Abbreviations
~X_1 = aenc((groupkey_request,sign(groupkey_request,~M_3),~M_4),~M) = aenc((groupkey_request,sign(groupkey_request,attsk_3),cert(attvid_3,pk(attsk_3),cask_4)),pk(cask_4))
~M_10 = 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_4)),pk(attsk_3))
~X_2 = aenc(((groupkey_response,getid(3-proj-3-tuple(adec(~M_9,~M_1))),3-proj-4-tuple(1-proj-2-tuple(adec(~M_10,~M_3))),a_5),sign((groupkey_response,getid(3-proj-3-tuple(adec(~M_9,~M_1))),3-proj-4-tuple(1-proj-2-tuple(adec(~M_10,~M_3))),a_5),~M_1)),getpk(3-proj-3-tuple(adec(~M_9,~M_1)))) = aenc(((groupkey_response,vid_10,gsk(attvid_3,gmsk_4),a_5),sign((groupkey_response,vid_10,gsk(attvid_3,gmsk_4),a_5),cask_4)),pk(vsk_6))
~M_17 = 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_4)),pk(vsk_5))
~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_9,pk(vsk_5),cask_4)),pk(cask_4))
~X_3 = aenc(((pseudocert(a_11,3-proj-4-tuple(1-proj-2-tuple(adec(~M_10,~M_3)))),revoke_request),sign((pseudocert(a_11,3-proj-4-tuple(1-proj-2-tuple(adec(~M_10,~M_3)))),revoke_request),~M_6),~M_7),~M) = aenc((pseudocert(a_11,gsk(attvid_3,gmsk_4)),revoke_request),sign((pseudocert(a_11,gsk(attvid_3,gmsk_4)),revoke_request),attsk_4),cert(attvid_4,pk(attsk_4),cask_4)),pk(cask_4))

A trace has been found.

Honest Process

Attacker

{1}new gmsk_4

{2}new cask_4

~M = pk(cask_4)

!

Beginning of process CASecretKeyReveal

{156}event CASKReveal(cask_4)

~M_1 = cask_4

{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 RSU_Register

Beginning of process RSU_Register

Beginning of process RSU_Revoke

Beginning of process RSU_Revoke

(~M_2,~M_3,~M_4) = (attvid_3,attsk_3,cert(attvid_3,pk(attsk_3),cask_4))

{6}new vid_10

{7}new vsk_6

{6}new vid_9

{7}new vsk_5

(~M_5,~M_6,~M_7) = (attvid_4,attsk_4,cert(attvid_4,pk(attsk_4),cask_4))

Beginning of process VehicleRegistration

{15}event ValidGroupKeyRequestSent(vid_9)

Beginning of process VehicleRegistration

{15}event ValidGroupKeyRequestSent(vid_10)

~M_8 = aenc((groupkey_request,sign(groupkey_request,vsk_5),cert(vid_9,pk(vsk_5),cask_4)),pk(cask_4))

~M_9 = aenc((groupkey_request,sign(groupkey_request,vsk_6),cert(vid_10,pk(vsk_6),cask_4)),pk(cask_4))

~X_1

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

{109}event ValidGroupKeyRequestReceived(cask_4,attvid_3)

{114}event ValidGroupPrivateKeySent(attvid_3,gsk(attvid_3,gmsk_4),gpk(gmsk_4))

~M_10

~X_2

{22}event ValidGroupPrivateKeyReceived(vid_10,gsk(attvid_3,gmsk_4),a_5)

!

Beginning of process VehicleSendMessages(vid_10,gsk(attvid_3,gmsk_4))

{24}new vpseudosk_3

{27}event PseudoCertCreated(vid_10,vpseudosk_3)

{29}new m_9

{31}event ValidMessageSent(vid_10,pseudocert(pk(vpseudosk_3),gsk(attvid_3,gmsk_4)),m_9)

{29}new m_8

{31}event ValidMessageSent(vid_10,pseudocert(pk(vpseudosk_3),gsk(attvid_3,gmsk_4)),m_8)

(~M_11,~M_12,~M_13) = (m_8,sign(m_8,vpseudosk_3),pseudocert(pk(vpseudosk_3),gsk(attvid_3,gmsk_4)))

(~M_14,~M_15,~M_16) = (m_9,sign(m_9,vpseudosk_3),pseudocert(pk(vpseudosk_3),gsk(attvid_3,gmsk_4)))

~M_8 = aenc((groupkey_request,sign(groupkey_request,vsk_5),cert(vid_9,pk(vsk_5),cask_4)),pk(cask_4))

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

{109}event ValidGroupKeyRequestReceived(cask_4,vid_9)

{114}event ValidGroupPrivateKeySent(vid_9,gsk(vid_9,gmsk_4),gpk(gmsk_4))

~M_17

~M_17

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

Beginning of process VehicleReport(vid_9, vsk_5, cert(vid_9,pk(vsk_5),cask_4), pk(cask_4), gpk(gmsk_4))

(~M_14,~M_15,~M_13) = (m_9,sign(m_9,vpseudosk_3),pseudocert(pk(vpseudosk_3),gsk(attvid_3,gmsk_4)))

{48}event RevocationAsked(vid_9,cert(vid_9,pk(vsk_5),cask_4),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_11,gsk(attvid_3,gmsk_4)),cert(attvid_4,pk(attsk_4),cask_4))

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

{130}event RevokedVid(attvid_3)

{131}insert revokedcerts(attvid_3)

~M_18

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

{127}event ValidRevocationReportReceived(pseudocert(pk(vpseudosk_3),gsk(attvid_3,gmsk_4)),cert(vid_9,pk(vsk_5),cask_4))

{153}get revokedcerts(attvid_3)

{129}event AlreadyRevoked(attvid_3)