## GENERATION OF KEYS

openssl genrsa -f4 -out private.txt 4096

openssl pkcs8 -topk8 -inform pem -in private.txt -outform PEM -nocrypt -out private8.txt

openssl rsa -in private.txt -outform PEM -pubout -out public.txt

## SIGN MESSAGE

The fixed message that you have to sign is : “MS-CLIENT V. 1.0”

Here are an example :

echo -n " MS-CLIENT V. 1.0" | openssl dgst -sha256 -sign private.txt -sigopt rsa\_padding\_mode:pss -sigopt rsa\_pss\_saltlen:-1 -hex

N. B. Two important things you have to send the “hex” of the signature, and you have to specify the “PSS” algorithm

## GENERATION OF COIN ADDRESS

On the blockchain we store the base64 of the public key so for making the calls you have to send to us the base64 of the content of file “public.txt”.

-----BEGIN PUBLIC KEY-----

MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA0rbUiQDYpEsxAJ6oZNxW

FhCwQxNFGvweQ19zF8W9qtqEb/c+2T579rrKdUt9ViGN/L/NE1DVsGWJjVplBzHS

/F994Gpt6dCqnt0mbS9FKFroiAz+zkNdP4oJKl9bhwB3tbA+5t2xgROCWURyunGX

naPwJqhYVyBCnktqa0AOJ3jNFC5iV9lVExV0EEVUGndqo6Y2cEtrCl79ZgHe30hf

u4yA7CE1UvdVCvvPxbXJGhgsmvTrvx5x8PZ4zHwT7/5vr0O12GuRe4WmkS+7ccvq

QBZuCPRT86M42h0UrWfUviU/hRQamRBPCQmhzLLXykf51K7y8BNW3+8qjzYGX27S

6YSoJo0/8ZLBzgQs557AvmvAWXi3XUpp7T3I14DL9dn4eNoU4Q6oXALAGzBQ453u

92VSB6xE/MmMw59adMMxweACMYsCMhLP0baZ0Ri+j7uKns1kYwVV3OOMJnA3fVgP

HhMSvE0F7rSEAW/CJ2p9BQ1Onn4Q0SKdXlolhek4xdGGiHe4XWvBS3yKStaYgB3J

JOqzh+nzoQX33/TYJr3Cj5+F8+sCP66joqsiGxnvVi2J7/waQq45VcexFor/Lc6n

skydNJf7hzW0C3zDPu64hQ/3SaBvPnPbjUvCHuYy/b4BHXwmLTHhCT+25WUyuekr

4l/3vOKK1Q9Do2QFvOX1F0UCAwEAAQ==

-----END PUBLIC KEY-----

Generated base64:



## SERVER CONFIGURATION

The server is running on the address : 174.138.12.115:8124

## READ BALANCE

For reading balance you have to send a get request with your address

Example :

<http://174.138.12.115:>=

## ASSIGN COIN

For assigning coins to a specific address you have to send a POST request to: http:// 174.138.12.115:8124/api/assignCoin

With this parameters (the body has to be x-www-form-urlencoded)

“Key” : “the baseof of your pub. key”

“amount” : “the amount of coins”

Example :

“key”:"",

“amount” : “80"

## SPEND COIN

For spends coins to a specific address you have to send a POST request to: http:// 174.138.12.115:8124/api/spendCoin

With this parameters (the body has to be x-www-form-urlencoded)

“key\_from” : “the baseof of your pub. key”

“key\_to” : “the new baseof addr.”

“amount” : “how many coins you want to spend”

“amount” : “signature”

Example :

“key\_from”:""

“key\_to”:“"

“amount” : "70"

“signature”:""