Abbreviations
~M_9 = aenc(((groupkey_response,vid_9,gsk(vid_9, gmsk_4),gpk(gmsk_4)),sign((groupkey_response,vid_9, gsk(vid_9,gmsk_4),gpk(gmsk_4)),cask_3)),pk(vsk_6))
~X_1 = aenc((groupkey_request,sign(groupkey_request,~M_2), ~M_3),~M) = aenc((groupkey_request,sign(groupkey_request, attsk_3),cert(attvid_3,pk(attsk_3),cask_3)),pk(cask_3))
~M_16 = aenc(((groupkey_response,attvid_3,gsk(attvid_3,gmsk_4),gpk(gmsk_4)),sign((groupkey_response, attvid_3,gsk(attvid_3,gmsk_4),gpk(gmsk_4)),cask_3)), pk(attsk_3))
~M_17 = aenc(((groupkey_response,vid_8,gsk(vid_8, gmsk_4),gpk(gmsk_4)),sign((groupkey_response,vid_8, gsk(vid_8,gmsk_4),gpk(gmsk_4)),cask_3)),pk(vsk_5))
~X_2 = (~M_13,~M_14,pseudocert(getpseudopk(~M_12),3-proj-4-tuple(1-proj-2-tuple(adec(~M_16,~M_2))))) = (m_9,sign(m_9,vpseudosk_3),pseudocert(pk(vpseudosk_3),gsk(attvid_3,gmsk_4)))
~M_18 = aenc(((pseudocert(pk(vpseudosk_3),gsk(attvid_3,gmsk_4)),revoke_request),sign((pseudocert(pk(vpseudosk_3),gsk(attvid_3,gmsk_4)),revoke_request), vsk_5),cert(vid_8,pk(vsk_5),cask_3)),pk(cask_3))
~X_3 = aenc(((pseudocert(a_13,3-proj-4-tuple(1-proj-2-tuple(adec(~M_16,~M_2)))),revoke_request),sign((pseudocert(a_13,3-proj-4-tuple(1-proj-2-tuple(adec(~M_16, ~M_2)))),revoke_request),~M_5),~M_6),~M) = aenc(((pseudocert(a_13,gsk(attvid_3,gmsk_4)),revoke_request), sign((pseudocert(a_13,gsk(attvid_3,gmsk_4)),revoke_request), attsk_4),cert(attvid_4,pk(attsk_4),cask_3)),pk(cask_3))

A trace has been found.

Honest Process

{1}new gmsk_4
{2}new cask_3

Attacker

~M = pk(cask_3)

!

{92}new attvid_4
{93}new attsk_4
{96}event AttackerGetsEnrollmentCertificate(attvid_4, pk(attsk_4))

{92}new attvid_3
{93}new attsk_3
{96}event AttackerGetsEnrollmentCertificate(attvid_3, pk(attsk_3))

Beginning of process CA

Beginning of process CA

Beginning of process CA

Beginning of process CA

Beginning of process CARevoke

Beginning of process CARevoke

(~M_1,~M_2,~M_3) = (attvid_3,attsk_3,cert(attvid_3, pk(attsk_3),cask_3))

{6}new vid_9
{7}new vsk_6

{6}new vid_8
{7}new vsk_5

(~M_4,~M_5,~M_6) = (attvid_4,attsk_4,cert(attvid_4, pk(attsk_4),cask_3))

Beginning of process Vehicle
{15}event ValidGroupKeyRequestSent(vid_8)

Beginning of process Vehicle
{15}event ValidGroupKeyRequestSent(vid_9)

~M_7 = aenc((groupkey_request,sign(groupkey_request, vsk_5),cert(vid_8,pk(vsk_5),cask_3)),pk(cask_3))

~M_8 = aenc((groupkey_request,sign(groupkey_request, vsk_6),cert(vid_9,pk(vsk_6),cask_3)),pk(cask_3))

aenc((groupkey_request,a_4,~M_3),~M) = aenc((groupkey_request, a_4,cert(attvid_3,pk(attsk_3),cask_3)),pk(cask_3))

~M_8 = aenc((groupkey_request,sign(groupkey_request, vsk_6),cert(vid_9,pk(vsk_6),cask_3)),pk(cask_3))

{116}get revokedcerts(=vid_9): else branch taken
{109}event ValidGroupKeyRequestReceived(cask_3, vid_9)
{114}event ValidGroupPrivateKeySent(vid_9,gsk(vid_9,gmsk_4),gpk(gmsk_4))

~M_9

~M_9

{22}event ValidGroupPrivateKeyReceived(vid_9,gsk(vid_9,gmsk_4),gpk(gmsk_4))

! ! !

Beginning of process VehicleSend(vid_9, gsk(vid_9, gmsk_4))
{24}new vpseudosk_3
{27}event PseudoCertCreated(vid_9,vpseudosk_3)

!

{29}new m_9
{31}event ValidMessageSent(vid_9,pseudocert(pk(vpseudosk_3),gsk(vid_9,gmsk_4)),m_9)

{29}new m_8
{31}event ValidMessageSent(vid_9,pseudocert(pk(vpseudosk_3),gsk(vid_9,gmsk_4)),m_8)

(~M_10,~M_11,~M_12) = (m_8,sign(m_8,vpseudosk_3), pseudocert(pk(vpseudosk_3),gsk(vid_9,gmsk_4)))

(~M_13,~M_14,~M_15) = (m_9,sign(m_9,vpseudosk_3), pseudocert(pk(vpseudosk_3),gsk(vid_9,gmsk_4)))

~X_1

{116}get revokedcerts(=attvid_3): else branch taken
{109}event ValidGroupKeyRequestReceived(cask_3, attvid_3)
{114}event ValidGroupPrivateKeySent(attvid_3,gsk(attvid_3,gmsk_4),gpk(gmsk_4))

~M_16

~M_7 = aenc((groupkey_request,sign(groupkey_request, vsk_5),cert(vid_8,pk(vsk_5),cask_3)),pk(cask_3))

{116}get revokedcerts(=vid_8): else branch taken
{109}event ValidGroupKeyRequestReceived(cask_3, vid_8)
{114}event ValidGroupPrivateKeySent(vid_8,gsk(vid_8,gmsk_4),gpk(gmsk_4))

~M_17

~M_17

{22}event ValidGroupPrivateKeyReceived(vid_8,gsk(vid_8,gmsk_4),gpk(gmsk_4))

! ! !

Beginning of process VehicleReport(vid_8, vsk_5, cert(vid_8,pk(vsk_5),cask_3), pk(cask_3), gpk(gmsk_4))

~X_2

{48}event RevocationAsked(vid_8,cert(vid_8,pk(vsk_5),cask_3),pseudocert(pk(vpseudosk_3),gsk(attvid_3,gmsk_4)))

~M_18

~X_3

{154}get revokedcerts(=attvid_4): else branch taken
{127}event ValidRevocationReportReceived(pseudocert(a_13,gsk(attvid_3,gmsk_4)),cert(attvid_4,pk(attsk_4), cask_3))
{153}get revokedcerts(=attvid_3): else branch taken
{130}event RevokedVid(attvid_3)

~M_18

{154}get revokedcerts(=vid_8): else branch taken
{127}event ValidRevocationReportReceived(pseudocert(pk(vpseudosk_3),gsk(attvid_3,gmsk_4)),cert(vid_8, pk(vsk_5),cask_3))
{153}get revokedcerts(=attvid_3): else branch taken

{130}event RevokedVid(attvid_3)

{131}insert revokedcerts(attvid_3)

{116}get revokedcerts(attvid_3)

{107}event RevokedCannotGetGroupKey(attvid_3)