Abbreviations

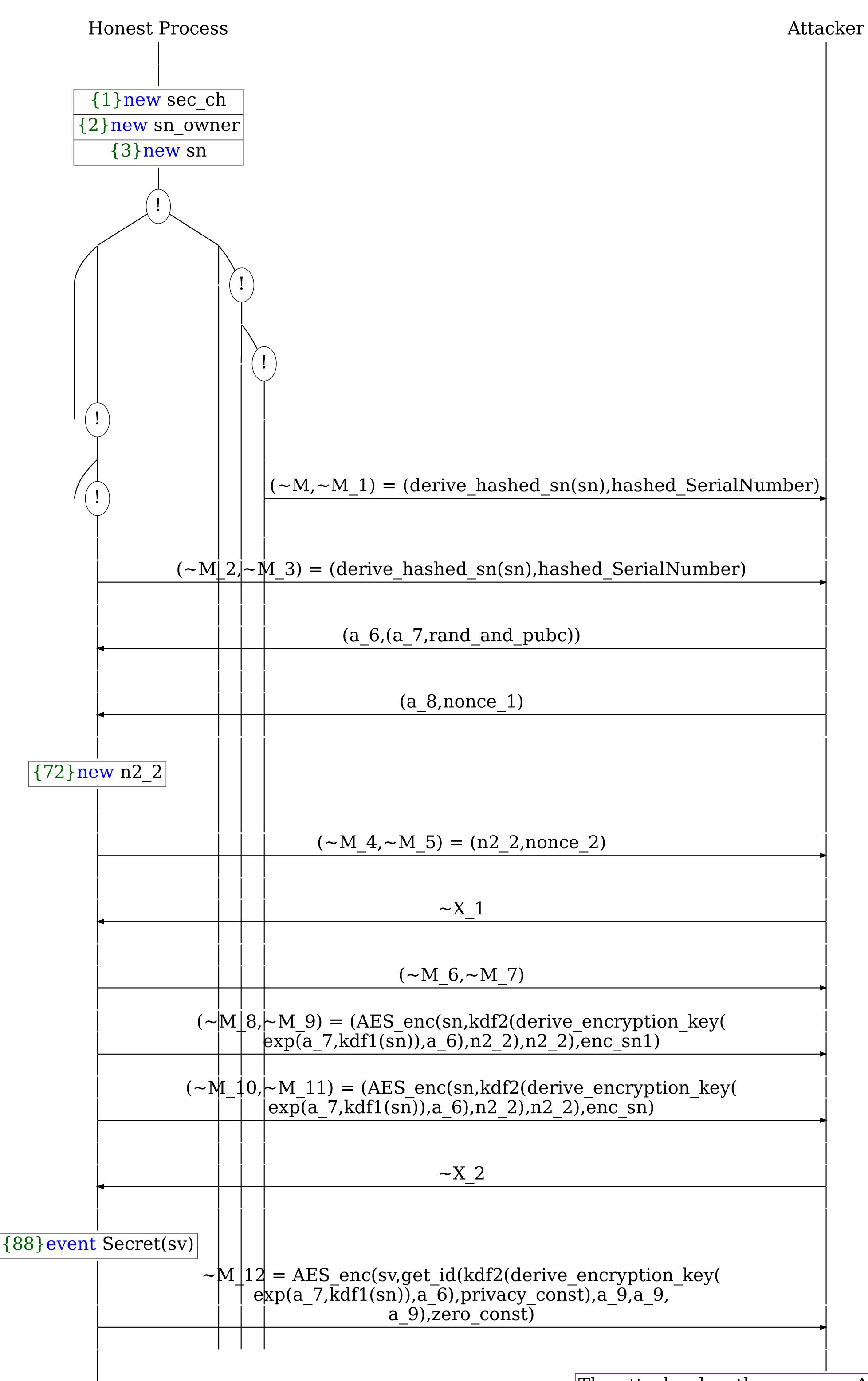
 \sim X_1 = (AES_enc(smartthings_const,kdf2(derive_encryption_key(exp(a_7,kdf1(hash_table(\sim M))),a_6),bleAuthentication_const), \sim M_4),enc_nonce_1) = (AES_enc(smartthings_const,

= (AES_enc(smartthings_const, kdf2(derive_encryption_key(exp(a_7,kdf1(sn)),a_6), bleAuthentication const),n2_2),enc_nonce_1)

 \sim M 7 = enc nonce 2

 \sim X_2 = (AES_enc(a_9,kdf2(derive_encryption_key(exp(a_7, kdf1(hash_table(\sim M))),a_6), \sim M_4), \sim M_4),enc_params)

(AES_enc(a_9,kdf2(derive_encryption_key(exp(a_7,kdf1(sn)),a_6),n2_2),n2_2),enc_params)



A trace has been found.

The attacker has the message AES_dec(~M_12,get_id(kdf2(derive_encryption_key(exp(a_7,kdf1(hash_table(~M))),a_6),privacy_const),a_9,a_9,a_9),zero_const)