Testing Procedures

# Login – Nonce comparison

1. Client Login Initiation:

* The client enters their email and passphrase to start the login process.

1. Public Key Retrieval:

* The Certificate Authority (CA) imports the client’s public key. This key is retrieved from the ‘users.json’ file using the client’s email.

1. Nonce Creation and Encryption:

* The CA creates a nonce (a random number used once).
* The CA encrypts the nonce with the client’s public key (obtained via their email).
* The encrypted nonce is sent to the client.

1. Client Decrypts and Re-encrypts the Nonce:

* The client decrypts the nonce using their private key.
* The client then encrypts the same nonce using the CA’s public key.
* The client sends the re-encrypted nonce back to the CA.

1. Nonce Verification:

* The CA decrypts the received nonce using its private key.
* The CA compares this decrypted nonce with the original nonce it created.
* If the nonces match, the login attempt is deemed successful.

This process ensures authenticity during login. The CA can confirm that the client is indeed the true client since they were able to decrypt the nonce encrypted with their public key and re-encrypt it with the CA's public key.

# Login – Nonce comparison

SERVER

A screenshot of a computer program

Description automatically generated

CLIENT

Description: Login is only successful if the exchanged encrypted, and subsequently decrypted nonce, matches with the original nonce created.

# Penetration Testing

## Man in the Middle Attack