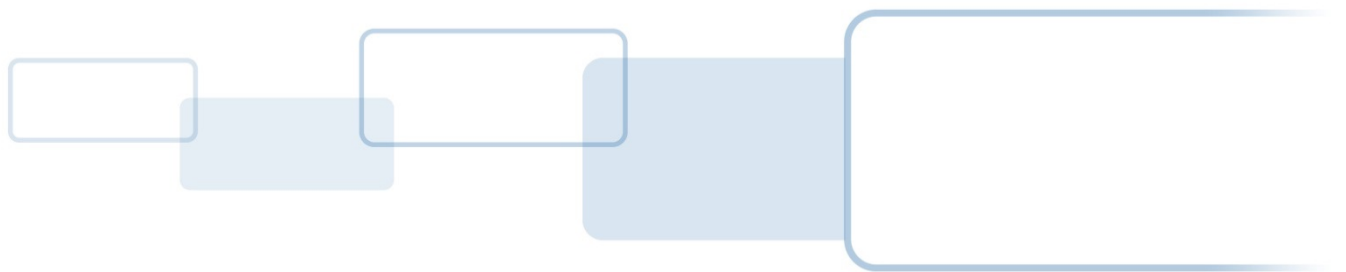




HID Mobile Access Solution Overview

PLT-02078, Rev. A.1
March 2015





Contents

1	Introduction	4
1.1	What is HID Mobile Access?	4
1.2	Document Purpose and Further Reference	4
1.3	Legal Framework	5
1.4	Definitions, Acronyms and Abbreviations	6
2	Possible Solution Variations	7
2.1	Choice of Communication Standard	7
2.2	Choice of Door Opening Mode	8
3	Solution Components	9
3.1	HID Mobile Access Readers.....	9
3.2	HID Mobile Access Portal	9
3.3	Mobile IDs.....	9
3.4	HID Mobile Access Application.....	10
4	Solution Deployment	11
4.1	Installing Mobile Readers	11
4.1.1	Infrastructure Requirements.....	11
4.1.2	Installation	11
4.1.3	Configuration	12
4.1.4	Environmental Considerations.....	12
4.2	Onboarding Process	13
4.3	Managing Users and Mobile IDs	13
4.3.1	Infrastructure Requirements.....	13
4.3.2	Requesting a Login to the HID Mobile Access Portal.....	13
4.3.3	Using the HID Mobile Access Portal.....	14
4.3.4	Recommended Enterprise Policies.....	15
4.4	Mobile Device Setup.....	15
4.4.1	Supported Devices	15
4.4.2	Installation of the HID Mobile Access App	15
4.4.3	Opening Doors with the HID Mobile Access App	16
4.4.4	User Training	16
4.5	The Role of the Access Control System	17
4.6	Extending the Service.....	17
4.7	Terminating the Service.....	17
5	Conclusion and Future Opportunities	17

Copyright

©2014 - 2015 HID Global Corporation/ASSA ABLOY AB.

All rights reserved. This document may not be reproduced, disseminated or republished in any form without the prior written permission of HID Global Corporation.

Trademarks

HID GLOBAL, HID, the HID logo, HID Mobile Access, iCLASS SE, multiCLASS SE, and Seos are the trademarks or registered trademarks of HID Global Corporation, or its licensors, in the U.S. and other countries.

Revision History

Date	Description	Version
3/11/15	Updated section 4.4.1 Supported Devices	A.1
10/1/14	Initial release	A.0

Contacts

For additional offices around the world, see www.hidglobal.com/contact.

North America

611 Center Ridge Drive
Austin, TX 78753
USA
Phone: 866-607-7339
Fax: 949 732 2120

Asia Pacific

19/F 625 King's Road
North Point, Island East
Hong Kong
Phone: 852 3160 9833
Fax: 852 3160 4809

Europe, Middle East and Africa

Haverhill Business Park Phoenix Road
Haverhill, Suffolk CB9 7AE
England
Phone: 44 (0) 1440 711 822
Fax: 44 (0) 1440 714 840

Brazil

Condomínio Business Center
Av. Ermanno Marchetti, 1435
Galpão A2 CEP 05038001
Lapa - São Paulo/SP
Brazil
Phone: 55 11 5514-7100

HID Global Technical Support: support.hidglobal.com

1 Introduction

1.1 What is HID Mobile Access?

HID Mobile Access® complements your existing access control solution. Besides using cards or fobs, your staff can now securely access the facility using their Android or iOS mobile device.

HID Mobile Access, powered by Seos® consists of the following components:

- **HID Mobile Access Portal:** A management portal that allows you to manage users and securely issue or revoke Mobile IDs to users' handsets. The portal is available as a hosted service.
- **HID Mobile Access Application:** This app is for Android and iOS devices
- **Mobile IDs:** The Mobile IDs with integrated Seos technology are for management of trusted identities
- **iCLASS SE® or multiCLASS SE® mobile-enabled Readers**

HID Mobile Access has been designed for commercial deployments in enterprises, educational institutions, government offices or health care facilities. ASSA ABLOY, HID Global's parent company, markets similar solutions using Seos technology to the hospitality, automotive and residential markets.

1.2 Document Purpose and Further Reference

This document is aimed at Enterprise Security Directors who have invested in *HID Mobile Access* as well as Project Managers responsible for deploying the solution in the enterprise as a first point of reference.

It provides a high level overview of the solution, how the components interact with each other and how you can get the most out of your investment.

Additionally, the following reference documents are available for more detailed information:

Document Name	Description	Target Audience	Available from
HID Mobile Access Frequently Asked Questions	Support documentation for portal administrators	Portal Administrators	HID Mobile Access Portal
HID Mobile Access Reader Deployment Guide	Information about reader installation and environmental considerations	Installers	HID Global Partner Portal HID Mobile Access Portal
HID Mobile Configuration Application User Guide	Information on how to use the Config App in order to change the BLE reader Configuration settings and update module firmware.	Installers	HID Global Partner Portal HID Mobile Access Portal
HID Mobile Access App User Guide	Explains the HID Mobile Access App and the interaction between the mobile device and the reader	Users	HID Mobile Access Portal

1.3 Legal Framework

You have purchased *HID Mobile Access* via an HID Global channel partner. In addition to any purchase orders or contracts you may have signed with your supplier, *HID Mobile Access* requires Portal Administrators and Users (the persons using *HID Mobile Access* on their mobile devices) to accept the following license agreements and privacy policies before they can start using the service:

Document Name	Description	Parties	Available from
HID Mobile Access Terms of Service	Informs Portal Administrators of their role and responsibilities in connection with the service. Contains information about HID Global's warranty and liability. Refers to the HID Secure Identity Services Privacy Policy.	HID Global - Portal Administrators	Accepted on registration of a user login for the portal
HID Secure Identity Services Privacy Policy	Covers data collected about Portal Administrators via the portal as well as user data uploaded by Portal Administrators and stored on HID Global servers.	HID Global - Portal Administrators	Displayed within the footer of each portal page
HID Mobile Access License and User Agreement	Grants license to use the service and governs obligations of how to use it responsibly.	HID Global - Users	Accepted during App registration process via click-through
HID Mobile Access Privacy Policy	Covers data collected about Users via the mobile device and stored on HID Global servers.	HID Global - Users	Accepted during App registration process via click-through

Due to the fact that Portal Administrators are transferring user data to the portal on behalf of the enterprise, you should additionally provide a privacy policy to your Users covering the transfer and storage of this data. The minimum data required to set up a User is first name, last name and email address.

1.4 Definitions, Acronyms and Abbreviations

Mobile ID	This is the virtual credential that is stored on the mobile device and issued or revoked via the <i>HID Mobile Access Portal</i> .
BLE	Bluetooth Low Energy (marketed under the name Bluetooth Smart)
HCE	Host-based Card Emulation - like NFC but controlled through software in the mobile device
NFC	Near Field Communications (typically 13.56 MHz air interface)
PACS	Physical Access Control System
Seos	A technology platform created by HID Global which provides a secure, portable, adaptable, device-agnostic way of managing secure identity information and applications.
SIO	Secure Identity Object - A managed set of identity data protected by a unified security architecture

2 Possible Solution Variations

2.1 Choice of Communication Standard

HID Mobile Access supports either Bluetooth Smart (BLE) or NFC for the communication between mobile device and reader.

BLE uses the 2.4 GHz radio frequency which allows for a longer read range, theoretically up to 10m, and higher bandwidth than NFC. Benefits are:

- Supports Android and iOS devices
- Supports short and long read distance
- Requires the *HID Mobile Access* module installed in the reader

NFC has originally been developed for contactless payment and operates at the same 13.56 MHz frequency as smart cards. Benefits are:

- Supports Android devices with the Operating System version 4.4 or higher (which includes the Host-based Card Emulation feature).
- Supports short read distance analog contactless smart cards (*Tap* mode)
- Supports the latest generation of mobile-enabled readers at launch, but many installed iCLASS SE readers in field will be able to be upgraded to the latest firmware in 2015. The *HID Mobile Access* module is not required for NFC only use.
- Slightly shorter transaction time over BLE

Note: There is no significant difference in battery consumption or security levels between the two communication standards.

2.2 Choice of Door Opening Mode

HID Mobile Access supports two different door opening modes: *Tap* or *Twist and Go*. The *Tap* mode is available for both communication standards (NFC and BLE), whereas the *Twist and Go* mode is only available with BLE.

Tap mode – the mobile device functions like a physical credential.

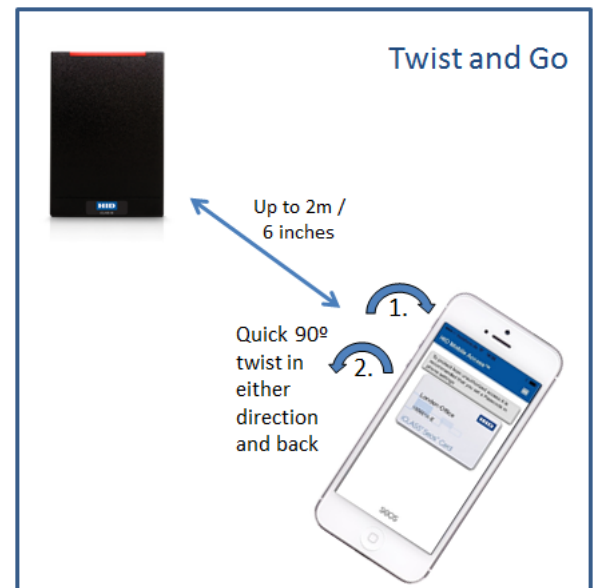
Touch the mobile device to the reader. If both BLE and NFC are enabled in the mobile device, the reader will default to using NFC for this mode because it is quicker.



Twist and Go mode – this uses HID Global's patented gesture technology to unlock the nearest door from a distance of up to 2 meters (6 feet).

The reading distance is configurable, however these settings may be different, due to environmental factors (i.e. the surface the reader is mounted on) and the hardware and software of the mobile device.

Setting a longer read distance is ideal for garages, ware houses and for vandal proof installations where the reader is on the inside of the door. It can also help meet some accessibility requirements for persons with mobility disablements.



3 Solution Components

3.1 HID Mobile Access Readers

HID iCLASS SE Mobile Access Readers are physical access wall mounted readers that read Mobile IDs (virtual credentials on mobile devices) as well as 13.56 MHz and 125 kHz contactless credentials (with the exception of Indala Prox). The reader achieves this by first securely reading a physical access card number and then transmitting the number to an access control panel. No special system modifications are required to read Mobile IDs. Existing Wiegand readers can easily be replaced and work with existing access control panel hardware.

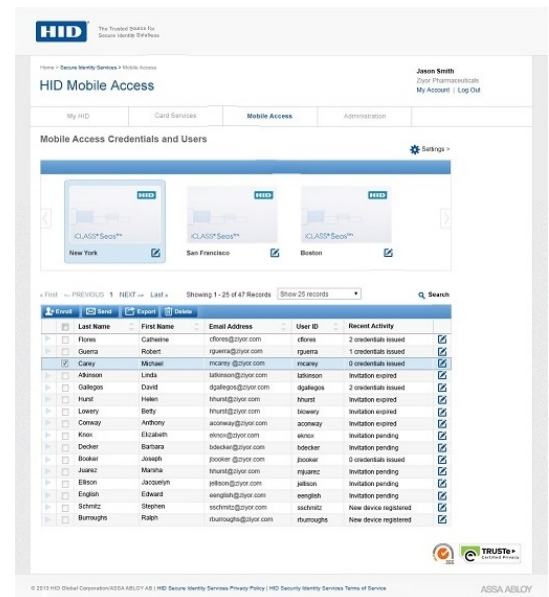


In order to use *HID Mobile Access* in BLE mode, an *HID Mobile Access* module is required to be installed at factory. Readers then also come with a special back plate which directs the read range to the front of the reader. Mobile Administration cards are necessary to transfer the reader into a state where the read range can be configured.

3.2 HID Mobile Access Portal

The *HID Mobile Access* Portal, or to be more specific, the *HID Mobile Access* application within HID Global's Secure Identity Services Portal, allows enterprise administrators to manage users and issue and revoke Mobile IDs to user's mobile devices.

The portal is a hosted service available to registered users via <https://managedservices.hidglobal.com>. Each enterprise has its own instance of the portal, which is set up by HID Global during the Onboarding Process. See *Section 4.2: Onboarding Process*.



3.3 Mobile IDs

Mobile IDs are the virtual credentials that are stored on the mobile device and issued or revoked via the *HID Mobile Access* Portal. Mobile IDs are unique to each device so that they cannot be copied. If a user switches devices a new Mobile ID must be issued.

Once the Onboarding Process has been completed, your purchased Mobile IDs will already be set up in the *HID Mobile Access* Portal. See *Section 4.2: Onboarding Process*.

3.4 HID Mobile Access Application

The *HID Mobile Access App (phone application)* manages the Mobile IDs and contains some limited user settings.

Users can download the *HID Mobile Access App* free of charge for Android mobile devices via *Play Store* and for iOS devices via the *Apple App* store.

However, ideally the Portal Administrator enrolls new users via the portal first. This generates an invitation email with the links to the respective app stores as well as a registration code. During the registration, users are asked to accept the *HID Mobile Access License and User Agreement* as well as the *HID Mobile Access License Agreement*. See *Section 1.3: Legal Framework* for more information.



4 Solution Deployment

4.1 Installing Mobile Readers

4.1.1 Infrastructure Requirements

HID Mobile Access requires a “Mobile-Enabled” iCLASS SE or multiCLASS SE reader which has been personalized for use with your organization’s Mobile IDs.

Mobile-Enabled	A Mobile-Ready reader that has been personalized for use with your organization’s Mobile IDs.
Mobile-Ready	<p>A “Mobile-Ready” reader is prepared for use with Mobile IDs but lacks specific company configuration. These readers are populated with all the necessary hardware and firmware to work with either BLE and/or NFC mobile devices, but lack the security synchronization for a specific end user company.</p> <p>Config cards to personalize mobile-ready readers can be requested during the onboarding process. HID Global will provide part numbers so these cards can be purchased.</p> <p>Enterprises may purchase and install mobile-ready readers (using generic part numbers) in preparation for moving to mobile at a later time.</p>
Mobile-Capable	<p>A “Mobile-Capable” reader is built from the base iCLASS SE platform prior to market introduction of HID Mobile Access. The reader is not prepared with the necessary hardware and/or firmware to work with Mobile IDs.</p> <p>In the near future, it will be possible to upgrade these readers to support HID Mobile Access, but this process is under development.</p>

If you have purchased readers and the *HID Mobile Access* service subscription at the same time, your readers will be personalized at factory to be Mobile-Enabled. In order to ensure that your existing credentials and environmental conditions will be taken into account, your installer will perform a site survey before placing his order with HID Global. You will then be assigned a custom part number for your readers, which will include all the personalization information for your readers.

If you have purchased the *HID Mobile Access* service subscription at a later time, after mobile-ready readers have already been installed at your site, your installer will personalize those readers using Configuration cards, creating Mobile-Enabled readers.

Installed Reader Infrastructure

There is no need to replace all your installed readers at the same time. *HID Mobile Access* readers look exactly like standard iCLASS SE readers. If you would like your users to recognize the readers with mobile capability, we recommend either using the blue LED light (which is an orderable configuration) or marking readers with a small dot sticker (available in retail).

4.1.2 Installation

The installation of *HID Mobile Access* readers should be performed by an experienced installer, but it should not be any more complicated than that of standard HID readers.

Existing Wiegand readers can easily be replaced and the new readers work with existing access control panel hardware.

4.1.3 Configuration

Depending on your environment and user requirements, *HID Mobile Access* may require some configuration steps after reader installation:

1. Personalization of Mobile-Ready readers

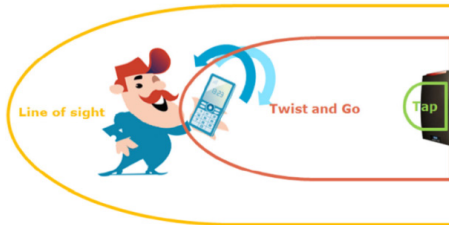
If you are using a Mobile-Ready reader, it must be personalized using a Configuration card. This turns your Mobile-Ready reader into a Mobile-Enabled reader, which can then be used in NFC mode without any additional configurations. See *Section 4.1.1: Infrastructure Requirements*, Mobile-Ready information.

If you have purchased readers and the *HID Mobile Access* service subscription at the same time this step will not be necessary.

2. Configure read range

This is only applicable if BLE is used for communication between mobile device and reader.

Your installer can configure the BLE read range of your reader using a *Mobile Admin* card and the *HID Mobile Access Configuration Application* (a.k.a. BLE Config App) currently available on Android. **Note:** The default setting for the reader is *Tap* mode. To adjust the read range for *Twist and Go*, your installer can adjust the following values:



- **Line of sight** corresponds to the distance at which a mobile device can see a reader. This is defined by the Tx value (transmit power of the BLE signal) in the *HID Mobile Access Module* firmware.
- **Twist and Go Threshold** defines the distance at which a user can do a *Twist and Go* gesture to trigger an unlock sequence.
- **Tap Threshold** defines the distance at which a user can hold the mobile device to a reader to trigger an unlock sequence.

The actual distance achieved with the above values is, dependent on environmental conditions at the site. **Note:** Your readers can be configured to only allow *Tap*.

Your installer has access to *the HID Mobile Access Reader Deployment Guide*, which contains additional information on how to install and configure *HID Mobile Access* readers.

4.1.4 Environmental Considerations

Environmental conditions at the site influence the achievable read distance. Metal takes power away from RF fields and thus decreases read ranges. This is true not only for BLE devices but contactless credentials as well. Plastic spacers (of 0.5" and 1.0", reader form factor dependent) can be used to space the reader away from metallic surfaces and reduce the impact the metal will have on read range. Your installer will be able to advise you accordingly.

Note: Spacers are orderable, and part numbers can be found in the *Mobile How to Order Guide* at <http://www.hidglobal.com/documents>.

4.2 Onboarding Process

The Onboarding Process is a HID Global internal process which is triggered on receipt of the purchase order for the **HID Mobile Access** service subscription from your supplier. During this process, HID Global will set up an instance of the portal for the enterprise and create the personalization specification for Mobile IDs and mobile-enabled readers.

If you wish to configure the read range for BLE, HID Global will also create the necessary *Mobile Admin* cards for you at that time.

The input for this process is:

- Purchase order for the HID Mobile Access service subscription
- Site survey/onboarding form
- Requesting a Login to the HID Mobile Access Portal, see Section 4.3.2.

The output of this process is:

- Custom part numbers for ordering Mobile IDs and mobile-enabled Readers (as input for your supplier to raise the corresponding purchase order).
- Portal account established
- Mobile IDs uploaded to the portal
- Creation of *Mobile Admin* cards

4.3 Managing Users and Mobile IDs

4.3.1 Infrastructure Requirements

The *HID Mobile Access* Portal can be accessed via the internet on <https://managedservices.hidglobal.com>.

The following browsers (latest versions) are supported:

- Internet Explorer 9.x and 10.x
- Firefox 37.0.2062.120 m
- Chrome 32.0.1
- Safari 5.1.7

4.3.2 Requesting a Login to the HID Mobile Access Portal

To setup an Administrator account for the *HID Mobile Access* Portal:

1. Request a log-in
 - With your web browser navigate to <https://managedservices.hidglobal.com>
 - Click the **Request an account** link located in the login pane.
 - After completing the online form with your company and contact information, you will receive a temporary password.
2. Log into the portal using this temporary password and complete the setup.
3. Log out and log back in to confirm that all is working as expected.

Note: Initially you will see only the **My Account** link. Within two business days, the *HID Mobile Access* link will appear in the navigation section on the right of the screen.



Then familiarize yourself with the portal functions; a good place to start is the *HID Mobile Access Frequently Asked Questions* document which can be downloaded from this page.

The first Administrator requesting a log-in will be setup as the Company Administrator. To setup additional portal users, send an email to SISRequest@HIDGlobal.com providing the details in the table below:

Email to: SISRequest@HIDGlobal.com

From: <<FirstName>> <<LastName>>, <<Company>>

Email Address	Last Name	First Name	Mobile Device	Role* (Administrator, Operator, Reviewer)

***Administrator:** Full access to all functionality.

Operator: Able to add mobile device holders and issue/revoke Mobile IDs, but cannot perform configuration operations.

Reviewer: Read only access. Cannot add/edit data, or issue/revoke Mobile IDs.

4.3.3 Using the HID Mobile Access Portal

The following features and functionalities are available at this time:

- Two-factor authentication on log-in.
- Enroll users individually or in batch by importing a .csv file
- Invite users individually or in batch. This function generates an invitation email with details on where to download the *HID Mobile Access Application* and a registration code.
- Edit invitation email (customize to the enterprise’s requirements).
- View status of invitations.
- Issue a Mobile ID to a mobile device. This can be done automatically as part of the enrollment process, or as a second manual step thereafter.
- Revoke a Mobile ID from a mobile device.
- Multiple credentials per enterprise (e.g. different credentials for different sites).
- Configure up to 5 devices per user and up to 10 Mobile IDs per device.
- Batch-download of users and Mobile IDs. This generates a .csv file that can be uploaded into the Access Control System in order to assign access rights to Mobile IDs.
- Change badge image to corporate colors (transferring the image to the mobile device will be available later in 2015).

Please refer to the *HID Mobile Access Frequently Asked Questions* document, available from the related links section of the Portal, or the Help link to the Knowledge Base for additional information.

4.3.4 Recommended Enterprise Policies

HID Global recommends implementing the following policies within your enterprise environment in combination with *HID Mobile Access* as part of your IT or HR policy:

- Install reporting process for loss of the mobile device and subsequent revoking of Mobile ID, and disabling of Mobile ID in the Access Control System.
- Ban jail broken mobile devices where the Operating System (OS) has been compromised. To jail break (or root) a device circumvents the built-in security and protection of the OS, opening the mobile device to high risk from malware and unsupported uses.
- Mandate the use of passcode or fingerprint (iPhone) scan as additional security mechanism against loss of the mobile device (setting within the application). While this reduces comfort, it enhances the security in comparison to regular access cards.
- Use a mobile device management system to manage company mobile devices (useful not only for mobile access, but also to secure company email and other vital company information). *HID Mobile Access* will work with most leading device management software.

4.4 Mobile Device Setup

4.4.1 Supported Devices

The following mobile devices are currently supported for *HID Mobile Access*:

Operating System	Verified Device Models
iOS 7+ with Bluetooth 4.0	<ul style="list-style-type: none"> • iPhone: 4S, 5, 5C, 5S, 6.6 Plus • iPad: Air, Mini, 3rd & 4th gen • iTouch
Android 4.3+ with Bluetooth 4.0 Android 4.4+ with Bluetooth 4.0 or NFC (Host Card Emulation)	<ul style="list-style-type: none"> • Google Nexus 5/6 • Samsung Galaxy Note 3/4, S4, S4 Plus, S5 • Sony Xperia Z2/Z3 • HTC One

Devices are added on a continual basis. **Note:** There may be regional differences in device operability, as OS versions are pushed at different times in each region.

4.4.2 Installation of the HID Mobile Access App

Upon enrolling a new user, the *HID Mobile Access* Portal generates an email to the user which contains the links to the app stores to download the application and the registration code. **Note:** This email can be customized for your company.

After downloading the application, the user is prompted to register by entering the 16-digit registration code and accepting the license agreement and privacy policy.

During the registration process, the device is registered with the *HID Mobile Access* Portal and Mobile IDs can now be pushed to the device. Depending on how this was set up in the portal, this either happens automatically within a couple of minutes after registration, or the Portal Administrator pushes this manually in a second step. The mobile device must be connected to the internet (either via mobile data network or Wi-Fi) during mobile device registration and Mobile ID delivery.

4.4.3 Opening Doors with the HID Mobile Access App

In order to open doors with the *HID Mobile Access Application*, Bluetooth and/or NFC must be enabled in the mobile device settings to communicate with the readers. The application will prompt the user, if this has not been done.

Opening doors with HID Mobile Access

1. Unlock the screen and open the *HID Mobile Access Application*. The application uses negligible battery power and can be left running in the background.
2. Open the door using *Tap* (NFC or BLE) or *Twist and Go* (BLE)

Note: *Tap* and *Twist and Go* must be enabled on the mobile device and the reader.

If you receive a **Reader out of range** error message on *Twist and Go*, move closer to the reader and try twisting the device again.

See *Section 2.2: Choice of Door Opening Mode* for more information.

The application offers additional features, but there may be differences in the user experience across Android and iOS devices:

Mobile ID Protection

This setting is on by default as it increases the security; it ensures that users have to enter the device PIN and open the App before they can open a door. Some users like to disable the Mobile ID Protection for more convenience. If disabled, there may be slight variations across different operating systems, Some phones may require users to push the home button to light up the screen, some phones may work with a black screen.

Sound and Vibration Feedback

You can enable and disable the sound and vibration on the *Settings* menu.

Twist and Go

The motion sensor can be disabled on the mobile device side, for readers set to long read distance.

4.4.4 User Training

Previous customer experience has shown that a short introduction and demo of the door opening experience for the first user groups enhances the user satisfaction with the solution.

- Show how the *Twist and Go* motion works. The application contains an animation within the *Help* menu, but it is best to see it in real life.
 - Make users aware of the NFC antenna in their mobile device when using *Tap* mode with NFC. Depending on mobile device model, the NFC antennas are placed in different areas of the mobile device.
 - Provide information on which doors have been set up for *Tap*, which for *Twist and Go* and which doors have potentially not yet been set up for mobile access.

An *HID Mobile Access User Guide* is provided for users, which will provide additional information. **Note:** This document is available via the Portal.

4.5 The Role of the Access Control System

The role of the Access Control Systems does not change with *HID Mobile Access*. The *HID Mobile Access Portal* allows issuing and revoking Mobile IDs, in a similar way to a card printer or card encoder today. Once a Mobile ID has been issued to a mobile device, the access rights for the Mobile ID must be set within the Access Control System in a second step. This also enhances the security of the solution.

4.6 Extending the Service

As soon as you have been through the onboarding process for *HID Mobile Access*, you have custom part numbers to order new mobile-enabled readers and additional Mobile IDs. Please ask your supplier to use these part numbers when placing their order with HID Global. All your personalization information is included in those part numbers.

4.7 Terminating the Service

Termination of service is possible on an annual basis with a notice period of 6 weeks to the renewal date of the *HID Mobile Access* service subscription.

After termination, the enterprise no longer has access to the *HID Mobile Access Portal* to manage Mobile IDs. Any Mobile IDs that have not been issued expire on termination.

Note: After termination, it is no longer possible to revoke Mobile IDs from User's mobile device. Mobile IDs, unless revoked prior to termination, will remain on the mobile device and can continue to be used for access control.

5 Conclusion and Future Opportunities

We hope you will enjoy implementing and using *HID Mobile Access* within your organization.

This first version of *HID Mobile Access* will continue to evolve quickly, and as an existing customer you will automatically benefit from some of the additional features and functionalities. These include the support for additional mobile device operating systems, new device hardware, new portal features and functionalities and security updates to the application. We will keep you informed of any changes via the *HID Mobile Access Portal*.

We are also planning some major new features, such as the inclusion of logical access or BLE support for the installed base of readers, which you can decide whether to adopt on a one by one basis.

