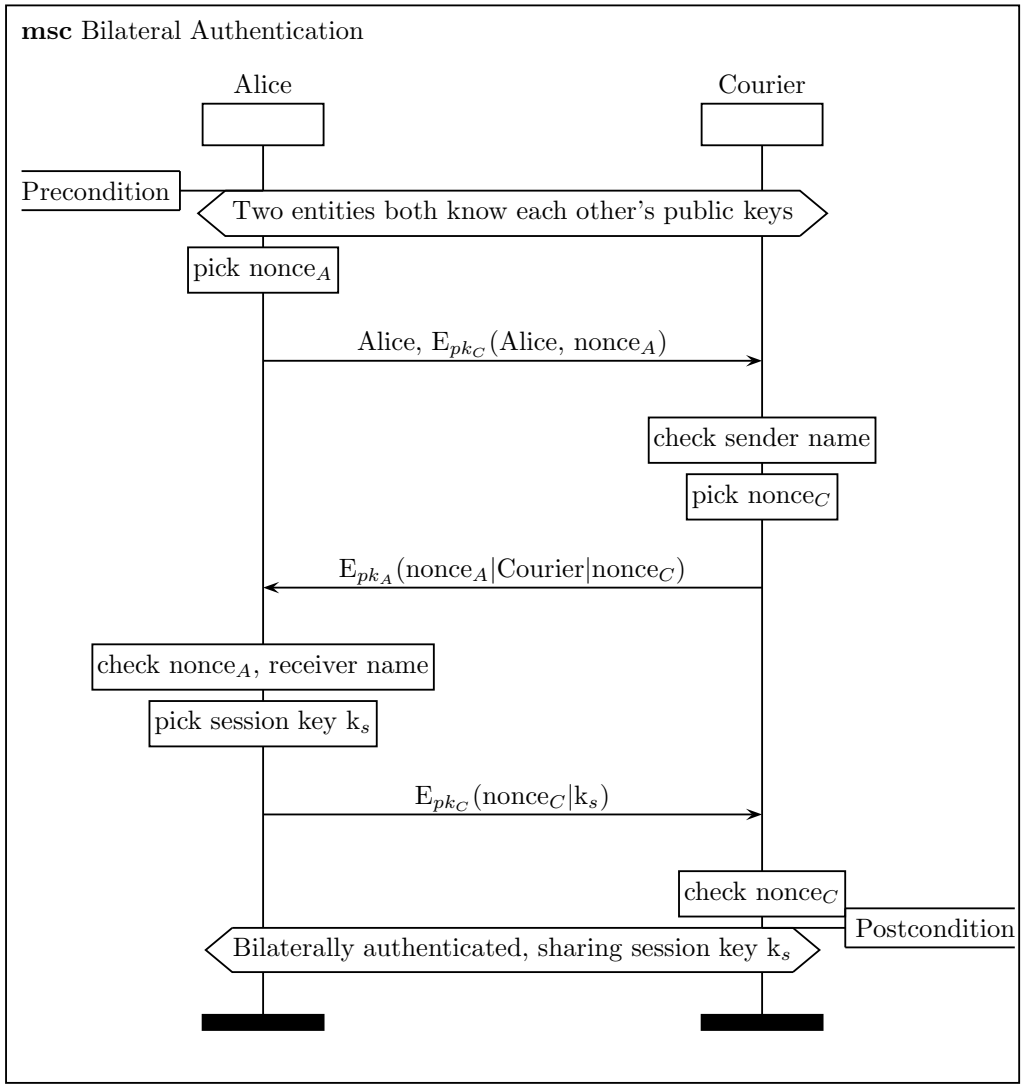
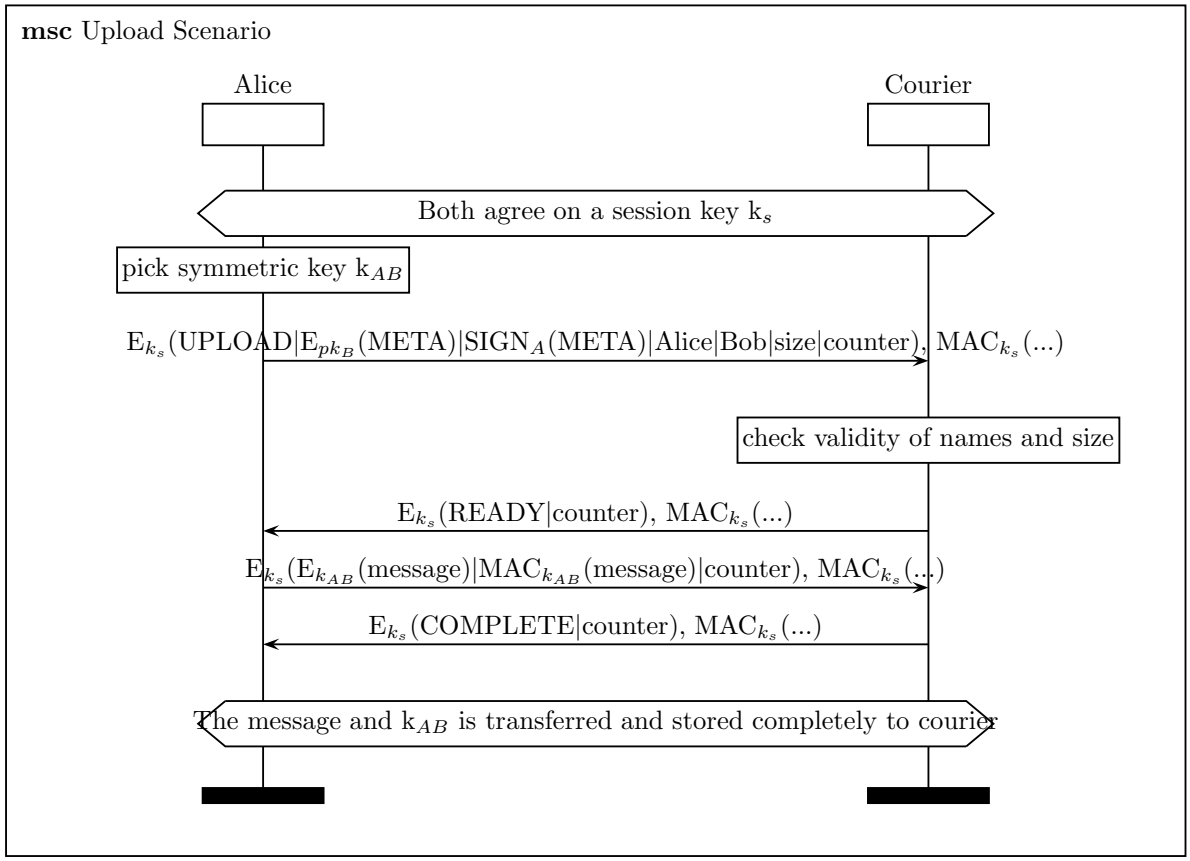
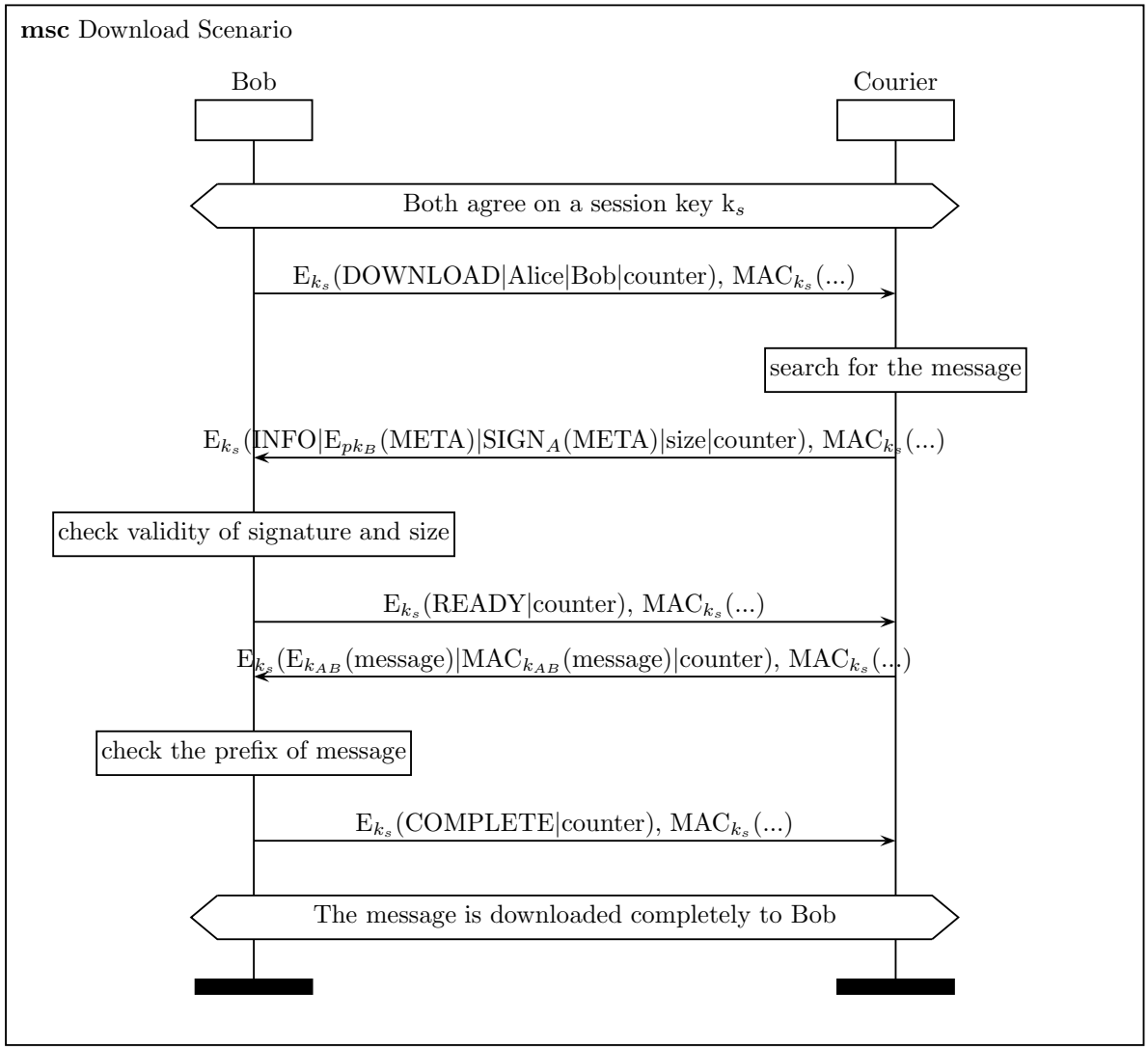

msc Bilateral Authentication
Alice
Courier
Precondition
Two entities both know each other's public keys
pick nonce$_A$
Alice, E$_{pk_C}$(Alice, nonce$_A$)
check sender name
pick nonce$_C$
E$_{pk_A}$(nonce$_A$|Courier|nonce$_C$)
check nonce$_A$, receiver name
pick session key k$_s$
E$_{pk_C}$(nonce$_C$|k$_s$)
check nonce$_C$
Postcondition
Bilaterally authenticated, sharing session key k$_s$



Where META = (k_{AB}|timestamp)



Where META = (k_{AB}|timestamp)