Abbreviations ~M_7 = aenc(((groupkey_response,vid_9,gsk(vid_9,gmsk_5),gpk(gmsk_5)),sign((groupkey_response,vid_9,gsk(vid_9,gsk(vid_9,gmsk_5)),gpk(gmsk_5)),cask_3)),pk(vsk_6)) \sim M_8 = aenc(((pseudocert(pk(a_5),gsk(attvid_2,

gmsk_5)),revoke_request),sign((pseudocert(pk(a_5), gsk(attvid_2,gmsk_5)),revoke_request),vsk_6),cert(vid_9,pk(vsk_6),cask_3)),pk(cask_3)) ~M_9 = aenc(((groupkey_response,vid_8,gsk(vid_8,gmsk_5),gpk(gmsk_5)),sign((groupkey_response,vid_8,gsk(vid_8,gsk(vid_8,gmsk_5)),cask_3)),pk(vsk_5)) $\sim X_1 = (a_10, sign(a_10, a_11), pseudocert(pk(a_11), gsk(-2, -M_1)))$

= (a_10,sign(a_10,a_11),pseudocert(pk(a_11),gsk(attvid_2,gmsk_5))) ~M_10 = aenc(((pseudocert(pk(a_11),gsk(attvid_2,gmsk_5)),revoke_request),sign((pseudocert(pk(a_11),gsk(attvid_2,gmsk_5)),revoke_request),vsk_5),cert(vid_8,pk(vsk_5),cask_3)),pk(cask_3)) Attacker **Honest Process** {1}new gmsk_5 {2}new cask_3 \sim M = pk(cask_3) Beginning of process CAGroupMasterSecretKeyReveal {156}event CAGMSKReveal(gmsk_5) {92}new attvid_2 {93} new attsk_2 {96} event AttackerGetsEnrollmentCertificate(attvid_2, pk(attsk_2)) \sim M_1 = gmsk_5 Beginning of process CA

Beginning of process CARevoke

Beginning of process CARevoke Beginning of process CA Beginning of process CA {6}new vid_8 {6}new vid_9 {7}new vsk_6 {7}new vsk_5 $(\sim M_2, \sim M_3, \sim M_4) = (attvid_2, attsk_2, cert(attvid_2, pk(attsk_2), cask_3))$ Beginning of process Vehicle {15} event ValidGroupKeyRequestSent(vid_8) ~M_5 = aenc((groupkey_request, sign(groupkey_request, vsk_5),cert(vid_8,pk(vsk_5),cask_3)),pk(cask_3)) Beginning of process Vehicle {15} event ValidGroupKeyRequestSent(vid_9) ~M_6 = aenc((groupkey_request,sign(groupkey_request, vsk_6),cert(vid_9,pk(vsk_6),cask_3)),pk(cask_3)) ~M_6 = 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)) \sim M_{_}7 {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)) (a_4,sign(a_4,a_5),pseudocert(pk(a_5),gsk(~M_2, ~M_1))) = (a_4,sign(a_4,a_5),pseudocert(pk(a_5), gsk(attvid_2,gmsk_5))) {48} event RevocationAsked(vid_9,cert(vid_9,pk(vsk_6),cask_3),pseudocert(pk(a_5),gsk(attvid_2,gmsk_5))) \sim M_8 aenc((groupkey_request,a_7, \sim M_4), \sim M) = aenc((groupkey_request,a_7,cert(attvid_2,pk(attsk_2),cask_3)),pk(cask_3)) ~M_5 = aenc((groupkey_request,sign(groupkey_request, vsk_5),cert(vid_8,pk(vsk_5),cask_3)),pk(cask_3)) {116}get revokedcerts(=vid_8): else branch taken {109}event ValidGroupKeyRequestReceived(cask 3, {114}event ValidGroupPrivateKeySent(vid_8,gsk(vid_8,gmsk_5),gpk(gmsk_5)) ~M 9 ~M 9 {22} event ValidGroupPrivateKeyReceived(vid_8,gsk(vid_8,gmsk_5),gpk(gmsk_5)) Beginning of process VehicleReport(vid_8, vsk_5, cert(vid_8,pk(vsk_5),cask_3), pk(cask_3), gpk(gmsk_5)) ~X_1 {48} event RevocationAsked(vid_8,cert(vid_8,pk(vsk_5),cask_3),pseudocert(pk(a_11),gsk(attvid_2,gmsk_5))) \sim M_10 \sim M_8 {154}get revokedcerts(=vid_9): else branch taken {127}event ValidRevocationReportReceived(pseudocert(pk(a_5),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) \sim M_10 {154}get revokedcerts(=vid_8): else branch taken {127}event ValidRevocationReportReceived(pseudocert(pk(a_11),gsk(attvid_2,gmsk_5)),cert(vid_8,pk(vsk_5),cask_3)) {153}get revokedcerts(=attvid_2): else branch taken

A trace has been found.

{116}get revokedcerts(attvid_2)

{130}event RevokedVid(attvid_2)

{131}insert revokedcerts(attvid_2)