Abbreviations
~M_4 = aenc(((groupkey_response,vid_10,gsk(vid_10,gmsk_5),gpk(gmsk_5)),sign((groupkey_response,vid_10,gsk(vid_10,gmsk_5),gpk(gmsk_5)),cask_3)),pk(vsk_6))
~M_5 = aenc(((pseudocert(pk(a_4),gsk(a_5,gmsk_5)),revoke_request),sign((pseudocert(pk(a_4),gsk(a_5,gmsk_5)),revoke_request),vsk_6),cert(vid_10,pk(vsk_6),cask_3)),pk(cask_3))
~M_6 = 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_5))
~M_7 = aenc(((pseudocert(pk(a_9),gsk(a_5,gmsk_5)),revoke_request),sign((pseudocert(pk(a_9),gsk(a_5,gmsk_5)),revoke_request),vsk_5),cert(vid_9,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

{6}new vid_10
{7}new vsk_6

{6}new vid_9
{7}new vsk_5

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

Beginning of process CA

Beginning of process CA

Beginning of process CARevoke

Beginning of process CARevoke

Beginning of process Vehicle
{15}event ValidGroupKeyRequestSent(vid_10)

~M_2 = aenc((groupkey_request,sign(groupkey_request,
vsk_5),cert(vid_9,pk(vsk_5),cask_3)),pk(cask_3))

~M_3 = aenc((groupkey_request,sign(groupkey_request,
vsk_6),cert(vid_10,pk(vsk_6),cask_3)),pk(cask_3))

~M_3 = aenc((groupkey_request,sign(groupkey_request,
vsk_6),cert(vid_10,pk(vsk_6),cask_3)),pk(cask_3))

{116}get revokedcerts(=vid_10): else branch taken
{109}event ValidGroupKeyRequestReceived(cask_3,
vid_10)
{114}event ValidGroupPrivateKeySent(vid_10,gsk(
vid_10,gmsk_5),gpk(gmsk_5))

~M_4

~M_4

{22}event ValidGroupPrivateKeyReceived(vid_10,
gsk(vid_10,gmsk_5),gpk(gmsk_5))

! ! !

Beginning of process VehicleReport(vid_10, vsk_6,
cert(vid_10,pk(vsk_6),cask_3), pk(cask_3), gpk(
gmsk_5))

(a_3,sign(a_3,a_4),pseudocert(pk(a_4),gsk(a_5,
~M_1))) = (a_3,sign(a_3,a_4),pseudocert(pk(a_4),
gsk(a_5,gmsk_5)))

{48}event RevocationAsked(vid_10,cert(vid_10,pk(
vsk_6),cask_3),pseudocert(pk(a_4),gsk(a_5,gmsk_5)))

~M_5

~M_2 = aenc((groupkey_request,sign(groupkey_request,
vsk_5),cert(vid_9,pk(vsk_5),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_6

~M_6

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

! ! !

Beginning of process VehicleReport(vid_9, vsk_5,
cert(vid_9,pk(vsk_5),cask_3), pk(cask_3), gpk(
gmsk_5))

(a_8,sign(a_8,a_9),pseudocert(pk(a_9),gsk(a_5,
~M_1))) = (a_8,sign(a_8,a_9),pseudocert(pk(a_9),
gsk(a_5,gmsk_5)))

{48}event RevocationAsked(vid_9,cert(vid_9,pk(
vsk_5),cask_3),pseudocert(pk(a_9),gsk(a_5,gmsk_5)))

~M_7

~M_5

{154}get revokedcerts(=vid_10): else branch taken
{127}event ValidRevocationReportReceived(pseudocert(
pk(a_4),gsk(a_5,gmsk_5)),cert(vid_10,pk(vsk_6),
cask_3))
{153}get revokedcerts(=a_5): else branch taken
{130}event RevokedVid(a_5)
{131}insert revokedcerts(a_5)

~M_7

{154}get revokedcerts(=vid_9): else branch taken
{127}event ValidRevocationReportReceived(pseudocert(
pk(a_9),gsk(a_5,gmsk_5)),cert(vid_9,pk(vsk_5),
cask_3))
{153}get revokedcerts(a_5)

{129}event AlreadyRevoked(a_5)