two-Pass unilateral authentication

Protocol Purpose

Authentication of a client to a server. This protocol models a situation in which the server wants to verify the client identity and starts the session. The client answers by sending his digital signature.

Definition Reference

- [CJ, ISO97]

Model Authors

- Haykal Tej, Siemens CT IC 3, 2003 and
- Luca Compagna et al, AI-Lab DIST University of Genova, November 2004

Alice&Bob style

```
1. B -> A : Rb, Text1
2. A -> B : {PKa,A}inv(PKs), Ra,Rb, B, Text2,{Ra,Rb,B,Text1}inv(PKa)
```

Problems considered: 1

Attacks Found

None

Further Notes

`inv(PKs)` is the private key of the server `C`; `{PKa,A}inv(PKs)` is the certificate of agent `A`.

HLPSL Specification

```
role iso2_Init (B,A    : agent,
                Pks    : public_key,
                Snd,Rec: channel(dy))
played_by B
def=

  local  State     : nat,
         Pka       : public_key,
         Rb        : text,
         Ra, Text2 : text

  init State := 0

  transition

   1. State = 0
      /\ Rec(start)
      =|>
      State' := 1
      /\ Rb' := new()
      /\ Snd(Rb'.ctext1)

   2. State = 1
      /\ Rec(Pka'.A.{Pka'.A}_inv(Pks).Ra'.Rb.B.Text2'.
                    {Ra'.Rb.B.ctext1}_inv(Pka'))
      =|>
      State' := 2
      /\ request(B,A,ra,Ra')

end role
```

```
role iso2_Resp (A,B    : agent,
                Pka,Pks: public_key,
                Snd,Rec: channel(dy))
played_by A
def=
```

```
  local  State     : nat,
         Ra        : text,
         Rb, Text1 : text

  init State := 0

  transition

   1. State = 0
      /\ Rec(Rb'.Text1')
      =|>
      State' := 2
      /\ Ra' := new()
      /\ Snd(Pka.A.{Pka.A}_inv(Pks).Ra'.Rb'.B.ctext2.
                   {Ra'.Rb'.B.Text1'}_inv(Pka))
      /\ witness(A,B,ra,Ra')

end role
```

```
role session (B, A : agent,
              Pka  : public_key,
              Pks  : public_key) def=

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

          iso2_Init(B,A,Pks,SB,RB)
       /\ iso2_Resp(A,B,Pka,Pks,SA,RA)

end role
```

```
role environment() def=

  const  ctext1,ctext2 : text,
         ra            : protocol_id,
         a,b,i         : agent,
```

```
        pkb,pks,pki    : public_key

  intruder_knowledge={i,a,b,pks,pki,inv(pki),ctext1,ctext2,
                      {pki.i}_inv(pks)}

  composition

        session(a,b,pkb,pks)
     /\ session(a,i,pki,pks)
     /\ session(i,b,pkb,pks)

end role
```

```
goal

   %ISO2_Init  authenticates ISO2_Resp on ra
   authentication_on ra

end goal
```

```
environment()
```

References

[CJ] J. Clark and J. Jacob. A Survey of Authentication Protocol Literature: Version 1.0, 17. Nov. 1997. URL: www.cs.york.ac.uk/~jac/papers/drareview.ps.gz.

[ISO97] ISO/IEC. ISO/IEC 9798-3: Information technology - Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques, 1997.