}new vsk_10
{13}new vid_15
{14}new vsk_11
{15}new attvid_5
{16}new attsk_5

Attacker

~M = pk(choice[cask_4,cask_5])

{177}event choice[AttackerGetsEnrollmentCertificate(attvid_4,pk(attsk_4)),AttackerGetsEnrollmentCertificate(attvid_5,pk(attsk_5))]

!

{182}event WaitingRequest

~X_1

~M_4 = choice[cert(vid_13,pk(vsk_9),cask_4),cert(vid_15,pk(vsk_11),cask_5)]

{103}event ValidGroupKeyRequestSent(choice[vid_13,vid_15])

~M_5

~M_6 = choice[cert(vid_12,pk(vsk_8),cask_4),cert(vid_14,pk(vsk_10),cask_5)]

{26}event ValidGroupKeyRequestSent(choice[vid_12,vid_14])

~M_7

~M_5

{209}event GroupKeyRequestReceived(choice[aenc((groupkey_request,nonce,sign(groupkey_request,vsk_9),cert(vid_13,pk(vsk_9),cask_4)),pk(cask_4)),aenc((groupkey_request,nonce,sign(groupkey_request,vsk_11),cert(vid_15,pk(vsk_11),cask_5)),pk(cask_5))])

{210}event choice[ValidGroupKeyRequestReceived(cask_4,vid_13),ValidGroupKeyRequestReceived(cask_5,vid_15)]

{215}event choice[ValidGroupPrivateKeySent(vid_13,gsk(vid_13,gmsk_4),gpk(gmsk_4)),ValidGroupPrivateKeySent(vid_15,gsk(vid_15,gmsk_5),gpk(gmsk_5))]

~M_8

~M_8

{114}new vpseudosk_10
{115}new vpseudosk_11
{116}new m_12

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