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)),gpk(gmsk_5)),cask_3)),pk(vsk_3))

-M_16 = aenc(((pseudocert(pk(vpseudosk_4),gsk(vid_6,gmsk_5)),revoke_request),sign((pseudocert(pk(vpseudosert(pk(vpseudosert(pk(vpseudosert(pk(vpseudosk_4),gsk(vid_6,gmsk_5)),revoke_request),vsk_3),cert(vid_6,pk(vsk_3),cask_3)),pk(cask_3))

-X_1 = aenc(((-M_15,revoke_request),sign((-M_15,revoke_request),-M_3),-M_4),-M)

= aenc(((pseudocert(pk(vpseudosk_5),gsk(vid_6,gmsk_5)),revoke_request),gsign((pseudocert(pk(vpseudosert(pk(v

