Abbreviations
~M_6 = aenc(((groupkey_response,vid_8,gsk(vid_8, gmsk_6),gpk(gmsk_6)),sign((groupkey_response,vid_8, gsk(vid_8,gmsk_6),gpk(gmsk_6)),cask_3)),pk(vsk_4))
~M_7 = aenc(((pseudocert(pk(a_4),gsk(a_5,gmsk_6)), revoke_request),sign((pseudocert(pk(a_4),gsk(a_5, gmsk_6)),revoke_request),vsk_4),cert(vid_8,pk(vsk_4),cask_3)),pk(cask_3))
~X_1 = aenc((groupkey_request,sign(groupkey_request,~M_3), ~M_4),~M) = aenc((groupkey_request,sign(groupkey_request, attsk_2),cert(attvid_2,pk(attsk_2),cask_3)),pk(cask_3))

A trace has been found.

Honest Process

Attacker

{1}new gmsk_6

{2}new cask_3

~M = pk(cask_3)

!

!

!

!

Beginning of process GroupMasterSecretKeyReveal

{156}event CAGMSKReveal(gmsk_6)

{6}new vid_8

{7}new vsk_4

{92}new attvid_2

{93}new attsk_2

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

Beginning of process RSU_Register

Beginning of process RSU_Revoke

~M_1 = gmsk_6

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

Beginning of process VehicleRegistration

{15}event ValidGroupKeyRequestSent(vid_8)

~M_5 = aenc((groupkey_request,sign(groupkey_request, vsk_4),cert(vid_8,pk(vsk_4),cask_3)),pk(cask_3))

~M_5 = aenc((groupkey_request,sign(groupkey_request, vsk_4),cert(vid_8,pk(vsk_4),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_6),gpk(gmsk_6))

~M_6

~M_6

{22}event ValidGroupPrivateKeyReceived(vid_8,gsk(vid_8,gmsk_6),gpk(gmsk_6))

! ! !

Beginning of process VehicleReport(vid_8, vsk_4, cert(vid_8,pk(vsk_4),cask_3), pk(cask_3), gpk(gmsk_6))

(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_6)))

{48}event RevocationAsked(vid_8,cert(vid_8,pk(vsk_4),cask_3),pseudocert(pk(a_4),gsk(a_5,gmsk_6)))

~M_7

~M_7

{154}get revokedcerts(=vid_8): else branch taken

{127}event ValidRevocationReportReceived(pseudocert(pk(a_4),gsk(a_5,gmsk_6)),cert(vid_8,pk(vsk_4), cask_3))

{153}get revokedcerts(=a_5): else branch taken

{130}event RevokedVid(a_5)

{131}insert revokedcerts(a_5)

Phase 1

{133}new updatedgmsk_2

Phase 2

!

Beginning of process VehicleRegistration

Beginning of process RSU_Register

~X_1

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

{145}event ValidGroupKeyRequestReceived(cask_3, attvid_2)

{150}event ValidGroupPrivateKeySent(attvid_2,gsk(attvid_2,updatedgmsk_2),gpk(updatedgmsk_2))