Abbreviations
~M_10 = aenc(((groupkey_response,vid_9,gsk(vid_9, gmsk_5),gpk(gmsk_5)),sign((groupkey_response,vid_9, gsk(vid_9,gmsk_5),gpk(gmsk_5)),cask_3)),pk(vsk_6))
~M_11 = aenc(((pseudocert(pk(a_6),gsk(attvid_3, gmsk_5)),revoke_request),sign((pseudocert(pk(a_6), gsk(attvid_3,gmsk_5)),revoke_request),vsk_6),cert(vid_9,pk(vsk_6),cask_3)),pk(cask_3))
~X_1 = aenc((groupkey_request,sign(groupkey_request,~M_6), ~M_7),~M) = aenc((groupkey_request,sign(groupkey_request, attsk_4),cert(attvid_4,pk(attsk_4),cask_3)),pk(cask_3))
~M_12 = aenc(((groupkey_response,attvid_4,gsk(attvid_4,gmsk_5),gpk(gmsk_5)),sign((groupkey_response, attvid_4,gsk(attvid_4,gmsk_5),gpk(gmsk_5)),cask_3)), pk(attsk_4))
~M_13 = aenc(((groupkey_response,vid_8,gsk(vid_8, gmsk_5),gpk(gmsk_5)),sign((groupkey_response,vid_8, gsk(vid_8,gmsk_5),gpk(gmsk_5)),cask_3)),pk(vsk_5))
~X_2 = ((groupkey_response,~M_5,gsk(~M_5,~M_1),gpk(~M_1)), 2-proj-2-tuple(adec(~M_12,~M_6)),pseudocert(~M, gsk(~M_2,~M_1))) = ((groupkey_response,attvid_4, gsk(attvid_4,gmsk_5),gpk(gmsk_5)),sign((groupkey_response, attvid_4,gsk(attvid_4,gmsk_5),gpk(gmsk_5)),cask_3), pseudocert(pk(cask_3),gsk(attvid_3,gmsk_5)))
~M_14 = aenc(((pseudocert(pk(cask_3),gsk(attvid_3, gmsk_5)),revoke_request),sign((pseudocert(pk(cask_3), gsk(attvid_3,gmsk_5)),revoke_request),vsk_5),cert(vid_8,pk(vsk_5),cask_3)),pk(cask_3))

A trace has been found.

Honest Process

Attacker

{1}new gmsk_5
{2}new cask_3

~M = pk(cask_3)

!

Beginning of process CAGroupMasterSecretKeyReveal
{156}event CAGMSKReveal(gmsk_5)

~M_1 = gmsk_5

{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_2,~M_3,~M_4) = (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_5,~M_6,~M_7) = (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_8 = aenc((groupkey_request,sign(groupkey_request, vsk_5),cert(vid_8,pk(vsk_5),cask_3)),pk(cask_3))

~M_9 = aenc((groupkey_request,sign(groupkey_request, vsk_6),cert(vid_9,pk(vsk_6),cask_3)),pk(cask_3))

~M_9 = aenc((groupkey_request,sign(groupkey_request, vsk_6),cert(vid_9,pk(vsk_6),cask_3)),pk(cask_3))

~M_9 = 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_5),gpk(gmsk_5))

~M_10

~M_10

{22}event ValidGroupPrivateKeyReceived(vid_9,gsk(vid_9,gmsk_5),gpk(gmsk_5))

! ! !

Beginning of process VehicleReport(vid_9, vsk_6, cert(vid_9,pk(vsk_6),cask_3), pk(cask_3), gpk(gmsk_5))

(a_5,sign(a_5,a_6),pseudocert(pk(a_6),gsk(~M_2, ~M_1))) = (a_5,sign(a_5,a_6),pseudocert(pk(a_6), gsk(attvid_3,gmsk_5)))

{48}event RevocationAsked(vid_9,cert(vid_9,pk(vsk_6),cask_3),pseudocert(pk(a_6),gsk(attvid_3, gmsk_5)))

~M_11

aenc((groupkey_request,a_8,~M_4),~M) = aenc((groupkey_request, a_8,cert(attvid_3,pk(attsk_3),cask_3)),pk(cask_3))

~X_1

{116}get revokedcerts(=attvid_4): else branch taken
{109}event ValidGroupKeyRequestReceived(cask_3, attvid_4)
{114}event ValidGroupPrivateKeySent(attvid_4,gsk(attvid_4,gmsk_5),gpk(gmsk_5))

~M_12

~M_8 = 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_5),gpk(gmsk_5))

~M_13

~M_13

{22}event ValidGroupPrivateKeyReceived(vid_8,gsk(vid_8,gmsk_5),gpk(gmsk_5))

! ! !

Beginning of process VehicleReport(vid_8, vsk_5, cert(vid_8,pk(vsk_5),cask_3), pk(cask_3), gpk(gmsk_5))

~X_2

{48}event RevocationAsked(vid_8,cert(vid_8,pk(vsk_5),cask_3),pseudocert(pk(cask_3),gsk(attvid_3, gmsk_5)))

~M_14

~M_11

{154}get revokedcerts(=vid_9): else branch taken
{127}event ValidRevocationReportReceived(pseudocert(pk(a_6),gsk(attvid_3,gmsk_5)),cert(vid_9,pk(vsk_6), cask_3))
{153}get revokedcerts(=attvid_3): else branch taken
{130}event RevokedVid(attvid_3)

~M_14

{154}get revokedcerts(=vid_8): else branch taken
{127}event ValidRevocationReportReceived(pseudocert(pk(cask_3),gsk(attvid_3,gmsk_5)),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)