public key initialisation

Protocol Purpose

Mutual Authentication with Public Key initialisation (in case the Authentication Server and Client don’t share a key)

Definition Reference

```
Kcg      : symmetric_key,
T1start  : text,
T1expire : text,
Ktemp    : symmetric_key
```

```
        Kcg     : symmetric_key,
        Kcs     : symmetric_key,
        T1start,T1expire : text,
        T2start,T2expire : text,
        T1      : text

  const sec_t_Kcg, sec_t_Kcs : protocol_id

  init  State := 21

  transition
    1. State  = 21  /\ RCV( S.N2’.
                           {U’.C.G.Kcg’.T1start’.T1expire’}_Kag.
                           {C.T1’}_Kcg’)
                           /\ not(in(T1’,L)) =|>
       State’ := 22 /\ Kcs’ := new()
                    /\ T2start’ := new()
                    /\ T2expire’ := new()
                    /\ SND(  U’.
                           {U’.C.S.Kcs’.T2start’.T2expire’}_Kgs.
                           {S.Kcs’.T2start’.T2expire’.N2’}_Kcg’
                         )
                    /\ L’ := cons(T1’,L)
                    /\ wrequest(G,C,t1,T1’)
                    /\ witness(G,C,n2,N2’)
                    /\ secret(Kcg’,sec_t_Kcg,{A,C,G})
                    /\ secret(Kcs’,sec_t_Kcs,{G,C,S})

end role
```

```
role server( S,C,G    : agent,
             Kgs   : symmetric_key,
             SND, RCV : channei-514(RC)1Kag.
```

U   : text,

```
end role
```