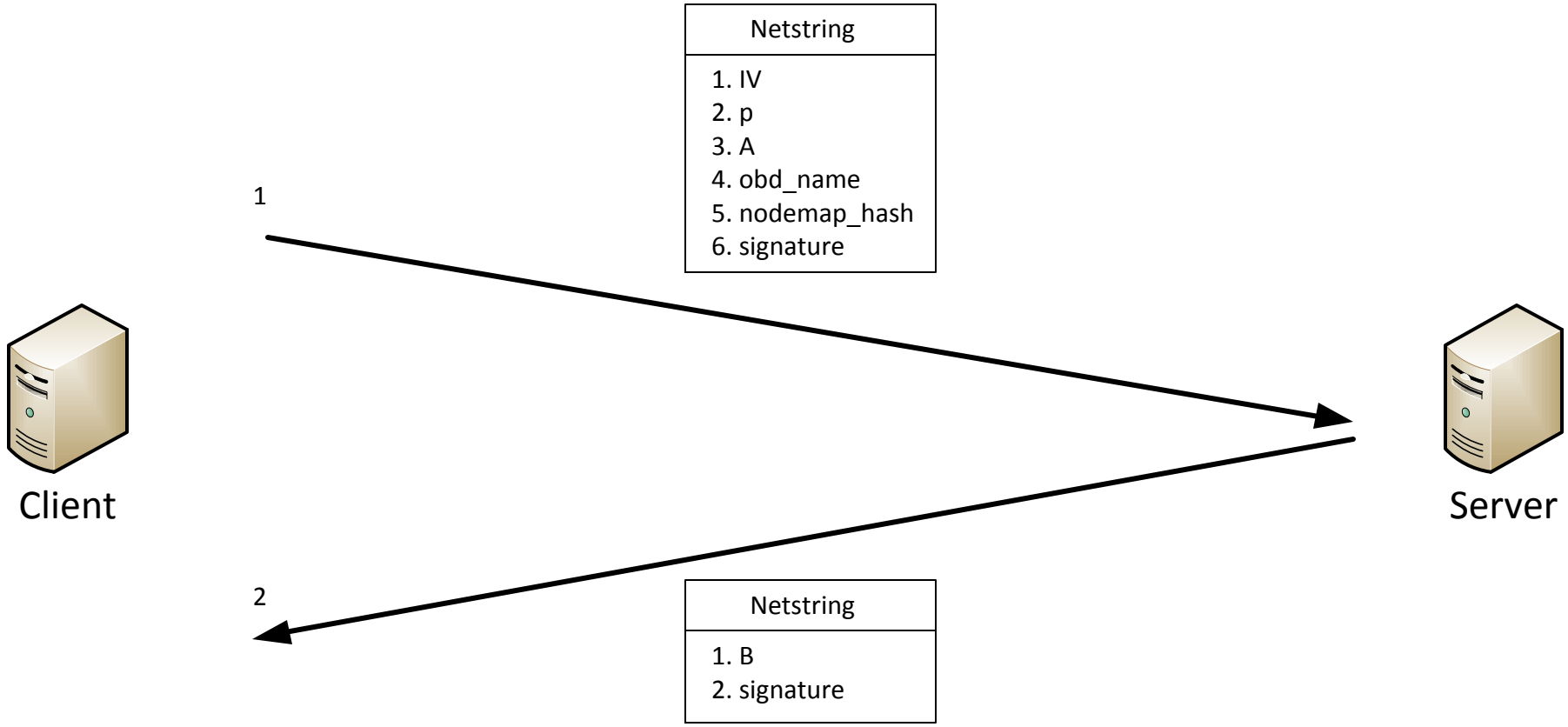
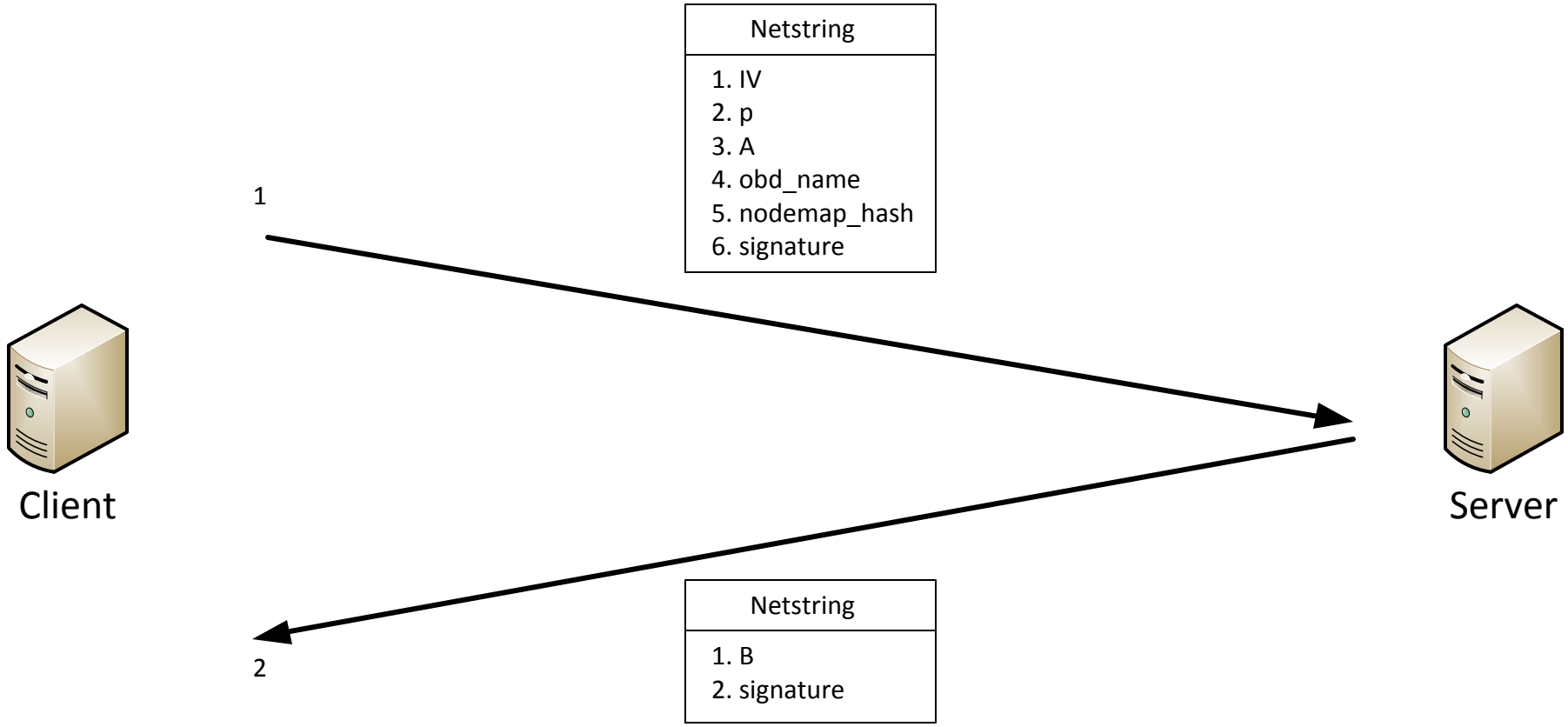
SEC_CTX_INIT RPC (skpi)



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)
B:	g^b mod p (responder key for DHKE)
obd_name:	Lustre target OBD name
nodemap_hash:	sha256(nodemap name), uses nodemap from shared key file
signature:	HMAC_SHA256(shared key, parameters)
g:	generator which is always 2 for Lustre
s:	Computed public key from DHKE (Client: B^a mod p; Server: A^b mod p)
Session key:	Session key KDF(shared key, otherinfo)
KDF:	Key Derivation Function from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br1.pdf page 58. KDF with use HMAC algorithm specified in shared key file and salt
salt:	Byte string combination of (Client NID || IV || Server NID || obd_name) this may require additional parameters to netstring above.

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
signature:	HMAC_SHA256(shared key, parameters)