**Project no. 0: Certification Authority (CA)**

You are required to (a) build a CA, and (b) build clients that wish to confidentially send messages suitably encrypted with public key of receiver, but only after they know the other client’s public key in a secure manner.

There are two ways for client A to know the public key of another client, B:

(a) Receive a “certificate” from B itself, or

(b) Get it from CA (which is rarely done).



We will presently limit the fields in the “certificate” to the following:

CERTA = ENCPR‐CA (IDA, PUA, TA, DURA, INFOCA)

where

• PR‐CA is private key of certification authority (PU‐CA is public key of certification authority)

• IDA is user ID,

• PUA is public key of A,

• TA is time of issuance of certificate.

To do so, you will need to:

• Decide you will use method (b) to obtain each other’s public key,

• Assume:

1. that clients already (somehow) know the public key of the certification authority,

2. that the clients have their corresponding private keys with themselves, and

3. that CA has the public keys of all the clients,

• Messages from CA to clients are encrypted using RSA algorithm and CA’s private key,

• Encrypted messages are sent/received between clients once they have each other client’s public key, and

finally

• Find a way to generate and encode “current time”.

Use the above to ensure client A can send 3 messages to B, viz Hello 1, Hello 2, and Hello 3. Client B in turn responds

with ACK 1, ACK 2, and ACK 3 to messages received from A.

**Solution:**

We have developed A Certification Authority – CA server and its Clients Applications such that the clients will interact with each other . Before sending any message, the client application get certified from the CA server, and then send the HELLO message to the specified client. The other client will be already in receiving mode for this message. Also the other client will send back the ACK message in same manner.

**Algorithms**

**Server :**

1. Read Server Private key which is stored locally

2. Get client ID

3. Decrypt message using private Key

4. Read Public Key

5. Compute actual Hash value using Public Key

6. Check if Message and Actual Hash are the same

7. If Same, then generate hash using Client ID, Pub Key and time and sent to client

8. Keep repeating steps 1 to 7 untill the server is running.

**Client:**

1. Set Connection Socket Parameters of application

2. Clients have five options

i) Get CA Certificate from the server

ii) Send HELLO message to client

iii) Read Hello message to client

iv) Send ACK message to client

v)Receive ACK Message to client

**Run Program And Output**

**Client 1:**

$ python client.py 5001 1

Set Connection Parameters

Client ID: 1

--------------------------------------------

Choose Operation :

(1) Get CA Certificate

(2) Send Hello Msg to Client

(3) Receive Hello Msg from client

(4) Send ACK Msg to Client

(5) Receive ACK Msg from client

1

Generate Certificate

Read Public Key for server and client

RSA Encryption using Public Key for server and client

Certificate saved!

Client ID: 1

--------------------------------------------

Choose Operation :

(1) Get CA Certificate

(2) Send Hello Msg to Client

(3) Receive Hello Msg from client

(4) Send ACK Msg to Client

(5) Receive ACK Msg from client

2

Enter Client ID: 2

Certificate verified!

Sent message to client 2

Client ID: 1

--------------------------------------------

Choose Operation :

(1) Get CA Certificate

(2) Send Hello Msg to Client

(3) Receive Hello Msg from client

(4) Send ACK Msg to Client

(5) Receive ACK Msg from client

1

Generate Certificate

Read Public Key for server and client

RSA Encryption using Public Key for server and client

Certificate saved!

Client ID: 1

--------------------------------------------

Choose Operation :

(1) Get CA Certificate

(2) Send Hello Msg to Client

(3) Receive Hello Msg from client

(4) Send ACK Msg to Client

(5) Receive ACK Msg from client

5

ACK Message received from client 2: ACK2

Client ID: 1

--------------------------------------------

Choose Operation :

(1) Get CA Certificate

(2) Send Hello Msg to Client

(3) Receive Hello Msg from client

(4) Send ACK Msg to Client

(5) Receive ACK Msg from client

**Client 2:**

$ python client.py 5002 2

Set Connection Parameters

Client ID: 2

--------------------------------------------

Choose Operation :

(1) Get CA Certificate

(2) Send Hello Msg to Client

(3) Receive Hello Msg from client

(4) Send ACK Msg to Client

(5) Receive ACK Msg from client

1

Generate Certificate

Read Public Key for server and client

RSA Encryption using Public Key for server and client

Certificate saved!

Client ID: 2

--------------------------------------------

Choose Operation :

(1) Get CA Certificate

(2) Send Hello Msg to Client

(3) Receive Hello Msg from client

(4) Send ACK Msg to Client

(5) Receive ACK Msg from client

3

Message received from client 1: hello1

Client ID: 2

--------------------------------------------

Choose Operation :

(1) Get CA Certificate

(2) Send Hello Msg to Client

(3) Receive Hello Msg from client

(4) Send ACK Msg to Client

(5) Receive ACK Msg from client

1

Generate Certificate

Read Public Key for server and client

RSA Encryption using Public Key for server and client

Certificate saved!

Client ID: 2

--------------------------------------------

Choose Operation :

(1) Get CA Certificate

(2) Send Hello Msg to Client

(3) Receive Hello Msg from client

(4) Send ACK Msg to Client

(5) Receive ACK Msg from client

4

Enter Client ID: 1

Certificate verified!

Sent message to client 1

Client ID: 2

--------------------------------------------

Choose Operation :

(1) Get CA Certificate

(2) Send Hello Msg to Client

(3) Receive Hello Msg from client

(4) Send ACK Msg to Client

(5) Receive ACK Msg from client

**Server :**

$ python server.py 5000

Client ID 1

Server Key Check using Pu-Pv key check

Client ID 2

Server Key Check using Pu-Pv key check

Client ID 2

Server Key Check using Pu-Pv key check

Client ID 1

Server Key Check using Pu-Pv key check