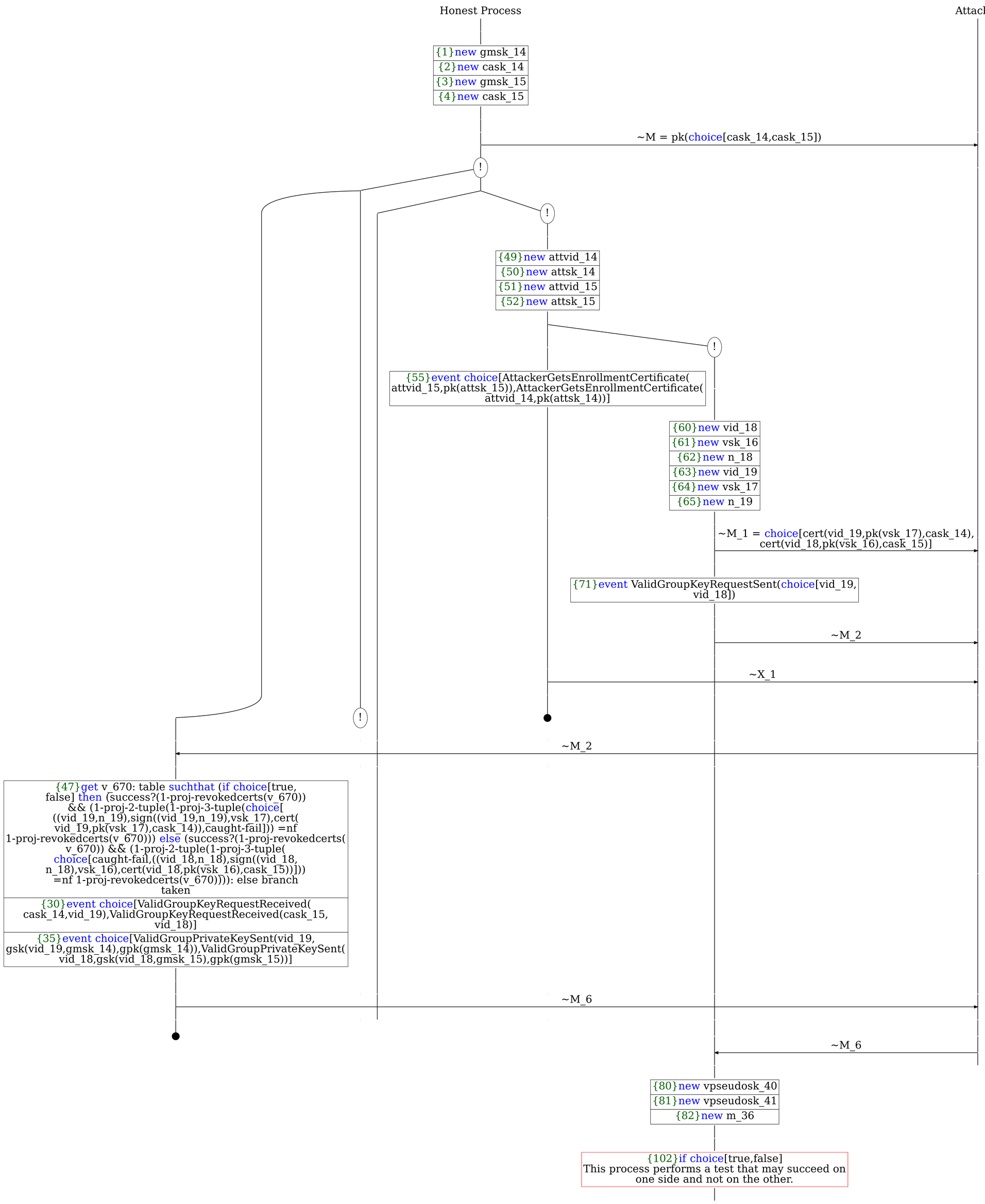
| Abbreviations |
| --- |
| ~M_2 = choice[aenc(((vid_19,n_19),sign((vid_19, n_19),vsk_17),cert(vid_19,pk(vsk_17),cask_14)), pk(cask_14)),aenc(((vid_18,n_18),sign((vid_18, n_18),vsk_16),cert(vid_18,pk(vsk_16),cask_15)), pk(cask_15))] |
| ~X_1 = (~M_3,~M_4,~M_5) = choice[(attvid_15,attsk_15, cert(attvid_15,pk(attsk_15),cask_14)),(attvid_14, attsk_14,cert(attvid_14,pk(attsk_14),cask_15))] |
| ~M_6 = choice[aenc(((groupkey_response,vid_19, n_19,gsk(vid_19,gmsk_14),gpk(gmsk_14)),sign((groupkey_response, vid_19,n_19,gsk(vid_19,gmsk_14),gpk(gmsk_14)), cask_14)),pk(vsk_17)),aenc(((groupkey_response, vid_18,n_18,gsk(vid_18,gmsk_15),gpk(gmsk_15)), sign((groupkey_response,vid_18,n_18,gsk(vid_18, gmsk_15),gpk(gmsk_15)),cask_15)),pk(vsk_16))] |

A trace has been found.