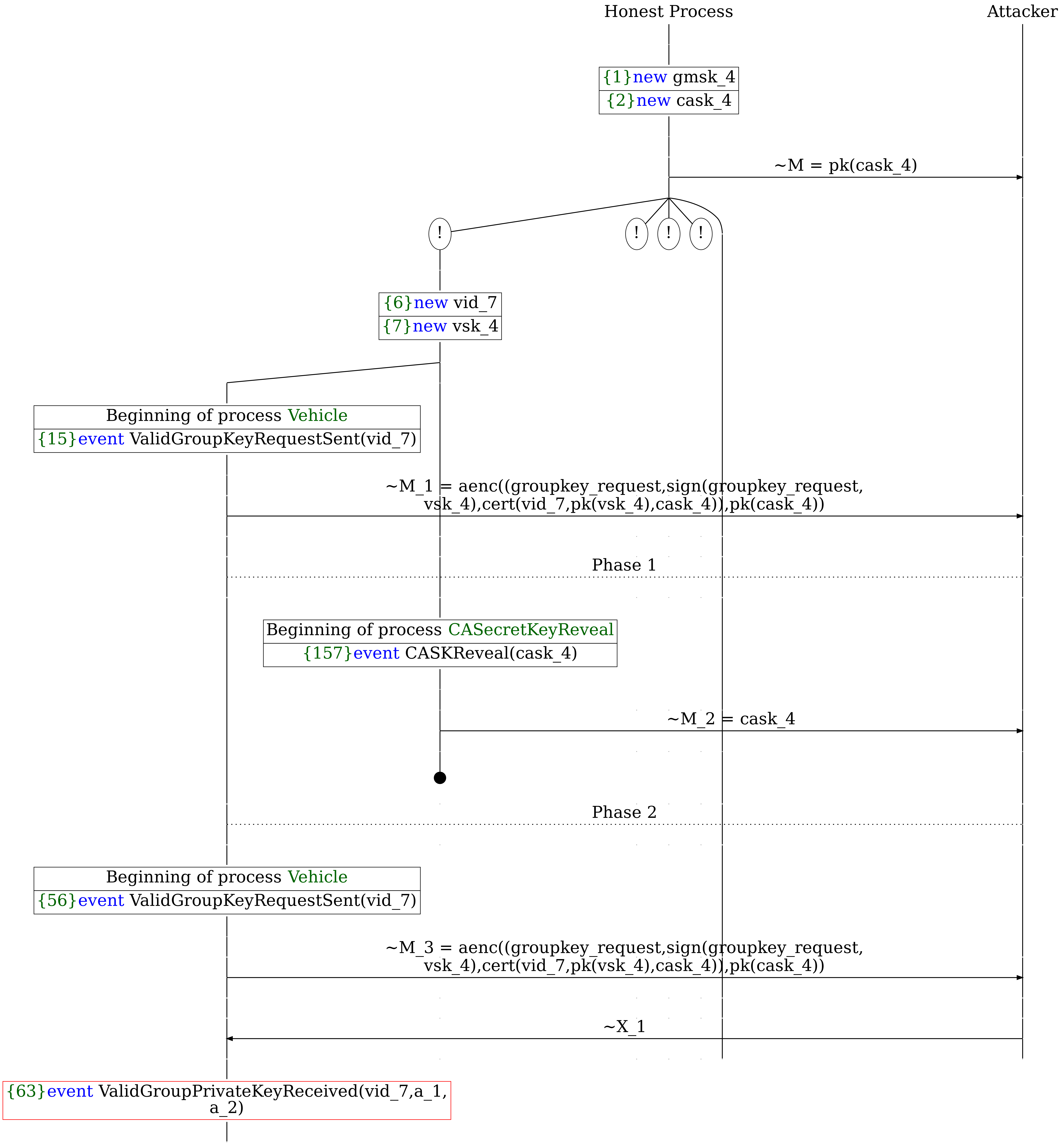
A trace has been found.

Abbreviations

~X_1 = aenc(((groupkey_response,getid(3-proj-3-tuple(adec(~M_1,~M_2))),a_1,a_2),sign((groupkey_response,getid(3-proj-3-tuple(adec(~M_1,~M_2))),a_1,a_2),~M_2)),getpk(3-proj-3-tuple(adec(~M_1,~M_2))))
=
aenc(((groupkey_response,vid_7,a_1,a_2),sign((groupkey_response,vid_7,a_1,a_2),cask_4)),pk(vsk_4))


Honest Process
Attacker
{1}new gmsk_4
{2}new cask_4
~M = pk(cask_4)
!
!
!
!
{6}new vid_7
{7}new vsk_4
Beginning of process Vehicle
{15}event ValidGroupKeyRequestSent(vid_7)
~M_1 = aenc((groupkey_request,sign(groupkey_request,vsk_4),cert(vid_7,pk(vsk_4),cask_4)),pk(cask_4))
Phase 1
Beginning of process CASecretKeyReveal
{157}event CASKReveal(cask_4)
~M_2 = cask_4
Phase 2
Beginning of process Vehicle
{56}event ValidGroupKeyRequestSent(vid_7)
~M_3 = aenc((groupkey_request,sign(groupkey_request,vsk_4),cert(vid_7,pk(vsk_4),cask_4)),pk(cask_4))
~X_1
{63}event ValidGroupPrivateKeyReceived(vid_7,a_1,a_2)