**UAE PASS Mobile Authentication Implementation Assessment Checklist**

Version Number 1.2

*Table of Contents*

[1. Assessment Details 3](#_Toc18326615)

[2. UAE PASS Implementation Check List 4](#_Toc18326616)

[3. UAE PASS Implementation Assessment Check List 5](#_Toc18326617)

# 1. Assessment Details

|  |  |
| --- | --- |
| ***Assessment Details*** | |
| *Assessment Date:* |  |
| *Relying Party:* |  |
| *Assessment Venue:* |  |
| *General Comments:* |  |
| *Recommendations:* |  |
| *Assessment Completed by:* |  |

# 2. UAE PASS Implementation Check List

***Disclaimer: C = Compliant, PC = Partial Compliant, NC = Non-Compliant, NA = Not Applicable.***

|  |  |  |
| --- | --- | --- |
| ***Sequence*** | ***Items and Case scenarios*** | ***Status***  ***(C, NC , PC, NA)*** |
|  | Login Scenarios for Verified Accounts (SOP2/SOP3) |  |
|  | Login Scenarios for unverified Accounts (SOP1) |  |
|  | Linking Scenarios implemented and tested. If linking not found then allow user registration.  (Automatic/Manual/Registration) |  |
|  | Auto-Populate user registration form with UAE PASS information and populated information should not be editable. |  |
|  | UUID attribute is stored for checking already linked accounts. |  |
|  | Logout is working as expected. |  |
|  | Design Consideration taken care. |  |

# 3. UAE PASS Implementation Assessment Check List

***Disclaimer: C = Compliant, PC = Partial Compliant, NC = Non-Compliant, NA = Not Applicable.***

|  |  |  |
| --- | --- | --- |
| ***Sequence*** | ***Items and Case scenarios*** | ***Status***  ***(C, NC , PC, NA)*** |
| **Mobile Authentication Attempt Scenarios** | | |
|  | User is a UAEPASS User and is attempting to log in to the application, having his UAEPASS App on the same mobile device. The app should invoke the web view to redirect the user to the UAEPASS app for confirmation without asking for any credentials (App-to-App Integration). |  |
|  | **On User Confirmation:** Control is shifted back to the application after confirmation the user is logged in successfully. |  |
|  | **On User Cancelation:** Control is shifted back to the application after cancelation and an appropriate message is shown. |  |
|  | User is a UAEPASS User and is attempting to login to the application, but doesn’t have his UAEPASS App on the same mobile device. The app should open a WebView to allow the user to login using UAEPASS login page. Or if the user doesn’t have UAE PASS in another device, have the user download the app from App store/play store |  |
| ***Account Linking Scenarios:***  If user already have an account with entity then allow him to link his existing Account with UAE PASS Account, it can be supported by two modes as applicable.  **Automatic Linking?** This is applicable if the relying party maintains the IDN number (or any other common attributes) for linking users with UAE PASS.  Other attributes like date of birth, passport number or any shared attribute between the User Profile in UAE PASS and Relying Party should be considered to find the exact match of the user.  **Manual Linking?** In Case of Manual Linking, User should be challenge for his SP account username and password and on successful authentication the linking can be achieved by storing the linking attributes (e.g. uuid, idn etc.) at SP side. This is one-time activity and should be done only on first linking attempt.  **Note: Once the linking is successful then entity should store UUID of the user as a linking attribute for subsequent login from the same user.** | | |
|  | Whenever any user logs in using UAEPASS then entity should first check for UUID in their system to identify this is already linked user and user should be able to login successfully. |  |
|  | User try to login into SP application using UAEPASS account and UUID not found in SP application then check for another linking attribute like IDN and if user linking attribute found then login should be successful. (Automatic Linking) |  |
|  | User try to login into SP application using UAEPASS account but no UUID and any other linking attribute found in SP application then:   1. Allow user to manually link account as per Manual Linking instruction. 2. allow user to register account with entity and registration form attributes should be auto-populated based on UAEPASS account.   Refer below screenshot for reference. |  |
| **Logout Scenarios** | | |
|  | When user logout from application then user should be challenged to login on next logon. |  |
| **Awareness:** As these points cannot be assessed technically, the entities should ensure the compliance for below points. | | |
|  | Relying Party's Call Center is aware of the Service and can provide basic information about how to use the UAE PASS Account and how to Register with the Service. |  |
|  | UAE PASS Oauth/OpenID Connect is the only used from the Web as well as Mobile Application of the Relying Party. |  |
|  | There should be no logs or storing of UAE PASS API data in client’s server (except user info data as per business). |  |
|  | Recommended to exchange the code to access token from backend channel of SP and not from mobile app directly. |  |
|  | If SP mobile app interacts with SP backend then SP backend should be protected by token validation mechanism for ensuring UAE PASS authenticated users. |  |
|  | UAE PASS Access Token expiration should be handled (if applicable) |  |