USER GUIDE
hidglobal.com An ASSA ABLOY Group brand

iCLASS SE® Biometric Reader
RKLB40; SRD MODEL: RKCLB40E

2. Initial Setup
When the Reader is first switched on, the Initial Setup menu is displayed which will take you through the following stages:
1. Select Language, Template Type and Operational Mode (all card types).
2. Choose Site Key (Seos® cards only).
3. Verify Admin (all card types).

Note: If Reader Initial Setup Configuration needs to be modified in the future, two configuration cards are included with the Reader to reset the Reader back to the Initial Setup menu. To complete Initial Setup reset:
1. Power cycle the Reader.
2. Within the first 15 seconds of power on, present and hold “SE BIO Initial Setup Reset Card 1” to the face of the Reader keypad until the Reader stops beeping and the LED is solid red or flashing blue/red.
3. Power cycle the Reader.
4. Present and hold “SE BIO Initial Setup Reset Card 2” to the face of the Reader keypad until the Reader stops beeping and the LED is solid red or flashing blue/red.

2.1 Initial Setup - Functional Selections
2.1.1 Select Language

<table>
<thead>
<tr>
<th>HID Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. English</td>
</tr>
<tr>
<td>2. Français</td>
</tr>
<tr>
<td>3. Español</td>
</tr>
<tr>
<td>4. &lt; more &gt;</td>
</tr>
</tbody>
</table>

Notes: To see additional languages select 4. < more >.

Available Languages
- English
- Français (French)
- Español (Spanish)
- Deutsch (German)
- Português (Portuguese)
- Italiano (Italian)
- Русский (Russian)
- 中文 (Chinese)
- 日本語 (Japanese)
- 한국어 (Korean)

1. Power on the Reader.
2. Select the language by pressing the corresponding number on the keypad. Example: For English, select 1.

Notes: All enrollment actions are performed locally to the Reader.
After Initial Setup, additional functionality for the chosen Operational Mode can be accessed via the Administration menu (see Section 2.1.4: Operational Mode).

13.56 MHz Credential Compatibility
- iCLASS® Seos® 8kB (iCLASS® Seos® 16kB - NOT COMPATIBLE)
- Standard iCLASS® 16-32kB bit Access Control Application (iCLASS SE and 2k bit Standard iCLASS - NOT COMPATIBLE)

Biometric Authentication Compatibility
- ANSI-378 template stored on iCLASS Seos credential
- bioCLASS® template stored on standard iCLASS credential (6180A enroller template - NOT COMPATIBLE)

This User Guide is for informational purposes only. HID makes no warranties, expressed or implied, in this summary. Company, product names and data used in sample output are fictitious. Specifications are subject to change without notice.
© 2017 - 2019 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, the HID Brick Logo, iCLASS SE, Secure Identity Object, and Seos are trademarks or registered trademarks of HID Global, or its licensors, in the U.S. and/or other countries. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

hidglobal.com An ASSA ABLOY Group brand
3. The selected language will appear on the screen.
   - Choose 1. Yes to confirm or 2. No to cancel and go back to
     the language selection dialog.

<table>
<thead>
<tr>
<th>HID Language</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>1. Yes</td>
<td>2. No</td>
</tr>
</tbody>
</table>

Note: Language selection will restart until a language is chosen.

4. From this point on, all screens will display in the selected language.

Note: To change the language after the Initial Setup, go to the Administration menu and select Configuration (see Section 4.2.3: Configuration Menu Functions).

2.1.2 Select Credential Type

Once the language is chosen, Initial Setup advances to the Credential Type menu. This configures the credential types that the Reader will enroll. To read Seos credentials, Seos must be selected during initial set-up to allow the Seos Site Key to be entered, after the Site Key has been entered the Credential Type configuration can be changed to allow iCLASS credential to be enrolled. Credential types setting does not configure the card types the reader will read, this is a factory configuration and by default the reader will read both iCLASS and Seos.

<table>
<thead>
<tr>
<th>HID Credential type</th>
<th>1. Seos</th>
<th>2. iCLASS</th>
</tr>
</thead>
</table>

1. To select the Template Type:
   - Select 1. Seos. This Mode enrolls Seos cards but will not enroll iCLASS or iCLASS SR cards.
   - Select 2. iCLASS. This Mode enrolls only iCLASS or iCLASS SR cards.

2. Once you make your choice a confirmation dialog appears, Choose 1. Yes to confirm or 2. No to cancel and return to the Template Type menu.

2.1.3 PIN Requirement (Local PIN Verify)

Note: PIN Required MUST be set to Not Required UNLESS reader is ordered with Local PIN Verify factory configuration option. Local PIN Verify is used extremely infrequently and therefore PIN Required MUST be configured to Not Required unless for special Local PIN Verify applications.

Note: If set to Required and the reader is ordered without Local PIN Verify configuration option, the reader will need to be reset via the supplied SE BIO Initial Setup Reset Cards to PIN Required set to Not Required.

Note: When the reader is ordered without Local PIN Verify configuration option, PIN data entered on keypad will be sent to the door controller for verification.

PIN Requirement is ONLY applicable to readers with Local PIN Verify factory configuration option. It selects whether a PIN enrolled to the card by the reader must be verified locally by the reader before the card data is sent to the door controller. If Required is chosen, a PIN number will be asked for when Users and Admins are enrolled, and also when cards are presented to a Reader to gain access. (For more information on PINs, see Second page of Configuration options in Section 4.2.3: Configuration Menu Functions).

   - Select 1. Required or 2. Not Required.
   - When you make your choice a confirmation dialog appears, Choose 1. Yes to confirm or 2. No to cancel.

2.1.4 Operational Mode

Once the Template Type and PIN Requirement choices are made, Initial Setup advances to the Operational Mode menu.

<table>
<thead>
<tr>
<th>HID Mode</th>
<th>1. Reader/Enroller</th>
<th>2. Enroller Only</th>
<th>3. Reader Only</th>
</tr>
</thead>
</table>

To select the Operational Mode:
   - Select 1 for Reader/Enroller: The Present Card menu will be the main interface thereafter. This mode allows the reader to act as either a reader or enroller.
   - Select 2 for Enroller Only: The Administration menu will be the main interface thereafter.
   - Select 3 for Reader Only: The Present Card menu will be the main interface thereafter.

Confirm the choice:
   - Select 1. Yes to confirm.
   - Select 2. No to cancel and return to the Operational Mode menu.
   - If you select 1. Yes, a confirmation dialog appears. Choose 1. Yes to confirm or 2. No to cancel.

This ends the Initial Setup - Functional Selections stage. The next stage differs, depending on the Template Type chosen.

Note: If the Reader is switched off at this point in the Initial Setup process it will return to this stage when it is switched back on.

2.2 Initial Setup – Site Key

Note: A Site Key must be entered for all readers with Template Type set to Seos (including both HID Elite and Standard Key readers), however, the Site Key is only used by Standard Key readers.

The Site Key setup follows the Operational Mode setup.

The Site Key encrypts the biometric credentials onto the card so they are unique to each site. The Site Key must be between 6 and 11 characters and must be entered identically onto all readers on that particular site.

To choose the Site Key:

1. Enter the Site Key and press #.
2. The reader will display Verify Key. Enter the Site Key number again and press #.

<table>
<thead>
<tr>
<th>HID Site Key</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter PIN</td>
<td>*****</td>
</tr>
</tbody>
</table>

Note: If the Site Key number is not entered within the timeout period the Reader will display Enrollment Failed and return to the Site Key menu.

3. Once the Site Key value has been successfully entered and verified, the Reader displays Success! and advances to the next stage.
2.3 Initial Setup – Verify Admin

The final stage of Initial Setup registers the Admin card. The Reader presents two choices: Enroll Admin or Present Card in order to verify an existing Admin card.

3. Operation – Reader

In Reader Mode, the display shows the Present Card screen.

4. Operation – Administration

4.1 Access the Administration Menu

If the Reader is configured to be a Reader/Enroller and the user wishes to access Administration mode, follow this procedure:

1. The Reader that is configured to be a Reader/Enroller displays the Present Card menu as its main screen.
2. Before you present a card, select 1 on the keypad.
3. Present an Admin card then remove the Admin card from the reading field and follow the on-screen prompts to verify biometric information and Local PIN Verify number as required.

4.2 Administration Menu Functions

From the Administration menu, access the functions below.

4.2.1 Manage Users

This presents the choice of enrolling or verifying a User; the standard Enrollment dialog is used (see Section 2.3.1: Enrollment Dialog).
4.2.2 Manage Admins

This presents the choice of enrolling an Admin or verifying an existing Admin card. Each option follows the standard Enrollment dialog (see Section 2.3.1: Enrollment Dialog). The other choice is to revoke an Admin. If this option is chosen the user must present an existing Admin card to the reader. Users need to ensure they always have at least one Admin card on the site as the only way to get a replacement Admin card is to reset the reader to the factory setup and go through the initial setup process.

4.2.3 Configuration Menu Functions

To access the Configuration menu, select 3 from the Administration menu.

**Note:** The options in the Configuration menu will differ, depending on how the Reader has been set up. For example, if the Reader has been set up for iCLASS or iCLASS SR cards, then non-relevant menus (e.g., Site Key) will not be displayed.

### Configuration Menu Functions

**Configuration**

1. Language: Changes the language.
2. Credential type: Changes the Template Type.
3. Mode: Changes the Operational Mode.
4. < more >

**Notes:**

- If the user changes the Template Type from iCLASS cards to Seos cards, then the user must exit the Administration menu before enrolling Seos User or Admin credentials. After exiting the Administration menu the reader will prompt the user to enter a Site Key for reader Seos operation. The Site Key can then be set and an Admin card created which matches the Site Key of the reader. **Note:** If the Template Type is changed in this way, all readers on a site must be reconfigured with the same Site Key.
- If the user changes the Template Type from Seos cards to iCLASS cards, then the Reader will reboot into Initial Setup - Verify Admin mode. The confirmation Yes/No dialog will display (because the Site Key is not required for iCLASS or iCLASS SR cards).

**Mode:** Changes the Operational Mode.

Select 4 < more > to see the next page of Configuration options.

### Second page of Configuration options

**Configuration**

1. PIN Required
2. BIO Required
3. Capture Quality
4. < more >

**Notes:**

- **PIN Required**
  - Yes: To require a Local PIN Verify for access.
  - No: Does not require a PIN for access (Default).
  
  **Note:** The PIN Required setting can only be changed from Yes to No if the reader is ordered with the Local PIN Verify factory configuration option. Also all cards on site may need to be re-enrolled, because they may have been previously enrolled when no Local PIN Verify was required. To facilitate this migration process, it is suggested that the user sets up one or more separate, dedicated enrollers that require a Local PIN Verify and use these enrollers to add PINs to users’ cards, including Admin cards. The site Readers are set to ignore Local PIN Verify so they will be able to accept the re-enrolled cards. Once all of the user cards have been re-enrolled then the rest of the Readers on the site can be reset to require Local PIN Verify.

**Note:** When a PIN is enrolled to iCLASS cards via the RKL40 reader, this PIN can be used by both RKL40 and R(P)K40 readers configured for Local PIN Verify.

- **BIO Required**
  - Yes: To require a fingerprint presentation for access (Default).
  - No: Does not require a fingerprint presentation for access.

**Note:** Seos Credentials require a fingerprint template enrolled on the credential for configuration option BIO Required = No. A fingerprint will not need to be presented for this option.

### Third page of Configuration options

**Configuration**

1. Firmware: Displays the Firmware information, if needed, when working with Technical Support.
2. Visitor Card Enabled

**Note:** Press # to bring up a page with the Site Key number. The Site Key number page is only visible to Admins and is a hidden option to prevent unintended display. The Site Key number should be kept secure. (Option only appropriate when the Template Type is set to Seos).

- **Visitor Card Enabled:** This option is only available if the Template Type is set to iCLASS.
  - Yes: To allow visitor cards to be used in this environment.
  - No: Do not allow visitor cards in this environment (Default).

If you select Yes and go to Manage Users there will now be a third choice in the Enrollment dialog: Enroll Visitor. Visitor cards are prepared ahead of time, are generic, and can be given to visitors without requiring them to enroll their biometric information. No fingerprint information will be processed by the reader. If PIN Required (Local PIN Verify) is set, visitors will need to be told what the Local PIN Verify PIN value is to permit access.

Select 4 < exit > to return to the first screen of Configuration options.

4.3 Sensor Cleaning

For optimum performance, it is recommended that you clean the biometric reader periodically. The use of a dry cloth is recommended to clean the acquisition surface. In order not to scratch the surface, remove all dust and residue with gentle movements.

**CAUTION:** Acidic liquids, alcohol or abrasive materials are prohibited.

4.4 Additional References

Documents kept up-to-date and available on-line:

- iCLASS SE Biometric Reader Advanced Use Case Application Note - [www.hidglobal.com/PLT-03345](http://www.hidglobal.com/PLT-03345)