Abbreviations  $\sim X_1 = PRF(PRF(a_3,a_1,\sim M_8),client_finished_label,hash($  $(a_1, M_8, M_3, penc(a_3, getPk(\sim M_3))))$ = PRF(PRF(a 3,a 1,serverRandom 4),client finished label,  $hash(a_1,serverRandom_4,cert(subjectServer_1,$ pk(skServer\_3),skCA\_1),penc(a\_3,pk(skServer\_3)))))  $\sim$  M\_10 = PRF(PRF(a\_3,a\_1,serverRandom\_4),server\_finished\_label, hash(((a\_1,serverRandom\_4,cert(subjectServer\_1, pk(skServer\_3),skCA\_1),penc(a\_3,pk(skServer\_3))), PRF(PRF(a\_3,a\_1,serverRandom\_4),client\_finished\_label, hash((a\_1,serverRandom\_4,cert(subjectServer\_1, pk(skServer\_3),skCA\_1),penc(a\_3,pk(skServer\_3)))))))  $\sim X_2 = (\sim M_7, HMAC(\sim M_7, PRF(PRF(a_3, a_1, \sim M_8), \sim M_8, a_1)))$ (constructURL(subjectServer\_1,path\_1),HMAC(constructURL( subjectServer\_1,path\_1),PRF(PRF(a\_3,a\_1,serverRandom\_4), serverRandom\_4,a\_1))) ~M 11 = sign(makeMUDfile(constructURL(subjectServer 1, path 1),aclList 2),skServer 3)  $\sim$ M\_12 = cert(subjectServer\_1,pk(skServer\_3),skCA\_1) ~M\_13 = HMAC((sign(makeMUDfile(constructURL(subjectServer 1, path 1),aclList\_2),skServer\_3),cert(subjectServer\_1, pk(skServer\_3),skCA\_1)),PRF(PRF(a\_3,a\_1,serverRandom\_4),

A trace has been found.

serverRandom\_4,a\_1)) Attacker **Honest Process** {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 skServer2\_1 {13}new subjectServer2\_1  $\sim$ M\_4 = cert(subjectServer2\_1,pk(skServer2\_1),skCA\_1) {17} new skAttacker\_1 (~M\_5,~M\_6) = (cert(subjectServer\_1,pk(skAttacker\_1), skRogueCA\_1),skAttacker\_1) {21} new path\_1 Beginning of process MUD\_File\_Server Beginning of process Thing(constructURL(subjectServer\_1, path\_1)) {104}event thingSentURL(constructURL(subjectServer\_1, path\_1))  $\sim M$  7 = constructURL(subjectServer\_1,path\_1) {106} event endThing  $a_1$ {27} event serverAuthnStarted(cert(subjectServer\_1, pk(skServer\_3),skCA\_1)) {28} new serverRandom 4  $(\sim M \ 8, \sim M \ 9) = (serverRandom \ 4, cert(subjectServer \ 1,$ pk(skServer\_3),skCA\_1))  $penc(a_3,getPk(\sim M_3)) = penc(a_3,pk(skServer_3))$ ~X 1 ~M 10 ~X\_2 {42} event serverReceivedURL(constructURL(subjectServer\_1, path\_1)) {43}new aclList\_2 {45} event serverSentMUDfile(cert(subjectServer\_1, pk(skServer\_3),skCA\_1),makeMUDfile(constructURL(subjectServer\_1,path\_1),aclList\_2))  $(\sim M 11, \sim M 12, \sim M 13)$