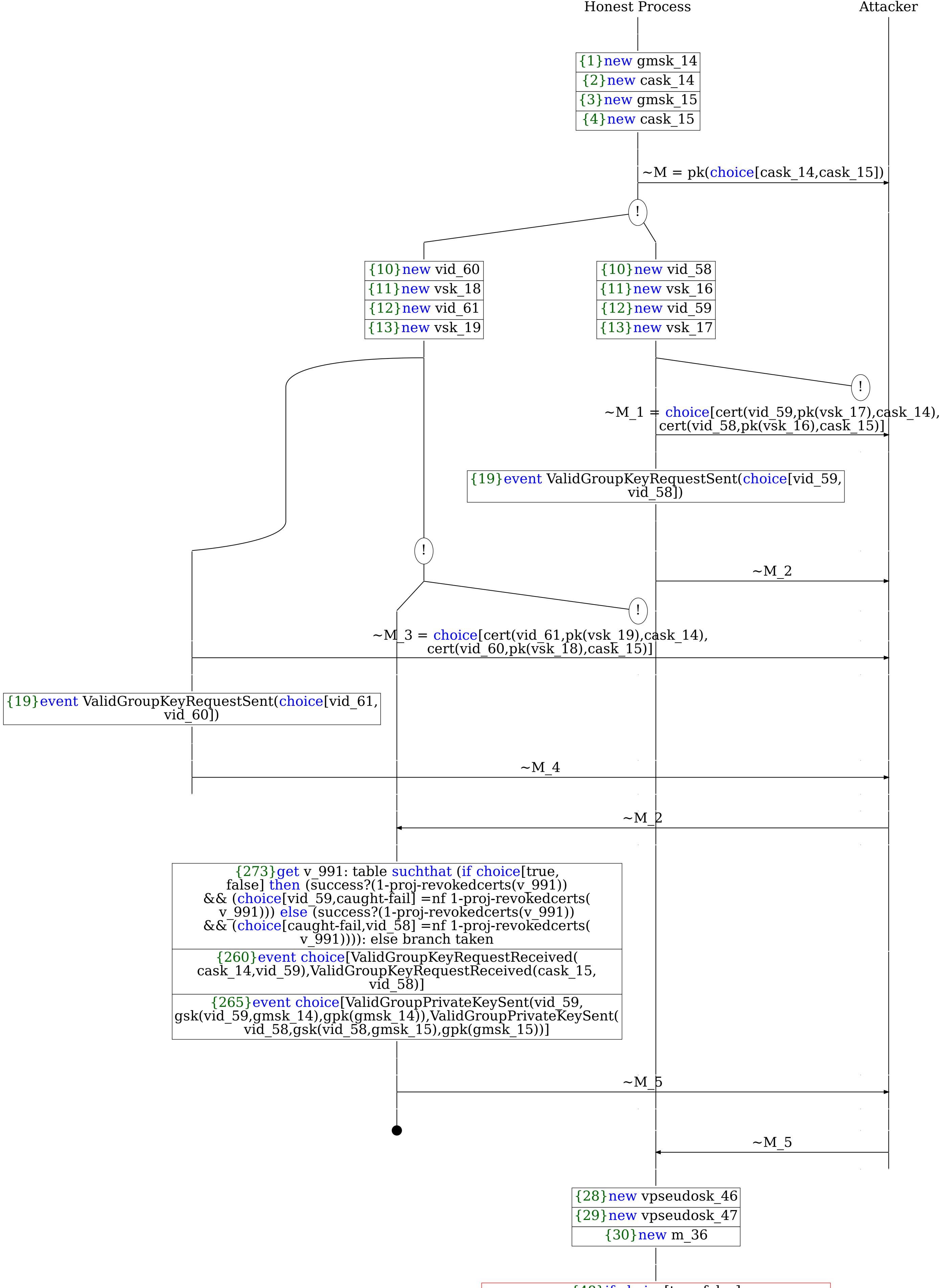
Abbreviations

~M\_2 = choice[aenc((groupkey\_request, sign(groupkey\_request, vsk\_17), cert(vid\_59, pk(vsk\_17), cask\_14)), pk(cask\_14)), aenc((groupkey\_request, sign(groupkey\_request, vsk\_16), cert(vid\_58, pk(vsk\_16), cask\_15)), pk(cask\_15))]

~M\_4 = choice[aenc((groupkey\_request, sign(groupkey\_request, vsk\_19), cert(vid\_61, pk(vsk\_19), cask\_14)), pk(cask\_14)), aenc((groupkey\_request, sign(groupkey\_request, vsk\_18), cert(vid\_60, pk(vsk\_18), cask\_15)), pk(cask\_15))]

~M\_5 = choice[aenc(((groupkey\_response, vid\_59, gsk(vid\_59, gmsk\_14), gpk(gmsk\_14)), sign((groupkey\_response, vid\_59, gsk(vid\_59, gmsk\_14), gpk(gmsk\_14)), cask\_14)), pk(vsk\_17)), aenc(((groupkey\_response, vid\_58, gmsk\_15), gpk(gmsk\_15)), sign((groupkey\_response, vid\_58, gsk(vid\_58, gmsk\_15), gpk(gmsk\_15)), cask\_15)), pk(vsk\_16))]

A trace has been found.



{48} if choice[true,false]
This process performs a test that may succeed on one side and not on the other.