~M_12 = aenc(((pseudocert(pk(vpseudosk_3),gsk(vid_12,gmsk_5)),revoke_request),sign((pseudocert(pk(vpseudocert(pk(vpseudosk_3),gsk(vid_12,gmsk_5)),revoke_request),vsk_7),cert(vid_11,pk(vsk_7),cask_3)),pk(cask_3)) ~M_16 = aenc(((groupkey_response,vid_10,gsk(vid_10, updatedgmsk_2),gpk(updatedgmsk_2)),sign((groupkey_response, vid_10,gsk(vid_10,updatedgmsk_2),gpk(updatedgmsk_2)), cask_3)),pk(vsk_6)) Attacker **Honest Process** \sim M = pk(cask_3) {6} new vid_10 {7} new vsk_6 {6} new vid_12 {7} new vsk_8 {6} new vid_11 {7} new vsk_7 Beginning of process CARevoke Beginning of process Vehicle
{15}event ValidGroupKeyRequestSent(vid_10) Beginning of process CA

Beginning of process CA ~M_1 = aenc((groupkey_request,sign(groupkey_request, vsk_6),cert(vid_10,pk(vsk_6),cask_3)),pk(cask_3)) Beginning of process Vehicle {15} event ValidGroupKeyRequestSent(vid_11) ~M_2 = aenc((groupkey_request,sign(groupkey_request, vsk_7),cert(vid_11,pk(vsk_7),cask_3)),pk(cask_3)) Beginning of process Vehicle
{15}event ValidGroupKeyRequestSent(vid_12) ~M_3 = aenc((groupkey_request,sign(groupkey_request, vsk_8),cert(vid_12,pk(vsk_8),cask_3)),pk(cask_3)) ~M_3 = aenc((groupkey_request,sign(groupkey_request,vsk_8),cert(vid_12,pk(vsk_8),cask_3)),pk(cask_3)) {116}get revokedcerts(=vid_12): else branch taken {109}event ValidGroupKeyRequestReceived(cask_3, vid_12) {114}event ValidGroupPrivateKeySent(vid_12,gsk(vid_12,gmsk_5),gpk(gmsk_5)) \sim M_4 ~M_4 {22} event ValidGroupPrivateKeyReceived(vid_12, gsk(vid_12,gmsk_5),gpk(gmsk_5)) Beginning of process VehicleSend(vid_12, gsk(vid_12, gmsk_5))

{24}new vpseudosk_3 {27} event PseudoCertCreated(vid_12,vpseudosk_3) {29} new m_9 {29} new m_8 {31}event ValidMessageSent(vid_12,pseudocert(pk(vpseudosk_3),gsk(vid_12,gmsk_5)),m_9) {31} event ValidMessageSent(vid_12,pseudocert(pk(vpseudosk_3),gsk(vid_12,gmsk_5)),m_8) $(\sim M_5, \sim M_6, \sim M_7) = (m_8, sign(m_8, vpseudosk_3), pseudocert(pk(vpseudosk_3), gsk(vid_12, gmsk_5)))$ $(\sim M_8, \sim M_9, \sim M_{10}) = (m_9, sign(m_9, vpseudosk_3), pseudocert(pk(vpseudosk_3), gsk(vid_12, gmsk_5)))$ {116}get revokedcerts(=vid_11): else branch taken \sim M_11 {22} event ValidGroupPrivateKeyReceived(vid_11, gsk(vid_11,gmsk_5),gpk(gmsk_5)) $(\sim M_8, \sim M_9, \sim M_7) = (m_9, sign(m_9, vpseudosk_3), pseudocert(pk(vpseudosk_3), gsk(vid_12, gmsk_5)))$ {48} event RevocationAsked(vid_11,cert(vid_11,pk(vsk_7),cask_3),pseudocert(pk(vpseudosk_3),gsk(vid_12,gmsk_5))) \sim M_12 {154}get revokedcerts(=vid_11): else branch taken {127} event ValidRevocationReportReceived(pseudocert(pk(vpseudosk_3),gsk(vid_12,gmsk_5)),cert(vid_11,pk(vsk_7),cask_3))

{153} get revokedcerts(=vid_12): else branch taken {130}event RevokedVid(vid_12) {131}insert revokedcerts(vid_12) Phase 1 Phase 2 Beginning of process Vehicle

{56} event ValidGroupKeyRequestSent(vid_11)

Beginning of process Vehicle

{56} event ValidGroupKeyRequestSent(vid_11) Beginning of process Vehicle {56} event ValidGroupKeyRequestSent(vid_12) Beginning of process CA ~M_13 = aenc((groupkey_request,sign(groupkey_request,vsk_6),cert(vid_10,pk(vsk_6),cask_3)),pk(cask_3)) \sim M_14 = aenc((groupkey_request, sign(groupkey_request,

~M_4 = aenc(((groupkey_response,vid_12,gsk(vid_12,gmsk_5),gpk(gmsk_5)),sign((groupkey_response,vid_12,gsk(vid_12,gmsk_5)),cask_3)),pk(vsk_8))

~M_11 = aenc(((groupkey_response,vid_11,gsk(vid_11,gmsk_5),gpk(gmsk_5)),sign((groupkey_response,vid_11,gsk(vid_11,gsk(vid_11,gsk(vid_11,gmsk_5)),cask_3)),pk(vsk_7))

A trace has been found.