Role of User

```
role edge (ED, NAD: agent, SKus: symmetric_key, SND, RCV: channel(dy))
played by ED
def=
        local
        State:nat,
        IDu, PWu, Bu, Aa, 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
        1. State = 0  /\  RCV(start) =|>
      State' := 1  /\  M' := H(IDu.Bu)
        /\ Aa' := new()
        /\ TW' := H(xor(Aa,H(Bu.PWu)))
%%% Identity is Shared BETWEEN ED and NAD
        /\  secret({IDu}, sp1, {ED,NAD})
%%% Password and Biometric  are only know to ED
        /\  secret({PWu,Bu}, sp2, {ED})
%%% Send Registration Request to NAD
        /\  SND({IDu.M'.TW'}_SKus)
%%% Receive Registration Reply to NAD
        2. State=1 /\ RCV({PIDr'.Du.Yu.Fu.Zu}_SKus) =|>
%%% Master key s is only known to NAD
        State' := 3 /\  secret({Ss}, sp3, {NAD})
%%% Authentication and Key Exchange Phase (Public Channel)
        /\ Fu' := H(IDu.TW)
        /\ Cu' :=  new()
%%%Here we assume that H(IDu.Ss)= AB'
        /\  AB' := xor(Du, H(IDu.TW))
        /\ Buj'  := xor(xor(xor(Zu,H(IDj.Cu')),TW),H(PIDr'.H(IDu.Ss)))
        /\ Xu' := xor(Yu, H(M.TW))
        /\ DIDu' := H(PIDr'.Xu.Cu')
%%% Send login request message M1 to NAD
        /\ SND(PIDr'.DIDu'.Buj'.Cu')
%%% U has freshly generated random number
        /\ witness(ED, NAD, cu, Cu')
%%% Receive Authentication message from NAD
        3. State=3 /\ RCV(Quj. Tu. Dj          ) =|>
        State' := 5 /\  Dj' := new() /\ PIDr' := new()
        /\ Quj' := H(H(IDu.Ss).Tu.Cu.Dj.Xu.IDj)
        /\ SKuj' := H(H(IDu.Ss). Cu. Dj. Xu. IDj)
      /\ Qujprime' := H(SKuj.H(IDu.Ss).Dj.Xu.IDj)
        /\ PIDrprime' := xor(Tu, H(PIDr'.H(IDu.Ss).Xu))
%%% Send authentication Reply to NAD
        /\ SND(Qujprime')
%%% ED's acceptance of values b' and Dj for ED by NAD
        /\ request(ED, NAD, dj, Dj')
        /\ request(ED, NAD, bprime, Bbprime)
end role
```