www.dsssasia.com

User Manual – DS3 OathToken
J2ME Midlet

Revision History

Date	Version	Description	Author
10/02/2006	1.0	Preliminary Version	Kwan Hon Luen

Contents

REVISION HISTORY **2**

CONTENTS **3**

1 INTRODUCTION **4**

2 MIDLET SCREEN FLOWS **5**

2.1 READY SCREEN 5
2.2 OATH TOKEN INITIALIZATION SCREEN 7
2.3 SEED DISPLAY SCREEN 8
2.4 SET PIN REQUEST SCREEN 9
2.5 SET PIN SCREEN 10
2.6 PIN VERIFICATION SCREEN 11
2.7 DISPLAY OTP SCREEN 13
2.7.1 The Options Available When PIN Is Set *14*
2.7.2 The Options Available When PIN Is Not Set *16*
2.8 DELETE LABEL SCREEN 18
2.9 CHANGE PIN SCREEN 19
2.10 REMOVE PIN SCREEN 20
2.11 MANAGE LABEL SCREEN 21
2.12 SCREEN SITEMAP 23

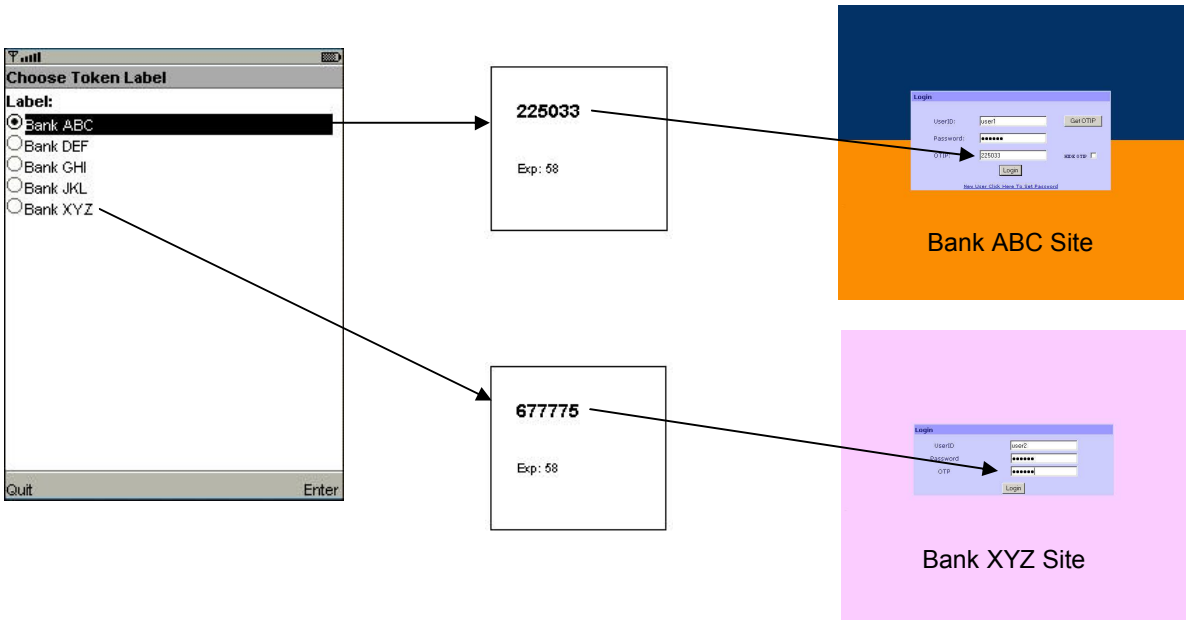
3 FREQUENTLY ASKED QUESTIONS **24**

1 Introduction

The OathToken MIDlet application is an extension of the flagship product of DS3, the Authentication Server. The application that is specially developed to be installed on handheld device, functions as another mobile authentication token conveniently used by the user to authenticate herself to the Authentication Server.

It allows the user to make use of the OATH HOTP algorithm (see http://www.openauthentication.org) to generate one-time passwords for strong 2nd factor authentication.

This document is the user guide for this MIDlet application, and walks the user through all the possible screen steps. The diagram below illustrates that using this MIDlet, it is possible to register oathtokens for different organization using unique labels. A maximum of 5 labels is supported by this midlet.



2 MIDlet Screen Flows

2.1 Ready Screen

When the application is selected on the handheld device, the following screen appears. At this screen, the MIDlet application is ready to be launched.

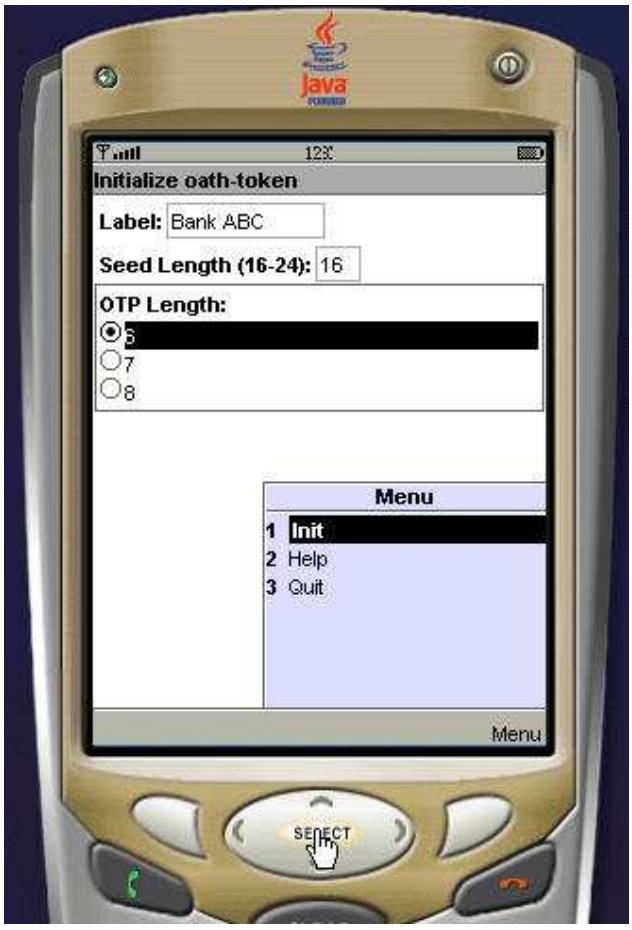
To launch the MIDlet application, the user clicks on the Launch button. Note that due to different device designs from various device manufacturers, the appearance of the options for the user to select will be different.

If no label has not been set, he will be brought the Oath Token Initialization Screen explained in Section 2.2.

If more than one label has been set and he had set a PIN to protect the label setting during the initialization steps, he will be brought to the PIN Verification Screen of the default label explained in Section 2.6.

If more than one label has been set and he had not set any PIN to protect the label setting during the initialization steps, he will be brought to the Display OTP Screen of the default label explained in Section 2.7.

2.2 Oath Token Initialization Screen

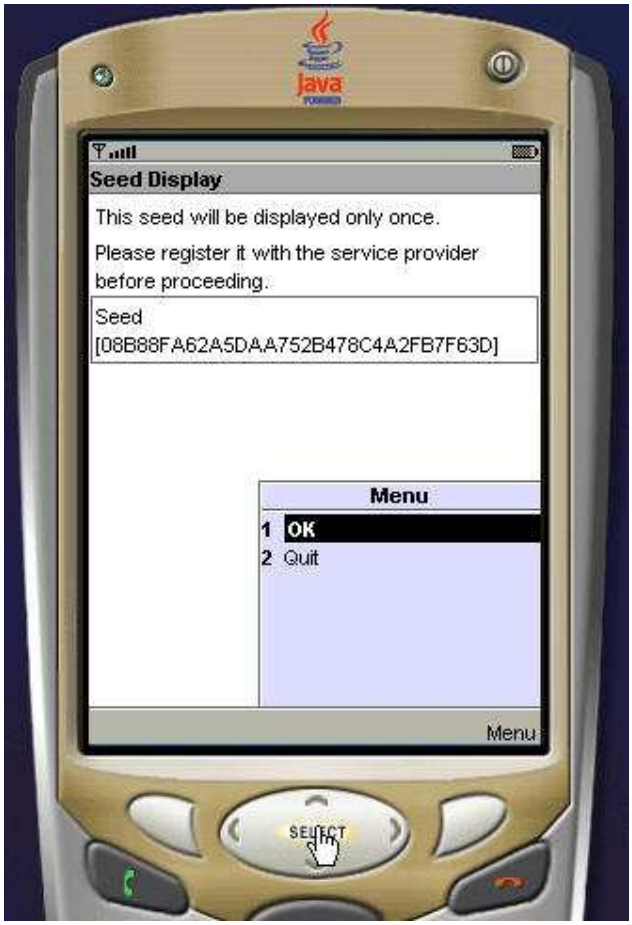


The user is required to enter a few settings to generate the seed value for registration with the Authentication Server.

Name	Description
Label	The label to identify this oath token (in alphanumeric) e.g. ABC Bank
Seed Length	The length of the seed in bytes between 16 and 24 e.g. 16
OTP Length	The length of the One-Time Password The OTP length is either 6, 7 or 8.

After the settings are entered, the user selects Initialize on the menu to confirm. He is brought to the Seed Display Screen explained in Section 2.3.

2.3 Seed Display Screen

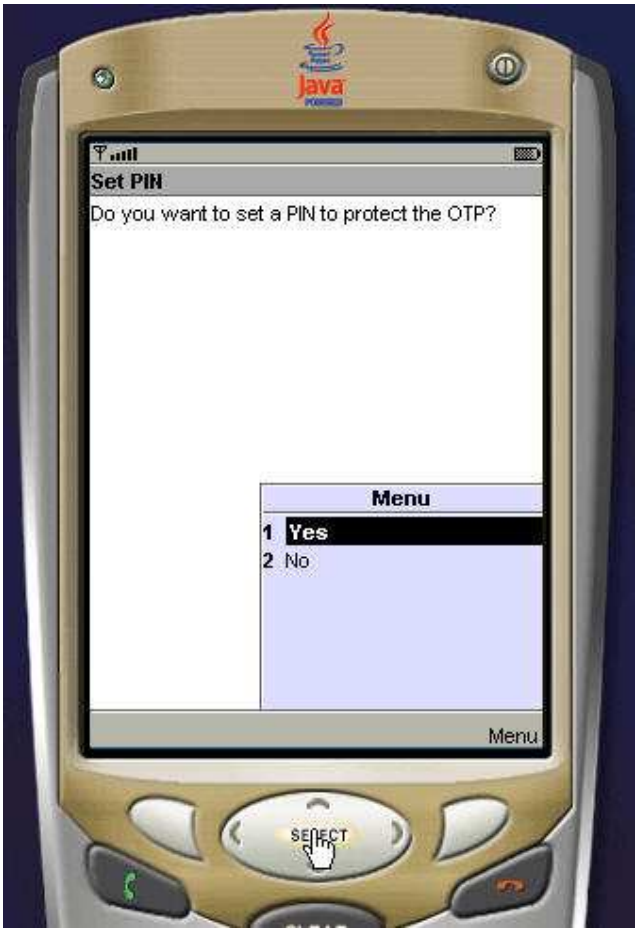


The user is requested to register the generated seed with the Authentication Server.

NOTE: It is important that this seed is kept secret as it is used for the generation of the one-time passwords. It is only displayed once upon the generation to allow for a user self-registration with the authentication service provider.

After the registration, the user selects OK on the menu, he is brought to the Set PIN Request Screen explained in Section 2.4.

2.4 Set PIN Request Screen



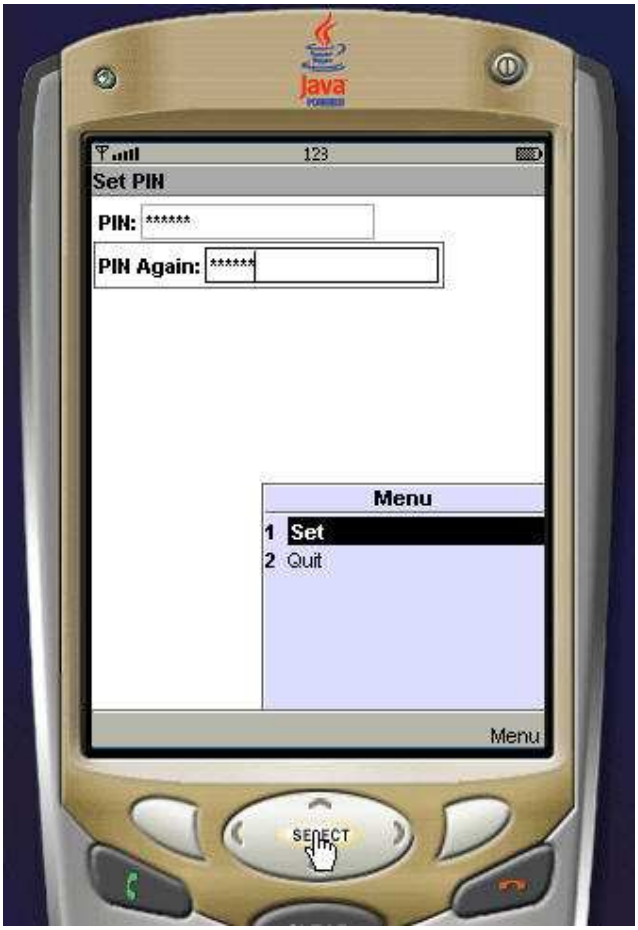
The user is requested to decide whether to set a PIN to protect the OTP.

If he selects NO on the menu, he will be brought to the Display OTP Screen explained in Section 2.7.

If he selects YES on the menu, he will be brought to the Set PIN Screen explained in Section 2.5.

The user can change his mind subsequently on whether to use a PIN to protect the OTP.

2.5 Set PIN Screen



The user is required to enter his PIN twice to set his PIN.

Name	Description
PIN	PIN to protect the OTP (in numeric) e.g. 123456
PIN Again	PIN to protect the OTP (in numeric) This PIN must match the previous entered PIN. e.g. 123456

After the matching PINs are entered, the user selects Set on the menu to confirm. He is brought back to the Ready Screen explained in Section 2.1.

2.6 PIN Verification Screen

The user is required to enter his PIN for verification.

Name	Description
Enter PIN	PIN to unlock for displaying OTP (in numeric) e.g. 123456

After the PIN is entered, the user selects OK on the menu to confirm. If he is correctly verified, he is brought to the Display OTP Screen explained Section 2.7.

Note that there are additional options on this screen,

- Delete Label option

  This is used when the user has forgotten his password and cannot be verified. Selecting this option brings the user to the Delete Label Screen explained in Section 2.8. This allows the user to decide whether to delete the oath token associated with the label and do the re-initialization again (if required).

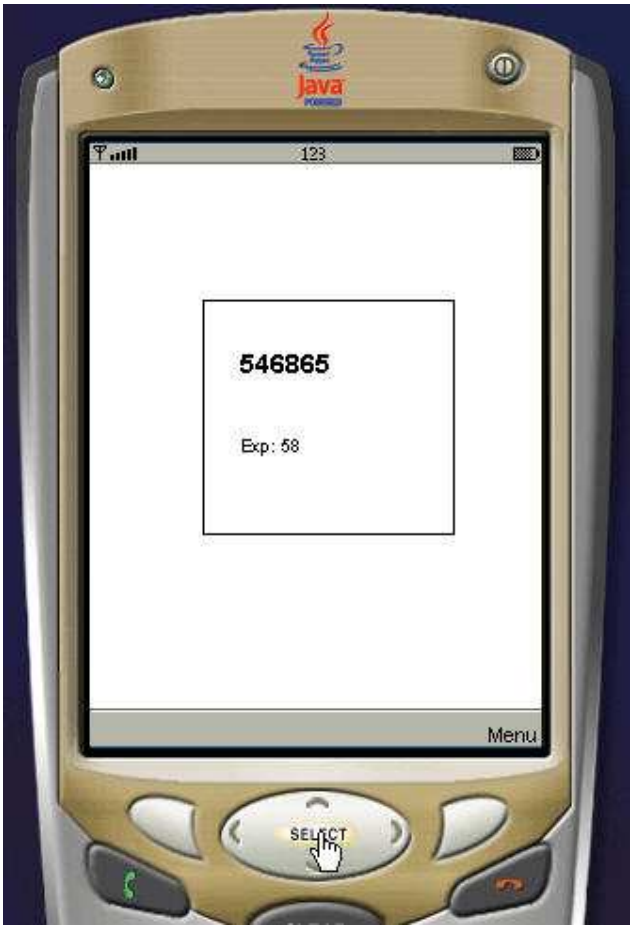
- Manage Label option

  This is used when the user wishes to switch over to an oath token identified by other labels, or the user wishes to initialize a new oath token under a new label. Selecting this option brings the user to the Manage Label Screen explained in Section 2.11.

- Display Label option

  The number of Display Label options shown depends on how many labels had been set. For example, Bank XYZ label has been set. This will be shown as Display Bank XYZ on the menu. Selecting this option will bring the user to the PIN Verification Screen of this selected label explained in Section 2.6, if he had set a PIN to protect this label setting. Selecting this option will bring the user to the Display OTP Screen of this selected label explained in Section 2.7, if he had not set any PIN to protect this label setting.

2.7 Display OTP Screen



At this screen, the OTP is generated and displayed for 60 seconds, before the user is brought to the Ready Screen explained in Section 2.1.

2.7.1 The Options Available When PIN Is Set

Note that there are additional options on the Display OTP screen, when the user's PIN is set.

- Change PIN option
  This is used when the user wishes to change his PIN. Selecting this option brings the user to the Change PIN Screen explained in Section 2.9.

- Remove PIN option
  This is used when the user wishes to remove his PIN. Selecting this option brings the user to the Remove PIN Screen explained in Section 2.10.

- Delete Label option
  This is used when the user has forgotten his password and cannot be verified. Selecting this option brings the user to the Delete Label Screen explained in Section 2.8. This allows the user to decide whether to delete the oath token associated with the label and do the re-initialization again (if required).

- Manage Label option

  This is used when the user wishes to switch over to an oath token identified by other labels, or the user wishes to initialize a new oath token under a new label. Selecting this option brings the user to the Manage Label Screen explained in Section 2.11.

- Display Label option

  The number of Display Label options shown depends on how many labels had been set. For example, Bank XYZ label has been set. This will be shown as Display Bank XYZ on the menu. Selecting this option will bring the user to the PIN Verification Screen of this selected label explained in Section 2.6, if he had set a PIN to protect this label setting. Selecting this option will bring the user to the Display OTP Screen of this selected label explained in Section 2.7, if he had not set any PIN to protect this label setting.

2.7.2 The Options Available When PIN Is Not Set

Note that there are additional options on the Display OTP screen, when the user's PIN is not set.

- Set PIN option

  This is used when the user wishes to set a PIN top protect the OTP. Selecting this option brings the user to the Set PIN Screen explained in Section 2.5.

- Delete Label option

  This is used when the user has forgotten his password and cannot be verified. Selecting this option brings the user to the Delete Label Screen explained in Section 2.8. This allows the user to decide whether to delete the oath token associated with the label and do the re-initialization again (if required).

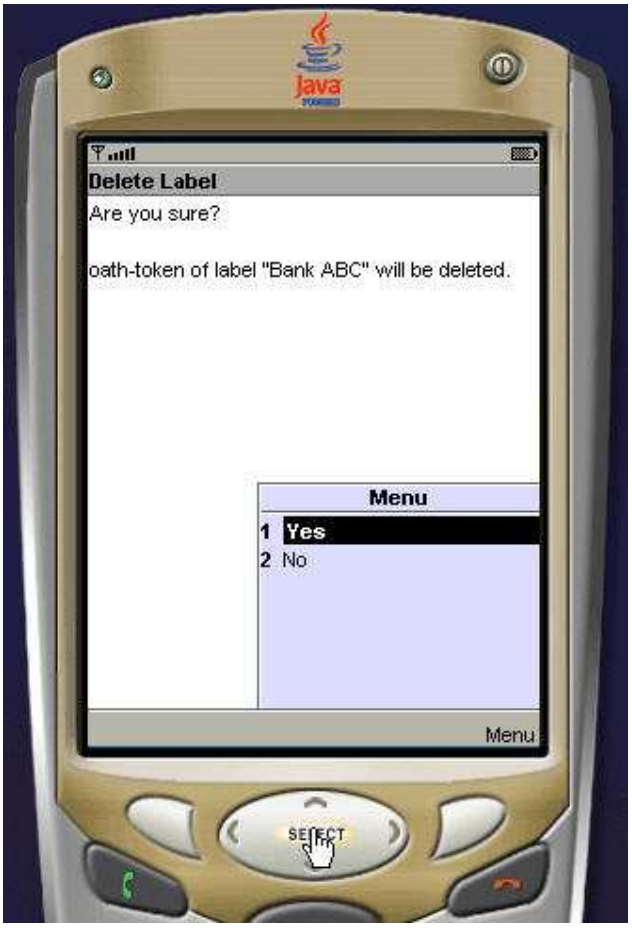
- Manage Label option

  This is used when the user wishes to switch over to an oath token identified by other labels, or the user wishes to initialize a new oath token under a new label. Selecting this option brings the user to the Manage Label Screen explained in Section 2.11.

- Display Label option

  The number of Display Label options shown depends on how many labels had been set. For example, Bank XYZ label has been set. This will be shown as Display Bank XYZ on the menu. Selecting this option will bring the user to the PIN Verification Screen of this selected label explained in Section 2.6, if he had set a PIN to protect this label setting. Selecting this option will bring the user to the Display OTP Screen of this selected label explained in Section 2.7, if he had not set any PIN to protect this label setting.

2.8 Delete Label Screen

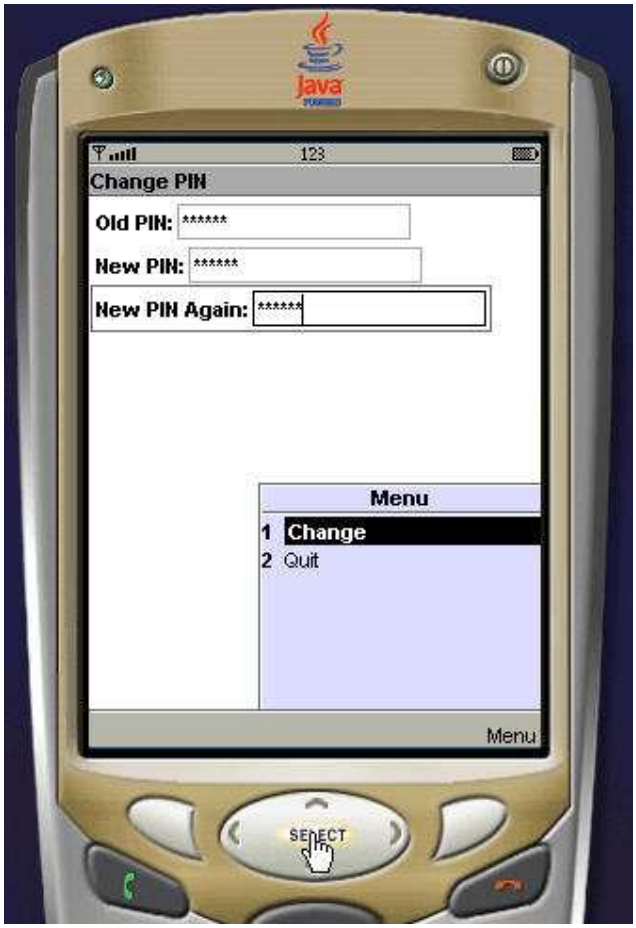


The user is requested to confirm the deletion of the oath token associated with the current label.

If he selects NO on the menu, the oath token will not be deleted, and he will be brought back to the Ready Screen explained in Section 2.1.

If he selects YES on the menu, the oath token will be deleted, and he will be brought back to the Ready Screen explained in Section 2.1.

2.9 Change PIN Screen



The user is required to enter his old PIN once and new PIN twice to change his PIN.

Name	Description
Old PIN	Current PIN to protect the OTP (in numeric) e.g. 123456
New PIN	New PIN to protect the OTP (in numeric) e.g. 654321
New PIN Again	New PIN to protect the OTP (in numeric) This PIN must match the previous entered New PIN. e.g. 654321

The user selects Change on the menu to confirm. He is brought back to the Ready Screen explained in Section 2.1.

2.10 Remove PIN Screen

The user is required to enter his current PIN once to remove his PIN.

Name	Description
Current PIN	Current PIN to protect the OTP (in numeric) e.g. 123456

The user selects Remove on the menu to confirm. He is brought back to the Ready Screen explained in Section 2.1.

2.11 Manage Label Screen

The options on this screen follow,

- Set Default Label option

  This is used when the user wishes to set an existing label as the default label. He clicks the label of his choice and selects this option. He is brought to the Ready Screen explained in Section 2.1.

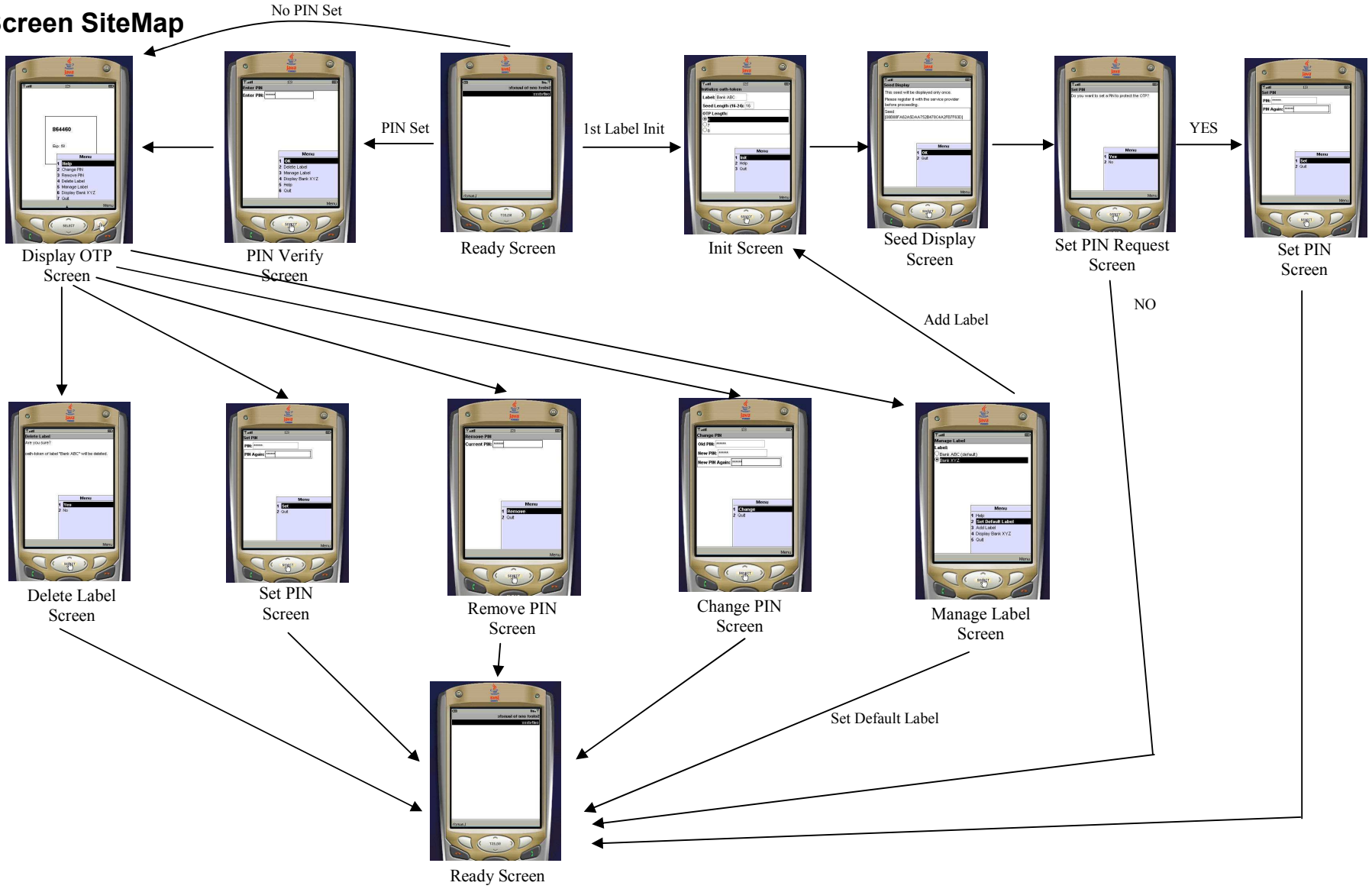
- Add Label option

  This is used when the user wishes to add an oath token under a new label. Selecting this option brings the user to the Oath Token Initialization Screen explained in Section 2.2.

- Display Label option

  The number of Display Label options shown depends on how many labels had been set. For example, Bank XYZ label has been set. This will be shown as Display Bank XYZ on the menu. Selecting this option will bring the user to the PIN Verification Screen of this selected label explained in Section 2.6, if he had set a PIN to protect this label setting. Selecting this option will bring the user to the Display OTP Screen of this selected label explained in Section 2.7, if he had not set any PIN to protect this label setting.

2.12 Screen SiteMap



3 Frequently Asked Questions

This section contains a list of frequently asked questions regarding the usage of the oathdsss token.

- *Do I have to pay for using this software ?*

  No. The J2ME midlet software is distributed for use free-of-charge.

- *Why is DSSS distributing this software ?*

  DSSS supplies backend infrastructure 2-factor authentication solutions. DSSS is also an adopting member of the OATH initiative. The distribution of this software is to promote awareness and acceptance in the use of alternative 2 factor authentication products for securing user access.

- *What phones do this token run on ?*

  This token has been written in J2ME MIDP 1.0, using the minimal libraries to ensure compatibility with as many phones as possible. The software has been tested on Nokia Series 40, 60, and 80, Sony Ericsson, O2, and Blackberry.

- *I've installed it on my phone. What do I do with it ?*

  During the configuration of the token upon start, the token will generate the secret seed which you require to register with your organization's authentication backend. This allows for the backend system to be able to authenticate your one-time passwords.

- *Is the token one-time password secure ?*

  The one-time password (OTP) is generated using an event-based response-only standard proposed by the OATH initiative called HOTP. It relies heavily on the irreversibility of SHA-1 to compute the OTP. See http://www.openauthentication.org. It has been reviewed by many experts and no known vulnerability exists.

- *Can the secret seed be stolen ? How do I protect it ?*

  The secret seed is stored on the phone encrypted. In order to prevent any compromise, you should use a user PIN to protect access to the seed. Also, as the OATH algorithm is event-based, you can track usage of the token by matching the usage count with the event counter in the back-end verification system.

- *I think I've encountered a bug in your software. How do I provide feedback on it ?*

  We welcome all feedback on the software. Please send a mail to support@dsssasia.com. Thank you.

- *I represent an organization interested to implement a 2-factor authentication solution. What do I need ?*

  The software is one-half of the 2nd factor authentication solution. Your organization has to implement the back-end verification system in order to complete the loop. Since the OATH algorithm is publicly available, there are already backend authentication solutions that will support this token. The DSSS Authentication Server is one of such solutions.