A trace has been found. **Honest Process** {1}new gmsk_4 {2}new cask_4 \sim M = pk(cask_4) {92} new attvid_4 {92} new attvid_3 [6] new vid_7 {93}new attsk_4 {93}new attsk_3 Beginning of process CARevoke Beginning of process CA Beginning of process CARevoke Beginning of process CA $\{7\}$ new vsk_4 {96} event AttackerGetsEnrollmentCertificate(attvid_3, {96} event AttackerGetsEnrollmentCertificate(attvid_4, pk(attsk_4)) pk(attsk_3)) $(\sim M_1, \sim M_2, \sim M_3) = (attvid_3, attsk_3, cert(attvid_3, pk(attsk_3), cask_4))$ $(\sim M_4, \sim M_5, \sim M_6) = (attvid_4, attsk_4, cert(attvid_4, pk(attsk_4), cask_4))$ Beginning of process Vehicle {15} event ValidGroupKeyRequestSent(vid_7) ~M_7 = aenc((groupkey_request,sign(groupkey_request, vsk_4),cert(vid_7,pk(vsk_4),cask_4)),pk(cask_4)) {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_7 = aenc((groupkey_request,sign(groupkey_request,vsk_4),cert(vid_7,pk(vsk_4),cask_4)),pk(cask_4)) {116}get revokedcerts(=vid_7): else branch taken {109}event ValidGroupKeyRequestReceived(cask_4, vid 7) {114}event ValidGroupPrivateKeySent(vid_7,gsk(vid_7,gmsk_4),gpk(gmsk_4)) \sim M_9 \sim M_9 {22} event ValidGroupPrivateKeyReceived(vid_7,gsk(vid_7,gmsk_4),gpk(gmsk_4)) Beginning of process VehicleReport(vid_7, vsk_4, cert(vid_7,pk(vsk_4),cask_4), pk(cask_4), gpk(gmsk_4)) ~X 2 {48} event RevocationAsked(vid_7,cert(vid_7,pk(vsk_4),cask_4),pseudocert(pk(a_6),gsk(attvid_3,gmsk_4))) ~M 10 {154}get revokedcerts(=attvid_4): else branch taken {127} event ValidRevocationReportReceived(pseudocert(a_8,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) \sim M₁ {154}get revokedcerts(=vid_7): else branch taken {127} event ValidRevocationReportReceived(pseudocert(pk(a_6),gsk(attvid_3,gmsk_4)),cert(vid_7,pk(vsk_4),cask_4)) {153}get revokedcerts(attvid_3) {129}event AlreadyRevoked(attvid_3)

Abbreviations $\sim X_1 = aenc((groupkey_request, sign(groupkey_request, \sim M_2), \sim M_3), \sim M)$ = aenc((groupkey_request,sign(groupkey_request, attsk_3),cert(attvid_3,pk(attsk_3),cask_4)),pk(cask 4)) ~M_8 = aenc(((groupkey_response,attvid_3,gsk(attvid_3,gmsk_4),gpk(gmsk_4)),sign((groupkey_response,attvid_3,gsk(attvid_3,g \sim M_9 = aenc(((groupkey_response,vid_7,gsk(vid_7, gmsk_4),gpk(gmsk_4)),sign((groupkey_response,vid_7, gsk(vid_7,gmsk_4),gpk(gmsk_4)),cask_4)),pk(vsk_4)) $a_5,a_6)$, pseudocert(pk(\overline{a}_6), gsk(attvid_3, gmsk_4))) \sim M_10 = aenc(((pseudocert(pk(a_6),gsk(attvid_3, gmsk_4)),revoke_request),sign((pseudocert(pk(a_6), gsk(attvid_3,gmsk_4)),revoke_request),vsk_4),cert(vid_7,pk(vsk_4),cask_4)),pk(cask_4)) $\sim X_3 = aenc((pseudocert(a_8, 3-proj-4-tuple(1-proj-2-tuple($ adec(~M_8,~M_2)))),revoke_request),sign((pseudocert(a_8,3-proj-4-tuple(1-proj-2-tuple(adec(\sim M_8, \sim M_2)))), revoke_request), \sim M_5), \sim M_6), \sim M) = aenc(((pseudocert(
a_8,gsk(attvid_3,gmsk_4)),revoke_request),sign(
(pseudocert(a_8,gsk(attvid_3,gmsk_4)),revoke_request),
attsk_4),cert(attvid_4,pk(attsk_4),cask_4)),pk(
cask_4)) Attacker