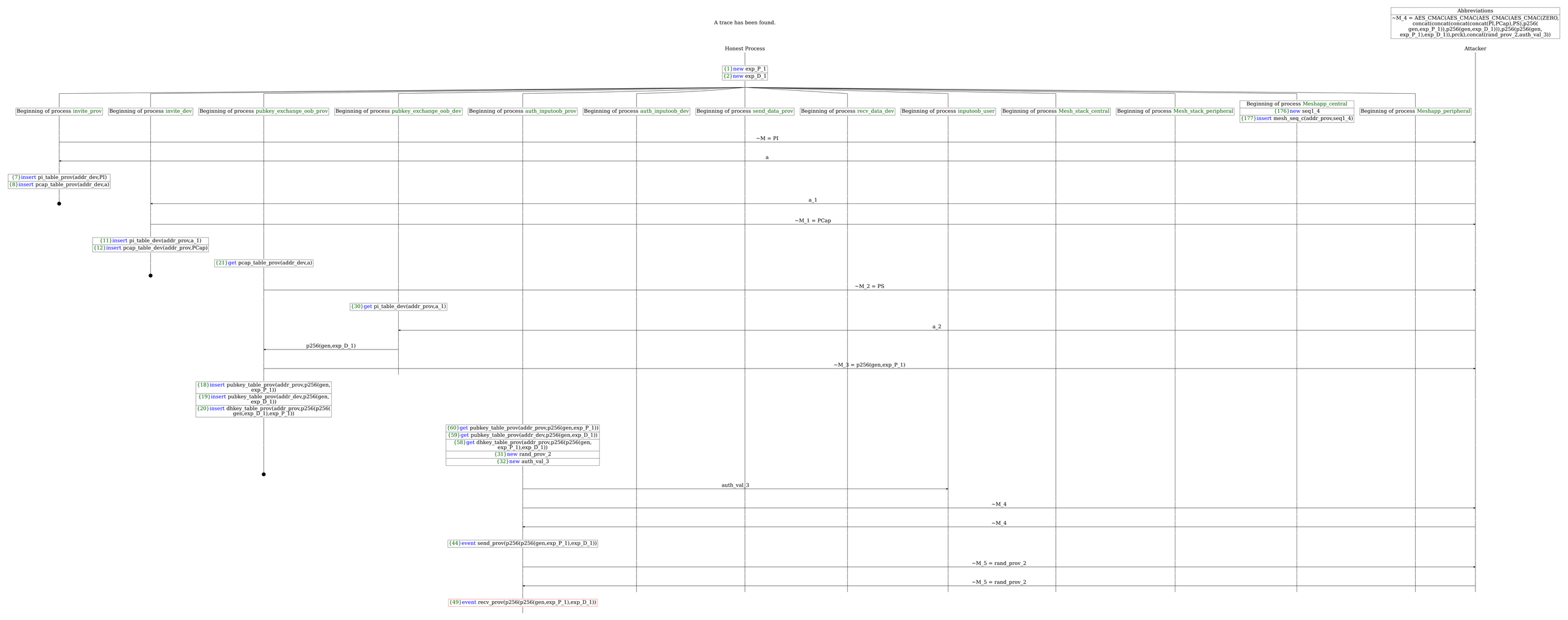
Abbreviations
~M_4 = AES_CMAC(AES_CMAC(AES_CMAC(ZERO, concat(concat(concat(concat(PI,PCap),PS),p256(gen,exp_P_1)),p256(gen,exp_D_1))),p256(p256(gen,exp_P_1),exp_D_1)),prck),concat(rand_prov_2,auth_val_3))
A trace has been found.
Honest Process
Attacker
{1}new exp_P_1
{2}new exp_D_1
Beginning of process invite_prov
Beginning of process invite_dev
Beginning of process pubkey_exchange_oob_prov
Beginning of process pubkey_exchange_oob_dev
Beginning of process auth_inputoob_prov
Beginning of process auth_inputoob_dev
Beginning of process send_data_prov
Beginning of process recv_data_dev
Beginning of process inputoob_user
Beginning of process Mesh_stack_central
Beginning of process Mesh_stack_peripheral
Beginning of process Meshapp_central
{176}new seq1_4
{177}insert mesh_seq_c(addr_prov,seq1_4)
Beginning of process Meshapp_peripheral
~M = PI
a
{7}insert pi_table_prov(addr_dev,PI)
{8}insert pcap_table_prov(addr_dev,a)
a_1
~M_1 = PCap
{11}insert pi_table_dev(addr_prov,a_1)
{12}insert pcap_table_dev(addr_prov,PCap)
{21}get pcap_table_prov(addr_dev,a)
~M_2 = PS
{30}get pi_table_dev(addr_prov,a_1)
a_2
p256(gen,exp_D_1)
~M_3 = p256(gen,exp_P_1)
{18}insert pubkey_table_prov(addr_prov,p256(gen,exp_P_1))
{19}insert pubkey_table_prov(addr_dev,p256(gen,exp_D_1))
{20}insert dhkey_table_prov(addr_prov,p256(p256(gen,exp_D_1),exp_P_1))
{60}get pubkey_table_prov(addr_prov,p256(gen,exp_P_1))
{59}get pubkey_table_prov(addr_dev,p256(gen,exp_D_1))
{58}get dhkey_table_prov(addr_prov,p256(p256(gen,exp_P_1),exp_D_1))
{31}new rand_prov_2
{32}new auth_val_3
auth_val_3
~M_4
~M_4
{44}event send_prov(p256(p256(gen,exp_P_1),exp_D_1))
~M_5 = rand_prov_2
~M_5 = rand_prov_2
{49}event recv_prov(p256(p256(gen,exp_P_1),exp_D_1))