SPKM-LIPKEY

Known initiator

Protocol Purpose

Provide a secure channel between a client and server, authenticating the client with a password, and a server with a public key certificate.

Definition Reference

RFC 2847, http://www.faqs.org/rfcs/rfc2847.html

Model Authors

-

Further Notes

1. State = 0 /\ RCV(start) =|>
   State’:= 1 /\ Na’ := new()St Na’ :neXSt()

```
transition

1. State  = 0 /\ RCV(A.S.Na'.Y'.{A.S.Na'.Y'}_inv(Ka)) =|>
   State':= 1 /\ Nb' := new()
              /\ Rnumber2' := new()
              /\ SND(A.S.Na'.Nb'.exp(G,Rnumber2').
                     {A.S.Na'.Nb'.exp(G,Rnumber2')}_inv(Ks))
              /\ Keycompleted'=exp(Y',Rnumber2')
              /\ secret(Login(A,S),sec_t_Log,{A})
              /\ secret(Pwd(A,S),  sec_t_Pwd,{A})
              /\ witness(S,A,ktrgtint,Keycompleted')
```

References