|  |
| --- |
|  |
| **First Time Login, Activate Security Token and Reset Password** |
| Business Requirement Specification for Single User |
|  |
| ***(PENRIL/BSN-CDB/BRS)***  ***Revision: 00*** |
| **11th August 2017**  Prepared By:    **Penril Datability (M) Sdn Bhd (816792-X)**  Suite A-07-07 Plaza Mon’t Kiara  No. 2, Jalan Kiara, Mon’t Kiara  50480 Kuala Lumpur, Malaysia  Tel: (603) 6201 2622Fax: (603) 6201 7622 |

# 

# DOCUMENT AMENDMENT LOG

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rev. No | Date Update | Description of Change | Update By  <Name, Dept> | Review By  <Name, dept> | Approved By  <Name, Dept> |
| 00 | 14/3/2018 | Changes according to current changes | Erni Suhaireen bt Zulkifli | Siti Norahayu |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Table of Contents

[DOCUMENT AMENDMENT LOG 2](#_Toc508884281)

[**Business Requirement Acceptance** 4](#_Toc508884282)

[**Section A: Introduction** 5](#_Toc508884283)

[1.1 Objective 6](#_Toc508884284)

[1.1 UPASS Application 7](#_Toc508884285)

[1.2 Page Flow Overview 7](#_Toc508884286)

[Section 2: Corporate Digital Banking Functions 10](#_Toc508884287)

[2 First Time Login (FTL) 10](#_Toc508884288)

[2.1 First Time Login for Single User 10](#_Toc508884289)

[2.1.1 Process Flow 10](#_Toc508884290)

[2.1.2 Screen Flows 10](#_Toc508884291)

[3 Login 18](#_Toc508884292)

[3.1 Login as Single User 18](#_Toc508884293)

[3.1.1 Process Flow 18](#_Toc508884294)

[3.1.2 Screen Flows 18](#_Toc508884295)

[4 Activate Token 21](#_Toc508884296)

[4.1 Process Flows 21](#_Toc508884297)

[4.2 Screen Flows 21](#_Toc508884298)

[5 Reset Password 27](#_Toc508884299)

[5.1 Reset Password / Unlock for Single User 27](#_Toc508884300)

[5.1.1 Process Flows 27](#_Toc508884301)

[5.1.2 Screen Flows 27](#_Toc508884302)

[Appendix 1: System Security 32](#_Toc508884303)

[Appendix 2: List Allowable Values 34](#_Toc508884304)

[Appendix 3: Internet Banking “Text” Input Fields Specification 35](#_Toc508884305)

[Appendix 4: Acceptable Characters for Validation 36](#_Toc508884306)

[Appendix 5: Download Report 38](#_Toc508884307)

[Appendix 6: Glossary 39](#_Toc508884308)

**Business Requirement Acceptance**

I/We hereby verify that this Business Requirement consist of all the requirements requested by BSN. The implemented system will fulfill ONLY this requirement.

I/We also hereby AGREE that this satisfies our entire requirement for **[First Time Login, Activate Token and Reset Password]**

Any future changes to this agreed scope will be treated as an enhancement to the system. Any future changes to the project timeline will be subjected to the final approval of the project steering committee.

**BSN:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Approved by** | **Role** | **Signature** | **Date** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Penril Datability (M) Sdn. Bhd.:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Approved by** | **Role** | **Signature** | **Date** |
|  | Project Manager |  |  |
|  | Team Lead |  |  |
|  | Senior Software Engineer |  |  |

**Section A: Introduction**

This document served as the business requirement and system specification of implementing First Time Login, Activate Token and Reset Password in BSN Interbank Banking system.

This document shall explain all the features and functionalities, which is elaborating with screen captures, process flow, descriptions, input fields specifications and error messages. All screen designs provided in this document are samples and only illustration purpose for easy understanding. The screen designs are not final.

## Objective

The objective of this document is to capture user requirements of transactional and administration modules of implementing First Time Login, Activate Token and Reset Password. This document will facilitate development and implementation of the mentioned modules of Internet Banking System for BSN.

The base line features description and screen designs will become a reference blueprint for the development team to develop the transactional and administration module. Hence, it is crucial that all stakeholders need to ensure the correctness and adequacy of the requirements captured in this document.

All stakeholders involved are expected to review and sign off this document before the development start. By signing off the document, the stakeholder has endorsed the correctness and accuracy and adequacy of the requirements documented in this document.

## UPASS Application

UPASS is a mobile application. This application will generate a one-time password for login, normally a 6 digits random number and to be input when login. This application will also generate a transaction signing code while performing any transaction. User are required to scan the QR code develop by IBS at Transaction Signing. The Approver or the Single User will be the key person using the UPASS Application to generate the One Time Password and Transaction Signing Code.

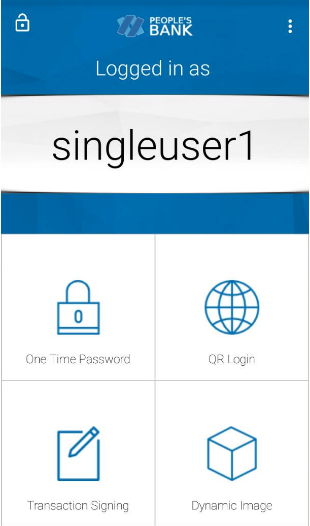


Figure 1: UPASS Application

## Page Flow Overview

Below diagram shows the overall view of the CDB system page flow. The detail of each function will be described later in this document.

Diagram 1: Overall CDB Page Flow Diagram



Section 2: Corporate Digital Banking Functions

# First Time Login (FTL)

For the first time Corporate Digital Banking access, customer requires to perform account activation via the First Time Login module. Once completed the FTL process, customer is able to access the CDB Systems.

## First Time Login for Single User

### Process Flow



Diagram 2: First Time Login for Single User Flow Diagram

There are two (2) participants involved in this process which is Single User and Maker. The process is defined by the following steps:

### Screen Flows

***Step 1:***

1. Single User accesses to First Time Login Selection from the Login screen of Corporate Digital Banking (CDB) System.

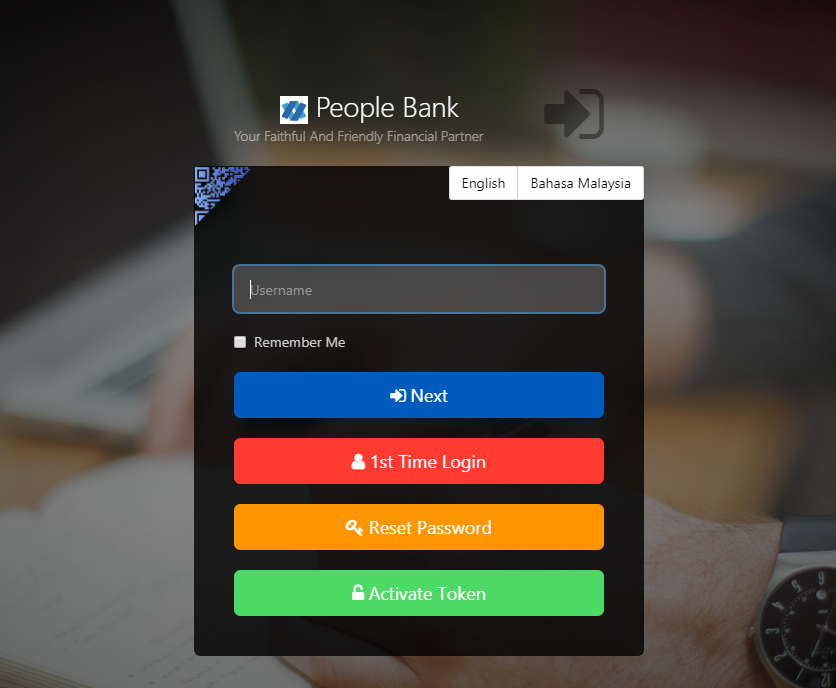


Figure 1: Login screen of Corporate Digital Banking (CDB) System

***Step 2:***

1. Single User selects First Time Login by clicking ‘Corporate User’ hyperlink text. To cancel the registration, Single User can click on the ‘Cancel’ button.

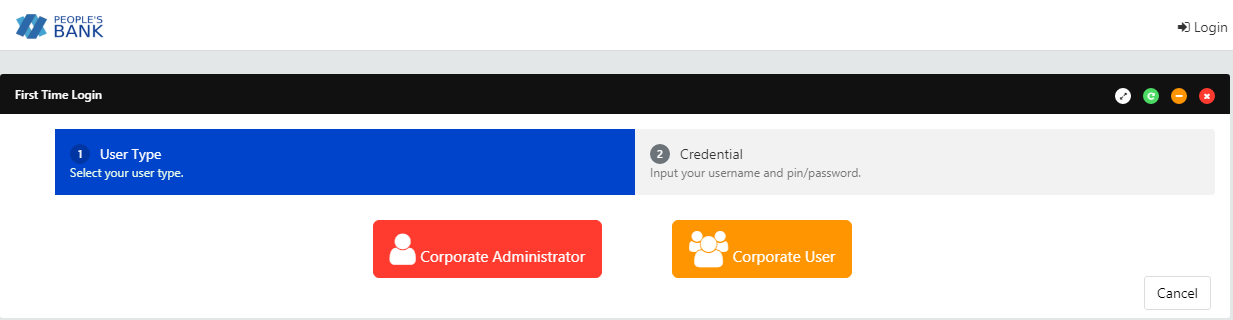


Figure 2: First Time Login Selection screen

**Action:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Action | Type | Description |
|  | Corporate User | Hyperlink | This actions will be used to display First time login with username and password screen |
|  | Cancel | Button | Contains an action to cancel FTL and go back to Login Page |

Table 1: First Time Login Selection Action

***Step 3:***

1. Single User inputs Username and default password and click on the “Next” button.
2. CDB System validates Username and Password. After the validation, CDB System will display First time Login screen.

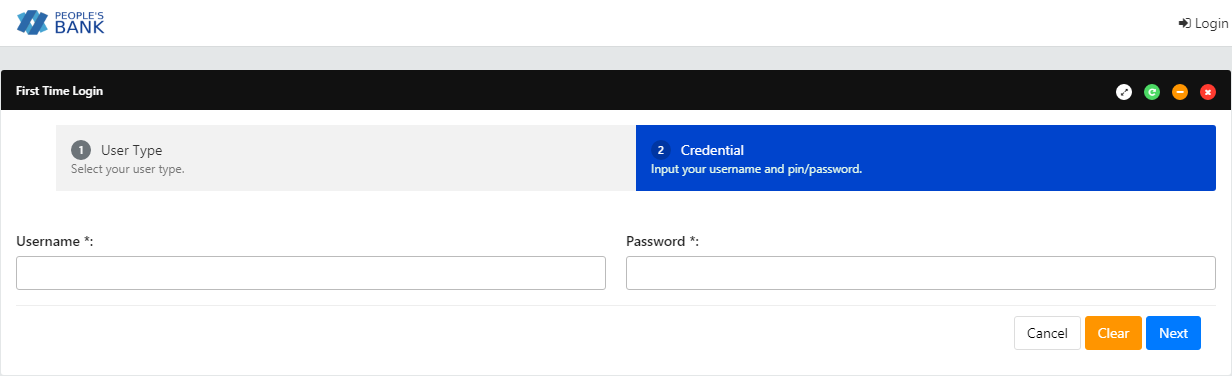


Figure 3: Username & Password input screen

**Input Specification:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Field | Field Type | Rule | Description | M/O |
|  | Username | Text Box | Min Length: 6  Max Length: 16  Alphanumeric | The unique personal identifier for the user. Username is unique in CDB. | M |
|  | Password | Text Box | Min Length: 8  Max Length: 12  Password must contain a mixture of numeric and alphabet format and cannot include these special character [“<>‘%;&+].> | This password use for First Time Login. User will be locked after [X] times of failed password validation, i.e. 3 times | M |

Table 2: Username & Password Input Specification

**Action:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Action | Type | Description |
|  | Next | Button | Contains an actions to validate Username and Password if it is correct then display Reset Password screen |
|  | Cancel | Button | Contains an action to shows the First Time Login Selection |
|  | Clear | Button | Contains an action to clear up all the entered fields |

Table 3: Username & Password Input Action

**List of available messages for the screen:**

|  |  |  |
| --- | --- | --- |
| **No** | **Event** | **Error Description in English** |
|  | Username is not inserted | Username is required. |
|  | Password is not inserted | Password is required. |
|  | Invalid username | Invalid username or password. |
|  | Invalid Password | Invalid username or password. |

Table 4: Username & Password Input available errors

***Step 2 (at IBS):***

1. If the role of the user is the Single User, the user is required to input the Registration Code that is generated by UPASS application after user scans the QR image.
2. User click “Next” button.
3. CDB System validates the Registration Code. If provided Registration Code is valid, CDB System will link the UPASS application to the user and activate the UPASS application. Subsequently, proceed to Reset Password Screen.

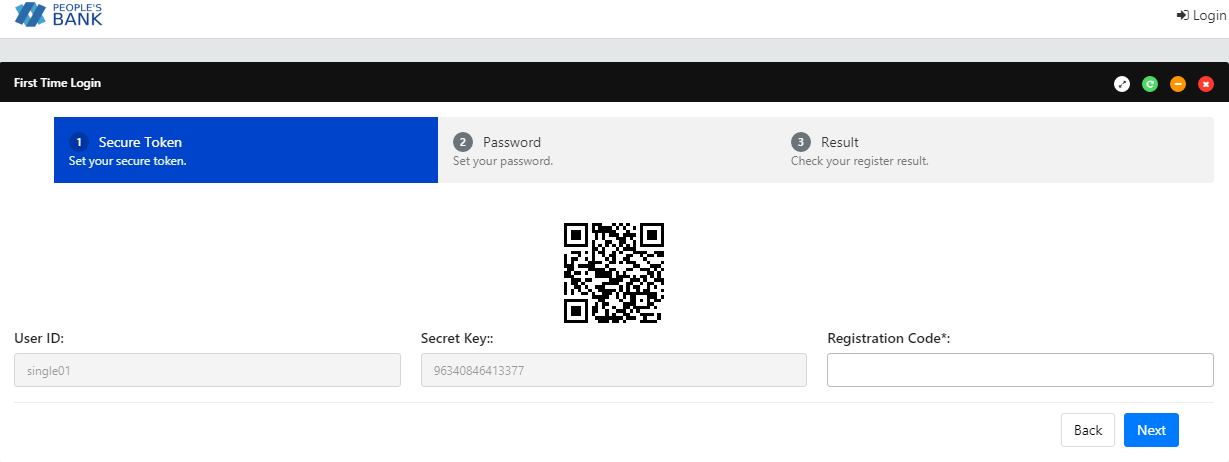


Figure 4: Registration Code Screen

**Input Specification:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Field | Field Type | Rule | Description | M/O |
|  | Registration Code | Text Box | Match Length: 13  Numeric | The unique identifier for the user to register a UPASS application | M |

Table 5: Registration Code

Input Specification

**Action:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Action | Type | Description |
|  | Next | Button | Validates the Registration Code. If provided Registration Code is valid, CDB System will link the UPASS to the user and activate the UPASS |
|  | Back | Button | Contains an action to go back to the previous page. |

Table 6: Registration Code

Action

**List of available messages for the screen:**

|  |  |  |
| --- | --- | --- |
| **No** | **Event** | **Error Description in English** |
|  | Registration Code number not inserted | Registration Code number is required. |
|  | Enter an invalid Registration Code | Invalid Registration Code |

Table 7: Secure Pass Input Available Errors

***Step 2 (at UPASS):***

1. User registers the UPASS application at mobile by click on “Register Device”.
2. User scans the QR images generated by IBS.
3. UPASS will generate Registration Code to be entered at “Registration Code” text field at IBS.

***Step 3:***

1. Single User inputs the New Password and Confirm Password in Reset Password screen and click on the “Next” button.
2. CDB System saves the New Password to IB Database and then redirect to the Login page.

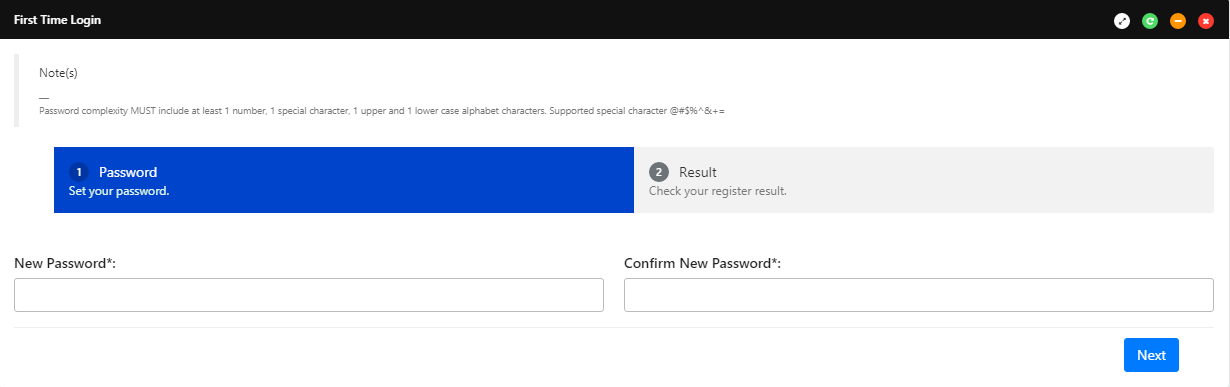


Figure 5: Reset Password screen

**Input Specification:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Field | Field Type | Rule | Description | M/O |
|  | New Password | Text Box | Min Length: 8  Max Length: 12  Password must contain a mixture of numeric and alphabet format and cannot include these special character [“<>‘%;&+].> | Input the new password to replace the existing password | M |
|  | Confirm New Password | Text Box | Must be same as Password field | Confirm the new password | M |

Table 8: Reset Password Input Specification

**Action:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Action | Type | Description |
|  | Next | Button | Contains an action to saves the new Password to the database |
|  | Back | Back | Contains an action to return to previous page |

Table 9: Reset Password Input Action

**List of available messages for the screen:**

|  |  |  |
| --- | --- | --- |
| **No** | **Event** | **Error Description in English** |
|  | Password is not inserted | Password is required. |
|  | Confirm Password is not inserted. | Confirm Password is required. |
|  | Fill in password contains with one of the criteria below:   1. Special character ["<>'%;&+].> 2. Digit only 3. alphabets only | Password must contain a mixture of numeric and alphabet format and cannot include these special character [“<>‘%;&+].> |
|  | Invalid Confirm Password | Confirm Password must be the same as Password |

Table 10: Reset Password available errors

***Step 4:***

1. CDB System displays the result to Single User. Single User can go back to Login screen by clicking the “Proceed to Login” button.

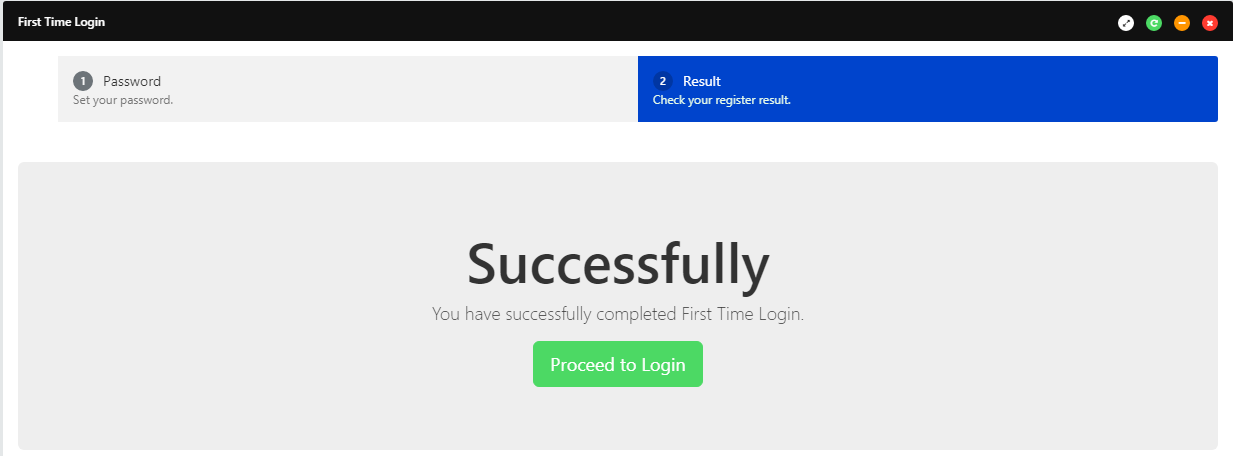


Figure 6: First Time Login Reset Password Result screen

**Display Fields:**

| **No** | **Field** | **Format** | **Description** |
| --- | --- | --- | --- |
|  | Successfully  You have successfully completed First Time Login | Text | Notification to show that the password successfully reset |

Table 11: First Time Login Reset password result Field

**Action:**

| **No** | **Action** | **Type** | **Description** |
| --- | --- | --- | --- |
|  | Proceed to Login | Button | Contains an action to go back to the main page to login |

Table 12: First Time Login Reset password result Action

# Login

The Login function required a valid username and password from Single User. Upon successful login, Single User will be able to access and perform relevant functions based on access rights.

## Login as Single User

### Process Flow



Diagram 3: Login as Single User Flow Diagram

### Screen Flows

***Step 1:***

1. Single User access to CDB Login screen.
2. CDB System display Login screen.
3. Single User keys in Username and click “Next” button



Figure 7: Login (Step 1) screen

**Input Specification:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Field | Field Type | Rule | Description | M/O |
|  | Username | Text Box | Min Length: 6  Max Length: 16  Alphanumeric | The unique personal identifier for the user. Username is unique in CDB. | M |

Table 13: Login (Step 1)

Input Specification

**Action:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Action | Type | Description |
|  | Next | Button | Contains an action to shows the next page. |

Table 14: Login (Step 1) Action

**List of available messages for the screen:**

|  |  |  |
| --- | --- | --- |
| **No** | **Event** | **Error Description in English** |
|  | Username is not inserted | Username is required. |
|  | Invalid username | Invalid username |
|  | Invalid role (Did not select checkbox, Secure Pass) | Your role is not correct. |

Table 15: Login (Step 2) available errors

***Step 2:***

1. CDB System displays the next page.
2. Single User keys in Password and OTP
3. Single User click “Next” button

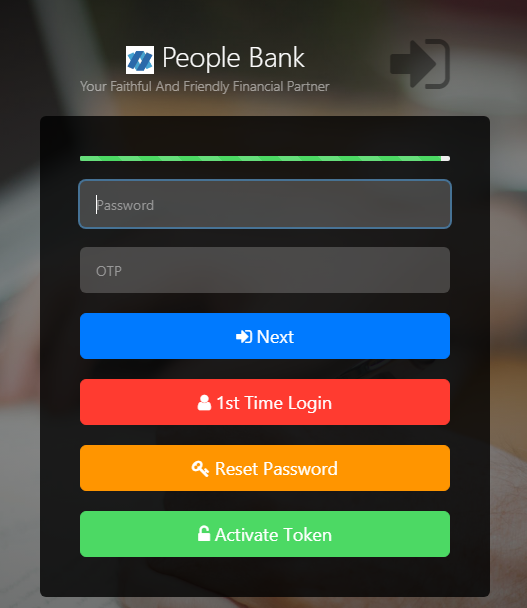


Figure 8: Login (Step 2) screen

**Input Specification:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Field | Field Type | Rule | Description | M/O |
|  | Password | Text Box | Min Length: 8  Max Length: 12  Password must contain a mixture of numeric and alphabet format and cannot include these special character [“<>‘%;&+].> | This password use for login. User will be locked after [X] times of failed password validation, i.e. 3 times | M |
|  | OTP | Text Box | Match Length: 6  Numeric | OTP pin that are generated through by UPASS. | M |

Table 16: Login (Step 2)

Input Specification

**Action:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Action | Type | Description |
|  | Next | Button | Contains an action to shows Home page. |

Table 17: Login (Step 2) Action

**List of available messages for the screen:**

|  |  |  |
| --- | --- | --- |
| **No** | **Event** | **Error Description in English** |
|  | Password is not inserted | Password is required. |
|  | OTP is not inserted | OTP is required. |
|  | Invalid Password | Invalid password. |
|  | Inserted invalid password more that [X] times | You have reached the maximum number of attempts. Please call BSN's Contact Centre at 1300-88-1900. |

Table 18: Login (Step 2) available errors

# Activate Token

This module allows Single User to activate his/her UPASS for use in CDB

## Process Flows



Diagram 4: Activated UPASS Flow Diagram

## Screen Flows

***Step 1:***

1. Single User access to Activate New Secure Pass Screen. CDB System display Activate New Secure Pass Screen.

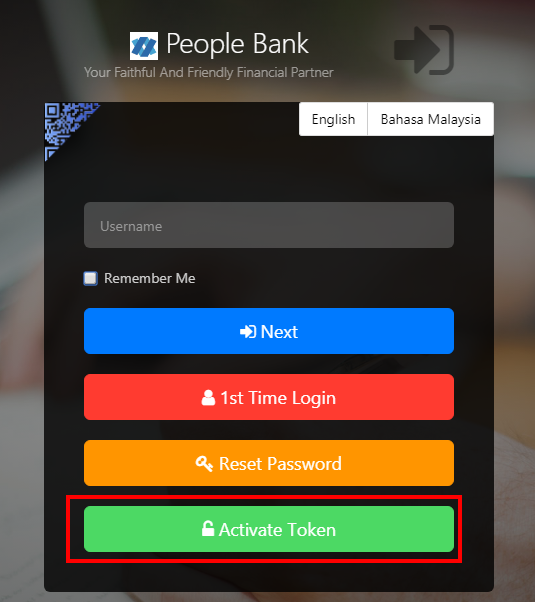


Figure 9: Login Screen

**Action:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Action | Type | Description |
|  | Activate Token | Button | This action will be used to display Mobile activation page. |

Table 19: Activate New Secure Pass input Action

***Step 2:***

1. Single User input Username & Password, and clicks “Next” button, or click ‘Cancel’ button to cancel Mobile Activation.
2. CDB System validates Username and Password. After the validation, it will display Token Registration Screen.

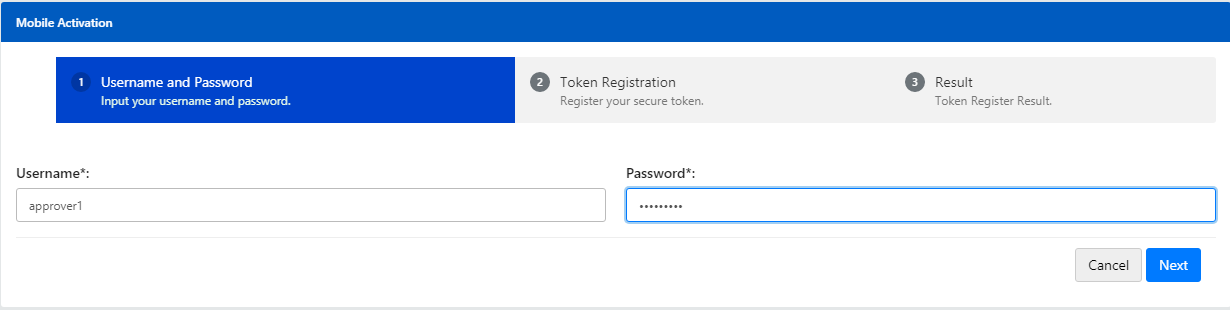


Figure 10: Username and Password Screen

**Input Specification:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Field | Field Type | Rule | Description | M/O |
|  | Username | Text Box | Min Length: 6  Max Length: 16  Alphanumeric | The unique personal identifier for the user. Username is unique in CDB. | M |
|  | Password | Text Box | Min Length: 8  Max Length: 12  Password must contain a mixture of numeric and alphabet format and cannot include these special character [“<>‘%;&+].> | This password use for login. User will be locked after [X] times of failed password validation, i.e. 3 times | M |

Table20: Username and Password Input Specification

**Action:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Action | Type | Description |
|  | Cancel | Button | Contains an action to go back to previous page. |
|  | Next | Button | Contains an action to show “activate new Secure Pass” screen |

Table 21: Username and Password Action

**List of available messages for the screen:**

|  |  |  |
| --- | --- | --- |
| **No** | **Event** | **Error Description** |
|  | Username is not inserted | Username is required. |
|  | Password is not inserted | Password is required. |
|  | Invalid username | Invalid username or password. |
|  | Invalid Password | Invalid username or password. |

Table 22: Username & Password Input available errors

***Step 3(at UPASS):***

1. Single User scan the QR image using UPASS application
2. System will display the new password and confirm password for UPASS application.

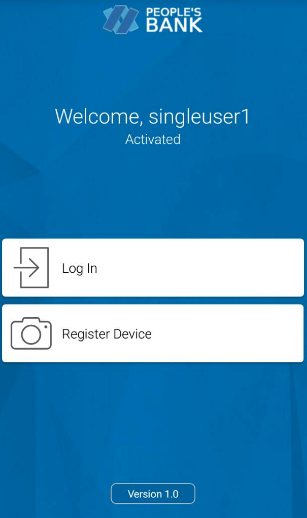


Figure 11: UPASS Login Screen

**Action:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Action | Type | Description |
|  | Register Device | Button | Contains an action to scan the QR code generated and display the new password and confirm password for UPASS application. |

Table 21: Username and Password Action

1. After password confirmation, system will display the Registration Code.
2. After entered the Registration Code at IBS, user click on “Next” button to scan the QR image at IBS Activate Token Result page to complete the registration.

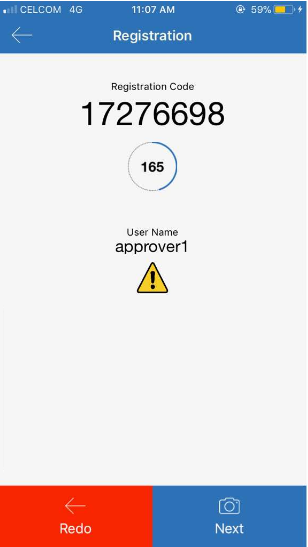


Figure 12: UPASS Registration Code Screen

***Step 3(at IBS):***

1. Single User enters the Registration Code generated at UPASS application then click on “Next” button.



Figure 10: Secure Pass Input Screen

**Input Specification:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Field | Field Type | Rule | Description | M/O |
|  | Registration Code | Text Box | Match Length:13  Numeric | The unique identifier for the user to register a UPASS | M |

Table 22: Assign New Secure Pass Specification

**Action:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Action | Type | Description |
|  | Back | Button | Contains an action to go back to previous page. |
|  | Next | Button | Contains an action to show “successful activation of mobile device for UPASS token” screen |

Table 23: Assign New Secure Pass Action

**List of available messages for the screen:**

|  |  |  |
| --- | --- | --- |
| **No** | **Event** | **Error Description** |
|  | Secure Pass Serial number is not inserted | Secure Pass Serial number is required. |
|  | Invalid Secure Pass | Your Secure Pass serial number is invalid. |

Table 24: Secure Pass Input available errors

***Step 4:***

1. CDB System validates the Registration and activates the UPASS. CDB System displays the result to the user. Single User can go back to Login Screen by click the “Proceed to Login” button.
2. Single User is required to scan the QR image at IBS Activate Token Result page to complete the registration at UPASS.

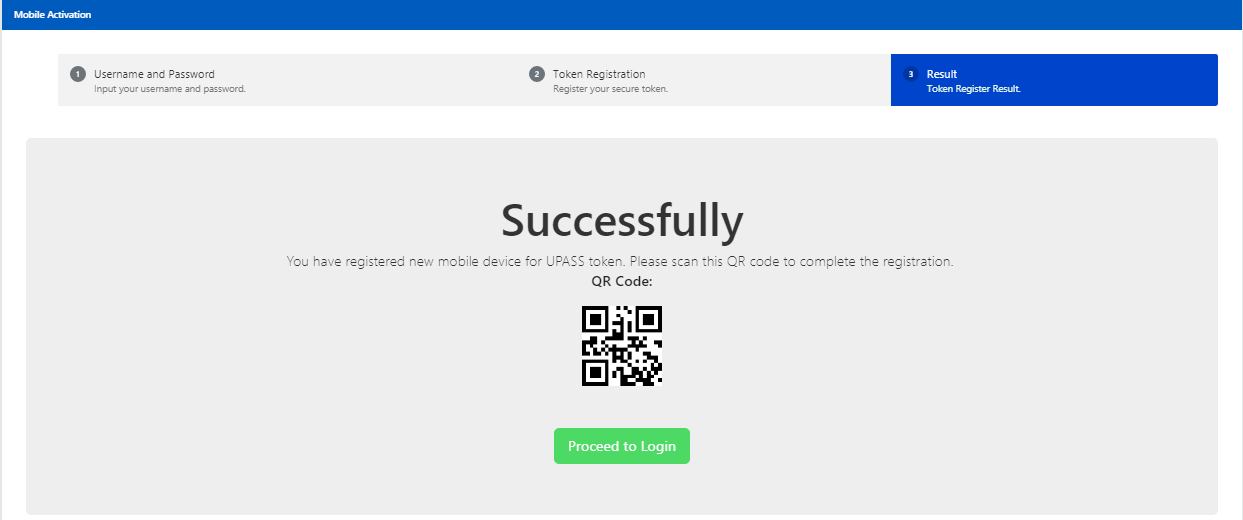


Figure 11: Token Register Result Screen

**Display Fields:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Field | Format | Description |
|  | Successfully  You have registered new mobile device for UPASS token. Please scan this QR code to complete the registration. | Text | Notification to show that the UPASS successfully activated |

Table 25: Token Register Result Display Field

**Action:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Action | Type | Description |
|  | Proceed to Login | Button | Go back to Login page |

Table 26: Token Register Result Action

# Reset Password

Single User uses this feature to reset their password in case they forget their password or if their account is locked. After resetting the information, user can regain access to the CDB system.

## Reset Password / Unlock for Single User

### Process Flows



Diagram 5: Reset Password / Unlock Single User for Initiator or Approver Flow Diagram

### Screen Flows

***Step 1:***

1. Single User access to Reset Password screen and CDB System display Reset Password screen.

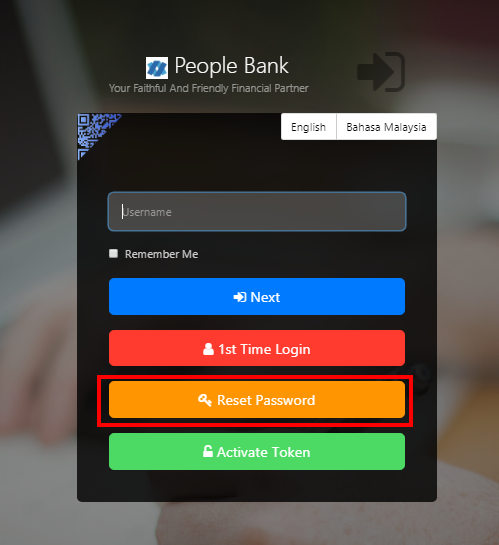


Figure 12: Login screen

**Action:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Action | Type | Description |
|  | Reset Password | Hyperlink | This action will be used to display Reset Password. |

Table 26: Reset Password Selection Action

1. CDB System display Reset Password Selection screen,
2. Single User selects ‘Corporate User’.

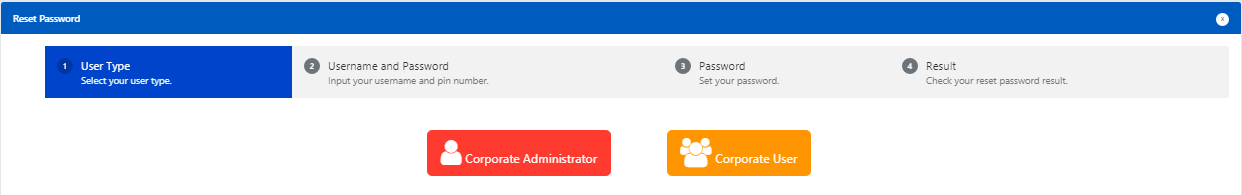


Figure 13: Reset Password Selection screen

**Action:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Action | Type | Description |
|  | Corporate User | Hyperlink | This actions will be used to display Reset password with username and password screen |

Table 27: Reset Password Selection Action

***Step 2:***

1. CDB System display Reset Password screen
2. Single User input Username and Password and click on the “Next” button.
3. CDB System validates Username and Password. After the validation, it will display Reset Password screen.

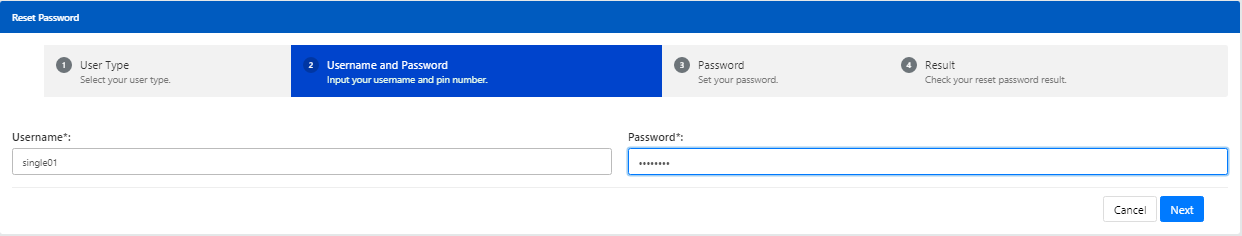


Figure 14: Username and Password screen

**Input Specification:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Field | Field Type | Rule | Description | M/O |
|  | Username | Text Box | Min Length: 6  Max Length: 16  Alphanumeric | The unique personal identifier for the user. Username is unique in CDB. | M |
|  | Password | Text Box | Min Length: 8  Max Length: 12  Password must contain a mixture of numeric and alphabet format and cannot include these special character [“<>‘%;&+].> | This default password use for reset password. | M |

Table 28: Username & Password Input Specification

**Action:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Action | Type | Description |
|  | Next | Button | Contains an actions to validate Username and Password if correct then display Reset Password screen |
|  | Cancel | Button | Contains an action to return to the previous page. |

Table 29: Username & Password Input Action

**List of available messages for the screen:**

|  |  |  |
| --- | --- | --- |
| **No** | **Event** | **Error Description in English** |
|  | Username is not inserted | Username is required. |
|  | Password is not inserted | Password is required. |
|  | Invalid username | Invalid username or password. |
|  | Invalid Password | Invalid username or password. |

Table 30: Username & Password Input available errors

***Step 3:***

1. Single User input the New Password and Confirm Password in Reset Password screen and clicks on the “Next” button to proceed with Reset Password or “Back” button to go back to previous screen.

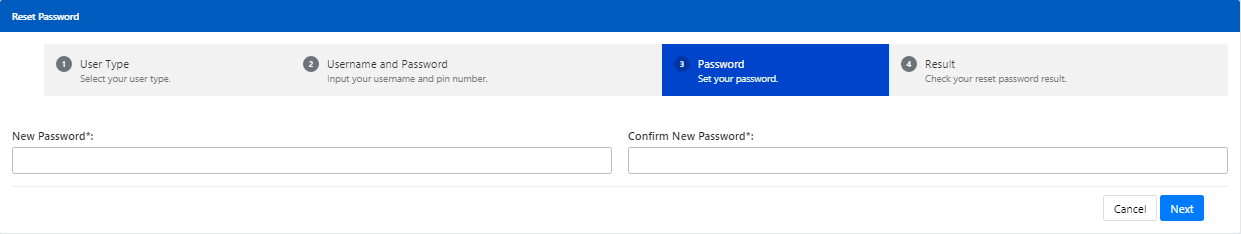


Figure 15: Reset Password screen

**Input Specification:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Field | Field Type | Rule | Description | M/O |
|  | New Password | Text Box | Min Length: 8  Max Length: 12  Password must contain a mixture of numeric and alphabet format and cannot include these special character [“<>‘%;&+].> | Input the new password to replace the existing password | M |
|  | Confirm Password | Text Box | Must be same as Password field | Confirm the new password | M |

Table 31: Reset Password Input Specification

**Action:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Action | Type | Description |
|  | Back | Button | Contains an action to return to the previous page. |
|  | Next | Button | Contains an action to saves the new Password to the database |

Table 32: Reset Password Input Action

**List of available messages for the screen:**

|  |  |  |
| --- | --- | --- |
| **No** | **Event** | **Error Description in English** |
|  | Password is not inserted | Password is required. |
|  | Confirm Password is not inserted. | Confirm Password is required. |
|  | Fill in password contains with one of the criteria below:   1. Special character ["<>'%;&+].>Digit only 2. alphabets only | Password must contain a mixture of numeric and alphabet format and cannot include these special character [“<>‘%;&+].> |
|  | Invalid Confirm Password | Confirm Password must be the same as Password |

Table 33: Reset Password available errors

1. CDB System saves the New Password to IB Database and display the result to Single User. Single User can go back to Login screen by click the “Proceed to Login” button.

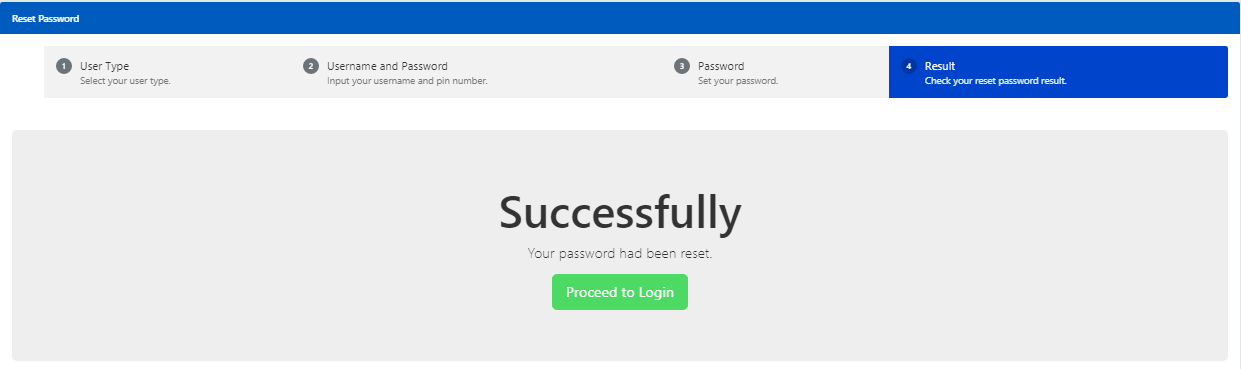


Figure 16: Reset Password Result screen

**Display Fields:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Field | Format | Description |
|  | Successfully  Your password had been reset | Text | Notification to show that the password successfully reset |

Table 34: Reset password result Field

**Action:**

|  |  |  |  |
| --- | --- | --- | --- |
| No | Action | Type | Description |
|  | Proceed to Login | Button | Contains an action to go back to the main page to login |

Table 35: Reset password result Action

# Appendix 1: System Security

|  |  |  |  |
| --- | --- | --- | --- |
| No | Single User ID and Password Control | Requirements | Remark |
|  | Single User ID | Single or combination of numeric, alphabet or alphanumeric. Underscore is accepted. **6 – 16** characters. | The rule is not parameterized. |
|  | Maximum password expiration | **No expiration** | System wide support and can be parameterized via the system configuration file |
|  | Password | Password must contain a mixture of numeric and alphabet format and cannot include these special character ["<>'%;&+].>  Permitted Password length are **8 - 12** characters |  |
|  | Maximum failed log-in attempts | **3 times.** (The Single User ID will subsequently be locked (disabled)) | The maximum number of attempts can be parameterized via the system configuration file. If the Single User ID is locked, the user must send a request to the administrator to reset the password. The application will force the user to change their password upon login. |
|  | Inactive/Dormant ID | Single User ID is automatically disabled by the system after **90** days of inactivity. | The number of days can be parameterized via the system configuration file. |
|  | Duplicate password control | For a minimum of **12** generations, the same passwords cannot be reused. | The number of generations can be parameterized via the system configuration file. |
|  | Last sign on information displayed | The last signed on details will be displayed to the user upon logging into the system | This is a standard feature. |
|  | Changing of passwords by user | Single User may change their passwords anytime they wish | This is standard feature. |
|  | No deletion of Single User IDs from application | Single User IDs that are obsolete must be able to be deleted (instead of just suspended) from the application | The same Single User ID cannot be reused even if restored. The deleted user will not show up on the user enquiry screen, but the record will still be stored in the database. |
|  | Password storage | Password is hashed using SHA-256 hashing algorithm | Combination of nonce and Password is encrypted using SHA-256 before being stored into Database. The hashed value will be used for authentication |

Table 36: Single User Authentication Rules

# Appendix 2: List Allowable Values

|  |  |  |
| --- | --- | --- |
| Field | Type | Values |
| Login as | Dropdown list | * Initiator * Approver |
| Status | Text field | * Successful * Pending * Unsuccessful |
| Action (Account details) / Quick Link | Dropdown list | * Account Details * Transaction History * BSN Online Trxn History |
| Action Status / Approver Status | Text field | * Approve * Reject |
| Batch Status | Text field | * Pending * Accepted |
| User Role | Dropdown list | * Initiator * Approver |
| User Status | Dropdown list | * New * Active * Suspended * Locked * Unlocked * Dormant |
| Secure Pass Status | Dropdown list | * Not assigned * Assigned * Faulty |

Table 37: List Allowable Values

# Appendix 3: Internet Banking “Text” Input Fields Specification

| No. | Item/Field | Data Type | Format & Length |
| --- | --- | --- | --- |
|  | Username (IB login ID) | Alphanumeric | * Min Length: 6 * Max Length: 16 |
|  | Password | Alphanumeric | * Min Length: 8 * Max Length: 12 * Minimum 1 numeric * Minimum 1 alphabet |
|  | Token Serial | Numeric | * Length: 13 |
|  | Token Pin | Numeric | * Length: 6 |
|  | Date | Date | * Format: DD/MM/YYYY |
|  | Transaction Amount | Decimal | * Max Length: 15 * Format: Decimal 15,2 |
|  | Transaction Remarks | Alphanumeric | * Max Length: 30 |
|  | Transaction Reference No | Alphanumeric | * Max Length: 20 |
|  | Transaction Details | Alphanumeric | * Max Length: 20 |
|  | Email | Email | * Max Length: 60 * Format: <email>@<emailhost>.<extension> |
|  | Beneficiary Nickname | Alphanumeric | * Max Length: 60 |
|  | Interbank Beneficiary Account Number | Numeric | * Max Length: 20 |
|  | Interbank Holder Name | Alphanumeric | * Max Length: 40 |
|  | Bill Account Number | Alphanumeric | * Max Length: 30 |
|  | Favourite Payee Nickname | Alphanumeric | * Max Length: 60 |
|  | Approval Remark | Alphanumeric | * Max Length: 30 |
|  | Name | Alphabet | * Max Length: 100 |
|  | Telephone Number | Alphanumeric | * Max Length: 32 |
|  | Mobile Number[[1]](#footnote-1) | Alphanumeric | * Max Length: 32 |
|  | Address | Alphanumeric | * Max Length: 256 |
|  | Approval Matrix | Numeric | * Length: 1 |

Table 38: Text Input Field Specifications

# Appendix 4: Acceptable Characters for Validation

|  |  |
| --- | --- |
| Validation Name | Acceptable characters |
| Text | No limitations |
| Alphanumeric with Dot & Slash | a-z, A-Z  0-9  Dot / Period (.)  Slash (/) |
| Alphanumeric with Space | a-z, A-Z  0-9  Space |
| Alphanumeric with spaces and underscore | a-z, A-Z  0-9  Space  Underscore (\_) |
| Alphanumeric with Space & Symbols | a-z, A-Z  0-9  Space  Ampersand (&)  Apostrophe (', `)  Left Bracket (()  Right Bracket ())  Comma (,)  Alias (@)  Question Mark (?) |
| Email | a-z, A-Z  0-9  Dot / Period (.)  Minus/Hypen (-)  Underscore (\_)  Minus/Hypen (-)  Must have one alias (@)  Format: <value>@<value>.<value> |
| Character(s) acceptable for URL path  URL Path | a-z, A-Z  0-9  Dot / Period (.)  Space  Ampersand (&  Plus (+)  Minus/Hypen (-)  Slash (/)  Equal (=)  Question Mark (?)  Underscore (\_) |

Table 39: Acceptable Characters for Validations

# Appendix 5: Download Report

Depending on the user’s browser settings and software availability,

* 1. the report can be automatically opened using default software for .xls file type, such as Microsoft Excel or OpenOffice.org Calc
  2. a dialog box will pop-up, asking further action from administrator whether to open the report using with software such as Microsoft Excel or OpenOffice.org Calc or to save the file

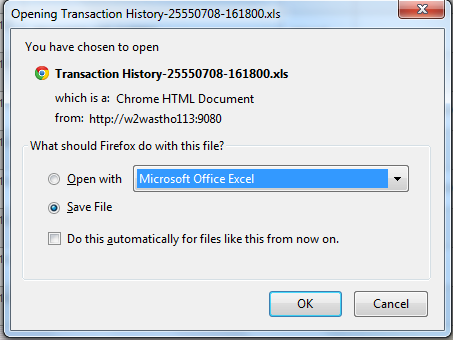


Figure 17: Example dialog box for Download Report

# Appendix 6: Glossary

| **Term** | **Definition** |
| --- | --- |
| CDB | **C**orporate **D**igital **B**anking System |
| IB | **I**nternet **B**anking |
| IBS | **I**nternet **B**anking **S**ystem |
| IBAM | **I**nternet **B**anking **A**dministration **M**anager (the administration module) |
| SME | **S**mall & **M**edium **E**nterprise |
| TAC | **T**ransaction **A**uthorization **C**ode  TAC is a temporary random six digits security code generated by the authentication server and sent to user by SMS using a SMS gateway. TAC is required as the second level security authentication before committing any bank transactions and user profile updates. |
| OTP | **O**ne **T**ime **P**assword, in this document it meant for the Secure Pass or Token 6 digit PIN from VASCO. |
| BNM | **B**ank **N**egara **M**alaysia |
| CASA | Current & Savings Account |
| FD | Fixed Deposit |

Table 40: Glossary

--- END ---

1. *Mobile Number format subject to change according to SMS Gateway specification* [↑](#footnote-ref-1)