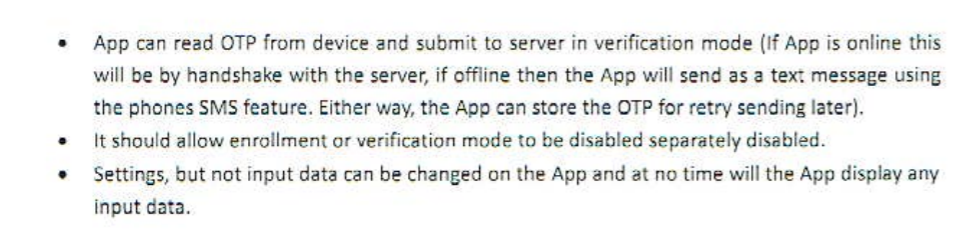
REMARKS ON POL APPLICATION DESING AND MOCKUP

**Feb 16th 2021**

**General: All Screens**

1. Kindly use attractive graphics and color scheme through out the App
2. Kindly use beautiful theme and button styles
3. The following items of the App requirements have not been addressed on the mock screens:



**Screen: Welcome Screen**

1. Please use HCM logo (to be provided) in place of the heart image
2. Just above the text “Version 1.0” add the text = “Powered By Human Capital Managers”

**Screen: Login Screen**

1. Remove the text “Not a Member?”
2. Bring the text “Forgot Password” down with “Register”
3. Remove the links “Home/Products/Company/Blog” at the bottom of the screen

**Screen: Registration Screen**

1. Please rename screen title to “HCM Associate Registration”
2. Additional fields are needed: Sur Name, First Name, Other Names
3. In Prod version, this screen will initiate the registration process only, the admin needs to approve and activate the account before the Associate will be able to login, but this feature can be bypassed for testing

**Screen: Scanning Screen**

1. What is the security risk for hackers to track the PoL device if we show the BLE Address here?
2. Is this BLE Address public or private and realizable? Will there be need to make payment to regulatory authorities for using this address?
3. If a user has 2 or more devices to register, how can he know which is which on the device list?
4. Can showing a SN on the device list, which is also printed at the back of each device be more productive and useful for identification?

**Screen: User List Screen/Result List Screen/User Detail Screen**

1. The server’s database will contain thousands of users so, it will be inefficient to show them all on this screen
2. If the device already contains an enrolled user
   1. The user information shows up in the User List Screen
   2. The App will provide the following options:
      1. To “Test the Device Function” – Go to the “Validation” Screen
      2. To “Re-programme the Device” – Go to “Reuse a PoL Token” Screen
3. If the device is completely empty of user information
   1. A new user can be searched on the server database using the fields: Organization (Required), EmploymentID (Required), Sur Name, First Name, Other Names, Phone number, Email Address.
   2. If more than one record is returned, the enrolment process cannot proceed till disambiguation occurs for duplicate users to be removed from the server
4. If only one matching record is found as should always be the case, the screen simply shows the User Detail Screen as returned by the server (Including picture image for visual identification)
5. There should be a button(on the user detail screen) to enrol this user’s fingerprint if not already enrolled
6. The user should be able to enrol with all 10 fingers, but not less than 3.
7. If user has already been enrolled on another device, the App should discover this and:
   1. Stop new enrolment process
   2. Provide the option of using the Unlink/Link feature – Go to “Unlink/Link PoL Device” Screen

**Screen: Validation Screen**

1. Please change caption “Secret Token” to “Firmware Generated Token”
2. When the 2 tokens make a perfect match, please highlight their backgrounds green to provide easy visual clue
3. When the 2 tokens are mismatched, please highlight their backgrounds red to provide easy visual clue
4. This screen is useful not only during testing phase but also after a PoL device is setup – the user will be asked to place his finger on the sensor and HCM associate will check to see if both boxes are green. In this case, inputs to the App should include user’s true fingerprint.

**Screen: Settings Screen**

1. This screen should be visible soon as the App connects to the PoL device to allow configuration changes even before assigning the device to a user
2. Secret key should not be stored or displayed by the App, but created on the server and read by the App for ultimate writing to the device.
3. While the App should be able to setup all the features necessary for the token to run (eg Secret keys, OTP validity, Calculation basis, OTP validity basis, skews and PoL Authentication cycle) these need not be available to be manipulated by the user as a setting feature for the App; they should be setup by admin on the server.
4. Time synchronization between the App and the device should be automatic and passive without the need for user action
5. Matching threshold is in the range of 0% to 100%, a slider may be the easiest control to use here
6. Limit parameters to be manipulated in the App setting to Threshold for biometric matching and OTP display duration only, all other settings come from the server.

**Additional Screens:**

**Screen: Reuse a PoL token**

1. A screen needs to be provided to allow reuse of an already primed PoL token, as in when the initial user has died
2. The current device user is unlinked from the device at the database
3. The data in the PoL is cleared from this screen
4. A new un-enrolled user to any PoL token can be enrolled to this now cleaned device in the regular manner
5. If a user has already been enrolled on the server and linked to a different device he cannot be enrolled again (See Unlink/Link PoL Devices below)

**Screen: Unlink/Link PoL Devices**

1. If a user that has already been enrolled has lost or damaged his device, he/she can be unlinked from the former device and linked to a new one
2. This feature depends on a Boolean switch by admin at the server level
   1. The unlink/link switch is “FALSE” by default
   2. After the necessary verification, the Admin turns the switch to “TRUE”
   3. The Unlink/Link Screen on the App checks for this value before allowing a user to be linked to another empty PoL token
   4. This screen cannot reformat or clean a none empty token
   5. Also this screen simply link user to a new token and transfer his data from the server to the device but not make new enrolment
3. The App first searches for the user from the database as in “User List” Screen
4. Then it requires the user to provide biometric data through a clean PoL device
5. The App then checks if the supplied biometric data matches the stored data from the server (The App may need to temporarily write this data unto the new device to allow it perform the fingerprint comparison)
   1. If the user matches with store biometric data the App unlinks him from the old device and links him to the new device
   2. If otherwise, the process is aborted and the new device again cleaned