~M_10 = aenc(((groupkey_response,vid_7,gsk(vid_7,gmsk_4),gpk(gmsk_4)),sign((groupkey_response,vid_7,gsk(vid_7,gsk(vid_7,gsk(vid_7,gsk(vid_7,gsk(yid_4)),cask_4)),pk(vsk_3)) A trace has been found. $a_6,a_7)$, pseudocert(pk(a_7), gsk(attvid_3, gmsk_4))) ~M_11 = aenc(((pseudocert(pk(a_7),gsk(attvid_3,gmsk_4)),revoke_request),sign((pseudocert(pk(a_7),gsk(attvid_3,gsk(attvid_3,gsk(attvid_3),revoke_request),vsk_3),cert(vid_7,pk(vsk_3),cask_4)),pk(cask_4)) ~X_3 = aenc(((pseudocert(a_9,3-proj-4-tuple(1-proj-2-tuple(adec(~M_9,~M_3)))),revoke_request),sign((pseudocert(a_9,3-proj-4-tuple(1-proj-2-tuple(adec(~M_9,~M_3)))),revoke_request),~M_6),~M_7),~M) = aenc(((pseudocert(a_9,gsk(attvid_3,gmsk_4)),revoke_request),sign((pseudocert(a_9,gsk(attvid_3,gmsk_4)),revoke_request),attsk_4),cert(attvid_4,pk(attsk_4),cask_4)),pk(cask_4)) Attacker **Honest Process** {1}new gmsk_4 {2}new cask_4 \sim M = pk(cask_4) Beginning of process CASecretKeyReveal {5}new vid_7 {6}new vsk_3 {155}event CASKReveal(cask_4) \sim M_1 = cask_4 {91}new attvid_4 {91}new attvid_3 {92}new attsk_3 {92} new attsk_4 Beginning of process CARegister | Beginning of process CARegister | Beginning of process CARegister | Beginning of process CARevoke | Beginning of process CAR {95} event AttackerGetsEnrollmentCertificate(attvid_3, pk(attsk_3)) {95} event AttackerGetsEnrollmentCertificate(attvid_4, pk(attsk_4)) $(\sim M_2, \sim M_3, \sim M_4) = (attvid_3, attsk_3, cert(attvid_3, pk(attsk_3), cask_4))$ $(\sim M_5, \sim M_6, \sim M_7) = (attvid_4, attsk_4, cert(attvid_4, pk(attsk_4), cask_4))$ Beginning of process VehicleRegistration {14} event ValidGroupKeyRequestSent(vid_7) ~M_8 = aenc((groupkey_request,sign(groupkey_request,vsk_3),cert(vid_7,pk(vsk_3),cask_4)),pk(cask_4)) $aenc((groupkey_request,a_2,\sim M_4),\sim M) = aenc((groupkey_request,a_4),\sim M)$ a_2,dert(attvid_3,pk(attsk_3),cask_4)),pk(cask_4)) {115}get revokedcerts(=attvid_3): else branch taken {108}event ValidGroupKeyRequestReceived(cask_4, {113}event ValidGroupPrivateKeySent(attvid_3,gsk(attvid_3,gmsk_4),gpk(gmsk_4)) ~M_8 = aenc((groupkey_request,sign(groupkey_request, vsk_3),cert(vid_7,pk(vsk_3),cask_4)),pk(cask_4)) {115}get revokedcerts(=vid_7): else branch taken {108}event ValidGroupKeyRequestReceived(cask_4, {113}event ValidGroupPrivateKeySent(vid_7,gsk(vid_7,gmsk_4),gpk(gmsk_4)) ~M 10 \sim M_10 {21} event ValidGroupPrivateKeyReceived(vid_7,gsk(vid_7,gmsk_4),gpk(gmsk_4)) Beginning of process VehicleReport(vid_7, vsk_3, cert(vid_7,pk(vsk_3),cask_4), pk(cask_4), gpk(gmsk_4)) {47} event RevocationAsked(vid_7,cert(vid_7,pk(vsk_3),cask_4),pseudocert(pk(a_7),gsk(attvid_3,gmsk_4))) \sim M_11 {153}get revokedcerts(=attvid_4): else branch taken {126} event ValidRevocationReportReceived(pseudocert(a_9,gsk(attvid_3,gmsk_4)),cert(attvid_4,pk(attsk_4),cask_4)) {152}get revokedcerts(=attvid_3): else branch taken {129}event RevokedVid(attvid_3) \sim M_11 {153}get revokedcerts(=vid_7): else branch taken {126} event ValidRevocationReportReceived(pseudocert(pk(a_7),gsk(attvid_3,gmsk_4)),cert(vid_7,pk(vsk_3),cask_4)) {152}get revokedcerts(=attvid_3): else branch taken {129}event RevokedVid(attvid_3) {130}insert revokedcerts(attvid_3) {115}get revokedcerts(attvid_3)

{106}event RevokedCannotGetGroupKey(attvid_3)

Abbreviations

 $\sim X_1 = aenc((groupkey_request, sign(groupkey_request, \sim M_3), \sim M_4), \sim M$

= aenc((groupkey_request, sign(groupkey_request, attsk_3),cert(attvid_3,pk(attsk_3),cask_4)),pk(

~M_9 = aenc(((groupkey_response,attvid_3,gsk(attvid_3,gmsk_4),gpk(gmsk_4)),sign((groupkey_response,attvid_3,gsk(attvid_3,g