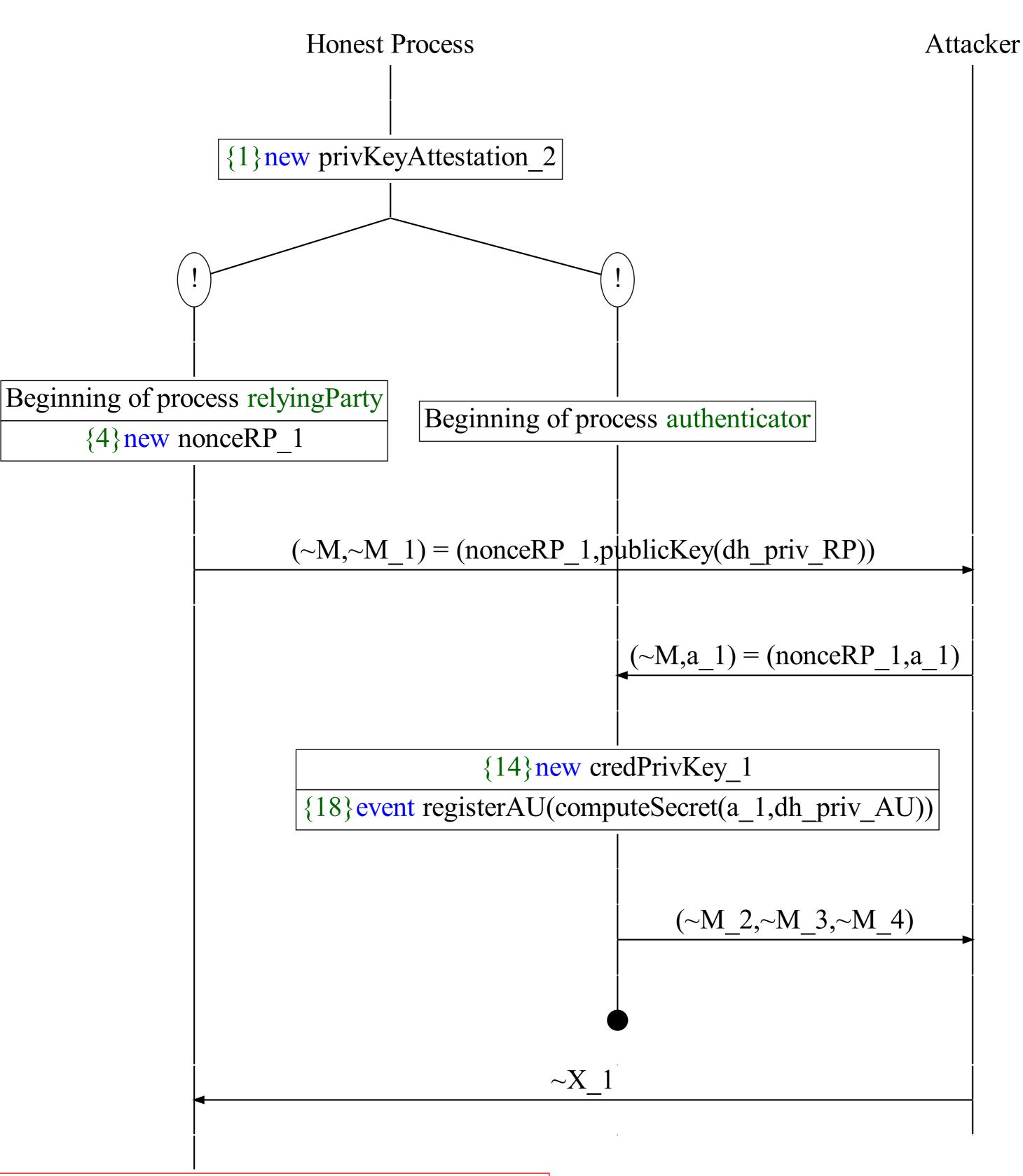
Abbreviations
\sim M_2 = vk(credPrivKey_1)
~M_3 = publicKey(dh_priv_AU)
\sim M_4 = sign((nonceRP_1,vk(credPrivKey_1),publicKey(
dh_priv_AU)),privKeyAttestation_2)
$\sim X_1 = (a_3, \sim M_2, \sim M_3, \sim M_4) = (a_3, vk(credPrivKey_1),$
<pre>publicKey(dh_priv_AU),sign((nonceRP_1,vk(credPrivKey_1),</pre>

publicKey(dh_priv_AU)),privKeyAttestation_2))

A trace has been found.



{10} event registerRP(computeSecret(publicKey(dh_priv_AU), dh_priv_RP))