Abbreviations ~M_6 = aenc(((groupkey_response,vid_6,gsk(vid_6,gmsk_5),gpk(gmsk_5)),sign((groupkey_response,vid_6,gsk(vid_6,gsk(vid_6,gmsk_5)),cask_3)),pk(vsk_3)) ~M_16 = aenc(((pseudocert(pk(vpseudosk_4),gsk(vid_6,gmsk_5)),revoke_request),sign((pseudocert(pk(vpseudosk_4),gsk(vid_6,gmsk_5)),revoke_request),vsk_3),cert(vid_6,pk(vsk_3),cask_3)),pk(cask_3)) = aenc(((pseudocert(a_9,gsk(vid_6,gmsk_5)), revoke_request),sign((pseudocert(a_9,gsk(vid_6, gmsk_5)),revoke_request),attsk_2),cert(attvid_2, pk(attsk_2),cask_3)),pk(cask_3)) **Honest Process** Attacker \sim M = pk(cask_3) {5}new vid_6 {6}new vsk_3 Beginning of process CAGroupMasterSecretKeyReveal {155}event CAGMSKReveal(gmsk_5) {91}new attvid_2 {92} new attsk_2 {95} event AttackerGetsEnrollmentCertificate(attvid_2, pk(attsk_2)) \sim M_1 = gmsk_5 Beginning of process CARegister Beginning of process CARegister Beginning of process CARevoke Beginning of process CARevoke $(\sim M_2, \sim M_3, \sim M_4) = (attvid_2, attsk_2, cert(attvid_2, pk(attsk_2), cask_3))$ Beginning of process VehicleRegistration {14} event ValidGroupKeyRequestSent(vid_6) ~M_5 = aenc((groupkey_request,sign(groupkey_request,vsk_3),cert(vid_6,pk(vsk_3),cask_3)),pk(cask_3)) \sim M_5 = aenc((groupkey_request, sign(groupkey_request, vsk_3),cert(vid_6,pk(vsk_3),cask_3)),pk(cask_3)) ~M_5 = aenc((groupkey_request,sign(groupkey_request,vsk_3),cert(vid_6,pk(vsk_3),cask_3)),pk(cask_3)) {115}get revokedcerts(=vid_6): else branch taken {108}event ValidGroupKeyRequestReceived(cask_3, vid 6) {113}event ValidGroupPrivateKeySent(vid_6,gsk(vid_6,gmsk_5),gpk(gmsk_5)) \sim M_6 \sim M_6 {21} event ValidGroupPrivateKeyReceived(vid_6,gsk(vid_6,gmsk_5),gpk(gmsk_5)) Beginning of process VehicleSendMessages(vid_6, gsk(vid_6,gmsk_5)) Beginning of process VehicleSendMessages(vid_6, gsk(vid_6,gmsk_5)) Beginning of process VehicleReport(vid_6, vsk_3, cert(vid_6,pk(vsk_3),cask_3), pk(cask_3), gpk(gmsk_5)) {23}new vpseudosk_5 {23}new vpseudosk_4 {26} event PseudoCertCreated(vid_6,vpseudosk_4) {26} event PseudoCertCreated(vid_6,vpseudosk_5) {28} new m_11 {28} new m_10 {28} new m_9 [30] event ValidMessageSent(vid_6,pseudocert(pk(vpseudosk_5),gsk(vid_6,gmsk_5)),m_11) 0} event ValidMessageSent(vid_6,pseudocert(pk(vpseudosk_4),gsk(vid_6,gmsk_5)),m_10) 0} event ValidMessageSent(vid_6,pseudocert(pk(vpseudosk_4),gsk(vid_6,gmsk_5)),m_9) $(\sim M_7, \sim M_8, \sim M_9) = (m_9, sign(m_9, vpseudosk_4), pseudocert(pk(vpseudosk_4), gsk(vid_6, gmsk_5)))$ $(\sim M_10,\sim M_11,\sim M_12) = (m_10,sign(m_10,vpseudosk_4),pseudocert(pk(vpseudosk_4),gsk(vid_6,gmsk_5)))$ $(\sim M_13,\sim M_14,\sim M_15) = (m_11,sign(m_11,vpseudosk_5), pseudocert(pk(vpseudosk_5),gsk(vid_6,gmsk_5)))$ $(\sim M_10, \sim M_11, \sim M_9) = (m_10, sign(m_10, vpseudosk_4), pseudocert(pk(vpseudosk_4), gsk(vid_6, gmsk_5)))$ {47} event RevocationAsked(vid_6,cert(vid_6,pk(vsk_3),cask_3),pseudocert(pk(vpseudosk_4),gsk(vid_6,gmsk_5))) \sim M_16 ~X_1 {153}get revokedcerts(=attvid_2): else branch taken {126}event ValidRevocationReportReceived(pseudocert(a_9,gsk(vid_6,gmsk_5)),cert(attvid_2,pk(attsk_2),cask_3)) {152}get revokedcerts(=vid_6): else branch taken {129}event RevokedVid(vid_6) {153}get revokedcerts(=vid_6): else branch taken {126}event ValidRevocationReportReceived(pseudocert(pk(vpseudosk_4),gsk(vid_6,gmsk_5)),cert(vid_6,pk(vsk_3),cask_3))

{152}get revokedcerts(=vid_6): else branch taken {129}event RevokedVid(vid_6) {115}get revokedcerts(vid_6)

{106} event RevokedCannotGetGroupKey(vid_6)