Abbreviations ~M_3 = aenc(((groupkey_response,vid_7,gsk(vid_7,gmsk_5),gpk(gmsk_5)),sign((groupkey_response,vid_7,gsk(vid_7,gsk(vid_7,gsk(vid_7,gsk(vid_7,gmsk_5)),gpk(gmsk_5)),cask_3)),pk(vsk_3)) **Honest Process** Attacker {1}new gmsk_5 {2}new cask_3 \sim M = pk(cask_3) Beginning of process CAGroupMasterSecretKeyReveal {155}event CAGMSKReveal(gmsk_5) \sim M_1 = gmsk_5 ~M_2 = aenc((groupkey_request,sign(groupkey_request, vsk_3),cert(vid_7,pk(vsk_3),cask_3)),pk(cask_3)) ~M_2 = 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_5),gpk(gmsk_5)) **∼**M 3 $(a_1,sign(a_1,a_2),pseudocert(pk(a_2),gsk(a_3, \sim M_1))) = (a_1,sign(a_1,a_2),pseudocert(pk(a_2), gsk(a_3,gmsk_5)))$

{5}new vid_7

{6}new vsk_3

Beginning of process VehicleRegistration

{14} event ValidGroupKeyRequestSent(vid_7)

{21} event ValidGroupPrivateKeyReceived(vid_7,gsk(vid_7,gmsk_5),gpk(gmsk_5))

Beginning of process VehicleReceiveMessage(vid_7, gpk(gmsk_5))

{37} event ValidMessageReceived(vid_7,a_1)

Beginning of process CARegister

∼M 3

A trace has been found.