My Health Pass Authorization and Validation Flows

Register

- Username and password sent via Post request **Assume password confirmation handled by front end
- If data is valid:
    - User object is created and inserted into DB
- Else:
    - Error message returned

Login

- Route wrapped with decorator to check redis to see if use is locked. Using redis to check this minimizes resources (DB threads) in the case of malicious requests
- Route wrapped with decorator to calculate request signature and check redis to see if request signature is locked
- Get user from DB
- Return error message if user is not found or user is locked
- If password is correct:
    - log user in
- Else:
    - Increment failed attempts by the request signature in redis by adding a key that will expire after the timespan set by the user lockout policy (10mins)
    - If max attempts set by the user lockout policy (13) is reached:
        - Set a locked key for that request signature in redis that will expire after the time set in the user lockout policy (20mins)
    - Increment failed attempts by User in redis
    - If max attempts set by config is reached:
        - Lock user in redis and db

Unlock User

- Email address sent via POST request
- Generate a random and unique token
- Set token for user in redis
- Generate a reset link containing token and email address
- Return link. *In reality we would send this link to the user's email address
- When user clicks link an endpoint extracts token and email
- If token exists and is not yet activated:
    - Invalidate token and unlock user
- In reality we can then redirect user to a password reset page and that flow would actually unlock the user