A trace has been found.

 \sim M_14 = aenc(((pseudocert(pk(vpseudosk_3),gsk(vid_10,gmsk_5)),revoke_request),sign((pseudocert(pk(vpseudosk_3),gsk(vid_10,gmsk_5)),revoke_request), vsk_5),cert(vid_9,pk(vsk_5),cask_3)),pk(cask_3)) ~X_1 = aenc((groupkey_request, sign(groupkey_request, ~M_2), ~M_3), ~M)
= aenc((groupkey_request, sign(groupkey_request, attsk_2), cert(attvid_2, pk(attsk_2), cask_3)), pk(cask_3)) Attacker **Honest Process** {1}new gmsk_5 {2}new cask_3 \sim M = pk(cask_3) {92} new attvid_2 {93}new attsk_2 Beginning of process CA Beginning of process CARevoke Beginning of process CA {96} event AttackerGetsEnrollmentCertificate(attvid_2, pk(attsk_2)) {6} new vid_10 [6] new vid_9 {7}new vsk_6 {7}new vsk_5 $(\sim M_1, \sim M_2, \sim M_3) = (attvid_2, attsk_2, cert(attvid_2, pk(attsk_2), cask_3))$ Beginning of process Vehicle {15} event ValidGroupKeyRequestSent(vid_9) ~M_4 = aenc((groupkey_request,sign(groupkey_request,vsk_5),cert(vid_9,pk(vsk_5),cask_3)),pk(cask_3)) Beginning of process Vehicle {15} event ValidGroupKeyRequestSent(vid_10) ~M_5 = aenc((groupkey_request,sign(groupkey_request,vsk_6),cert(vid_10,pk(vsk_6),cask_3)),pk(cask_3)) ~M_5 = aenc((groupkey_request,sign(groupkey_request, vsk_6),cert(vid_10,pk(vsk_6),cask_3)),pk(cask_3)) {116}get revokedcerts(=vid_10): else branch taken {109}event ValidGroupKeyRequestReceived(cask_3, {114}event ValidGroupPrivateKeySent(vid_10,gsk(vid_10,gmsk_5),gpk(gmsk_5)) \sim M_6 {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_8 {31} event ValidMessageSent(vid_10,pseudocert(pk(vpseudosk_3),gsk(vid_10,gmsk_5)),m_8) $(\sim M_7, \sim M_8, \sim M_9) = (m_8, sign(m_8, vpseudosk_3), pseudocert(pk(vpseudosk_3), gsk(vid_10, gmsk_5)))$ $(\sim M_10, \sim M_11, \sim M_12) = (m_9, sign(m_9, vpseudosk_3), pseudocert(pk(vpseudosk_3), gsk(vid_10, gmsk_5)))$ ~M_4 = aenc((groupkey_request,sign(groupkey_request, vsk_5),cert(vid_9,pk(vsk_5),cask_3)),pk(cask_3)) {116}get revokedcerts(=vid_9): else branch taken {109}event ValidGroupKeyRequestReceived(cask_3, {114}event ValidGroupPrivateKeySent(vid_9,gsk(vid_9,gmsk_5),gpk(gmsk_5)) \sim M_13 {22} event ValidGroupPrivateKeyReceived(vid_9,gsk(vid_9,gmsk_5),gpk(gmsk_5)) Beginning of process VehicleReport(vid_9, vsk_5, cert(vid_9,pk(vsk_5),cask_3), pk(cask_3), gpk(gmsk_5)) $(\sim M_10, \sim M_11, \sim M_9) = (m_9, sign(m_9, vpseudosk_3), pseudocert(pk(vpseudosk_3), gsk(vid_10, gmsk_5)))$ {48} event RevocationAsked(vid_9,cert(vid_9,pk(vsk_5),cask_3),pseudocert(pk(vpseudosk_3),gsk(vid_10,gmsk_5))) ~M 14 ~M_14 {154}get revokedcerts(=vid_9): else branch taken {127} event ValidRevocationReportReceived(pseudocert(pk(vpseudosk_3),gsk(vid_10,gmsk_5)),cert(vid_9,pk(vsk_5),cask_3)) {153}get revokedcerts(=vid_10): else branch taken {130}event RevokedVid(vid_10) {131}insert revokedcerts(vid_10) Phase 1

Phase 2

Beginning of process Vehicle

Beginning of process Vehicle

{29}new m_9

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

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

{145}event ValidGroupKeyRequestReceived(cask_3, attvid_2)

{133}new updatedgmsk_2

Beginning of process CA

~X 1