Banking Application using Public Key Infrastructure

Team 2

Aakash Bandari

Nima Aghli

Rahul Thawal

Soma Kiran Kumar Nellipudi

Sriteja Nallamilli

Problem Statement

Banking Application

❑ Client

❑ Server

❑ CA

Client

- Handles user registration and login.
- Sends deposit, withdrawal and balance enquiry requests.
- Signs request with private key of client and then encrypt it with server’s public key.

Server

- Receives the request from client decrypts message with private key of server then validates the message with public key of client .
- Run SQL queries in database for each requests from client.
- Answer balance enquiry and withdrawal requests after encrypting them with AES.

CA

- ❏ Providing client public key to server
- ❏ Providing server public key to client

Tools and Softwares used

❑ Java

❑ MySql

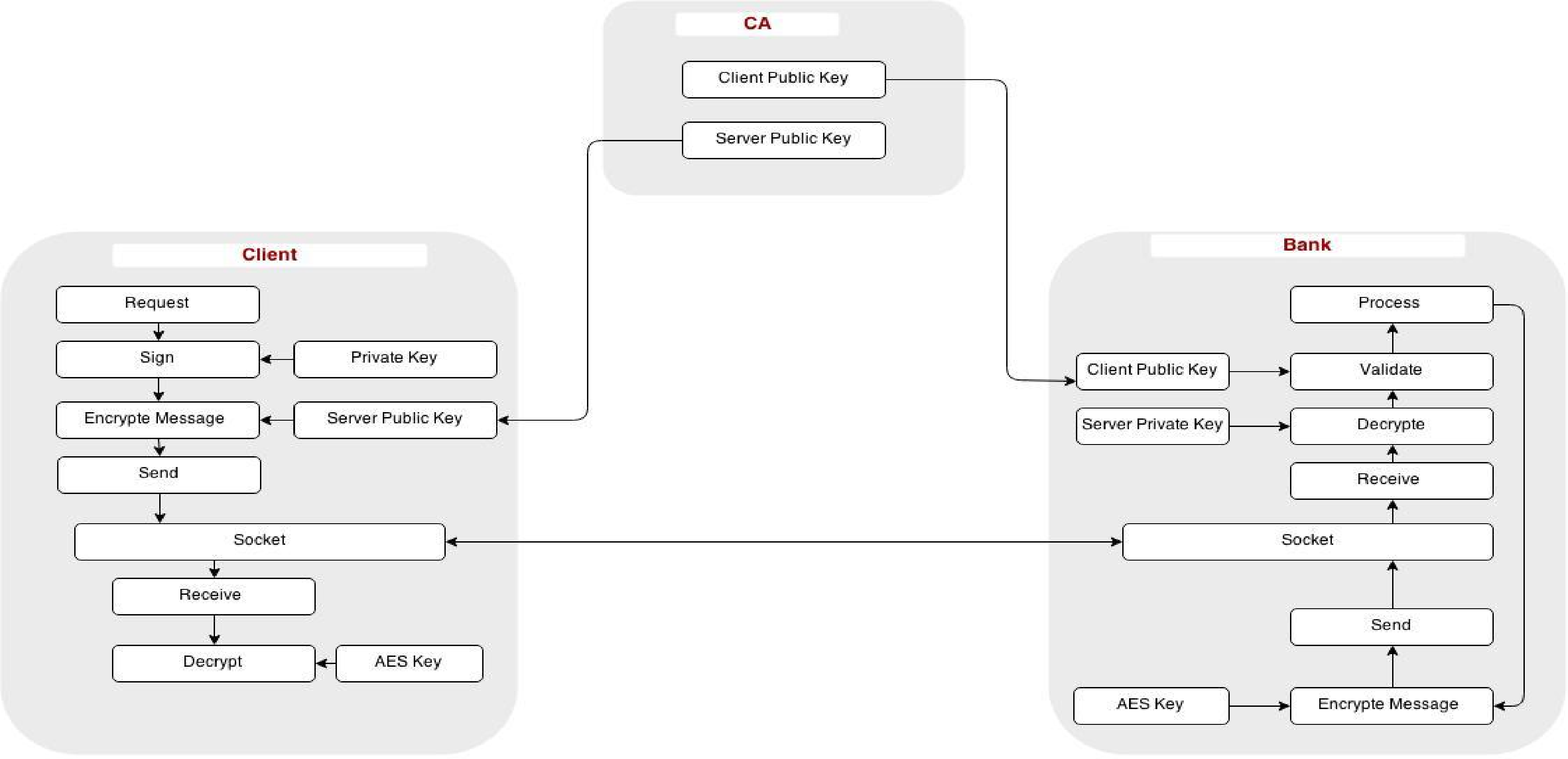
❑ Wireshark

Algorithms and Approach Used

- RSA to create public and private key.
- RSA with SHA1 for signature .
- AES

  Message encryption from server to client

Work Flow of the Application



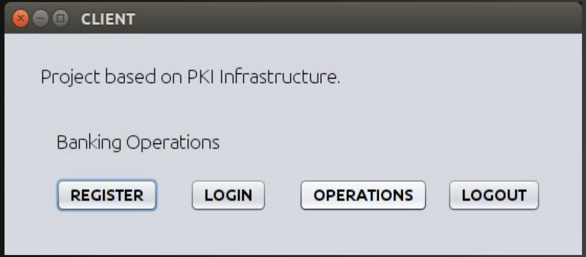
Confidentiality & Integrity.

Using Private key of client and public of server and encrypting both keys we ensure confidentiality.

Authentication

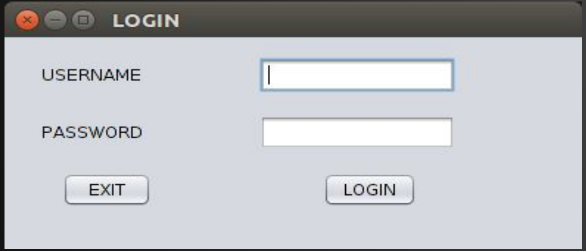
User need to login into system which would provide authentication.

Screenshots of the project



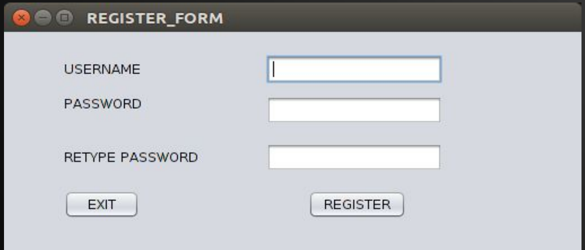
Project based on PKI Infrastructure.

Banking Operations



USERNAME

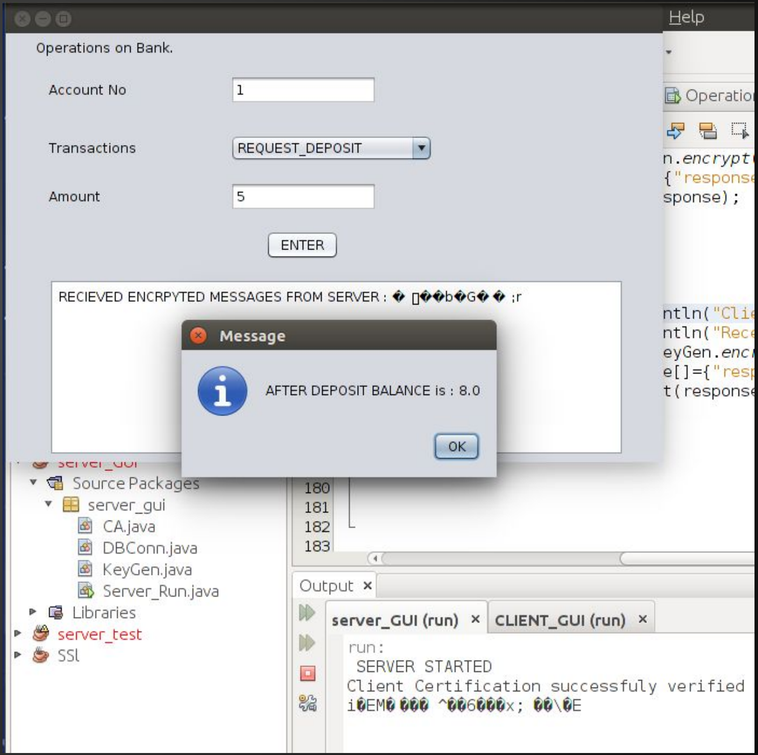
PASSWORD



USERNAME

PASSWORD

RETYPE PASSWORD



Operations on Bank.

Account No: 1

Transactions: REQUEST_DEPOSIT

Amount: 5

RECIEVED ENCRPYTED MESSAGES FROM SERVER : � ▯��b�G� � ;r

AFTER DEPOSIT BALANCE is : 8.0

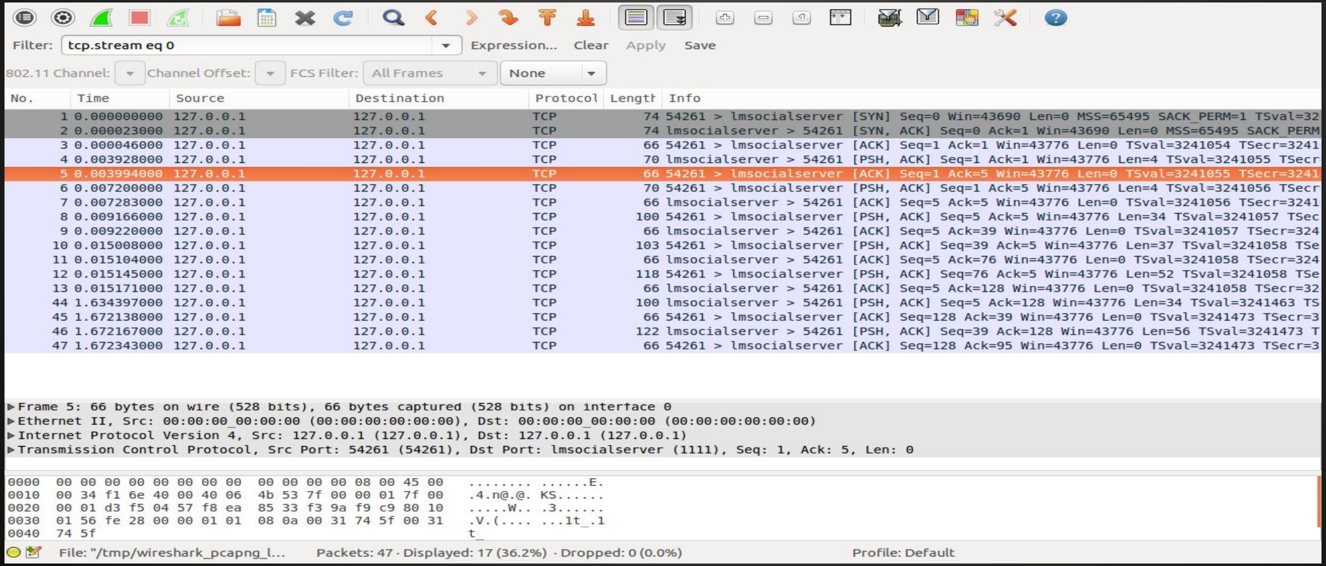
```
n.encrypt
{"response
sponse);

ntln("Clie
ntln("Rece
eyGen.enc
e[]={"resp
t(response
```

```
run:
 SERVER STARTED
Client Certification successfuly verified
i�EM� ��� ^��6���x; ��\�E
```

Network Traffic Monitor

- Wireshark is used to capture packet exchange between client and server .



Filter: tcp.stream eq 0

802.11 Channel: Channel Offset: FCS Filter: All Frames None

```
No.      Time          Source          Destination     Protocol Length Info
       1 0.000000000   127.0.0.1       127.0.0.1       TCP       74 54261 > lmsocialserver [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=1 TSval=32
       2 0.000023000   127.0.0.1       127.0.0.1       TCP       74 lmsocialserver > 54261 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495 SACK_PERM
       3 0.000046000   127.0.0.1       127.0.0.1       TCP       66 54261 > lmsocialserver [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=3241054 TSecr=3241
       4 0.003928000   127.0.0.1       127.0.0.1       TCP       70 lmsocialserver > 54261 [PSH, ACK] Seq=1 Ack=1 Win=43776 Len=4 TSval=3241055 TSecr
       5 0.003994000   127.0.0.1       127.0.0.1       TCP       66 54261 > lmsocialserver [ACK] Seq=1 Ack=5 Win=43776 Len=0 TSval=3241055 TSecr=3241
       6 0.007200000   127.0.0.1       127.0.0.1       TCP       70 54261 > lmsocialserver [PSH, ACK] Seq=1 Ack=5 Win=43776 Len=4 TSval=3241056 TSecr
       7 0.007283000   127.0.0.1       127.0.0.1       TCP       66 lmsocialserver > 54261 [ACK] Seq=5 Ack=5 Win=43776 Len=0 TSval=3241056 TSecr=3241
       8 0.009166000   127.0.0.1       127.0.0.1       TCP      100 54261 > lmsocialserver [PSH, ACK] Seq=5 Ack=5 Win=43776 Len=34 TSval=3241057 TSec
       9 0.009220000   127.0.0.1       127.0.0.1       TCP       66 lmsocialserver > 54261 [ACK] Seq=5 Ack=39 Win=43776 Len=0 TSval=3241057 TSecr=324
      10 0.015008000   127.0.0.1       127.0.0.1       TCP      103 54261 > lmsocialserver [PSH, ACK] Seq=39 Ack=5 Win=43776 Len=37 TSval=3241058 TSe
      11 0.015104000   127.0.0.1       127.0.0.1       TCP       66 lmsocialserver > 54261 [ACK] Seq=5 Ack=76 Win=43776 Len=0 TSval=3241058 TSecr=324
      12 0.015145000   127.0.0.1       127.0.0.1       TCP      118 54261 > lmsocialserver [PSH, ACK] Seq=76 Ack=5 Win=43776 Len=52 TSval=3241058 TSe
      13 0.015171000   127.0.0.1       127.0.0.1       TCP       66 lmsocialserver > 54261 [ACK] Seq=5 Ack=128 Win=43776 Len=0 TSval=3241058 TSecr=32
      44 1.634397000   127.0.0.1       127.0.0.1       TCP      100 lmsocialserver > 54261 [PSH, ACK] Seq=5 Ack=128 Win=43776 Len=34 TSval=3241463 TS
      45 1.672138000   127.0.0.1       127.0.0.1       TCP       66 54261 > lmsocialserver [ACK] Seq=128 Ack=39 Win=43776 Len=0 TSval=3241473 TSecr=3
      46 1.672167000   127.0.0.1       127.0.0.1       TCP      122 lmsocialserver > 54261 [PSH, ACK] Seq=39 Ack=128 Win=43776 Len=56 TSval=3241473 T
      47 1.672343000   127.0.0.1       127.0.0.1       TCP       66 54261 > lmsocialserver [ACK] Seq=128 Ack=95 Win=43776 Len=0 TSval=3241473 TSecr=3
```

```
▶Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▶Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
▶Transmission Control Protocol, Src Port: 54261 (54261), Dst Port: lmsocialserver (1111), Seq: 1, Ack: 5, Len: 0
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E.
0010  00 34 f1 6e 40 00 40 06  4b 53 7f 00 00 01 7f 00   .4.n@.@. KS......
0020  00 01 d3 f5 04 57 f8 ea  85 33 f3 9a f9 c9 80 10   .....W.. .3......
0030  01 56 fe 28 00 00 01 01  08 0a 00 31 74 5f 00 31   .V.(.... ...1t_.1
0040  74 5f                                              t_
```

File: "/tmp/wireshark_pcapng_l... Packets: 47 · Displayed: 17 (36.2%) · Dropped: 0 (0.0%) Profile: Default

Merits and Limitations

Merits

❏ Secured from Man in the middle attack.

Limitation

❏ Exposed to Replay attacks.

❏ The Project holds good only for the balance check. It can be implemented for further transactions as well.

❏ Requests between client and server is secured but sql requests sent from server to MySQL is vulnerable.

Thank You !!!