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))

A trace has been found.

~M_7 = aenc(((pseudocert(pk(a_3),gsk(attvid_2, gmsk_5)),revoke_request),sign((pseudocert(pk(a_3), gsk(attvid_2,gmsk_5)),revoke_request),vsk_3),cert(vid_6,pk(vsk_3),cask_3)),pk(cask_3))

Honest Process Attacker {1}new gmsk_5 {2}new cask_3 \sim M = pk(cask_3) {5}new vid_6 Beginning of process CAGroupMasterSecretKeyReveal {6}new vsk_3 {155}event CAGMSKReveal(gmsk_5) {91} new attvid_2 {92} new attsk_2 Beginning of process CARevoke {95} event AttackerGetsEnrollmentCertificate(attvid_2, pk(attsk_2)) \sim M_1 = gmsk_5 Beginning of process CARegister Beginning of process CARegister $(\sim M_2, \sim M_3, \sim M_4) = (attvid_2, attsk_2, cert(attvid_2, pk(attsk_2), cask_3))$ 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)) ~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, {113}event ValidGroupPrivateKeySent(vid_6,gsk(vid_6,gmsk_5),gpk(gmsk_5)) ~M 6 \sim M_6 {21} event ValidGroupPrivateKeyReceived(vid_6,gsk(vid_6,gmsk_5),gpk(gmsk_5)) Beginning of process VehicleReport(vid_6, vsk_3, cert(vid_6,pk(vsk_3),cask_3), pk(cask_3), gpk(gmsk_5)) $(a_2,sign(a_2,a_3),pseudocert(pk(a_3),gsk(\sim M_2, \sim M_1))) = (a_2,sign(a_2,a_3),pseudocert(pk(a_3), gsk(attvid_2,gmsk_5)))$ {47} event RevocationAsked(vid_6,cert(vid_6,pk(vsk_3),cask_3),pseudocert(pk(a_3),gsk(attvid_2,gmsk_5))) \sim M₂7 aenc((groupkey_request,a_5, \sim M_4), \sim M) = aenc((groupkey_request, a_5,cert(attvid_2,pk(attsk_2),cask_3)),pk(cask_3)) $\sim M_{-}7$ {153}get revokedcerts(=vid_6): else branch taken {126} event ValidRevocationReportReceived(pseudocert(pk(a_3),gsk(attvid_2,gmsk_5)),cert(vid_6,pk(vsk_3),cask_3)) {152}get revokedcerts(=attvid_2): else branch taken {129}event RevokedVid(attvid_2) {130}insert revokedcerts(attvid_2) {115}get revokedcerts(attvid_2) {106}event RevokedCannotGetGroupKey(attvid_2)