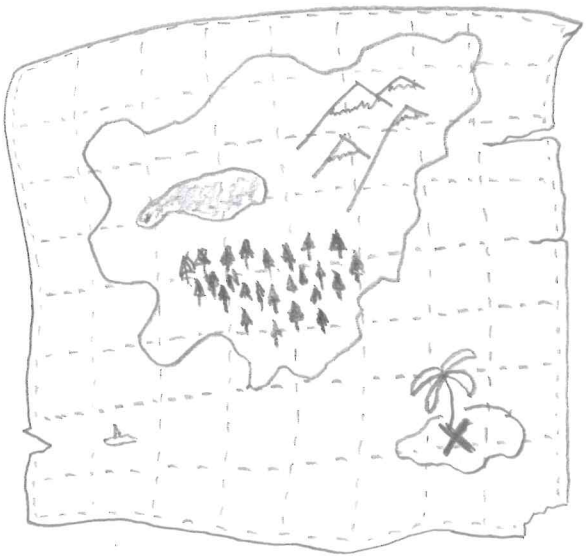
YOU ASK DNS



Client Hello:

Protocol Version

Session ID

Cipher suite

Compression method

Server Hello:

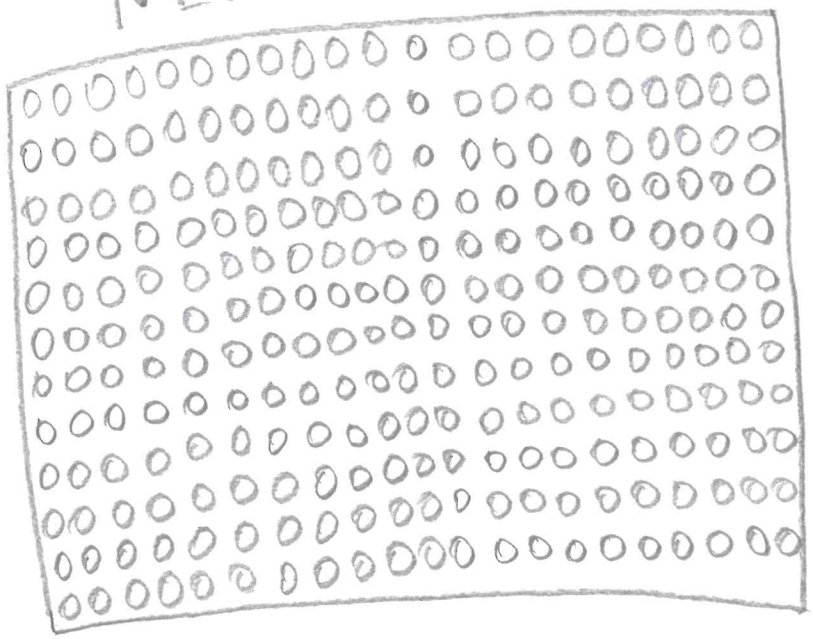
Server certificate

key Exchange method → RSA

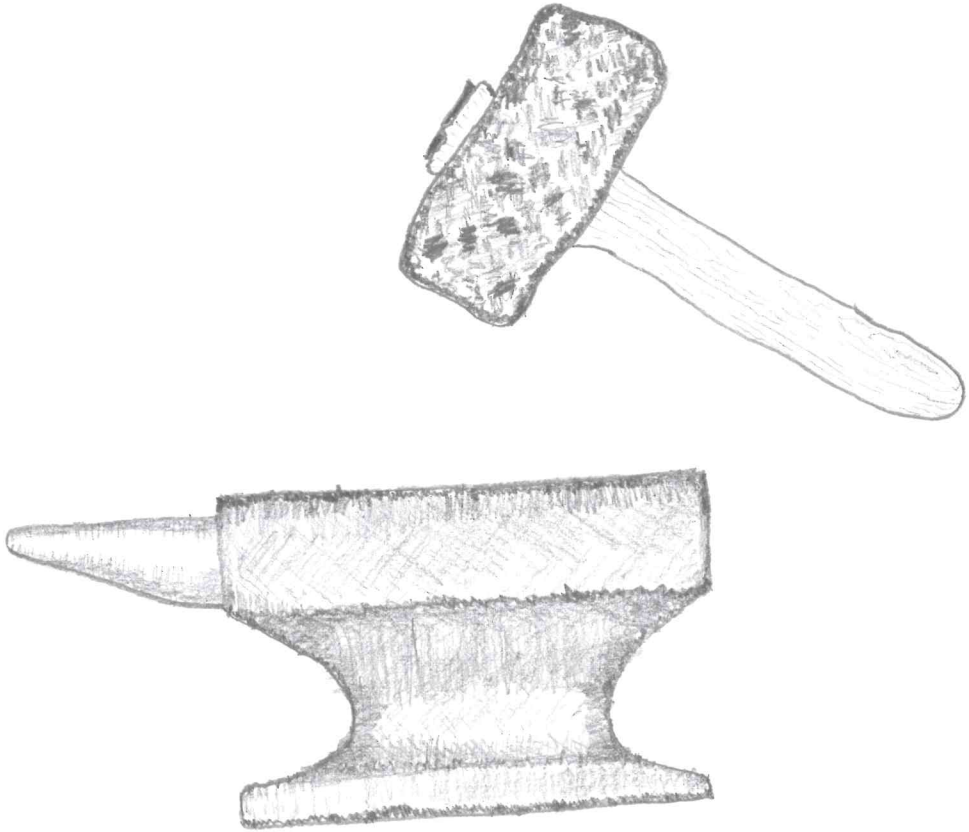
key Exchange method → Diffie Hellman

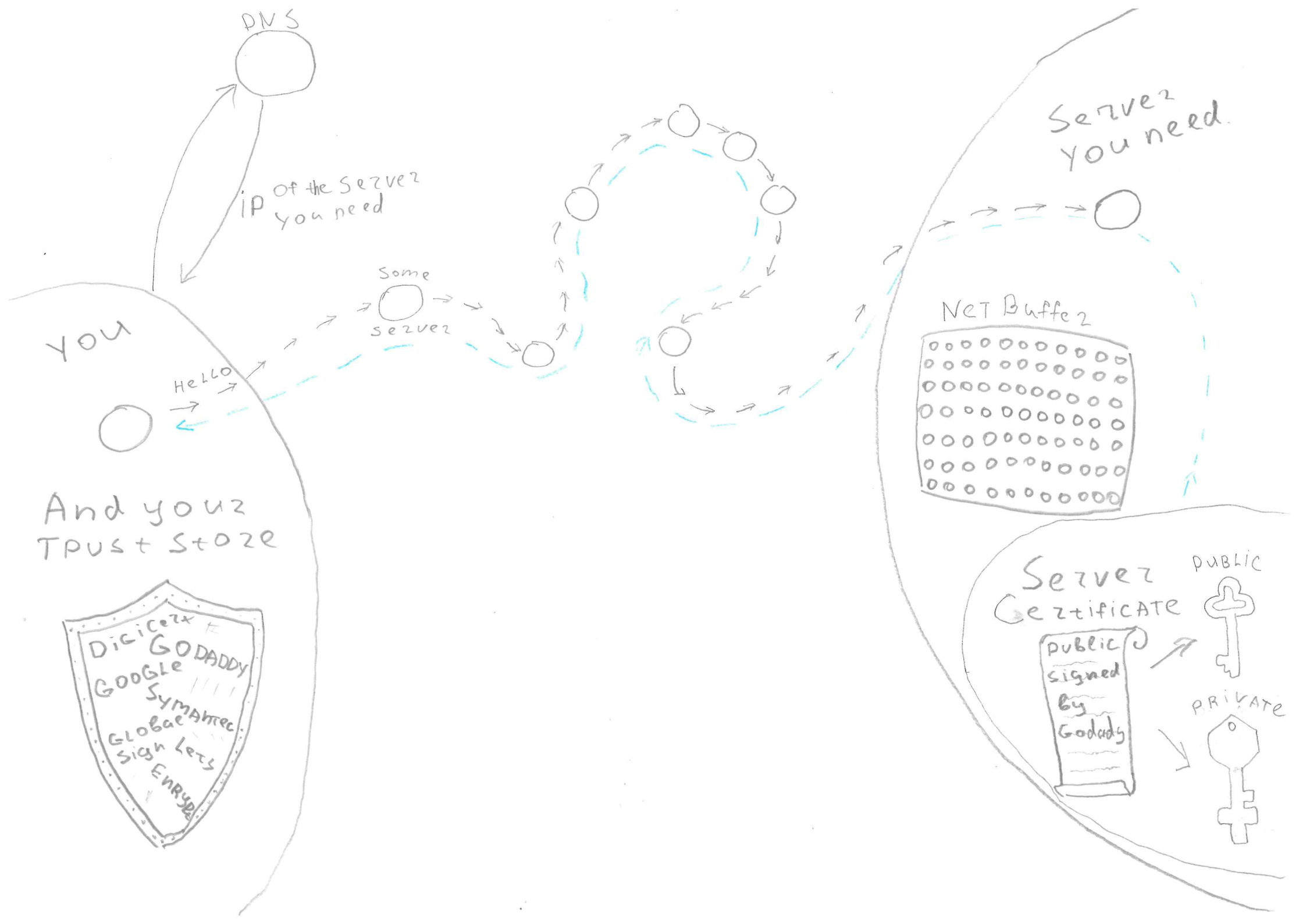
TLS Handshake done.

NET Buffer

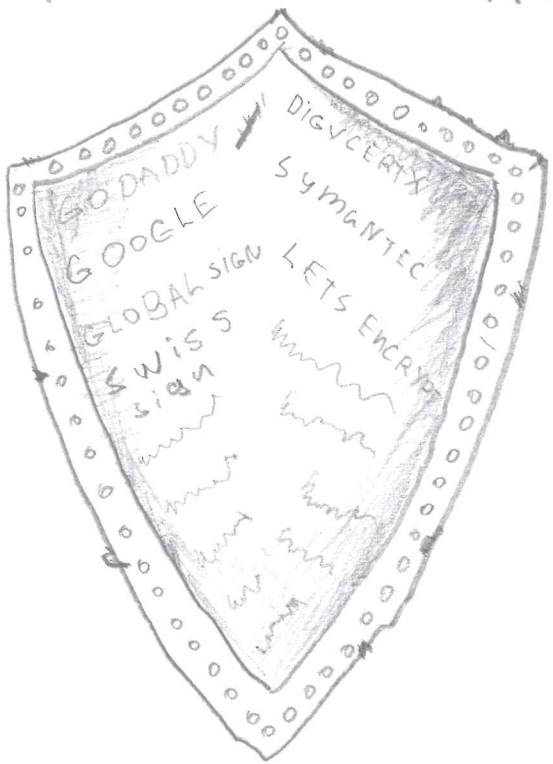


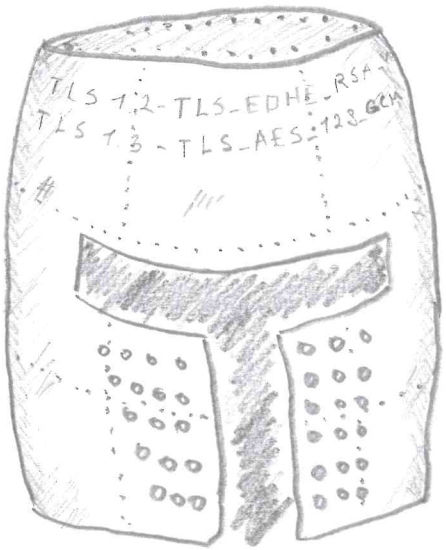
Now we need to forge keys

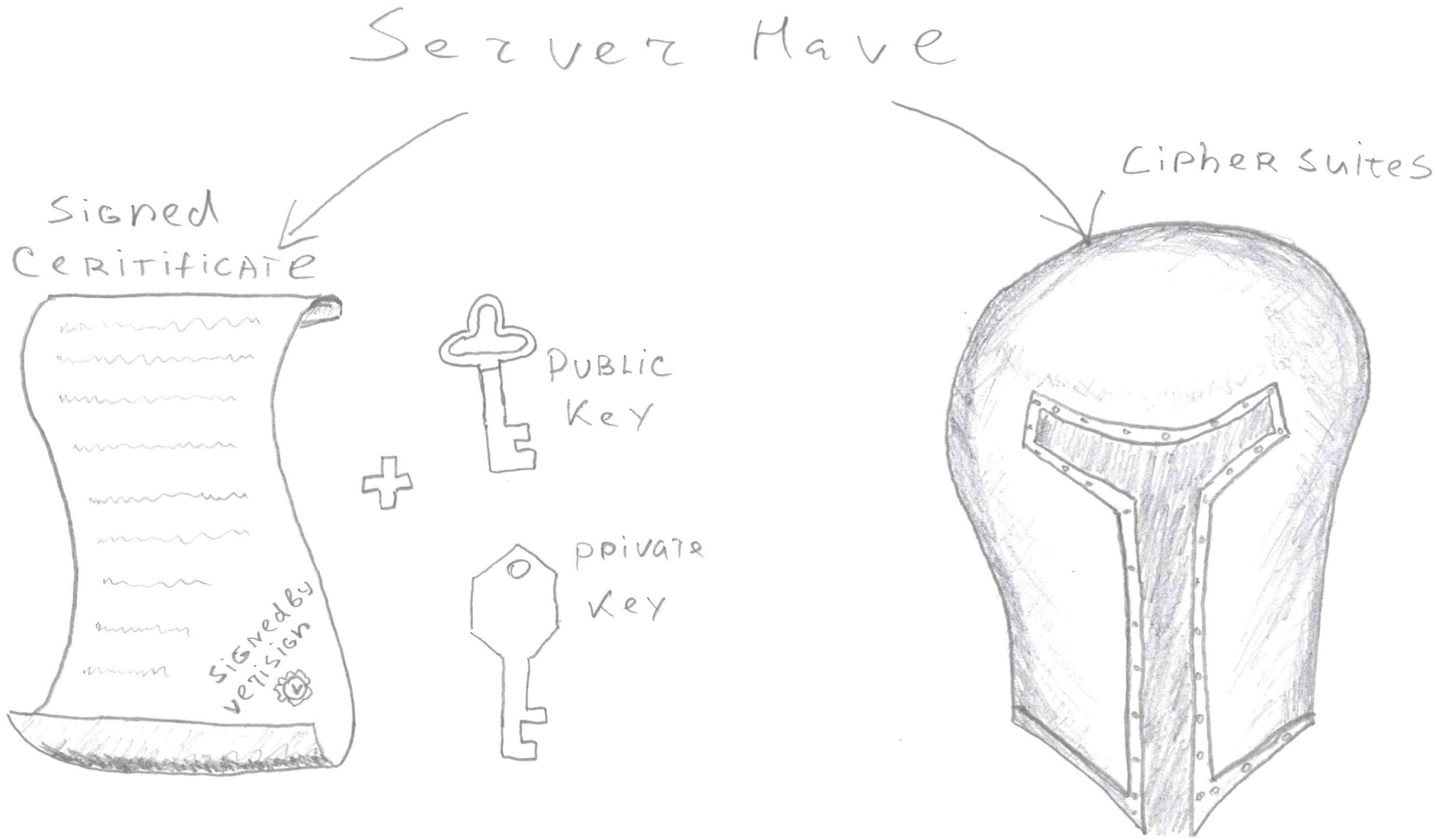


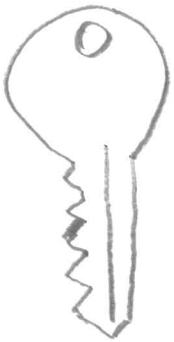

DNS
IP of the server you need
Some server
you
Hello
And your Trust Store
DigiCert
GODADDY
Google
Symantec
Global Sign
Let's Encrypt
Server you need
Net Buffer
Server Certificate
public signed by Godady
PUBLIC
PRIVATE

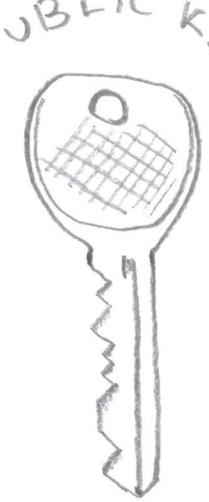
You have

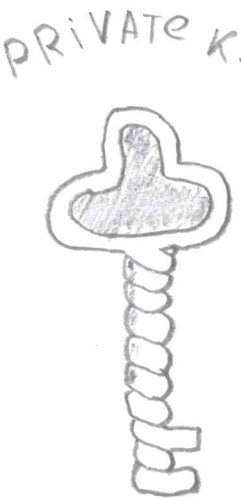

TRUST STORE
GODADDY
DIGICERT
GOOGLE
SYMANTEC
GLOBALSIGN
LETS ENCRYPT
SWISS SIGN


CIPHERSUITES
TLS 1.2 - TLS_EDHE_RSA
TLS 1.3 - TLS_AES_128_GCM


Server Have
Signed Ceritificate
Signed by verisign
PUBLIC Key
ppivate Key
Cipher Suites




PUBLIC KEY


PRIVATE KEY


SESSION OR
MASTER KEY
YK82