The following are command screenshot key generate by using openssl genpkey for bob and alice as example.

openssl genpkey -algorithm RSA -out alice-private-key.pem -aes256// generate private key for alice

openssl genpkey -algorithm RSA -out bob-private-key.pem -aes256//generate private key for bob

Extract public key for both from private key

openssl rsa -in alice-private-key.pem -out alice-public-key.pem –pubout

openssl rsa -in bob-private-key.pem -out bob-public-key.pem –pubout

Exchange public alice and bob

Ln –s /home/Desktop/alice/bob-publlic-key.pem

Ln –s /home/Desktop/bob/alice-publlic-key.pem

Let’s take one example message.txt <hello friend>

openssl rsautl -encrypt -inkey bob-public-key.pem -pubin -in message.txt -out message.enc

To decrypt the message using RSA, Bob can use his private key as follows:

openssl rsautl -decrypt -inkey bob\_private\_key.pem -in message.enc -out decrypted\_message.txt

RSA Signing using dgst:

To sign a message using OpenSSL, follow these steps:

Create a message in a file called message.txt<be secret>

Generate a SHA-256 hash of the message by typing the following command:

openssl dgst -sha256 -sign alice\_private\_key.pem -out signature.bin message.txt

To verify the signature, Bob can type the following command:

openssl dgst -sha256 -verify alice\_public\_key.pem -signature signature.bin message.txt

If the signature is valid, OpenSSL will output "Verified OK".

If Alice need a certificate, how She generate a certificate signing request and sends to the Certification Authority?

Generate a private key for Alice:

openssl genpkey -algorithm RSA -out alice\_private\_key.pem

Generate a CSR using the private key:

openssl req -new -key alice\_private\_key.pem -out alice.csr

Verify Bob's certificate using the CA's certificate:

openssl verify -CAfile ca.crt bob.crt

If the verification is successful, OpenSSL will output "OK".

Extract Bob's public key from his certificate:

openssl x509 -in bob.crt -pubkey -noout > bob\_public\_key.pem

This will extract Bob's public key from his certificate and save it in a file called bob\_public\_key.pem.

Alice can now use Bob's public key to encrypt messages to Bob or verify digital signatures from Bob.