

Soft Token Application -Small & Medium Business User Manual
Oracle Banking Digital Experience
Patchset Release 22.2.5.0.0

Part No. F72987-01

October 2024

Soft Token Application - Small & Medium Business User Manual

October 2024

Oracle Financial Services Software Limited

Oracle Park

Off Western Express Highway

Goregaon (East)

Mumbai, Maharashtra 400 063

India

Worldwide Inquiries:

Phone: +91 22 6718 3000

Fax: +91 22 6718 3001

www.oracle.com/financialservices/

Copyright © 2006, 2024, Oracle and/or its affiliates. All rights reserved.

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 failsafe, 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.

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.

This software or hardware and documentation may provide access to or information on 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. 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.



Table of Contents

1. Preface	1-1
1.1 Purpose	1-1
1.2 Audience	1-1
1.3 Documentation Accessibility	1-1
1.4 Critical Patches	1-1
1.5 Diversity and Inclusion	1-1
1.6 Conventions	1-1
1.7 Screenshot Disclaimer	1-2
1.8 Acronyms and Abbreviations	1-2
2. Transaction Host Integration Matrix	2-1
3. Soft Token Application	3-1
3.1 Registration	3-1
3.2 Login & OTP Generation	3-6

1. Preface

1.1 Purpose

Welcome to the User Guide for Oracle Banking Digital Experience. This guide explains the operations that the user will follow while using the application.

1.2 Audience

This manual is intended for Customers and Partners who setup and use Oracle Banking Digital Experience.

1.3 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 customers that have purchased support have access to electronic support through My Oracle Support. For information, visit, <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

1.4 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](#).

1.5 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.

1.6 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.
<i>Italic</i>	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.

1.7 Screenshot Disclaimer

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.

1.8 Acronyms and Abbreviations

The list of the acronyms and abbreviations that you are likely to find in the manual are as follows:

Abbreviation	Description
OBDX	Oracle Banking Digital Experience

2. Transaction Host Integration Matrix

Legends

NH	No Host Interface Required.
✓	Pre integrated Host interface available.
✗	Pre integrated Host interface not available.

Sr No	Transaction / Function Name	Oracle FLEXCUBE Core Banking 11.10.0.0.0	Oracle FLEXCUBE Universal Banking 14.7.4.0.0
1	Soft Token Application	NH	NH

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.

Features Supported In Application

- Online registration
- OTP generation

3.1 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.

Register page

10:42

 Futura Bank

English ▼

Futura Secure

Register

To continue to Futura Secure

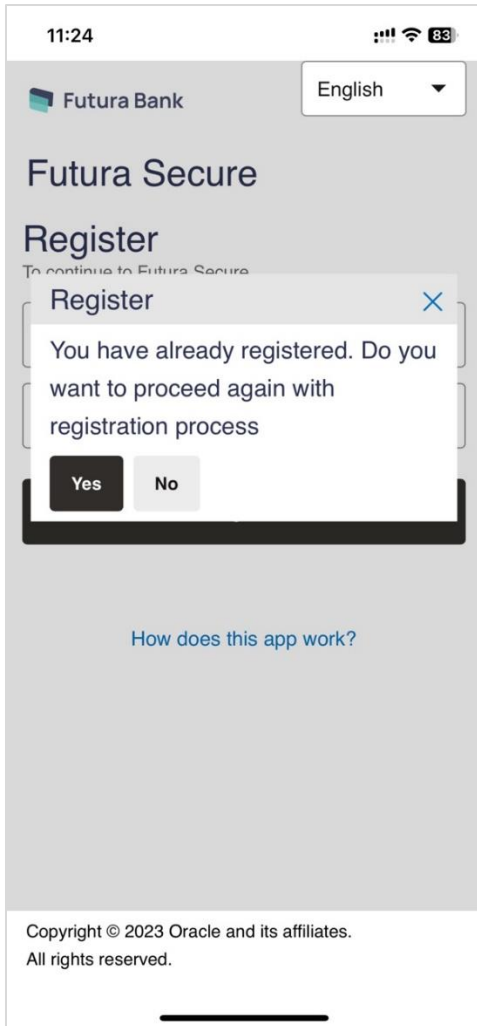
Username
RogerBohr

NetBanking Password
●●●●●●●● 

Register

[How does this app work?](#)

Copyright © 2023 Oracle and its affiliates.
All rights reserved.



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.

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.

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. 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.

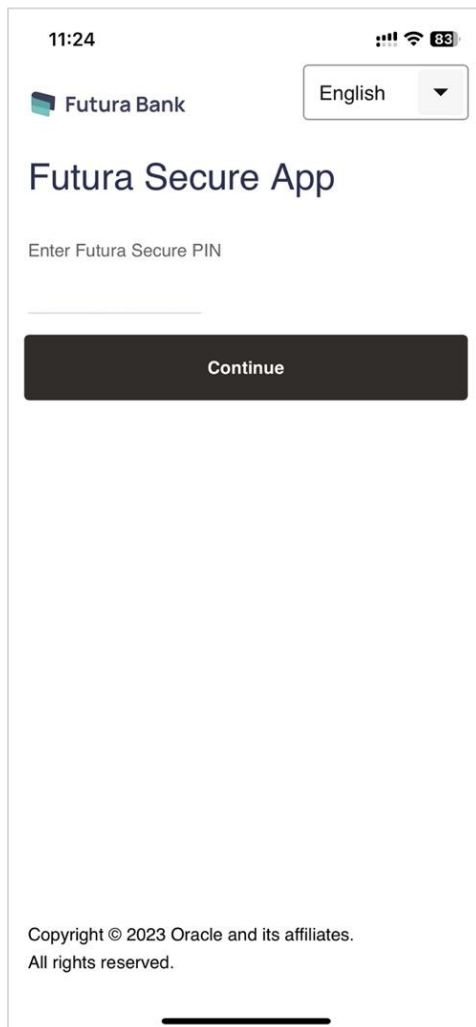
3.2 Login & OTP Generation

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).

PaySecure PIN



11:24

Futura Bank English

Futura Secure App

Enter Futura Secure PIN

Continue

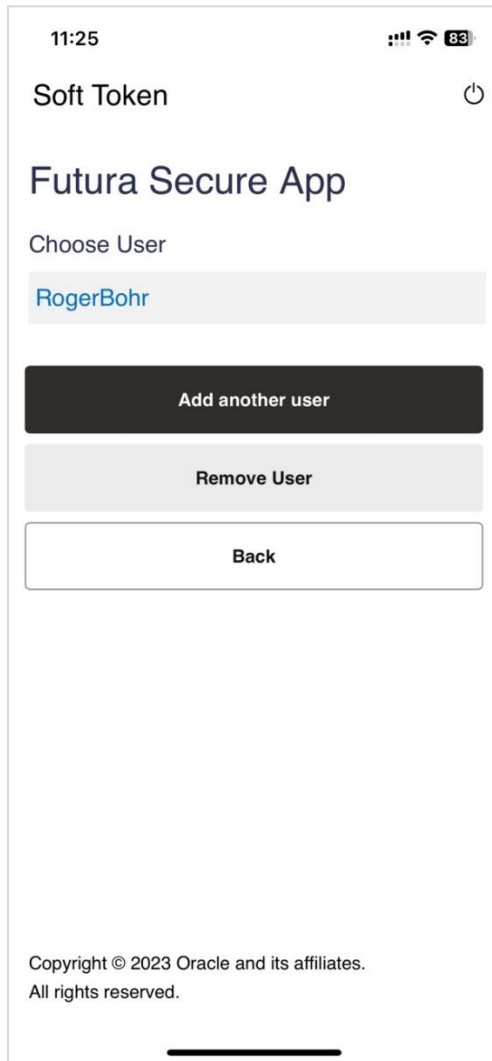
Copyright © 2023 Oracle and its affiliates.
All rights reserved.

Field Description

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

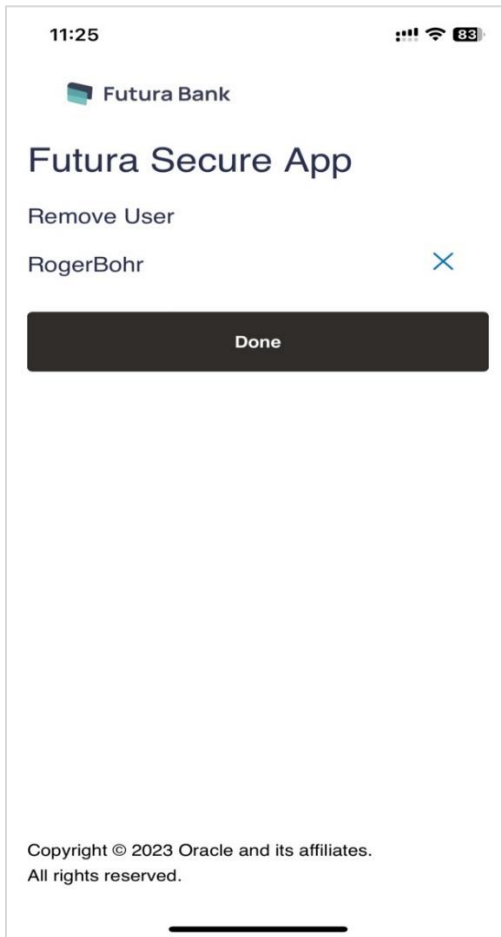
2. Enter the **PIN**, and click **Continue**.
The **Choose User** screen appears.

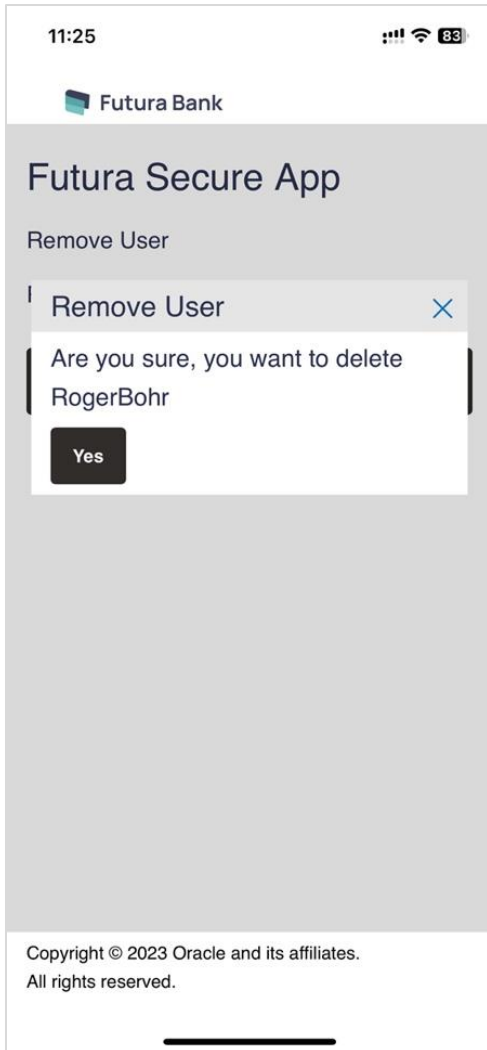
Choose User



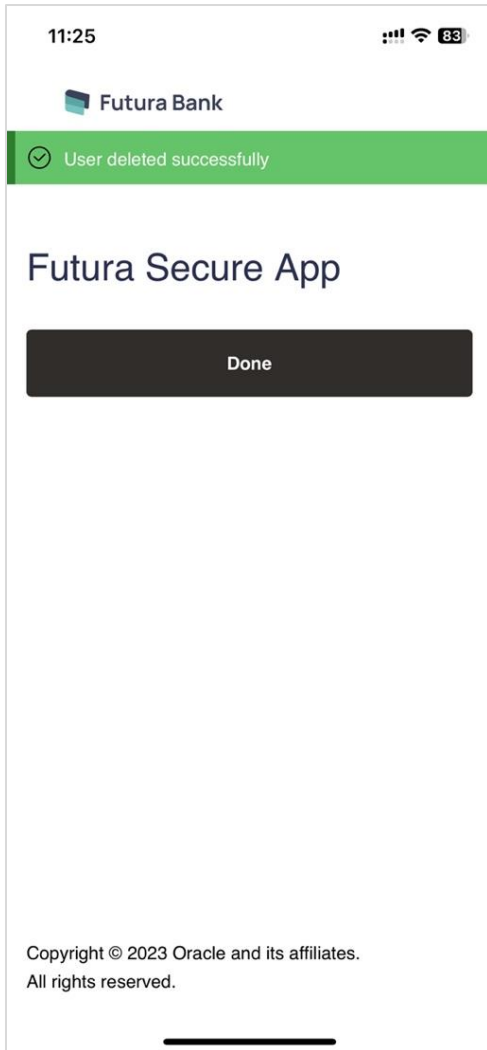
3. Select the user. The user is prompted to enter the code.
OR
Click **Add Another User** to add another account. For more information refer Registration section.
OR
Click **Remove User**.

Remove User



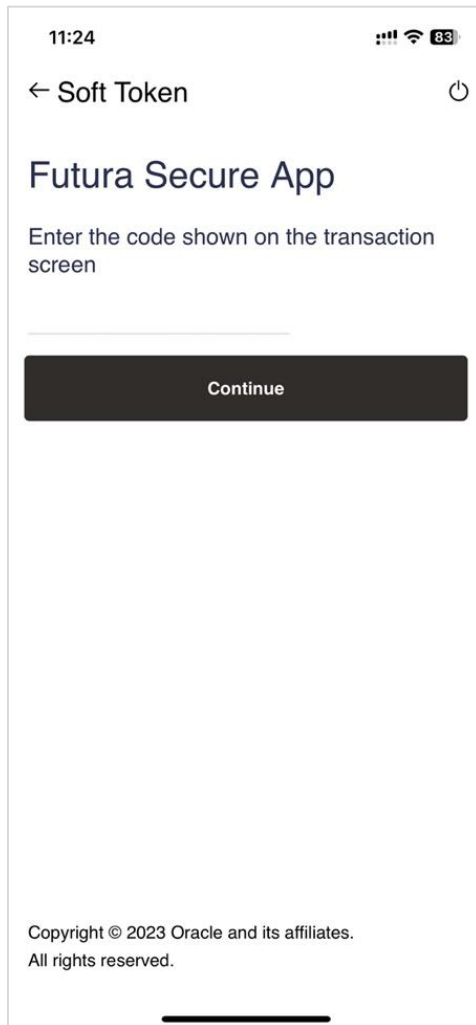


4. Click  against a user to remove a user. A popup message appears prompting to confirm the user deletion.
5. Click **Yes** to delete the user. User deleted message is displayed.



6. Click **Done**.

Soft Token Code

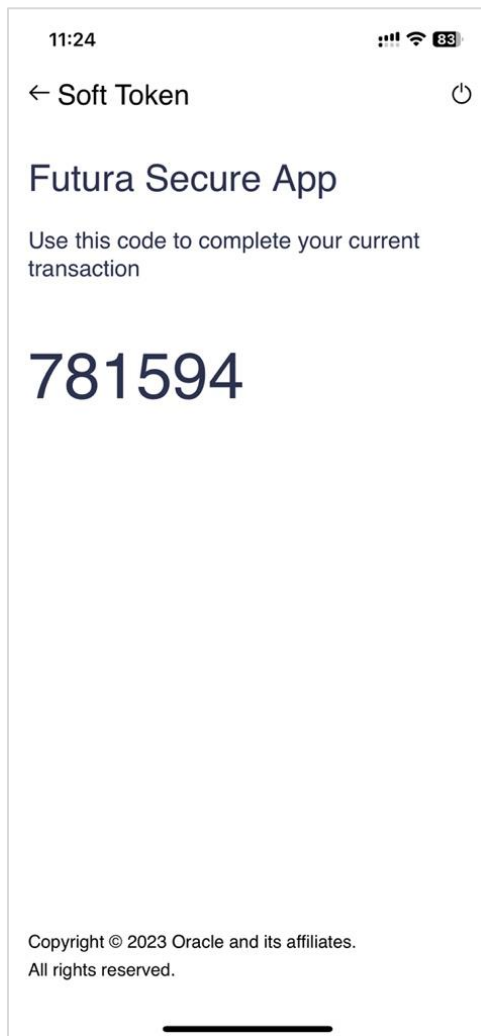
A screenshot of a mobile application interface. At the top, the status bar shows the time 11:24, signal strength, Wi-Fi, and battery at 83%. Below the status bar is a navigation bar with a back arrow and the text "Soft Token" on the left, and a power icon on the right. The main content area has the title "Futura Secure App" in a large font. Below the title is the instruction "Enter the code shown on the transaction screen". A large, dark rectangular button with the word "Continue" in white is centered below the instruction. At the bottom of the screen, there is a copyright notice: "Copyright © 2023 Oracle and its affiliates. All rights reserved." and a horizontal line.

Field Description

Field Name	Description
Enter the 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.

Generated Soft Token Code (HOTP based)



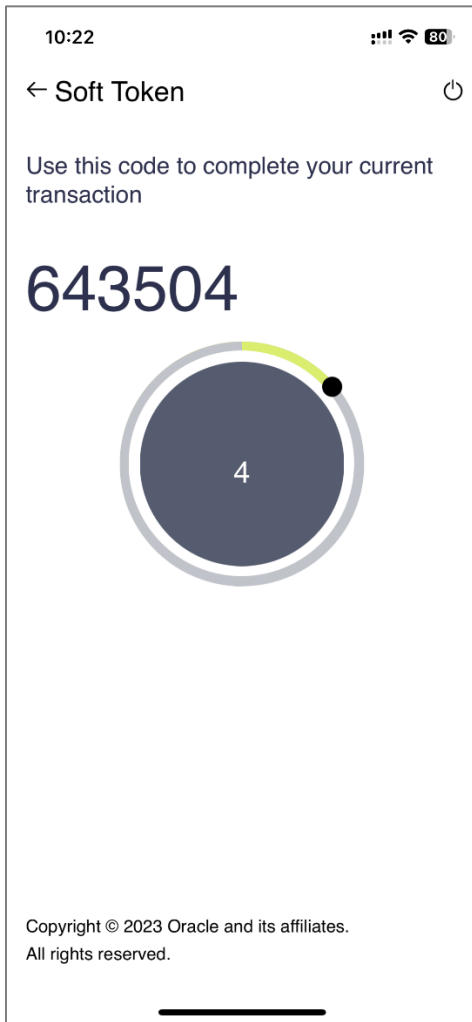
9. Use the generated Soft Token PIN to complete the current transaction.

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.

Generated Soft Token Code (TOTP based)



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.