ISO1 Public Key Unilateral Authentication Protocol

one-pass unilateral authentication

Protocol Purpose

A client authenticates himself to a server by sending a digital signature.

```
  const ctext    : text,
        a, b     : agent,
        pka, pks : public_key

  intruder_knowledge={a,b,pks,pka}

  composition

        session(a,b,pka,pks)
     /\ session(a,b,pka,pks)

end role
```

```
goal

   %ISO1_Resp authenticates ISO1_Init on na
   authentication_on na

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.