Oracle® Banking Digital Experience

Small & Medium Business Soft Token Application User Manual

Release 25.1.0.0.0
G38571-01
September 2025

Oracle Banking Digital Experience Small & Medium Business Soft Token Application User Manual, Release 25.1.0.0.0

G38571-01

Contents

Preface

Purpose

This guide is designed to help acquaint you with the Oracle Banking application. This guide provides answers to specific features and procedures that the user need to be aware of the module to function successfully.

Before you Begin

Kindly refer to our **Getting Started User Guide** for common elements, including Symbols and Icons, Conventions Definitions, and so forth.

Pre-requisites

Specify **User ID** and **Password**, and login to **Home** screen.

Audience

This document is intended for the following audience:

- Customers
- Partners

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Critical Patches

Oracle advises customers to get all their security vulnerability information from the Oracle Critical Patch Update Advisory, which is available at Critical Patches, Security Alerts and Bulletins. All critical patches should be applied in a timely manner to ensure effective security, as strongly recommended by Oracle Software Security Assurance.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Resources

For more information on any related features, refer to the following documents:

- Oracle Banking Digital Experience Installation Manuals
- Oracle Banking Digital Experience Licensing Manuals

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

Convention	Meaning
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Screenshot Disclaimer

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes; actual screens that appear in the application may vary based on selected browser, theme, and mobile devices.

Acronyms and Abbreviations

The list of the acronyms and abbreviations used in this guide are as follows:

Table 1 Acronyms and Abbreviations

Abbreviation	Description
OBDX	Oracle Banking Digital Experience

Basic Actions

Most of the screens contain icons to perform all or a few of the basic actions. The actions which are called here are generic, and it varies based on the usage and the applicability. The table below gives a snapshot of them:

Table 2 Basic Actions and Descriptions

Action	Description
Back	In case you missed to specify or need to modify the details in the previous segment, click **Back** to navigate to the previous segment.
Cancel	Click **Cancel** to cancel the operation input midway without saving any data. You will be alerted that the input data would be lost before confirming the cancellation.
Next	On completion of input of all parameters, click **Next** to navigate to the next segment.
Save	On completion of input of all parameters, click **Save** to save the details.
Save & Close	Click **Save & Close** to save the data captured. The saved data will be available in **View Business Product** with *In Progress* status. You can work on it later by picking it from the **View Business Product**.
Submit	On completing the input of all parameters, click **Submit** to proceed with executing the transaction.
Reset	Click **Reset** to clear the data entered.
Refresh	Click **Refresh** to update the transaction with the recently entered data.
Download	Click **Download** to download the records in PDF or XLS format.

Symbols and Icons

The following are the symbols/icons you are likely to find in this guide:

Table 3 Symbols and Icons

Symbols and Icons	Description
	Add data segment
	Close
	Maximize
	Minimize
	Open a list
	Open calendar
	Perform search
	View options
	View records in a card format for better visual representation.
	View records in tabular format for better visual representation.

Post-requisites

After finishing all the requirements, please log out from the **Home** screen.

1

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.

Features Supported In Application:

- Online registration
- OTP generation
- Registration
- Login & OTP Generation

1.1 Registration

Business users can register on soft token application (PaySecure Application) using their Digital Banking login credentials. Post validating the credentials, user has to set the new PIN to login into the PaySecure application for generating OTP.

Pre-Requisites

- The user must download Futura Bank PaySecure application and have a valid account with bank with online banking enabled.

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.

Figure 1-1 Register page

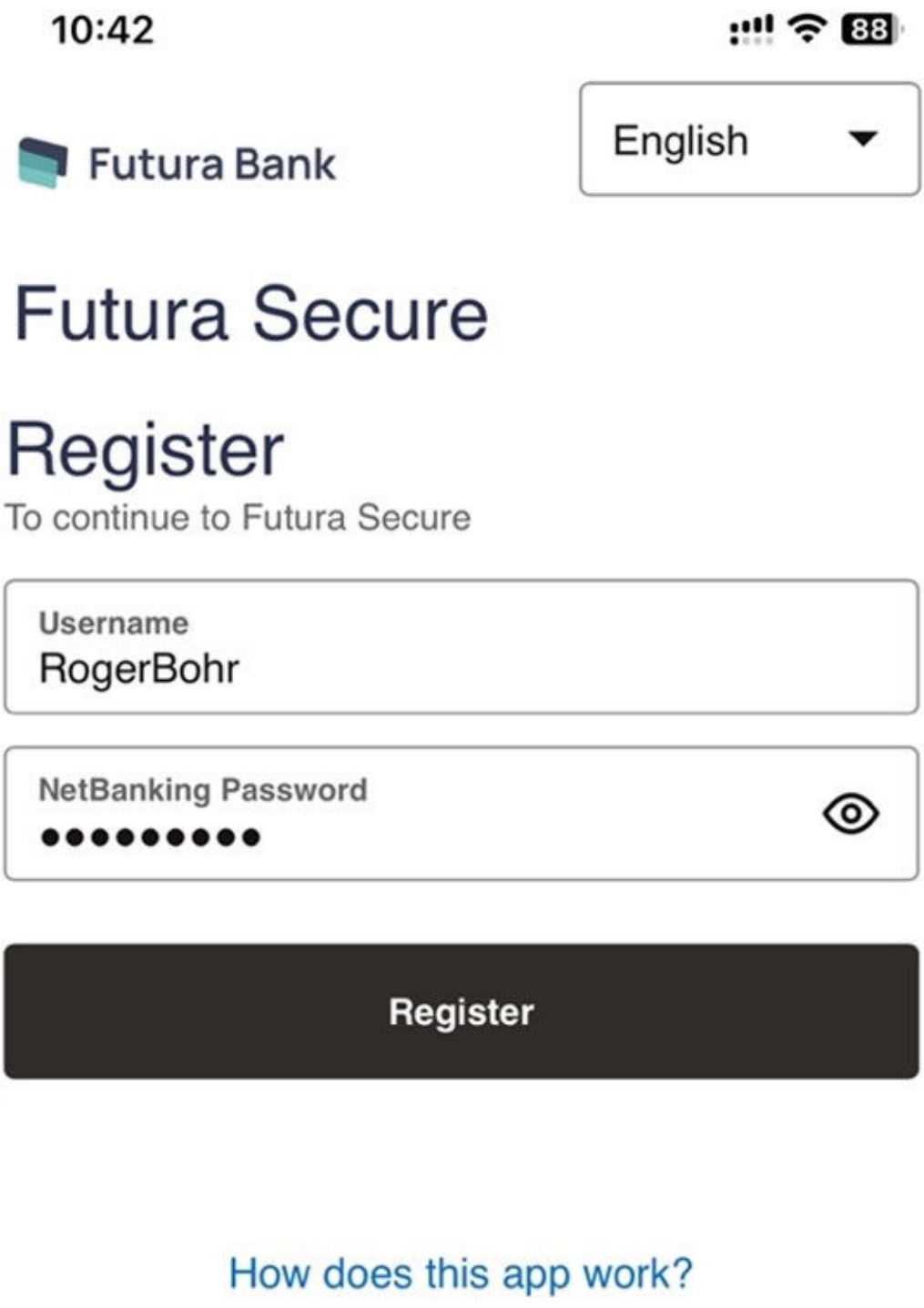


Table 1-1 Field Description

Field Name	Description
Username	Login id provided by the bank.
Net Banking Password	The password for channel access.

4. Click **Register** to register on the app.

   The **Set a PIN** screen appears with prompt to select a new PIN.

Figure 1-2 Set a PIN

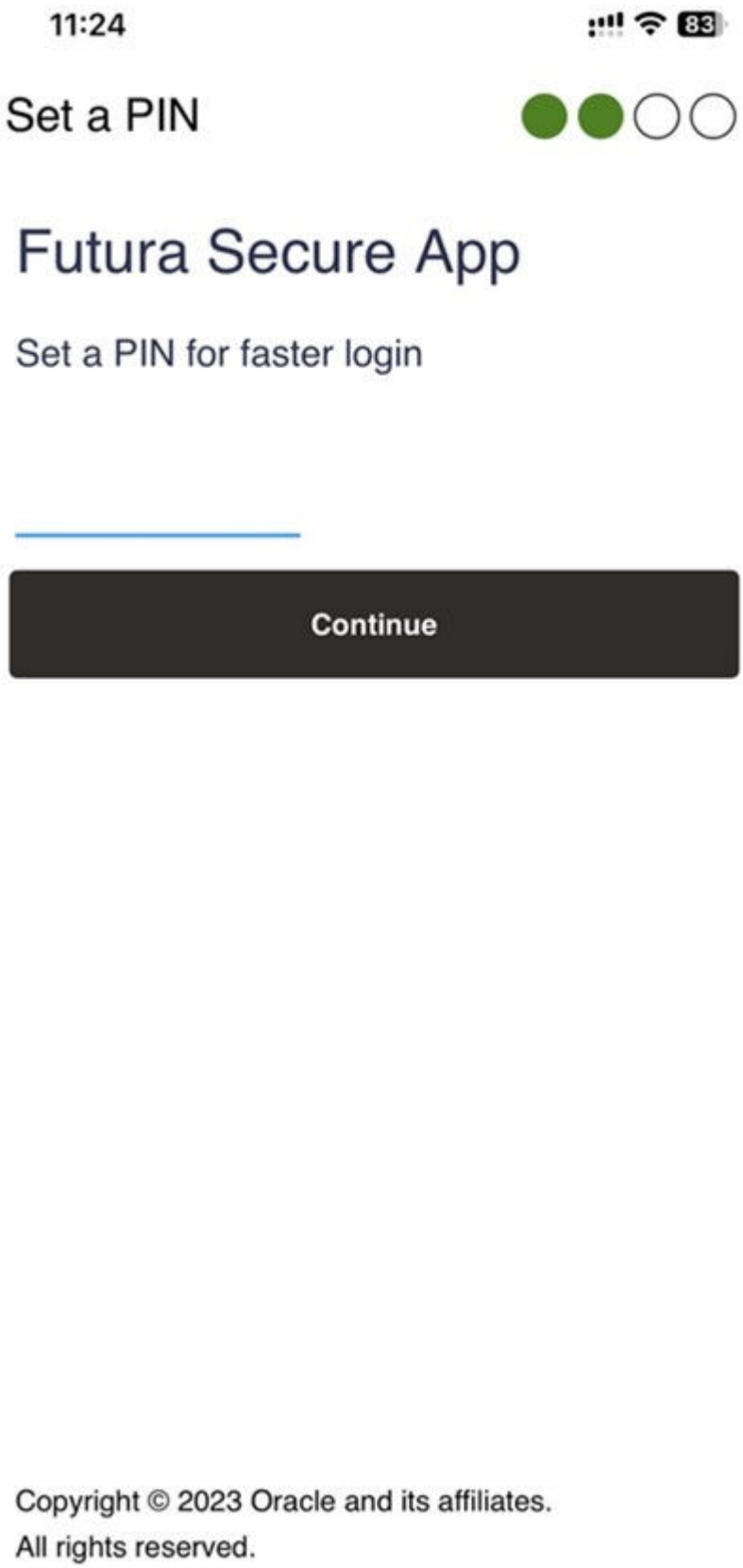


Table 1-2 Field Description

Field Name	Description
Enter PIN	The PIN to be set for the PaySecure.

5. In the **Enter PIN** field, enter the PIN to be set.
6. Click **Continue** to proceed to the next screen.

Figure 1-3 Set a PIN - Re-enter PIN

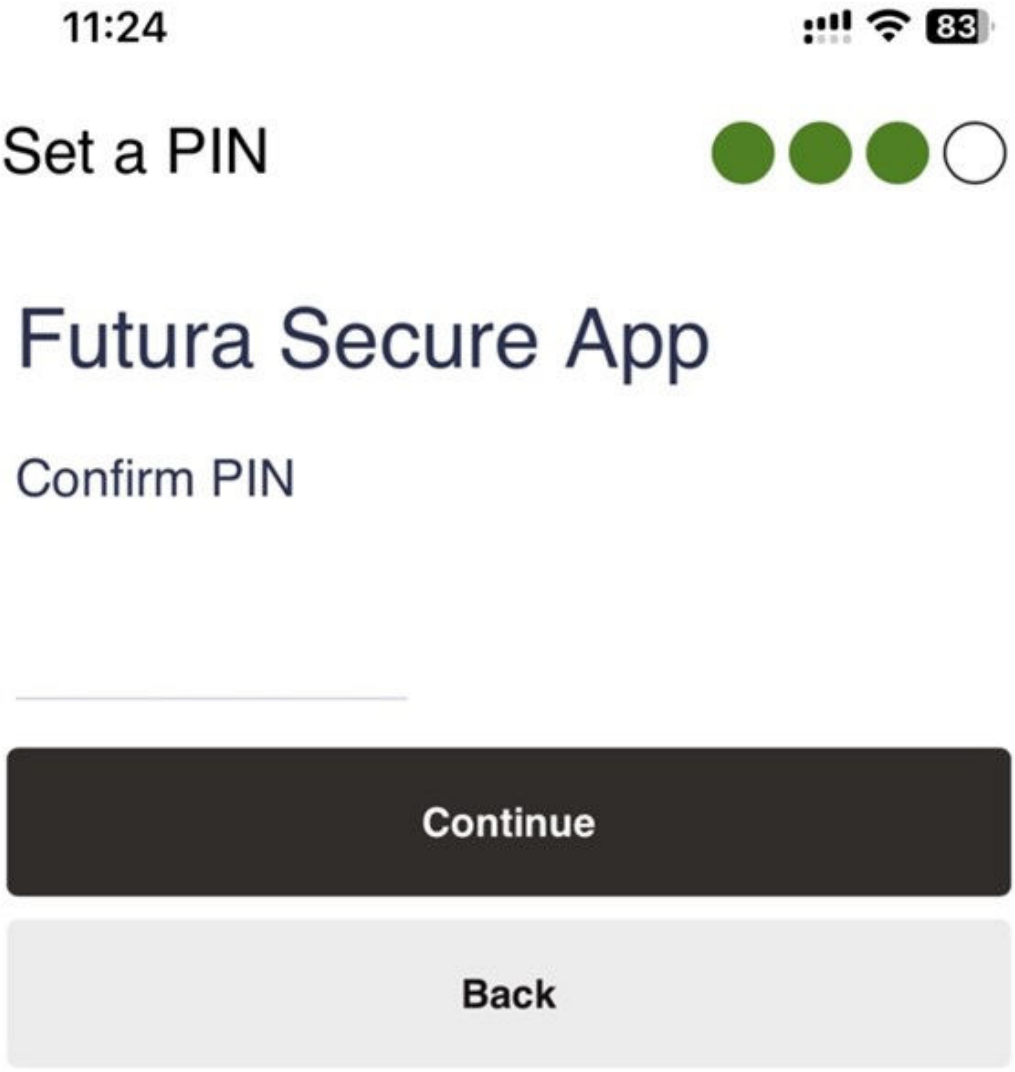


Table 1-3 Field Description

Field Name	Description
Re-enter PIN	Retype PIN number to be set for the PaySecure.

7. In the **Re-enter PIN** field, re-enter a PIN to confirm.
8. Click **Continue** to proceed to next screen. User will be directed to the screen to generate an OTP.

   OR

   Click **Back** to go back to previous screen.

1.2 Login & OTP Generation

Once the registration is successful, from the subsequent logins user has to use the PIN to login into the PaySecure application. Post authentication, user will be provided with an option to either select the user for which OTP is to be generated (if multiple users are registered using same application) or to register another user on same device and application.

To generate OTP or login into PaySecure application:

1. Register on soft token application (PaySecure Application).

Figure 1-4 PaySecure PIN

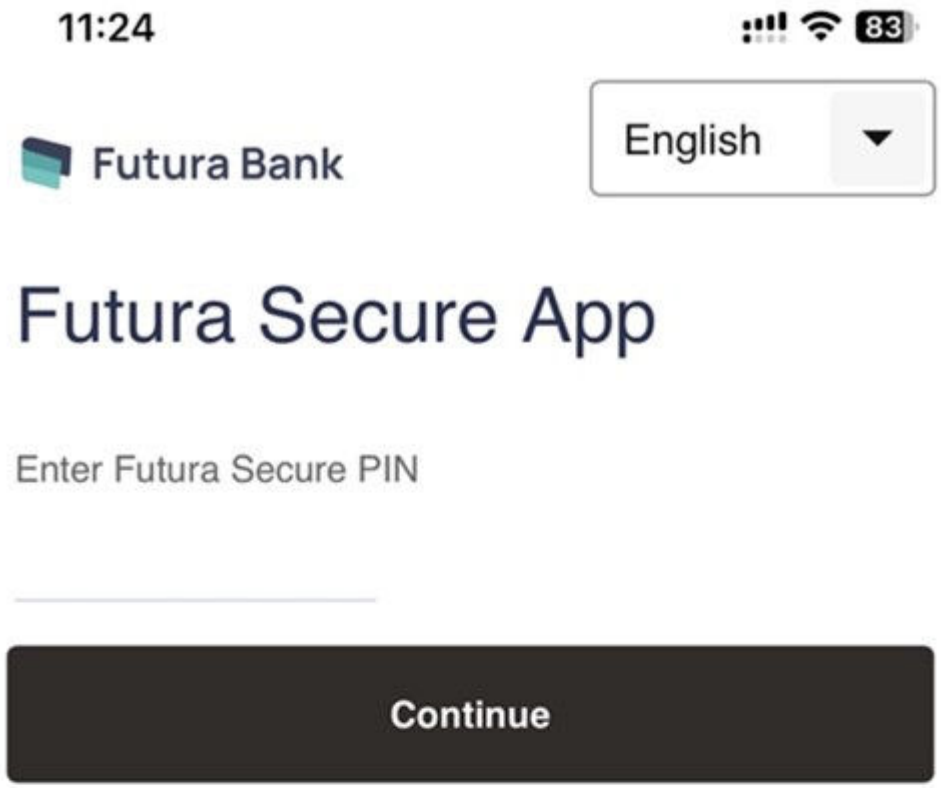


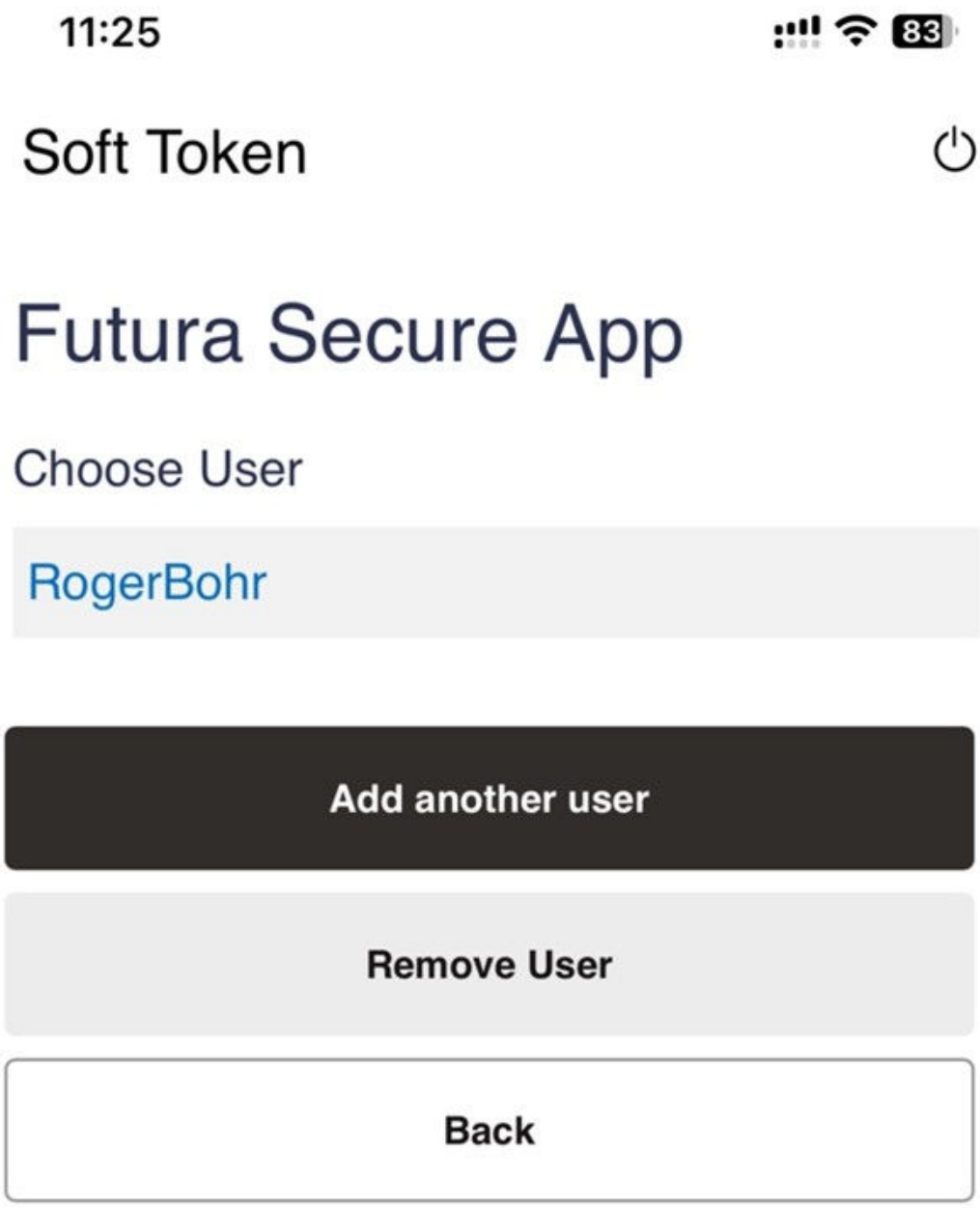
Table 1-4 Field Description

Field Name	Description
Enter PIN	Enter the PIN to login into the application.

2. Enter the **PIN**, and click **Continue**.

   The **Choose User** screen appears.

Figure 1-5 Choose User



3. Select the user. The user is prompted to enter the code.

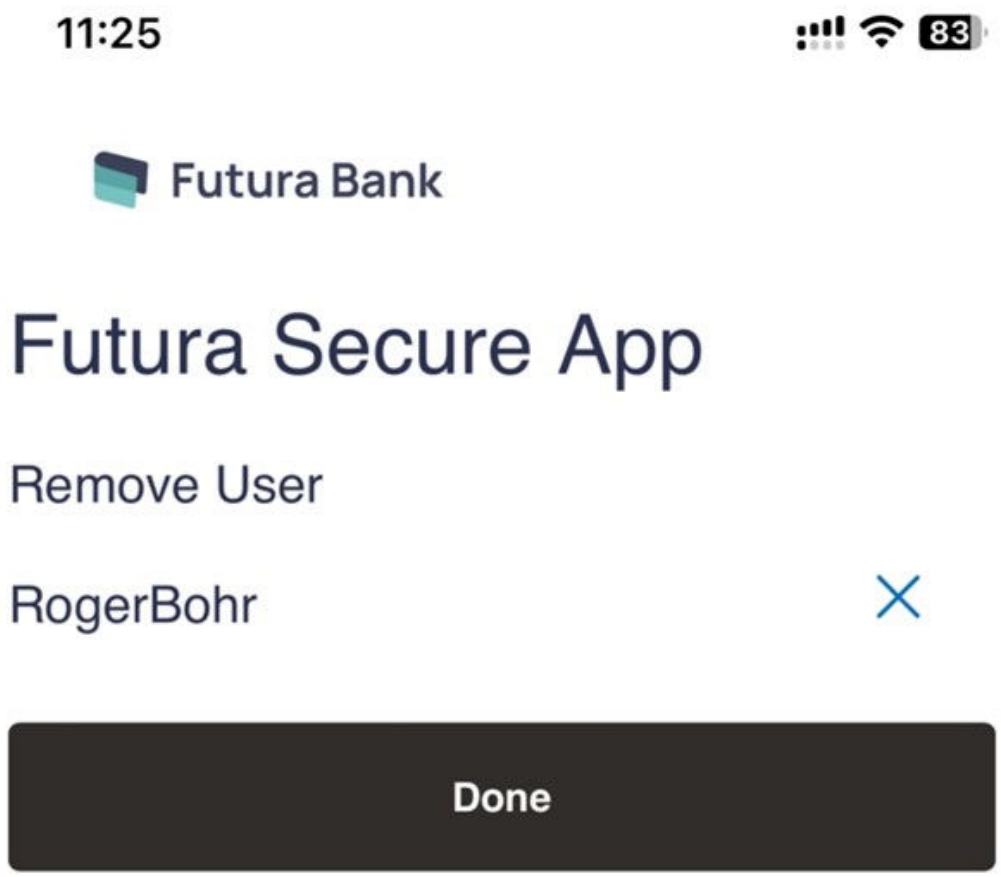
   OR

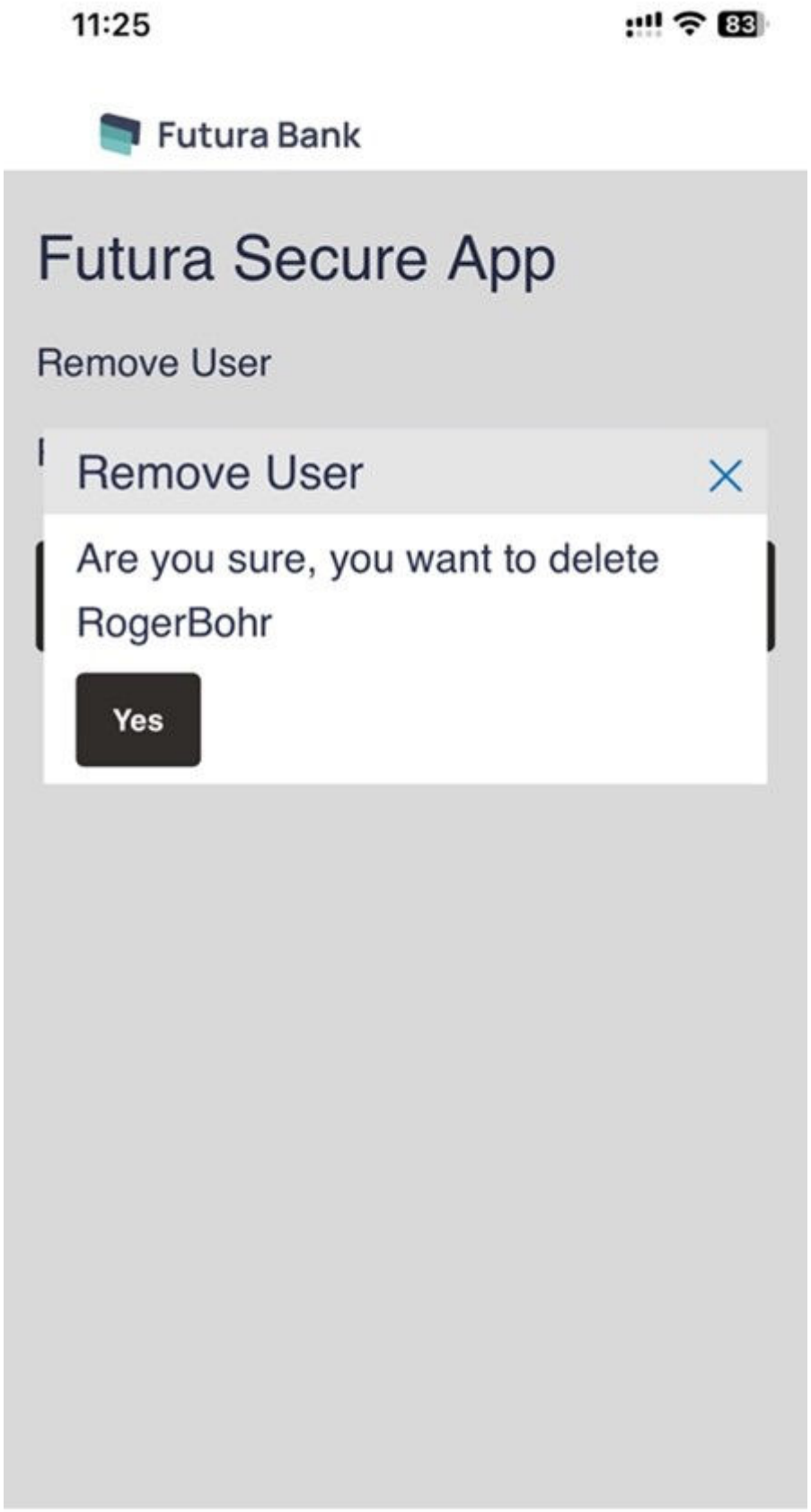
   Click **Add Another User** to add another account. For more information refer **Registration**section.

   OR

   Click **Remove User**.

Figure 1-6 Remove User





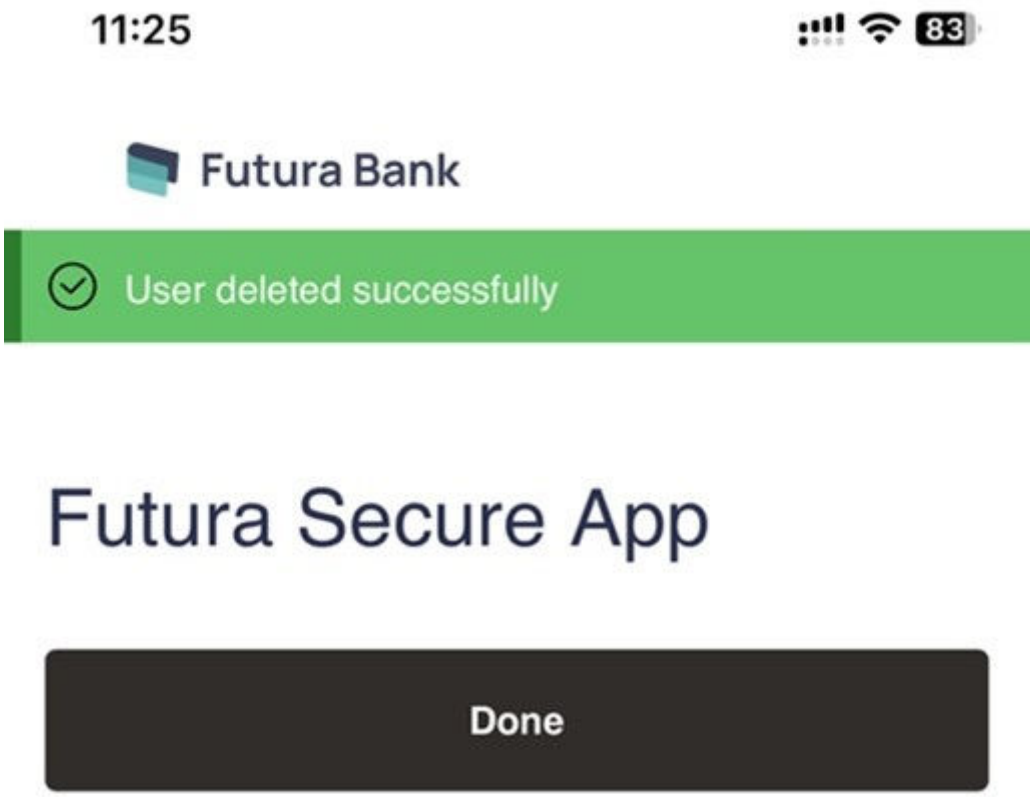
4. Click  icon against a user to remove a user.

   A popup message appears prompting to confirm the user deletion.

5. Click **Yes** to delete the user. User deleted message is displayed.

   User deleted message is displayed.

Figure 1-7 Soft Token Code



6. Click **Done**.

Figure 1-8 Soft Token Code

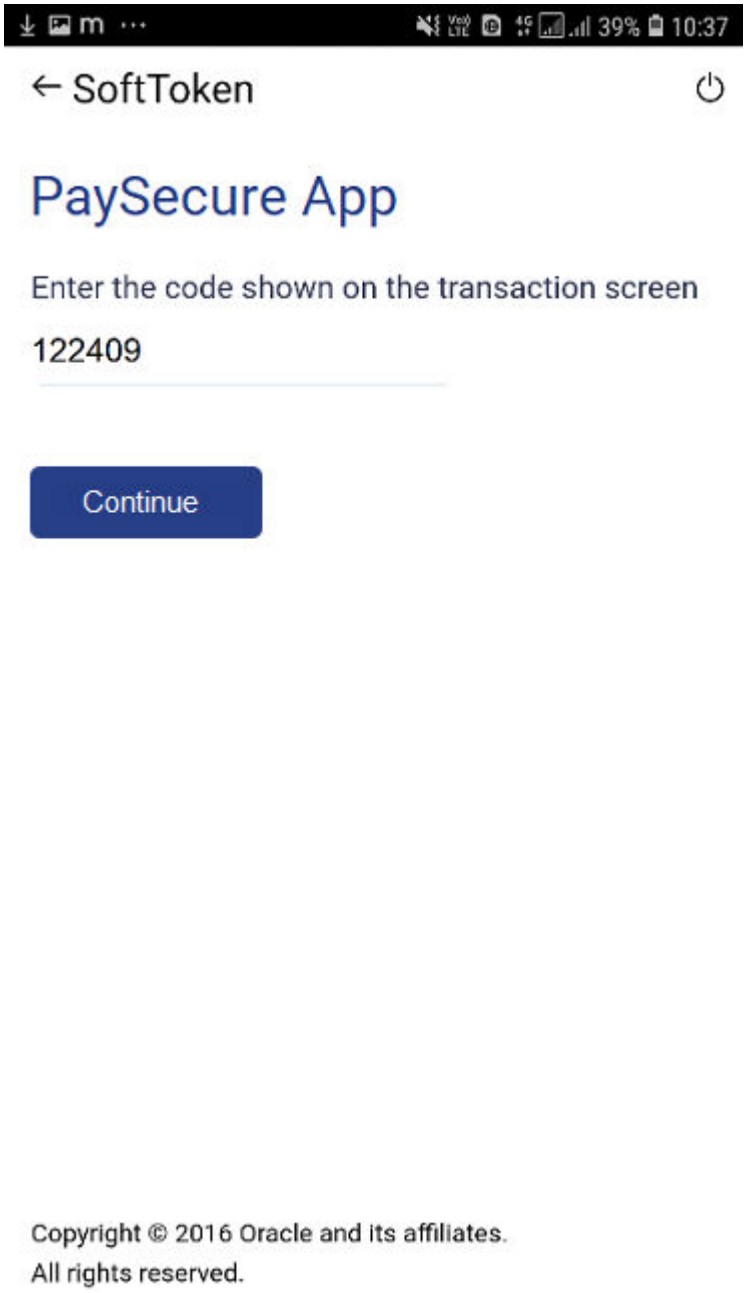


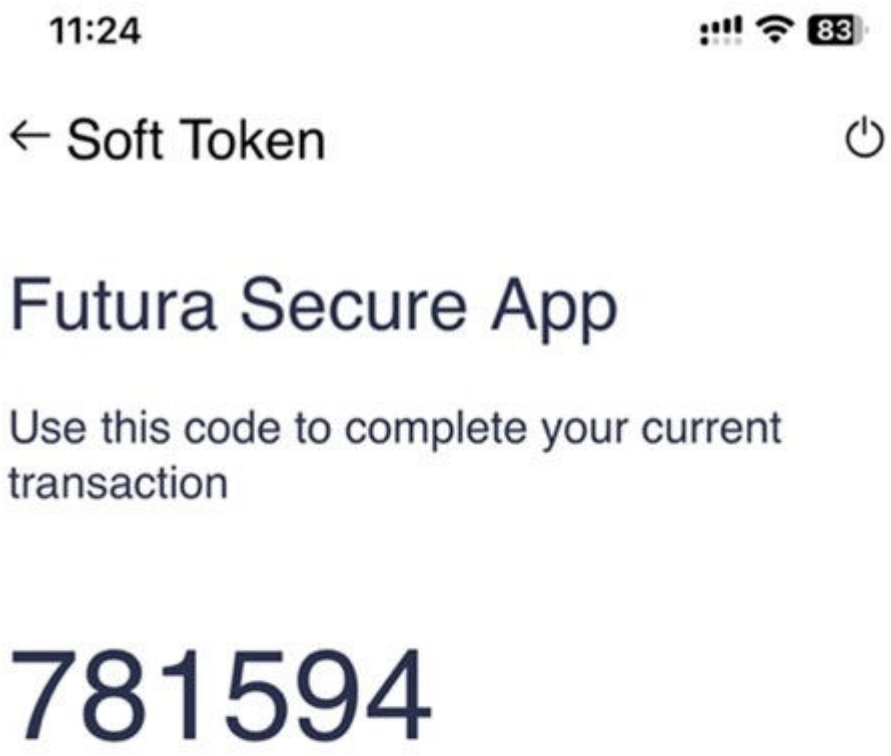
Table 1-5 Field Description

Field Name	Description
Enter Code	The Soft Token code displayed on transaction screen.

7. In the **Enter the code** field, enter the code appear on transaction screen.
8. Click **Continue** to proceed to next screen.

The Soft Token code generated successfully.

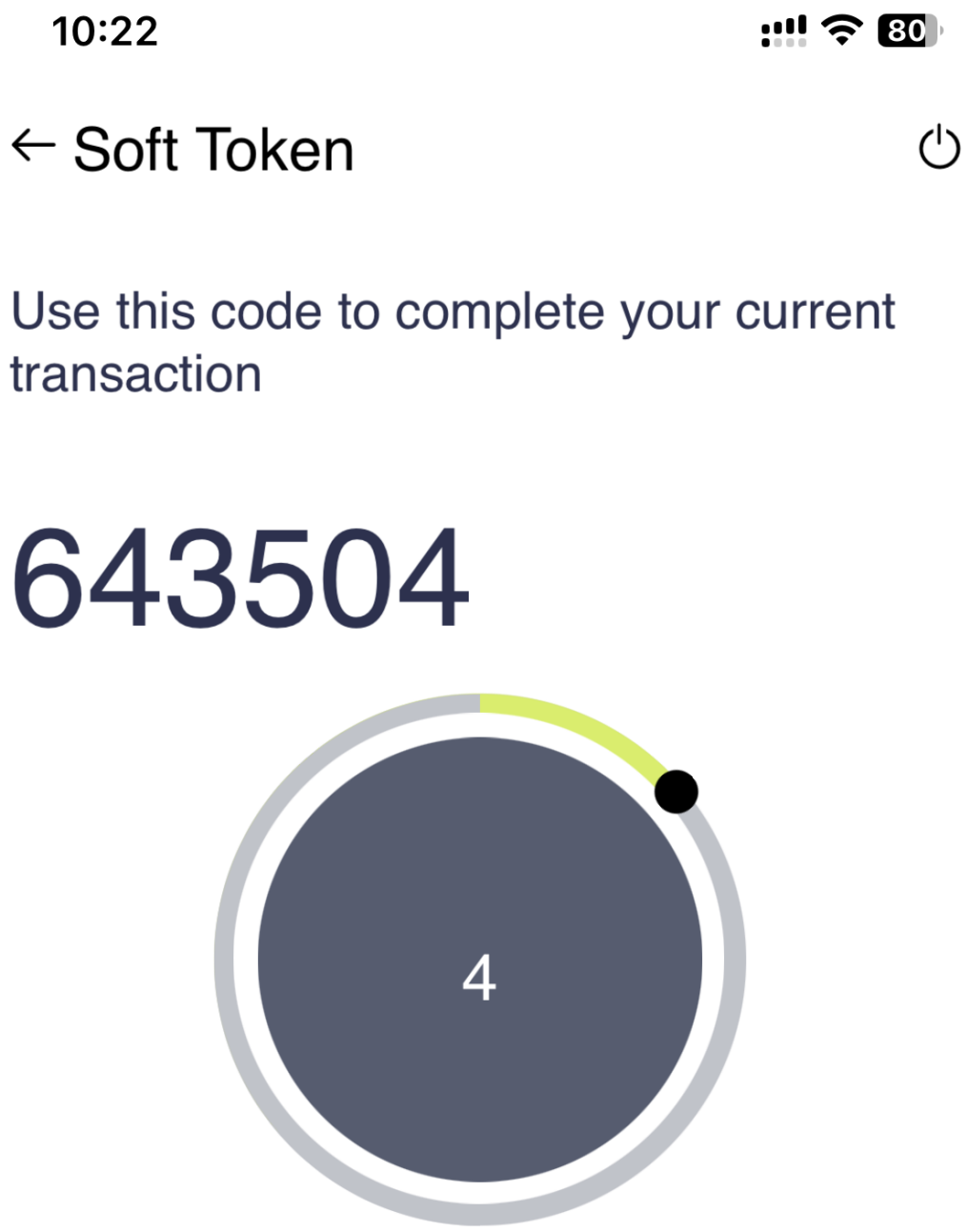
Figure 1-9 Generated Soft Token Code (HOTP based)



9. 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.

Figure 1-10 Generated Soft Token Code (TOTP based)



2 FAQ

1. **While setting up secure PIN in application 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 application 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. **How can I reset the PIN if I forget the PIN?**
   Currently, forgot PIN is not supported. In case 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 beyond the maximum allowed failure attempts then what are consequences?**
   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. **In case of multiple users, is PIN required for all users?**
   No, PIN is not required for all users. PIN is for the App and is setup during first user registration, after which the registered user can add / delete other users.

   For changing the PIN, the App needs to be reinstalled.
6. **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.
7. **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.
8. **Is internet 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.
9. **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.
10. **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.
11. **What are all the use cases where App gets locked?**
    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.

12. **If App gets locked, can the Admin unlock the App or assist customer to unlock it?**
    Not applicable.
13. **Can language translation be done for this App?**
    Yes.
14. **What is the Length of token or OTP?**
    Length of the token is configurable, by default it is six.
15. **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.
16. **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 be locked.
17. **Currently OTP & Token are supported by 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.
18. **Is Self-registration is available for user without admin intervention. Currently bank is live with customer and has one maintenance i.e. check box 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.
19. **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.
20. **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.

Index