Abbreviations

~M_4 = AES_CMAC(AES_CMAC(AES_CMAC(ZERO, 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,zero))

Attacker **Honest Process** {1}new exp_P_1 {2}new exp_D_1 Beginning of process invite_prov Beginning of process auth_staticoob_prov Beginning of process auth_staticoob_dev Beginning of process auth_staticoob_dev Beginning of process auth_staticoob_prov Beginning of process auth_staticoob_dev Beginning o \sim M = PI {7}insert pi_table_prov(addr_dev,PI)
{8}insert pcap_table_prov(addr_dev,a) \sim 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) \sim M_2 = PS {30} get pi_table_dev(addr_prov,a_1) $p256(gen,exp_D_1)$ $\sim M_3 = p256(gen, exp_P_1)$ {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)) {57} get pubkey_table_prov(addr_prov,p256(gen,exp_P_1))
{56} get pubkey_table_prov(addr_dev,p256(gen,exp_D_1))
{55} get dhkey_table_prov(addr_prov,p256(p256(gen,exp_P_1),exp_D_1)) {32}new rand_prov_2 \sim M_4 \sim M_4 $[42] \frac{1}{\text{event send_prov}} (p256(p256(gen, exp_P_1), exp_D_1))$ \sim M_5 = rand_prov_2 \sim M_5 = rand_prov_2

 $\{46\}$ event recv_prov(p256(p256(gen,exp_P_1),exp_D_1))