| 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_15,sign(groupkey_request,vsk_13),cert(vid_19,pk(vsk_13),cask_6)),pk(cask_6)),aenc((groupkey_request,nonce_16,sign(groupkey_request,vsk_14),cert(vid_20,pk(vsk_14),cask_7)),pk(cask_7))] |
| ~M_7 = choice[aenc((groupkey_request,nonce_14,sign(groupkey_request,vsk_12),cert(vid_18,pk(vsk_12),cask_6)),pk(cask_6)),aenc((groupkey_request,nonce_17,sign(groupkey_request,vsk_15),cert(vid_21,pk(vsk_15),cask_7)),pk(cask_7))] |
| ~M_8 = choice[aenc(((groupkey_response,nonce_15,vid_19,gsk(vid_19,gmsk_6),gpk(gmsk_6)),sign((groupkey_response,nonce_15,vid_19,gsk(vid_19,gmsk_6),gpk(gmsk_6)),cask_6)),pk(vsk_13)),aenc(((groupkey_response,nonce_16,vid_20,gsk(vid_20,gmsk_7),gpk(gmsk_7)),sign((groupkey_response,nonce_16,vid_20,gsk(vid_20,gmsk_7),gpk(gmsk_7)),cask_7)),pk(vsk_14))] |

A trace has been found.

Honest Process

{1}new gmsk_6
{2}new cask_6
{3}new vid_18
{4}new vsk_12
{5}new nonce_14
{6}new vid_19
{7}new vsk_13
{8}new nonce_15
{9}new attvid_6
{10}new attsk_6
{11}new gmsk_7
{12}new cask_7
{13}new vid_20
{14}new vsk_14
{15}new nonce_16
{16}new vid_21
{17}new vsk_15
{18}new nonce_17
{19}new attvid_7
{20}new attsk_7

Attacker

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

!

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

{192}event WaitingRequest

~X_1

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

{110}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)]

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

~M_7

~M_5

{219}event GroupKeyRequestReceived(choice[aenc((groupkey_request,nonce_15,sign(groupkey_request,vsk_13),cert(vid_19,pk(vsk_13),cask_6)),pk(cask_6)),aenc((groupkey_request,nonce_16,sign(groupkey_request,vsk_14),cert(vid_20,pk(vsk_14),cask_7)),pk(cask_7))])

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

{225}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

{119}new vpseudosk_16
{120}new vpseudosk_17
{121}new m_16

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