Mobile device story

The story for mobile app authentication goes like following

1. Every time we open the mobile app, the device checks whether it is registered or not using 'CheckDeviceRegistered' service call.
    a. If registered, then shows the screen for entering 4-digit login PIN (referred as PIN screen here onwards.)
    b. If **not** then shows the usual login screen with username and password (referred as login screen here onwards).
2. When on login screen the device shows a button to register the device which on pressed should make a call to 'GetRegistrationCode'. This service call returns back an 8-digit alpha-numeric registration-code. This registration-code is shown to the user on screen. If an already registered device again makes a call to GetRegistrationCode then the existing registration would be deleted.
3. After getting the registration-code, the user goes to his dossier in WebApp and completes the registration by providing his registration-code and a PIN for the device.
4. When device registration is complete user closes the screen which was showing him registration-code. After closing the screen, call to 'CheckDeviceRegistered' is made and follows the steps as mentioned in point 1.
5. In the PIN screen the user should provide his 4-digit PIN that he setup in dossier, this 4-digit PIN is sent to 'LoginByPin' service call along with deviceFootprint. This service returns back same loginResponse as on the current login mechanism with username and password
    a. If authentication is **successful**, 'resultSuccess' property is true in response. This login response consists of a property 'auth-Token' which should be sent as 'x-user-id' for the subsequent requests for authentication.[We have used the same existing mechanism for authentication of requests.]
    b. If authentication is **not successful**, 'resultSuccess' property is false in response.
    c. If authentication is **not successful,** for more than 3 times then the device will be under lock for 5 minutes. If the user does not wants to wait for 5 minutes then he can go the dossier's mobile page and unlock the device from there. The no. of unsuccessful attempts and lockdown time in minutes is both configurable from database.
6. For removing device a call is made to RemoveRegistration.

Web application story

Dossier's "mobile" tab.

- To use the PIN system for Mobile, user should register his mobile
    - Mobile user should request for the 8 digit registration code from Mobile and he will get the 8 digit code as response.
    - Navigation to Mobile Tab in Dossier
      (login→ click on Username→ click on Mobile Tab)
      It will be visible only when the client level setting for that user's client is true.
      If it is visible then click on "+Add device" button, a popup will appear to enter registration code. If it is valid then another popup will appear for the user to add mobile device name and configure the pin for his mobile device.
      If invalid then user will get a error message as "Enter Valid Registration Code".
    - Device name should be 50 characters length and should not be duplicate for the user. If it exceeds more than 50 characters it will truncate the remaining characters and continue
    - Only 4-digit numbers are allowed as PIN.
    - If the registration is successful, user can see his mobile details in the grid present in Dossier Mobile tab and can login through his device using the same pin.
- The actions in the grid for mobile are -
    - Remove : When clicked first asks for the confirmation from user. If user confirms as "Ok" then the device registration is removed by deleting the record from the database.
    - Change PIN : This is used to change the 4 digit PIN.
    - Unlock: : To unlock the device when device is under lockdown if the user does now wants to wait for 5 minutes.

Client level settings

- There is Client level Settings for this Implementation in Misc.aspx

(login as admin → Setup→ Customers→ Divisions → select for a Division → Division Tab → Misc Settings)

- In this page in Mobile Settings tab "Enable Mobile Auto Login" check box is present,if this checkbox is checked then only the contact for that client can have pin based login feature enabled(By Default it will be true)
- If we uncheck the checkbox,then asks for the confirmation from user. If user confirms as "Ok",then it will delete all the configured device for that client for mobile auto login and we can't configure PIN based login for the users of that particular client.
- These changes take effect when user clicks the save button on the page.