Project Title: Multi-Factor Authentication add-on for OpenVPN

Application – "DefAuth"

Team Name	Ministry	Team Leader Name	Team Leader Contact Detail	College Name	Collage Location
DEFENDERS	ISRO	Sriram M	**Email:** sriramm1997@gmail.com **Cell:** 9655077056	Thiagarajar college of Engineering	Madurai, TamilNadu, India

- **Open Source Technology used**
    - LAMP stack
    - Android SDK
    - OpenVPN server and Client
    - Shell Script
    - Node.js and JSON Web Tokens
    - Web Application

- **Approach/Procedure**

- **New User Registration procedure**
    - Employee ID
    - Password (only numeric)
    - IMEI – Fetched secretly from the mobile device for possession factor
      (Restricted to one mobile device only, else raise ticket to admin to release lock)
    - Now open "DEFAuth" mobile application and select "New User" and enter Employee ID to initiate session in mobile for first time registration
    - The IMEI + User ID is fetched and updated in Database
    - After successful registration of mobile device the user is automatically logged out.

- **Existing User Login Procedure**

    - The existing user shall open the web application and enter Employee id and password
    - Now a QR code is displayed on the web screen
    - Open the "DEFAuth" app - This app is inbuilt with app lock
        - Finger Print verification for Bio metric enabled device
        - PIN lock for other devices
    - The QR code can be scanned only using the previously registered and verified mobile device.

- Once the IMEI of the mobile device is verified with the database TOTP auto verification from server side takes place in the backend.
- The TOTP and IMEI is verified using the JWT token against the userID.
- The JWT token once generated can only be used for 10 minutes and the validity expires thereafter.

Finally the JWT validity is verified and VPN access is provided using a customized shell script containing the OVPN file credentials to the client.
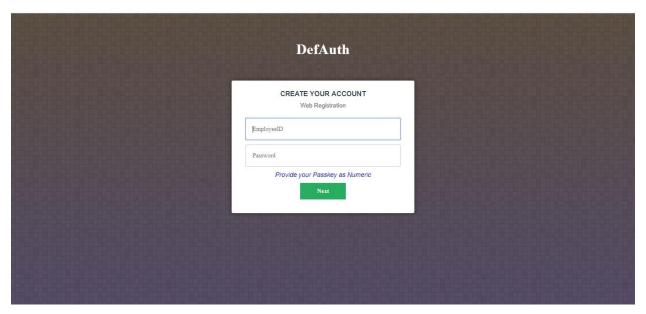
- **Dynamic User Status details in DB**

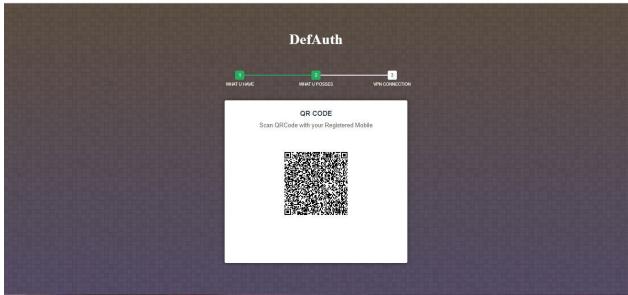(Format: status number -> current status)

- 0 -> user has registered in website page
- 1 -> user updated his/her IMEI
- 2 -> user is logged in
- 3 -> user is logged out
- 4 -> TOTP is verified for user

- <u>**Web Application Images**</u>

SMART INDIA HACKATHON '17

DefAuth

CREATE YOUR ACCOUNT
Web Registration

EmployeeID

Password

Provide your Passkey as Numeric

Next

DefAuth

1 — WHAT U HAVE   2 — WHAT U POSSES   3 — VPN CONNECTION

QR CODE
Scan QRCode with your Registered Mobile

- **Mobile App Images**