Abbreviations

~M\_6 = aenc(((groupkey\_response,vid\_7,gsk(vid\_7,gmsk\_6),gpk(gmsk\_6)),sign((groupkey\_response,vid\_7,gsk(vid\_7,gsk(vid\_7,gmsk\_6),gpk(gmsk\_6)),cask\_3)),pk(vsk\_3))

~M\_7 = aenc(((pseudocert(pk(a\_3),gsk(a\_4,gmsk\_6)), revoke\_request),sign((pseudocert(pk(a\_3),gsk(a\_4, gmsk\_6)),revoke\_request),vsk\_3),cert(vid\_7,pk( vsk\_3),cask\_3)),pk(cask\_3))

 $VSK_3$ ),  $CaSK_3$ ),  $PK(CaSK_3)$ )  $\sim X_1 = aenc((groupkey\_request, sign(groupkey\_request, \sim M_3), \sim M_4), \sim M$ 

~M\_4),~M)
= aenc((groupkey\_request,sign(groupkey\_request,attsk\_2),cert(attvid\_2,pk(attsk\_2),cask\_3)),pk(cask\_3))

A trace has been found.

