

Abbreviations	
~M_2 =	choice [aenc((groupkey request,sign(groupkey request, vsk 13),cert(vid 43,pk(vsk 13),cask 10)),pk(cask 10)), aenc((groupkey request,sign(groupkey request,vsk 12), cert(vid 42,pk(vsk 12),cask 11)),pk(cask 11))]
~X_1 = (~M_3,~M_4,~M_5) =	choice [(attvid 11,attsk 11, cert(attvid 11,pk(attsk 11),cask 10)),(attvid 10, attsk 10,cert(attvid 10,pk(attsk 10),cask 11))]
~M_7 =	choice [aenc((groupkey request,sign(groupkey request, vsk 15),cert(vid 45,pk(vsk 15),cask 10)),pk(cask 10)), aenc((groupkey request,sign(groupkey request,vsk 14), cert(vid 44,pk(vsk 14),cask 11)),pk(cask 11))]
~M_8 =	choice [aenc(((groupkey response,vid 43, gsk(vid 43,gmsk 10),gpk(gmsk 10)),sign((groupkey response, vid 43,gsk(vid 43,gmsk 10),gpk(gmsk 10)),cask 10)), pk(vsk 13)),aenc(((groupkey response,vid 42,gsk(vid 42,gmsk 11),gpk(gmsk 11)),sign((groupkey response, vid 42,gsk(vid 42,gmsk 11),gpk(gmsk 11)),cask 11)), pk(vsk 12))]

