Abbreviations
~M_8 = aenc(((groupkey_response,vid_11,gsk(vid_11, gmsk_5),gpk(gmsk_5)),sign((groupkey_response,vid_11, gsk(vid_11,gmsk_5),gpk(gmsk_5)),cask_3)),pk(vsk_8))
~M_9 = aenc(((pseudocert(pk(a_6),gsk(attvid_2, gmsk_5)),revoke_request),sign((pseudocert(pk(a_6), gsk(attvid_2,gmsk_5)),revoke_request),vsk_8),cert(vid_11,pk(vsk_8),cask_3)),pk(cask_3))
~M_10 = 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_7))
~M_17 = 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))
~X_1 = (~M_14,~M_15,pseudocert(getpseudopk(~M_13),gsk(~M_2,~M_1))) = (m_10,sign(m_10,vpseudosk_3),pseudocert(pk(vpseudosk_3),gsk(attvid_2,gmsk_5)))
~M_18 = aenc(((pseudocert(pk(vpseudosk_3),gsk(attvid_2,gmsk_5)),revoke_request),sign((pseudocert(pk(vpseudosk_3),gsk(attvid_2,gmsk_5)),revoke_request), vsk_6),cert(vid_9,pk(vsk_6),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_2

{93}new attsk_2

{96}event AttackerGetsEnrollmentCertificate(attvid_2, pk(attsk_2))

Beginning of process CA

Beginning of process CA

Beginning of process CA

Beginning of process CA

Beginning of process CARevoke

Beginning of process CARevoke

{6}new vid_11

{7}new vsk_8

{6}new vid_10

{7}new vsk_7

{6}new vid_9

{7}new vsk_6

(~M_2,~M_3,~M_4) = (attvid_2,attsk_2,cert(attvid_2, pk(attsk_2),cask_3))

Beginning of process Vehicle

{15}event ValidGroupKeyRequestSent(vid_9)

~M_5 = aenc((groupkey_request,sign(groupkey_request, vsk_6),cert(vid_9,pk(vsk_6),cask_3)),pk(cask_3))

Beginning of process Vehicle

{15}event ValidGroupKeyRequestSent(vid_10)

~M_6 = aenc((groupkey_request,sign(groupkey_request, vsk_7),cert(vid_10,pk(vsk_7),cask_3)),pk(cask_3))

Beginning of process Vehicle

{15}event ValidGroupKeyRequestSent(vid_11)

~M_7 = aenc((groupkey_request,sign(groupkey_request, vsk_8),cert(vid_11,pk(vsk_8),cask_3)),pk(cask_3))

~M_7 = aenc((groupkey_request,sign(groupkey_request, vsk_8),cert(vid_11,pk(vsk_8),cask_3)),pk(cask_3))

{116}get revokedcerts(=vid_11): else branch taken

{109}event ValidGroupKeyRequestReceived(cask_3, vid_11)

{114}event ValidGroupPrivateKeySent(vid_11,gsk(vid_11,gmsk_5),gpk(gmsk_5))

~M_8

~M_8

{22}event ValidGroupPrivateKeyReceived(vid_11, gsk(vid_11,gmsk_5),gpk(gmsk_5))

!

!

!

Beginning of process VehicleReport(vid_11, vsk_8, cert(vid_11,pk(vsk_8),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_2,gmsk_5)))

{48}event RevocationAsked(vid_11,cert(vid_11,pk(vsk_8),cask_3),pseudocert(pk(a_6),gsk(attvid_2, gmsk_5)))

~M_9

aenc((groupkey_request,a_8,~M_4),~M) = aenc((groupkey_request, a_8,cert(attvid_2,pk(attsk_2),cask_3)),pk(cask_3))

~M_6 = aenc((groupkey_request,sign(groupkey_request, vsk_7),cert(vid_10,pk(vsk_7),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_10

~M_10

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

!

!

!

Beginning of process VehicleSend(vid_10, gsk(vid_10, gmsk_5))

{24}new vpseudosk_3

{27}event PseudoCertCreated(vid_10,vpseudosk_3)

!

{29}new m_10

{31}event ValidMessageSent(vid_10,pseudocert(pk(vpseudosk_3),gsk(vid_10,gmsk_5)),m_10)

{29}new m_9

{31}event ValidMessageSent(vid_10,pseudocert(pk(vpseudosk_3),gsk(vid_10,gmsk_5)),m_9)

(~M_11,~M_12,~M_13) = (m_9,sign(m_9,vpseudosk_3), pseudocert(pk(vpseudosk_3),gsk(vid_10,gmsk_5)))

(~M_14,~M_15,~M_16) = (m_10,sign(m_10,vpseudosk_3), pseudocert(pk(vpseudosk_3),gsk(vid_10,gmsk_5)))

~M_5 = 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_17

~M_17

{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))

~X_1

{48}event RevocationAsked(vid_9,cert(vid_9,pk(vsk_6),cask_3),pseudocert(pk(vpseudosk_3),gsk(attvid_2,gmsk_5)))

~M_18

~M_9

{154}get revokedcerts(=vid_11): else branch taken

{127}event ValidRevocationReportReceived(pseudocert(pk(a_6),gsk(attvid_2,gmsk_5)),cert(vid_11,pk(vsk_8), cask_3))

{153}get revokedcerts(=attvid_2): else branch taken

{130}event RevokedVid(attvid_2)

~M_18

{154}get revokedcerts(=vid_9): else branch taken

{127}event ValidRevocationReportReceived(pseudocert(pk(vpseudosk_3),gsk(attvid_2,gmsk_5)),cert(vid_9, pk(vsk_6),cask_3))

{153}get revokedcerts(=attvid_2): else branch taken

{130}event RevokedVid(attvid_2)

{131}insert revokedcerts(attvid_2)

{116}get revokedcerts(attvid_2)

{107}event RevokedCannotGetGroupKey(attvid_2)