Abbreviations
~X_1 = aenc((groupkey_request,sign(groupkey_request,~M_8),~M_9),~M) = aenc((groupkey_request,sign(groupkey_request,attsk_7),cert(attvid_7,pk(attsk_7),cask_3)),pk(cask_3))
~M_14 = aenc(((groupkey_response,attvid_7,gsk(attvid_7,gmsk_4),gpk(gmsk_4)),sign((groupkey_response,attvid_7,gsk(attvid_7,gmsk_4),gpk(gmsk_4)),cask_3)),pk(attsk_7))
~X_2 = aenc((groupkey_request,sign(groupkey_request,~M_5),~M_6),~M) = aenc((groupkey_request,sign(groupkey_request,attsk_6),cert(attvid_6,pk(attsk_6),cask_3)),pk(cask_3))
~M_15 = aenc(((groupkey_response,attvid_6,gsk(attvid_6,gmsk_4),gpk(gmsk_4)),sign((groupkey_response,attvid_6,gsk(attvid_6,gmsk_4),gpk(gmsk_4)),cask_3)),pk(attsk_6))
~X_3 = aenc((groupkey_request,sign(groupkey_request,~M_2),~M_3),~M) = aenc((groupkey_request,sign(groupkey_request,attsk_5),cert(attvid_5,pk(attsk_5),cask_3)),pk(cask_3))
~M_16 = 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_3)),pk(attsk_5))
~M_17 = aenc(((groupkey_response,vid_7,gsk(vid_7,gmsk_4),gpk(gmsk_4)),sign((groupkey_response,vid_7,gsk(vid_7,gmsk_4),gpk(gmsk_4)),cask_3)),pk(vsk_4))
~X_4 = ((groupkey_response,~M_4,3-proj-4-tuple(1-proj-2-tuple(adec(~M_15,~M_5))),4-proj-4-tuple(1-proj-2-tuple(adec(~M_14,~M_8))),2-proj-2-tuple(adec(~M_15,~M_5)),pseudocert(~M_3-proj-4-tuple(1-proj-2-tuple(adec(~M_16,~M_2))))) = ((groupkey_response,attvid_6,gsk(attvid_6,gmsk_4),gpk(gmsk_4)),sign((groupkey_response,attvid_6,gsk(attvid_6,gmsk_4),gpk(gmsk_4)),cask_3),pseudocert(pk(cask_3),gsk(attvid_5,gmsk_4)))
~M_18 = aenc(((pseudocert(pk(cask_3),gsk(attvid_5,gmsk_4)),revoke_request),sign((pseudocert(pk(cask_3),gsk(attvid_5,gmsk_4)),revoke_request),vsk_4),cert(vid_7,pk(vsk_4),cask_3)),pk(cask_3))
~X_5 = aenc(((pseudocert(a_12,3-proj-4-tuple(1-proj-2-tuple(adec(~M_16,~M_2)))),revoke_request),sign((pseudocert(a_12,3-proj-4-tuple(1-proj-2-tuple(adec(~M_16,~M_2)))),revoke_request),~M_11),~M_12),~M) = aenc(((pseudocert(a_12,gsk(attvid_5,gmsk_4)),revoke_request),sign((pseudocert(a_12,gsk(attvid_5,gmsk_4)),revoke_request),attsk_8),cert(attvid_8,pk(attsk_8),cask_3)),pk(cask_3))

A trace has been found.

Honest Process

Attacker

{1}new gmsk_4

{2}new cask_3

~M = pk(cask_3)

{6}new vid_7

{7}new vsk_4

{92}new attvid_8

{93}new attsk_8

{96}event AttackerGetsEnrollmentCertificate(attvid_8, pk(attsk_8))

{92}new attvid_7

{93}new attsk_7

{96}event AttackerGetsEnrollmentCertificate(attvid_7, pk(attsk_7))

{92}new attvid_6

{93}new attsk_6

{96}event AttackerGetsEnrollmentCertificate(attvid_6, pk(attsk_6))

{92}new attvid_5

{93}new attsk_5

{96}event AttackerGetsEnrollmentCertificate(attvid_5, pk(attsk_5))

Beginning of process CA

Beginning of process CA

Beginning of process CA

Beginning of process CA

Beginning of process CA

Beginning of process CARevoke

Beginning of process CARevoke

(~M_1,~M_2,~M_3) = (attvid_5,attsk_5,cert(attvid_5, pk(attsk_5),cask_3))

(~M_4,~M_5,~M_6) = (attvid_6,attsk_6,cert(attvid_6, pk(attsk_6),cask_3))

(~M_7,~M_8,~M_9) = (attvid_7,attsk_7,cert(attvid_7, pk(attsk_7),cask_3))

(~M_10,~M_11,~M_12) = (attvid_8,attsk_8,cert(attvid_8, pk(attsk_8),cask_3))

Beginning of process Vehicle

{15}event ValidGroupKeyRequestSent(vid_7)

~M_13 = aenc((groupkey_request,sign(groupkey_request, vsk_4),cert(vid_7,pk(vsk_4),cask_3)),pk(cask_3))

aenc((groupkey_request,a_5,~M_3),~M) = aenc((groupkey_request, a_5,cert(attvid_5,pk(attsk_5),cask_3)),pk(cask_3))

~X_1

{116}get revokedcerts(=attvid_7): else branch taken

{109}event ValidGroupKeyRequestReceived(cask_3, attvid_7)

{114}event ValidGroupPrivateKeySent(attvid_7,gsk(attvid_7,gmsk_4),gpk(gmsk_4))

~M_14

~X_2

{116}get revokedcerts(=attvid_6): else branch taken

{109}event ValidGroupKeyRequestReceived(cask_3, attvid_6)

{114}event ValidGroupPrivateKeySent(attvid_6,gsk(attvid_6,gmsk_4),gpk(gmsk_4))

~M_15

~X_3

{116}get revokedcerts(=attvid_5): else branch taken

{109}event ValidGroupKeyRequestReceived(cask_3, attvid_5)

{114}event ValidGroupPrivateKeySent(attvid_5,gsk(attvid_5,gmsk_4),gpk(gmsk_4))

~M_16

~M_13 = aenc((groupkey_request,sign(groupkey_request, vsk_4),cert(vid_7,pk(vsk_4),cask_3)),pk(cask_3))

{116}get revokedcerts(=vid_7): else branch taken

{109}event ValidGroupKeyRequestReceived(cask_3, vid_7)

{114}event ValidGroupPrivateKeySent(vid_7,gsk(vid_7,gmsk_4),gpk(gmsk_4))

~M_17

~M_17

{22}event ValidGroupPrivateKeyReceived(vid_7,gsk(vid_7,gmsk_4),gpk(gmsk_4))

Beginning of process VehicleReport(vid_7, vsk_4, cert(vid_7,pk(vsk_4),cask_3), pk(cask_3), gpk(gmsk_4))

~X_4

{48}event RevocationAsked(vid_7,cert(vid_7,pk(vsk_4),cask_3),pseudocert(pk(cask_3),gsk(attvid_5,gmsk_4)))

~M_18

~X_5

{154}get revokedcerts(=attvid_8): else branch taken

{127}event ValidRevocationReportReceived(pseudocert(a_12,gsk(attvid_5,gmsk_4)),cert(attvid_8,pk(attsk_8),cask_3))

{153}get revokedcerts(=attvid_5): else branch taken

{130}event RevokedVid(attvid_5)

~M_18

{154}get revokedcerts(=vid_7): else branch taken

{127}event ValidRevocationReportReceived(pseudocert(pk(cask_3),gsk(attvid_5,gmsk_4)),cert(vid_7,pk(vsk_4),cask_3))

{153}get revokedcerts(=attvid_5): else branch taken

{130}event RevokedVid(attvid_5)

{131}insert revokedcerts(attvid_5)

{116}get revokedcerts(attvid_5)

{107}event RevokedCannotGetGroupKey(attvid_5)