Abbreviations

~M_6 = aenc(((groupkey_response,vid_8,gsk(vid_8,gmsk_5),gpk(gmsk_5)),sign((groupkey_response,vid_8,gsk(vid_8,gsk(vid_8,gmsk_5)),cask_4)),pk(vsk_3))

gsk(vid_o,ginsk_3),gpk(ginsk_3)),cdsk_4)),pk(vsk_3))

~M_13 = aenc(((pseudocert(pk(vpseudosk_3),gsk(vid_8,gmsk_5)),revoke_request),sign((pseudocert(pk(vpseudosk_3),gsk(vid_8,gmsk_5)),revoke_request),vsk_3),cert(vid_8,pk(vsk_3),cask_4)),pk(cask_4))

~X_1 = aenc((groupkey_request,sign(groupkey_request,~M_3),~M_4),~M)

A trace has been found.

