Alice   **Bob**

1. Alice generates a new public key-private key pair, (PK_A, SK_A)

2. PK_A →

3. Bob generates a new public key-private key pair, (PK_B, SK_B)

4. PK_B ←

5. Bob encrypts facial recognition parameters for his face, F_B and a current time stamp, T_B, with Alice's public key
$M_1 = E(PK_A, F_B \mathbin{\|} T_B)$

6. M_1 ←

7. Alice computes $F_B = D(SK_A, M_1)$

8. Alice encrypts facial recognition parameters for her face, F_A and a current time stamp, T_A, with Bob's public key
$M_2 = E(PK_B, F_A \mathbin{\|} T_A)$

9. M_2 →

10. Bob computes $F_A = D(SK_B, M_2)$

11. Bob computes Alice's location, L_A from the channel state information obtained from the transmission signal in step 8

12. Alice computes Bob's location, L_B from the channel state information obtained from the transmission signal in step 6

13. Bob runs a facial recognition model on any faces adjacent to location L_A, to identify Alice's face

14. Alice runs a facial recognition model on any faces adjacent to location L_B, to identify Bob's face

15. Bob visually verifies that the face selected by the protocol is Alice's

16. Alice visually verifies that the face selected by the protocol is Bob's

17. Alice and Bob have authenticated each other's signals and can establish secure communications