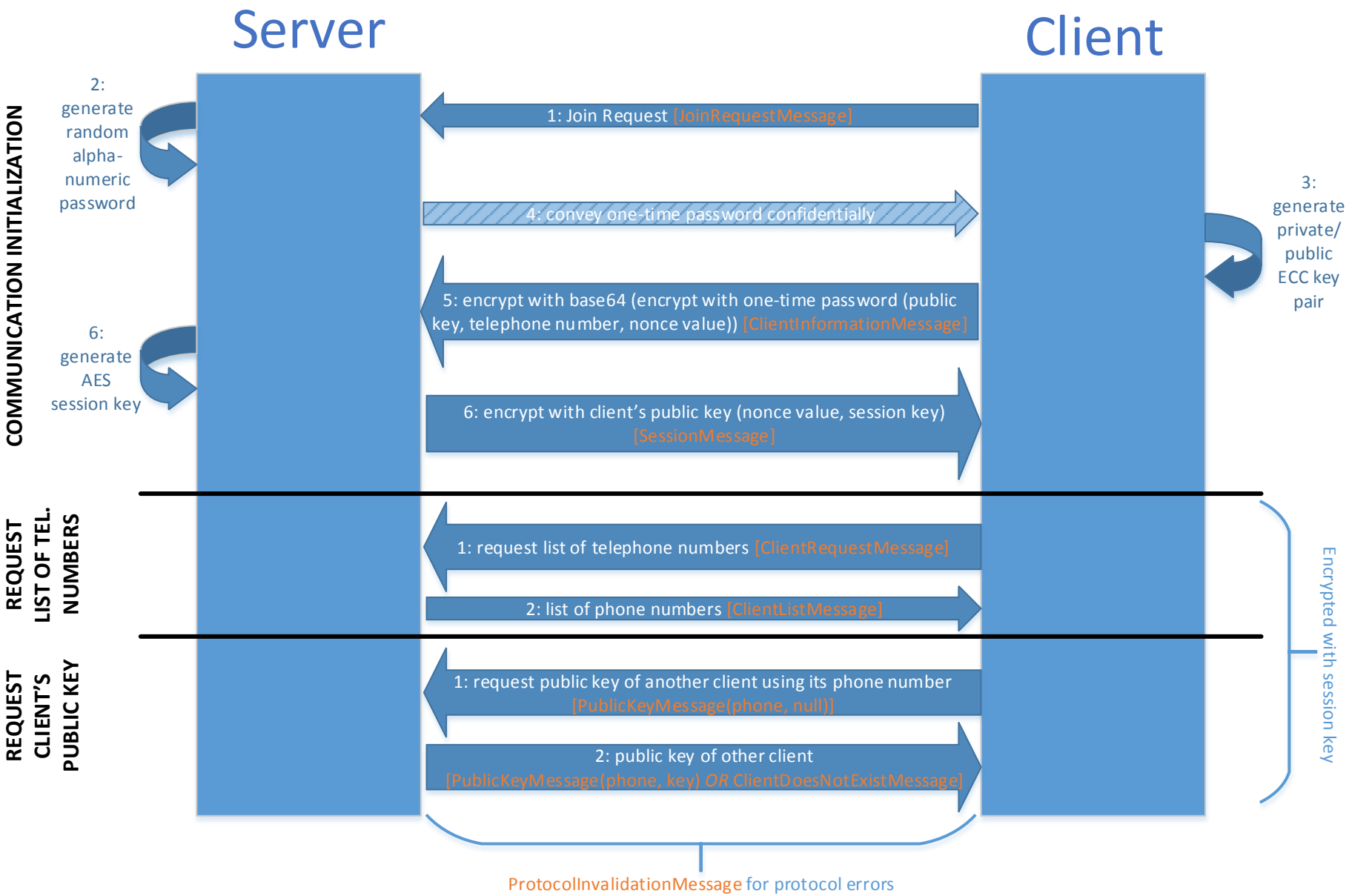
Server
Client
COMMUNICATION INITIALIZATION
2: generate random alpha-numeric password
1: Join Request [JoinRequestMessage]
4: convey one-time password confidentially
3: generate private/ public ECC key pair
5: encrypt with base64 (encrypt with one-time password (public key, telephone number, nonce value)) [ClientInformationMessage]
6: generate AES session key
6: encrypt with client's public key (nonce value, session key) [SessionMessage]
REQUEST LIST OF TEL. NUMBERS
1: request list of telephone numbers [ClientRequestMessage]
2: list of phone numbers [ClientListMessage]
REQUEST CLIENT'S PUBLIC KEY
1: request public key of another client using its phone number [PublicKeyMessage(phone, null)]
2: public key of other client [PublicKeyMessage(phone, key) OR ClientDoesNotExistMessage]
Encrypted with session key
ProtocolInvalidationMessage for protocol errors