**UAE PASS Authentication Implementation Assessment Checklist**

Version Number 1.3

*Table of Contents*

[1. Assessment Details 3](#_Toc18326567)

[2. UAE PASS Implementation Check List 4](#_Toc18326568)

[3. UAE PASS Implementation Assessment Check List 5](#_Toc18326569)

# 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)*** |
| ***Authentication Scenarios:***  Basic Authentication function like all user types (SOP1, SOP2 and SOP3) should be able to login. | | |
|  | Verified users (SOP2/SOP3) can login successfully using UAE PASS Account. |  |
|  | Verified **Visitor** (SOP3) can login successfully using UAE PASS Account. |  |
|  | Unverified users (SOP1) are able to login successfully using UAE PASS account. The SP should handle the authorization or flow in their side as per the user types and their business. |  |
|  | If User cancel the authentication request from the web page then it should be properly handled. |  |
|  | If User cancel the authentication request from mobile app then it should be properly handled. |  |
| ***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 other 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. |  |
| **User Types Handling** | | |
|  | On Successful authentication at UAE PASS the control is sent back to SP irrespective of user type. The SP should handle the authorization or flow in their side as per the user types and their business.  **SOP1 :** In case of SOP1, UAE PASS will not return the Emirates ID number attribute as the user has still not verified his/her emirates ID at this stage. SP should handle in case SOP1 is not allowed at their end by showing the appropriate error message. |  |
|  | In case user type is other than SOP1, SOP2 and SOP3 then appropriate error message should be displayed. |  |
|  | | |
|  | The SP uses the UAE PASS Logos wherever applicable on Relying Party's Portal as per the shared design guidelines. |  |
| **Logout Scenarios** | | |
|  | Service Provider Initiated Logout is implemented in such a way that it should clear UAE PASS and SP application session and redirected based on redirect parameter in logout url. |  |
| **Awareness:** As these points cannot be assessed technically, the entities should ensure the complanace 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). |  |
|  | UAE PASS Access Token expiration should be handled (if applicable) |  |

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