Abbreviations
~M_9 = aenc(((groupkey_response,vid_7,gsk(vid_7, gmsk_5),gpk(gmsk_5)),sign((groupkey_response,vid_7, gsk(vid_7,gmsk_5),gpk(gmsk_5)),cask_3)),pk(vsk_4))
~M_10 = aenc(((pseudocert(pk(a_5),gsk(attvid_4, gmsk_5)),revoke_request),sign((pseudocert(pk(a_5), gsk(attvid_4,gmsk_5)),revoke_request),vsk_4),cert(vid_7,pk(vsk_4),cask_3)),pk(cask_3))
~X_1 = aenc(((pseudocert(a_10,gsk(~M_5,~M_1)),revoke_request), sign((pseudocert(a_10,gsk(~M_5,~M_1)),revoke_request), ~M_3),~M_4),~M) = aenc(((pseudocert(a_10,gsk(attvid_4, gmsk_5)),revoke_request),sign((pseudocert(a_10, gsk(attvid_4,gmsk_5)),revoke_request),attsk_3), cert(attvid_3,pk(attsk_3),cask_3)),pk(cask_3))

A trace has been found.

Honest Process

{1}new gmsk_5

{2}new cask_3

~M = pk(cask_3)

Attacker

!

!

!

!

!

Beginning of process CAGroupMasterSecretKeyReveal

{156}event CAGMSKReveal(gmsk_5)

{6}new vid_7

{7}new vsk_4

~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 CARevoke

Beginning of process CARevoke

(~M_2,~M_3,~M_4) = (attvid_3,attsk_3,cert(attvid_3, pk(attsk_3),cask_3))

(~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_7)

~M_8 = aenc((groupkey_request,sign(groupkey_request, vsk_4),cert(vid_7,pk(vsk_4),cask_3)),pk(cask_3))

~M_8 = aenc((groupkey_request,sign(groupkey_request, vsk_4),cert(vid_7,pk(vsk_4),cask_3)),pk(cask_3))

{116}get revokedcerts(=vid_7): else branch taken

{109}event ValidGroupKeyRequestReceived(cask_3, vid_7)

{114}event ValidGroupPrivateKeySent(vid_7,gsk(vid_7,gmsk_5),gpk(gmsk_5))

~M_9

~M_9

{22}event ValidGroupPrivateKeyReceived(vid_7,gsk(vid_7,gmsk_5),gpk(gmsk_5))

! ! !

Beginning of process VehicleReport(vid_7, vsk_4, cert(vid_7,pk(vsk_4),cask_3), pk(cask_3), gpk(gmsk_5))

(a_4,sign(a_4,a_5),pseudocert(pk(a_5),gsk(~M_5, ~M_1))) = (a_4,sign(a_4,a_5),pseudocert(pk(a_5), gsk(attvid_4,gmsk_5)))

{48}event RevocationAsked(vid_7,cert(vid_7,pk(vsk_4),cask_3),pseudocert(pk(a_5),gsk(attvid_4, gmsk_5)))

~M_10

aenc((groupkey_request,a_7,~M_7),~M) = aenc((groupkey_request, a_7,cert(attvid_4,pk(attsk_4),cask_3)),pk(cask_3))

~M_10

{154}get revokedcerts(=vid_7): else branch taken

{127}event ValidRevocationReportReceived(pseudocert(pk(a_5),gsk(attvid_4,gmsk_5)),cert(vid_7,pk(vsk_4), cask_3))

{153}get revokedcerts(=attvid_4): else branch taken

{130}event RevokedVid(attvid_4)

~X_1

{154}get revokedcerts(=attvid_3): else branch taken

{127}event ValidRevocationReportReceived(pseudocert(a_10,gsk(attvid_4,gmsk_5)),cert(attvid_3,pk(attsk_3), cask_3))

{153}get revokedcerts(=attvid_4): else branch taken

{130}event RevokedVid(attvid_4)

{131}insert revokedcerts(attvid_4)

{116}get revokedcerts(attvid_4)

{107}event RevokedCannotGetGroupKey(attvid_4)