# Table of Contents

1. Preface........................................................................................................................................... 4  
   1.1 Intended Audience .................................................................................................................. 4  
   1.2 Documentation Accessibility .................................................................................................. 4  
   1.3 Access to Oracle Support ......................................................................................................... 4  
   1.4 Structure .................................................................................................................................. 4  
   1.5 Related Information Sources ................................................................................................. 4  
2. Transaction Host Integration Matrix................................................................................................. 5  
3. Soft Token Application .................................................................................................................... 6  
   FAQs.................................................................................................................................................. 11
1. **Preface**

1.1 **Intended Audience**

This document is intended for the following audience:

- Customers
- Partners

1.2 **Documentation Accessibility**


1.3 **Access to Oracle Support**


1.4 **Structure**

This manual is organized into the following categories:

*Preface* gives information on the intended audience. It also describes the overall structure of the User Manual.

*Introduction* provides brief information on the overall functionality covered in the User Manual.

The subsequent chapters provide information on transactions covered in the User Manual.

Each transaction is explained in the following manner:

- Introduction to the transaction
- Screenshots of the transaction
- The images of screens used in this user manual are for illustrative purpose only, to provide improved understanding of the functionality; actual screens that appear in the application may vary based on selected browser, theme, and mobile devices.
- Procedure containing steps to complete the transaction- The mandatory and conditional fields of the transaction are explained in the procedure.

If a transaction contains multiple procedures, each procedure is explained. If some functionality is present in many transactions, this functionality is explained separately.

1.5 **Related Information Sources**

For more information on Oracle Banking Digital Experience Release 18.1.0.0.0, refer to the following documents:

- Oracle Banking Digital Experience Licensing Guide
- Oracle Banking Digital Experience Installation Manuals
## 2. Transaction Host Integration Matrix

### Legends

<table>
<thead>
<tr>
<th></th>
<th>No Host Interface Required.</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Pre integrated Host interface available.</td>
</tr>
<tr>
<td>✗</td>
<td>Pre integrated Host interface not available.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sr No</th>
<th>Transaction / Function Name</th>
<th>FCR 11.7.0.0.0</th>
<th>UBS 12.3.0.0.0</th>
<th>UBS 12.4.0.0.0</th>
<th>UBS 14.0.0.0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Soft Token Application</td>
<td>NH</td>
<td>NH</td>
<td>NH</td>
<td>NH</td>
</tr>
</tbody>
</table>
3. **Soft Token Application**

Security tokens are generally used in environments with higher security requirements as part of a multifactor authentication system. Soft tokens give the same security advantages of multifactor authentication, while simplifying distribution and lowering costs.

A Soft token app is a two-factor authentication based on Passcode or PIN and something you have (an authenticator such as smartphone), protecting your sensitive networked information and data. A soft token is a software-based security token that generates a single-use 6 digit login PIN or passcode.

**To generate a single-use login PIN:**

1. Launch **PaySecure** App.
2. In the **Bank Username** field enter the username.
3. In the **Password** field enter the password.

**Register page**
Field Description

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Login id provided by the bank.</td>
</tr>
<tr>
<td>Net Banking Password</td>
<td>The password for channel access.</td>
</tr>
</tbody>
</table>

4. Click Register to register on the app. The Set a PIN screen appears with prompt to select a new PIN.

Set a PIN

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PaySecure PIN</td>
<td>The PIN number to be set for the PaySecure.</td>
</tr>
</tbody>
</table>

5. In the PaySecure PIN field, enter the PIN to be set.
6. Click Continue to proceed to the next screen.
## Field Description

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Retype PaySecure PIN</strong></td>
<td>The code sent to the customer to their registered email id or mobile number.</td>
</tr>
</tbody>
</table>

7. In the **PaySecure PIN** field re-enter a PIN.
8. Click **Continue** to proceed to next screen.
   OR
   Click **Back** to go back to previous screen.
Software Token Code

Field Description

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the code</td>
<td>The Soft Token code displayed on transaction screen.</td>
</tr>
</tbody>
</table>

9. In the **Enter the code** field, enter the code appear on transaction screen.

10. Click **Continue** to proceed to next screen. The Soft Token code generated successfully.
11. Use the generated Soft Token PIN to complete the current transaction.

**Note:**
For the Time based Soft Token Code, the code dynamically changes after every 30 sec. User has to configure App while installing and choose TOTP (Time-based one-time password) option which is a temporary passcode.

By default HOTP (HMAC-based one-time password (OTP) algorithm) is selected, which is internet based.
**FAQs**

1. **While setting up secure PIN in App can, 2FA be introduced post login with credentials and before setting up PIN?**
   
   Yes, this is supported in the product. (Only OTP).

2. **What other options are available other than PIN to setup in App like Fingerprint, Eye, pattern, etc. In addition, can we change/switch to other options after login to App?**
   
   Only PIN is supported out of box.

3. **What is process/workflow of forget PIN? If PIN is used to login App and person forgets so how can he reset or change it?**
   
   Currently, forgot PIN is not supported. Incase if user enters the incorrect PIN for more than 'N' times, then the user will need to re-register in the app using his internet banking credentials and redefine the PIN.

4. **If incorrect PIN is entered for, 3/5 configurable times then what are consequences like will App be lock, any change require to be done by ADMIN/User?**
   
   User/App will not get locked but will be forced to re-register in the app using his internet banking credentials and redefine the PIN.

5. **This APP is supported in Android/IOS with which version. In addition, is it supported by other Platform like blackberry/Windows/etc. and with which respective version?**
   
   No, only iOS (11, 12) and android (six and above) are supported out of box.
6. Can this App be installed in rooted device?
Before the soft token app, installation there will be a check if a device is rooted. Whereas, post app installation, if a device is rooted, there will be no change since this is an offline app.

7. Is internet is required to use this App post first time login to use or can be used without internet?
Internet is required during app installation and for first time login. Post that internet is not required.

8. Will time difference of mobile device in terms of time zone and with different timings set to phone (i.e. 15 min early) and OBDX server will cause any problem?
HOTP does not have any impact. In case of TOTP, the time zone offsets are already handled. However, in case of a device time mismatching with the server time, in that case there will be issue.

9. If a person changes mobile device or if a person uninstall and install the App in same device, is activation again required?
User will need to re-register in the app using his internet banking credentials and redefine the PIN.

10. What are all the use cases where App gets lock?
User/App will not be locked but will be forced to re-register in the app using his internet banking credentials and redefine the PIN. There are no use cases for app lock.

11. If App gets lock, can Admin unlock the APP or assist customer to unlock it?
Not applicable.

12. Can language translation can be done for this App?
Yes.

13. What is the Length of token or otp?
Length of the token is configurable, by default it is six.

14. What is the maximum time of code to validate TOTP and HOTP?
Maximum time to validate TOTP is n buckets of 30 seconds, wherein n is configurable and default value is six. As far as HOTP is, concerned expiry is configurable.

15. After how many number if invalid attempts the app will be locked?
Number of allowed invalid attempts are configurable as a part of app build. App will not get locked.

16. Currently OTP & Token is supported from this APP or only Token?
A token, which will be generated by an app, is a onetime password (OTP) to be used to authenticate the transaction.
17. **Is Self-registration is available for user without admin intervention. Currently bank is live with customer and has one maintenance i.e. checkbox to tick for soft app registration can these be short-circuited and user himself register for this?**

   There is no admin intervention required for app registration; the user himself will register for the app.

18. **Can I register PaySecure app on multiple devices for same user?**

   No, registering PaySecure application on multiple devices for the same user is not allowed. The token generated from the latest installed mobile app would be valid.

19. **Can I register multiple user ids using one PaySecure application installed on one device?**

    Yes, you can register multiple users on PaySecure application installed on one device.