Role of NAD

```
role networkdevice (ED, NAD: agent, SKus: symmetric_key, SND,RCV: channel(dy))
played_by NAD
def=
          local
                    State:nat,
                    IDu, PWu, Bu, Aa, Bb, Cu, M,AB, TW: text,
                    Lu, Xu, Yu, Fu, Zu, PIDr, Bbprime, Du: text,
                    Buj, IDj, Quj, PIDrprime, Qujprime, Dj, Tu, SKuj,Ss, DIDu: text,
                    H: hash_func
          const
                    sp1,sp2, sp3, a, b,  bprime, dj, cu       : protocol_id
          init
                    State := 0
          transition
%%% User Registration Phase
          1. State =  0 /\ RCV({IDu.M.TW}_SKus) =|>
%%% Identity IDu is shared between ED and NAD
          State' := 2 /\  secret({IDu}, sp1, {ED,NAD})
%%% Password and Biometric  are only know to ED
          /\  secret({PWu,Bu}, sp2, {ED})
%%% Computation
          /\ Lu' := H(M.Ss)
          /\ Bb' := new()
          /\ Xu' := H(Lu'.H(Ss.Bb))

          /\ Yu' := xor(Xu', H(M.TW))
          /\ Zu' := xor(xor(Lu',H(Ss       . Bb)),TW)
          /\ Fu' := H(H(IDu.TW))
          /\ PIDr' :={IDu.Ss.Bb}_SKus
          /\ Du' := xor(H(IDu.Ss), H(IDu.TW))
          /\ SND(PIDr'. Du'. Yu'.Fu'.Zu')
%%% Mutual Authentication
%%% Receive login request Message M1 from ED
          2. State = 2 /\ RCV(PIDr. DIDu. Buj.Cu') =|>
%%% We decrytp PIDr by using master key of CCS
          State' := 4 /\   PIDr':= IDu.Ss.Bb
          /\ Lu' := xor(xor(xor(Buj,H(H(IDj.Cu'))),H(PIDr.H(IDu.Ss))),H(Ss.Bb))
          /\ Xu' := H(Lu'.H(Ss.Bb))
          /\ DIDu' := H(PIDr'.Xu'.Cu')
          /\ Bbprime' := new()
          /\ Dj' := new()
          /\ PIDrprime' := xor(H(IDu.Ss), H(Ss.Bbprime'))
          /\ Tu' := xor(PIDrprime',H(PIDr'.H(IDu.Ss).Xu'))
          /\ Quj' :=H(H(IDu.Ss).Tu'.Cu'.Dj'.Xu'.IDj)
%%% Send request message M2 to ED publicly
          /\ SND(Quj'.Tu'.Dj')
%%% Freshly generated Random number b' and Dj
          /\ witness(ED, NAD, dj, Dj')
          /\ witness(ED, NAD, bprime, Bbprime')
%%% Receive request message M3 to ED publicly
          3. State = 4 /\ RCV(Qujprime') =|>
%%% NAD acceptance of value Cu generated by ED for NAD
            State' := 6  /\ Cu' := new()      /\ request(ED, NAD, cu, Cu')
          /\ SKuj' := H(H(IDu.Ss). Cu'. Dj. Xu. IDj)
       /\ Qujprime' := H(SKuj.H(IDu.Ss).Dj.Xu.IDj)
end role
```