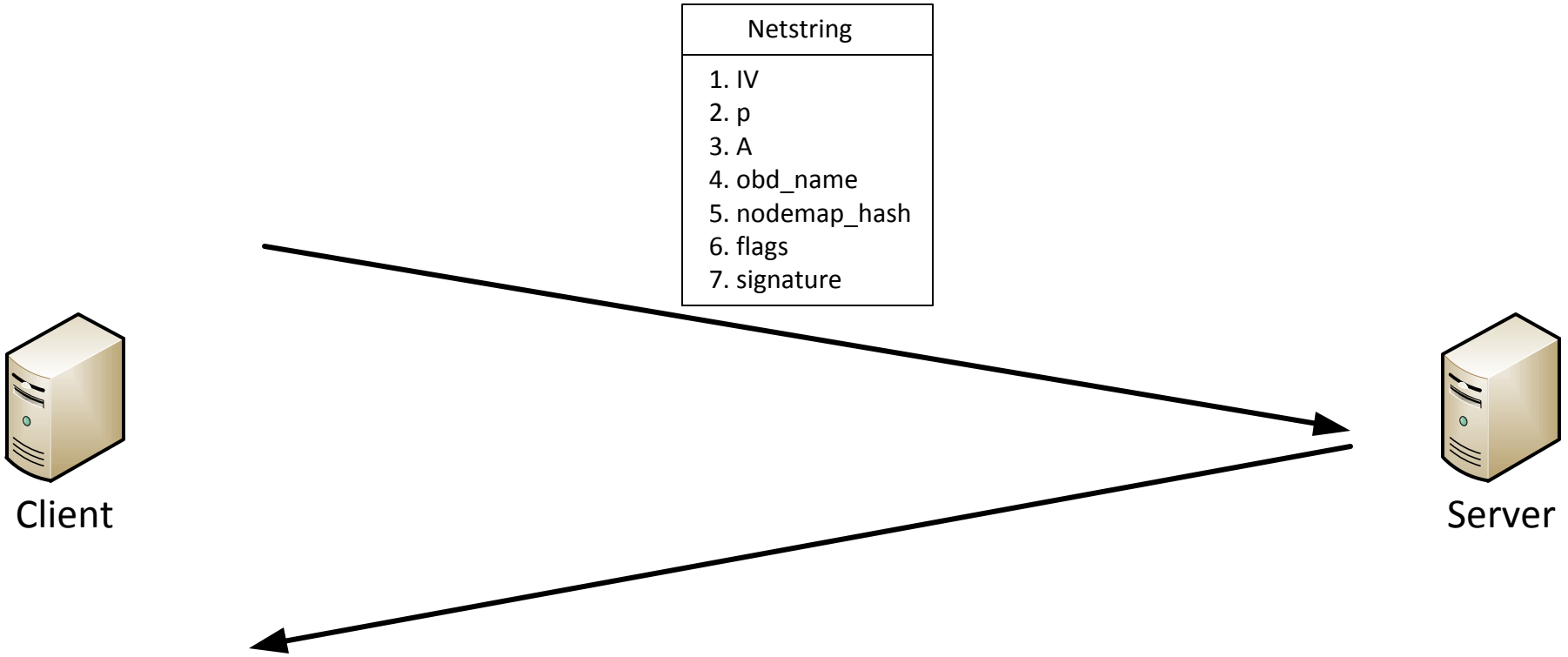
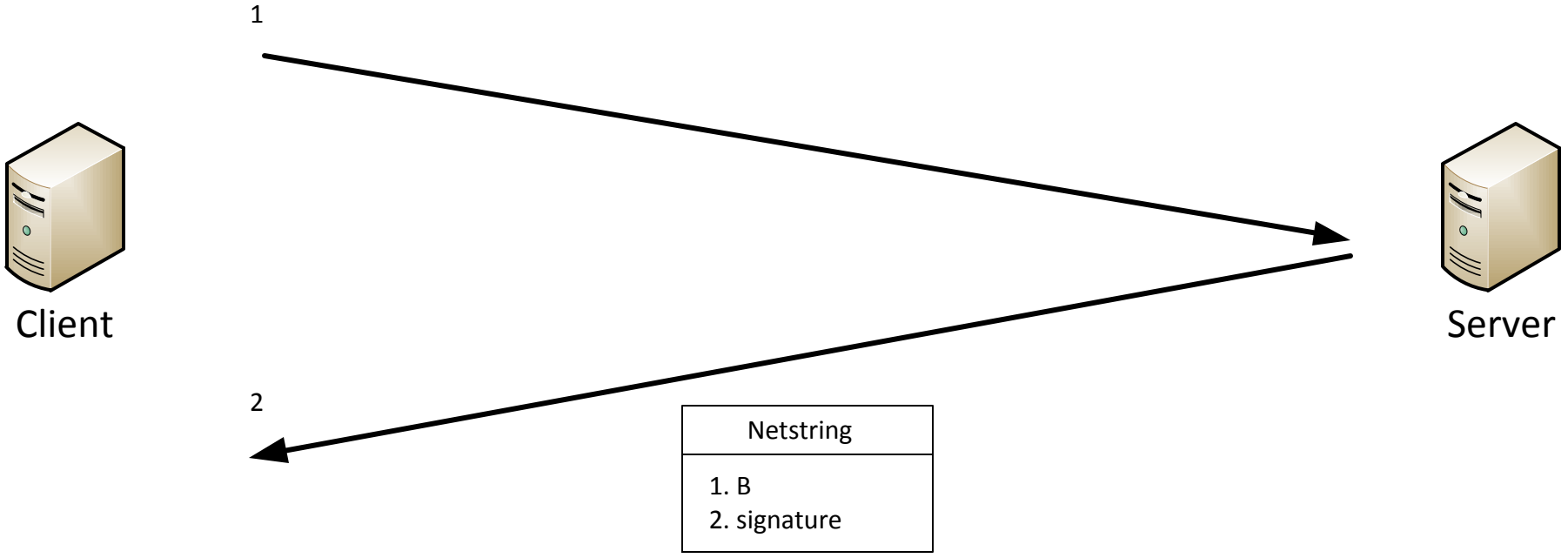
SEC_CTX_INIT RPC (skpi)



1. Client (initiator) sends a netstring of the following parameters to the server

IV:	Initialization vector (random 8 byte array) generated by the client
p:	Large prime of size greater to or equal then size specified in shared key file
A:	g^a mod p (initiator key for DHKE)
obd_name:	Lustre target OBD name
nodemap_hash:	SHA256(nodemap name), uses nodemap from shared key file
flags:	Lustre related security flags
signature:	HMAC_SHA256(key, msg) where shared key is the key and parameters is msg

SEC_CTX_INIT RPC (skpi)



2. Server (responder) verifies the signature from the client
3. Server verifies the nodemap_hash is correct
4. Server sends back a netstring with it's public key and a signature

B: g^b mod p (responder key for DHKE)
signature: HMAC_SHA256(key, msg) where shared key is the key and parameters is msg

SEC_CTX_INIT RPC (skpi)

Client

Server

$$S = B^a \pmod{p}$$

$$S = A^b \pmod{p}$$

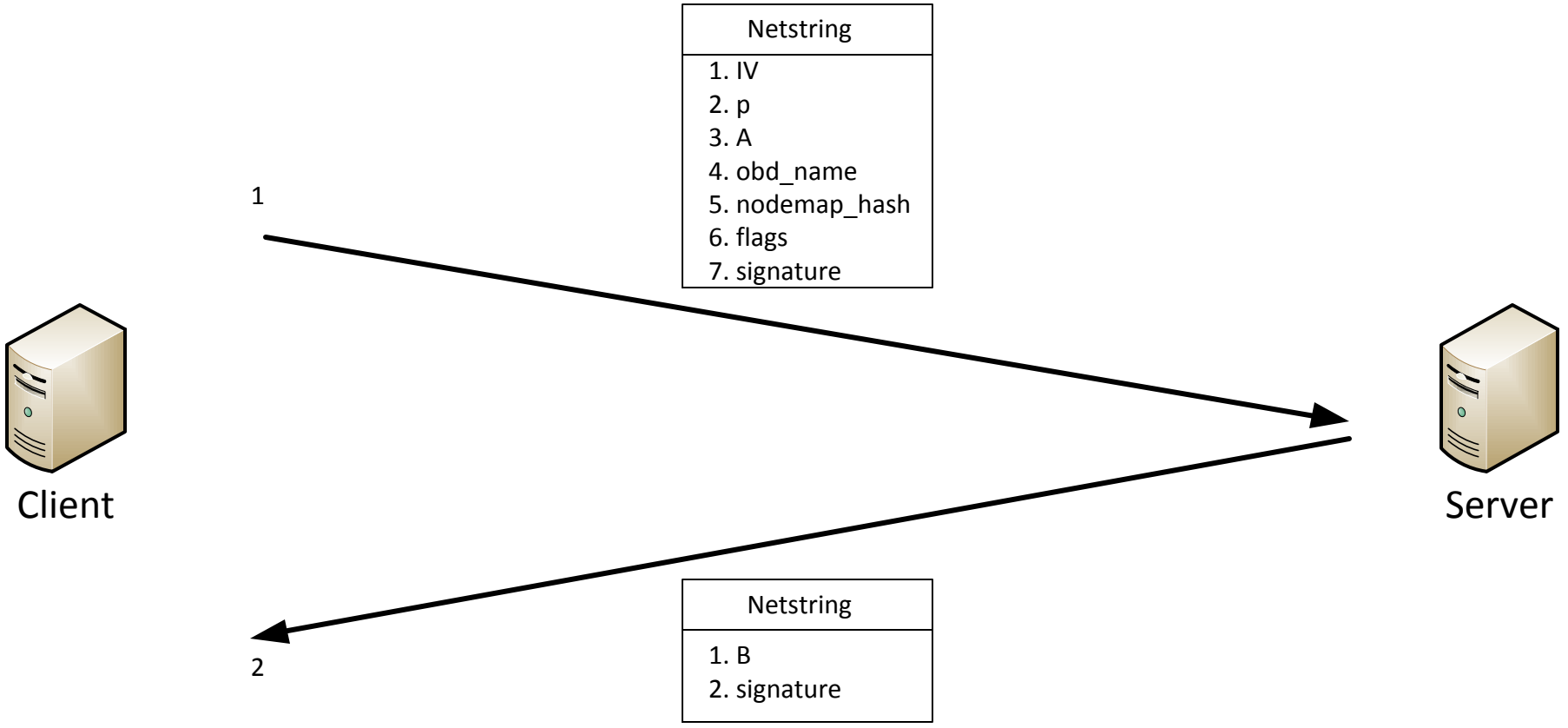
$$SessionKey = HMAC(SharedKey, Counter \,||\, S \,||\, ClientNID \,||\, KeyBindingInfo)$$

5. The Key derivation function calculates the session key for both the client and server. It uses the HMAC version specified NIST Special Publication SP 800-56B Rev 1 (Sep 2014) Section 5.5.1. The HMAC algorithm used is the one provided in the shared key file. The shared key is used as the key to the HMAC algorithm and the message is specified in OtherInfo.

S:	Computed public key from DHKE (Client: B^a mod p; Server: A^b mod p)
K**DF**:	Key derivation function
counter:	Counter starting at 0 used in session key construction
HMAC:	HMAC(key, msg) using HMAC algorithm specified in the shared key file, where key is the shared key and msg is Otherinfo
OtherInfo:	Concatenation of the following bytes: Counter, S, Client NID, Key Binding Info
Key Binding Info:	Is the client's netstring from page 1
Session key:	Session key KDF(shared key, OtherInfo)

* The || is the concatenation of multiple buffers

SEC_CTX_INIT RPC (ski)



IV: Unused 0 byte value
p: Unused 0 byte value
A: Unused 0 byte value
B: Unused 0 byte value
obd_name: Lustre target OBD name
nodemap_hash: sha256(nodemap name), uses nodemap from shared key file
flags: Lustre related security flags
signature: HMAC_SHA256(shared key, parameters)