$\sim X_1 = aenc((groupkey_request, sign(groupkey_request, \sim M_6), \sim M_7), \sim M$ = aenc((groupkey_request, sign(groupkey_request, attsk_5),cert(attvid_5,pk(attsk_5),cask_4)),pk(\sim M_12 = aenc(((groupkey_response,attvid_5,gsk(attvid_5,gmsk_4),gpk(gmsk_4)),sign((groupkey_response, attvid_5,gsk(attvid_5,gmsk_4),gpk(gmsk_4)),cask_4)), $\sim X_2 = aenc((pseudocert(a_6, 3-proj-4-tuple(1-proj-2-tuple($ A trace has been found. a_6,gsk(attvid_5,gmsk_4)),revoke_request),sign((pseudocert(a_6,gsk(attvid_5,gmsk_4)),revoke_request), attsk_6),cert(attvid_6,pk(attsk_6),cask_4)),pk(~X_3 = aenc(((pseudocert(a_8,3-proj-4-tuple(1-proj-2-tuple(adec(~M_12,~M_6)))),revoke_request),sign((pseudocert(a_8,3-proj-4-tuple(1-proj-2-tuple(adec(~M_12,~M_6)))),revoke_request),~M_3),~M_4),~M)
= aenc(((pseudocert(a_8,3-proj-4-tuple(1-proj-2-tuple(adec(~M_12,~M_6))))),revoke_request),~M_3),~M_4),~M) **Honest Process** Attacker {1}new gmsk_4 {2}new cask_4 \sim M = pk(cask_4) {5}new vid_7 Beginning of process CASecretKeyReveal {155}event CASKReveal(cask_4) {6}new vsk_3 \sim M_1 = cask_4 {91}new attvid_6 {91}new attvid_4 {91}new attvid_5 {92}new attsk_4 {92} new attsk_6 {92} new attsk_5 Beginning of process CARegister Beginning of process CARegister Beginning of process CARevoke Beginning of process CARevoke {95} event AttackerGetsEnrollmentCertificate(attvid 4, {95} event AttackerGetsEnrollmentCertificate(attvid_6, {95} event AttackerGetsEnrollmentCertificate(attvid_5 pk(attsk_4)) $(\sim M_2, \sim M_3, \sim M_4) = (attvid_4, attsk_4, cert(attvid_4, pk(attsk_4), cask_4))$ $(\sim M_5, \sim M_6, \sim M_7) = (attvid_5, attsk_5, cert(attvid_5, pk(attsk_5), cask_4))$ $(\sim M_8, \sim M_9, \sim M_10) = (attvid_6, attsk_6, cert(attvid_6, pk(attsk_6), cask_4))$ Beginning of process VehicleRegistration {14} event ValidGroupKeyRequestSent(vid_7) ~M_11 = aenc((groupkey_request,sign(groupkey_request, vsk_3),cert(vid_7,pk(vsk_3),cask_4)),pk(cask_4)) aenc((groupkey_request,a_3, \sim M_7), \sim M) = aenc((groupkey_request,a_3,cert(attvid_5,pk(attsk_5),cask_4)),pk(cask_4)) ~X 1 {115}get revokedcerts(=attvid_5): else branch taken {108}event ValidGroupKeyRequestReceived(cask_4, attvid_5) {113}event ValidGroupPrivateKeySent(attvid_5,gsk(attvid_5,gmsk_4),gpk(gmsk_4)) \sim M_12 {153}get revokedcerts(=attvid_6): else branch taken {126} event ValidRevocationReportReceived(pseudocert(a_6,gsk(attvid_5,gmsk_4)),cert(attvid_6,pk(attsk_6), {152}get revokedcerts(=attvid_5): else branch taken {129}event RevokedVid(attvid_5) ~X_3 {153}get revokedcerts(=attvid_4): else branch taken {126} event ValidRevocationReportReceived(pseudocert(a_8,gsk(attvid_5,gmsk_4)),cert(attvid_4,pk(attsk_4),cask_4)) {152}get revokedcerts(=attvid_5): else branch taken {129}event RevokedVid(attvid_5) {130}insert revokedcerts(attvid_5) {115}get revokedcerts(attvid_5) {106}event RevokedCannotGetGroupKey(attvid_5)

Abbreviations