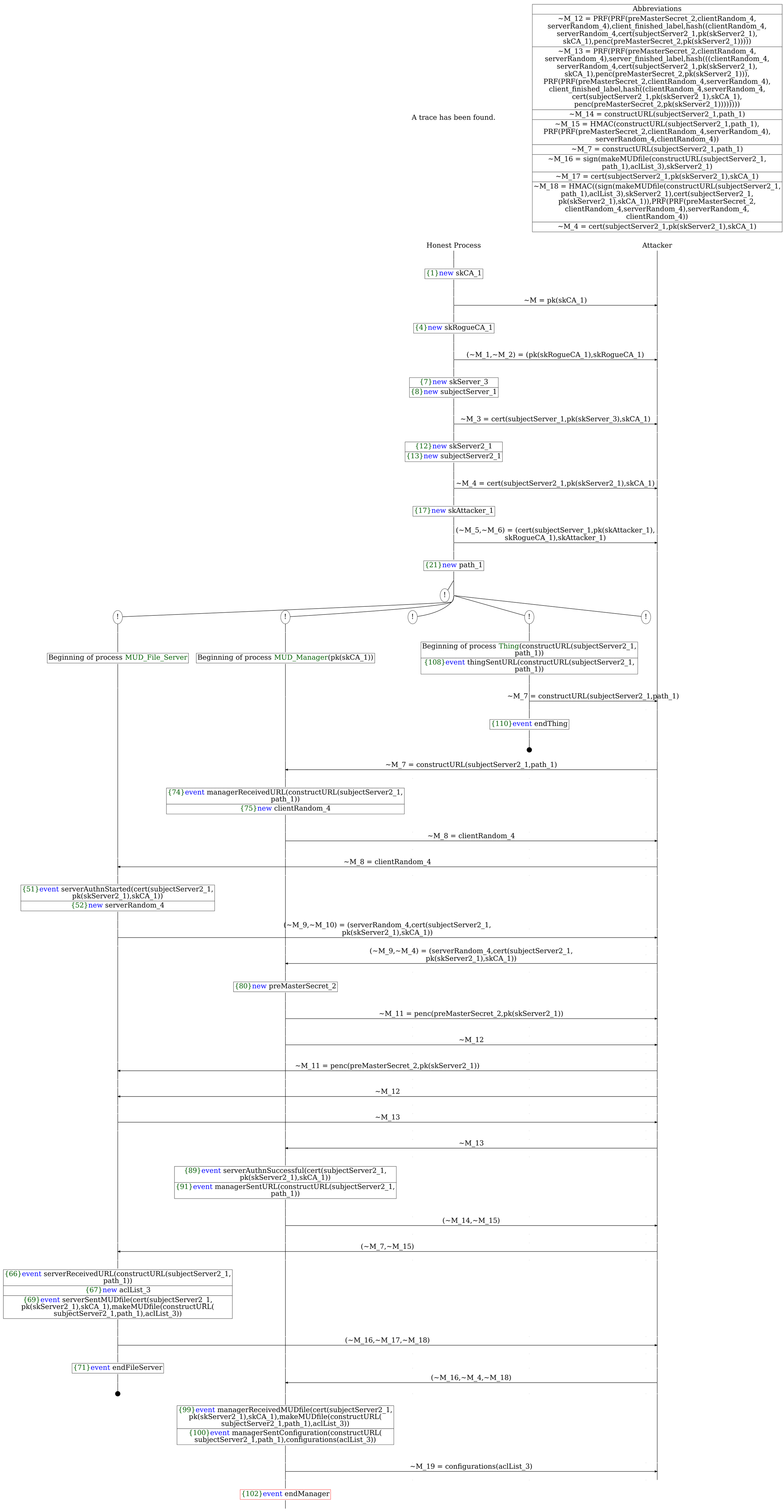
Abbreviations
~M_12 = PRF(PRF(preMasterSecret_2,clientRandom_4, serverRandom_4),client_finished_label,hash((clientRandom_4, serverRandom_4,cert(subjectServer2_1,pk(skServer2_1), skCA_1),penc(preMasterSecret_2,pk(skServer2_1)))))
~M_13 = PRF(PRF(preMasterSecret_2,clientRandom_4, serverRandom_4),server_finished_label,hash(((clientRandom_4, serverRandom_4,cert(subjectServer2_1,pk(skServer2_1), skCA_1),penc(preMasterSecret_2,pk(skServer2_1))), PRF(PRF(preMasterSecret_2,clientRandom_4,serverRandom_4), client_finished_label,hash((clientRandom_4,serverRandom_4, cert(subjectServer2_1,pk(skServer2_1),skCA_1), penc(preMasterSecret_2,pk(skServer2_1))))))))
~M_14 = constructURL(subjectServer2_1,path_1)
~M_15 = HMAC(constructURL(subjectServer2_1,path_1), PRF(PRF(preMasterSecret_2,clientRandom_4,serverRandom_4), serverRandom_4,clientRandom_4))
~M_7 = constructURL(subjectServer2_1,path_1)
~M_16 = sign(makeMUDfile(constructURL(subjectServer2_1, path_1),aclList_3),skServer2_1)
~M_17 = cert(subjectServer2_1,pk(skServer2_1),skCA_1)
~M_18 = HMAC((sign(makeMUDfile(constructURL(subjectServer2_1, path_1),aclList_3),skServer2_1),cert(subjectServer2_1, pk(skServer2_1),skCA_1)),PRF(PRF(preMasterSecret_2, clientRandom_4,serverRandom_4),serverRandom_4, clientRandom_4))
~M_4 = cert(subjectServer2_1,pk(skServer2_1),skCA_1)
A trace has been found.
Honest Process
Attacker
{1}new skCA_1
~M = pk(skCA_1)
{4}new skRogueCA_1
(~M_1,~M_2) = (pk(skRogueCA_1),skRogueCA_1)
{7}new skServer_3
{8}new subjectServer_1
~M_3 = cert(subjectServer_1,pk(skServer_3),skCA_1)
{12}new skServer2_1
{13}new subjectServer2_1
~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 MUD_Manager(pk(skCA_1))
Beginning of process Thing(constructURL(subjectServer2_1, path_1))
{108}event thingSentURL(constructURL(subjectServer2_1, path_1))
~M_7 = constructURL(subjectServer2_1,path_1)
{110}event endThing
~M_7 = constructURL(subjectServer2_1,path_1)
{74}event managerReceivedURL(constructURL(subjectServer2_1, path_1))
{75}new clientRandom_4
~M_8 = clientRandom_4
~M_8 = clientRandom_4
{51}event serverAuthnStarted(cert(subjectServer2_1, pk(skServer2_1),skCA_1))
{52}new serverRandom_4
(~M_9,~M_10) = (serverRandom_4,cert(subjectServer2_1, pk(skServer2_1),skCA_1))
(~M_9,~M_4) = (serverRandom_4,cert(subjectServer2_1, pk(skServer2_1),skCA_1))
{80}new preMasterSecret_2
~M_11 = penc(preMasterSecret_2,pk(skServer2_1))
~M_12
~M_11 = penc(preMasterSecret_2,pk(skServer2_1))
~M_12
~M_13
~M_13
{89}event serverAuthnSuccessful(cert(subjectServer2_1, pk(skServer2_1),skCA_1))
{91}event managerSentURL(constructURL(subjectServer2_1, path_1))
(~M_14,~M_15)
(~M_7,~M_15)
{66}event serverReceivedURL(constructURL(subjectServer2_1, path_1))
{67}new aclList_3
{69}event serverSentMUDfile(cert(subjectServer2_1, pk(skServer2_1),skCA_1),makeMUDfile(constructURL(subjectServer2_1,path_1),aclList_3))
(~M_16,~M_17,~M_18)
{71}event endFileServer
(~M_16,~M_4,~M_18)
{99}event managerReceivedMUDfile(cert(subjectServer2_1, pk(skServer2_1),skCA_1),makeMUDfile(constructURL(subjectServer2_1,path_1),aclList_3))
{100}event managerSentConfiguration(constructURL(subjectServer2_1,path_1),configurations(aclList_3))
~M_19 = configurations(aclList_3)
{102}event endManager