~M_8 = aenc(((groupkey_response,attvid_4,gsk(attvid_4,gmsk_4),gpk(gmsk_4)),sign((groupkey_response,attvid_4, gsk(attvid_4,gmsk_4),gpk(gmsk_4)),cask_3)),pk(\sim X_2 = aenc(((pseudocert(a_3,3-proj-4-tuple(1-proj-2-tuple(A trace has been found. adec(~M_8,~M_5)))),revoke_request),sign((pseudocert(a_3,3-proj-4-tuple(1-proj-2-tuple(adec(\sim M_8, \sim M_5)))), revoke_request), \sim M_2), \sim M_3), \sim M) = aenc(((pseudocert(~M_10 = aenc(((groupkey_response,vid_7,gsk(vid_7,updatedgmsk_2)),sign((groupkey_response,vid_7,gsk(vid_7,updatedgmsk_2)),gpk(updatedgmsk_2)),cask_3)),pk(vsk_3)) **Honest Process** {1}new gmsk_4 {2}new cask_3 \sim M = pk(cask_3) {5}new vid_7 {6}new vsk_3 {91}new attvid_4 {91}new attvid_3 {92} new attsk_4 {92}new attsk_3 Beginning of process CARegister Beginning of process CARevoke {95} event AttackerGetsEnrollmentCertificate(attvid_3, pk(attsk_3)) {95} event AttackerGetsEnrollmentCertificate(attvid_4, pk(attsk_4)) $(\sim M_1, \sim M_2, \sim M_3) = (attvid_3, attsk_3, cert(attvid_3, pk(attsk_3), cask_3))$ $(\sim M_4, \sim M_5, \sim M_6) = (attvid_4, attsk_4, cert(attvid_4, pk(attsk_4), cask_3))$ Beginning of process VehicleRegistration {14} event ValidGroupKeyRequestSent(vid_7) ~M_7 = aenc((groupkey_request,sign(groupkey_request, vsk_3),cert(vid_7,pk(vsk_3),cask_3)),pk(cask_3)) $\sim X$ {115}get revokedcerts(=attvid_4): else branch taken {108}event ValidGroupKeyRequestReceived(cask_3, attvid_4) {113}event ValidGroupPrivateKeySent(attvid_4,gsk(attvid_4,gmsk_4),gpk(gmsk_4)) ~X 2 {153}get revokedcerts(=attvid_3): else branch taken {126} event ValidRevocationReportReceived(pseudocert(a_3,gsk(attvid_4,gmsk_4)),cert(attvid_3,pk(attsk_3),cask_3)) {152}get revokedcerts(=attvid_4): else branch taken {129}event RevokedVid(attvid_4) {130}insert revokedcerts(attvid_4) Phase 1 {132}new updatedgmsk_2 Phase 2 Beginning of process VehicleRegistration {55} event ValidGroupKeyRequestSent(vid_7) Beginning of process CARegister ~M_9 = aenc((groupkey_request,sign(groupkey_request, vsk_3),cert(vid_7,pk(vsk_3),cask_3)),pk(cask_3)) ~M_7 = aenc((groupkey_request,sign(groupkey_request, vsk_3),cert(vid_7,pk(vsk_3),cask_3)),pk(cask_3)) {151}get revokedcerts(=vid_7): else branch taken {144}event ValidGroupKeyRequestReceived(cask_3, vid 7) {149}event ValidGroupPrivateKeySent(vid_7,gsk(vid_7,updatedgmsk_2),gpk(updatedgmsk_2)) \sim M_10 ~M 10 {62} event ValidGroupPrivateKeyReceived(vid_7,gsk(vid_7,updatedgmsk_2),gpk(updatedgmsk_2)) Beginning of process VehicleSendMessages(vid_7, gsk(vid_7,updatedgmsk_2)) {64} new vpseudosk_3 {67} event PseudoCertCreated(vid_7,vpseudosk_3) {69} new m_7

{71} event ValidMessageSent(vid_7,pseudocert(pk(vpseudosk_3),gsk(vid_7,updatedgmsk_2)),m_7)

Abbreviations

 $\sim X_1 = aenc((groupkey_request, sign(groupkey_request, \sim M_5), \sim M_6), \sim M$

= aenc((groupkey_request, sign(groupkey_request, attsk_4),cert(attvid_4,pk(attsk_4),cask_3)),pk(