A trace has been found.

Abbreviations
~M_2 = vk(credPrivKey_1)
~M_3 = exp(g,dh_priv_AU)
~M_4 = sign((nonceRP_1,vk(credPrivKey_1),exp(g,dh_priv_AU)), privKeyAttestation_2)
~X_1 = (a_3,~M_2,~M_3,~M_4) = (a_3,vk(credPrivKey_1), exp(g,dh_priv_AU),sign((nonceRP_1,vk(credPrivKey_1), exp(g,dh_priv_AU)),privKeyAttestation_2))