```
a 2,a,serverRandom 4),client finished label,hash(
                                                                                           (a,serverRandom_4,cert(subjectServer_1,pk(skServer_3),
                                                                                                      skCA 1),penc(a 2,pk(skServer 3)))))
                                                                                      ~M_10 = PRF(PRF(a_2,a,serverRandom_4),server_finished_label,
                                                                                              hash(((a,serverRandom_4,cert(subjectServer_1,pk(
                                                                                               skServer_3),skCA_1),penc(a_2,pk(skServer_3))),
                                                                                            PRF(PRF(a_{\overline{2}},a,serve\overline{Random_{\overline{4}}}),client_finished_label,
                                                                                              hash((a,serverRandom_4,cert(subjectServer_1,pk(
                                                                                              skServer 3),skCA 1),penc(a 2,pk(skServer 3))))))))
                                                                                       \sim X_2 = (getURL(\sim M_7), HMAC(getURL(\sim M_7), \overline{PRF(PRF(a_2,a_7))})
                                                                                                                \simM 8),\simM 8,a)))
                                                                                                       = (constructURL(subjectServer 1,
                                                                                            path 1),HMAC(constructURL(subjectServer 1,path 1),
                                                                                            PRF(PRF(a 2,a,serverRandom_4),serverRandom_4,a)))
                                                                                         ~M 11 = sign(makeMUDfile(constructURL(subjectServer 1,
                                                                                                         path 1),aclList 2),skServer 3)
                                                                                            \simM 12 = cert(subjectServer 1,pk(skServer 3),skCA 1)
                                                                                     \simM_13 = HMAC((sign(makeMUDfile(constructURL(subjectServer_1,
                                                                                             path_1),aclList_2),skServer_3),cert(subjectServer_1,
                                                                                          pk(skServer 3),skCA 1)),PRF(PRF(a 2,a,serverRandom 4),
                                                                                                              serverRandom_4,a))
                                                                                                                     Attacker
                                             Honest Process
                                             {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
                                                         \simM 4 = cert(subjectServer2 1,pk(skServer2 1),skCA 1)
                                      {17} new skServerAttacker_1
                                                      (~M_5,~M_6) = (cert(subjectServer_1,pk(skServerAttacker_1), skRogueCA_1),skServerAttacker_1)
                                             {21}new path_1
                                                            ~M 7 = certDevice(subjectServer 1,constructURL(
                                                                  subjectServer 1,path 1),skRogueCA 1)
            Beginning of process MUD_File_Server
     {31} event serverAuthnStarted(cert(subjectServer_1, pk(skServer_3),skCA_1))
                   {32}new serverRandom 4
                                               (\sim M_8, \sim M_9) = (serverRandom_4, cert(subjectServer_1, pk(skServer_3), skCA_1))
                                                                    penc(a_2,getPk(\sim M_3)) = penc(a_2,pk(skServer_3))
                                                                         ~X 1
                                                                         ~M 10
                                                                          ~X 2
{46} event serverReceivedURL(constructURL(subjectServer_1, path_1))
                       {47} new aclList 2
    {49} 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)
                    {51} event endFileServer
```

A trace has been found.

Abbreviations

 $\sim X_1 = PRF(PRF(a_2,a,\sim M_8),client_finished_label,hash($

 $(a,\sim M_8,\sim \overline{M}_3,pen\overline{c}(a_2,get\overline{P}k(\sim M_3))))$

= PRF(PRF(