Oracle® Banking Digital Experience Cloud Service

Soft Token Application User Manual

Release 25.1.1.0.0
G46549-02
October 2025

Oracle Banking Digital Experience Cloud Service Soft Token Application User Manual, Release 25.1.1.0.0

G46549-02

Copyright © 2015, 2025, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Purpose i
Audience i
Documentation Accessibility i
Diversity and Inclusion i
Conventions ii
Related Resources ii
Screenshot Disclaimer ii
Acronyms and Abbreviations ii
Basic Actions ii
Symbols and Icons iii

1 Soft Token Application

1.1 Registration 1
1.2 Login & OTP Generation 7

2 FAQ

Index

Copyright © 2015, 2025, Oracle and/or its affiliates.

Preface

- Purpose
- Audience
- Documentation Accessibility
- Diversity and Inclusion
- Conventions
- Related Resources
- Screenshot Disclaimer
- Acronyms and Abbreviations
- Basic Actions
- Symbols and Icons

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.

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.

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

Copyright © 2015, 2025, Oracle and/or its affiliates.

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.

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

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

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
OBDXCS	Oracle Banking Digital Experience Cloud Service

Basic Actions

Copyright © 2015, 2025, Oracle and/or its affiliates.

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.

Copyright © 2015, 2025, Oracle and/or its affiliates.

Table 3 (Cont.) Symbols and Icons

Symbols and Icons	Description
	View records in tabular format for better visual representation.

Copyright © 2015, 2025, Oracle and/or its affiliates.

1

Soft Token Application

This topic describes the Soft Token Application process and its features.

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
  This topic provides the systematic instructions to register on soft token application (PaySecure Application) using their Digital Banking login credentials.
- Login & OTP Generation
  This topic provides the systematic instructions of generating OTP and login into PaySecure application.

1.1 Registration

This topic provides the systematic instructions to register on soft token application (PaySecure Application) using their Digital Banking login credentials.

Business users canost validating the credentials, user has to set the new PIN to login into the PaySecure application for generating OTP.

Pre-Requisites

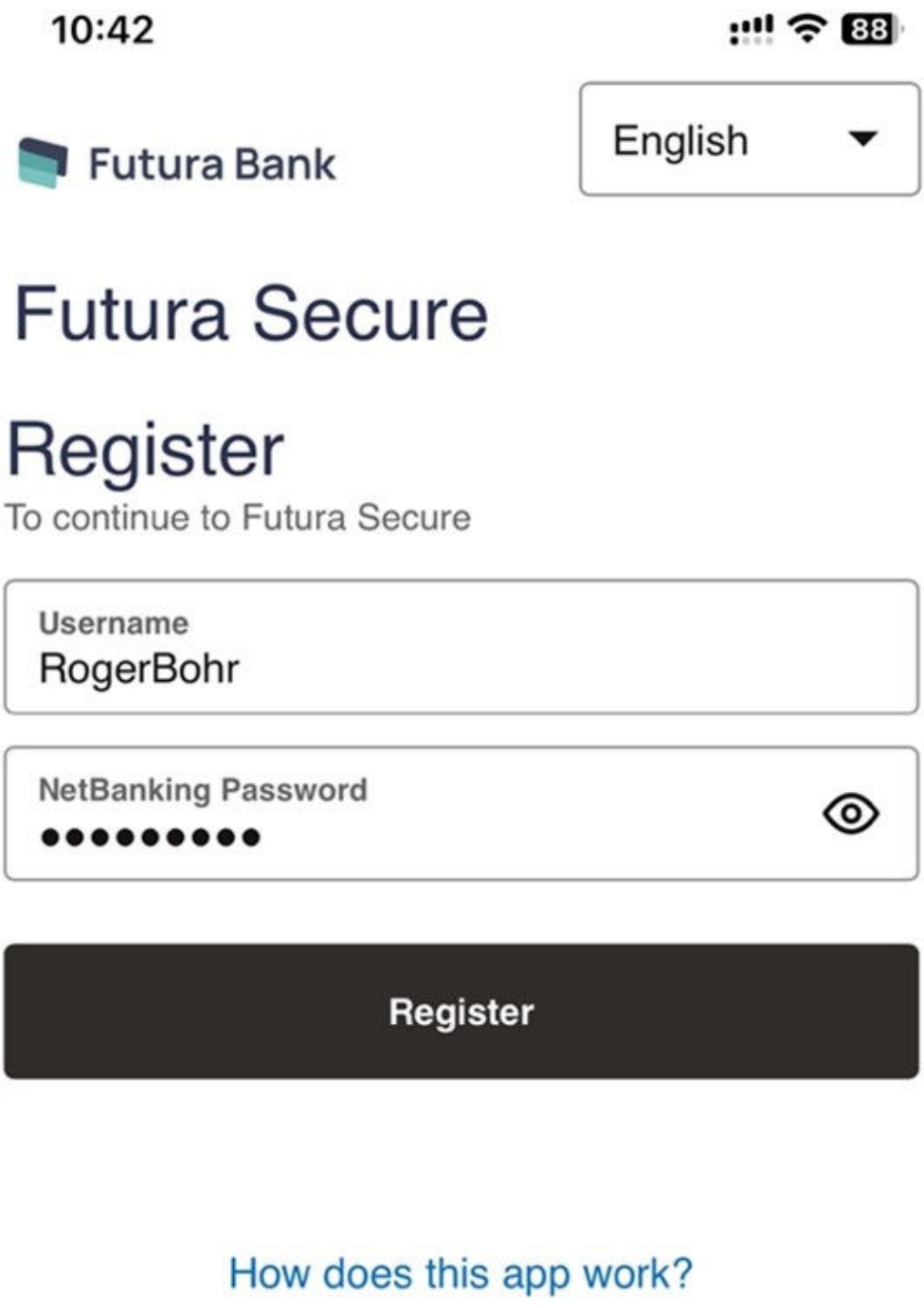
- The user must download Futura Bank PaySecure application and have a valid account with bank with online banking enabled.

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.

Copyright © 2015, 2025, Oracle and/or its affiliates.

Figure 1-1 Register page



Copyright © 2015, 2025, Oracle and/or its affiliates.

> **Note**
>
> The fields which are marked as Required are mandatory.

For more information on fields, refer to the field description table.

Table 1-1 Register page - Field Description

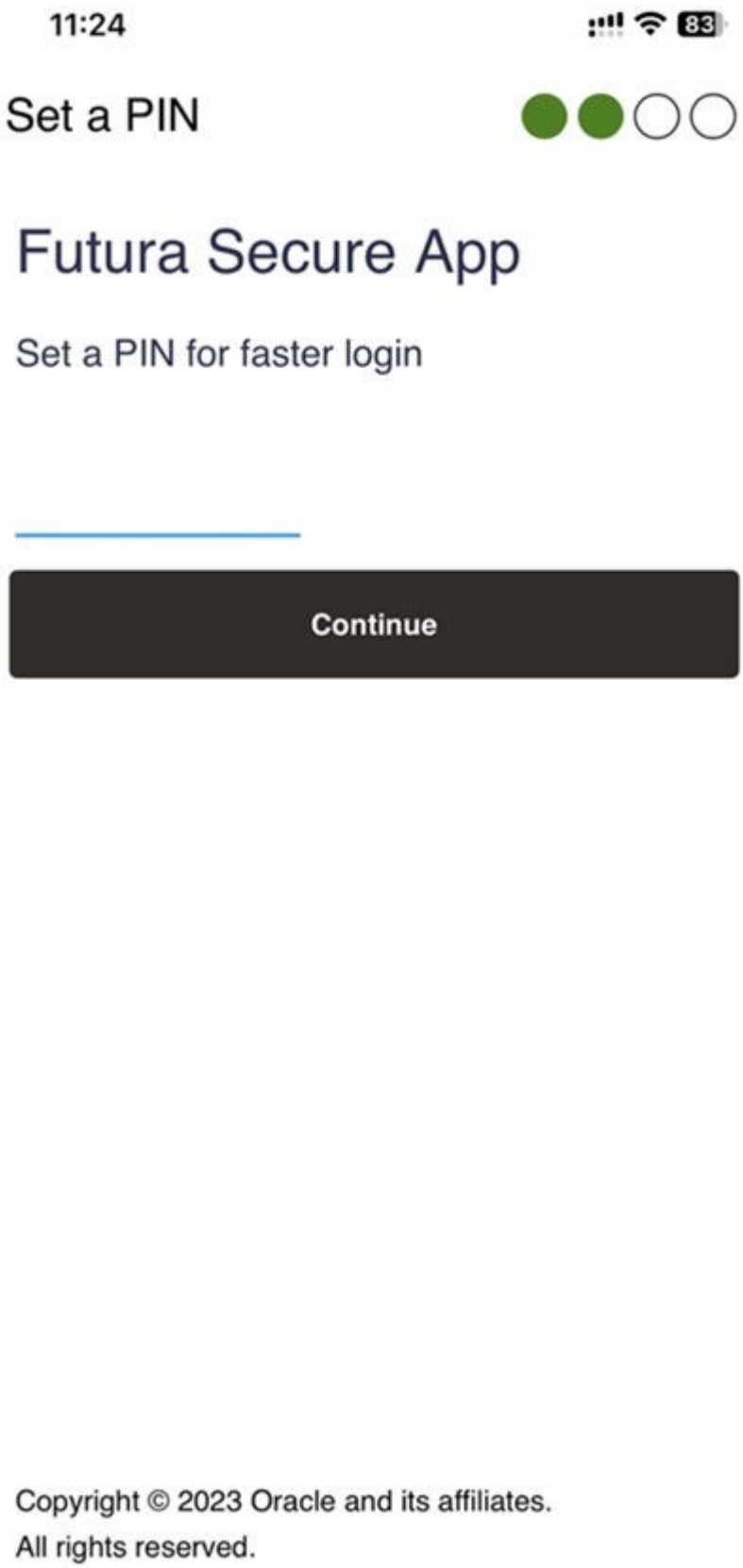
Field Name	Description
Username	Login id provided by the bank.
Net Banking Password	The password for channel access.

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

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

Copyright © 2015, 2025, Oracle and/or its affiliates.

Figure 1-2 Set a PIN



Copyright © 2015, 2025, Oracle and/or its affiliates.

> **Note**
>
> The fields which are marked as Required are mandatory.

For more information on fields, refer to the field description table.

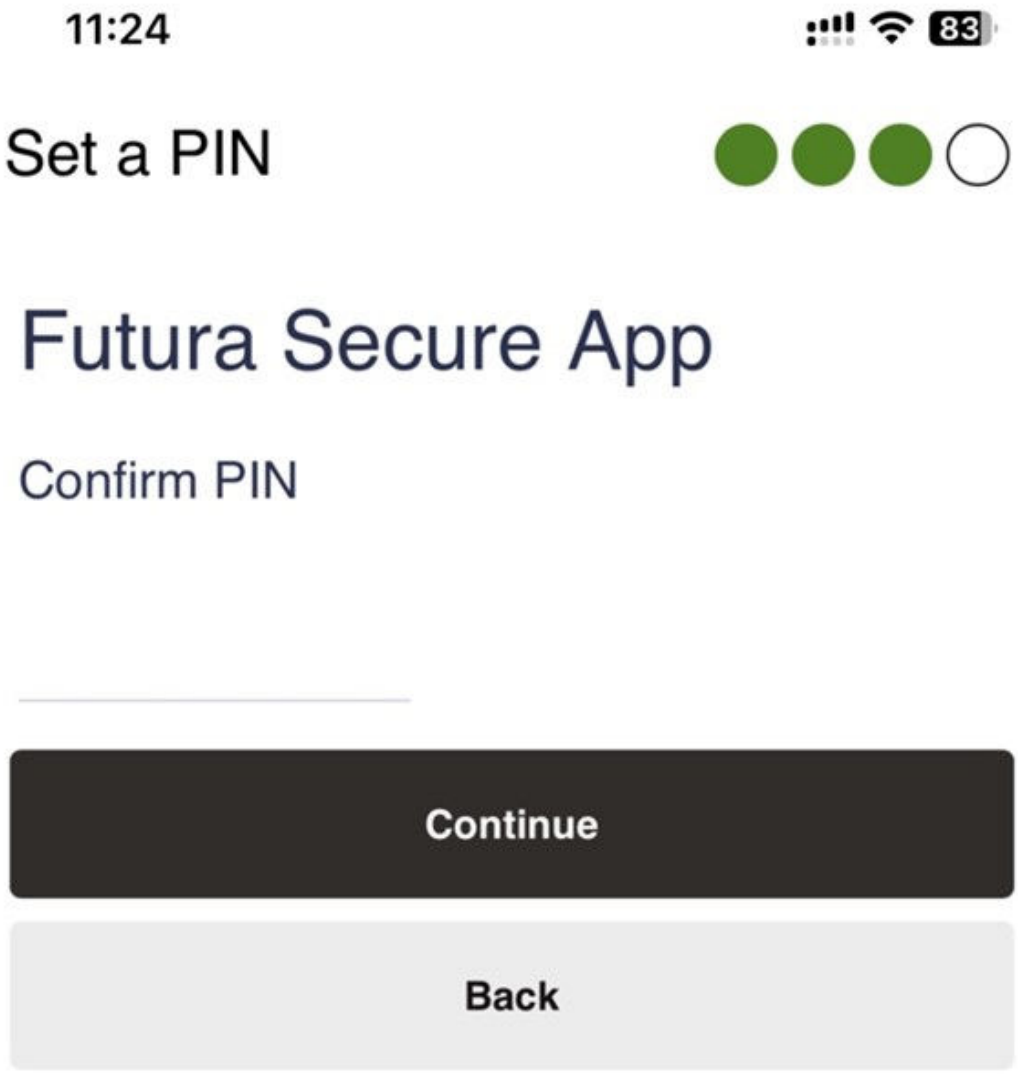
Table 1-2 Set a PIN - Field Description

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.

Copyright © 2015, 2025, Oracle and/or its affiliates.

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



Copyright © 2015, 2025, Oracle and/or its affiliates.

> **Note**
>
> The fields which are marked as Required are mandatory.

For more information on fields, refer to the field description table.

Table 1-3 Set a PIN - Re-enter PIN - 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. Perform one of the following actions:
   - Click **Continue** to proceed to next screen.

     User will be directed to the screen to generate an OTP.
   - Click **Back** to go back to previous screen.

1.2 Login & OTP Generation

This topic provides the systematic instructions of generating OTP and login into PaySecure application.

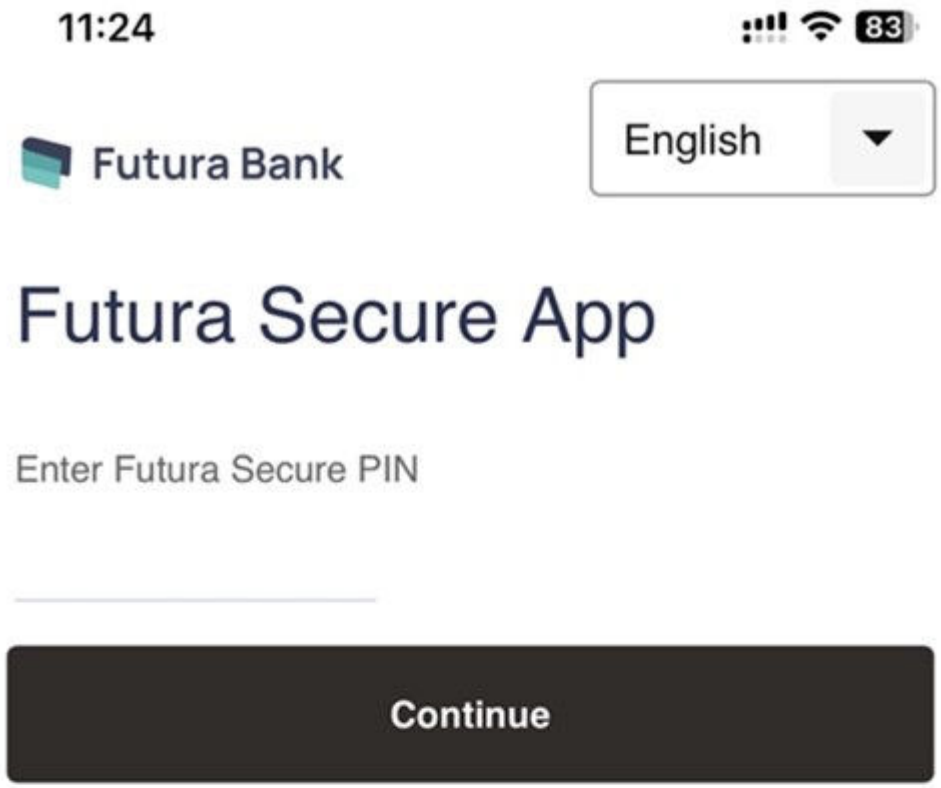
Once the registration is successful, from the subsequent logins user has to use the PIN to login into the PaySecure application. Post authentication, user will be provided with an option to either select the user for which OTP is to be generated (if multiple users are registered using same application)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

Copyright © 2015, 2025, Oracle and/or its affiliates.

Figure 1-4 PaySecure PIN



Copyright © 2015, 2025, Oracle and/or its affiliates.

> **Note**
>
> The fields which are marked as Required are mandatory.

For more information on fields, refer to the field description table.

Table 1-4 PaySecure PIN - Field Description

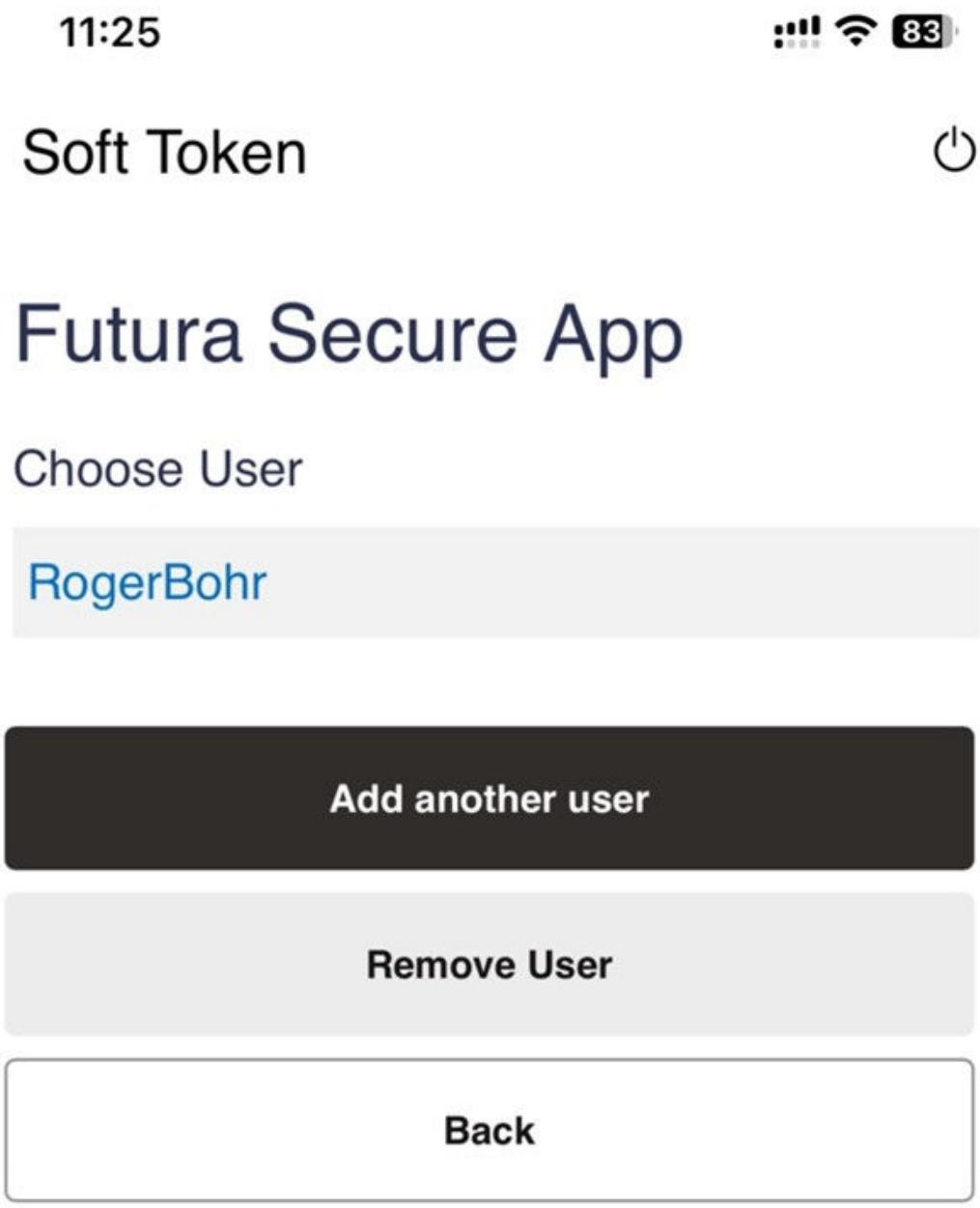
Field Name	Description
Enter PIN	Enter the PIN to login into the application.

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

   The **Choose User** screen appears.

Copyright © 2015, 2025, Oracle and/or its affiliates.

Figure 1-5 Choose User



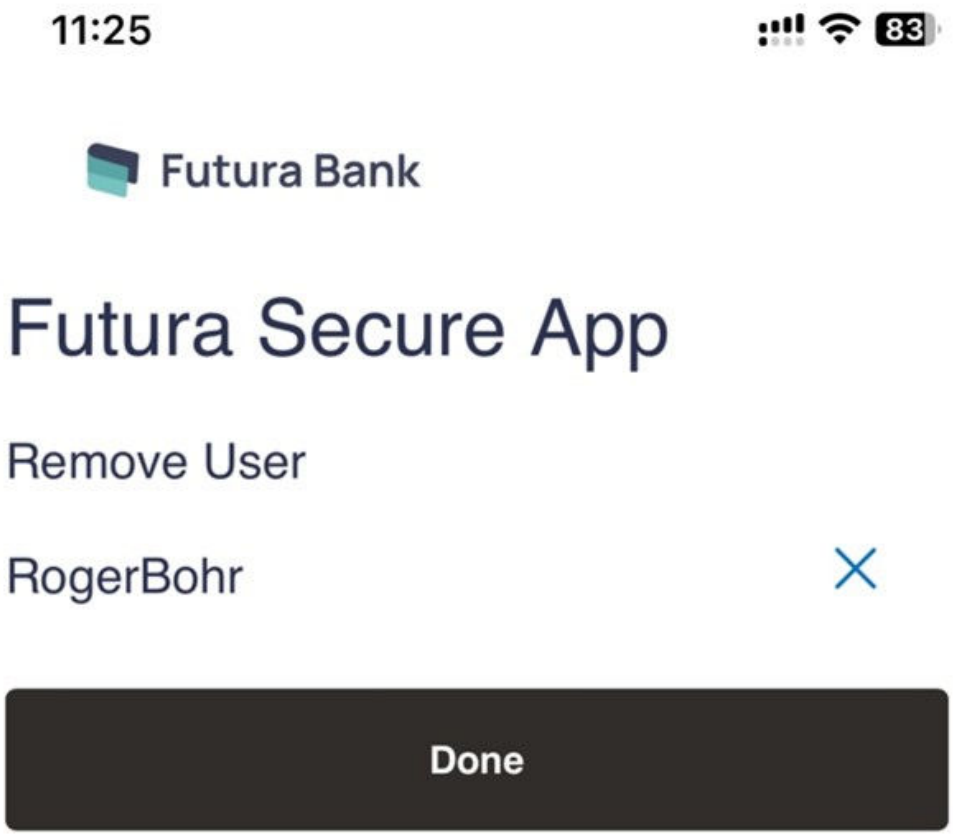
Copyright © 2015, 2025, Oracle and/or its affiliates.

3. Perform one of the following actions:
   - Select the user.

     The user is prompted to enter the code.
   - Click **Add Another User** to add another account. For more information refer **Registration**section.
   - Click **Remove User**.

Copyright © 2015, 2025, Oracle and/or its affiliates.

Figure 1-6 Remove User



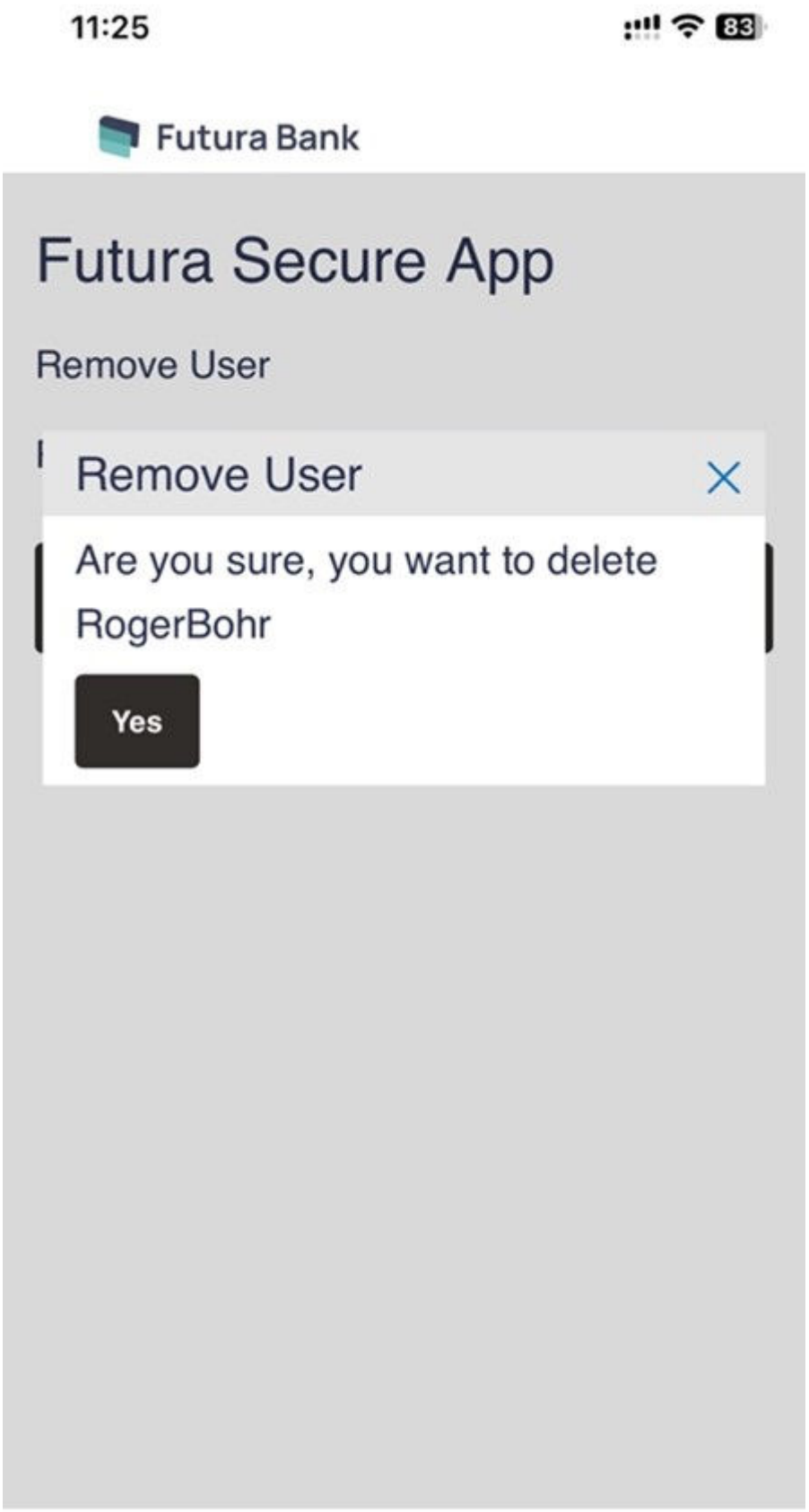
Copyright © 2015, 2025, Oracle and/or its affiliates.

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

   A popup message appears prompting to confirm the user deletion.

Copyright © 2015, 2025, Oracle and/or its affiliates.

Figure 1-7 Remover user popup screen



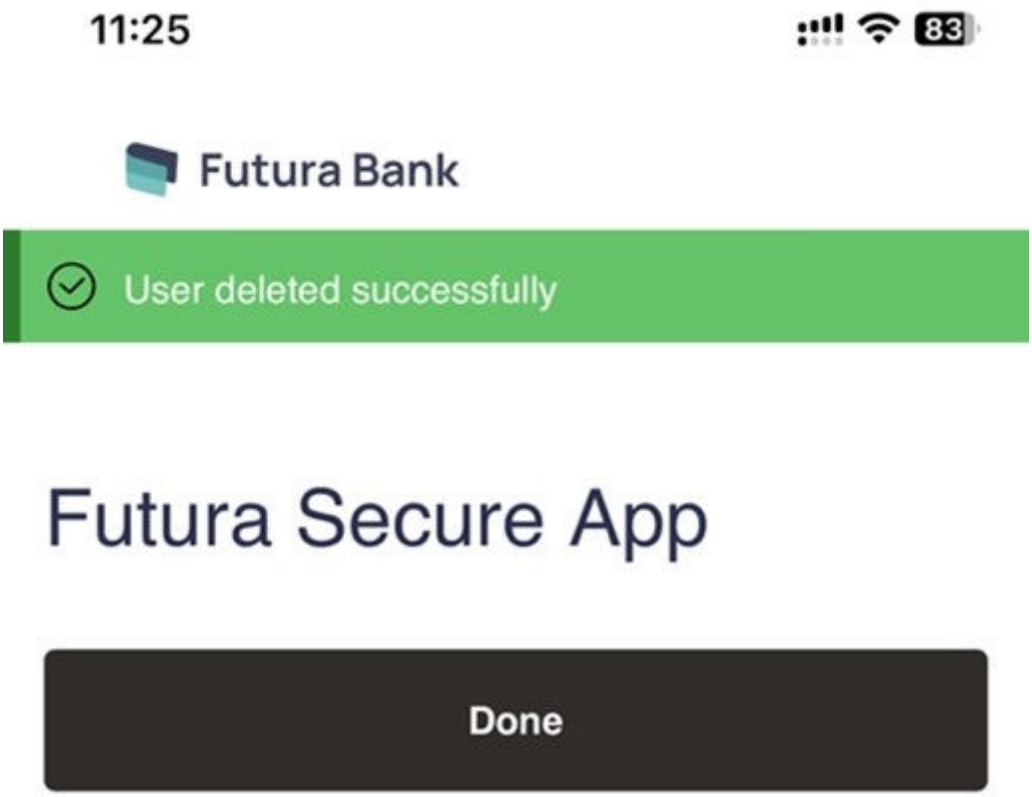
Copyright © 2015, 2025, Oracle and/or its affiliates.

a. Click **Yes** to delete the user.

   User deleted message is displayed.

Copyright © 2015, 2025, Oracle and/or its affiliates.

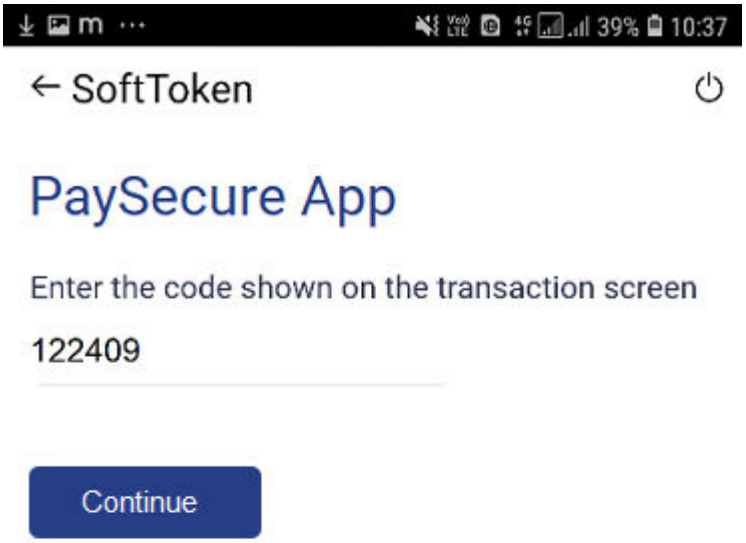
Figure 1-8 Soft Token Code



Copyright © 2015, 2025, Oracle and/or its affiliates.

b. Click **Done**.

Figure 1-9 Soft Token Code



Copyright © 2016 Oracle and its affiliates.
All rights reserved.

> **Note**
>
> The fields which are marked as Required are mandatory.

For more information on fields, refer to the field description table.

Table 1-5 Soft Token Code - Field Description

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

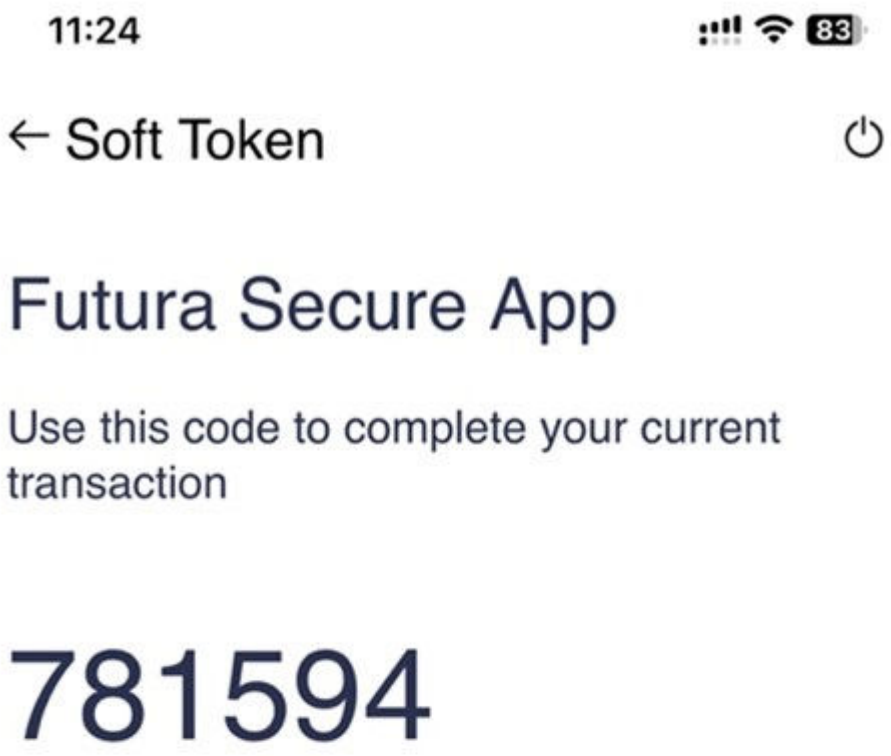
c. In the **Enter the code** field, enter the code appear on transaction screen.

d. Click **Continue** to proceed to next screen.

The Soft Token code generated successfully.

Copyright © 2015, 2025, Oracle and/or its affiliates.

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



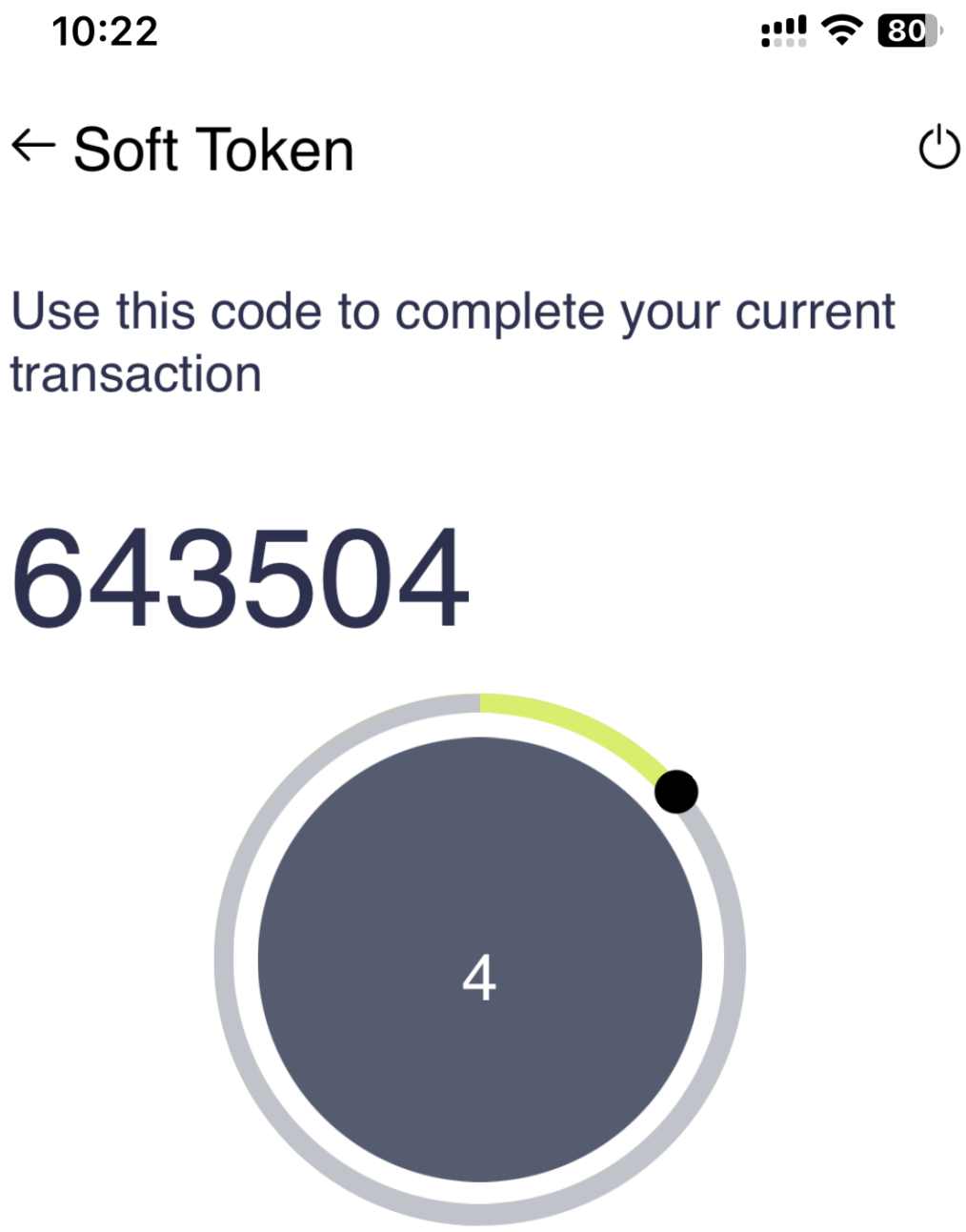
Copyright © 2015, 2025, Oracle and/or its affiliates.
Copyright © 2023 Oracle and its affiliates.
All rights reserved

5. 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.

Copyright © 2015, 2025, Oracle and/or its affiliates.

Figure 1-11 Generated Soft Token Code (TOTP based)



Copyright © 2015, 2025, Oracle and/or its affiliates.

Copyright © 2015, 2025, Oracle and/or its affiliates.

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.

Copyright © 2015, 2025, Oracle and/or its affiliates.

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.

Copyright © 2015, 2025, Oracle and/or its affiliates.

Index

L

Login & OTP Generation, *7*

R

Registration, *1*

S

Soft Token Application, *1*

Copyright © 2015, 2025, Oracle and/or its affiliates.