with forwardable ticket

where Acs := {C,T2'}_Kcs (T2 is a timestamp)

****

An alternative instance of the protocol in action. Theltr-14.445Td[cl)1(ie)1(nt)-514(c

```
    G,S,C,A            : agent,
    Kag,Kgs            : symmetric_key,
    SND,RCV            : channel(dy),
    L                  : text set)
played_by G def=

  local
    State    : nat,
    N2       : text,
    U        : text,
    Kcg      : symmetric_key,
    Kcs      : symmetric_key,
    T1start  : text,
    T2start  : text,
    T1expire : text,
    T2expire : text,
    T1       : text,
    IP_ADDR  : text,
    Forwardable_or_not  : protocol_id

  const  forwardable,
         sec_t_Kcg,
         sec_t_Kcs   : protocol_id

  init   State := 21

  transition

 1. State  = 21
      /\ RCV(IP_ADDR'.S.N2'.
             {U'.C.G.Kcg'.T1start'.T1expire'}_Kag.
             {C.T1'}_Kcg'.
             Forwardable_or_not')
      %% T1' should not have been received before
      /\ not(in(T1',L))
    =|>
    State' := 22
      /\ Kcs' := new()
      /\ T2start' := new()
      /\ T2expire' := new()
      /\ SND(U'.
```

```
  const forwardable,
        un_forwardable : protocol_id,
        sec_c_Kcg1,
        sec_c_Kcg2,
        sec_c_Kcs      : protocol_id

  init  State := 1

  transition

 1. State  = 1  /\ RCV(start)  =|>
    State' := 2 /\ N1' := new()
                /\ SND(U.G.N1')

21. State  = 2  /\ RCV(U.Tcg'.{G.Kcg'.T1start'.T1expire'.N1}_Kca) =|>
    State' := 3 /\ N2' := new()
                /\ T1' := new()
                /\ IP_ADDR' := new()
                /\ SND(IP_ADDR'.S.N2'.Tcg'.{C.T1'}_Kcg'.forwardable)
                /\ witness(C,G,t1,T1')
                /\ request(C,A,n1,N1)
                /\ secret(Kcg',sec_c_Kcg1,{A,C,G})

22. State  = 2  /\ RCV(U.Tcg'.{G.Kcg'.T1start'.T1expire'.N1}_Kca) =|>
    State' := 4 /\ SND(IP_ADDR'.S.N2'.Tcg'.{C.T1'}_Kcg'.un_forwardable)
                /\ witness(C,G,t1,T1')
                /\ request(C,A,n1,N1)
                /\ secret(Kcg',sec_c_Kcg2,{A,C,G})

 3. State  = 3  /\ RCV(U.Tcs1'.{S.Kcs'.T2start'.T2expire'.N2}_Kcg) =|>
    State' := 4 /\ SND(IP_ADDR.S.N2.Tcs1'.{C.T1}_Kcg5051
    /G34 2eq2est(C,A,n1,N1)
```

```
end role
```

```
role session(
    A,G,C,S                  : agent,
    U                        : text,
    Kca,Kgs,Kag              : symmetric_key,
    LS,LG                    : text set) def=

  local
    SendC,ReceiveC           : channel (dy),
    SendS,ReceiveS           : channel (dy),
    SendG,ReceiveG           : channel (dy),
    SendA,ReceiveA           : channel (dy)

  composition
    client(C,G,S,A,U,Kca,SendC,ReceiveC)
 /\ server(S,C,G,Kgs,SendS,ReceiveS,LS)
 /\ ticketGrantingServer(G,S,C,A,Kag,Kgs,SendG,ReceiveG,LG)
 /\ authenticationServer(A,C,G,Kca,Kag,SendA,ReceiveA)

end role
```

```
role environment() def=

  local LS, LG : text set

  const
    a,g,c,s                      : agent,
    u1,u2                        : text,
    k_ca,k_gs,k_ag,k_ia          : symmetric_key,
    t1,t2a,t2b,n1,n2             : protocol_id,
    forwardable, un_forwardable  : protocol_id

  init LS = {} /\ LG = {}

  intruder_knowledge = {a,g,c,s,k_ia,forwardable,u1,u2
```

```
}
```