MyID

Self-Service Kiosk

Installation and Configuration Guide

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK
www.intercede.com | info@intercede.com | @intercedemyid | +44 (0)1455 558111

Document reference: IMP1753-13

April 2017

Copyright

Whilst Intercede Limited has made every effort in the preparation of this manual to ensure the accuracy of the information, the information contained in this manual is delivered without warranty, either express or implied. Intercede Limited will not be held liable for any damages caused, or alleged to be caused, either directly or indirectly by this manual.

Licenses and Trademarks

Conventions Used in this Document

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important
  - Bulleted lists are used when the order is unimportant or to show alternatives

- **Bold** is used for menu items and for labels.

  For example:
  - "Record a valid email address in **'From' email address**"
  - Select **Save** from the **File** menu

- *Italic* is used for emphasis and to indicate references to other sections within the current document:

  For example:
  - "Copy the file *before* starting the installation"
  - "See *Issuing a Card* for further information"

- ***Bold and italic*** are used to identify the titles of other documents.

  For example: "See the ***Release Notes*** for further information."

  Unless otherwise explicitly stated, all referenced documentation is available on the installation CD.

- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.

- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.

- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

Warning: You must take a backup of your database before making any changes to it.

Contents

1 Introduction

This document describes the installation and configuration of the MyID® Self-Service Kiosk.

The Self-Service Kiosk is designed to run on a shared PC and allow any cardholder to collect, activate or update their devices, and to request and collect temporary or replacement devices.

The user interface is designed to guide users through the process without requiring extensive training or documentation.

1.1 Prerequisites and installation

For prerequisites and installation instructions, see the readme document provided with this release, which provides details of the MyID versions, software updates and other software you need to have installed on your server and clients.

- Self-Service Kiosk client

  Provided in this software update.
- Web Service Architecture

  You must have the following MyID web services installed on your web server:
  - MyID Process Driver
  - MyID Data Source

  See the ***Web Service Architecture Installation and Configuration Guide*** for details. This document is provided with MyID.

  You are recommended to set up SSL on the connection between the Self-Service Kiosk clients and the MyID web services. See section *2.3*, *Setting up SSL* for details.
- MyID client components

  The Self-Service Kiosk incorporates its own version of the MyID Client Components. You do not have to install the Client Components separately.
- MyID BioPack

  Provided as a separate MyID software update.

  If you intend to use biometric readers on the client PCs, you must install BioPack package of biometric components both on the MyID application server and on each client PC on which you want to use biometrics.

1.1.1 Communication between the Self-Service Kiosk and MyID

To allow your clients to communicate with the MyID server, your PC must be able to communicate with the URLs of the MyID mobile web services; for example:

```
https://myserver/MyIDProcessDriver/
```

```
https://myserver/MyIDDataSource/
```

Where `myserver` is the name of the server on which the MyID web services are installed.

1.1.2 Minimum client PC specifications

Your client PC must meet the following minimum specifications:

- 1 GHz 32-bit (x86) or 64-bit (x64) processor
- 1 GB RAM (32-bit) or 2 GB RAM (64-bit)
- 2 GB hard disk free space
- The Self-Service Kiosk supports the following resolutions:
  - 1024x768
  - 1280x1024
  - 1920x1080
- Network access

1.1.3 Supported operating systems

The Self-Service Kiosk is supported on the following client operating systems:

- Windows 7 (32-bit)
- Windows 7 (64-bit)
- Windows 8.1 (32-bit)
- Windows 8.1 (64-bit)
- Windows 10 (32-bit)
- Windows 10 (64-bit)

1.1.4 Supported biometrics

The Self-Service Kiosk supports the following devices for biometric verification:

- Cross Match Verifier 300 (Windows 7 32-bit only)
- Cross Match Verifier 310 (Windows 7 32-bit and 64-bit only)
- Precise MC-250
- SecuGen Hamster IV
- SecuGen iD-USB-SC/PIV

Note: Do not attach Precise and CrossMatch devices to the same client PC, or you may experience problems that prevent you from scanning fingerprints.

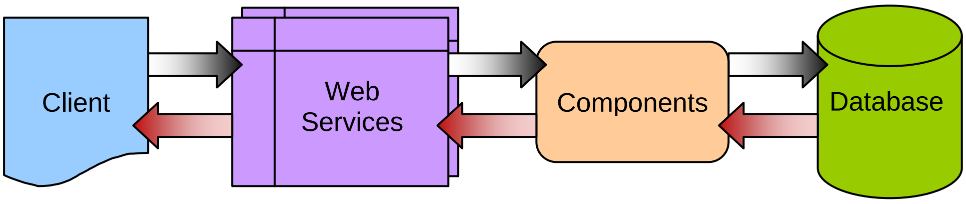
Note: The Cross Match matching library is not currently supported on MyID servers running Windows Server 2012. However, you can use the Cross Match Verifier reader on clients connected to a Windows Server 2012 client if the fingerprints were enrolled using Precise and the matching library is set to Precise. See the ***Cross Match Integration Guide*** for details.

Biometric verification is supported only on MyID PIV systems. It is not supported on MyID Enterprise systems.

Biometric verification is not supported on Windows 10.

1.2 Overview

1.2.1 Architecture



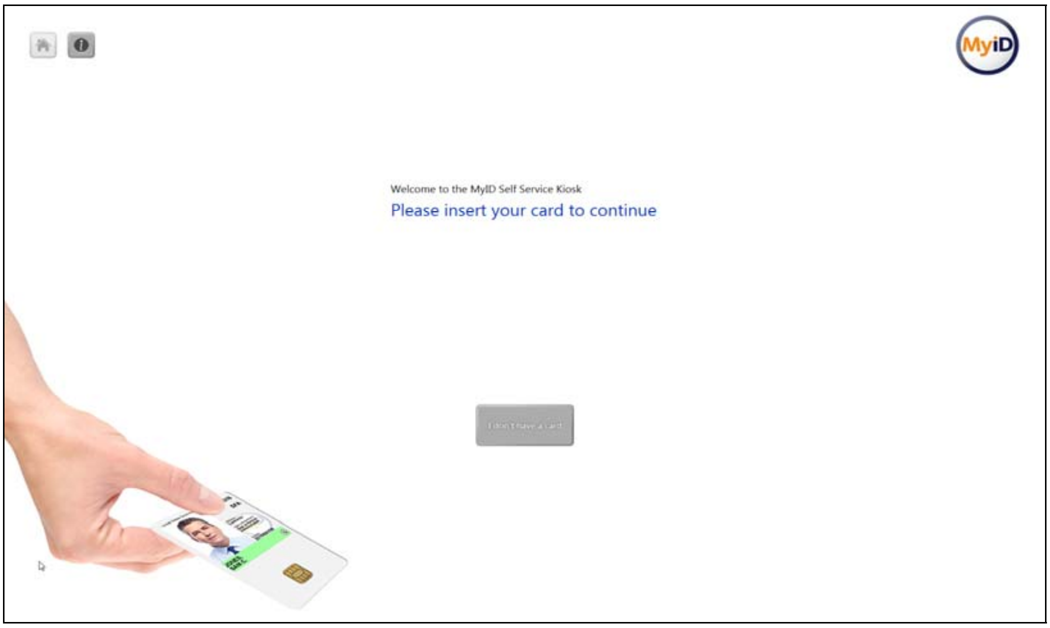
The Self-Service Kiosk passes requests through HTTP or HTTPS to the MyID Data Source and MyID Process Driver web services; both services are required for full operation. The web services communicate using DCOM with the MyID components on the application server; these components provide the business logic and communicate with the MyID database. Responses are returned to the client through the MyID web services.

The web services, components and database may be on separate servers, or on the same server. The two web services must be installed on the same server.

The range of operations you can perform with the Self-Service Kiosk depends on the edition of MyID you are using – you can perform different operations with the PIV and Enterprise editions.

1.2.2 Self-Service Kiosk

The Self-Service Kiosk is designed to run in a public space with users having little or no MyID experience. The Self-Service Kiosk guides users through self-service operations such as card activation. Ideally, the Self-Service Kiosk should run on a dedicated shared PC, and run at startup.


Welcome to the MyID Self Service Kiosk

Please insert your card to continue

A simple scenario would be:

1. A cardholder who has been issued a card that needs to be activated approaches the Kiosk and inserts their card.
2. The Kiosk detects that an Activation job is available for the device.
3. The Kiosk guides the user through the process of activating their card.

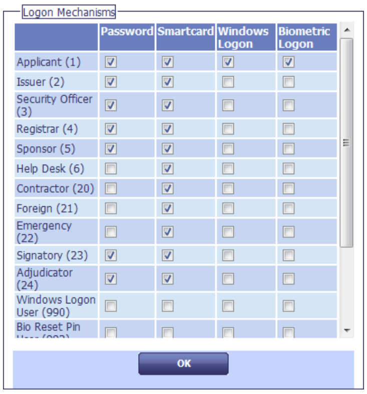
1.2.3 Authentication

The cardholder can authenticate to the MyID server using the following methods:

Method	Self-Service Kiosk
Smart card logon	Y
Security phrase logon	Y
Windows authentication	N
Authentication codes	Y
Logon codes	Y
Biometric logon	For unlocking only

See the MyID documentation for details of setting up the various types of authentication. The Self-Service Kiosk uses the same configuration for authentication as MyID Desktop clients.

When you set up the roles for access to particular workflows, you must make sure that the role has the correct logon methods; for example, if you add all the workflows to the Applicant role, and are using security phrase logon, you must set the Applicant role to have access to the Password logon mechanism.



Logon Mechanisms

	Password	Smartcard	Windows Logon	Biometric Logon
Applicant (1)	☑	☑	☑	☑
Issuer (2)	☑	☑	□	□
Security Officer (3)	☑	☑	□	□
Registrar (4)	☑	☑	□	□
Sponsor (5)	☑	☑	□	□
Help Desk (6)	□	☑	□	□
Contractor (20)	□	☑	□	□
Foreign (21)	□	☑	□	□
Emergency (22)	□	☑	□	□
Signatory (23)	☑	☑	□	□
Adjudicator (24)	☑	☑	□	□
Windows Logon User (990)	□	□	□	□
Bio Reset Pin	□	□	□	□

1.3 Self-Service Kiosk features

Control over which features are available to Self-Service Kiosk users is maintained within MyID by using the standard roles mechanism.

Cardholders who use the Self-Service Kiosk must have permission to log on to MyID using passwords; for example, by having a role that has access to these workflows and that has **Password** selected in its **Logon Methods**. For example, if you grant the cardholders the Applicant role, then add all the workflows to the Applicant role, you must set the Applicant role to have access to the Password logon mechanism.

Use the **Edit Roles** workflow to specify which workflows are available.

The Self-Service Kiosk can carry out the following operations:

- Check for outstanding jobs for the current user.
- Collect a card.

  Requires access to the **Collect My Card** workflow.
- Activate a card.

  Requires access to the **Activate Card** workflow.

  Note: This is not supported on MyID Enterprise.
- Update a card.

  Requires access to the **Collect My Updates** workflow.
- Request and collect a replacement card.

  Requires access to the **Collect My Card** and **Replace My Card** workflows.
- Collect a certificate renewal.

  Requires access to the **Collect My Certificates** workflow.
- Issue a temporary card

  Requires access to the **Request My Temporary Card** workflow.
- Reset the PIN and unlock the card

  Requires access to the **Unlock Card** and **Unlock My Card** workflows.

2 Configuring the Self-Service Kiosk

2.1 Server location

The Self-Service kiosk is configured to communicate with the MyID Web Services server when you install the Self-Service Kiosk. If you want to change the server, you can edit the configuration file.

To edit the configuration file:

1. On the client PC, back up the `MyIDKiosk.exe.config` file in the following folder:

   ```
   C:\Program Files\Intercede\MyIDSelfServiceKiosk\
   ```

   On 64-bit systems, this is:

   ```
   C:\Program Files (x86)\Intercede\MyIDSelfServiceKiosk\
   ```

2. Using a text editor, open the `MyIDKiosk.exe.config` file.

   Note: Make the changes to the config file exactly as shown. The case is important.

3. Edit the `value` parameter in the following line:

   ```
   <add key="Server" value="http://myserver.example.com/"></add>
   ```

   For example:

   ```
   <add key="Server" value="http://myserver2.example.com/"></add>
   ```

4. Save the configuration file.
5. Restart the Kiosk.

2.2 Kiosk page timeout

The Self-Service kiosk is configured to time out after 30 seconds, and ends the current workflow after that period of inactivity. If you want to change the timeout, you can edit the configuration file.

To edit the configuration file:

1. On the client PC, back up the `MyIDKiosk.exe.config` file in the following folder:

   ```
   C:\Program Files\Intercede\MyIDSelfServiceKiosk\
   ```

   On 64-bit systems, this is:

   ```
   C:\Program Files (x86)\Intercede\MyIDSelfServiceKiosk\
   ```

2. Using a text editor, open the `MyIDKiosk.exe.config` file.

   Note: Make the changes to the config file exactly as shown. The case is important.

3. Add the following line to the `<appSettings>` section:

   ```
   <add key="PageTimeoutSeconds" value="30"></add>
   ```

   The value is the timeout in seconds; in this example, 30 seconds.

4. Save the configuration file.
5. Restart the Kiosk.

2.3 Setting up SSL

2.3.1 One-way SSL

If you want to configure the Self-Service Kiosk to use one-way SSL for its communications with the MyID Web Services server, you must install the server's certificate under the Trusted Root Certification Authorities in the user's certificate store.

2.3.2 Two-way SSL

Note: If your server is set up to use two-way SSL, you must set up your client to use two-way SSL. If you do not use the `/ssl` command-line option, an error is displayed.

Note: The Self-Service Kiosk does not support two-way SSL using a certificate stored on a smart card.

To use two-way SSL using a specific certificate:

1. Install the client certificate in the user's personal store.

   The client certificate must have the Client Authentication application policy – this has the following OID:

   ```
   1.3.6.1.5.5.7.3.2
   ```

   Note: Make sure that you issue the client certificate from a different certificate authority from the one you use to issue certificates to end users.

2. Find the client certificate's serial number:

   a) Run the `CertMgr.msc` snap-in.

   b) Expand **Personal > Certificates**.

   c) Double-click the client certificate.

   d) Click the **Details** tab.

3. Run the application using the following command line:

   ```
   MyIDKiosk.exe /ssl /sslsn:<serial number>
   ```

   where:

   `<serialnumber>` – the serial number of the client certificate. Enter the serial number without spaces. For example, if the serial number is:

   ```
   62 00 00 00 34 fe 3c a9 a8 1c 98 6a f1 00 00 00 00 00 34
   ```

   use the following command line

   ```
   MyIDKiosk.exe /ssl /sslsn:6200000034fe3ca9a81c986af1000000000034
   ```

Note: If you copy the serial number from the **Details** tab of the certificate properties dialog, you may inadvertently copy a non-printing character at the start of the serial number. You must make sure that you delete this character from the Kiosk command line. (Position the cursor before the `:` in the command line. Press the right-cursor key once. The cursor appears after the colon. Press the right-cursor key again. If the cursor does not move to after the first number in the serial number, there is a non-printing character present; press the Backspace key to delete it.)

If you run the application with the `/ssl` command line option but omit the `/sslsn` option, the application carries out the following:

1. The application checks the application settings file for the details of the last certificate that was successfully used to log on.
2. If no details are found, if the certificate is no longer in the personal store, or the server rejects the certificate, the application searches the personal store for certificates that match the issuer DN (optionally set up when you install the application) and have the Client Authentication policy.
3. If more than one certificate is found, the application displays a list of certificates for the user to select.

When the application has successfully logged on to the server using a certificate, the certificate's details are stored in the user's application settings file.

2.4 Accessing the web services for the first time

If you access the Kiosk after the web services have been installed on the server, you may experience a timeout that prevents the Kiosk from operating. This is caused by the processing required by the web services when they are first accessed.

As a workaround, you can access the web service page using a web browser before attempting to use the Kiosk. Access the following web page:

```
http://myserver/myidprocessdriver/processdriver.asmx
```

where `myserver` is the name of the web services server.

2.5 Running the Self-Service Kiosk

The installation program creates a shortcut for the Self-Service Kiosk. You are recommended to run the application in one of the following ways:

- Run the Self-Service Kiosk using the shortcut icon.
- Run the Self-Service Kiosk using a Windows Logon script, or by putting a shortcut in the Startup program group.

  This starts up the Kiosk when the user logs in to Windows, and is appropriate for a stand-alone shared PC used exclusively as a kiosk.

2.5.1 Command-line parameters

To run the Self-Service Kiosk from the command line:

1. Open a command prompt and change to the Kiosk folder:

   ```
   C:\Program Files\Intercede\MyIDSelfServiceKiosk\
   ```

   On a 64-bit system, this is:

   ```
   C:\Program Files (x86)\Intercede\MyIDSelfServiceKiosk\
   ```

2. Type the following, and press Enter:

   ```
   MyIDKiosk.exe
   ```

   To run the Kiosk in Derived Credentials mode, use the following command line:

   ```
   MyIDKiosk.exe /dc
   ```

2.5.2 Closing down the Kiosk

The Kiosk does not have an on-screen control to allow you to shut it down, as it is meant to run continuously. When an administrator needs to shut the Kiosk down, you can do so as follows:

- On the keyboard, press ALT+F4.

2.6 Translating the user interface

The Self-Service Kiosk supports translation of the on-screen text to change the terminology used or to change the language completely.

Contact Intercede customer support for details, quoting reference SUP-71.

2.7 Logging

You can set up your Self-Service Kiosk to write debug information to a log file. You may need to provide this information to Intercede customer support.

Contact customer support quoting reference SUP-236.

2.8 Job filtering

You may not want every client application to handle every job that is available for the cardholder. For example, you may want your Self-Service Kiosks to handle only activation jobs, and require your cardholders to use their Self-Service Apps to handle all other jobs on their own workstations. You can set up the web service to provide a customized list of jobs.

See the ***Web Service Architecture Installation and Configuration Guide*** for details of setting up job filtering; this document is provided with the software update that installs the web services.

2.9 Temporary credential profile

The Issue Temporary Card option in the Self-Service Kiosk issues a temporary card to the user. If you set the **Temporary Credential Profile Name** configuration option, the Kiosk issues a temporary card using the specified credential profile. If you do not set this option, the credential profile used for the original card is used.

See the ***Administration Guide*** for details of setting up a credential profile for temporary replacement cards.

To set the temporary credential profile:

1. From the **Configuration** category, select **Operation Settings**.
2. On the **General** tab, set the following option:
   - **Temporary Credential Profile Name** – set this to the name of a credential profile to be used for temporary cards.
3. Click **Save changes**.

The card profile must be available to all cardholders you want to be able to obtain temporary cards through the Self-Service Kiosk. If this profile requires validation, the Issue Temporary Card option in the Kiosk will allow the cardholder only to request a temporary card, not collect it; if the profile does not require validation, a cardholder can use the Issue Temporary Card option in the Kiosk to request and collect a temporary card.

3 Troubleshooting

- **Inserting an unknown card type causes the Kiosk to fail**

  If you insert an unknown card type, and the Kiosk appears to stop working, it is possible that an error window has opened behind the Kiosk window. See the *Error when unrecognized card is inserted* entry in section *4*, *Known Issues*.

- **You do not have sufficient privileges to perform this operation**

  When inserting either a known or unknown card, you may see an error similar to:

  ```
  You do not have sufficient privileges to perform this operation
  ```

  This is because you do not have access to the workflow. Make sure that the built-in user account `mobile` has access to the **Request Derived Credential** workflow.

- **Logon Failed/Logon Denied**

  When inserting either a known or unknown card, you may see an error similar to:

  ```
  Logon Failed
  Logon Denied
  ```

  This may be because the built-in user account `mobile` is disabled. Check in MyID that the user is enabled.

4 Known Issues

- **CrossMatch Verifier outer edges issue**

  A problem currently exists where the outer edges of the finger print reader do not detect the finger when placed on the scanner plate of a CrossMatch Verifier. A finger placed in the centre of the scanner plate is detected correctly.

- **CrossMatch Verifier first time operations**

  When you scan a fingerprint for the first time using a CrossMatch Verifier, the scan does not work: the capture area lights up but no fingerprint is received by the Self-Service Kiosk. However. if you restart the Self-Service Kiosk and rescan it operates correctly.

- **Cannot run the Self-Service Kiosk if MyID is open in a browser**

  You cannot run the Self-Service Kiosk if you have an Internet Explorer window open at the MyID webpage. This is because both the Self-Service Kiosk and the MyID web application conflict with each other over card transaction locking.

- **Cannot choose a card in the Self-Service Kiosk**

  If you have more than one card reader, the Self-Service Kiosk does not allow you to select which reader to use. If you have unissued smart cards in more than one reader, and are collecting a card issuance job, the Self-Service Kiosk will select one of the cards without any user intervention.

- **Self-Service Kiosk and Virtual Smart Cards**

  The Self-Service Kiosk does not currently support Virtual Smart Cards. If you want to use Virtual Smart Cards with the Kiosk, contact customer support for more information.

- **Compatibility with previous versions of the biometric components**

  There is no backwards compatibility with older version of the MyID biometric components (BioPack). A future release will provide backwards compatibility.

- **Timeout after installation**

  If you access the Kiosk after the web services have been installed on the server, you may experience a timeout that prevents the Kiosk from operating. This is caused by the processing required by the web services when they are first accessed.

  As a workaround, you can access the web service page using a web browser before attempting to use the Kiosk. Access the following web page:

  ```
  http://myserver/myidprocessdriver/processdriver.asmx
  ```

  where `myserver` is the name of the web services server.

- **Error entering multiple lines of text for replacement card reasons**

  When requesting a replacement card using the Self-Service Kiosk, you are prompted to enter a reason for the replacement. If you enter multiple lines of text, an error is displayed. As a workaround, enter a single line of text.

- **Truncated text at low screen resolutions in Self-Service Kiosk**

  If you run the Self-Service Kiosk at a screen resolution of 1024x768, some text may be truncated. As a workaround, run the Self-Service Kiosk at a resolution of 1280x1024 or 1920x1080.

- **Error when unrecognized card is inserted**

  If you insert an unrecognized card, the Self-Service Kiosk may present an error dialog *behind* the Kiosk window. On an unattended Kiosk, there may be no way to close the error dialog. As a workaround, you can set a value in the registry to prevent the error dialog appearing.

  On the Self-Service Kiosk PC, browse to the Card Drivers key.

  On a 64-bit system, this is:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Intercede\Edefice\Card
  Drivers\
  ```

  On a 32-bit system, this is:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\Card Drivers\
  ```

  If the `Card Drivers` key does not exist, create it.

  Create a DWORD value called `Silent`, and set the value to `1`.

- **Error when installing**

  You may see an error similar to the following when installing the Kiosk:

  ```
  Error 1301. The installer has insufficient privileges to access this
  directory:
  C:\Program Files (x86)\Intercede\MyIDSelfServiceKiosk.
  The installation cannot continue. Log on as an administrator or
  contact your system administrator.
  ```

  You do not need to have administrative privileges to install the Self-Service Kiosk. However, you must make sure that you have the correct permissions to install software to the folder you have selected; for example, your system administrator may not permit you to install software to the default folder. In this case, choose a different destination location during the installation process.

- **Problems collecting or updating cards**

  If you experience problems when collecting or updating cards, try increasing the **Certificate Refresh Threshold** option on the **Certificates** tab of the **Operation Settings** workflow to a higher value; for example, `45`.

  This problem may manifest with an error similar to:

  ```
  One of the certificates that have been requested for you has failed
  to issue. Please contact your administrator.
  ```

  Note that the certificate may have issued correctly even though the card update has failed.

- **Enter PIN twice for card update and certificate renewal jobs**

  If you have terms and conditions enabled for the credential profile, and the **Terms and Conditions During Device Update** configuration option is set to `Yes`, you are required to enter the PIN both before the terms and conditions are displayed and after accepting the terms and conditions.

- **Cannot process any jobs until a VSC job has been collected**

  If a user has more than one job to be collected, and one of them is a Virtual Smart Card (VSC) job, you must collect the VSC (for example, using the Self-Service App) before you can process any of the other jobs.