Abbreviations $\sim M_8 = \text{certDevice}(\text{subjectServer}_1, \text{constructURL}(\text{subjectServer}_1, \text{constructURL})$ path 1),pk(skThingAttacker 1),skRogueCA 1) \sim M 9 = skThingAttacker 1 $\sim X_1 = PRF(PRF(a_2,a,\sim M_10),client_finished_label,hash($ $(a,\sim M_10,\sim M_3,penc(\bar{a}_2,getPkServer(\sim M_3))))$ PRF(PRF(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))))) \sim M_12 = 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))), $PRF(PRF(a_{\overline{2}},a,serverRandom_{\overline{4}}),client_finished_label,$ hash((a,serverRandom 4,cert(subjectServer 1,pk(skServer 3),skCA 1),penc(a 2,pk(skServer 3)))))))) \sim X_2 = (getURL(\sim M_8),HMAC(getURL(\sim M_8),PRF(PRF(a_2,a, \sim M 10), \sim M 10,a))) = (constructURL(subjectServer 1, path 1),HMAC(constructURL(subjectServer 1,path 1), PRF(PRF(a_2,a,serverRandom_4),serverRandom_4,a))) ~M 13 = sign(makeMUDfile(constructURL(subjectServer 1, path_1),aclList_2),skServer_3) ~M_14 = cert(subjectServer_1,pk(skServer_3),skCA_1) \sim M_15 = 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),

A trace has been found.

```
serverRandom 4,a))
                                                                                                                        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 skManager_2
                                                                                                                                                                                                    \simM 4 = pk(skManager 2)
                                                                                                               {15}new skServer2_1
                                                                                                        {16}new subjectServer2_1
                                                                                                                                                         \simM 5 = cert(subjectServer2 1,pk(skServer2 1),skCA 1)
                                                                                                      {20} new skServerAttacker_1
                                                                                                                                               (\sim M_6, \sim M_7) = (cert(subjectServer_1, pk(skServerAttacker_1), pk(skServer_1), pk(skServer_1), pk(skServer_1), pk(skServer_1), pk(skServer_1), pk(s
                                                                                                                                                                                      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
            {40} event serverAuthnStarted(cert(subjectServer_1, pk(skServer_3),skCA_1))
                                                   {41}new serverRandom 4
                                                                                                                          (\sim M_10, \sim M_11) = (serverRandom_4, cert(subjectServer_1, otherwise))
                                                                                                                                                                          pk(skServer 3),skCA 1))
                                                                                                                           penc(a_2,getPkServer(\sim M_3)) = penc(a_2,pk(skServer_3))
                                                                                                                                                                                                       ~X 1
                                                                                                                                                                                                    ~M 12
                                                                                                                                                                                                       ~X 2
{55} event serverReceivedURL(constructURL(subjectServer 1,
                                                                            path 1))
                                                               {56} new aclList 2
           {58} event serverSentMUDfile(cert(subjectServer_1, pk(skServer_3),skCA_1),makeMUDfile(constructURL(subjectServer_1,path_1),aclList_2))
                                                                                                                                                                           (\sim M_13, \sim M_14, \sim M_15)
                                                    {60} event endFileServer
```