Abbreviations

~X\_1 = aenc((groupkey\_request,sign(groupkey\_request,~M\_2), ~M\_3),~M)

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

~M\_5 = aenc(((groupkey\_response,attvid\_2,gsk(attvid\_2,gmsk\_5),gpk(gmsk\_5)),sign((groupkey\_response,attvid\_2,gsk(attvid\_2,gmsk\_5),gpk(gmsk\_5)),cask\_3)),pk( attsk\_2))

~M\_6 = aenc(((groupkey\_response,vid\_7,gsk(vid\_7,gmsk\_5),gsk(gmsk\_5)),sign((groupkey\_response,vid\_7,gsk(vid\_7,gmsk\_5),gpk(gmsk\_5)),cask\_3)),pk( attsk\_2))

~M\_6 = aenc(((groupkey\_response,vid\_7,gsk(vid\_7,gmsk\_5),gsk(gmsk\_5)),cask\_3)),pk(vsk\_4))

~X\_2 = (a\_4,sign(a\_4,a\_5),pseudocert(pk(a\_5),3-proj-4-tuple(1-proj-2-tuple(adec(~M\_5,~M\_2)))))

= (a\_4,sign(a\_4,a\_5),pseudocert(pk(a\_5),gsk(attvid\_2,gmsk\_5)))

