Abbreviations \sim M_84059 = non_confirmable \sim M 84060 = CoAP POSTCode ~M 84061 = messageid 82688 \sim M 84062 = token 82681 \sim M 84065 = partial iv 82685 \sim M_84066 = IDri_82682 \sim M 84067 = idcontext 82684 \sim M_84064 = aeadEncrypt(HKDF(msecret_82686,msalt_82687, (IDri_82682,idcontext_82684,AES_CCM,label_key, alg key length(AES CCM,label key))),aeadNonce(IDri 82682, partial iv 82685, HKDF (msecret 82686, msalt_82687,(emptyId,idcontext_82684,AES_CCM,label_iv, alg_key_length(AES_CCM,label_iv)))),((CoAP_GETCode, isLightBulbTurnedOn),msg1(a_82669,a_82670)),(encrypt0, oscore_version_one,AES_CCM,IDri_82682,partial_iv_82685)) $\sim X_1 = (a_82679, a_82678, a_82677, a_82676, (\sim M_84065, \sim M_83843, \sim M_84065, \sim M_840$ ~M 83844),~M 84064) = (a 82679,a 82678,a 82677, a_82676,(partial_iv_82685,IDri_82682,idcontext_82684), aeadEncrypt(HKDF(msecret_82686,msalt_82687,(IDri_82682, idcontext 82684,AES_CCM,label_key,alg_key_length(AES_CCM,label_key))),aeadNonce(IDri_82682,partial_iv_82685, HKDF(msecret_82686,msalt_82687,(emptyId,idcontext_82684, AES_CCM,label_iv,alg_key_length(AES_CCM,label_iv)))), ((CoAP_GETCode,isLightBulbTurnedOn),msg1(a_82669, a 82670)),(encrypt0,oscore version one,AES CCM, IDri 82682, partial iv 82685))) \sim M 84302 = non confirmable ~M 84303 = CoAP CHANGEDCode \sim M 84304 = responseId 82731 A trace has been found. \sim M 84305 = a 82676 \sim M 84306 = empty ~M 84307 = aeadEncrypt(HKDF(msecret 82686,msalt 82687, (IDir_82683,idcontext_82684,AES_CCM,label_key, alg_key_length(AES_CCM,label_key))),aeadNonce(IDri 82682, partial iv 82685, HKDF (msecret 82686, msalt_82687,(emptyId,idcontext_82684,AES_CCM,label_iv, alg_key_length(AES_CCM,label_iv)))),((CoAP_CONTENTCode, bounded by((CoAP GETCode, is LightBulbTurnedOn))), msg2(a_82670,a_82669)),(encrypt0,oscore_version_one, AES CCM,IDri 82682,partial iv 82685)) \sim X 2 = (\sim M 84062,a 82673,a 82674,a 82675,empty, \sim M 84307) (token_82681,a_82673,a_82674,a_82675,empty,aeadEncrypt(HKDF(msecret_82686,msalt_82687,(IDir_82683,idcontext_82684, AES_CCM,label_key,alg_key_length(AES_CCM,label_key))), aeadNonce(IDri 82682, partial iv 82685, HKDF (msecret 82686, msalt_82687,(emptyId,idcontext_82684,AES_CCM,label_iv, alg_key_length(AES_CCM,label_iv)))),((CoAP_CONTENTCode, bounded_by((CoAP_GETCode,isLightBulbTurnedOn))), msg2(a_82670,a_82669)),(encrypt0,oscore_version_one, AES_CCM,IDri_82682,partial_iv_82685))) $\sim X_3 = (\sim M_84062, a_82673, a_82674, a_82675, empty, \sim M_84307)$ (token 82681,a 82673,a 82674,a 82675,empty,aeadEncrypt(HKDF(msecret 82686,msalt 82687,(IDir 82683,idcontext 82684, AES_CCM,label_key,alg_key_length(AES_CCM,label_key))), aeadNonce(IDri 82682, partial iv 82685, HKDF (msecret 82686, msalt 82687, (emptyId, idcontext 82684, AES CCM, label iv, alg_key_length(AES_CCM,label_iv)))),((CoAP_CONTENTCode,

bounded_by((CoAP_GETCode,isLightBulbTurnedOn))), msg2(a_82670,a_82669)),(encrypt0,oscore_version_one, AES_CCM,IDri_82682,partial_iv_82685))) Honest Process Attacker a 82670 a 82669 a 82671 {4}new IDir_82683 {5}new IDri_82682 {6}new msecret_82686 {7}new msalt_82687 {8} new idcontext_82684 $(\sim M_83842, \sim M_83843, \sim M_83844) = (IDir_82683, IDri_82682,$ idcontext 82684) {10} insert security_context_lookup(a_82670,a_82669, IDir_82683,IDri_82682,msecret_82686,msalt_82687, idcontext $826\overline{8}4$) {11} insert security_context_lookup(a_82669,a_82670, IDri_82682,IDir_82683,msecret_82686,msalt_82687, idcontext_82684) Beginning of process oscore_initiator Beginning of process oscore_responder Beginning of process oscore_initiator_response_receiver Beginning of process oscore_initiator_response_receiver a **8**2669 {20} new token_82681 {21}new messageid_82688 {22} new partial_iv_82685 a_82670 {39} get security_context_lookup(a_82669,a_82670, IDri_82682,IDir_82683,msecret_82686,msalt_82687, idcontext $826\overline{8}4$) {34}insert token_to_message_lookup(a_82669,token_82681, (a_82670,IDri_82682,IDir_82683,idcontext_82684, partial_iv_82685,aeadNonce(IDri_82682,partial_iv_82685, HKDF(msecret_82686,msalt_82687,(emptyId,idcontext_82684, AES_CCM,label_iv,alg_key_length(AES_CCM,label_iv)))))) {35} event beginInitiator(a_82669,a_82670,(CoAP_GETCode, isLightBulbTurnedOn)) {37} event integrityReq(CoAP_GETCode,isLightBulbTurnedOn, $msg1(a_82\overline{6}69,a_82670))$ (~M_84059,~M_84060,~M_84061,~M_84062,(~M_84065, ~M 84066,~M \$4067),~M 84064) a 82670 ~X 1 {64} get security_context_lookup(a_82670,a_82669, IDir_82683,IDri_82682,msecret_82686,msalt_82687, idcontext 82684) {63} get replay_window(=a_82670,partial_84253: bitstring) suchthat (partial_84253 = partial_iv_82685): else branch taken {52} event integrityReq(CoAP_GETCode,isLightBulbTurnedOn, msg1(a_82669,a_82670)) {53} insert replay window(a 82670, partial iv 82685) {54} new responseId_82731 {60} event endResponder(a_82669,a_82670,(CoAP_GETCode, isLightBulbTurnedOn)) {61} event beginResponder(a_82669,a_82670,bounded_by((CoAP_GETCode, is LightBulb TurnedOn))) (~M_84302,~M_84303,~M_84304,~M_84305,~M_84306, ~M 84307) a 82669 ~X_2 {81} get token_to_message_lookup(a_82669,token_82681, (a_82670,IDri_82682,IDir_82683,idcontext_82684, partial_iv_82685,aeadNonce(IDri_82682,partial_iv_82685, HKDF(msecret_82686,msalt_82687,(emptyId,idcontext_82684, AES_CCM,label_iv,alg_key_length(AES_CCM,label_iv)))))) {80} get security_context_lookup(a_82669,a_82670, IDri 82682, IDir 82683, msecret 82686, msalt 82687, idcontext $826\overline{8}4$) {79} get used_tokens(=a_82669,acceptedT_84448: bitstring) suchthat (acceptedT_84448 = token_82681): else branch taken a 82669 ~X_3 {81} get token to message lookup(a 82669, token 82681, (a 82670,IDri 82682,IDir 82683,idcontext 82684,

partial iv 82685, aeadNonce(IDri 82682, partial iv 82685, HKDF(msecret 82686,msalt 82687,(emptyId,idcontext 82684, AES_CCM, label_iv, alg_key_length(AES_CCM, label_iv)))))) {80} get security_context_lookup(a_82669,a_82670, IDri_82682,IDir_82683,msecret_82686,msalt_82687, idcontext $826\overline{8}4$) {79} get used_tokens(=a_82669,acceptedT_85219: bitstring) suchthat (accepted $\overline{T}_85219 = token_{\overline{8}2681}$): else branch taken {75}insert used tokens(a 82669,token 82681)

{76} event match(a 82675,(CoAP CONTENTCode,bounded by((CoAP GETCode, is LightBulbTurnedOn))))

{76} event match(a 82675,(CoAP CONTENTCode,bounded by(

{77} event endInitiator(a_82669,a_82670,bounded_by(CoAP_GETCode,isLightBulbTurnedOn)))

{77} event endInitiator(a 82669,a 82670,bounded by((CoAP GETCode, is LightBulbTurnedOn)))

{75} insert used tokens(a 82669,token 82681)

(CoAP GETCode, is LightBulbTurnedOn))))

{78} event here