```
Abbreviations
                                           \sim X_1 = PRF(PRF(a_3,a_1,\sim M_8),client_finished_label,hash(
                                                   (a_1, \sim M_8, \sim M_4, penc(a_3, getPk(\sim M_4))))
                                               PRF(a_3,a_1,serverRandom_4),client_finished_label,
                                               hash((a_1,serverRandom_4,cert(subjectServer2_1,
                                             pk(skServer2_1),skCA_1),penc(a_3,pk(skServer2_1)))))
                                      \sim M_10 = PRF(PRF(a_3,a_1,serverRandom_4),server_finished_label,
                                               hash(((a_1,serverRandom_4,cert(subjectServer2_1,
 A trace has been found.
                                            pk(skServer2_1),skCA_1),penc(a_3,pk(skServer2_1))),
PRF(PRF(a_3,a_1,serverRandom_4),client_finished_label,
                                               hash((a_1,serverRandom_4,cert(subjectServer2_1,
                                            pk(skServer2_1),skCA_1),penc(a_3,pk(skServer2_1)))))))
                                       \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(subjectServer2_1,path_1),HMAC(
                                               constructURL(subjectServer2_1,path_1),PRF(PRF(a_3,a_1,serverRandom_4),serverRandom_4,a_1)))
     Honest Process
                                                                      Attacker
     \{1\} new skCA 1
                                   \simM = 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
               \simM_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 Thing(constructURL(subjectServer2_1,
                               path_1))
    {108} event thingSentURL(constructURL(subjectServer2_1,
                               path_1))
                             \simM_7 = constructURL(subjectServer2_1,path_1)
                         {110}event endThing
                  a_1
```

Beginning of process MUD_File_Server {51} event serverAuthnStarted(cert(subjectServer2_1, pk(skServer2_1),skCA_1)) {52}new serverRandom 4 $(\sim M_8, \sim M_9) = (serverRandom_4, cert(subjectServer2_1, pk(skServer2_1), skCA_1))$ $penc(a_3,getPk(\sim M_4)) = penc(a_3,pk(skServer2_1))$ ~X 1 ~M 10 ~X 2