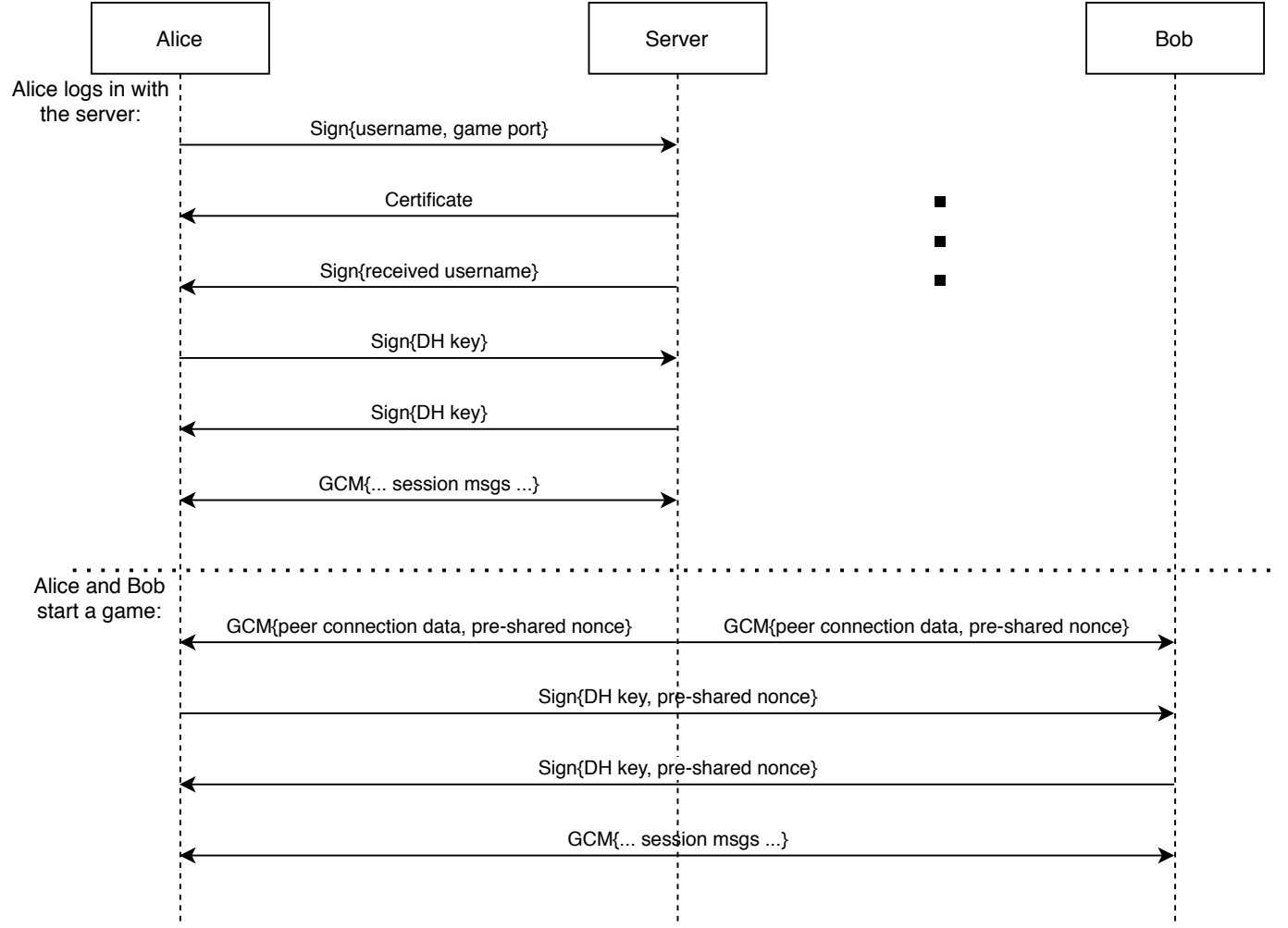
Alice
Server
Bob
Alice logs in with the server:
Sign{username, game port}
Certificate
Sign{received username}
Sign{DH key}
Sign{DH key}
GCM{... session msgs ...}
Alice and Bob start a game:
GCM{peer connection data, pre-shared nonce}
GCM{peer connection data, pre-shared nonce}
Sign{DH key, pre-shared nonce}
Sign{DH key, pre-shared nonce}
GCM{... session msgs ...}