```
      Cert   : message

  const secx   : protocol_id

  init   State := 0

  accept State = 1

  transition

   1. State = 0
      /\ Rcv(B.Nb'.PKb'.Cert')
      /\ Cert' = {B.PKb'}_inv(PKs)
      =|>
      State'=1
      /\ X' := new()
      /\ Snd({X'}_PKb'.{Nb'.M.SCm}_X')
      /\ secret(X',secx,{B,M})
      /\ witness(M,B,x,X')

end role
```
