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_3)),pk(~M_8 = aenc(((groupkey_response,attvid_3,gsk(attvid_3,gmsk_4),gpk(gmsk_4)),sign((groupkey_response,attvid_3,gsk(attvid_3,gsk(attvid_3,gsk(attvid_3,gsk(attvid_3,gsk(attvid_3)),cask_3)),pk(~M_9 = aenc(((groupkey_response,vid_7,gsk(vid_7,gmsk_4),gpk(gmsk_4)),sign((groupkey_response,vid_7,gsk(vid_7,gsk(vid_7,gmsk_4),gpk(gmsk_4)),cask_3)),pk(vsk_3)) \sim X_2 = (a_4,sign(a_4,a_5),pseudocert(pk(a_5),3-proj-4-tuple(1-proj- $\overline{2}$ -tuple(adec($\sim M_8$, $\sim M_2$))))) A trace has been found. $= (a_4, sign($ $a_4,a_5)$, pseudocert(pk(a_5), gsk(attvid_3, gmsk_4))) \sim M_10 = aenc(((pseudocert(pk(a_5),gsk(attvid_3, gmsk_4)),revoke_request),sign((pseudocert(pk(a_5), gsk(attvid_3,gmsk_4)),revoke_request),vsk_3),cert(vid_7,pk(vsk_3),cask_3)),pk(cask_3)) $\sim X_3 = aenc((pseudocert(a_7,3-proj-4-tuple(1-proj-2-tuple($ adec(~M_8,~M_2)))),revoke_request),sign((pseudocert(**Honest Process** Attacker {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 CARegister Beginning of process CARevoke 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) \sim M_7 = aenc((groupkey_request, sign(groupkey_request, vsk_3),cert(vid_7,pk(vsk_3),cask_3)),pk(cask_3)) ~X_1 {115}get revokedcerts(=attvid_3): else branch taken {108}event ValidGroupKeyRequestReceived(cask_3, attvid_3) {113}event ValidGroupPrivateKeySent(attvid_3,gsk(attvid_3,gmsk_4),gpk(gmsk_4)) ~M_7 = aenc((groupkey_request,sign(groupkey_request, vsk_3),cert(vid_7,pk(vsk_3),cask_3)),pk(cask_3)) {115}get revokedcerts(=vid_7): else branch taken {108} event ValidGroupKeyRequestReceived(cask_3, vid 7) {113}event ValidGroupPrivateKeySent(vid_7,gsk(vid_7,gmsk_4),gpk(gmsk_4)) \sim M_9 ~M 9 {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_3), pk(cask_3), gpk(gmsk_4)) {47} event RevocationAsked(vid_7,cert(vid_7,pk(vsk_3),cask_3),pseudocert(pk(a_5),gsk(attvid_3,gmsk_4))) \sim M₁₀ {153}get revokedcerts(=attvid_4): else branch taken {126} event ValidRevocationReportReceived(pseudocert(a_7,gsk(attvid_3,gmsk_4)),cert(attvid_4,pk(attsk_4),cask_3)) {152}get revokedcerts(=attvid_3): else branch taken {129}event RevokedVid(attvid_3) {130}insert revokedcerts(attvid_3) \sim M_10 {153}get revokedcerts(=vid_7): else branch taken {126}event ValidRevocationReportReceived(pseudocert(pk(a_5),gsk(attvid_3,gmsk_4)),cert(vid_7,pk(vsk_3),cask_3)) {152}get revokedcerts(attvid_3) {128}event AlreadyRevoked(attvid_3)