three-pass mutual authentication

Protocol Purpose

Two parties authenticate each other. Aim of the Mutual authentication is to make sure to each of

HLPSL Specification

```
role iso4_Init ( A,B: agent,
                 Pkb,Pks: public_key,
                 Snd,Rec: channel(dy))
played_by B
def=

  local  State         : nat,
         Pka           : public_key,
         Nb            : text,
         Na,Text2,Text3: text

  const ctext1,ctext4,ctext5: text

  init State := 0

  transition

   1. State = 0
      /\ Rec(start)
      =|>
      State' := 1
      /\ Nb' := new()
      /\ Snd(Nb'.ctext1)
      /\ witness(B,A,nb,Nb')

   2. State = 1
      /\ Rec(Pka'.A.{Pka'.A}_inv(Pks).Na'.Nb.B.Text3'.
             {Na'.Nb.B.Text2'}_inv(Pka'))
      =|>
      State' := 2
      /\ Snd(Pkb.B.{Pkb.B}_inv(Pks).Nb.Na'.A.ctext5.{Nb.Na'.A.ctext4}_inv(Pkb))
      /\ request(B,A,na,Na')

end role
```

```
role ibo4_Resp ( B,A: agent,
                 Pka,Pkb: public_key,
```

```
              Pka,Pkb,Pks: public_key) def=

  local SA,RA,SB,RB: channel (dy)

  composition

         iso4_Init(A,B,Pkb,Pks,SA,RA)
      /\ iso4_Resp(B,A,Pka,Pks,SB,RB)

end role
```

```
role environment() def=

 const na, nb             : protocol_id,
       a, b, i            : agent,
       pka, pkb, pks, pki : public_key

 intruder_knowledge={a,b,pki,inv(pki),pks,
                     ctext1,ctext4,ctext5,{pki.i}_inv(pks),
```

```
end goal
```

```
environment()
```

References

[CJ] J. Clark and J. Jacob. A Survey of Authentication Protocol Literature: Version 1.0, 17. Nov. 1997. URL: