MyID

Client Components

Release Notes

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

Document reference: IMP1657-52

February 2018

Copyright

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

The MyID® Client Components are installed on each client machine, and allow your end users to use the MyID server. The client components also allow interaction between the MyID Windows clients and smart cards, Trusted Platform Modules, and peripherals such as document scanners and web cams.

The MyID Windows clients include:

- MyID Desktop
- MyID Self-Service App
- MyID Self-Service Kiosk
- MyID Administration Client (accessed through Internet Explorer for older versions of MyID)

1.1 Documentation

The following documents are provided with the MyID client components

- ***UMC-28.0.1000.1_readme.html***

  The readme file provided with the patch contains information on prerequisites and the procedure for installing the client components.

- ***Client Components Release Notes***

  This document.

  Contains information about the supported hardware and software for the current version of the client components along with any known issues in this release.

1.2 In this release

Release UMC-28.0.1000.1 contains the following changes:

- Support for SafeNet Authentication Client version 10.4.
- Support for Gemalto Prime PIV v2.1 Applet on TOP DL V2.1 platform.

  These cards require MyID 10.8 Update 2 or later.
- Support for IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1.

  These cards require MyID 10.8 Update 2 or later.
- Support for Giesecke & Devrient PIV SCE v7.0.

  These cards require MyID 10.8 Update 2 or later.

1.3 In previous releases

1.3.1 Release UMC-27.0.1000.1

Release UMC-27.0.1000.1 contained the following changes:

- Bug fixes.

1.3.2 Release UMC-26.0.1000.1

Release UMC-26.0.1000.1 contained the following changes:

- The ***Smart Card Integration Guide*** and the ***Printer Integration Guide*** have been removed. These documents are now provided with the main MyID release documentation as of MyID 10.8.
- Information previously included in this document on configuring Internet Explorer and on supported hardware and software has been moved into the ***Installation and Configuration Guide***.
- Generic Lock User PIN implemented for all devices managed through PKCS#11.
- Updated to support the detection of Intel Authenticate issued through MyID when the Intel Authenticate service is installed.

1.3.3 Release UMC-25.0.1000.1

Release UMC-25.0.1000.1 contained the following changes:

- Updated to support MyID 10.7 Update 1.
- Support for Yubico YubiKey 4 devices.
- Support for SafeNet Authentication Client v10.1.29.0.
- Support for eToken 5110 devices.

  See the ***Smart Card Integration Guide*** for details of new middleware and devices.

1.3.4 Release UMC-24.0.1000.1

Release UMC-24.0.1000.1 contained the following changes:

- Support for ECC certificates.

  MyID now supports the issuance of certificates based on elliptic curve cryptography (ECC) as well as RSA.

  You can issue ECC certificates to PIV cards (256 and 384-bit certificates are permitted by FIPS 201-2), and to smart cards that use a minidriver (256, 384, or 521-bit).

  See the ***Microsoft CA Integration Guide*** for details of configuring MyID to issue ECC certificates.
- Updated support for Windows 7 Virtual Smart Cards (VSCs).

  VSCs can now be supported by a minidriver on Windows 7. The additional support includes the ability to unblock a VSC remotely using a challenge/response algorithm.
- Added support for Intercede Intel Authenticate when used in conjunction with the MyID Intel Authenticate Mini-driver and Virtual Reader.
- Support for Gemalto Classic Client 6.3.8.
- Security enhancements for the enveloping component.
- Support for the Fargo HDP4500 printer.
- Using smart cards with native MyID Desktop workflows.

  Newer versions of MyID use updated workflows that use the native capabilities of MyID Desktop instead of embedded web pages. These workflows do not work with all smart cards.

  In MyID 10.7, the **Erase Card**, **Reset Card PIN**, **Print Card**, **Unlock Credentials** and **Cancel Credential** workflows do not work with older cards.

See the *Using smart cards with native MyID Desktop workflows* section in the ***Smart Card Integration Guide*** for details of unsupported cards.

1.3.5 Release UMC-23.0.1000.1

Release UMC-23.0.1000.1 contained the following changes:

- Support for H10302 format HID Prox Cards.
- Support for Fargo HDP 8500 printer.

  See the ***Printer Integration Guide*** for details.

1.3.6 Release UMC-22.0.1000.1

Release UMC-22.0.1000.1 contained the following changes:

- A more descriptive error is provided when scanning is not configured.
- Support for new PIN locking functionality for PIV cards.

1.3.7 Release UMC-21.0.1000.1

Release UMC-21.0.1000.1 contained the following changes:

- Support for Oberthur ID-One PIV v2.3.5 cards.

  Important: On any MyID system that is intended to issue ID-One PIV v2.3.5 cards, you must configure MyID with the required IIN value. See the *Serial numbers for Oberthur PIV cards* section of the ***Smart Card Integration Guide*** for details.
- Giesecke & Devrient Card issuance fix.
- Performance enhancement to Enveloping component.
- Improved error message when Scanner Driver Support is set to WIA on Windows 7 or later.
- Change to ignore intermittent ATR returned from Fargo printer.

1.3.8 Release UMC-20.0.1000.1

Release UMC-20.0.1000.1 contained the following changes:

- Windows 10 support for Virtual Smart Cards.
- SafeNet SAC9 support.
- Giesecke & Devrient SmartCafé Expert v6.0 support.
- TicTok cards support for activity time out in seconds.

  The credential profile contains a **PIN Inactivity Timer** setting in the **PIN Settings**. This value is in minutes. In previous versions of MyID, for TicTok cards, this setting was in seconds, and users were recommended to set up a separate credential profile for TicTok cards, and to set the **PIN Inactivity Timer** setting to the required number of minutes multiplied by 60. *This is no longer the case*. You must now specify a value in minutes. If you set up this workaround for a previous version, you must contact Intercede customer support, quoting reference SUP-203.

1.3.9 Release UMC-19.1.1000.1

Release UMC-19.1.1000.1 contained the following changes:

- Update to the ***Smart Card Integration Guide*** to remove Common Criteria cards and add information on the PIN Inactivity Timer setting for TicTok cards.
- Passwords for PFX files can support only ASCII characters.
- The DeviceProfile XML script is now defensive.
- VSC issuance fix.

1.3.10 Release UMC-19.0.1000.1

Release UMC-19.0.1000.1 contained the following changes:

- GlobalPlatform Keys can now be managed on Gemalto MD3810 and MD830 cards.
- Updates to ensure VSCs are removed from the client machine on cancellation.

1.3.11 Release UMC-18.0.1000.1

Release UMC-18.0.1000.1 contained the following changes:

- TicTok PKCS#11 improvements.
- Oberthur backwards compatibility of older serial numbers.
- Preserve GINA unblock flag on new installations.
- VSC issuance fix if no card readers have been present on client.

1.3.12 Release UMC-17.0.1000.1

Release UMC-17.0.1000.1 contained the following changes:

- Support for MyID version 10.3.
- Zebra printer extended support and bug fixes.

1.3.13 Release UMC-16.0.1000.1

Release UMC-16.0.1000.1 contained the following change:

- Updates to support enhanced Derived Credentials features.

  See the ***Derived Credentials Installation and Configuration Guide*** in the Mobile Identity Management release for details.

1.3.14 Release UMC-15.0.1000.3

Release UMC-15.0.1000.3 contained the following change:

- SafeNet SC650 V3 cards are supported with SafeNet High Assurance Client v2.12.013.

1.3.15 Release UMC-15.0.1000.2

Release UMC-15.0.1000.2 contained the following change:

- Addresses an issue where collecting a Virtual Smart Card or Device Identity using the Self-Service App caused an error.

1.3.16 Release UMC-15.0.1000.1

Release UMC-15.0.1000.1 contained the following changes:

- Support for deletion of certificates from TPM.
- Support for AT_SIGNATURE type certificates.
- Support for Gemalto minidriver 8.4.5.0.
- Support for Gemalto MD840 and MD3840 cards.
- Support for Save As dialog using the Microsoft Common Item Dialog for operating systems released after Windows XP.

1.3.17 Release UMC-10.1.1000.14

Release UMC-10.1.1000.14 contained the following changes:

- Support for envelope version 1.3.
- Clarified support for remote unlock for Safenet cards.

1.3.18 Release UMC-10.0.1000.13

Release UMC-10.0.1000.13 contained the following change:

- Addresses an issue where MyID was ignoring the GlobalPlatform Keys during card issuance for Oberthur ID-One cards with device type CSSI – Oberthur Technologies.

1.3.19 Release UMC-10.0.1000.12

Release UMC-10.0.1000.12 contained the following changes:

- Support for Safenet High Assurance Client v2.12.
- Support for Zebra ZXP-8 printer on Windows 7 (32-bit).

1.3.20 Release UMC-10.0.1000.10

Release UMC-10.0.1000.10 contained the following changes:

- Support for MyID version 10.0.
- Windows XP is now supported only on existing systems that already use XP.

1.3.21 Release UMC-10.0.1000.9

Release UMC-10.0.1000.9 contained the following changes:

- Minor bug fixes.

1.3.22 Release UMC-10.0.1000.8

Release UMC-10.0.1000.8 contained the following changes:

- Support for Windows 8.1.

1.3.23 Release UMC-10.0.1000.6

Release UMC-10.0.1000.6 contained the following changes:

- Support for Charismathics PIV applet.

  See the ***Device Integration Guide*** for details.

- Removal of support for Safran Morpho devices.

1.3.24 Release UMC-10.0.1000.5

Release UMC-10.0.1000.5 contained the following change:

- Support for the Datacard CD800 printer.

  See the ***Printer Integration Guide*** for details.

1.3.25 Release UMC-10.0.1000.3

Release UMC-10.0.1000.3 contained the following changes:

- Support added for TCOS minidriver-based devices.
- Support added for Safenet Authentication Client 8.2.

  Safenet Authentication Client 8.1 is now supported only for maintenance devices on existing systems.
- Support added for Gemalto MD830 devices.
- Support on PIV systems for the Gemalto MD3810 devices – support is as PKI cards only, not as PIV cards.

1.3.26 Release UMC-10.0.1000.2

Release UMC-10.0.1000.2 contained the following changes:

- Support for Zebra printers. See the ***Printer Integration Guide*** for details.
- Support added for Oberthur ID-One PIV (v2.3.4) devices.
- The following devices are no longer supported:
  - Giesecke & Devrient StarSign FIPS 201.
  - SafeNet SC400 PIV.

1.3.27 Release UMC-10.0.1000.1

Release UMC-10.0.1000.1 contained the following changes:

- Aladdin middleware is not supported on the same installation as SafeNet middleware. If you currently use Aladdin tokens and middleware with MyID, and want to use the Aladdin middleware instead of the SafeNet Authentication Client middleware, contact Intercede customer support for details, quoting reference SUP-5.
- Support added for Athena IDProtect cards with Athena IDProtect minidriver.

  Note: Cards using Athena IDProtect PKCS#11 middleware are not currently supported. Contact customer support for more information, quoting reference SUP-4.
- Support added for Gemalto MD3810 devices.
- Support added for Gemalto IDPrime PIV Card v2.0.

  Note: Due to changes in serial number recognition on the latest version of the Gemalto PIV card, older versions of the card may no longer be recognized. Use of the IDPrime PIV Card v2.0 card requires an update to the MyID server. Contact customer support for more information, quoting reference SUP-3.
- Protiva PIV TPC DM (v1.2) devices are no longer supported on new or existing installations of MyID.

- Support added for Oberthur Authentic Webpack v4.4.5

  This release addresses the known issues for Oberthur devices that were listed in the previous version (C000MG006).

  Support for Oberthur Authentic Webpack v4.4.2 is now maintenance-only.
- Support added for the following Oberthur tokens:
  - ID-One Cosmo v7.0.1-n Token Slim v2.0 (Authentic V3 Applet)
  - ID-One Cosmo v7.0.1-n Token Slim v2.1 (Authentic V3 Applet)
  - ID-One Cosmo v7.0.1-n Token Slim v2.0 (IAS-ECC Applet)
  - ID-One Cosmo v7.0.1-n Token Slim v2.1 (IAS-ECC Applet)
- Oberthur devices using Oberthur Authentic WebPack are no longer supported on Windows XP clients.
- Support added for Oberthur ID-One Cosmo v7.0.1 with IAS Standard applet devices, using the Oberthur IAS-ECC minidriver.
- Support added for SafeNet eToken 4100 devices.
- Support added for SafeNet SC650 devices.
- Support added for TicTok v1.1 devices.
- Support for Axalto devices is now maintenance-only.
- The Remote PIN Management utility for PIV cards is provided.

  See the ***PIV Integration Guide*** for details.

2 Client Component Versions

2.1 New client component version numbers

In previous versions of MyID, the version reported for the client components in Add/Remove Programs was the major MyID product release version. As the client components are now independent of the MyID product version, the version reported in Add/Remove Programs is now the version of the client components themselves; for example: `10.0.411.1`.

Previous versions of MyID also displayed the file version and product version on the Component Download Page if the client components were the wrong version. Now, only the product version of the client components is displayed.

2.2 Specifying minimum and preferred versions

Note: The client component version options are not supported for clients using MyID Desktop or the Self-Service Apps. For more information, contact customer support quoting reference SUP-219.

You can configure the requirements for versions of client components installed on users' machines. You can specify the minimum version required and the preferred version. You can also specify what happens when a user attempts to log on to MyID using a version of the client components that does not meet the minimum or preferred versions.

The client component version behavior is determined by values of configuration options. To set these configuration options, within MyID, from the **Configuration** category select **Security Settings**. The client component version behavior settings are on the **Logon** tab.

- **Minimum Supported Client Components Version** – Type the minimum version of the client components that you want to be able to access MyID. If a user attempts to log on to MyID using client components that are lower than this version, the **Minimum Supported Client Components Upgrade Action** configuration setting determines what the user can do.

  If this option is left blank, the minimum allowed version of the client components is the same as that of the client components available on the MyID server.

  If this option is set to 0, no version checking is carried out.

- **Minimum Supported Client Components Upgrade Action** – Select the action if the client components do not meet the specified minimum level:

  - **Prevent** – The user is denied access to MyID. Select this option where the end users do not have the appropriate permissions to install new client components.
  - **Force** – The user is informed that new components are available and will be automatically downloaded. This is the default value, and is equivalent to the previous functionality.
  - **Offer** – The user is asked if they want to update their components. If they do not update, the user is allowed to proceed to the logon page; however, certain operations may not perform correctly. If the user chooses to update, the components are automatically downloaded.
  - **Warn** – The user is asked if they want to proceed onto the logon page. Select this option when you do not want the user to download the components automatically but want the user to be able to continue using MyID.

- **Preferred Client Components Version** – Type the preferred version of the client components.

  If a user attempts to log on to MyID using client components that are equal to or higher than this version, the user can access MyID directly.

  If a user attempts to log on to MyID using client components that are less than this version, but equal to or higher than the **Minimum Supported Client Components Version** setting, the **Preferred Client Components Version Upgrade Action** setting determines what the user can do.

- **Preferred Client Components Version Upgrade Action** – Select the action if the client components are between the specified minimum version and the preferred version:

  - **Prevent** – The user cannot proceed to the MyID logon page. Select this option where the end users do not have the appropriate permissions to install new client components.
  - **Force** – The user is informed that new components are available and will be automatically downloaded. This is the default value.
  - **Offer** – The user is asked if they want to update their components. If they do not update, the user is allowed to proceed to the logon page; however, certain operations may not perform correctly. If the user chooses to update, the components are automatically downloaded.
  - **Warn** – The user is asked if they want to proceed onto the logon page. Select this option when you do not want the user to automatically download the components but want the user to be able to continue using MyID.

2.2.1 Four-part and one-part client version numbers

In the **Minimum Supported Client Components Version** and **Preferred Client Components Version** option, you can either specify the whole four-part version (for example, `10.0.411.1`) or a one-part version (for example `411`) – if you specify a single-part version, only the third part of the client version number is checked.

2.3 Client component settings example

If you want to prevent end users downloading the client components, and want only one version of the client components to be installed across all user workstations, set the following options:

- **Minimum Supported Client Components Version** – Set to `0` (this disables version checking) or to the version number of the current set of client components; you can find this version number by looking at the Add/Remove Programs utility in the Windows Control Panel.
- **Minimum Supported Client Components Upgrade Action** – Set to **Prevent**. If no client components are installed or if a version of client components with a version earlier than the current version being used (for example, `10.0.411.1`) a message is displayed informing the user that the client components are out of date but will not allow them to download the components.
- **Preferred Client Components Version** – Set to `0` to disable checking, as only one version of the client components is required.

Preferred Client Components Version Upgrade Action – This setting is ignored, as the **Preferred Client Components Version** is set to 0.

3 Known Issues

- **Image capture in 64-bit Internet Explorer**

  The image capture control is not available in the 64-bit version of Internet Explorer. When you attempt to launch the image capture control, a pop-up message appears saying image capture is not available.

  As a workaround, you can use the 32-bit version of Internet Explorer on the 64-bit version of Windows 7.

- **Automated Testing and Internet Explorer security settings**

  This version of the client components allows you to use MyID website using the default level of security for the Trusted sites or Local Intranet zones. However, the Automated Testing toolkit feature does not operate correctly with the default settings, and displays the following error:

  ```
  Automation server can't create object.
  ```

  See the ***Installation and Configuration Guide*** for details.

- **Exporting MI Reports to Excel and Internet Explorer security settings**

  This version of the client components allows you to use MyID website using the default level of security for the Trusted sites or Local Intranet zones. However, the feature that allows you to export MI Reports to Excel does not operate correctly with the default settings; the option to export to Excel does not appear on screen.

  See the ***Installation and Configuration Guide*** for details.

- **Aware PreFace and Internet Explorer security settings**

  This version of the client components allows you to use MyID website using the default level of security for the Trusted sites or Local Intranet zones. However, Aware PreFace does not operate correctly with the default settings.

  See the ***Installation and Configuration Guide*** for details.

- **Internet Explorer Error when using MI Reports**

  You may see an Internet Explorer error similar to the following when using MI Reports:

  ```
  This page is accesing information that is not under its control.
  This poses a security risk. Do you want to continue?
  ```

  Make sure that the **Web Service URL** configuration option on the **General** tab of the **Operation Settings** workflow is set to use the same protocol (http or https) as you are using to access MyID. See the *Management Information Reports* chapter of the ***Administration Guide*** for details.

- **Unable to issue PROX cards**

  If you cannot issue a PROX card because the card was not detected in MyID, you require an update to your MyID server. Contact Intercede customer support quoting reference SUP-10 to obtain the patch.

- **Epson Perfection V500 Photo lockup**

  If you experience problems with the Epson Perfection V500 Photo locking the browser, try reinstalling the Epson drivers.

- **Epson Perfection V500 Photo cropped image**

  When scanning with the Epson Perfection V500 Photo, part of the image may be cropped; this is a driver issue, and occurs whether scanning within MyID or using a different application.

- **No video camera was found error**

  Under some circumstance, you may see an error similar to:

  ```
  No video camera was found. Try checking your connection or your drivers.
  ```

  This may be caused by a conflict between a built-in webcam and an external webcam. As a workaround, use the Windows device manager to disable the internal webcam.

- **Upload button missing after scanning**

  There is an intermittent error that may occur after scanning a document, where the **Upload Image** button is disabled, with the result that you cannot upload the scanned image. Clearing the browser cache may fix the problem temporarily, but the issue may occur again.

  For a software update that addresses this issue, contact customer support, quoting reference SUP-51.

- **Installer window disappears**

  After you click the **Install** button on the installation program, the installer window disappears until the installation has completed. You can click the icon on the taskbar to display the installer window.

- **List of printers does not appear**

  If the list of printers does not appear when you are attempting to print from MyID, set the **Initialize and script ActiveX controls not marked as safe for scripting** option in Internet Options.