Supplementary: HLPSL code

```
role mobileuser(
           MU,FA,HA    : agent,
           SKmh        : symmetric_key,
           H           : hash_func,
           SND, RCV    : channel(dy))

played_by MU def=

     local State                        : nat,
     K,N0,PIDm                    : text,
     Kuh,Kfh                            : text,
     IDm, PWm                     : text,
     IDh, IDf                     : text,
     SK                           : text,
     Nm,Nf,N1,N2,N3,N4,N,F,Tm,Tf        : text,
     Nx,Ny,NN,FF,Ntm,Ntf,Nxy,Nyx,Nxx,Nyy    : text,
     V1,V2,V3,V4,V5,V6                  : text

     const mu_fa_n1, mu_ha_n1,fa_ha_n2, fa_mu_n2, ha_mu_n3,
ha_fa_n4,s0,s1,s2,s3,s4,s5,s6,s7,s8    : protocol_id

     init State := 0

     transition

     1. State =0      /\ RCV(start) =|>
        State':= 1    /\ N0':=new()
                 /\ PIDm':=H(IDm.N0')
                 /\ SND({IDm.PIDm'}_SKmh)
                 /\ secret(N0',s0,{MU})
                 /\ secret(IDm,s1,{MU,HA})


     2. State = 1     /\ RCV({IDh.{IDm.IDh.Nm'}_K.Nm'}_SKmh) =|>
           State':= 2 /\ secret({K},s2,{HA})
                 /\ secret(Nm',s3,{MU,HA})
                 /\ N1':= new()
                 /\ Tm':= new()
                 /\ Kuh':= H(IDm.Nm')
                 /\ Nx':= xor(Kuh',N1')
                 /\ V1':= H(PIDm.Kuh'.N1'.Tm')
                 /\ SND({IDm.IDh.Nm'}_K.Nx'.V1'.IDh.Tm')
                 /\ secret(N1',s4,MU)
                 /\ witness(MU,FA,mu_fa_n1,N1')
                 /\ witness(MU,HA,mu_ha_n1,N1')
```

```
      3. State = 2     /\
RCV(xor(xor(H(IDf.Nf),xor(H(IDf.Nf),N2')),H(IDm.Nm)).xor({IDm.IDh.N3'}
_K,H(H(IDm.Nm))).xor(N3',H(H(IDm.Nm))).H(xor({IDm.IDh.N3'}_K,H(H(IDm.N
m))).H(IDm.Nm).xor(H(IDm.Nm),xor(H(IDm.Nm),N1)).xor(H(IDf.Nf),xor(H(ID
f.Nf),N2')).N3').H(H(xor(xor(xor(H(IDm.Nm),xor(H(IDm.Nm),N1)),H(IDf.Nf
)),H(IDf.Nf)).N2').xor(xor(xor(H(IDm.Nm),xor(H(IDm.Nm),N1)),H(IDf.Nf))
,H(IDf.Nf)).N2')) =|>

         State':= 3    /\ secret(Nf,s5,{FA,HA})
                 /\ secret(N2',s6,FA)
                 /\ secret(N3',s7,HA)
                 /\ N2':=
xor(xor(xor(H(IDf.Nf),xor(H(IDf.Nf),N2')),H(IDm.Nm)),Kuh)
                 /\ N3':= xor(xor(N3',H(H(IDm.Nm))),H(Kuh))
                 /\ SK':= H(N1.N2')
                 /\ V6':= H(SK'.N2'.N1)
                 /\ SND(V6')
                 /\ request(MU,HA,ha_mu_n3,N3')
                 /\ request(MU,FA,fa_mu_n2,N2')
      end role


role homeagent(
           MU,FA,HA    : agent,
           SKmh        : symmetric_key,
           H           : hash_func,
           SND, RCV    : channel(dy))


played_by HA def=

      local State                        : nat,
      K,N0,PIDm                    : text,
      Kuh,Kfh                            : text,
      IDm, PWm                     : text,
      IDh, IDf                     : text,
      SK                           : text,
      Nm,Nf,N1,N2,N3,N4,N,F,Tm,Tf      : text,
      Nx,Ny,NN,FF,Ntm,Ntf,Nxy,Nyx,Nxx,Nyy    : text,
      V1,V2,V3,V4,V5,V6                  : text

      const mu_fa_n1, mu_ha_n1,fa_ha_n2, fa_mu_n2, ha_mu_n3,
ha_fa_n4,s0,s1,s2,s3,s4,s5,s6,s7,s8    : protocol_id

      init State := 0
      transition

      1. State = 0     /\ RCV({IDm.H(IDm.N0')}_SKmh) =|>
         State':= 1    /\ secret(N0',s0,{MU})
                 /\ secret(IDm,s1,{MU,HA})
                 /\ Nm':= new()
                 /\ N':= {IDm.IDh.Nm'}_K
```

```
                /\ SND({IDh.N'.Nm'}_SKmh)
                /\ secret({K},s2,{HA})
                /\ secret(Nm',s3,{MU,HA})


     2. State = 1    /\
RCV({IDm.IDh.Nm}_K.xor(H(IDm.Nm),N1').{IDf.IDh.Nf}_K.xor(H(IDf.Nf),N2'
).H(H(IDm.N0').H(IDm.Nm).N1'.Tm').H(IDf.H(IDf.Nf).N2'.Tf').Tm'.Tf') =|>
        State':= 2   /\ secret(N1',s4,MU)
                /\ secret(Nf,s5,{FA,HA})
                /\ secret(N2',s6,FA)
                /\ Kuh':= H(IDm.Nm)
                /\ Kfh':= H(IDf.Nf)
                /\ N1':= xor(Kuh',xor(H(IDm.Nm),N1'))
                /\ N2':= xor(Kfh',xor(H(IDf.Nf),N2'))
                /\ N3':= new()
                /\ N4':= new()
                /\ Nxy':= xor(N2',Kuh')
                /\ Nxx':= xor(N3',H(Kuh'))
                /\ Nyx':= xor(N1',Kfh')
                /\ Nyy':= xor(N4',H(Kfh'))
                /\ NN':= xor({IDm.IDh.N3'}_K,H(Kuh'))
                /\ FF':= xor({IDf.IDh.N4'}_K,H(Kfh'))
                /\ V3':= H(NN'.Kuh'.N1'.N2'.N3')
                /\ V4':= H(FF'.Kfh'.N1'.N2'.N4')
                /\ SND(Nxy'.Nyx'.NN'.FF'.Nxx'.Nyy'.V3'.V4')
                /\ secret(N3',s7,HA)
                /\ secret(N4',s8,HA)
                /\ request(HA,FA,fa_ha_n2,N2')
                /\ request(HA,MU,mu_ha_n1,N1')
                /\ witness(HA,MU,ha_mu_n3,N3')
                /\ witness(HA,FA,ha_fa_n4,N4')

     end role


role foreignagent(
           MU,FA,HA   : agent,
           H          : hash_func,
           SND, RCV   : channel(dy))

played_by FA def=


     local State                    : nat,
     K,N0,PIDm                  : text,
     Kuh,Kfh                        : text,
     IDm, PWm                   : text,
     IDh, IDf                   : text,
     SK                         : text,
     Nm,Nf,N1,N2,N3,N4,N,F,Tm,Tf      : text,
     Nx,Ny,NN,FF,Ntm,Ntf,Nxy,Nyx,Nxx,Nyy   : text,
```

```
      V1,V2,V3,V4,V5,V6                : text

      const mu_fa_n1, mu_ha_n1,fa_ha_n2, fa_mu_n2, ha_mu_n3,
ha_fa_n4,s0,s1,s2,s3,s4,s5,s6,s7,s8    : protocol_id

      init State := 0

      transition

      1. State = 0     /\
RCV({IDm.IDh.Nm'}_K.xor(H(IDm.Nm'),N1').H(H(IDm.N0').H(IDm.Nm').N1'.Tm
').IDh.Tm') =|>
         State':= 1    /\ secret(IDm,s1,{MU,HA})
                       /\ secret(K,s2,{HA})
                       /\ secret(Nm',s3,{MU,HA})
                       /\ secret(N1',s4,MU)
                       /\ N2':= new()
                       /\ Tf':=new()
                       /\ Kfh':= H(IDf.Nf)
                       /\ Ny':= xor(Kfh',N2')
                       /\ V2':= H(IDf.Kfh'.N2'.Tf')
                       /\
SND({IDm.IDh.Nm'}_K.xor(H(IDm.Nm'),N1').{IDf.IDh.Nf}_K.Ny'.H(H(IDm.N0'
).H(IDm.Nm').N1').V2'.Tm'.Tf')
                       /\ secret(Nf,s5,{FA,HA})
                       /\ secret(N2',s6,FA)
                       /\ witness(FA,HA,fa_ha_n2,N2')

      4. State = 3     /\
RCV(xor(xor(H(IDf.Nf),xor(H(IDf.Nf),N2)),H(IDm.Nm)).xor(xor(H(IDm.Nm),
xor(H(IDm.Nm),N1)),H(IDf.Nf)).xor({IDm.IDh.N3'}_K,H(H(IDm.Nm))).xor({I
Df.IDh.N4'}_K,H(H(IDf.Nf))).xor(N3',H(H(IDm.Nm))).xor(N4',H(H(IDf.Nf))
).H(xor({IDm.IDh.N3'}_K,H(H(IDm.Nm))).H(IDm.Nm).xor(H(IDm.Nm),xor(H(ID
m.Nm),N1)).xor(H(IDf.Nf),xor(H(IDf.Nf),N2)).N3').H(xor({IDf.IDh.N4'}_K
,H(H(IDf.Nf))).H(IDf.Nf).xor(H(IDm.Nm),xor(H(IDm.Nm),N1)).xor(H(IDf.Nf
),xor(H(IDf.Nf),N2)).N4')) =|>

         State':= 4    /\ secret(N3',s7,HA)
                       /\ secret(N4',s8,HA)
                       /\ N1':=
xor(xor(xor(H(IDm.Nm),xor(H(IDm.Nm),N1)),H(IDf.Nf)),Kfh)
                       /\ N4':= xor(xor(N4',H(H(IDf.Nf))),H(Kfh))
                       /\ SK':= H(N1'.N2)
                       /\ V5':= H(SK'.N1'.N2)
                       /\
SND(xor(xor(H(IDf.Nf),xor(H(IDf.Nf),N2)),H(IDm.Nm)).xor({IDm.IDh.N3'}_
K,H(H(IDm.Nm))).xor(N3',H(H(IDm.Nm))).H(xor({IDm.IDh.N3'}_K,H(H(IDm.Nm
))).H(IDm.Nm).xor(H(IDm.Nm),xor(H(IDm.Nm),N1)).xor(H(IDf.Nf),xor(H(IDf
.Nf),N2)).N3').V5')
                       /\ request(FA,HA,ha_fa_n4,N4')
                       /\ witness(FA,MU,fa_mu_n2,N2)
```

```
      5. State = 4     /\
RCV(H(H(N1.xor(xor(xor(H(IDf.Nf),xor(H(IDf.Nf),N2)),H(IDm.Nm)),H(IDm.N
m))).xor(xor(xor(H(IDf.Nf),xor(H(IDf.Nf),N2)),H(IDm.Nm)),H(IDm.Nm)).N1
)) =|>
         State':= 5    /\ request(FA,MU,mu_fa_n1,N1)


      end role


role session(
           MU,FA,HA   : agent,
           SKmh       : symmetric_key,
              H       : hash_func)

def=

      local SD1,SD2,SD3,RV1,RV2,RV3 : channel(dy)

      composition

           mobileuser(MU,FA,HA,SKmh,H,SD1,RV1)
           /\ homeagent(MU,FA,HA,SKmh,H,SD2,RV2)
           /\ foreignagent(MU,FA,HA,H,SD3,RV3)
end role

role environment()

def=

const mu,fa,ha              : agent,
skmh                  : symmetric_key,
h                     : hash_func,
idh,idf               : text,
nx,ny,ntm,ntf,nxy,nxx,nyx,nyy,nn,ff,tm,tf   : text,
v1,v2,v3,v4,v5,v6           : text,

mu_fa_n1, mu_ha_n1,fa_ha_n2, fa_mu_n2, ha_mu_n3,
ha_fa_n4,s0,s1,s2,s3,s4,s5,s6,s7,s8   : protocol_id

intruder_knowledge={mu,ha,fa,h,idh,idf,nx,ny,ntm,ntf,nxy,nxx,nyx,nyy,n
n,ff,tm,tf,v1,v2,v3,v4,v5,v6}

composition

session(mu,fa,ha,skmh,h)
/\session(i,fa,ha,skmh,h)
/\session(mu,i,ha,skmh,h)
/\session(mu,fa,i,skmh,h)

end role
```

```
goal

secrecy_of s0,s1,s2,s3,s4,s5,s6,s7,s8



authentication_on mu_fa_n1, mu_ha_n1,fa_ha_n2, fa_mu_n2, ha_mu_n3,
ha_fa_n4

end goal

environment()
```