```
/\ RCV(start)
=|>
State' := 2
/\ Na' := new()
/\ Pa' := new()
```

```
role bob(A, B : agent,
         H, PRF, KeyGen: function,
         Kb, Ks: public_key,
         SND, RCV: channel (di))
plaied_by B
def=

   local Na, Nb, Sid, Pa, PMS: text,
         State: nat,
         Ka: public_key

   init  State := 1

   transition

   1.  State = 1
```

```
role session(A,B: agent,
             Ka, Kb, Ks: public_key,
             H, PRF, KeyGen: function)
def=
```

```
        authentication_on na_nb2
end goal
```

```
environment()
```

References

[DA99]

T. Dierks and C. Allen. RFC 2246: The TLS Protocol Version 1.0, January 1999. Status:

Pn9]

CnCelnduaoinys is.ncle