

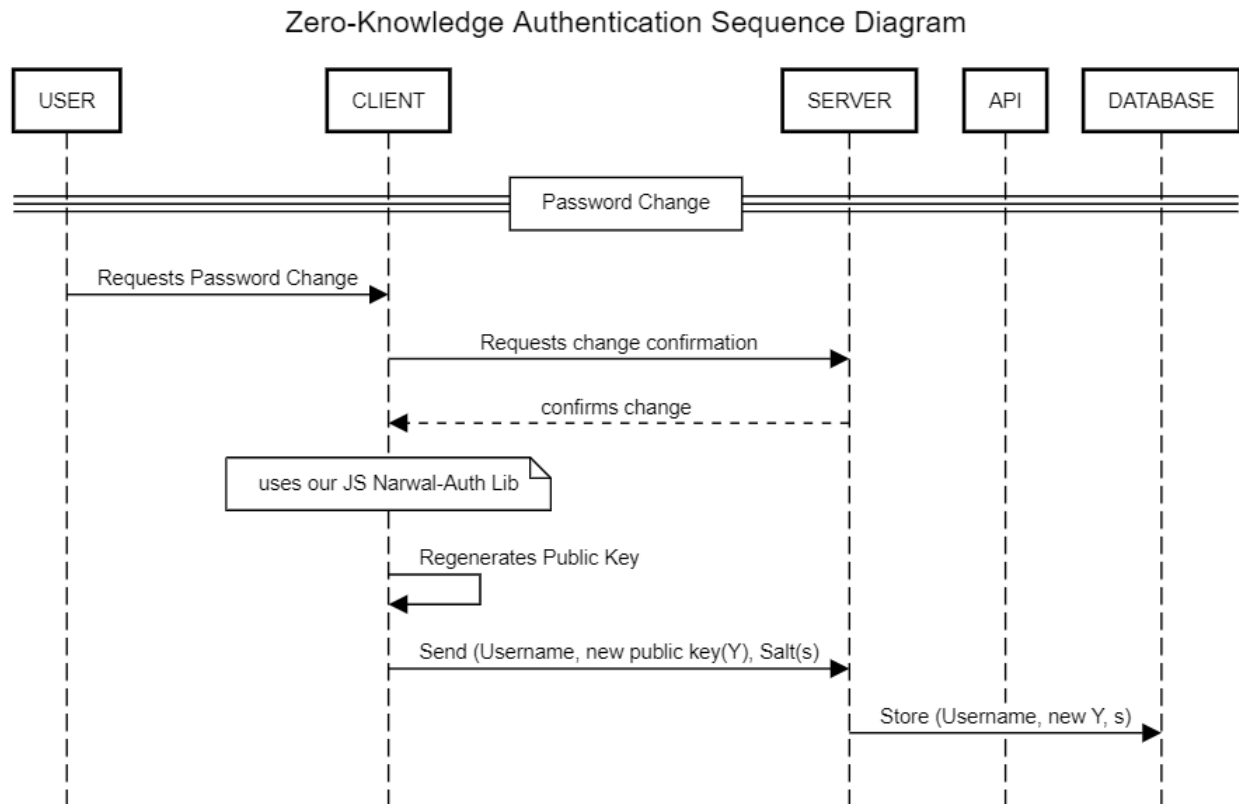
SUPERVISOR: AHMED HANIF



NARWAL AUTH API DELIVERABLE 6

**MUHAMMAD NASEEM
SAMI NAEEM
KYNAT MANSHA**

Password Change Sequence



Methodology:

- Client and Server would handle any user password change requests.
- Server confirms the desired change and sends a flag to client to allow change.
- Client browser accepts the new Password entry.
- Client browser calls upon a “GeneratePublicKey” function of our Narwal Auth Library.
- Narwal Auth Library generates a new Public Key and sends it to the Client.
- Client forwards the key to the server for updating and storing in the Database.

Our Website

The image displays two screenshots of a web browser interface. The top screenshot shows the 'Sign Up' page at the URL 'localhost:5173/signup'. The page features a dark blue card with the title 'Sign Up' in white. Below the title are four input fields: 'Name', 'Email', 'Password', and 'Forgot Password?'. A green 'Sign Up' button is positioned at the bottom of the card. The bottom screenshot shows the 'Login' page at the URL 'localhost:5173/login#'. This page also features a dark blue card with the title 'Login' in white. Below the title are two input fields: 'Email' (containing 'naseem@email.com') and 'Password' (containing masked characters). A green 'Sign in' button is at the bottom of the card. Both pages have a light gray background and a dark blue browser header.

Description:

- A simplistic approach to setting up our login and signup page as that's all we currently need to demonstrate our Zero-Knowledge authentication system.
- Users can sign up and Log in or request for a password change.
- All entered information is logged into our MongoDB database.
- Basic validation check in place to make sure the entered password is strong enough.