[redacted]

$$A \rightarrow B : \{A, \{N_a\}_K^s\}_{pub(B)}^a$$
$$B \rightarrow A : \{B, N_b\}_{pub(A)}^a$$
$$A \rightarrow B : \{K, N_b\}_{pub(B)}^a$$
$$B \rightarrow A : \{N_a\}_{pub(A)}^a$$

Initial knowledge: We suppose that agents A and B initially know public keys $pub(C)$ of agent C, for any agent C.

Data generated during the protocol:

- N_a is a nonce generated by A.
- K is a symmetric key generated by A for further communications with B.
- N_b is a nonce generated by B.

Protocol description:

- **Step 1**
  - Alice starts the protocol by sending her identity A together with a freshly generated random number N_a encrypted with the freshly generated symmetric key K. This message is encrypted using an asymmetric encryption algorithm with B's public key (denoted $pub(B)$). We suppose that only agent Bob (whose identity is B) knows the secret key corresponding to $pub(B)$.
- **Step 2**
  - Bob receives the message $\{A, \{N_a\}_K^s\}_{pub(B)}^a$ sent by Alice.
  - Using his private key, Bob decrypts the message and retains $\{N_a\}_K^s$.
  - He sends his identity B together with a freshly generated nonce N_b encrypted with A's public key ($pub(A)$) to Alice.
- **Step 3**
  - Alice receives the message $\{B, N_b\}_{pub(A)}^a$.
  - Using her private key, Alice decrypts the message, checks that it includes Bob's identity B, and extracts N_b.
  - She sends the symmetric key K together with N_b encrypted with B's public key ($pub(B)$) to Bob.
- **Step 4**
  - Bob receives the message $\{K, N_b\}_{pub(B)}^a$.
  - He decrypts the message and checks that the nonce N_b corresponds to the nonce previously generated and sent to Alice.
  - He then uses the key K to decrypt $\{N_a\}_K^s$ (which he had previously received in **Step 2**) and get N_a. He then sends N_a encrypted with A's public key ($pub(A)$) to Alice.
- **Step 5**
  - Upon reception of this message, Alice decrypts it and checks that the nonce corresponds to the one she had previously generated. This way, Alice confirms that Bob actually knows the key and was able to decrypt $\{N_a\}_K^s$.

Security properties:

- *Authentication*:
  - When Bob receives the third message ($\{K, N_b\}_{pub(B)}^a$), he knows that the message comes from Alice, because only Alice could decrypt $\{B, N_b\}_{pub(A)}^a$ and obtain N_b;

- When Alice receives the fourth message ($\{N_a\}^a_{pub(A)}$), she knows that the message comes from Bob, because only Bob could decrypt $\{K, N_b\}^a_{pub(B)}$, obtain the key K, and decrypt $\{N_a\}^s_K$.

- *Confidentiality*:
  - The key K is transferred in **Step 3**, after the identity of Bob has been confirmed to Alice. Thus, it remains secret from an attacker that tries to impersonate Alice;
  - In the absence of an active attacker, N_b, K and N_a are only known by Alice and Bob.

Cost:
65 + 54 + 54 + 3 = 176
1st message: 1 + (50 + 1 + (10 + 1 +1)) + 1 = 65
2nd message: 1 + (50 + 1 + 1) + 1 = 54
3rd message: 1 + (50 + 1 + 1) + 1 = 54
4th message: 1 + 1 + 1 = 3