~M_8 = certDevice(subjectServer_1,constructURL(subjectServer_1, path_1),pk(skThingAttacker_1),skRogueCA_1) \sim M_9 = skThingAttacker_1 ~M_19 = PRF(PRF(preMasterSecret_2,clientRandom_4, serverRandom_4),client_finished_label,hash((clientRandom_4, serverRandom_4,cert(subjectServer_1,pk(skServer_3), skCA_1),penc(preMasterSecret_2,pk(skServer_3)))))) ~M_20 = PRF(PRF(preMasterSecret_2,clientRandom_4, serverRandom_4), server_finished_label, hash(((clientRandom_4, serverRandom_4,cert(subjectServer_1,pk(skServer_3), skCA_1),penc(preMasterSecret_2,pk(skServer_3))), PRF(PRF(preMasterSecret_2,clientRandom_4,serverRandom_4), client_finished_label,hash((clientRandom_4,serverRandom_4, cert(subjectServer_1,pk(skServer_3),skCA_1),penc(preMasterSecret_2,pk(skServer_3)))))))) ~M_21 = constructURL(subjectServer_1,path_1) A trace has been found. \sim M_22 = HMAC(constructURL(subjectServer_1,path_1), PRF(PRF(preMasterSecret_2,clientRandom_4,serverRandom_4), serverRandom_4,clientRandom_4)) $\sim X_1 = (getURL(\sim M_8), \sim M_22) = (constructURL(subjectServer_1,$ path 1),HMAC(constructÚRL(subjectServer_1,path_1), PRF(PRF(preMasterSecret_2,clientRandom_4,serverRandom_4), serverRandom_4,clientRandom_4))) \sim M_23 = sign(makeMUDfile(constructURL(subjectServer_1, path_1),aclList_3),skServer_3) \sim M_24 = cert(subjectServer_1,pk(skServer_3),skCA_1) \sim M_25 = HMAC((sign(makeMUDfile(constructURL(subjectServer_1, path_1),aclList_3),skServer_3),cert(subjectServer_1, pk(skServer_3),skCA_1)),PRF(PRF(preMasterSecret_2, clientRandom_4, serverRandom_4), serverRandom_ $\overline{4}$, clientRandom_4)) \sim M_3 = cert(subjectServer_1,pk(skServer_3),skCA_1) **Honest Process** Attacker {1}new skCA_1 \sim M = pk(skCA_1) {4}new skRogueCA_1 $(\sim M_1, \sim M_2) = (pk(skRogueCA_1), skRogueCA_1)$ {7}new skServer_3 {8}new subjectServer_1 \sim M_3 = cert(subjectServer_1,pk(skServer_3),skCA_1) {12} new skManager_2 \sim M_4 = pk(skManager_2) {15}new skServer2_1 {16}new subjectServer2_1 \sim M_5 = cert(subjectServer2_1,pk(skServer2_1),skCA_1) {20} new skServerAttacker_1 (~M_6,~M_7) = (cert(subjectServer_1,pk(skServerAttacker_1), skRogueCA_1),skServerAttacker_1) {24} new path_1 {25}new skThing_3 {29}new skThing2_1 {33}new skThingAttacker_1 $(\sim M_8, \sim M_9)$ Beginning of process MUD_File_Server Beginning of process Thing Beginning of process Thing Beginning of process MUD_Manager {126} event thingSentURL(constructURL(subjectServer_1, {126}event thingSentURL(constructURL(subjectServer_1, path_1)) path_1)) ~M_10 = certDevice(subjectServer_1,constructURL(subjectServer_1,path_1),pk(skThing_3),skCA_1) ~M_11 = certDevice(subjectServer_1,constructURL(subjectServer_1,path_1),pk(skThing_3),skCA_1) $(\sim M \ 10,a_2) = (certDevice(subjectServer_1,constructURL($ subjectServer_1,path_1),pk(skThing_3),skCA_1), {89}new sharedKey_4 {90} new nonceM_2 $(\sim M_12, \sim M_13) = (nonceM_2, penc(sharedKey_4, pk(skThing_3)))$ $(\sim M_12, \sim M_13) = (nonceM_2, penc(sharedKey_4, pk(skThing_3)))$ \sim M_14 = senc(nonceM_2,sharedKey_4) {131}event endThing \sim M_14 = senc(nonceM_2,sharedKey_4) {94} event managerReceivedURL(constructURL(subjectServer_1, path_1)) {95}new clientRandom_4 \sim M 15 = clientRandom 4 \sim M_15 = clientRandom_4 {40} event serverAuthnStarted(cert(subjectServer_1, pk(skServer_3),skCA_1))
{41} new serverRandom_4 $(\sim M_16, \sim M_17) = (serverRandom_4, cert(subjectServer_1, pk(skServer_3), skCA_1))$ $(\sim M_16, \sim M_3) = (serverRandom_4, cert(subjectServer_1, pk(skServer_3), skCA_1))$ {100}new preMasterSecret_2 \sim M_18 = penc(preMasterSecret_2,pk(skServer_3)) \sim M_19 \sim M_18 = penc(preMasterSecret_2,pk(skServer_3)) \sim M_19 ~M 20 ∼M 20 {109}event serverAuthnSuccessful(cert(subjectServer_1, pk(skServer_3),skCA_1)) {111} event managerSentURL(constructURL(subjectServer_1, path_1)) $(\sim M_21, \sim M_22)$ ~X 1 {55} event serverReceivedURL(constructURL(subjectServer_1, path_1)) {56} new aclList_3 {58} event serverSentMUDfile(cert(subjectServer_1, pk(skServer_3),skCA_1),makeMUDfile(constructURL(subjectServer_1,path_1),aclList_3)) $(\sim M_23, \sim M_24, \sim M_25)$ {60} event endFileServer $(\sim M_23, \sim M_3, \sim M_25)$ {120}event managerReceivedMUDfile(cert(subjectServer_1, pk(skServer_3),skCA_1),makeMUDfile(constructURL(subjectServer_1,path_1),aclList_3)) {121}event managerSentConfiguration(constructURL(subjectServer_1,path_1),configurations(aclList_3), a_2) ~M_26 = sign((configurations(aclList_3),a_2,constructURL(subjectServer_1,path_1)),skManager_2) {123}event endManager

Abbreviations