MyID Enterprise
Version 12.13.0

Release Notes

Copyright

Licenses and Trademarks

The Intercede® and MyID® word marks and the MyID® logo are registered trademarks of Intercede in the UK, US and other countries.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such. All other trademarks acknowledged.

Apache log4net

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

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:

  For example:
  - Copy the file *before* starting the installation.
  - Do *not* remove the files before you have backed them up.
- ***Bold and italic*** hyperlinks 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 product installation media.
- 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 changes made to MyID® in version 12.13.0 and earlier releases, including new and updated features, integration updates, and general improvements.

For an archive of release notes information from MyID 11.0 to 11.8, see the provided PDF file:

- ***Release Notes MyID 11 Enterprise***

2 Updates in MyID 12.13.0

This chapter provides details of the changes in MyID 12.13.0, including:

- New and updated features – new features in this version of MyID, and major improvements to existing features.

- Integration updates – updates to MyID's support for smart cards and other credentials, certificate authorities, printers, and HSMs.

- Improvements – minor updates to existing functionality.

Important: At MyID version 12.9, the version of .NET Core used was updated. This affects the MyID servers and all clients. See section *6.3.2*, *.NET Core 8.0* for details.

Important: Microsoft is making changes to DCOM security over the course of releases in 2021 to 2023 that may affect your system, depending on your configuration. See section *13.2.2*, *Microsoft Windows DCOM server security changes* for details.

2.1 New and updated features

This section contains information on the new and updated features in MyID 12.13.0.

2.1.1 End-User License Agreement acceptance

MyID CMS licenses now contain an End-User License Agreement (EULA). You can view the text of the EULA in a browser; you must review and accept the EULA before installing the license.

You can view the URL of the accepted EULA on the **License Details** screen of the **Licensing** workflow or on the **License** tab of the **System Status** report.

Note: If you are upgrading MyID from an earlier version, you must review and accept the EULA the next time you install a new or updated license. For further information on this change, contact Intercede quoting SUP-399.

For information on installing a license with an EULA, see the *Installing license details* section in the ***Administration Guide***.

2.1.2 Integration with MyID SecureVault

MyID SecureVault is a secure key archival module that allows you to store, generate, and recover private keys. MyID SecureVault integrates with MyID CMS to provide key storage and recovery, and also provides an API that allows you to integrate it with your own systems; you can use MyID SecureVault on the MyID CMS server, or as a standalone key archive.

MyID SecureVault is available as a separate product. See:

www.intercede.com/myid-product-suite/myid-secure-vault/

For more information on integrating MyID CMS and MyID SecureVault, see the *Integrating with MyID SecureVault* section in the ***Administration Guide***.

2.1.3   External identity providers for the MyID Client for Mac

You can configure MyID to set up an external OpenID Connect identity provider (for example, Microsoft Entra or Google) to provide authentication to the MyID Client for Mac.

You can then use the external identity provider to provide authentication to MyID when you collect a job or start the **Change Security Phrases** or **Reset My PIN** operations.

This feature was introduced in MyID 12.12 for the Self-Service App and has now been extended to support the MyID Client for Mac.

See the *Using external identity providers* section in the *MyID Authentication Guide* guide.

2.1.4   Importing certificates through the MyID Core API

You can use the MyID Core API to import certificates that were issued by a different system; this allows MyID to manage the certificates as if they had been issued by MyID. This feature is available only through the API, not through the MyID Operator Client.

This feature is designed to allow organizations to bring additional management control to certificates that are issued through other solutions; for example, end-entity certificates issued by automatic enrollment, SSL certificates, or certificates from legacy certificate authorities that have no other management capability.

Once you have imported a certificate, MyID CMS:

- Assigns the certificate to a user account for ownership tracking. You can view details on the **Certificates** tab of the View Person screen in the MyID Operator Client.

- Includes the certificate information in reports generated by the MyID Operator Client or the MyID Core API.

  See the *Viewing a certificate* section in the *MyID Operator Client* guide.

- Displays the certificate details recorded at import.

  See the *Viewing a certificate* section in the *MyID Operator Client* guide.

- Generates certificate renewal notifications for the imported certificate, allowing warning of expiry of the certificate. Where appropriate, you can issue new certificates through MyID from a connected certificate authority.

- When certificate private keys are imported, MyID provides secure storage and recovery of the certificate.

  You can also integrate this with the new MyID SecureVault key store.

- Enables revocation control of the certificate, if a connection to the certificate authority exists in MyID.

  See the *Revoking, suspending, and unsuspending certificates* section in the *MyID Operator Client* guide.

The API provides the following endpoints:

- `POST /api/Certificates/import`

  This endpoint allows you to import a certificate, and optionally create a person from the information contained in the certificate.

- `POST /api/People/{id}/certificateImport`

  This endpoint allows you to import a certificate for a specific person who already exists in the MyID database.

See the *Importing certificates* section in the *MyID Core API* guide.

2.1.5   MyID Client for Windows

MyID CMS now provides a Windows version of the MyID Client for Mac. The MyID Clients for Windows and Mac have substantially the same functionality to provide a unified experience for your users across different operating systems; for the differences, see the *Differences between the MyID Client for Windows and MyID Client for Mac* section in the **MyID Client for Windows** guide.

You can use the MyID Client for Windows as an alternative to the Self-Service App for self-service actions and tasks on Windows PCs. The MyID Client for Windows will replace the Self-Service App as the primary user interface for self service operations; however, the Self-Service App will continue to be provided until replacement of all capabilities has been achieved and to allow customers time to plan deployment. For details of the current differences in supported functionality, see the *Differences between the MyID Client for Windows and the Self-Service App* section in the **MyID Client for Windows** guide.

For more information on installing and using the MyID Client for Windows, see the **MyID Client for Windows** guide.

2.1.6   MyID Client StatusBar Service

If you are a MyID Client for Mac user, you can use the MyID Client StatusBar Service to display notifications on the menu bar when new tasks are available; for example, when you have a certificate renewal task.

You can opt to install the MyID Client StatusBar Service during the installation process for the MyID Client for Mac. Once installed, the service starts automatically whenever you log on to your Mac and runs in the background to check periodically for new tasks on the MyID server.

You can then launch the MyID Client for Mac from a MyID Client StatusBar Service notification.

For more information, see the *Launching the MyID Client for Mac from the MyID Client StatusBar Service* section of the **MyID Client for Mac** guide.

2.1.7 Requesting key recovery through the MyID Core API

You can now use the MyID Core API to request a smart card or soft certificate package containing recovered certificates and keys.

MyID provides processes to recover certificates with archived/escrowed private keys securely to allow continued access to information that has been encrypted with the certificate. As part of the ongoing modernization of MyID, additional capabilities have been added to provide better management of these processes. New API endpoints have been added to allow you to create requests for key recovery, and the collection process has been updated to allow recovery as software certificates, as an update to an existing issued smart card, or as a new smart card issuance. A future MyID release will extend these capabilities further, to include new user interfaces to create and manage requests and additional secret key recovery management processes.

The API now provides the following endpoints:

- POST api/people/{id}/requests

  This endpoint allows you to request a key recovery smart card or soft certificate package for a person.

- POST api/devices/{id}/certificateRecovery

  This endpoint allows you to create an update for an existing issued device; this update contains recovered keys.

See the *Requesting key recovery* section in the **MyID Core API** guide.

These new features are an *addition* to existing MyID capabilities. You can continue to operate the key recovery processes that existed in previous releases of MyID. Note, however, that these features will be deprecated once the modernization of the functionality has been completed.

The **Credential Profiles** workflow has been enhanced to allow you to specify soft certificate key recovery locations. See the *Setting up the credential profile for key recovery* section in the **Administration Guide** for details.

If you issue dedicated key recovery cards in your current MyID installation, you may notice that the **Key Recovery Only** setting in the **Credential Profiles** workflow has moved from the **Issuance Settings** section to a new dedicated **Key Recovery** section. The existing key recovery features are not affected by this change and there is no need to modify your credential profile settings.

2.2 Integration updates

This section contains details of updates to MyID 12.13.0's support for integration with smart cards and other credentials, certificate authorities, printers, and HSMs.

There are no integration updates in this release.

2.3 Improvements

This section provides details of minor improvements to existing functionality within MyID 12.13.0.

2.3.1 General bug fixes and improvements

This release contains general bug fixes and minor improvements as part of a program of continuous improvement.

2.3.2 Customization files for the Self-Service Request Portal

The `myid.json` file that you use to customize the Self-Service Request Portal for external identity providers is overwritten by the MyID server update or upgrade process. To prevent having to re-apply your changes, you can now make your customizations in an override file named `myid.production.json` in the same folder as the `myid.json` file; this file is not overwritten by the update or upgrade process.

For more information, see the *Configuring the Self-Service Request Portal for external identity providers* section in the **Derived Credentials Self-Service Request Portal** guide.

2.3.3 Excluding characters from server-generated PINs

When you are using server generated PINs, you may want to exclude some characters from the generated PINs; for example, if you are generating alphanumeric PINs, you may want to exclude the numbers `0` and `1`, and the letters `O`, `o`, `I`, and `l` (capital O, lower-case O, capital I, lower-case L).

In the **PIN Settings** section of the credential profile, you can now set the **Exclude these characters** option to specify which characters you want to exclude from the generated PINs.

For details, see the *Excluding characters from the generated PINs* section in the **Administration Guide**.

2.3.4 Selective device update

MyID now allows you to request selective updates to be applied to devices with a PIV applet; for example, you can update the biometric data on a PIV smart card without affecting other certificates or data objects on the card. This powerful feature is configurable, but its capabilities may vary depending on the devices in use, the data to be amended, and other configuration of your MyID installation. The feature may also affect the PIV compliance of cards that are managed by MyID. For this reason, use of the feature is not available by default; for further details on use and configuration, contact Intercede quoting SUP-398.

2.4 End of support features in MyID 12.13.0

This section contains information about features that are no longer supported in MyID as of MyID 12.13.0.

There are no end of support features in this release.

2.5 Documentation updates in MyID 12.13.0

This section contains information on new and updated documentation in MyID 12.13.0.

2.5.1   Administration Guide

The ***Administration Guide*** has been updated with the following:

- Added information about the following new configuration option:

  - **Allow Certificate User Creation**

  See the *Certificates page (Operation Settings)* section.

- Added information on End-User License Agreements.

  See the *Installing license details* and *View current license status* sections.

- Updated the format for the **Auto launch workflow in self service operations** configuration option.

  See the *Setting the number of security phrases required to authenticate* and *Issuance Processes page (Operation Settings)* sections.

- Correction: removed `UserAccountID` from the list of banned words for PINs.

  See the *Enforcing banned words in PINs* section.

- Added information about excluding characters from server generated PINs.

  See the *Excluding characters from the generated PINs* section.

- Updated information on the **Show Generated PINs** configuration option.

  See the *PINs page (Security Settings)* section.

2.5.2   Configuring Logging

The ***Configuring Logging*** guide has been updated with the following:

- Added `rest.provision` to the list of web services for which you can configure logging.

  See the *MyID REST and authentication web services* section.

2.5.3   Derived Credentials Self-Service Request Portal

The ***Derived Credentials Self-Service Request Portal*** guide has been updated with the following:

- Added information about using the `myid.production.json` override file to prevent changes being lost at upgrade.

  See the *Customizing the properties file*, *Configuring your external identity provider*, *Configuring the Self-Service Request Portal for external identity providers*, *Sample configuration for Entra*, and *Error code reference* sections.

2.5.4   Entrust JASTK CA Integration Guide

The ***Entrust JASTK CA Integration Guide*** has been updated with the following:

- The Entrust Authority Security Toolkit for the Java Platform (ETJava) version 9 does not support ECC keys for escrow.

  See the *Introduction* and *Troubleshooting error messages* sections.

2.5.5 Error Code Reference

The ***Error Code Reference*** guide has been updated with the following:

- Added the following error messages relating to importing certificates:
  - WS40075 – Only one of x509 or pkcs12 must be set.
  - WS40076 – If using pkcs12 then password must be set
  - WS40077 – There was an error importing the certificate.
  - WS40078 – User creation not allowed.
  - WS40079 – PKCS12 password is invalid.
  - WS40080 – Provide a valid base64 pfx certificate.
  - WS40081 – Provide a valid certificate.
  - WS40082 – Select a valid certPolicyID.
  - WS40083 – User is not in the MyID Database.
  - WS40084 – Cannot find unique user to assign.
  - WS40085 – Certificate already exists.
  - WS50066 – This device already has an active request.

  See the *MyID Operator Client error codes* section.

- Added another possible cause for the following error:
  - REST007 – Unrecoverable error has occurred

  See the *MyID Identity Agent error codes* section.

- Added the following errors:
  - 881116 – Failed to sign the terms and conditions.
  - 890598 – A problem has been reported by Windows (<error>). Check the Microsoft documentation for further details.
  - 890705 – This request must be collected by the user account named in the request.

  See the *Web Service error codes* section.

- Updated the following error:
  - 85125 – The private key for a server signing certificate is not available. Please consult the product documentation.

  See the *Web Service error codes* section.

2.5.6 Configuring Logging

The ***Configuring Logging*** guide has been updated with the following:

- Added `rest.provision` to the list of web services for which you can configure logging.

  See the *MyID REST and authentication web services* section.

2.5.7　Installation and Configuration Guide

The ***Installation and Configuration Guide*** guide has been updated with the following:

- Updated screenshot to include the HSM button.

  See the *Selecting the servers* section.

2.5.8　MyID Authentication Guide

The ***MyID Authentication Guide*** has been updated with the following:

- Updated information about configuring Microsoft Entra.

  See the *Configuring Microsoft Entra* section.

- Added information about using external identity providers with the MyID self-service applications.

  See the *Using external identity providers for the self-service applications* section.

2.5.9　MyID Client for Mac

The ***MyID Client for Mac*** guide has been updated with the following:

- Added details of using an external identity provider.

  See the *Changing your security phrases*, *Resetting your PIN*, *Collecting a device*, and *Collecting a replacement device* sections.

- Added information about the MyID Client StatusBar Service.

  See the *Installing and uninstalling the MyID Client for Mac* and *Launching the MyID Client for Mac from the MyID Client StatusBar Service* sections.

2.5.10　MyID Client for Windows

The ***MyID Client for Windows*** guide is new for this release.

2.5.11　MyID Core API

The ***MyID Core API*** guide has been updated with the following:

- Added a new chapter on using the API to import certificates.

  See the *Importing certificates* section.

2.5.12　MyID Operator Client

The ***MyID Operator Client*** guide has been updated with the following:

- Added details for requesting information about creating custom reports.

  See the *Working with reports* section.

2.5.13　Operator's Guide

The ***Operator's Guide*** has been updated with the following:

- Reference to the reports available in the MyID Operator Client.

  See the *Working with reports* and *Running MI reports* sections.

2.5.14 Self-Service App

The **Self-Service App** has been updated with the following:

- Moved configuration information about external identity providers to the **MyID Authentication Guide**.

  See the *Using an external identity provider* section.

2.5.15 REST Web Service Notifications

The **REST Web Service Notifications** guide has been updated with the following:

- Added information on how to ensure that mapping file changes are picked up.

  See the *Creating a mapping file* section.

2.5.16 Smart Card Integration Guide

The **Smart Card Integration Guide** has been updated with the following:

- Added clarification on which card formats are recommended for YubiKey devices.

  See the *Card format* section.

2.5.17 System Interrogation Utility

The **System Interrogation Utility** guide has been updated with the following:

- Removed mentions of Microsoft SQL Server 2016.

  See the *Description of derived tests* section.

2.6 Known issues resolved in MyID 12.13.0

This section lists the known issues that have been resolved in MyID 12.13.0. These are issues that were found across both editions of MyID – Enterprise and PIV – and may not all be relevant for your system.

- IKB-394 – Requirement to set security questions not enforced from the MyID Operator Client in self service operations when Integrated Windows Logon is used.

3 Updates in MyID 12.12.0

This chapter provides details of the changes in MyID 12.12.0, including:

- New and updated features – new features in this version of MyID, and major improvements to existing features.

- Integration updates – updates to MyID's support for smart cards and other credentials, certificate authorities, printers, and HSMs.

- Improvements – minor updates to existing functionality.

Important: At MyID version 12.9, the version of .NET Core used was updated. This affects the MyID servers and all clients. See section *6.3.2, .NET Core 8.0* for details.

Important: Microsoft is making changes to DCOM security over the course of releases in 2021 to 2023 that may affect your system, depending on your configuration. See section *13.2.2, Microsoft Windows DCOM server security changes* for details.

3.1 New and updated features

This section contains information on the new and updated features in MyID 12.12.0.

3.1.1 External identity providers for the Self-Service App

You can configure MyID to set up an external OpenID Connect identity provider (for example, Microsoft Entra or Google) to provide authentication to the MyID Self-Service App.

You can then use the external identity provider to provide authentication to MyID when you collect a job or start the **Change Security Phrases** or **Reset My PIN** operations.

See the *Using external identity providers* section in the *MyID Authentication Guide* guide.

3.1.2 Physical printed cards

If you have cards that have no chips (contact or contactless) but comprise only a printable surface or a magnetic stripe, you can create a credential profile that allows you to print, issue, and manage these cards.

This is an enhancement of the **Magnetic Stripe (Only)** credential profile option that was previously available in MyID. The **Magnetic Stripe (Only)** option in the **Card Encoding** section of the **Credential Profiles** workflow has now been renamed **Physical Printed Card**, and cards issued using this option are now assigned a serial number and added to the MyID database. This means that you can manage these cards; for example, you can request, validate, print, replace, renew, enable, disable, or cancel these devices.

In addition, the card issuance is audited (which you can view, for example, in the **Device History** tab of the View Device screen) and you can view the preview images of the front and back card layouts on the **Audit Details** tab of the View Audit screen.

When you make lifecycle changes to the cards (for example, disabling or canceling the cards) the system makes the changes in the MyID database, adds the operation to the audit trail, and reports the changes to any connected external systems through notifications. This also means you can use the MyID Core API to check the status of a card by providing its serial number to query the MyID database.

Physical printed cards are issued with a **Device Type** of **Physical** that you can use to search for them using reports. Physical printed cards are also counted separately in the **Issued devices by Category** report.

See the *Setting up a credential profile for physical printed cards* section in the ***Administration Guide*** for more information.

3.1.3 Requesting and collecting mobile derived credentials

You can now use the Self-Service Request Portal on a mobile (iOS or Android) device, if you have a mobile card reader. You visit the SSRP website on the mobile device, use the attached mobile card reader to present your existing credential, and the SSRP displays a link that allows you to collect the derived credential directly on the mobile device. To configure this feature, you must set up the credential profile to specify which app you want to use to collect the derived credential.

Previously, the SSRP always displayed a QR code to allow you to collect mobile credentials. Now, the SSRP displays a QR code if you are using the SSRP from a non-mobile device, or if you are using the SSRP from a mobile device but do not have an app collection link configured. You can also configure your credential profile to make the SSRP display a QR code in addition to an app collection link.

For information, see the *Using the SSRP on a mobile device* and *Setting up the credential profiles for derived credentials* sections in the ***Derived Credentials Self-Service Request Portal***.

3.1.4　Automating the MyID Installation Assistant

You can now automate the MyID Installation Assistant so that it can run without user interaction. For example, you can:

- Set up additional MyID servers to join to an existing load-balanced deployment.
- Deploy a server configuration to a new environment; for example, when transitioning from development or pre-production to production servers.

To automate the MyID Installation Assistant, go through the MyID Installation Assistant screens to provide all of the information needed for your installation, then, at the end, instead of starting the installation process, export your settings to a registry file that you can subsequently use to run the installation without user interaction on the current server, or on any other server.

For more information, see the *Automating an installation* section in the ***Installation and Configuration Guide***.

As part of this feature, there is also an updated version of the GenMaster utility that is now fully integrated within the MyID Installation Assistant.

See the *Using GenMaster* section in the ***Installation and Configuration Guide***.

3.2　Integration updates

This section contains details of updates to MyID 12.12.0's support for integration with smart cards and other credentials, certificate authorities, printers, and HSMs.

3.2.1　Amazon Web Services

You can now install MyID onto servers hosted on Amazon Web Services (AWS) EC2 virtual machines and use an Amazon RDS for SQL Server database instance.

See the ***Amazon Web Services Integration Guide*** for details.

3.2.2　BlackBerry UEM

MyID now supports BlackBerry Unified Endpoint Manager (UEM) for MDM validation when you are issuing mobile devices. MyID can check that the mobile device is valid for issuance by querying the BlackBerry UEM server.

For more information, see the *Setting up an external system for BlackBerry UEM* section in the ***Mobile Identity Management*** guide.

3.2.3　YubiKey FIPS devices

The support for YubiKey FIPS devices with firmware version 5.7 or later has been amended in line with changes enforced by the latest device firmware. When issuing YubiKey v57 FIPS devices, the token does not create credentials unless the PIN, PUK, and 9B key have been changed. Therefore you must set the set the **Security Officer PIN Type** option to **Random** and configure customer 9B keys.

Additionally, the YubiKey v57 FIPS devices have a minimum user PIN length of eight digits and block commonly used PIN values as an additional security feature.

See the *Issuing YubiKey v57 FIPS devices*, *PIN length*, and *PIN policy considerations for YubiKey v57 FIPS devices* sections in the ***Smart Card Integration Guide***.

3.2.4 Entrust JASTK CA integration

MyID now supports integration with Entrust CA using the Entrust Authority Security Administration Toolkit for Java (JASTK).

This support for JASTK supersedes MyID's integration with Entrust using the Entrust Administration Toolkit for C, as documented in the ***Entrust CA Integration Guide***. For assistance with migrating from the Entrust Administration Toolkit for C to the Entrust Authority Security Administration Toolkit for the Java Platform (JASTK), contact Intercede customer support quoting reference SUP-389.

For information about the differences between MyID's integration with Entrust through JASTK as opposed to through the Entrust Administration Toolkit for C, see the *Differences with JASTK* section of the ***Entrust JASTK CA Integration Guide***.

3.2.5 SQL Server versions

MyID has now been tested with the following SQL Server versions:

- SQL Server 2022 – CU13 (16.0.4125.3 – May 2024)
- SQL Server 2019 – CU27 (15.0.4375.4 – June 2024)
- SQL Server 2017 – CU31 (14.0.3456.2 – September 2022)

See the *Database versions* section of the ***Installation and Configuration Guide*** for details.

3.3 Improvements

This section provides details of minor improvements to existing functionality within MyID 12.12.0.

3.3.1 General bug fixes and improvements

This release contains general bug fixes and minor improvements as part of a program of continuous improvement.

3.3.2 Certificate housekeeping

MyID now provides a stored procedure that allows your database administrator to clean up certificates in the MyID database that are no longer required; for example, you may no longer want to retain the records of failed or revoked certificates. MyID also now provides a database trigger that cleans up PKCS #10 requests from the database once the certificate has been issued.

For more information about the `sp_CertificateCleanup` stored procedure and the `tu_TidyPKCS10Request` trigger, see the *Certificate housekeeping* section in the ***Administration Guide***.

3.3.3 TLS 1.3

TLS 1.3 is the latest version of the TLS protocol. TLS, which is used by https and other network protocols for encryption, is the modern version of SSL.

MyID CMS has been tested in environments where older TLS protocols are disabled, and therefore TLS 1.3 is in use. The majority of MyID functionality continues to operate as expected; however, you must consider the impact on the broader infrastructure used with MyID.

For more information, see the *Securing MyID with TLS 1.2 and TLS 1.3* section in the *System Security Checklist*.

3.3.4 Extended support for RSA 3072 and 4096 bit keys

At version 12.11, MyID introduced support for RSA 3072 and 4096 bit keys on selected devices and with selected CAs.

This support has now been extended to more CAs; you can now use the following:

* Microsoft CA.

* PrimeKey EJBCA.

* Entrust JASTK.

* Entrust CA Gateway.

* DigiCert ONE.

Additionally, MyID now uses SHA-384 as a hashing algorithm when issuing devices with RSA 3072 and 4096 bit keys:

* When requesting certificates with RSA 3072 or 4096 bit keys for smart cards or soft certificates, MyID uses SHA-384 in the hashing of the PKCS#10.

* When signing or logging onto MyID with a certificate, for RSA 3072 or 4096 bit keys, MyID uses SHA-384 for hashing rather than SHA256.

    Note: Because RSA 3072 and 4096 bit keys were introduced in MyID 12.11, but SHA-384 for those keys was introduced in MyID 12.12, you cannot use the version of MyID Desktop issued with MyID 12.12 or later to log on to a MyID 12.11 server with devices issued with RSA 3072 or 4096 bit keys; you must upgrade your server *before* you upgrade your client software.

SHA-384 is part of the SHA-2 family of hashing algorithms, like the already-supported SHA-256 algorithm.

See the *Smart Card Integration Guide* for full details of which devices support RSA 3072 and 4096 bit keys.

You can now use the MyID Client for Mac to collect devices with RSA 3072 or 4096 bit keys; however, SHA-384 is not yet supported.

Important: You must ensure that your CA is configured to allow SHA-256 hashing in the certificate policy to allow you to issue certificates to devices that do not support SHA-384.

Note: If you want to use RSA 3072 and 4096 bit keys for Windows logon, you must ensure that the combination of devices and drivers you are using supports these keys for Windows logon. Check with your device vendor whether specific drivers are required.

* **IKB-410 – Support for RSA 3072 and 4096 bit keys for mobile devices requires further updates.**

    MyID issues certificates to mobiles using RSA keys with a key length of 2048 bits. Support for certificate issuance using RSA keys with lengths of 3072 or 4096 bits requires additional updates to mobile apps that integrate with MyID CMS; for example, integrations with mobile device management systems where the MDM app is used to integrate with MyID.

    Contact Intercede for further information on support for RSA keys with lengths of 3072 or 4096 bits on mobile devices, quoting reference IKB-410.

3.3.5   Custom configuration files for web.oauth2

When configuring your web.oauth2 web service to add custom clients, scopes, API resources, and identity resources to allow you to work with the MyID Core API, you can edit arrays in the `appsettings.Production.json` file for the web.oauth2 web service. Because elements in this array are determined by their index, you must pad the array to the correct size to correspond to the entries in the `appsettings.json` file and prevent accidentally overwriting other clients.

In MyID 12.11, a feature was introduced that allowed you to use separate configuration files for your custom clients to simplify this process, and to allow for greater maintainability. This feature has now been extended to include separate files for scopes, API resources, and identity resources.

See the *Custom configuration files* section in the *__MyID Core API__* guide.

3.3.6   Alphabetical list of endpoints in the MyID Core API documentation

The API endpoints in the Swagger documentation for the MyID Core API are now ordered alphabetically within each category by default. Previously the endpoints were unordered. You can revert to the previous ordering by changing the `OrderAlphabetically` setting in the MyID Core API `appsettings.Production.json` file to `false`.

See the *Accessing the API documentation* section in the *__MyID Core API__* guide.

3.4   End of support features in MyID 12.12.0

This section contains information about features that are no longer supported in MyID as of MyID 12.12.0.

There are no end of support features in this release.

3.5 Documentation updates in MyID 12.12.0

This section contains information on new and updated documentation in MyID 12.12.0.

3.5.1 Administration Guide

The *Administration Guide* has been updated with the following:

- Added information about the following new configuration option:
    - **Use SHA1 encryption for certificates issued as PFX files**

    See the *Server page (Security Settings)* section.

- Added a note on User SIDs and MyID Desktop.

    See the *Limitations* section.

- Added information on collecting derived credentials directly on a mobile device.

    See the *Collection Instructions* section.

- Added information on creating a credential profile for physical printed cards.

    See the *Setting up a credential profile for physical printed cards* section.

- Added information about using external identity providers with the Self-Service App.

    See the *Logon Priority page (Security Settings)* and *Self-Service Unlock Authentication* sections.

3.5.2 Advanced Configuration Guide

The *Advanced Configuration Guide* has been updated with the following:

- Added information on how to use an Entrust nShield HSM with multiple MyID application servers.

    See the *Multiple application servers* section.

3.5.3 Amazon Web Services Integration Guide

The *Amazon Web Services Integration Guide* is new for this release.

3.5.4 Derived Credentials Self-Service Request Portal

The *Derived Credentials Self-Service Request Portal* has been updated with the following:

- Added information on collecting derived credentials directly on a mobile device.

    See the *SSRP overview*, *Setting up the credential profiles for derived credentials*, and *Troubleshooting mobile device collection* sections.

- Added information about configuring the SSRP for TLS 1.3.

    See the *Using TLS 1.3* section.

- Added information about backing up SSRP customizations before an upgrade.

    See the *Customizing the Self-Service Request Portal* and *External identity providers* sections.

3.5.5 Entrust JASTK CA Integration Guide

The *Entrust JASTK CA Integration Guide* is new for this release.

3.5.6 Entrust nShield HSM Integration Guide

The *Entrust nShield HSM Integration Guide* has been updated with the following:

- Added information on how to use an Entrust nShield HSM with multiple MyID application servers.

  See the *Configure remote file system / client connectivity* section.

3.5.7 Error Code Reference

The *Error Code Reference* has been updated with the following:

- Added the following error relating to importing certificates:
  - WS40086 – There is no valid group to assign to the imported user.

  See the *MyID Operator Client error codes* section.

- Added the following errors relating to issuing devices:
  - 9008112 – Reset PIN is not available for this device.
  - 9008115 – Card cannot be updated as content signer will expire during card lifetime.
  - 9008118 – Enrollment data has not been validated within the last 24 hours.
  - 9008120 – Cannot be a known Dual-Interface Card.

  See the *Web Service error codes* section.

3.5.8 Installation and Configuration Guide

The *Installation and Configuration Guide* has been updated with the following:

- Added information on the new version of GenMaster.

  See the *Using GenMaster*, *Configuring the master keys*, and *Configuring the startup user account* sections.

- Added information on automating the MyID Installation Assistant.

  See the *Automating an installation* section.

- Added information about backing up SSRP customizations before an upgrade.

  See the *Upgrading systems with customized Self-Service Request Portal features* section.

- Updated the list of supported SQL Server versions.

  See the *Database versions* section.

3.5.9 Microsoft Windows CA Integration Guide

The *Microsoft Windows CA Integration Guide* has been updated with the following:

- Added information on setting up certificates on a remote CA.

  See the *Setting up certificates* section.

- Added information on configuring firewalls.

  See the *Firewall configuration* section.

3.5.10 Mobile Authentication

The *Mobile Authentication* guide is now deprecated.

3.5.11   Mobile Identity Management

The *Mobile Identity Management* guide has been updated with the following:

- Updated throughout for the deprecation of the Identity Agent app.

3.5.12   MyID Core API

The *MyID Core API* guide has been updated with the following:

- Added information on creating custom configuration files for the web.oauth2 service.

  See the *Custom configuration files* section.

- Added information on the new configuration option for the documentation that shows the API endpoints alphabetically.

  See the *Accessing the API documentation* section.

3.5.13   MyID Operator Client

The *MyID Operator Client* guide has been updated with the following:

- Added information on troubleshooting the server name not resolving.

  See the *Server name does not resolve* section.

- Added information about logging on using an external identity provider.

  See the *Signing in using an external identity provider* section.

- Updated the list of MyID Client Service features.

  See the *MyID Operator Client error messages* section.

3.5.14   Printer Integration Guide

The *Printer Integration Guide* has been updated with the following:

- Added information about support for contactless card readers.

  See the *Support for contactless card readers* section.

3.5.15   Self-Service App

The *Self-Service App* has been updated with the following:

- Added information about using external identity providers.

  See the *Using an external identity provider* section.

3.5.16   Smart Card Integration Guide

The *Smart Card Integration Guide* has been updated with the following:

- Added additional information about YubiKey v5.7 FIPS devices.

  See the *Issuing YubiKey v57 FIPS devices*, *PIN policy considerations for YubiKey v57 FIPS devices*, and *Interoperability for Yubico smart cards* sections.

- Added information about using RSA 3072 and 4096 bit keys for Windows logon.

  See the *Issuing YubiKey v57 FIPS devices* section.

- Added information about recommended settings for the Per Container PIN Policy for the Card Authentication Certificate container (`5FC101`) for YubiKey devices.

  See the *PIN policy settings* section.

3.5.17 System Security Checklist

The **System Security Checklist** has been updated with the following:

- Added information about MyID's support for TLS 1.3.

  See the *Securing MyID with TLS 1.2 and TLS 1.3* and *Database communications* section.

3.6 Known issues resolved in MyID 12.12.0

This section lists the known issues that have been resolved in MyID 12.12.0. These are issues that were found across both editions of MyID – Enterprise and PIV – and may not all be relevant for your system.

- IKB-216 – Magnetic stripe only card issuance not supported in Collect Card or Batch Collect Card.

- IKB-392 – Software certificates fail to import on older Windows versions or Apple Devices.

- IKB-402 –YubiKey-specific data model settings may prevent PIN reset in the Self-Service App.

4 Updates in MyID 12.11.0

This chapter provides details of the changes in MyID 12.11.0, including:

- New and updated features – new features in this version of MyID, and major improvements to existing features.

- Integration updates – updates to MyID's support for smart cards and other credentials, certificate authorities, printers, and HSMs.

- Improvements – minor updates to existing functionality.

Important: At MyID version 12.9, the version of .NET Core used was updated. This affects the MyID servers and all clients. See section *6.3.2*, *.NET Core 8.0* for details.

Important: Microsoft is making changes to DCOM security over the course of releases in 2021 to 2023 that may affect your system, depending on your configuration. See section *13.2.2*, *Microsoft Windows DCOM server security changes* for details.

4.1 New and updated features

This section contains information on the new and updated features in MyID 12.11.0.

4.1.1 MyID Client for Mac

MyID CMS now provides a client for macOS computers that allows you to carry out a wide range of self-service operations.

Using the MyID Client for Mac, you can:

- Change the PIN of your device.

- Change your security phrases.

- Reset your PIN.

- Update your device.

- Collect a device.

- Activate a device.

- Collect an update for your device.

- Collect a replacement device.

- Collect a certificate renewal.

The current release supports a selection of YubiKey and IDEMIA devices on Apple Mac computers with ARM-based M series Apple silicon running the one of the following operating system versions:

- Monterey – version 12.7.1 (21G920)

- Ventura – version 13.4

- Sonoma – version 14 to 14.2.1 (23C71)

For more information, see the *MyID Client for Mac* guide.

4.1.2 Printed identity documents

MyID now allows you to create and manage printed identity documents. These documents are printed onto paper or card, rather than onto smart cards. You can include user photographs, organization logos, text information from the person's user account in MyID, and barcodes in your printed identity document.

Once you have printed the identity documents, you can manage them through MyID. You can renew or replace printed identity documents, and enable, disable or cancel them.

As printed identity documents are physical pieces of paper, there are no credentials stored on them to be physically enabled, disabled, or canceled. However, you can still change their status within MyID so that they appear as enabled, disabled, or canceled if an operator checks the device record, either through the MyID Operator Client or using the MyID Core API. For example, you could print a barcode with the device serial number on the identity document, then use the MyID Core API to create a simple application that takes the output from a barcode scanner and checks the device serial number against the MyID database to return the status of the identity document.

Request events (when a request for a printed identity document is added or updated) and lifecycle events (when a printed identity document is issued, canceled, enabled or disabled) generate the same notifications as lifecycle events for smart cards, and you can use these notifications to integrate with your systems.

For more information about printed identity documents, see the ***Printed Identity Documents*** guide.

4.1.3 Restricting inactive users

You can now restrict the access to administrative MyID features for users who have not logged in for a set amount of time. When a user is restricted, they are allowed only those features provided by the **Cardholder** role, and all other roles that they have are restricted. This affects their access to all MyID applications: MyID Desktop, the Self-Service App, and so on; it also affects access to the MyID Core API.

See the *Restricting inactive users* section in the ***Administration Guide*** for more information.

4.1.4 Reassigning devices

You can use the MyID Core API to reassign devices from one person to another. This feature is available only through the API, not through the MyID Operator Client.

The API provides the following endpoint:

- `POST /api/Devices/{id}/reassign`

The device must:

- be fully issued and active.
- be issued with a credential profile that has **Contact** as the **Card Encoding**.
- not contain additional identity certificates.
- not be issued with a credential profile that has the **Key Recovery Only** option set.
- not already be issued to the target person.

If the request is successful, MyID:

- Returns a block of JSON containing details about the device, including its new owner.
- Transfers the ownership of the device, and its certificates, in the MyID database to the new owner.

  Note: The physical device is unaffected by this change. Only the MyID database is updated.

- Cancels any existing requests for the device.
- Triggers a REST notification.

See the *Reassigning devices* section in the ***MyID Core API*** guide.

4.1.5 Mobile Identity Document enhancements

You can now issue Mobile Identity Documents as derived credentials through the Self-Service Request Portal. For information on how to set up a Mobile Identity Document credential profile, see the *Creating a mobile identity document credential profile* section of the ***Derived Credentials Self-Service Request Portal*** guide.

Also, you can now specify MDM restrictions in credential profiles used to issue mobile identity documents. You can configure a credential profile to issue only to devices registered with the MDM, and you can require particular attributes of registered devices as stored in the MDM.

For more information, see the *Creating the mobile identity document credential profile* section in the ***Mobile Identity Documents*** guide.

4.1.6 Multiple MDM connectors

You can now set up multiple MDM connectors for issuing your mobile credentials. If you have multiple MDM external systems configured, you can select which one to use in the credential profile. If you have only one MDM external system, it is selected automatically.

You can set up multiple MDM connectors of the same type, or multiple MDM connectors of mixed types; for example, you could set up two Intune connectors and one VMWare connector on the same MyID system.

If you upgrade from a system where only one MDM connection was supported, any credential profiles that have MDM restrictions configured are updated to select your registered MDM.

See the *Setting up your MDM system* section in the ***Mobile Identity Management*** guide.

4.2 Integration updates

This section contains details of updates to MyID 12.11.0's support for integration with smart cards and other credentials, certificate authorities, printers, and HSMs.

4.2.1 Entrust Datacard printers

The following Entrust Datacard printer is now supported with MyID:

- Sigma DS3.

    Note: The printer name is displayed as XPS Card Printer.

See the *Entrust Datacard printers* section in the ***Printer Integration Guide***.

4.2.2 Entrust nShield HSMs

MyID CMS can now integrate with the Entrust nShield 5c HSM. MyID CMS has now been tested with new configurations of the Entrust nShield HSMs.

See the *Hardware and software requirements* section of the ***Entrust nShield HSM Integration Guide***.

4.2.3 Yubico devices

MyID now supports the following Yubico devices:

- YubiKey v5.7
- YubiKey v5.7 FIPS

Note: Due to limitations in naming with non-alphanumeric characters, the YubiKey 5.7 and YubiKey 5.7 FIPS devices are known as "YubiKey v57" and "YubiKey v57 FIPS" within MyID.

See the *Yubico smart cards* section in the ***Smart Card Integration Guide***.

4.3 Improvements

This section provides details of minor improvements to existing functionality within MyID 12.11.0.

4.3.1 General bug fixes and improvements

This release contains general bug fixes and minor improvements as part of a program of continuous improvement.

This release incorporates the following hotfixes:

- HOTFIX-12.2.0.8 – Allow ability to configure the deferral period used when sending notifications.

4.3.2 Customizing the MyID Operator Client authentication pop-up window

You can now customize the size of the MyID Authentication pop-up window in the MyID Operator Client. This can be useful if you are authenticating with an external IDP – it allows you to increase the length of the window to show a longer list of options without scrolling, or to change the size of the pop-up window to fit the sign-in options for an external IDP.

For more information, see the *Changing the size of the authentication pop-up* section in the ***MyID Operator Client*** guide.

4.3.3 Custom client configuration files for web.oauth2

Previously, when configuring your web.oauth2 web service to add custom clients to allow you to work with the MyID Core API, you had to edit an array in the `appsettings.Production.json` file. Because elements in this array were determined by their index, you needed to pad the array to the correct size to correspond to the entries in the `appsettings.json` file and prevent accidentally overwriting other clients.

To simplify this process, and to allow for greater maintainability, you can now create a separate configuration file for each client in the `CustomClients` subfolder. By default, this is:

```
C:\Program Files\Intercede\MyID\web.oauth2\CustomClients\
```

These custom client configuration files each contain the details for a single client, which is identified by its `ClientID`. If the `ClientID` already exists in the `appsettings.Production.json` or `appsettings.json` file, the details from the custom client configuration file completely replace the existing settings for that client; if the `ClientID` does not exist, the client is added to the configuration for the web service.

Note: You can continue to use the `appsettings.Production.json` file for your client configuration if you want, but you are recommended to move any clients you have created into their own custom client configuration files.

For more information, see the *Configuring web.oauth2 for server-to-server authentication* and *Configuring web.oauth2 for end-user based authentication* sections in the ***MyID Core API*** guide.

4.3.4   Disambiguating accounts in the Self-Service Request Portal

If your system has multiple accounts that have the same DN, but are differentiated by an account attribute, you can now specify additional attributes in the Self-Service Request Portal configuration file that allow you to disambiguate these accounts.

See the information on the `<person>` node in the *Configuration file format* section of the ***Derived Credentials Self-Service Request Portal*** guide.

4.3.5   Expanding images in the MyID Operator Client

To view an enlarged version of a captured image on the Edit Person screen or the View Person screen, you can now click an image preview on the **Details** tab. To close the enlarged image, click elsewhere on the screen.

See the *Viewing images* section in the ***MyID Operator Client*** guide.

4.3.6   MyID Core API JavaScript examples

As a supplement to the set of worked examples for server-to-server communication with the MyID Core API provided in the previous release, a new worked example for end user authentication has been added, using JavaScript to create a web page, authenticate to MyID as a user, then obtain an access token and call the API, first to obtain a list of people, and then to obtain further information about a specific person.

By the time you complete this example, you should have a basic understanding of how to authenticate to the server as an end user and call the API from a web page to obtain information from the server.

See the *Example – user authentication* section in the ***MyID Core API*** guide.

4.3.7 RSA 3072 and 4096 bit keys

MyID now supports RSA keys with lengths of 3072 or 4096 bits. These key lengths are supported when using the following certificate authorities:

- Microsoft CA.

- PrimeKey EJBCA.

For a Microsoft CA, where the HSM supports RSA key export, it is used for the generation of archived RSA keys; see the *Enable key archiving* section in the ***Microsoft Windows CA Integration Guide***. This feature has been tested with Entrust nShield and Thales Luna HSMs.

Support for these keys on devices is dependent on the device. Currently, these keys are supported on the following:

- IDEMIA ID-One PIV 2.4.2 on Cosmo V8.2 (3072 only)

  Note: 3072 bit keys are supported only on devices conforming to *BAP#087586 – ID-One PIV 2.4 on Cosmo v8.2 SPE+*.

- YubiKey v57 FIPS (3072 and 4096)

- YubiKey v57 (3072 and 4096)

- Thales SafeNet eToken Fusion FIPS (3072 and 4096)

- Thales SafeNet eToken Fusion FIPS USB-C (3072 and 4096)

- Android and iOS devices (3072 and 4096)

- Soft certificates (3072 and 4096)

Note: MyID currently uses the SHA-256 hash algorithm when issuing larger key sizes.

See the ***Smart Card Integration Guide*** for full details of which devices support keys of these lengths.

Note: Currently, you cannot use the MyID Client for Mac to collect devices with RSA 3072 or 4096 bit keys.

4.3.8 Searching certificates by User SID

You can now search for certificates either by whether it has a User SID associated with it using the **User SID Present** search criterion, or search for a certificate by its **User SID** in the **Certificates** report.

For more information, see the *Certificates report* section in the ***MyID Operator Client*** guide.

4.3.9 Title bar enhancements for the MyID Operator Client

The title bar for the MyID Operator Client now displays the logon name and the last logon time of the currently logged-on operator.

Additionally, the **MyID** label at the left of the title bar now appears both before and after logon; as this is a translatable label, you can (for example) use different labels for your pre-production system and your production system. For information about translating the MyID interface, contact customer support quoting reference SUP-138.

See the *MyID Operator Client user interface* section in the ***MyID Operator Client*** guide.

4.4 End of support features in MyID 12.11.0

This section contains information about features that are no longer supported in MyID as of MyID 12.11.0.

There are no end of support features in this release.

4.5 Documentation updates in MyID 12.11.0

This section contains information on new and updated documentation in MyID 12.11.0.

4.5.1 Administration Guide

The ***Administration Guide*** has been updated with the following:

- The *REST web services notifications* section has been moved into a separate guide.

  See the ***REST Web Service Notifications*** guide.

- Added information on a new feature that can restrict users if they do not log in for a set amount of time.

  See the *Restricting inactive users* section.

- Added information on new certificate search options relating to User SIDs.

  See the *Including user security identifiers in certificates* section.

- Added information about the following new configuration options:

  - **Notification API Abort Timeout**
  - **Notification Web Abort Timeout**

  See the *Notifications page (Operation Settings)* section.

4.5.2 Derived Credentials Self-Service Request Portal

The ***Derived Credentials Self-Service Request Portal*** has been updated with the following:

- Added information on how the Self-Service Request Portal can now issue mobile identity documents as derived credentials.

  See the *Creating a mobile identity document credential profile* section.

- Extended information about SSL certificates.

  See the *SSL certificates* and *Error code reference* sections.

- You no longer need to edit the dictionary in the SSRP web application when you have set the **Client certificates** option in IIS to **Require**.

  See the *Web applications* section.

4.5.3 Entrust nShield HSM Integration Guide

The ***Entrust nShield HSM Integration Guide*** has been updated with the following:

- Added information on the new integration with the Entrust nShield 5c HSM, and updated how the nShield HSMs have been tested.

  See the *Hardware and software requirements* section.

- Updated information on FIPS140-2 level 3.

  See the *FIPS140-2 level 3* and *FIPS 140-2 level 3 authorization for generating or importing keys* sections.

- Updated information in initializing the keyserver database key.

  See the *Initialize the Keyserver Database key as an HSM protected key* section.

- Added information about the Remote Admin Client.

  See the *The role of the HSM card reader* section.

- Added information about running nShield's `enquiry` command line utility.

  See the *Configure remote file system / client connectivity* section.

4.5.4 Lifecycle API

The ***Lifecycle API*** guide has been updated with the following:

- Updated with a limitation – the Lifecycle API does not reset logon dates when used to restrict inactive users.

  See the *Restricting inactive users* section.

4.5.5 Microsoft Windows CA Integration Guide

The ***Microsoft Windows CA Integration Guide*** has been updated with the following:

- Added information on support for RSA 3072 and 4096 bit keys.

  See the *RSA support* section.

4.5.6 Mobile Identity Documents

The ***Mobile Identity Documents*** guide has been updated with the following:

- You can now specify MDM restrictions in the credential profile of mobile identity documents.

  See the *Creating the mobile identity document credential profile* section.

4.5.7 Mobile Identity Management

The ***Mobile Identity Management*** guide has been updated with the following:

- Added information on using multiple MDM connectors.

  See the *Setting up your MDM system* section.

- Clarified role and logon mechanism requirements.

  See the *Granting access to the workflows* section.

4.5.8 MyID Client for Mac

The ***MyID Client for Mac*** guide is new for this release.

4.5.9 MyID Core API

The **MyID Core API** guide has been updated with the following:

- A set of examples for creating a website that uses end-user authentication to call the MyID Core API.

  See the *Example – user authentication* section.

- Added information about custom client configuration files for web.oauth2.

  See the *Configuring web.oauth2 for server-to-server authentication* and *Configuring web.oauth2 for end-user based authentication* sections.

- Added information about using the API to reassign devices.

  See the *Reassigning devices* section.

4.5.10 MyID Operator Client

The **MyID Operator Client** guide has been updated with the following:

- Added information about enhancements to the MyID Operator Client title bar.

  See the *MyID Operator Client user interface* section.

- Added information on viewing expanded images.

  See the *Viewing images* section.

- Added information on a new report on restricted users.

  See the *People with Restricted Access to Operations report* section.

- Added information on new certificate search options relating to User SIDs.

  See the *Certificates report* section.

- Added information on customizing the size of the authentication pop-up window.

  See the *Changing the size of the authentication pop-up window* section.

- Added further clarification on when the MyID Client Service is required.

  See the *Required software* section.

4.5.11 Operator's Guide

The **Operator's Guide** has been updated with the following:

- A note on the PIN limitations of the MyID Card Utility.

  See the *Remote PIN Management utility for PIV cards* section.

- A note on the PIN limitations of the Unlock Credential Provider.

  See the *Unlock credential provider* section.

- Updated screenshots throughout.

4.5.12 PrimeKey EJBCA CA Integration Guide

The *PrimeKey EJBCA CA Integration Guide* has been updated with the following:

- Updated information on formats for custom certificate extensions.

  See the *Configuring custom certificate extensions* section.

- Updated information on the handling of subject DNs.

  See the *Generating a certificate subject DN* section.

- Updated the supported EJBCA version.

  See the *Supported PrimeKey EJBCA versions* section.

- Added information on support for RSA 3072 and 4096 bit keys.

  See the *RSA support* section.

4.5.13 Printed Identity Documents

The *Printed Identity Documents* guide is new for this release.

4.5.14 Printer Integration Guide

The *Printer Integration Guide* has been updated with the following:

- A new known issue has been added to the XID printers section.

  See the *Known issues for XID printers* section.

- Added information on a newly supported Entrust printer.

  See the *Entrust printers* section.

- Added known issue for Entrust printers with Identiv uTrust 5500 reader boards.

  See the *Limitations and known issues for Entrust printers* section.

4.5.15 REST Web Services Notifications

The *REST Web Service Notifications* guide contains information that has been moved from the *Administration Guide* into a separate document.

4.5.16 Smart Card Integration Guide

The *Smart Card Integration Guide* has been updated with the following:

- Added information about YubiKey v5.7 and YubiKey v5.7 FIPS devices.

  See the *Yubico smart cards* section.

- Added information about support for RSA 3072 and 4096 bit keys for each device type.

  See each chapter in the guide.

- When you enable or disable interfaces on YubiKey tokens (for example, using the `YubiKeyNoOTP.xml` card format file) you must remove the token and re-insert it for the changes to take effect.

  See the *Enabling and disabling device capabilities* section.

4.6 Known issues resolved in MyID 12.11.0

This section lists the known issues that have been resolved in MyID 12.11.0. These are issues that were found across both editions of MyID – Enterprise and PIV – and may not all be relevant for your system.

- There are no known issues resolved in this release.

5 Updates in MyID 12.10.0

This chapter provides details of the changes in MyID 12.10.0, including:

- New and updated features – new features in this version of MyID, and major improvements to existing features.

- Integration updates – updates to MyID's support for smart cards and other credentials, certificate authorities, printers, and HSMs.

- Improvements – minor updates to existing functionality.

Important: At MyID version 12.9, the version of .NET Core used was updated. This affects the MyID servers and all clients. See section *6.3.2*, *.NET Core 8.0* for details.

Important: Microsoft is making changes to DCOM security over the course of releases in 2021 to 2023 that may affect your system, depending on your configuration. See section *13.2.2*, *Microsoft Windows DCOM server security changes* for details.

5.1 New and updated features

This section contains information on the new and updated features in MyID 12.10.0.

5.1.1 Using external identity providers

Many organizations are now using systems such as Microsoft Entra or Okta as an identity provider (IdP) within their identity and access management ecosystem. These systems, and many others including Microsoft and Google, have adopted the OpenID Connect protocol as a means of federating identity information with other systems, providing a common way of authenticating a person, and then providing information about a person to the system. For example, an initial credential provided by the IdP – a password, or temporary access credential such as Microsoft TAP – can be used as authentication to start registration of more secure passwordless authentication methods such as certificates on a secure device or a FIDO passkey.

You can now use external OpenID Connect identity providers (for example, Microsoft Entra or Google) to provide authentication to MyID for the following scenarios:

- Creating a self-service request for derived credentials, including the creation of a new account in MyID if needed. The user can then immediately start the collection of a security device with certificates, such as a YubiKey or other smart card, or the collection of Windows Hello credentials, or can start downloading certificates onto a mobile for use with Microsoft Intune or VMWare Workspace ONE. You can also use this process to register a FIDO passkey with MyID CMS.

  The Self-Service Request Portal (SSRP) supports the following types of identity provider:

  - OpenID Connect – you authenticate to an external identity provider (for example, Microsoft Entra), and SSRP generates a request for derived credentials based on the claims returned by the external system. You can then collect the credentials. This is new for this release.

  - SSL – you log in with your certificate (for example, on a PIV card or other secure device) and SSRP generates a request for credentials based on the client certificate stored on the card. This is existing functionality.

  You can configure SSRP for multiple OpenID providers; SSRP provides a choice to the user when they access the SSRP website. You can also configure SSRP for one or more OpenID providers *in addition to* the SSL provider; the user can select which authentication method to use when they access the SSRP website. You can also continue to use SSRP exclusively for client certificate-based authentication.

  For more information, see the *External identity providers* section in the ***Derived Credentials Self-Service Request Portal*** guide.

- Logging on to the MyID Operator Client or any other system that uses the MyID web.oauth2 authentication service.

  This provides supplemental authentication options that you can use instead of the existing logon mechanisms; for example, on the MyID Authentication screen in the MyID Operator Client, you could select **Microsoft Entra ID** instead of **Smart Card** or **Security Questions**, and authenticate to the MyID Operator Client using your Microsoft account instead of inserting your card or typing your passwords..

  You can configure MyID to add new users from the configured external identity provider, to accept users only if they already exist in MyID, or to update existing users with details from the configured external identity provider. You can map the information available

from the external identity providers to MyID user attributes; for example, if the external identity provider has an email address attribute, you can store this in the **Email** field for a person in MyID.

For more information, see the *Setting up an external identity provider* section in the ***MyID Authentication*** guide.

5.1.2 Allowing a user attribute to be mapped to the card label

You can now use any attribute of a person as a card label. These card labels are encoded digitally onto the card; the label may be visible, for example, within the smart card client software.

Previously the card label was fixed as the full name of the cardholder; this is still the default.

You can configure this mapping using the **Card label mapping** configuration option (on the **Devices** tab of the **Operation Settings** workflow).

Use the format:

```
person.<attribute>
```

where:

* `<attribute>` – any column in the `vPeopleUserAccounts` view in the MyID database.

For example, you may want to use the following:

* `person.LogonName`
* `person.Email`
* `person.FullName`
* `person.SAMAccountName`
* `person.UserPrincipalName`

Note: This feature is supported with Thales Authentication Devices used with SafeNet Minidriver or SafeNet Authentication Client Middleware.

See the *Devices page (Operation Settings)* section in the ***Administration Guide*** for details.

5.1.3 Managing directories through the MyID Core API

You can use the MyID Core API to manage your directories.

For example, you may want to update the passwords for all of your directories. You can write a script that iterates through your directories, tests the connection for each directory using the new password, then, if that succeeds, updates the directory configuration with the new password, then finally verifies that MyID can still connect to the directory.

The API provides features that allow you to:

* Get a list of directories.
* Get details for a specific directory.
* Test the connection to the directory using new credentials.
* Update the settings for a directory.
* Verify the connection to the directory using the existing credentials.

See the *Managing directories* section in the ***MyID Core API*** guide.

5.1.4 MyID Core API examples

A set of worked examples for server-to-server communication with the MyID Core API has been added, using Python scripts to obtain an access token and call the API. It then goes on to provide example scripts that take you from getting simple results from the MyID database to adding a person, requesting a device, and checking the status of the request. Further examples are provided for getting multiple-page reports and working with access tokens.

By the time you complete these examples, you should have a basic understanding of how to authenticate to the server and call the API to obtain and post information to and from the server.

See the *Example – server-to-server* section in the **MyID Core API** guide.

5.1.5 Self-Service App for macOS

Self-service management of YubiKey devices and IDEMIA PIV cards is now available for beta testing on Apple macOS computers.

The app is supported on ARM-based M series Apple silicon devices running the following operating system versions:

- Monterey – version 12.7.1 (21G920)
- Ventura – version 13.4
- Sonoma – version 14 to 14.2.1 (23C71)

The app allows you to manage the following devices:

- YubiKey 4 (PIV/smart card interface only)
- YubiKey 5 (PIV/smart card interface only)
- YubiKey FIPS (PIV/smart card interface only)
- IDEMIA ID-One PIV 2.4.2

  Note: IDEMIA ID-One cards with Secure PIN Entry (SPE) are *not* supported.

Using the app, you can:

- Collect your smart card, including the issuance of new and recovered certificates.
- Activate your smart card.
- Change your PIN.
- Reset your PIN.
- Update your device.
- Change your security phrases.

If you want to take part in the beta test program, contact Intercede customer support quoting SUP-385.

5.1.6 Unrestricted card cancellation in the Self-Service App and Self-Service Kiosk

Unrestricted card cancellation is now supported in the latest versions of both the Self-Service App and the Self-Service Kiosk. Previously, this feature was available only in MyID Desktop.

For information on using this feature, see the *Issuance Settings* section in the **Administration Guide**.

Due to changes in the way the applications select cards to support this feature, if you use the latest versions of the Self-Service App or the Self-Service Kiosk with a server running any version of MyID before MyID 12.10, you cannot collect new device issuances unless you disable unrestricted card cancellation on those clients.

To disable unrestricted card cancellation in the Self-Service App, see the *Disabling unrestricted cancellation* section in the **Self-Service App** guide.

To disable unrestricted card cancellation in the Self-Service Kiosk, see the *Disabling unrestricted cancellation* section in the **Self-Service Kiosk** guide.

5.1.7 Upgrading from MyID Professional

The Professional edition of MyID is no longer being developed. You can upgrade your existing installation of MyID Professional to the latest version of MyID Enterprise.

For information on the upgrade process, see the *Upgrading from MyID Professional* section in the **Installation and Configuration Guide**.

5.1.8   User categories and relationships

MyID is often used to meet bespoke requirements for an organization that go beyond managing credentials for employees. For example, you can use MyID to manage credentials for both employees and external visitors to an organization, with different attributes and processes for capturing enrollment data. In some cases, user accounts may represent other organizations that have a need for certificates for authentication, signing, or encryption. Additionally, it can be important to map relationships between user accounts, to allow related accounts to be easily identified and to provide simple reporting and access to the information.

To support these situations, MyID has been enhanced to:

- Allow user categories to be defined.

- Support dedicated attributes and forms for adding, editing, and viewing accounts within each category.

- Define relationship types and allow you to add and remove relationships between accounts.

- Allow a relationship to be assigned automatically when an account is created.

These features are accessed by:

- Configuring categories, attributes, forms, and relationship types using additional tools (MyID Project Designer) – once applied, these create the new forms and operations that you can access in the MyID Operator Client and through the MyID Core API.

- Adding or removing relationships between user accounts using the MyID Core API.

- Listing relationships on the **Relationships** tab of the View Person screen.

- Seeing the number of user accounts in each category in the system status report.

For information on the **Relationships** tab, see the *Working with relationships* section in the ***MyID Operator Client*** guide.

For information on using the MyID Core API, see the ***MyID Core API*** guide.

For information on using relationships and user categories, contact Intercede customer support to discuss the requirements of your project, quoting reference SUP-384.

5.2   Integration updates

This section contains details of updates to MyID 12.10.0's support for integration with smart cards and other credentials, certificate authorities, printers, and HSMs.

5.2.1   Egofy smart cards

TicTok smart cards are now known as Egofy smart cards.

For information on these smart cards, see *Egofy smart cards* section in the ***Smart Card Integration Guide***.

5.2.2   Support for IDP printers

MyID now supports the following IDP printer:

- IDP Smart-51

MyID has been tested with the above printer, and the same driver and SDK supports the IDP Smart-31, which may operate correctly with MyID; however, the IDP Smart-31 printer has not been tested with the latest version of MyID.

See the *IDP printers* section in the ***Printer Integration Guide*** for more information.

5.2.3   Support for Thales HSM client software version 7.13.0

MyID has been tested with the following Thales HSM firmware and client software:

- Firmware 7.13.0, Client 7.13.0 (non FIPS).

See the *Supported Thales Luna HSM models* section in the ***Thales Luna HSM Integration Guide***.

5.2.4   Thales Multifinger Scanner CS500f integration

MyID now provides support for integration with the Thales Multifinger Scanner CS500f.

Support for 10-Slap fingerprint enrollment requires additional software to be installed onto your MyID environment. If you would like access to this feature, or want to discuss use of an alternative fingerprint reader, contact your Intercede account manager for further details.

5.3   Improvements

This section provides details of minor improvements to existing functionality within MyID 12.10.0.

5.3.1   General bug fixes and improvements

This release contains general bug fixes and minor improvements as part of a program of continuous improvement.

This release incorporates the following hotfixes:

- HOTFIX-12.4.1.15 – Allows reprovisioning of devices that are configured to be disabled at issuance.
- HOTFIX-12.4.1.16 – Addresses issues related to system performance, stored procedure results, jobs in the Self-Service App, and Update My Device.
- HOTFIX-12.5.0.13 – Addresses an issue with Reset My PIN.
- HOTFIX-12.5.0.14 – Archived Certificate Pre-Recovery.
- HOTFIX-12.6.0.6 – Support for derived UUID and Terms and Conditions in the Collect Updates workflow.
- HOTFIX-12.8.0.3 – This patch fixes a card printing issue; dynamic font sizing no longer scales text larger than expected on FIPS card layouts.
- HOTFIX-12.9.0.1 – Fix to address an issue with dates not appearing in the correct timezone.

5.3.2 Card layout dynamic text display

You can now display dynamic text on a card layout in a more user friendly way by selecting the **Use Display Text** checkbox.

For example, when you select this option, the card layout displays an enabled card to have an **Enabled** value of `Yes`, instead of `1`.

You can use this option only for dynamic text that is based on a list configured in the **List Editor**, or is otherwise available in the `SelectOptions` table in the MyID database; for these attributes, there is a separate `Value` and `DisplayValue`. If you attempt to set this for other forms of dynamic text, an error occurs.

Note: This option is disabled for custom dynamic text elements.

For more information, see the *Adding dynamic text* section in the ***Administration Guide*** guide.

5.3.3 Database installation scripts

You may want to review the scripts used to install the MyID database for troubleshooting purposes. Your Database Administrator may also want to evaluate the database scripts before allowing you to run them on your database.

A copy of the scripts is now available in the product installation image.

For more information, see the *Database installation scripts* section in the ***Installation and Configuration Guide***.

5.3.4 Disabling UPN and SAMAccountName checks for the Self-Service App

If you launch the Self-Service App without the `/un` parameter and there is no `MYID_USERNAME` environment variable configured, by default, MyID carries out a series of checks. If you do not have a UPN or SAMAccountName, these checks fail, and you cannot view your jobs in the Self-Service App.

To remedy this, you can set the **Ignore UPN and SAMAccountName checks for Self-Service jobs** configuration option (on the **Self-Service** page of the **Security Settings** workflow) to `Yes`, and MyID ignores the UPN and SAMAccountName checks, allowing you to view your available jobs.

See the *Disabling UPN and SAMAccountName checks for the Self-Service App* section in the ***Web Service Architecture*** guide.

5.3.5 Hiding the Tools menu

The **Tools** menu in the MyID Operator Client allows you to carry out batch operations; for example, requesting devices for multiple people, or approving multiple requests. You can now control access to this menu using a new option in the **Edit Roles** workflow.

To access the **Tools** menu, a user must now have a role with the **Tools Menu** option from the **Configuration** section of the **Edit Roles** workflow.

If a user cannot access the **Tools** menu, then they cannot carry out batch operations within the MyID Operator Client.

By default, the **Cardholder** and **PasswordUser** roles have this option enabled, which means that most users have access to the **Tools** menu by default. You can amend your roles to restrict access if necessary.

For more information, see the *Working through multiple records as a batch operation* section in the **MyID Operator Client** guide.

5.3.6 Ignoring cards inserted before running Batch Collect Card

When you run the **Batch Collect Card** workflow, MyID Desktop ignores any cards that you inserted before you ran the workflow.

You can disable this behavior by configuring MyID Desktop. For more information, see *Ignoring cards inserted before running Batch Collect Card* section in the **Installation and Configuration Guide**.

5.3.7 New reports

The following reports are now available in the MyID Operator Client:

- The **Person Status Summary** report.

  This report displays a list of people with summary information about their devices and requests.

  See the *Person Status Summary report* section in the **MyID Operator Client** guide

- The **Request Fulfillment** report.

  This report contains device lifecycle requests with device and group information.

  See the *Request Fulfillment report* section in the **MyID Operator Client** guide

5.3.8 Pre-recovering certificates

You can now improve the performance of the final certificate provisioning step when using the rest.provision service to provision to mobile devices by configuring MyID to store a copy of recovered archived certificates temporarily. This reduces the chance of a timeout from the mobile framework.

Set the **Pre-recover archived certificates for the rest.provison API** configuration option (on the **Certificates** page of the **Operation Settings** workflow) to Yes configure this feature. See the *Certificates page (Operation Settings)* section in the **Administration Guide**.

5.3.9 Refreshing the web service cache

When using the MyID Operator Client or other systems that use the rest.core, rest.provision, or web.oauth2 web services, the web services will now check whether they need to refresh any cached information if it has been more than five seconds (by default) since they last checked.

This includes configuration options, email templates, logon mechanisms, and changes made through server configuration (CONFIG) updates or Project Designer scripts. Previously, you were required to recycle the web service application pools on the MyID web server if you wanted to ensure that MyID was using the latest settings.

In practice, this means that if you make a change (for example, to a configuration option), after a maximum of five seconds, the change is reflected in the behavior of the MyID Operator Client without having to reset the web server.

You can change the default cache refresh time of five seconds if necessary.

A new endpoint that allows you to repopulate the cache has also been added to the MyID Core API.

For more information, see the *Refreshing the cache* section in the ***MyID Operator Client*** guide.

5.3.10 Requiring security questions to be set in the SSA

You can now require users to set the required number of security phrases when collecting a job in the Self-Service App by setting the new **Auto launch workflow in self service operations** option on the **Issuance Processes** page in **Operation Settings** workflow.

The supported values for this option are currently:

- blank

  If you leave the option blank, this feature is disabled; the option is blank by default.

- `1,110`

  If you set this option to `1,110`, when a user collects a card update, card collection, or card activation job in the Self-Service App, if the user has fewer security phrases set than the **Number of security questions to register** configuration option, the user is asked to set that number of security phrases.

For card activation jobs, you can collect the job before you set the security phrases; for all other types of job, you must capture the security phrases before you are allowed to collect the job.

Note: If you want this to use this feature for self activation collections, you must also use the **Edit Roles** workflow to give the **Activation User** role permissions to the **Change My Security Phrases** operation.

For more information, see the *Issuance Processes page (Operation Settings)* section in the ***Administration Guide*** guide.

5.3.11   Storing User SID values for certificates

If you issue or import a certificate that contains the User SID certificate extension, MyID now parses the contents of the extension from the certificate and writes the User SID into the certificate's record in the MyID database – the value is stored in the `UserSID` field of the `Certificates` table. If you issue or import a certificate that does not contain the User SID certificate extension, MyID sets the `Certificates.UserSID` field to an empty string.

This affects all certificates you import or issue after installing MyID 12.10. The Certificate Table User SID Utility is provided to allow you to extract the User SID from existing certificates and update the certificate's record in the MyID database.

See the *Including user security identifiers in certificates* section in the ***Administration Guide*** for details.

5.4 **End of support features in MyID 12.10.0**

This section contains information about features that are no longer supported in MyID as of MyID 12.10.0.

There are no end of support features in this release.

5.5 Documentation updates in MyID 12.10.0

This section contains information on new and updated documentation in MyID 12.10.0.

5.5.1 Administration Guide

The *Administration Guide* has been updated with the following:

- Added information about the **Card label mapping** configuration option, which allows you to specify the attribute from the cardholder's user account that is encoded as the card label on the device when it is issued.

  See the *Devices page (Operation Settings)* section.

- Corrected the security phrase complexity example strings to be correctly formatted, and added a note to clarify how to format a security phrase complexity string correctly.

  See the *Setting rules for security phrases* section.

- Added information about using the MyID Core API for directory management.

  See the *Managing directories through the MyID Core API* section.

- Added information on the new option, **Auto launch workflow in self service operations**, which makes setting the required number of security phrases become a requirement for users collecting jobs in the SSA.

  See the *Issuance Processes page (Operation Settings)* section.

- Added information about storing User SID values for certificates, including the Certificate Table User SID Utility.

  See the *Including user security identifiers in certificates* section.

- Added information on the new option, **Use Display Text**, which can be toggled for dynamic text in the card layout editor and allows more user friendly text to be displayed on cards.

  See the *Adding or changing text* section.

- Added information on the new logon mechanisms available for OpenID Connect authentication.

  See the *Logon Mechanisms page (Security Settings)* section.

- Added information about the **Ignore UPN and SAMAccountName checks for Self-Service jobs** configuration option.

  See the *Self-Service page (Security Settings)* section.

- Removed note on inability to rotate barcodes, as you can now rotate barcodes.

  See the *Adding a 1D barcode* section.

- The **Image Source** field on the **Card Layout Editor** is now labeled **Formatter**.

  See the *Images and backgrounds* section.

- The **Issuance Notification URL** configuration option is now deprecated.

  See the *Notifications page (Operation Settings)* section.

5.5.2   Configuring Logging

The ***Configuring Logging*** has been updated with the following:

- Added specific information for setting up logging for the MyID Notifications Service.

    See the *MyID Notifications Service* section.

5.5.3   Derived Credentials Self-Service Request Portal

The ***Derived Credentials Self-Service Request Portal*** guide has been updated with the following:

- Details of setting up external identity providers using OpenID Connect.

    See the *External identity providers* section.

- Removal of Internet Explorer 11 as a supported browser.

    See the *Introduction* section.

5.5.4   Entrust CA Gateway Integration Guide

The ***Entrust CA Gateway Integration Guide*** has been updated with the following:

- Updated to include the new passcode generation rules, which make the generated passcodes meet the requirements stated in the Entrust CA application version 2.8.10+ documentation.

    See the *Limitations* section.

5.5.5   Error Code Reference

The ***Error Code Reference*** has been updated with the following:

- Updated the error text for the following certificate related errors; with extra information about the specific causes for the errors included in the detail:

    - OC10019 – A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.

    - OC10020 – A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.

    - OC10021 – A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.

    - OC10022 – A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.

    - OC10023 – A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.

    - OC10024 – A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.

    - OC10025 – A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.

    - OC10026 – A technical problem occurred when processing the certificate using MyID client services. This issue requires detailed troubleshooting by a system administrator. Please consult MyID documentation for more information.

    See the *MyID Operator Client error codes* section.

- Added the following new error message relating to licensing:

    - OA10073 – Logon is not permitted - the system license has expired. Contact a system administrator.

    See the *MyID Operator Client error codes* section.

- Added the following new error messages relating to managing directories through the MyID Core API:

    - WS40068 – The directory connection failed with the supplied credentials.

    - WS40069 – Supplied credentials cannot build a valid server location.

    See the *MyID Operator Client error codes* section.

- Added the following error messages relating to external identity providers:

- OA10074 – External logon failed, no matching MyID user found.
- OA10075 – External logon failed, external logon mechanism invalid.
- OA10076 – External logon failed, external logon is not available in standalone mode.
- OA10077 – External logon failed, the attempted logon failed.
- OA10078 – External logon failed, no mappings found for claims.
- OA10079 – External logon failed, a mandatory attribute is not present in either the claims or the user info.
- OA10080 – External logon failed, no claims supplied by external identity provider.

See the *MyID Operator Client error codes* section.

5.5.6   Installation and Configuration Guide

The ***Installation and Configuration Guide*** has been updated with the following:

- Added information about upgrading from MyID Professional to MyID Enterprise.

  See the *Upgrading from MyID Professional* section.

- Added information on ignoring cards in the **Batch Collect Card** workflow and how to disable it.

  See the *Ignoring cards inserted before running Batch Collect Card* section.

- Added information about the provision of database scripts in the product installation image.

  See the *Database installation scripts* section.

- Added a warning about the 2-way SSL/TLS script making unsupported changes to the MyID Operator Client.

  See the *Configuring MyID for 2-way SSL/TLS* section.

- Clarified the requirement for Windows PowerShell 5.1.

  See the *Windows PowerShell 5.1* section.

5.5.7   Implementation Guide

The ***Implementation Guide*** has been updated with the following:

- Information about the Certificate Table User SID Utility.

  See the *Certificate Table User SID Utility* section.

5.5.8   Mobile Identity Management

The ***Mobile Identity Management*** guide has been updated with the following:

- Added the clarification that only one MDM may be used for each MyID instance.

  See the *Supported Mobile Device Management integration* and *Setting up your MDM system* sections.

- Added clarification on setting up Intune as an Azure application.

  See the *Setting up your MDM system* section.

5.5.9 MyID Authentication Guide

The ***MyID Authentication Guide*** has been updated with the following:

- Information about using OpenID Connect systems as external identity providers.

  See the *Setting up an external identity provider* chapter.

5.5.10 MyID Core API

The ***MyID Core API*** guide has been updated with the following:

- A set of example Python scripts for server-to-server communication with the MyID Core API.

  See the *Example – server-to-server* section.

- Added information on setting up cross-origin resource sharing.

  See the *Cross-origin resource sharing* section.

- Added information about managing directories, and the provided sample script.

  See the *Managing directories* and *Sample PowerShell script for managing directories* section.

5.5.11 MyID Operator Client

The ***MyID Operator Client*** guide has been updated with the following:

- Updated the instructions for calling the reports through the API, updated the listing for each report to include the report ID, and removed the list of parameters where included as this is available through the API documentation.

  See the *Running reports through the MyID Core API* section and each report listed in the *Available reports* section.

- Added the **Submit Adjudication?** field to the People report.

  See the *People report* section.

- Added information on the new cache refreshing feature. Also removed the requirement to recycle the application pools from several procedures now that it is no longer necessary due to the cache refresh.

  See the *Refreshing the cache* section.

- Added detail about the suitability of "friendly" certificate policy names for inclusion in soft certificate file names.

  See the *Customizing certificate file names* section.

- Added information on the new visibility toggle for the **Tools** menu.

  See the *Working through multiple records as a batch operation* section.

- Added information about the **Person Status Summary** and **Request Fulfillment** reports.

  See the *Person Status Summary report* and *Request Fulfillment report* sections.

- Updated the fields available on the Assign Device (Search) screen.

  See the *Searching for a device to assign* section.

- Added information on the compatibility of PFX files with various operating systems. This information has been added where relevant, for example:

  See the *Collecting a soft certificate* section.

- Added information on the new features of user categories and relationships.

  See the *Working with relationships* section.

- Added a warning about the 2-way SSL/TLS script making unsupported changes to the MyID Operator Client.

  See the *2-way SSL/TLS* section.

5.5.12 Operator's Guide

The ***Operator's Guide*** has been updated with the following:

- Added clarification on temporary card cancellation behavior.

  See the *Canceling temporary cards* section.

5.5.13 PrimeKey EJBCA CA Integration Guide

The *PrimeKey EJBCA CA Integration Guide* has been updated with the following:

- Updated information on the logging of the EJBCA connector in MyID.

  See the *Logging* section.

- Added information about removing duplicate attributes from an End Entity Profile.

  See the *Removing repeated attributes* section.

5.5.14 Printer Integration Guide

The *Printer Integration Guide* has been updated with the following:

- Added support for IDP Smart printers.

  See the *IDP printers* section.

- Added troubleshooting for Datacard CR805 printers.

  See the *Troubleshooting Datacard printers* section.

5.5.15 Self-Service App

The *Self-Service App* has been updated with the following:

- Unrestricted card cancellation is now supported in the latest versions of the Self-Service App.

  See the *Disabling unrestricted cancellation* section.

5.5.16 Self-Service Kiosk

The *Self-Service Kiosk* has been updated with the following:

- Unrestricted card cancellation is now supported in the latest versions of the Self-Service Kiosk.

  See the *Disabling unrestricted cancellation* section.

5.5.17 Smart Card Integration Guide

The *Smart Card Integration Guide* has been updated with the following:

- TicTok devices are now known as Egofy devices.

  See the *Egofy smart cards* section.

5.5.18 Thales Luna HSM Integration Guide

The *Thales Luna HSM Integration Guide* has been updated with the following:

- Added information on the compatibility of MyID with Thales HSM Client software version 7.13.0. They are compatible.

  See the *What is needed?* section.

5.5.19 Web Service Architecture

The *Web Service Architecture* guide has been updated with the following:

- Details of disabling the UPN and SAMAccountName checks for the Self-Service App.

  See the *Disabling UPN and SAMAccountName checks for the Self-Service App* section.

5.6　Known issues resolved in MyID 12.10.0

This section lists the known issues that have been resolved in MyID 12.10.0. These are issues that were found across both editions of MyID – Enterprise and PIV – and may not all be relevant for your system.

6 Updates in MyID 12.9.0

This chapter provides details of the changes in MyID 12.9.0, including:

- New and updated features – new features in this version of MyID, and major improvements to existing features.

- Integration updates – updates to MyID's support for smart cards and other credentials, certificate authorities, printers, and HSMs.

- Improvements – minor updates to existing functionality.

Important: At MyID version 12.9, the version of .NET Core used was updated. This affects the MyID servers and all clients. See section *6.3.2, .NET Core 8.0* for details.

Important: Microsoft is making changes to DCOM security over the course of releases in 2021 to 2023 that may affect your system, depending on your configuration. See section *13.2.2, Microsoft Windows DCOM server security changes* for details.

6.1 New and updated features

This section contains information on the new and updated features in MyID 12.9.0.

6.1.1 Adding barcodes to card layouts

You can add 1D and 2D barcodes to your card layouts; these barcodes can contain information from the cardholder's record. You can print these barcodes on physical cards or include them on the layouts used for mobile credentials: mobile badge layouts and mobile identity documents.

MyID supports the following formats for barcodes:

- 1D barcode

  This is a standard 1D barcode in Code 39 format. You can add a barcode in this format for any auto text field on a card layout by selecting the **Barcode** font. MyID supports the Code 39 Extended character set.

  Previously MyID supported 1D barcodes using a font installed on the client PC to render the barcode. The barcode is now rendered on the MyID server, removing the need to have the font installed.

- 2D barcode

  These are PDF417 2D barcodes in either horizontal or vertical orientation. You must use custom attributes to hold the 2D barcode data. Use of 2D barcodes requires customization using Project Designer. For more information, contact customer support, quoting reference SUP-155.

  2D barcodes were introduced in MyID 12.8. This release enhances the support for 2D barcodes (including the display of errors for troubleshooting) and improves their scaling.

  Note: 2D barcodes are supported on printed cards, the MyID Wallet app, and mobile apps developed using the Identity Agent Framework. You cannot use 2D barcodes in the MyID Identity Agent app.

For more information, see the *Adding barcodes* section in the ***Administration Guide***.

6.1.2 Mobile identity documents

MyID's mobile identity documents feature allows you to request a mobile identity document and associated graphical badge layouts, and provision them to the wallet app on your mobile device.

You can include user photographs, organization logos, text information from the person's user account in MyID, and barcodes (both 1D and PDF417 2D) on these graphical badge layouts.

In contrast to a mobile identity, a mobile identity document provides information *about* a person, rather than a credential that proves *who* a person is.

You can use mobile identity documents for a variety of purposes. For example:

- Driver's license.

- Age verification.

- Proof of entitlement (for example, loyalty cards).

- Proof of qualification (for example, accreditations, education).

- Proof of access rights (military bases, sites and so on).

- Proof of authority (warrant cards and so on).

MyID provides a standards-based mobile identity document feature, complying with ISO/IEC 18013-5. Mobile identity documents issued by MyID are verifiable, cryptographically secure, and incorporate privacy by design.

Intercede provides a sample document format, which works with the MyID Wallet app, but your organization may want to create its own document formats, and its own wallet app using the MyID Identity Agent Framework API; this allows you to include custom attributes in your mobile identity documents. For more information on this process, contact Intercede customer support quoting reference SUP-381.

See the ***Mobile Identity Documents*** guide for details.

6.1.3 Sorting, grouping, and filtering records

The MyID Operator Client now allows you to work with your tables of records (for example, search reports, data tables within tabs in forms, and batch results) in a flexible way. You can:

- Move and resize columns.

- Display and hide columns.

- Sort on single or multiple columns.

- Group and filter records.

- Change the row spacing.

You can also use the sorting feature when requesting report results using the MyID Core API.

For more information, see the *Working with tables of records* section in the ***MyID Operator Client*** guide.

6.1.4   Viewing which attributes have changed

The **Attribute Changes** tab has been added to the View Audit screen and the View Person screen. This tab displays a list of the fields that have changed for the device or person, as well as their previous and new values.

For more information, see the *Viewing audit details* section in the ***MyiD Operator Client*** guide.

6.2   Integration updates

This section contains details of updates to MyiD 12.9.0's support for integration with smart cards and other credentials, certificate authorities, printers, and HSMs.

6.2.1   Entrust v10

MyiD now supports Entrust v10 using the current integration with Entrust Administration Toolkit for C. This is in addition to accessing Entrust v10 through the Entrust Gateway.

The following caveats apply for integration with Entrust v10:

- It is not possible for Intercede to replicate all Entrust configurations, so customers must test integration within a non-production environment before deploying in production.

- Support for integration is 'like for like' when compared to integration with Entrust v8.x – therefore no new capabilities available in Entrust v10 are supported at this time.

- The Entrust Security Manager Advanced setting `CertificateEntropy` must be set to `Off` – 128-bit serial number certificates and therefore the Entrust v10 features to support multiple nodes in a cluster are not supported.

- Where further issues are raised, Intercede will investigate with best endeavors to achieve a resolution, but ultimately may not be able to resolve problems without further support from Entrust or migration to alternative toolkits.

Intercede is continuing to investigate support for Entrust Security Administration Toolkit for Java, as a replacement for Entrust Administration Toolkit for C. A further statement will be provided when more information is available.

For further assistance with this issue, contact Intercede customer support quoting reference SUP-379.

See the *Supported Entrust versions* and *Entrust v10-specific behavior* sections in the ***Entrust CA Integration Guide*** for details.

6.2.2 MIFARE devices

MyID now allows you to issue and manage contactless cards that use a MIFARE interface; this includes both single-interface MIFARE devices and dual-interface MIFARE devices that also have a contact chip. For devices that have only a MIFARE interface, the MIFARE serial number is stored in MyID as the device serial number.

You can use the **Proximity Card Check** option in the credential profile to check the MIFARE serial numbers of the MIFARE devices you are issuing. See the *Issuance Settings* section in the *Administration Guide* for details.

Important: Support for MIFARE devices requires both:

- Updated MyID client software; use the versions provided with MyID 12.9 or later.

- An additional update for your MyID system. Contact customer support quoting reference SUP-380 for more information.

6.3 Improvements

This section provides details of minor improvements to existing functionality within MyID 12.9.0.

6.3.1 General bug fixes and improvements

This release contains general bug fixes and minor improvements as part of a program of continuous improvement.

This release incorporates the following hotfixes:

- HOTFIX-12.8.0.1 – Addresses known issues from the MyID version 12.8.0 release.

- HOTFIX-12.7.0.2 – Character support for EJBCA and software certificates.

- HOTFIX-12.5.0.12 – Addresses an issue with adjudication.

- HOTFIX-12.4.1.14 – Resolves an issue that was resulting in expired suspended certificates' status being changed back to active status.

- HOTFIX-12.4.1.13 – Support for unrestricted roles when Restrict Roles on Child Groups is enabled.

- HOTFIX-12.2.0.6 – Addresses card printing and authentication code issues.

- HOTFIX-11.7.5.6 – Status Mapping Update.

- HOTFIX-11.6.2.11 – Addresses issues relating to Windows Logon when using the MyID Web Client if an IIS session timeout occurs.

6.3.2 .NET Core 8.0

MyID has been updated to require .NET Core 8.0 instead of .NET Core 6.0. You must update your servers and clients with .NET Core 8.0.

See the *.NET Core Hosting* and *Before you upgrade* sections in the *Installation and Configuration Guide*.

Note: This also affects the MyID Document Uploader utility. See the *Prerequisites* section in the *MyID Document Uploader* guide.

6.3.3 Additional timestamp fields for certificates

MyID now records additional timestamps for certificate processes. The additional information is stored in the MyID database; you can use this information in your own reporting, either through direct access to the database or through custom management information reports.

Note: Currently, this information is not available on MyID Operator Client screens or through the standard reports.

The additional fields are:

- `Certificates` table:

  - `RevokeStartTime` – set when MyID starts to revoke a certificate.

  - `RevokeCompleteTime` – set when MyID completes revoking a certificate.

  - `IssueStartTime` – set when MyID starts to issue a certificate.

  - `IssueCompleteTime` – set when MyID completes issuing a certificate.

6.3.4 Data link files for archive databases

When modifying an installation to add an archive database, if you run the installation from the MyID application server, the installer now automatically updates the Universal Data Link (UDL) files used by MyID to point to the archive database.

In some circumstance you may need to update these files manually. See the *Creating an archive database* section in the ***Advanced Configuration Guide*** for details.

6.3.5 Logon name in REST notifications

The following REST notifications have been enhanced to include the logon name of the person who owns the device:

- REST Device Issued

- REST Device Cancelled

- EnableCard

- DisableCard

The logon name appears in the person node in the output JSON; for example:

```
"person": {
    "logonName": "Jane Smith"
}
```

See the *REST Device Issued notification*, *REST Device Cancelled notification*, *EnableCard notification*, and *DisableCard notification* sections in the ***Administration Guide***.

6.3.6 MSIX optional packages update

Some of the MSIX optional packages (`DSKLauncher`, `MCSLauncher`, and `SSALauncher`) have been updated to version 1.1.0 for the MyID Client Suite 1.5.0.If you are using MSIX, you must upgrade your clients to the updated MSIX files.

See the *Upgrading to the MyID Client Suite 1.5.0* section in the ***MyID Client MSIX Installation Guide***.

6.3.7   Project Designer base file changes in MyID 12.9

MyID Project Designer allows you to create your own customizations on top of the MyID base system. The base project files change from release to release with enhancements to support the latest features; you must be aware of these changes and consider the effect they may have on your existing customizations.

6.3.7.1 Attribute changes

The `Kind` attribute has the following new entries in its picklist:

- Display text `Contactless Card`, underlying value `ContactlessCard`.
- Display text `MFA Token`, underlying value `mfa`.
- Display text `Mobile Identity Document`, underlying value `Document`.

The `Device Category` attribute has the following new entries in its picklist:

- Display text `MFA Token`, underlying value `mfa`.
- Display text `Mobile Identity Document`, underlying value `Document`.

New device attributes:

- `Mifare Serial Number`, which maps to the `MifareDevices.SerialNumber` database field.

New adjudication attributes:

- `Decision Time`, which maps to the `Adjudication.DecisionTime` database field.
- `System Response Time`, which maps to the `Adjudication.SystemResponseTime` database field.
- `System Submit Time`, which maps to the `Adjudication.SystemSubmitTime` database field.

New certificate attributes:

- `Issuance Complete Time`, which maps to the `Certificates.IssueCompleteTime` database field.
- `Issuance Start Time`, which maps to the `Certificates.IssueStartTime` database field.
- `Revocation Complete Time`, which maps to the `Certificates.RevokeCompleteTime` database field.
- `Revocation Start Time`, which maps to the `Certificates.RevokeStartTime` database field.

New audit attributes:

- `Operator Account ID`, which maps to the `Audit.iManagerID` database field.
- `User Account ID`, which maps to the `Audit.iUserAccountID` database field.

6.3.7.2 Form changes

The View Device form now has the new fields `MiFare Serial Number` and `Device Version`.

6.3.7.3 Report changes

The **Unrestricted Audit Report** report now has an **End Timestamp** column.

The **Unrestricted Audit Report** has added the text `(historic)` to the **Person (Logon Name)** and **Operator (Logon Name)** search criteria labels.

The **Assign Device Search** report now has a **MiFare Serial Number** column, and matching search criterion (which is free text).

The **Assigned Devices** and **Devices** reports now have a **Device Version** column, and matching search criterion (which is free text).

The **People**, **People with Biometrics** and **People Without Biometrics** reports now have a **Group Name** search criterion (which is free text) – this is in addition to the group picker search criterion (this was required for the sorting feature).

The **Assigned Devices**, **Mobile Devices** and **Devices** reports now have **Enabled** (drop-down `Yes/No`) and **Owner** (free text) search criteria.

The **Requests** and **Requests for review** reports now have **Full Name** and **Task Type** search criteria (both free text).

The **Certificates** report now has an **ID** search criterion (which is free text).

All report fields have a `FlexW` attribute, defaulting to `3` (that is, all have equal width), with a number of overrides set to suitable values.

All report fields have an `Order` attribute (which was already present before), defaulting to `None` (that is, all have no default sort order), but there are now a number of overrides set to suitable values for the sorting feature.

The classic web **MI Reports** workflow now always has a **Certificates** report included. MyID Enterprise had it already, but it was missing in MyID PIV. It now exists in both, with the same definition.

6.4   End of support features in MyID 12.9.0

This section contains information about features that are no longer supported in MyID as of MyID 12.9.0.

There are no end of support features in this release.

6.5   Documentation updates in MyID 12.9.0

This section contains information on new and updated documentation in MyID 12.9.0.

6.5.1   Administration Guide

The *Administration Guide* has been updated with the following:

- Updated the output from the REST Device Issued, REST Device Cancelled, EnableCard, and DisableCard notifications to include the logon name for the device owner.

  See the *REST Device Issued notification*, *REST Device Cancelled notification*, *EnableCard notification*, and *DisableCard notification* sections.

- Added information on using MIFARE devices with the **Proximity Card Check** option in the credential profile.

  See the *Issuance Settings* section.

- Added information about adding barcodes to card layouts.

  See the *Adding barcodes* section.

- Added details of the **Disable Report Count** configuration option.

  See the *General page (Operation Settings)* section.

6.5.2   Advanced Configuration Guide

The *Advanced Configuration Guide* has been updated with the following:

- Updated procedures for creating archive databases for archiving, audit, and binary objects.

  See the *Creating an archive database* section.

6.5.3   Entrust CA Integration Guide

The *Entrust CA Integration Guide* has been updated with the following:

- Added details of support for Entrust v10.

  See the *Supported Entrust versions* and *Entrust v10-specific behavior* sections.

6.5.4 Error Code Reference

The ***Error Code Reference*** has been updated with the following:

- Extended the potential causes of the following errors:
  - OA10004 – Your username or security response is incorrect, or you may not have permission to access this client.
  - OC10004 – The server could not be contacted. Please try again.
  - WS50032 – The conditions on the Operation with ID <operation ID> prohibit use of the operation for the target entity.

  See the *MyID Operator Client error codes* section.

- Added the following new error codes related to sorting records:
  - WS50086 – At least one of the order by fields selected is not an orderable field.
  - WS50087 – At least one of the order by fields selected is an invalid field name.
  - WS40067 – Directory searches do not allow multiple column sorting.
  - WS60000 – Database timeout. Please contact your administrator for more information.
  - WS60001 – The search query timed out. Please contact your administrator for more information.

  See the *MyID Operator Client error codes* section.

- Extended the potential causes of the following error:
  - IA80010 – Problem initializing the key store.

  See the *MyID Identity Agent error codes* section.

6.5.5 Installation and Configuration Guide

The ***Installation and Configuration Guide*** has been updated with the following:

- Updated the required version of .NET Core from 6.0 to 8.0.
  See the *.NET Core Hosting* and *Before you upgrade* sections.
- Added information on setting ActiveX options for embedded web pages in MyID Desktop.
  See the *ActiveX support for embedded web pages* section.
- Added a note on using the **Custom LDAP Mappings** option.
  See the *Upgrading systems with custom LDAP mappings* section.
- Added advice on backing up customized card data model files before upgrading.
  See the *Upgrading systems with customized card data models* section.

6.5.6 Mobile Identity Documents

The ***Mobile Identity Documents*** guide is new for this release.

6.5.7　MyID Core API

The *MyID Core API* guide has been updated with the following:

- Updated the samples for server-to-server authentication.

  See the *Configuring web.oauth2 for server-to-server authentication* section.

6.5.8　MyID Document Uploader

The *MyID Document Uploader* guide has been updated with the following:

- Updated the required version of .NET Core from 6.0 to 8.0.

  See the *Prerequisites* section.

- Added recommendations for setting character encoding for HTML documents.

  See the *Setting HTML encoding* section.

6.5.9　MyID Operator Client

The *MyID Operator Client* guide has been updated with the following:

- Updated information about setting the Chrome allow list for Windows authentication.

  See the *Configuring browsers for Windows authentication* section.

- Added information on the **Attribute Changes** tab on the View Audit screen.

  See the *Viewing audit details* section.

- Added requirements relating to locking down the REST web services.

  See the *The rest.core web service configuration file* section.

- Added information on sorting, filtering, and grouping tables of records.

  See the *Working with tables of records* section.

- Brought the list of fields in the reports up to date.

  See the *Working with reports* section.

6.5.10　MyID Client MSIX Installation Guide

The *MyID Client MSIX Installation Guide* has been updated with the following:

- Added details of upgrading the optional packages.

  See the *Upgrading to the MyID Client Suite 1.5.0* section.

6.5.11　PrimeKey EJBCA Integration Guide

The *PrimeKey EJBCA Integration Guide* has been updated with the following:

- Added information about unsupported characters in the user DN.

  See the *Unsupported characters in the DN* section.

6.5.12　Printer Integration Guide

The *Printer Integration Guide* has been updated with the following:

- Updated the version of the card reader driver for Entrust Datacard printers.

  See the *Entrust Datacard printers* section.

6.5.13 Smart Card Integration Guide

The *Smart Card Integration Guide* has been updated with the following:

- Added information about using YubiKey devices with remote servers.

  See the *Configuring YubiKey devices for remote servers* section.

6.5.14 System Security Checklist

The *System Security Checklist* has been updated with the following:

- Added requirements relating to locking down the REST web services.

  See the *Firewall to protect MyID website* section.

- Added information about blocking HTTP host header injection.

  See the *Blocking HTTP host header injection* section.

6.6 Known issues resolved in MyID 12.9.0

This section lists the known issues that have been resolved in MyID 12.9.0. These are issues that were found across both editions of MyID – Enterprise and PIV – and may not all be relevant for your system.

- IKB-376 – Failure when collecting a request to reprovision a device.

7 Updates in MyID 12.8.0

This chapter provides details of the changes in MyID 12.8.0, including:

- New and updated features – new features in this version of MyID, and major improvements to existing features.

- Integration updates – updates to MyID's support for smart cards and other credentials, certificate authorities, printers, and HSMs.

- Improvements – minor updates to existing functionality.

Important: At MyID version 12.3, the version of .NET Core used was updated. This affects the MyID servers and all clients. See section *13.3.7*, *.NET Core versions* for details.

Important: Microsoft is making changes to DCOM security over the course of releases in 2021 to 2023 that may affect your system, depending on your configuration. See section *13.2.2*, *Microsoft Windows DCOM server security changes* for details.

7.1 New and updated features

This section contains information on the new and updated features in MyID 12.8.0.

7.1.1 Additional REST notifications

In addition to the existing notifications for Issuing, canceling, enabling, and disabling devices, MyID now provides REST notifications for:

- Adding, editing, enabling, disabling, and deleting people.

- Adding and updating Issue Card requests.

See the *REST web service notifications* section in the ***Administration Guide***.

7.1.2 Managing certificates in the MyID Operator Client

You can now manage certificates in the MyID Operator Client. The new **Certificates** category allows you to search for certificates and view their details, as well as carry out certificate management operations.

You can now:

- View the details of a certificate.

  You can run a report that returns a list of certificates, view the certificates assigned to a person, view the certificates assigned to a device, or view the certificates assigned to an additional identity.

  See *Viewing a certificate*.

- Revoke, suspend, or unsuspend a certificate.

  See *Revoking, suspending, and unsuspending certificates*.

- Pause and resume processing of a certificate.

  See *Pausing and resuming certificate processing*.

- Change the renewal settings for a certificate.

  See *Changing renewal settings for a certificate*.

For more information, see the *Working with certificates* chapter in the **MyID Operator Client** guide.

These certificate operations are also available through the MyID Core API.

Note: These features supersede the following MyID Desktop workflows:

- **Certificate Requests**
- **Issued Certificates**
- **Revoked Certificates**

As a result, you can no longer launch these workflows from the **Certificate Administration** section of the **More** category within the MyID Operator Client; you can, however, still launch these workflows from within MyID Desktop.

7.1.3 Printing PDF417 2D barcodes

MyID now has the capability to include PDF417 2D barcodes on card layouts, where you can use custom attributes to hold the 2D barcode data.

Use of this feature requires customization using Project Designer. For more information, contact customer support, quoting reference SUP-155.

7.1.4 Reinstating devices

Previously, you could launch the **Reinstate Card** workflow in MyID Desktop from the View Device screen in the MyID Operator Client. This feature has been superseded by the new **Reinstate** option on the View Device screen in the MyID Operator Client, which provides a more flexible and fully-featured method of reinstating smart cards that have been mistakenly erased or canceled; for example, when a cardholder reports their device as missing, then subsequently finds it before the replacement device has been issued.

When you reinstate a device, MyID creates a request for a new device, linked to the original device's serial number; you must collect this request onto the original device, and it is issued with the same expiry date as the original. You must carry out the same issuance process as defined in the credential profile; for example, the credential profile may require activation, or require authentication codes.

Unlike the MyID Desktop version, this new method of reinstating devices does not require the credential profile to be configured for activation, and works with any smart card, not just PIV cards.

For more information, see the *Reinstating a device* section in the ***MyID Operator Client*** guide.

7.1.5 Viewing the history for a device

The **Device History** tab on the View Device screen now allows you to view the audit trail for a device relating to its current owner.

You must have a role that has access to the View User Audit or View Full Audit feature to view this tab. If you have role permissions to the View Full Audit feature, you can also click on an entry in the list to display the View Audit screen, which contains further information about the actions carried out relating to the device. If the device has been canceled or erased, and you have role permissions to the View Full Audit feature, you can view the entire history of the device for all of its previous owners.

For more information, see the *Viewing a device's history* section in the ***MyID Operator Client*** guide.

7.1.6 Viewing the initial PIN for a device

If you have configured your credential profile to generate an initial PIN for the device using the **EdeficePinGenerator** or **EdeficePolicyPinGenerator** algorithm, MyID can regenerate the PIN that was used when the device was issued using the same secure method, and display it on the View Device screen.

As this is sensitive information, the field that displays the initial PIN on the View Device screen is protected by a special role named View Device Initial PIN. Only operators who have this role can see the initial PIN.

For more information, see the *Viewing the initial PIN for a device* section in the ***MyID Operator Client*** guide.

7.2 Integration updates

This section contains details of updates to MyID 12.8.0's support for integration with smart cards and other credentials, certificate authorities, printers, and HSMs.

7.2.1 Entrust PKI integration improvements

This release includes the following Entrust PKI integration improvements:

- Configuring critical section protection.
- Deactivation of card authentication users.

See the *Configuring critical section protection* and *Deactivation of card authentication users* sections in the ***Entrust CA Integration Guide*** for details.

7.2.2 Giesecke+Devrient – CoolKey devices

MyID now supports the following Giesecke+Devrient devices:

- Giesecke+Devrient SCE v7.0 smart cards with the CoolKey applet

Important: If you are using Giesecke+Devrient SCE v7.0 smart cards with the CoolKey applet, you cannot use SCE v7.0 smart cards without the CoolKey applet – the cards have the same identifier and cannot be distinguished within MyID. If you install the configuration update for CoolKey support, the cards are identified as "GieseckeDevrient – CoolKey".

Support for the CoolKey applet on these cards requires an additional software update. For information about acquiring this update, contact customer support quoting reference SUP-323.

See the *Giesecke+Devrient smart cards* section in the ***Smart Card Integration Guide***.

7.2.3 iOS operating system versions supported

The list of iOS operating system versions supported for mobile identities has been updated. MyID now supports:

- iOS 17, 16, 15.

See the *Supported devices* section in the ***Mobile Identity Management*** guide for details.

7.2.4   Thales authentication devices

MyID now supports the following devices, using the SafeNet Minidriver 10.8 R9:

- Thales IDPrime 931nc - NXP Mifare EV1 4Kb

- Thales IDPrime 931 FIDO

- Thales IDPrime 941B CC - NXP Mifare EV1 4Kb

- Thales IDPrime 940C

- Thales SafeNet eToken Fusion CC USB Mini

- Thales SafeNet eToken Fusion CC USB-C

- Thales SafeNet eToken Fusion FIPS

- Thales SafeNet eToken Fusion FIPS USB-C

- SafeNet eToken 5110+ CC (940C)

The following existing devices have also been tested using the SafeNet Minidriver 10.8 R9:

- IDPrime MD930 FIPS Level 3

- IDPrime MD3940

- IDPrime MD940

- SafeNet eToken 5300 FIPS (Mini)

- SafeNet eToken 5300 (USB-C)

- SafeNet eToken 5300 (Micro)

See the *Thales authentication devices* section in the ***Smart Card Integration Guide***.

7.3   Improvements

This section provides details of minor improvements to existing functionality within MyID 12.8.0.

7.3.1   General bug fixes and improvements

This release contains general bug fixes and minor improvements as part of a program of continuous improvement.

This release incorporates the following hotfixes:

- HOTFIX-12.4.1.10 – Restricting operator role permissions when self activating a credential.

- HOTFIX-12.5.0.2 – Support for PDF417 Barcodes in card layouts.

- HOTFIX-12.5.0.3 – Entrust PKI Integration improvements.

- HOTFIX-12.5.0.6 – Performance improvements.

- HOTFIX-12.5.0.7 – Improved performance for date range searches on the audit report.

- HOTFIX-12.5.0.8 – System performance and stability improvements.

- HOTFIX-12.6.0.2 – Support for rotated card layout elements and subject entity picklists.

7.3.2 Controlling roles for self-service activation

You can use the **Restrict Self Activation** configuration option (on the **Self-Service** page of the **Security Settings** workflow) to control the roles used for self-service activation. When this options is set to `Yes`, you have access to the operations allowed by the **Activation User** role *only* if these operations are already permitted by your assigned roles; if the **Restrict Self Activation** configuration option is set to `No`, you have access to *all* operations allowed by the **Activation User** role, whether or not your own assigned roles provide access.

See the *Configuring a credential profile for activation* section in the ***Administration Guide***.

7.3.3 Date and time formats in the MyID Operator Client

You can now specify the date and time formats used in the MyID Operator Client by setting the locale for your browser. The MyID Operator Client now picks up the browser's locale setting automatically.

Previously, you had to use the `render_date.date_format` and `render_date.date_time_format` settings using the translation toolkit. This is no longer required.

7.3.4 Device categories

Each device that you work with in MyID now belongs to a *device category*.

When you select the **Card Encoding** for a credential profile, you specify the category. This **Device Category** groups the various card encoding options into logical categories; for example, contact chip cards, contactless cards, and magnetic stripe cards are all treated as part of the **Card** category.

You can use the device category to search for individual devices; most device search reports contain **Device Category** in the **Additional Search Criteria** section. You can also use the **Issued devices by category** report to display the total number of issued devices by device type, including details of their category.

For more information, see the *Working with device categories* section in the ***MyID Operator Client*** guide.

7.3.5 File names for soft certificates

The automatically generated file names for soft certificates have now been improved to prevent any characters being used from the logon name or policy name that would create invalid file names. Any spaces in the file name, or characters that are not valid for file names (that is, `~` or `$` as the first character, or any of the following characters `" < > | : * ? \ /`) are now replaced by underscores.

See the *Customizing certificate file names* section in the ***MyID Operator Client*** guide for details.

7.3.6 Folders for soft certificates

Previously, if you selected a folder into which to download your soft certificates, and the folder already contained a .pfx file with the same name, MyID overwrote the older file without warning.

Now, if you select a folder that already contains .pfx files, the MyID Operator Client displays a warning and allows you to change the folder, ignore the warning, or cancel the operation.

See the *Collecting a soft certificate* section in the ***MyID Operator Client*** guide for details.

7.3.7 License warning levels

The threshold at which license warnings are sent out has been changed so that you now specify the number of remaining available user or credential licenses at which you want MyID to send an email warning; for example, if you have 1000 licenses, you might set the **Warn When Available Licenses Reaches** value to 100, so MyID sends an email to the configured email address when the number of available remaining licenses drops to 100.

See the *License management* section in the *__Administration Guide__*.

7.3.8 Revoking access tokens for the MyID authentication server

You can now use the revocation endpoint to revoke web.oauth2 access tokens used for end-user authentication with the MyID Core API.

See the *Revoking access tokens* section in the *__MyID Core API__* guide for details.

7.3.9 Rotating text in the Card Layout Editor

You can now rotate text fields in the Card Layout Editor using the **Rotate Text** button on the toolbar.

See the *Formatting text* section in the *__Administration Guide__*.

7.3.10 Simplified Microsoft VSC credential profiles

Previously, you could create a credential profile that had both **Contact** and **Microsoft VSC** selected for its **Card Encoding** option. However, the Self-Service App treated such credential profiles as VSC credential profiles, so this was not a recommended configuration (for VSC credential profiles, you were recommended to select **Microsoft VSC** only) and has now been removed as an option to prevent confusion. When you select **Microsoft VSC**, you cannot select any other options (other than **Derived Credential**).

See the *Setting up a credential profile for VSCs* section in the *__Microsoft VSC Integration Guide__*.

When upgrading a system that has a credential profile with both **Contact** and **Microsoft VSC** selected, the credential profile is altered to remove the **Contact** option. If you prefer to use the credential profile for **Contact** cards, you must edit the credential profile before upgrading and remove the **Microsoft VSC** option; you may also wish to copy the credential profile, and edit the credential profiles so that one has **Contact** and the other has **Microsoft VSC** selected.

For more advice on this situation, contact Intercede customer support, quoting reference SUP-378.

7.4 Documentation updates in MyID 12.8.0

This section contains information on new and updated documentation in MyID 12.8.0.

7.4.1 Administration Guide

The **_Administration Guide_** has been updated with the following:

- Added clarification about using the **Allow requests without user data approved** configuration option.

  See the *Allowing device requests before the user's data is approved* and *Issuance Settings* sections.

- Added information about viewing server-generated initial PINs on the View Device screen in the MyID Operator Client.

  See the *PIN generation* section.

- For clarity, the information about using authentication codes for logging on to MyID using the MyID authentication server (for example, the MyID Operator Client, or the MyID Core API) has been split into its own section.

  See the *Logon using authentication codes* section.

- Updated the description for the blue audit icon.

  See the *Running the audit report* section.

- Added new REST notifications for people and requests in addition to devices.

  See the *REST web service notifications* section.

- Updated information about license limits; which now use the **Warn When Available Licenses Reaches** value to trigger email license warnings when the number of remaining available user or credential licenses drops to this value.

  See the *License management* section.

- Added information on working with device categories.

  See the *Card Encoding* section.

- Added information about the **Rotate Text** button in the **Card Layout** Editor.

  See the *Formatting text* section.

- Added information about the new **Restrict Self Activation** configuration option.

  See the *Configuring a credential profile for activation* and *Self-Service page (Security Settings)* sections.

7.4.2 Derived Credentials Self-Service Request Portal

The **_Derived Credentials Self-Service Request Portal_** guide has been updated with the following:

- Corrected the logic for available roles when there is an existing user.

  See the *Credential profile restrictions* section.

7.4.3 Entrust CA Integration Guide

The **Entrust CA Integration Guide** has been updated with the following:

- Added details of support for critical section protection.

  See the *Configuring critical section protection* section.

- Added details of support for the deactivation of card authentication users.

  See the *Deactivation of card authentication users* section.

7.4.4 Error Code Reference

The *Error Code Reference* has been updated with the following:

- Added the following errors:

    - OC10033 – Error notifying the server of sign out. Your client has still been signed out.

    - WS30025 – must be a date in the past within correct range.

    - WS30026 – must be a date in the future within correct range.

    - WS40062 – The device is currently assigned and cannot be reinstated.

    - WS40063 – The device has not previously been assigned and cannot be reinstated.

    - WS40064 – The device is in an invalid state and cannot be reinstated.

    - WS40065 – Device cannot be reinstated because it is not a card.

    - WS40066 – The certificate cannot have its renewal status changed as it is not currently issued.

    - WS50068 – Replacement card has gone too far through issuance to reinstate previous device.

    - WS50069 – The operator does not have sufficient scope to view the requests of this account.

    - WS50070 – The provided certificate cannot be suspended or revoked as it is not currently issued.

    - WS50071 – The provided certificate cannot be suspended or revoked as it has been issued by the 'Unmanaged' certificate authority.

    - WS50072 – You do not have permission to suspend or revoke this certificate.

    - WS50073 – The provided certificate cannot be unsuspended as it is not suspended.

    - WS50074 – You do not have permission to unsuspend this certificate.

    - WS50075 – The provided revocation reason cannot be used for this certificate.

    - WS50076 – The provided certificate cannot be paused as it is not pending issuance or revocation.

    - WS50077 – You do not have permission to pause this certificate.

    - WS50078 – The provided certificate cannot be paused as no retries will be attempted.

    - WS50079 – The provided certificate cannot be resumed as it is not pending issuance or revocation.

    - WS50080 – You do not have permission to resume this certificate.

    - WS50081 – The provided certificate cannot be unsuspended as it has been issued by the 'Unmanaged' certificate authority.

    - WS50082 – The certificate cannot have its renewal status changed as it has been issued by the 'Unmanaged' certificate authority.

    - WS50083 – You do not have permission to change the renewal status of this certificate.

- WS50084 – The maximum number of devices for a given licence has been exceeded.

  See the *MyID Operator Client error codes* section.

- Updated the text for the following error:

  - OC10011 – The item is not available. This may be due to the item changing status, the link no longer being valid or you do not have permission to access this information.

  See the *MyID Operator Client error codes* section.

7.4.5 Installation and Configuration Guide

The ***Installation and Configuration Guide*** has been updated with the following:

- Added instructions for ensuring hotfix and configuration package scripts are trusted.

  See the *Installing a server configuration package* and *Applying a hotfix* sections.

- Added a cross-reference to the client software prerequisites for the MyID Client WebSocket Service.

  See the *Installing the MyID Client WebSocket Service* section.

- Updated information about upgrading systems with customized configuration files

  See the *Upgrading systems with customized configuration files* section.

7.4.6 Microsoft Virtual Smart Card Integration Guide

The ***Microsoft VSC Integration Guide*** has been updated with the following:

- Updated information on setting the card encoding options in the credential profile for VSCs.

  See the *Setting up a credential profile for VSCs* section.

7.4.7 MyID Core API

The ***MyID Core API*** guide has been updated with the following:

- Information about the revocation endpoint that allows you to revoke access tokens.

  See the *Revoking access tokens* section.

7.4.8   MyID Operator Client

The ***MyID Operator Client*** guide has been updated with the following:

- Added information about working with certificates in the MyID Operator Client.

  See the *Working with certificates* and *Certificates report* sections.

- Removed information about launching MyID Desktop certificate workflows that have now been superseded by MyID Operator Client certificate management features.

  See the *Using Certificate Administration workflows* section.

- Updated the details of the automatic file name generation for soft certificates, which now prevent invalid file names from being generated.

  See the *Customizing certificate file names* section.

- Added information about viewing initial server-generated PINs on the View Device screen.

  See the *Viewing the initial PIN for a device* section.

- The **Reinstate Card** workflow in MyID Desktop has now been replaced by the **Reinstate** option on the View Device screen.

  See the *Reinstating a device* section.

- Updated the list of available fields in the Unassigned Devices report.

  See the *Unassigned Devices report* section.

- Updated the list of available fields in the Requests report.

  See the *Requests report* section.

- Updated the list of available fields in the Devices report.

  See the *Devices report* section.

- Updated the list of available fields in the Stock Transfers report.

  See the *Stock Transfers report* section.

- Updated the list of available fields in the Additional Identities (AID) report.

  See the *Additional Identities (AID) report* section.

- Added information about using the **Device History** tab to view the audit trail for a device.

  See the *Viewing a device's history*, *Working with the audit trail*, and *Viewing audit details* sections.

- Updated the information on using the View Full Audit role permission.

  See the *Viewing a person's history* and *Unrestricted Audit Report* sections.

- Added information on working with device categories.

  See the *Working with device categories* and *Issued devices by category report* sections.

- Added the **Device Category** field to the list of additional search criteria in several reports relating to devices.

  See the *Assign Device Search report*, *Assigned Devices report*, *Awaiting Delivery report*, *Devices report*, *Mobile Devices report*, *Requests report*, and *Unassigned Devices report* sections.

- Added information about a warning dialog if the selected folder already contains soft certificate files that may be overwritten.

  See the *Collecting a soft certificate* section.

7.4.9 Mobile Identity Management

The *Mobile Identity Management* guide has been updated with the following:

- Removed a restriction on historic certificates that was due to a limitation of 50 characters on certificate names on Samsung Android devices.

  See the *Setting up support for historic certificates* section.

- Updated the list of iOS versions supported.

  See the *Supported devices* section.

7.4.10 Smart Card Integration Guide

The *Smart Card Integration Guide* has been updated with the following:

- Added information about Giesecke+Devrient SCE v7.0 smart cards with the CoolKey applet.

  See the *Giesecke+Devrient smart cards* section.

- Added information about nine new Thales devices.

  See the *Thales authentication devices* section.

- Deprecated five old Thales devices.

  See the *Thales authentication devices* section.

- Updated the driver version for several existing Thales devices to SafeNet Minidriver 10.8 R9.

7.4.11 Web Service Architecture

The *Web Service Architecture* guide has been updated with the following:

- Updated information about upgrading systems with customized configuration files
  See the *Reverse proxies and load balancing* section.

7.5 End of support features in MyID 12.8.0

This section contains information about features that are no longer supported in MyID as of MyID 12.8.0.

There are no end of support features in this release.

7.6 Known issues resolved in MyID 12.8.0

This section lists the known issues that have been resolved in MyID 12.8.0. These are issues that were found across both editions of MyID – Enterprise and PIV – and may not all be relevant for your system.

- IKB-372 – Error occurs on collection of software certificates when invalid characters are in the file name.

- IKB-373 – A Print PIN Mailer Document request is created when a soft certificate is issued even if the credential profile is not configured for mailing documents.

8 Updates in MyID 12.7.0

This chapter provides details of the changes in MyID 12.7.0, including:

- New and updated features – new features in this version of MyID, and major improvements to existing features.

- Integration updates – updates to MyID's support for smart cards and other credentials, certificate authorities, printers, and HSMs.

- Improvements – minor updates to existing functionality.

Important: At MyID version 12.3, the version of .NET Core used was updated. This affects the MyID servers and all clients. See section *13.3.7*, *.NET Core versions* for details.

Important: Microsoft is making changes to DCOM security over the course of releases in 2021 to 2023 that may affect your system, depending on your configuration. See section *13.2.2*, *Microsoft Windows DCOM server security changes* for details.

8.1 New and updated features

This section contains information on the new and updated features in MyID 12.7.0.

8.1.1 Additional identities in the MyID Operator Client

Previously, you could manage additional identities in the MyID Operator Client by launching the **Manage Additional Identities** and **Manage My Additional Identities** workflows in MyID Desktop.

This feature allows a secondary identity to be provided for a person's user account in MyID, so that certificates for that identity can be issued and stored on the same device as the primary identity. For example, where a person also has privileged access accounts for system administration or secure system access. This is also useful where different certificate-based credentials are required by systems that are not directly connected to your local infrastructure.

You can now use the **Additional Identities** tab on the View Person screen in the MyID Operator Client to manage your additional identities without having to launch MyID Desktop. Previously you could import additional identities from your directory; now, as an alternative, you can create and edit additional identities manually.

In the MyID Operator Client, you can now:

- Create an additional identity manually, providing all the details without importing the record from a directory.

- Edit an additional identity that you have created manually.

- Import an additional identity from a directory.

- Remove an additional identity.

When importing an additional identity, you can use the following configuration options to filter the results returned from the directory:

- **Additional Identity LDAP Operator User Filter** – restricts the active directory user accounts that are available for selection when adding an additional identity for another person. This uses LDAP Search Filter syntax, providing a highly configurable mechanism to ensure only appropriate accounts can be selected; for example members of a particular directory security group or organizational unit.

- **Additional Identity LDAP Self-Service User Filter** – restricts the active directory user accounts that are available to those that match a specified pattern when compared to attributes of the self-service user. This also uses LDAP Search Filter syntax, and can provide accounts that match part of the self-service user's logon name.

Important: These LDAP user filters are applicable only when using the **Import Additional Identity** feature in the MyID Operator Client; these settings do not affect the **Manage Additional Identities** workflow in MyID Desktop.

For more information, see the *Working with additional identities* chapter in the *MyID Operator Client* guide.

You can also use the MyID Core API to manage your additional identities; for example:

- `POST /api/People/{id}/additionalIdentities` to create a new additional identity for a person.

- `PATCH /api/AdditionalIdentities/{id}` to edit an additional identity for a person.

For information about accessing the MyID Core API, see the *MyID Core API* guide. See the *Accessing the API documentation* section for details of viewing the API documentation.

8.1.2 Accepting delivery for devices

If your system is set up for a delivery stage within the device issuance process that allows you to confirm that the device has been delivered to the applicant, you must mark a device as delivered before it can be activated. The request job remains at the Awaiting Delivery status until you have confirmed that the device has been delivered.

Previously, you could launch the **Deliver Card** workflow from the MyID Operator Client. This feature has been superseded by the new **Accept Delivery** feature in the MyID Operator Client, which allows you to accept delivery for a device from the View Device screen. You can also accept delivery for a batch of devices; the new **Awaiting Delivery** report assists with this process.

See the *Accepting delivery for a device* section in the *MyID Operator Client* guide.

8.1.3 Batch operations

You can now carry out the following operations on multiple items in the MyID Operator Client:

- Request devices.

  See the *Requesting devices for multiple people* section.

- Request mobile devices.

  See the *Requesting mobile devices for multiple people* section.

- Request updates.

  See the *Requesting updates for multiple devices* section.

- Cancel devices.

  See the *Canceling multiple devices* section.

- Approve requests.

  See the *Approving multiple requests* section.

- Reject requests.

  See the *Rejecting multiple requests* section.

- Add people from a directory.

  See the *Adding multiple people from a directory* section.

- Set the disposal status of devices.

  See the *Setting the disposal status of multiple devices* section.

- Accept delivery of devices.

  See the *Marking multiple devices as delivered* section.

See the relevant section of the *MyID Operator Client* guide for details.

8.1.4 Controlling device assignments for groups

You may want to control the use of device assignments for individual groups; for example, you may have multiple subsidiary organizations using your MyID system, but you may want to restrict one of the organizations to have a maximum number of devices, and to be able to assign and issue those devices for a limited time.

This feature helps control device assignments for individual group, but it does not override or modify how MyID system licenses are consumed, which are calculated for the entire installation.

To do this, you can create a new group to which you assign all users from that organization, or use an existing group that contains all users from that organization. Create or amend the group using the **Add Group** or **Amend Group** workflows, and set the **Device Assignment End Date** and **Maximum Number of Assigned Devices** options.

You can also set these options through the MyID Core API by setting the `deviceLimit` and `expiryDate` options when adding or editing a group.

You can use the **Assigned Devices by Group** report in the MyID Operator Client to help manage these device assignments. This report lists each group that has devices assigned or issued to it, and displays the limits you have set on the group.

See the *Controlling device assignments for groups* section in the ***Administration Guide*** for details.

8.1.5 Device disposal

You can now set the device disposal status when canceling a device in the MyID Operator Client, and change the disposal status of a canceled device. To assist in managing the disposal status of your devices, the **Device Disposal** report is provided.

See the *Canceling a device*, *Disposing of a device*, and *Device Disposal report* sections in the ***MyID Operator Client*** guide.

8.1.6 Importing people from a directory

Previously, to add a person from a directory to the MyID database using the MyID Operator Client, you could search for a person in the directory then use the Edit Person option; saving the person's details imported the person into the MyID database.

You can now import people from a directory in the following additional ways:

- On the View Person (Directory) screen, select one of the following options:
  - **Request Mobile** or **Request Mobile (View Auth Code)** – imports the person and request a mobile device.
  - **Request Device** – imports the person and request a device.
  - **Import** – imports the person from the directory.
- On the **Tools** menu of the People search results screen:
  - **Import** – imports multiple people at the same time in a batch.

See the *Adding a person* section in the ***MyID Operator Client*** guide.

8.1.7 Inventory management

The inventory control feature allows you to set up locations within your organization, to assign stock of devices to these locations, to set minimum stock levels and re-order quantities, to transfer stock between locations, and to view reports on your inventory.

See the *Working with inventory management* section in the *MyID Operator Client* guide.

8.1.8 Requesting a device cancellation

You can now request the cancellation for a device in the MyID Operator Client. This allows you to cancel a device if the credential profile that was used to issue it had the **Validate Cancellation** option set.

Note: The device remains active and available for use until the cancellation request is approved. If the request is rejected, no cancellation takes place.

See the *Requesting a cancellation for a device* section in the *MyID Operator Client* guide.

8.1.9 Reviewing requests

MyID provides a new report, **Requests for review**, that provides a list of all requests that are awaiting validation. You can then either approve, reject, or cancel these requests individually, or in a batch.

See the *Requests for review report* and *Approving, rejecting, and canceling requests* sections in the *MyID Operator Client* guide. .

8.1.10   Soft certificates

MyID now allows you to request, collect, and manage soft certificate packages in the MyID Operator Client. This feature has been substantially enhanced, and you can now print transport and PIN mailer documents from the MyID Operator Client, and automatically save soft certificate files to attached USB drives.

New reports are provided to assist with printing and reprinting mailing documents.

Certificate file names are now automatically generated, whereas previously you were required to provide the file name at the point of issuance; this streamlines the issuance process. You can customize the format used for these file names, including using substitutions for personal information and dates and times.

Important: Collecting soft certificates in the MyID Operator Client requires the MyID Client Service to be running on the client, and the rest.provision web service to be running on the web server. In addition, you must have the WebView2 component installed on the client PC to be able to print transport or mailing documents; see the *Microsoft WebView2 Runtime* section in the ***Installation and Configuration Guide**.

See the *Working with soft certificates* section in the ***MyID Operator Client**** guide for details of requesting, collecting, and managing soft certificate packages, including printing transport and PIN mailing documents, and configuring file names for certificate packages. See the *Print PIN Mailer report* and *Reprint PIN Mailer report* sections in the ***MyID Operator Client**** guide for details of the new reports.

Important: There are changes to the credential profile configuration for soft certificates; you must review your credential profiles to ensure that they are suitable for your requirements.

In particular, previous versions of MyID had the following options for **Storage Method** for certificate policies for soft certificates:

- **Local Store** – equivalent to **SystemStore** in the current version.

- **Password Protected PFX File** – equivalent to **FileStore** in the current version.

- **Choose During Issuance** – no longer supported. Certificate policies that were marked as **Choose During Issuance** are treated as **FileStore** when you attempt to collect them in the MyID Operator Client, and are updated to specify **FileStore** when you modify the credential profile.

See the *Setting up a credential profile for soft certificates* section in the ***Administration Guide**** for details of setting up a credential profile that allows you to issue software certificate packages.

Note: By default, when MyID issues software certificates, it encrypts the passwords protecting the PFX files using AES256/SHA2. However, some Operating Systems do not support this modern security standard, which creates a problem when importing the certificates onto these; for example, any Apple OS (macOS or iOS), any Windows Server OS lower than Windows 2019, and any Windows client OS lower than Windows 10 build 1709. If you want to import software certificates onto an OS that does support not the encryption of PFX files using AES256/SHA2, you must set the **Use SHA1 encryption for certificates issued as PFX files** option in the **Server** tab of the **Security Settings** workflow to `Yes`.

8.2 Integration updates

This section contains details of updates to MyID 12.7.0's support for integration with smart cards and other credentials, certificate authorities, printers, and HSMs.

8.2.1 Configurable PROX support

The mechanism used to read contactless proximity (PROX) data from smart cards has been modified in this release. Currently supported PROX card formats will continue to operate as before, but it is now possible to configure MyID to recognize additional serial number formats.

Advanced configuration of MyID is required for this feature; contact Intercede quoting SUP-77 for further information.

8.2.2 Entrust nShield HSMs in FIPS 140-2 L3 mode

MyID now supports HSMs running in FIPS 140-2 L3 mode. When using this mode, the HSM does not allow 3DES and RSA 1024.

This release of MyID has been tested with the following Entrust nShield configuration:

nShield Model	Security World Client	Connect Image	Security World Version	FIPS Certified	FIPS Firmware
Connect XC	12.80.4	12.80.5	v3 - DLf3072s256mAEScSP800131Ar1	Yes	12.72.1

If you are using a different configuration of the nShield HSM, you are recommended to use the HSM Test Utility to validate integration

See the *Hardware and software requirements* section of the ***Entrust nShield HSM Integration Guide*** for details.

8.2.3 Escrow support in DigiCert ONE

MyID now supports escrow for certificates issued through DigiCert ONE, allowing the certificates to be archived and then recovered at a later time. This feature requires additional permissions to be set up in the DigiCert portal.

See the *Configuring permissions for escrow* section in the ***DigiCert ONE Integration Guide*** for details.

8.2.4 PrimeKey EJBCA versions

The current version of MyID has been tested with:

- PrimeKey EJBCA Enterprise PKI version 7.11.01.

See the *Supported PrimeKey EJBCA versions* section of the ***PrimeKey EJBCA Integration Guide***.

8.2.5 SQL Authentication

You can now use SQL Authentication instead of Windows Authentication when configuring how the MyID application server communicates with the database server for all types of MyID system. Previously, SQL Authentication was supported only on systems using SQL Azure.

See the *Configuring SQL Server for SQL Authentication* section in the ***Installation and Configuration Guide*** for details.

8.2.6 SQL Server 2022

You can now use SQL Server 2022 as the database for MyID.

See the *Database versions* section of the ***Installation and Configuration Guide*** for details.

8.2.7 Thales authentication devices

MyID now supports the following devices:

- SafeNet eToken 5110+ CC (940B)

See the *Thales authentication devices* section in the ***Smart Card Integration Guide***.

8.2.8 Thales SC650 – CoolKey devices

MyID now supports the following Thales Trusted Cyber Technologies devices:

- SC650 V4.2 smart cards with the CoolKey applet

Important: If you are using SC650 V4.0 or V4.2 smart cards with the CoolKey applet, you cannot use SafeNet SC650 V4.1 (90M) smart cards – the cards have the same identifier and cannot be distinguished within MyID. If you install the configuration update for CoolKey support, the cards are identified as "SC650 – CoolKey". In addition, the SC650 V4.0 and V4.2 smart cards appear as the same device type, but have different GlobalPlatform key requirements. You cannot mix types of SC650 smart card on your system.

Support for the CoolKey applet on these cards requires an additional software update. For information about acquiring this update, contact customer support quoting reference SUP-323.

See the *Thales Trusted Cyber Technologies smart cards* section in the ***Smart Card Integration Guide***.

8.3 Improvements

This section provides details of minor improvements to existing functionality within MyID 12.7.0.

8.3.1 General bug fixes and improvements

This release contains general bug fixes and minor improvements as part of a program of continuous improvement.

8.3.2 Customizing the number of Add buttons

By default, the MyID Operator Client displays up to two **Add** buttons; for example, you may have a customized system with different types of People you can add. If there are additional options, these are available using the **...** option. You can adjust the number of displayed **Add** buttons; for example, you may have three different types of people, and want all three **Add** buttons to be visible.

See the *Changing the number of Add buttons* section in the ***MyID Operator Client*** guide.

8.3.3 MyID Client Service configuration options

The MyID Client Service now has the following additional options that allow you to configure the behavior when printing mailing documents or saving soft certificates:

- `AllowAutoSave` – determines whether MyID can select an external drive to which it can write soft certificates.
- `AllowedSaveFileExtensions` – provides a list of allowed file extensions that you can use to write soft certificates to a file.
- `AllowPrintWithoutConfirm` – determines whether MyID can print a mailing document silently without confirmation.
- `EmptyDriveIgnoreRecycleBin` – determines whether MyID can ignore the Recycle Bin when checking if an external drive is empty.
- `EmptyDriveIgnoreVolumeInformation` – determines whether MyID can ignore the special `VolumeInformation` directory that Windows adds to all drives by default when checking if an external drive is empty.

See the *Configuring certificate saving and printing* section in the ***MyID Operator Client*** guide.

8.3.4 Server restart check

The System Interrogation Utility has been updated with SIU-099, which checks whether the server needs to be restarted before installing MyID. Pending updates may interfere with the MyID installation process.

See the *Restarting your servers* section of the ***Installation and Configuration Guide*** for details.

8.3.5 Upgrading client software

This release of MyID uses a new code signing certificate; this means that if you install the MyID Client Service for the current release, you *must* also install the corresponding versions of all other MyID client software from this release.

The reason for this is that the MyID Client Service validates the signatures of external applications (for example, MyID Desktop and the Self-Service App) and as a result will refuse to load the applications in the event of a mismatch of versions; you are recommended to upgrade all of your client software to the versions provided in this release.

You can identify this issue in the MyID Client Service logs; an error similar to the following:

```
Client signature is not trusted
```

indicates that the MyID Client Service did not recognize the certificate used by the client software.

This situation also occurs when managing VSCs. If you are using the client applications provided with this release of MyID, you must also upgrade your Windows Integration Service (WSVC) software to the matching version provided with this release of MyID.

You may want to consider the benefits of MSIX installation for automatically updating your client software; see the *Configuring automatic updates* section in the ***MyID Client MSIX Installation Guide***.

8.4 Documentation updates in MyID 12.7.0

This section contains information on new and updated documentation in MyID 12.7.0.

8.4.1 Administration Guide

The *Administration Guide* has been updated with the following:

- Added information about the options for controlling licenses for individual groups.

  See the *Controlling device assignments for groups* section.

- Clarified that the **Proximity Card Check** option in the credential profile affects collection only using the **Collect Card** and **Batch Collect Card** workflows.

  See the *Issuance Settings* section.

- Updated advice relating to the **Display warnings for unsecured issuance** configuration option.

  See the *Device Security page (Security Settings)* section.

- Updated the information on additional identities to refer to the new additional identities features in the MyID Operator Client.

  See the *Additional identities* chapter.

- Added the **Additional Identity LDAP Operator User Filter** and **Additional Identity LDAP Self-Service User Filter** configuration options.

  See the *LDAP page (Operation Settings)* section.

- Clarified the lists used for identity documents.

  See the *Setting up authentication methods for activation* and *Changing list entries* sections.

- Added a note about replacement certificate policies having the same requirements as the policies they are superseding.

  See the *Superseding certificate policies* section.

- Updated the details for creating a credential profile for soft certificates.

  See the *Setting up a credential profile for soft certificates* section.

- Updated the instructions for creating a credential profile to cover selecting templates for print mailing documents and transport documents for soft certificate packages.

  See the *Working with credential profiles* section.

- Added details of the **Import Devices Sequential Range Limit** configuration option.

  See the *Import & Export page (Operation Settings)* section.

8.4.2 Derived Credentials Self-Service Request Portal

The *Derived Credentials Self-Service Request Portal* guide has been updated with the following:

- Added error numbers `0010` and `0011`.

  See the *Error code reference* section.

- Added information on disabling TLS 1.3.

  See the *Disabling TLS 1.3* section.

8.4.3   DigiCert ONE Integration Guide

The *DigiCert ONE Integration Guide* has been updated with the following:

- Added a statement that MyID integrates with DigiCert ONE using the DigiCert® Trust Lifecycle Manager REST API.

  See the *Introduction* section.

- Added information about escrow support.

  See the *Configuring permissions for escrow* and *Escrow error messages* sections.

- Added details of the new **Dual Control for Key Recovery** option.

  See the *Configuring the CA in the Certificate Authorities workflow* section.

8.4.4   Entrust CA Gateway

The *Entrust CA Gateway Integration Guide* has been updated with the following:

- Clarified support for certificate authorities that have not been tested by Intercede.

  See the *Supported Entrust CA Gateway versions* section.

8.4.5   Entrust CA Integration Guide

The *Entrust CA Integration Guide* has been updated with the following:

- Removed obsolete **Entrust Enabled** configuration setting.

  See the *Prerequisites* section.

- Added troubleshooting for Card Server Error During Process error.

  See the *Troubleshooting error messages* section.

8.4.6   Entrust nShield HSM Integration Guide

The *Entrust nShield HSM Integration Guide* has been updated with the following:

- Removed the limitations relating to encryption using an AES transport key.

  See the *Hardware and software requirements* section.

- Added information about support for FIPS 140-2 L3 mode.

  See the *Hardware and software requirements* section.

- Added detail about the tested Entrust nShield configuration.

  See the *Hardware and software requirements* section.

- Added restrictions relating to using the CSP with FIPS 140-2 L3 mode.

  See the *Install nShield CSP* section.

8.4.7 Error Code Reference

The *Error Code Reference* has been updated with the following:

- Added the following errors:

  - OC10019 – A problem occurred when collecting the certificates. Please retry the operation.

  - OC10020 – A problem occurred when collecting the certificates. Please retry the operation.

  - OC10021 – A problem occurred when collecting the certificates. Please retry the operation.

  - OC10022 – A problem occurred when collecting the certificates. Please retry the operation.

  - OC10023 – A problem occurred when collecting the certificates. Please retry the operation.

  - OC10024 – A problem occurred when collecting the certificates. Please retry the operation.

  - OC10025 – A problem occurred when collecting the certificates. Please retry the operation.

  - OC10026 – A problem occurred when collecting the certificates. Please retry the operation.

  - OC10028 – The printer is unavailable. Please check the printer is operational and not in use.

  - OC10029 – The printer reported the print operation has failed. Please see the printer for further details.

  - OC10030 – The MyID Client Service was unable to read the document.

  - OC10031 – The MyID Client Service was unable to read the document.

  - OC10032 – A problem occurred when collecting the certificates. Please retry the operation.

  - WS10006 – Unable to substitute values, entity name invalid.

  - WS10007 – Unable to substitute values, field name invalid.

  - WS30024 – Serial number range information must be supplied.

  - WS40048 – The location cannot be updated because an existing location has the requested name.

  - WS40049– The device cannot be transferred because it is in an invalid state.

  - WS40050 – The device cannot be canceled and have its disposal status set to <Status>.

  - WS40051 – The device is still active and has not expired, so cannot have its disposal status changed.

  - WS40052 – The device has expired but the system is configured to not allow expired devices to have their disposal status changed.

- WS40053 – The device selected cannot be disposed. Please refer to product documentation for further guidance.

- WS40054 – The additional identity specified already exists.

- WS40055 – The request doesn't have an assigned device.

- WS40056 – The credential profile does not have a document for the requested doctype.

- WS40057 – Unable to generate a server document, the request type is invalid.

- WS40058 – Unable to generate a server document, the status of the request is invalid.

- WS40059 – Unable to generate a server document, the collection period is over.

- WS40060 – Unable to generate a server document, PIN Mailer request not found.

- WS40061 – Unable to generate a server document, unknown document type.

- WS50050 – The request is not at a valid status for this operation.

- WS50057 – The user has an existing request or device that exists with a different exclusive group, the request cannot be collected.

- WS50059 – The selected user has no fingerprint rolls available for EFT export.

- WS50060 – Maximum number of generated sequential serial numbers exceeded.

- WS50061 – The attempt to assign a device has been rejected. The device assignment end date for the group that this person is associated with has passed.

- WS50062 – The attempt to assign a device has been rejected. The maximum number of assigned devices for the group that this person is associated with has been exceeded.

- WS50063 – The selected directory person is already in the MyID database.

- WS50064 – You are not allowed to deliver this device.

- WS50065 – The device already has an active request.

- WS50067 – The selected certificate policy does not allow identity mapping.

See the *MyID Operator Client error codes* section.

- Added the following errors:

  - 21777 – This job can not be collected as a self-service operation as it requires countersigning.

  - 890703 – The attempt to assign a device has been rejected. The device assignment end date for the group that this person is associated with has passed.

  - 890704 – The attempt to assign a device has been rejected. The maximum number of assigned devices for the group that this person is associated with has been exceeded.

See the *Web Service error codes* section.

- Updated the possible causes of the following error:

  - -99910011 – The printer failed to print the selected layout. Please contact your system administrator.

See the *Printer error codes* section.

- Extended the causes and workarounds for the following errors:
    - OC10006 – MyID Client Service error.
    - OA10007 – Your OTP has been entered incorrectly, is locked, has expired, or you do not have permission to perform this operation. Please try again.

    See the *MyID Operator Client error codes* section.

8.4.8 FIDO Authenticator Integration Guide

The *FIDO Authenticator Integration Guide* has been updated with the following:

- Information on checking the feature delegation options in IIS.

    See the *Checking IIS configuration* section.

- Added a statement that MyID can work with any FIDO compatible authenticator that meets the technical standards set by the FIDO Alliance.

- See the *Supported authenticators* section.

8.4.9 Installation and Configuration Guide

The *Installation and Configuration Guide.pdf* has been updated with the following:

- Clarified the PowerShell version requirements.

    See the *Running post-install PowerShell scripts* section.

- Added instructions for configuring SQL Server for SQL Authentication.

    See the *Configuring SQL Server for SQL Authentication* section.

- Updated the list of supported SQL Server versions to include SQL Server 2022.

    See the *Database versions* section.

- Added WebView2 as a requirement for using the MyID Operator Client for printing mailing documents.

    See the *Client workstation* section.

- Added instructions for restarting the servers before installing MyID.

    See the *Restarting your servers* section.

- Updated the description for the rest.provision web service to state that is now used for collecting soft certificates as well as mobile identities.

    See the *Selecting the server roles and features*, *Modifying the installation*, and *Checking the web services* sections.

- Removed SQL Server 2016 from the list of supported database versions.

    See the *Database versions* section.

- Added a note that the Microsoft Visual C++ Redistributable is prerequisite for the Microsoft OLE DB Driver 19 for SQL Server.

    See the *Installing the database software* section.

8.4.10 Microsoft Azure Integration Guide

The ***Microsoft Azure Integration Guide*** has been updated with the following:

- Moved the SQL Authentication requirements out of the document into the Installation and Configuration Guide.

  See the *Prerequisites* section.

8.4.11 Mobile Authentication

The ***Mobile Authentication*** guide has been updated with the following:

- Updated details of supported server operating systems for the AD FS Adapter

  See the *AD FS Adapter Mobile* and *Managing themes* sections.

8.4.12 MyID Authentication Guide

The ***MyID Authentication Guide*** has been updated with the following:

- Added a clarification about allowing users to skip the MyID Authentication screen if only one logon mechanism is available.

  See the *Configuring authentication to skip the MyID Authentication screen* section.

8.4.13　MyID Operator Client

The ***MyID Operator Client*** guide has been updated with the following:

- Added information about importing devices.

  See the *Importing a range of devices*, *Importing devices from a manifest file*, and *Viewing imported devices* sections.

- Added information about inventory control features.

  See the *Working with inventory management* section.

- Added information about the locations feature.

  See the *Working with locations* section.

- Added information about stock limits.

  See the *Working with stock limits* section.

- Added information about transferring stock.

  See the *Working with stock transfers* section.

- Added new reports for inventory control.

  See the *Available Device Stock report*, *Device Import Requests report*, *Locations report*, *Stock Limits report*, *Stock Per Location report*, and *Stock Transfers report* sections.

- Added information about the **Accept Delivery** feature. This supersedes the ability to launch the **Deliver Card** workflow, which has now been removed from the MyID Operator Client.

  See the *Accepting delivery for a device* section.

- Added information on the new Awaiting Delivery report.

  See the *Awaiting Delivery report* section.

- Added details of the `numberOfAddActionsShown` option that allows you to customize the number of **Add** buttons displayed.

  See the *Changing the number of Add buttons* section.

- Added the Assigned Devices by Group report.

  See the *Assigned Devices by Group report* section.

- Added details about importing people from a directory, including importing batches of people.

  See the *Adding a person from a directory* and *Adding multiple people from a directory* sections.

- Added details of requesting devices for multiple people.

  See the *Requesting devices for multiple people* section.

- Added details of requesting mobile devices for multiple people.

  See the *Requesting mobile devices for multiple people* section.

- Added details of requesting updates for multiple devices.

  See the *Requesting updates for multiple devices* section.

- Added details of canceling multiple devices.

See the *Canceling multiple devices* section.

- Added details of approving and rejecting multiple requests.

  See the *Approving multiple requests* and *Rejecting multiple requests* sections.

- Added information about setting device disposal status.

  See the *Canceling a device*, *Disposing of a device*, and *Device Disposal report* sections.

- Added information about MyID Client Service configuration options relating to printing mailing documents and saving soft certificates.

  See the *Configuring certificate saving and printing* section.

- Added troubleshooting information on resolving mismatched client software versions due to a change in the code signing certificate.

  See the *Mismatched client software versions* section.

- Added the Requests for review report.

  See the *Requests for review report* section.

- Added information on the **Request Cancel** option.

  See the *Requesting a cancellation for a device* section.

- Added information about the new additional identities features in the MyID Operator Client, and removed the links from the MyID Operator Client to the MyID Desktop **Manage Additional Identities** and **Manage My Additional Identities** workflows.

  See the new *Working with additional identities* chapter, and the *Additional Identities (AID) report* section.

- Added information on the new soft certificate collection process in the MyID Operator Client, including printing mailing documents.

  See the new *Working with soft certificates* chapter, and the *Print PIN Mailer report* and *Reprint PIN Mailer report* sections.

- Added details of the **Import Devices Sequential Range Limit** configuration option.

  See the *Importing a range of devices* section.

8.4.14 Operator's Guide

The ***Operator's Guide*** has been updated with the following:

- Added information about the options for controlling licenses for individual groups.
  See the *Adding a group* and *Changing a group* sections.

- Clarified the lists used for identity documents.
  See the *Authenticating users* and *Unlocking cards and resetting PINs* sections.

- Added further troubleshooting information for printing card layouts.
  See the *Troubleshooting card layout preview issues* section.

8.4.15   PrimeKey EJBCA Integration Guide

The *PrimeKey EJBCA Integration Guide* has been updated with the following:

- Added information setting the minimum password strength for the Key Management end entity.

  See the *Configuring end entity profiles* section.

- Added troubleshooting information for problems with certificate policies.

  See the *Troubleshooting certificate policies* section.

- Added a note on support for integration with other certification authorities and HSMs.

  See the *PrimeKey integration with other certification authorities and HSMs* section.

- Updated the required setting for the **Allow subject DN override by End Entity Information** configuration to **Enabled**.

  See the *Configuring certificate profiles* section.

- Added information about repeated policy attributes.

  See the *Repeated policy attributes* section.

- Added information about removing attributes.

  See the *Removing attributes* section.

8.4.16   Smart Card Integration Guide

The *Smart Card Integration Guide* has been updated with the following:

- Added information about SafeNet eToken 5110+ CC (940B) tokens.

  See the *Thales authentication devices* section.

- Updated the details of eToken 5300 devices – they do not support on-device PIN policies.

  See the *Supported features for Thales authentication devices* and *PIN policy settings* sections.

- Added information about support for SC650 V4.2 devices with the CoolKey applet.

  See the *Thales Trusted Cyber Technologies smart cards* section.

- Updated the recommended PIV 9B customer key diversity algorithm for YubiKey SC and YubiKey SC FIPS devices to be DiverseYB108 for devices with diverse factory keys *and* static factory keys. Previously Diverse2 was recommended for YubiKey SC and YubiKey SC FIPS devices with static factory keys.

  See the *Cryptographic keys for Yubico cards* section.

8.4.17   System Interrogation Utility

The ***System Interrogation Utility*** guide has been updated with the following:

- Added test SIU-099 to cover checking whether the server requires a restart before installing MyID.

  See the *Description of derived tests* section.

- Updated tests SIU-009 and SIU-010 to state that SQL Server 2016 causes a warning due to being end of support.

  See the *Description of derived tests* section.

8.4.18   System Security Checklist

The ***System Security Checklist*** has been updated with the following:

- Updated advice relating to the **Display warnings for unsecured issuance** configuration option.

  See the *Securing Devices* section.

8.4.19   Thales Luna HSM Integration Guide

The ***Thales Luna HSM Integration Guide*** has been updated with the following:

- Updated the version of DPoD client software to v10.5.0-470.

  See the *Supported Thales Luna HSM models* section.

- Updated the version of Luna HSM Client software to 10.4.1.

  See the *Supported Thales Luna HSM models* section.

- Removed the limitations relating to encryption using an AES transport key.

  See the *What is needed?* section.

8.5   End of support features in MyID 12.7.0

This section contains information about features that are no longer supported in MyID as of MyID 12.7.0.

See:

- section *8.5.1*, *SQL Server 2016*.

8.5.1   SQL Server 2016

Support for SQL Server 2016 as the MyID database has now ended. MyID makes use of features that are available only in SQL Server 2017 onwards.

See the *Database versions* sections in the ***Installation and Configuration Guide*** for details of supported server operating systems.

8.6   Known issues resolved in MyID 12.7.0

There are no known issues resolved in this release.

9 Updates in MyID 12.6.0

This chapter provides details of the changes in MyID 12.6.0, including:

- New and updated features – new features in this version of MyID, and major improvements to existing features.

- Integration updates – updates to MyID's support for smart cards and other credentials, certificate authorities, printers, and HSMs.

- Improvements – minor updates to existing functionality.

Important: At MyID version 12.3, the version of .NET Core used was updated. This affects the MyID servers and all clients. See section *13.3.7*, *.NET Core versions* for details.

Important: Microsoft is making changes to DCOM security over the course of releases in 2021 to 2023 that may affect your system, depending on your configuration. See section *13.2.2*, *Microsoft Windows DCOM server security changes* for details.

9.1 New and updated features

This section contains information on the new and updated features in MyID 12.6.0.

9.1.1 Checking card suitability

You can configure MyID to call out to an external web service before collecting, updating, or activating a device, passing details of the device and the cardholder so that the external web service can determine whether the collection, update, or activation can proceed.

Using your own web service, you can carry out checks on the device and the cardholder to ensure that your organization's business processes have been followed before providing them with credentials for access.

For example, you may have a list of device serial numbers that should be retired; when the operator inserts the card, MyID passes the serial number to the web service, which is then checked against the list. If the device should be retired, the web service passes a response to MyID that the device is not suitable.

You must write your own web service to receive the request from MyID, check that the device is suitable, and respond to the MyID server.

See the *Checking card suitability* section in the *Administration Guide* for details.

9.1.2 Credential Web Service methods

The Credential Web Service has been updated with the following new methods, which allow systems to request and collect certificates from a certificate authority connected to MyID:

- The `RequestCertificate` method requests a non-archived "Software Certificate" for the specified user, for use as a .CER certificate.

  See the *RequestCertificate* section.

- The `GetCertificate` method collects a CRT "Software Certificate" P7 for the specified request, for use as a .CER/.CRT certificate.

  See the *GetCertificate* section.

- The `RequestCertificatePfx` method requests a PFX "Software Certificate" P12 for the specified user, for use as a .PFX certificate.

  See the *RequestCertificatePfx* section.

- The `GetCertificatePfx` method collects a Password Protected PFX "Software Certificate" P12 for the specified request, for use as a .PFX certificate.

  See the *GetCertificatePfx* section.

- The `IsAlive` method is used to determine if the Credential Web Service is running and able to connect to the database through COM.

  See the *IsAlive* section.

The ***Credential Web Service*** guide has also been updated with new error messages relating to these methods; see the *Error messages* section.

9.1.3 Displaying user images and full names in the Select Security Device dialog

When you click **Read Card** in the MyID Operator Client, the Select Security Device dialog now displays the cardholder's user image and full name along with the device serial number if you have scope or administrative group permissions that allow you to manage the owner of the device.

In addition, you can set the **Show Full Name at Logon** and **Show Photo at Logon** options (on the **Logon** page of the **Security Settings** workflow) to configure this screen to display the associated user image and full name of the cardholder, even if you do not have scope or administrative group permissions that allow you to manage the owner of the device.

See the *Reading a device* section in the ***MyID Operator Client*** guide.

You can also use the MyID Client Service API to launch the Select Security Device dialog as an authenticated session that allows you to view the user images and full names if the operator has the appropriate permissions; you must obtain an extension grant and then use the resulting access token to call the API. See the *Obtaining an extension token for Select Security Device* section in the ***MyID Core API*** guide for details.

Note: This feature requires an updated version of the MyID Client Service. You must have the version provided with MyID 12.6 (MCS-1.9.1000.1) or later. If you do not have a supported version installed, the behavior is as in previous versions: the Select Security Device dialog does not display the cardholder's user image and full name.

9.1.4 Enforcing banned words in user PINs

For user specified PINs, you can select the **Enforce Banned Words** option in the **PIN Settings** section of the **Credential Profiles** workflow to prevent the user from using particular words in their PINs.

The banned words include dynamic words (for example, the device serial number, or the person's logon name) and a static word list (for example, `password` or `admin`).

See the *Enforcing banned words in PINs* section in the ***Administration Guide*** for details.

9.1.5 Group selection enhancements

Group selection in MyID has been enhanced with the following features:

- You can display descriptions rather than names in the Group selection dialog.

- You can select a group from a drop-down list rather than a hierarchical tree view; you can choose to select the group by name or description.

- When selecting from a drop-down list, you can type in the box to filter the results.

- Once you have selected a group, if it has a description, it is displayed below the Group box.

These features relate to groups in the MyID database, not groups in your directory; for example, when searching for a person in MyID, or selecting the group for a device or request.

See the *Selecting a group* section in the ***MyID Operator Client*** guide.

9.1.6   Microsoft KB5014754 and user security identifiers

MyID now allows you to import user security identifiers (user SIDs) from your directory and store them as part of a person's record in MyID. When you add a person from a directory, or perform a directory synchronization, the user SID is updated in the person's record.

You can include the user SID in the attribute mappings for certificate templates for Microsoft and PrimeKey EJBCA CAs. This is important to ensure compliance with the authentication requirements relating to Microsoft *KB5014754*.

User SIDs affect the following areas:

- Importing people from directories.

- Synchronizing directory information.

- Importing user SIDs through APIs.

- Storing user SIDs for additional identities.

- Specifying a user SID as a required attribute for a credential profile.

- Issuing certificates using the user SID as an extended attribute.

You can view or edit a person's SID on the **Account** tab for a person's record in the MyID Operator Client, and the SID for a person's additional identity on the **Additional Identities (AID)** report..

Previous versions of MyID did not import, synchronize, or store the user SID, or use the user SID to issue certificates. You may have to synchronize the people in your system with the directory and update your CA configuration to make use of this feature.

The **People** search report in the MyID Operator Client has been extended to include a new additional search criterion **User SID Present** to assist with the identification of user accounts that do not have this information present.

If you are using additional identities, as there is no method of synchronizing the additional identities with the directory, you must remove them and add them again. A new report, **Additional Identities (AID)**, is provided in the MyID Operator Client to assist with this process. This allows you to locate users that do not have a User SID registered against an additional identity

See the *Including user security identifiers in certificates* section in the *Administration Guide*.

9.1.7 OLE DB Driver 19

From MyID 12.6, you must have the Microsoft OLE DB Driver 19 for SQL Server (MSOLEDBSQL) installed.

Previous versions of MyID from MyID 11.0 required Microsoft OLE DB Driver 18 for SQL Server; these versions are not compatible with each other. You must upgrade to Microsoft OLE DB Driver 19 for SQL Server before installing or upgrading MyID.

All components provided with MyID 12.6, including any optional modules that require access to the database, have been updated to use Microsoft OLE DB Driver 19. See the readme files for the individual modules for details.

For more information about supported versions of the Microsoft OLE DB Driver, contact customer support quoting reference SUP-324.

For more information about the Microsoft OLE DB Driver, see the *Installing the database software* section in the **Installation and Configuration Guide**.

9.1.8 Repeating derived credential revocation checks

By default, seven days after MyID issues derived credentials, it checks the original credentials that were used to request the derived credentials. If, during this period, the original credentials became no longer valid (for example, if the PIV authentication certificate is revoked), MyID revokes the derived credentials.

You can now also configure MyID to repeat the revocation check at regular intervals using the **Derived Credential Revocation Check Interval** option (on the **Certificates** page of the **Operation Settings** workflow).

See the *Setting the credential check period* section in the **Derived Credentials Self-Service Request Portal** guide for details.

9.1.9 REST web service notifications

You can configure MyID to send a notification to a REST-based web service for device lifecycle events. For example, you can update a physical access control system (PACS) to enable or disable access for a particular card when it is issued or managed in MyID, or inform connected systems such as a workflow automation platform, endpoint management solution, or stock control system when credentials have been issued to a person.

MyID provides standard notifications for issuing, canceling, enabling, and disabling devices. To implement each of these notifications, you must set up an external system connection within MyID that provides details of your REST web service, including authentication details, and a mapping file that describes the format of the payload that you want to send to the web service endpoint.

MyID provides sample mapping files for each of the standard notifications. You can write your REST-based web service to consume the payload provided by these notifications, or use the provided mapping files as a basis for your own requirements.

See the *REST web service notifications* section in the **Administration Guide**.

9.1.10   Terms and conditions enhancements

This release contains multiple enhancements for handling the acceptance of terms and conditions when a cardholder activates or updates a device.

9.1.10.1 HTML-based terms and conditions documents for the Self-Service App and the Self-Service Kiosk

The Self-Service App and the Self-Service Kiosk now use the same HTML template method for presenting terms and conditions as is used in the Activation and Assisted Activation workflows in MyID Desktop.

You must upgrade your Self-Service App and Self-Service Kiosk clients to use the versions provided with MyID 12.6 as a minimum; previous versions of the self-service clients continue to use the `TermsConditions.txt` file on the web server.

Important: If you were previously using a customized version of the `TermsConditions.txt` file, you must copy the content from this file into a new HTML template.

You must also install the Microsoft WebView2 Runtime on each client PC (MyID Desktop, Self-Service App, and Self-Service Kiosk) to allow the presentation of the HTML-based terms and conditions document to the cardholder. MyID Desktop has been updated to use the same WebView2 component as the self-service applications. WebView2 is a component that is also used by Microsoft 365 Apps, so may already be present on your systems.

See the *Customizing terms and conditions* section in the *Administration Guide*.

9.1.10.2 Printing terms and conditions

The introduction of this feature also means that you can print the terms and conditions document from the Self-Service App and Self-Service Kiosk; note, however, that printing from the Self-Service Kiosk is disabled by default – see the *Enabling printing of terms and conditions* section in the *Self-Service Kiosk* guide.

9.1.10.3 Email signed terms and conditions to the cardholder

When using HTML terms and conditions, you can configure MyID to email a copy of the signed terms and conditions to the cardholder using the new **Email Terms and Conditions** option on the **Devices** tab of the **Operation Settings** workflow.

See the *Emailing terms and conditions* section in the *Administration Guide*.

9.1.10.4 Upload new HTML terms and conditions templates to the database

MyID now provides the MyID Document Uploader, which allows you to upload HTML templates for terms and conditions to the database. This tool has limited scope – it does not allow you to edit, delete, or overwrite existing templates – but you can copy existing templates to use as a basis for new templates, and it greatly simplifies the procedure for uploading a template to the database.

See the *MyID Document Uploader* guide.

9.2   Integration updates

This section contains details of updates to MyID 12.6.0's support for integration with smart cards and other credentials, certificate authorities, printers, and HSMs.

9.2.1 Entrust enhancements

You can configure Entrust certificate policies to make the NACI value mandatory (the `piv_interim` attribute). This is typically required for the PIV Authentication and PIV Card Authentication certificates. When MyID adds the user to Entrust, it now includes the user's NACI value, allowing you to issue certificates where the NACI value is mandatory.

Note: This feature is not currently supported with Entrust CA Gateway.

See the *Certificates with mandatory NACI values* section in the ***Entrust CA Integration Guide*** for details.

9.2.2 Global PIN supported devices

The list of devices on which Global PIN is supported has been extended to include the following:

- *BAP#087584 – ID-One PIV 2.4 on Cosmo v8.2 NPIVP*

- *BAP#087586 – ID-One PIV 2.4 on Cosmo v8.2 SPE+*

See the *Global PIN support* section of the ***Smart Card Integration Guide***.

9.2.3 IDEMIA smart cards

An additional specification has been added for IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1 smart cards:

- *BAP#087487 – ID-One PIV 2.4 on Cosmo v8.1 CIV (with 125Khz prox loop)*

  Note: The historic bytes for the BAP#087487 device `80`, `31`, `C1`, `52`, `xx`, `12` indicate that this card has been initialized using the CIV configuration. The prox loop is not supported.

See the *IDEMIA smart cards* section in the ***Smart Card Integration Guide*** for details.

9.2.4 SafeNet SC650 smart cards

MyID now supports the use of the 90Meter minidriver for SafeNet SC650 4.1 smart cards.

Previously, you could use SafeNet SC650 V4.1 smart cards with the SafeNet AT High Assurance Client software. This software is no longer supported. Instead, you must use the 90Meter minidriver.

Note, however, that you cannot use the 90Meter minidriver to upgrade or reissue smart cards that were issued with the SafeNet AT High Assurance Client.

See the *Thales Trusted Cyber Technologies smart cards* section in the ***Smart Card Integration Guide*** for details.

9.2.5 SQL Server versions

The versions of SQL Server with which MyID has been tested have been updated. MyID has now been tested with the following SQL Server versions:

- SQL Server 2019 – CU18 (15.0.4261.1 - September 2022)

- SQL Server 2017 – CU31 (14.0.3456.2 - September 2022)

See the *Database versions* section of the ***Installation and Configuration Guide*** for details.

9.2.6 Thales authentication devices

MyID now supports the following devices:

- SafeNet eToken 5110+ FIPS Level 3

See the *Thales authentication devices* section in the ***Smart Card Integration Guide***.

9.2.7 Windows 10 and 11 version 22H2

MyID now supports Windows 10 version 22H2 and Windows 11 version 22H2.

See the *Operating systems* section in the ***Installation and Configuration Guide*** for details of supported client operating systems.

9.2.8 Windows Server 2022

MyID now supports Windows Server 2022 as a server operating system.

See the *Operating systems* and *Server roles for Windows Server 2022* sections in the ***Installation and Configuration Guide*** for details.

9.3 Improvements

This section provides details of minor improvements to existing functionality within MyID 12.6.0.

9.3.1 General bug fixes and improvements

This release contains general bug fixes and minor improvements as part of a program of continuous improvement.

This release incorporates the following hotfixes:

- HOTFIX-11.6.2.7 – Ensure that the Card Profile ID is cleared on unassigned devices.

- HOTFIX-11.6.2.9 – Default certificates are now used when issuing certificate renewals.

- HOTFIX-12.1.0.1 – Adds the Customer Configurable Dictionary for User PIN Policy feature.

- HOTFIX-12.2.0.2 – Card printing font size improvements.

- HOTFIX-12.4.1.4 – Addresses issue that occurs when issuing virtual certificates.

- HOTFIX-12.4.1.5 – Configurable authentication code complexity for automatically-generated activation codes.

9.3.2 AES encryption

MyID has been updated to replace use of Triple-DES encryption (TDEA) in low level processes; for example, secure communication between MyID clients and servers. AES Encryption is now used for new MyID installations.

Important: AES encryption is supported with MyID client software provided with MyID 12.6 or later only. Accordingly, TDEA is retained if you are upgrading from earlier versions of MyID to provide backwards compatibility with older MyID clients. You can configure MyID to continue to use TDEA where technical constraints require this using the **Envelope Transport Key Algorithm** configuration option on the **Server** page of the **Security Settings** workflow.

Additionally, if you are issuing mobile identities using Identity Agent or MyID Authenticator, you must set the **Envelope Transport Key Algorithm** configuration option to `3DES`; a future update for these mobile apps will provide support for AES. Apps developed using Identity Agent Framework version 3.9 or later, which use the rest.provision mobile provisioning API, can support AES; for apps developed using earlier versions, set the option to `3DES`.

See the *Server page (Security Settings)* section of the ***Administration Guide*** and the *Configuring MyID for 3DES encryption* section of the ***Mobile Identity Management*** guide for details.

This change has been made in accordance with NIST Guidance on use of Triple-DES encryption and you are encouraged to check your own security policies to determine when you should modify your installations to use AES Encryption.

9.3.3 Card authentication certificate serial numbers

By default, the serial number used in the DN for certificates written to the Card Auth container on a PIV-compatible card are in decimal format, where the numeric components are decimal values separated by – symbols. However, some legacy systems require the serial number in hexadecimal format.

You can control the format of the serial number used with the **Card Authentication Certificate ID Format** configuration option on the **Certificates** page of the **Operation Settings** workflow. You can select decimal serial numbers, or hexadecimal format in either upper or lower case, depending on the requirements of your certificate authority.

Note: This feature is intended for use with Entrust certificate authorities only. Also, this configuration flag is respected only when carrying out the following operations:

- Any Self-Service App operations.
- Any Self-Service Kiosk operations.
- MyID Desktop:
  - Activate Card
  - Assisted Activation
  - Batch Collect Card
  - Collect Card
  - Collect Updates

If you use any other operation that writes certificates to a device, the Card Auth certificate is issued with a decimal serial number, whatever the configured value for the **Card Authentication Certificate ID Format** configuration option.

See the *Certificates page (Operation Settings)* section in the ***Administration Guide*** for details.

9.3.4 Certificate maintenance processor

MyID now has a feature that allows you to generate a list of certificates that meet a set of criteria and export them to a file; for example, certificates that are expiring within the next six weeks. The data in the file includes details about each certificate, including policy name, expiry date, and user information.

This feature requires additional database configuration to use it; contact Intercede quoting SUP-373 for further details.

9.3.5 Configuring license notifications

You can now configure MyID to hide the licensing expiry message that appears on the dashboard from users who do not have access to the **Licensing** workflow; set the **Show License Info to All Operators** configuration option on the **Notifications** page of the **Operation Settings** workflow to `No`. By default, this option is set to Yes, which means that all users see the license expiry warning on their dashboard when they log in.

See the *License management* section in the ***Administration Guide*** for details.

9.3.6 Dynamically changing text size

In the **Card Layout Editor**, you can now apply a formatter to auto text boxes to ensure that their contents are scaled to fit on the card when printed.

You can also link two auto text boxes to ensure that their contents are scaled by the same amount.

See the *Dynamically changing text size* section in the ***Administration Guide*** for details.

9.3.7 Lifecycle API schema correction

The `Afficiate` value in the `EmployeeAssociation` node in the `PIVSchemaTypes` schema has been corrected to be `Affiliate`.

See the *PivCardRequest/Agency/Applicant/Position/EmployeeAssociation* and *PIVSchemaTypes schema* sections in the ***Lifecycle API*** guide.

9.3.8 OpenSSL version update

The version of OpenSSL used within MyID was updated to OpenSSL v3.0.7 at MyID version 12.5. This was in response to recent high priority CVE reports:

- X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602)
- X.509 Email Address Variable Length Buffer Overflow (CVE-2022-3786)

MyID is not directly affected by the reported issues, but is being updated to keep in line with available versions of OpenSSL.

The following utilities and additional modules have now been updated for the current release:

- Audit Verifier Tool
- Bureau Integration
- HID PivClass PACS Integration
- Image Migration Utility
- Key Migration Utility
- MSCAWebService
- Server Events API
- Unique User ID Service
- Unlock Credential Provider

9.3.9 RevocationDelay for validate cancellation

The `RevocationDelay` option for CMSCardRequest in the Lifecycle API has been updated to ensure that the feature is valid for cancellations that must be validated.

If the credential profile is configured so that it must be validated before cancellation, the certificates are not canceled until the specified number of hours after the cancellation request is approved.

See the *CMSCardRequest/Group/User/Actions/RevocationDelay* section in the ***Lifecycle API*** guide for details of this option.

9.3.10 SQL Server permissions

The requirements for SQL Server permissions for the MyID installation user have been simplified.

If you need to create a new database, or add the MyID COM and Authentication users as SQL Server logins to the MyID and Authentication databases, the installation user must have `sysadmin` privileges.

If you are installing into an existing database, and have the SQL Server logins already in place, you do not need `sysadmin` privileges.

The MyID Installation Assistant runs test SIU-097 as part of its pre-installation check to ensure that you have the required permissions.

See the *Database configuration considerations* and *Installation account* sections in the ***Installation and Configuration Guide*** for details.

9.4 Documentation updates in MyID 12.6.0

This section contains information on new and updated documentation in MyID 12.6.0.

9.4.1 Administration Guide

The *Administration Guide* has been updated with the following:

- Added the **Enforce Banned Words** option for credential profiles.

  See the *PIN Settings* and *Enforcing banned words in PINs* sections.

- Added the **Derived Credential Revocation Check Interval** configuration option and revised the list of available derived credential options for MyID Enterprise.

  See the *Certificates page (Operation Settings)* section.

- Added the **Card Authentication Certificate ID Format** configuration option.

  See the *Certificates page (Operation Settings)* section.

- Added information about user security identifiers (user SIDs).

  See the *Including user security identifiers in certificates* section.

- Added information about using user SIDs with additional identities.

  See the *User SIDs in additional identities* and *Setting up additional identities* section.

- Added information about requiring user SIDs as requisite user data requirements in a credential profile.

  See the *Requisite User Data* section.

- Added a new chapter about the card suitability check.

  See the *Checking card suitability* section.

- Added details of the **FitTextFormatter** in the Card Layout Editor.

  See the *Dynamically changing text size* section.

- Added the **Email Terms and Conditions** configuration option.

  See the *Devices page (Operation Settings)* and *Emailing terms and conditions* sections.

- Updating the details on the different methods used for terms and conditions for different clients and workflows, requirements for the WebView2 component, and details of emailing terms and conditions.

  See the *Customizing terms and conditions* section.

- Added the **Show License Info to All Operators** configuration option.

  See the *Notifications page (Operation Settings)* section.

- Added the **Envelope Transport Key Algorithm** configuration option.

  See the *Server page (Security Settings)* section.

- Added a new section about sending notifications to REST-based web services.

  See the *REST web service notifications* section.

- Added information about managing REST notifications in the **Managing Notifications** workflow.

  See the *Using the Notifications Management workflow* section.

9.4.2 Credential Web Service

The *Credential Web Service* guide has been updated with the following:

- New methods have been added.

  See the *RequestCertificate*, *GetCertificate*, *RequestCertificatePfx*, *GetCertificatePfx*, *IsAlive*, *Error messages*, and *Default settings* sections.

9.4.3 Derived Credentials Self-Service Request Portal

The *Derived Credentials Self-Service Request Portal* guide has been updated with the following:

- Added the **Derived Credential Revocation Check Interval** option and revised the list of available derived credential options for MyID Enterprise.

  See the *MyID configuration options* section.

9.4.4 Entrust CA Gateway

The *Entrust CA Gateway Integration Guide* has been updated with the following:

- Added a note about consulting the Entrust documentation for additional requirements to ensure that you have an operational Entrust system available through the Gateway.

  See the *Supported Entrust CA Gateway versions* section.

- Updated the API and Application versions that have been tested with MyID.

  See the *Supported Entrust CA Gateway versions* section.

9.4.5 Entrust CA Integration Guide

The *Entrust CA Integration Guide* has been updated with the following:

- Added details of support for mandatory NACI attributes.

  See the *Certificates with mandatory NACI values* section.

9.4.6 Error Code Reference

The *Error Code Reference* has been updated with the following:

- Updated the details of the following error:
  - WS50016 – The person selected does not have all required information for this credential profile. Check the Person History audit details to identify the missing requisite user data.

  See the *MyID Operator Client error codes* section.

- Updated the details of the following error:
  - 85188 – Unable to connect to the authentication server.
  - 881044 – now general failure to carry out Integrated Windows Logon as a possible cause of the error.

  See the *Web Service error codes* section.

- Added the following errors:
  - 890800 – Token validation failed.
  - 890801 – Issuer validation failed.
  - 9007152 – The card suitability check has failed.

  See the *Web Service error codes* section.

- Added the following errors:
  - -99900033 – An unknown error has occurred, contact customer support.
  - 890606 – Microsoft WebView2 Runtime <VERSION> or higher is not installed. Please contact your administrator.

  See the *MyID Windows client error codes* section.

- Added the following error:
  - IA12002 – Decryption failure.

  See the *MyID Identity Agent error codes* section.

9.4.7 Installation and Configuration Guide

The ***Installation and Configuration Guide.pdf*** has been updated with the following:

- Updated the required version of the OLE DB Driver from 18 to 19.

  See the *Installing the database software* and *Upgrading MyID* sections.

- Added requirement for the SqlServer PowerShell module to run SIU tests against the database.

  See the *Running SIU tests against the database* and *Upgrading MyID* sections.

- Added requirement for the installation user to have either the `sysadmin` role or the `securityadmin` role to run the test SIU-097.

  See the *Database configuration considerations* section.

- Added a clarification that the MyID installation program is designed to be run from within the MyID Installation Assistant.

  See the *Running the installation program* section.

- Added requirements for the Microsoft WebView2 Runtime on client workstations.

  See the *Microsoft WebView2 Runtime* section.

- Added requirements for the .NET Core Desktop Runtime to be installed on the application server if you want to use the MyID Document Uploader utility.

  See the *Installing .NET Framework and .NET Core* section.

- Updated the versions of Windows 10 and Windows 11 supported for client workstations.

  See the *Operating systems* section.

- Updated the supported server operating systems to include Windows Server 2022.

  See the *Operating systems* and *Server roles for Windows Server 2022* sections.

- Updated the versions of SQL Server supported.

  See the *Database versions* section.

9.4.8 Lifecycle API

The ***Lifecycle API*** guide has been converted to HTML, in line with the rest of the MyID documentation set, and also contains the following:

- The `Afficiate` value in the `EmployeeAssociation` node in the `PIVSchemaTypes` schema has been corrected to be `Affiliate`.

  See the *PivCardRequest/Agency/Applicant/Position/EmployeeAssociation* and *PIVSchemaTypes schema* sections.

- Added nodes for importing the user security identifier (user SID) for PIV and Enterprise.

  For PIV, see the *PivCardRequest/Agency/Applicant/Account/UserSID* and *PIVSchemaTypes schema* sections.

  For Enterprise, see the *CMSCardRequest/Group/User/Account/UserSID* and *CMSSchemaTypes schema* sections.

9.4.9 Microsoft Windows CA Integration Guide

The *Microsoft Windows CA Integration Guide* has been updated with the following:

- Added information about user security identifiers (user SIDs).

  See the *Enable certificate templates for issuance within MyID* and *Adding extensions to certificate templates* sections.

- Updated the supported operating systems to include Windows Server 2022.

  See the *Hardware and software requirements* section.

9.4.10 Mobile Identity Management

The *Mobile Identity Management* guide has been updated with the following:

- Updated the section on using derived credentials with an MDM.

  See the *MDMs and derived credentials* section.

- Added information about 3DES and AES encryption.

  See the *Configuring MyID for 3DES encryption* section

  Added information about installing the rest.provision service.

  See the *REST API for provisioning mobile credentials* section

9.4.11 MyID Authentication Guide

The *MyID Authentication Guide* has been updated with the following:

- Updated the required version of the OLE DB Driver from 18 to 19.

  See the *Installing the standalone authentication service* section.

9.4.12 MyID Client MSIX Installation Guide

The *MyID Client MSIX Installation Guide* has been incorporated into the main documentation set. Previously, this was available only as a PDF in the folder containing the MSIX installation programs.

9.4.13 MyID Core API

The *MyID Core API* document has been updated with the following:

- Added information on obtaining an extension grant to launch the Select Security Device dialog using the MyID Client Service API.

  See the *Obtaining an extension token for Select Security Device* section.

- Added a note about avoiding requesting access tokens unnecessarily.

  See the *Calling the API from an external system* section.

9.4.14 MyID Document Uploader

The *MyID Document Uploader* guide is new for this release.

9.4.15 MyID Operator Client

The *MyID Operator Client* guide has been updated with the following:

- Added information about the display of user images and full names on the Select Security Device dialog.

  See the *Reading a device* section.

- Added further configuration for load balanced systems.

  See the *Load balancing*, *Setting the issuer for load-balanced systems*, and *MyID Operator Client pass-through authentication with a load balancer* sections.

- Added a note on the credential profile permissions needed when requesting an update for a device.

  See the *Requesting an update for a device* section.

- Added information about user security identifiers (user SIDs).

  See the *Editing a person*, *Searching for a person*, and *Additional Identities (AID) report* section.

- Added a new section on using the Group dialog, including information on selecting the list view and viewing descriptions.

  See the *Selecting a group* section; also added links from the *Adding a person*, *Searching for a person*, *Searching for a device*, and *Searching for a request* sections.

- Updated the People report to include the **User SID Present** and **Enabled** additional criteria, and the **Enabled** field in the report.

  See the *People report* section.

9.4.16 PrimeKey EJBCA Integration Guide

The *PrimeKey EJBCA Integration Guide* has been updated with the following:

- Added information about user security identifiers (user SIDs).

  See the *Prerequisites*, *Configuring custom certificate extensions*, and *Configuring the CA within MyID* sections.

9.4.17 Self-Service App

The *Self-Service App* guide has been updated with the following:

- Added requirements for the Microsoft WebView2 Runtime to display HTML-based terms and conditions templates.

  See the *Prerequisites* section.

9.4.18 Self-Service Kiosk

The *Self-Service Kiosk* guide has been updated with the following:

- Added requirements for the Microsoft WebView2 Runtime to display HTML-based terms and conditions templates.

  See the *Prerequisites* section.

- Added information on enabling the printing of terms and conditions in the Self-Service Kiosk.

  See the *Enabling printing of terms and conditions* section.

9.4.19 Smart Card Integration Guide

The *Smart Card Integration Guide* has been updated with the following:

- Updated information about SafeNet SC650 V4.1 smart cards.

  See the *Thales Trusted Cyber Technologies smart cards* section.

- An additional specification – BAP#087487 – has been added for IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1 smart cards.

  See the *IDEMIA smart cards* section.

- Information about SafeNet eToken 5110+ FIPS Level 3 tokens has been added.

  See the *Thales authentication devices* section.

- The list of devices on which Global PIN is supported has been extended.

  See the *Global PIN support* section.

9.4.20 Symantec (DigiCert) Managed PKI Integration Guide

The *Symantec MPKI Integration Guide* has been updated with the following:

- Updated Symantec MPKI version that has been tested with MyID.

  See the *Hardware and software requirements* section.

9.4.21 System Interrogation Utility

The *System Interrogation Utility* guide has been updated with the following:

- Added test SIU-022 to cover checking that the required PowerShell module for running database tests is installed.

  See the *Description of derived tests* section.

- Updated test SIU-097 with the requirement for the installation user to have either the `sysadmin` role or the `securityadmin` role.

  See the *Description of derived tests* section.

- Updated the list of tests to specify Windows Server 2022 as a supported operating system.

  See the *Description of derived tests* section.

9.4.22   System Security Checklist

The *System Security Checklist* has been updated with the following:

- Updated the instructions for setting up TLS 1.2 to remove the requirement to update the UDL files, as this is carried out by the MyID installation program.

  See the *Securing MyID with TLS 1.2* section.

- Updated the procedure for removing details of the IIS server to remove the configuration required for older, unsupported operating systems.

  See the *Remove details of the IIS server* section.

9.4.23   Thales Luna HSM Integration Guide

The *Thales Luna HSM Integration Guide* has been updated with the following:

- Updated the location of instructions in the Thales documentation for configuring a connection.

  See the *Configuring the connection for DPoD* section.

9.5   End of support features in MyID 12.6.0

This section contains information about features that are no longer supported in MyID as of MyID 12.6.0.

See:

- section *9.5.2*, *Windows Server 2016*.

- section *9.5.1*, *SafeNet AT High Assurance Client*.

9.5.1   SafeNet AT High Assurance Client

Previously, you could use SafeNet SC650 V4.1 smart cards with the SafeNet AT High Assurance Client software. This software is no longer supported. Instead, you must use the 90Meter minidriver.

Note, however, that you cannot use the 90Meter minidriver to upgrade or reissue smart cards that were issued with the SafeNet AT High Assurance Client.

See the *Thales Trusted Cyber Technologies smart cards* section in the *Smart Card Integration Guide* for details.

9.5.2   Windows Server 2016

Windows Server 2016 is no longer supported as a server operating system.

See the *Operating systems* sections in the *Installation and Configuration Guide* for details of supported server operating systems.

9.6   Known issues resolved in MyID 12.6.0

This section lists the known issues that have been resolved in MyID 12.6.0. These are issues that were found across both editions of MyID – Enterprise and PIV – and may not all be relevant for your system.

- IKB-361 – Problem using Microsoft OLE DB Driver 19 for SQL Server.

- IKB-366 – Cannot add an additional identity if the DN contains an ampersand.

- IKB-368 – Certificates issued through PrimeKey EJBCA or DigiCert certificate authorities fail to be installed to iOS system store.

- IKB-369 – Not all add-on modules may be listed in the Package Manager.

- IKB-370 – Incorrect examples in the API documentation for some endpoints.

10 Updates in MyID 12.5.0

This chapter provides details of the changes in MyID 12.5.0, including:

- New and updated features – new features in this version of MyID, and major improvements to existing features.

- Integration updates – updates to MyID's support for smart cards and other credentials, certificate authorities, printers, and HSMs.

- Improvements – minor updates to existing functionality.

Important: At MyID version 12.3, the version of .NET Core used was updated. This affects the MyID servers and all clients. See section *13.3.7*, *.NET Core versions* for details.

Important: Microsoft is making changes to DCOM security over the course of releases in 2021 to 2023 that may affect your system, depending on your configuration. See section *13.2.2*, *Microsoft Windows DCOM server security changes* for details.

10.1 New and updated features

This section contains information on the new and updated features in MyID 12.5.0.

10.1.1 Working with mobile devices in the MyID Operator Client

You can now use the MyID Operator Client to work with mobile devices. You can now:

- Request a mobile device for another person.

- Request a replacement mobile device.

- Enable or disable a mobile device.

- Request an update for a mobile device.

- Request a renewal for a mobile device.

- Cancel a mobile device.

The MyID Operator Client provides new operations for requesting mobile devices and replacement mobile devices, and opens up the existing enable/disable, update, renew, and cancel operations to mobile devices.

See the *Requesting a mobile device for a person* and *Requesting a replacement mobile device* sections in the *MyID Operator Client* guide.

You can also carry out all of these processes through the MyID Core API. See the *Accessing the API documentation* section in the *MyID Core API* guide for details of accessing the API documentation, which contains details of the relevant methods.

Credential profiles for mobile devices have been enhanced with notification schemes to support requests for mobile devices made through the MyID Operator Client or through the MyID Core API.

See the *Configuring SMS and email notifications for the MyID Operator Client* section in the *Mobile Identity Management* guide.

10.1.2 Canceling multiple requests

If you have several requests to cancel at the same time, you can now cancel them in a batch instead of canceling them one by one.

When you search for requests in the MyID Operator Client, you can now select multiple items in the search results, then use the **Tools** menu to select the **Cancel Request** option.

See the *Canceling multiple requests* section in the ***MyID Operator Client*** guide.

10.1.3 Checking the web services

The MyID Installation Assistant now carries out a series of checks on the MyID web services as part of its post-installation check.

This ensures that the services have been installed and are running. It does not confirm that the optional web services have been configured fully and are available for use, however; as these web services are secure by default you must review the documentation for each service to ensure that you have configured them correctly and the correct authentication is in place for you to be able to make use of them.

See the *Checking the web services* section in the ***Installation and Configuration Guide***.

10.1.4 Customizing the number of buttons in the button bar

By default, the MyID Operator Client now displays four buttons in the button bar; in previous releases, only two buttons were displayed. You can also increase or decrease the number of buttons displayed by editing a configuration file on the web server. The minimum number of buttons displayed is one; if you set the limit high enough, you can display a button for each action to which you have access.

See the *Using the button bar* and *Changing the number of buttons displayed in the button bar* sections in the ***MyID Operator Client*** guide.

10.1.5 Enabling and disabling devices

You can now use the **Enable Device** and **Disable Device** options in the MyID Operator Client to enable or disable devices. This is an alternative to using the **Enable/Disable Card** workflow in MyID Desktop.

This feature is also now available through the MyID Core API.

If you are upgrading to the current version of MyID, any users who previously had access to the **Enable/Disable Card** or the **Enable / Disable ID** workflow will be granted access to the **Enable Device** and **Disable Device** options.

See the *Enabling and disabling devices* section in the ***MyID Operator Client*** guide.

10.2   Key Migration Utility

The Key Migration Utility is available from Intercede to help you manage the cryptographic keys that protect your MyID installation. The utility can help you:

- Strengthen HSM resident keys; for example, migrating from a Triple-DES key to an AES key.

- Migrate from a registry-based key to a HSM-protected key.

- Change the Master Key of your installation.

The utility is available on request – contact Intercede support to obtain this, quoting reference SUP-362.

Name	Where is it?
Key Migration Utility	Available on request.

10.2.1   Limiting the lifetime of derived credentials

When you issue derived credentials, you may not want the lifetime of the newly-issued credentials to exceed the lifetime of the deriving certificate. You can now configure MyID to limit the lifetime of derived credentials using the **Limit derived credential lifetime to deriving credential** configuration option (on the **Certificates** page of the **Operation Settings** workflow).

See the *MyID configuration options* section in the ***Derived Credentials Self-Service Request Portal*** for details.

10.2.2   Managing credentials from the MyID Authentication screen

You can now launch the Self-Service App from the MyID Authentication screen to allow you to manage your credentials (for example, changing your security phrases or resetting your device PIN) without first signing in to MyID.

See the *Managing your credentials from the MyID Authentication screen* section in the ***MyID Operator Client*** guide.

This feature is also available for your own systems that use the MyID authentication web service; you can enable or disable this feature using the `EnableSelfService` option in the app settings file for a particular client type. See the *Editing the configuration file* section in the ***MyID Authentication Guide*** for details.

10.2.3   MyID Operator Client with multiple simultaneous users

You can now use the MyID Operator Client in client environments with simultaneous users; for example, on a virtualized desktop hosted by Microsoft Remote Desktop Services.

Additional configuration is required; see the *Installing the MyID Client WebSocket Service* section in the ***Installation and Configuration Guide*** for details.

Some limitations exist when using connected peripherals, which are described in the *Virtual environments and remote connections* section of the ***Installation and Configuration Guide***.

10.2.4 Saving smart card container data

You can now configure MyID to save the data that is written to a smart card container when issuing a smart card using a data model. This allows you to store the data and pass it to other systems; for example, your PACS.

See the *Saving container data* section in the ***Smart Card Integration Guide***.

10.2.5 Specifying logon details when requesting authentication codes

The authentication server has been enhanced to allow you to pass logon details in the request for authentication codes. You can now specify which logon mechanism to use, and, if you are using authentication codes, you can provide the logon name for the specified user to be pre-populated in the **Username or email address** field on the Authentication Code Login dialog.

See the *Requesting an authorization code* section in the ***MyID Authentication Guide*** for details.

10.2.6 Timeouts and re-authentication in the MyID Operator Client

The MyID Operator Client now allows you to extend your authenticated session after signing in. If you continue using the MyID Operator Client, your authentication is extended every time you make a call to the server (for example, by opening a new screen, running a report, or saving data). As long as it has been less than two hours since you last used the MyID Operator Client, your session is extended automatically.

If it has been more than two hours, you must re-authenticate using the same user and logon method. Once you have done so, you can continue working with the MyID Operator Client.

For more details, see the *Timeouts and re-authentication* section in the ***MyID Operator Client*** guide.

You can also use this feature of the authentication server to extend your authenticated session for calls to the API when using user authentication. See the *Using refresh tokens* section in the ***MyID Core API*** guide for details.

10.2.7 Viewing audit details in the MyID Operator Client

You can now click on an entry in the list of audit records (either on the **History** tab of the View Person screen or in the **Unrestricted Audit Report**) in the MyID Operator Client and view the details recorded in the audit trail.

This includes any trace records providing detailed information about the stages of the process being audited, any changes to the card content, and signing details. Trace records are nested under their parent audit record.

If the audit contains a binary object (for example, a user image or signed Terms and Conditions document) you can click on a link to view the stored image or document in a new window.

See the *Working with the audit trail* and *Viewing audit details* sections in the ***MyID Operator Client*** guide for details.

10.2.8 Viewing extended information about a device

You can now launch the **Identify Device (Administrator)** workflow from the View Device screen in the MyID Operator Client. This workflow provides additional information about the device, including the initial server-generated PIN, if available.

See the *Viewing extended information about a device* section in the ***MyID Operator Client*** guide for details.

10.2.9 Windows authentication for the MyID Operator Client

You can now use Integrated Windows Logon as an authentication method for signing in to the MyID Operator Client.

See the *Signing in using Windows authentication* section in the ***MyID Operator Client*** guide.

You can also use Windows authentication when using the web.oauth2 authentication web service for OpenID Connect. You can enable or disable Windows authentication for each client type using the `EnableWindowsLogin` option in the appsettings file, and can specify the Windows authentication method when calling `/connect/authorize` using the `acr_values=logonmechanism:windows` parameter. See the *Editing the configuration file* and *Requesting an authorization code* sections in the ***MyID Authentication Guide*** for details.

10.2.10 Windows Logon Certificates utility

The Windows Logon Certificates utility provides PowerShell scripts that allow you to create strong certificate mappings in Active Directory using the `X509IssuerSerialNumber` mapping (as defined in KB5014754) to enable certificates issued by MyID to be used for Windows Logon after "Full Enforcement Mode" is enabled on domain controllers. The installation program provided updates the MyID database to allow you to run the scripts; you are recommended to run the PowerShell scripts as scheduled tasks on the appropriate servers.

For background on this procedure, see the following Microsoft Knowledge Base article:

- ***KB5014754***: Certificate-based authentication changes on Windows domain controllers.

See the *Windows Logon Certificates utility* section in the ***Implementation Guide*** for further details.

10.3 Integration updates

This section contains details of updates to MyID 12.5.0's support for integration with smart cards and other credentials, certificate authorities, printers, and HSMs.

10.3.1 Enabling and disabling YubiKey capabilities

Previously, you could use the `CardDataModel\SupportedInterfaces` node in the card format file for YubiKey SC and YubiKey SC FIPS tokens to enable or disable the token capabilities as accessed through the USB interface. This feature has been enhanced to allow you to enable or disable token capabilities through either the USB or NFC interface.

The `CardDataModel\USBCapabilities` node is now used to configure the capabilities of the USB interface; the `CardDataModel\NFCCapabilities` node is used to configure the NFC capabilities.

See the *Enabling and disabling device capabilities* section in the ***Smart Card Integration Guide***.

10.3.2 Entrust CA Gateway

MyID has been tested with the following CA versions using the Entrust CA Gateway:

- Entrust v10
- Entrust v8.3

See the *Prerequisites* section in the **Entrust CA Gateway Integration Guide** for details.

10.3.3 FIDO updates

The support for FIDO devices has been updated in this release:

- The instructions for obtaining the FIDO metadata have been updated. You no longer need to obtain an access token. MyID now obtains the metadata from the FIDO Alliance MDS3 server.

  See the *Setting up the FIDO metadata* section in the **FIDO Authenticator Integration Guide**.

- You can now specify multiple origins, where multiple sub-domains of a registrable domain can be used for authentication.

  See the *Multiple origins* section in the **FIDO Authenticator Integration Guide**.

10.3.4 Mobile operating systems supported

The list of iOS and Android operating systems supported for mobile identities has been updated. MyID now supports:

- iOS 16, 15, 14.
- Android 13.0, 12.0, 11.0, 10.0.

See the *Supported devices* section in the **Mobile Identity Management** guide for details.

10.3.5 Thales authentication devices

MyID now supports the following devices:

- SafeNet eToken 5110+ FIPS Level 2

See the *Thales authentication devices* section in the **Smart Card Integration Guide**.

10.3.6 VMWare Workspace ONE Mobile Device Management

You can now configure an external system to allow MyID to communicate with your VMWare Workspace ONE Mobile Device Management (MDM) system.

You can configure a credential profile to issue only to devices registered with the MDM, and you can require particular attributes of registered devices as stored in the MDM.

See the *Setting up an external system for Workspace ONE* and *Configuring credential profiles for MDM restrictions* sections in the **Mobile Identity Management** guide.

10.4 Improvements

This section provides details of minor improvements to existing functionality within MyID 12.5.0.

10.4.1 General bug fixes and improvements

This release contains general bug fixes and minor improvements as part of a program of continuous improvement.

10.4.2 Additional People search criteria

You can now use the following additional search criteria when searching the MyID database for people:

- **Role** – Select the person's role from the drop-down list.

- **SAM Account Name** – Type the person's SAM Account Name, which appears on the **Account** tab of the View Person screen. You can use wildcards.

- **User Principal Name** – Type the person's User Principal Name, which appears on the **Account** tab of the View Person screen. You can use wildcards.

See the *People report* section in the **_MyID Operator Client_** guide for details.

10.4.3 Certificate renewal and PIN unlock for mobile identities

The MyID Core API has been updated to allow headless authentication for mobile identities. This provides improvements for PIN unlocking and certificate renewals.

The `EnableHeadlessCardLogin` and `EnableHeadlessPassphraseLogin` properties have been added to the application settings configuration file for the `myid.rest.mobile` client. These work in conjunction with the **Smart Card Logon** and **Password Logon** mechanisms respectively to allow access to the certificate renewal and PIN unlock features.

Note: Use of these features by mobile applications requires a corresponding update to the Identity Agent Framework and SDK – contact your Intercede account manager for further details.

See the *Editing the configuration file* section in the **_MyID Authentication Guide_** for details.

10.4.4 Displaying user images and names on the logon screen

You can set the **Show Full Name at Logon** and **Show Photo at Logon** options (on the **Logon** page of the **Security Settings** workflow) to configure the Select Security Device screen in the MyID Operator Client to display the associated user image and full name of the cardholder.

If there is a **Device Friendly Name** specified in the credential profile that was used to issue the device, this is also displayed on the Select Security Device screen.

Note: If you enable this feature, it is possible to obtain user photos and cardholder names without authentication.

See the *Signing in to MyID* section in the **_MyID Operator Client_** guide for details.

10.4.5   Maximum size and backups for logging

The instructions for configuring logging have been enhanced with the procedure for setting a maximum file size for your log files, and optionally a backup location to be used when the log exceeds the maximum file size. This feature applies to the registry logging method for server components.

See the *Maximum log size and backups* section in the ***Configuring Logging*** guide.

10.4.6   OpenSSL version update

The version of OpenSSL used within MyID, including the HSM Test Utility (HTU) and the Windows Integration Service (WSVC), has been updated to OpenSSL v3.0.7. This is in response to recent high priority CVE reports:

- X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602)
- X.509 Email Address Variable Length Buffer Overflow (CVE-2022-3786)

MyID is not directly affected by the reported issues, but is being updated to keep in line with available versions of OpenSSL.

Some utilities and additional modules will be updated in future product updates:

- Audit Verifier Tool
- TPM Utility
- Bureau Integration
- Image Migration Utility
- HID PivClass PACS Integration
- Server Events API

10.4.7   Section 508 improvements

Improvements have been made to MyID client support for the Section 508 accessibility standards. Section 508 support statements are available on the Intercede customer portal:

forums.intercede.com/documentation/section-508/

10.4.8   Selecting a website for the remote Microsoft CA web service

You can now select the website into which you want to install the web service for the Remote Microsoft Certificate Authority.

This requires running a PowerShell script to populate the list of available websites in IIS before launching the installation program.

See the *Installing the web service* section in the ***Microsoft Windows CA Integration Guide***.

10.4.9 Updating DNs for the SSRP

You can use the `ImportPIVDN` option in the `ssrp.conf.xml` configuration file for the Derived Credentials Self-Service Request Portal (SSRP) to control whether the PIV DN (`Xu55`) field is populated from the deriving credential. If `ImportPIVDN` is set to `true`, the PIV DN (`Xu55`) field is populated; otherwise, it is left blank. You can specify the `ImportPIVDN` option for each role.

Note: By default, from MyID 12.5 onwards, the value is set to `true` for the default role of `984`, while in previous releases the node was absent and so defaulted to `false`.

See the *Configuration file format* section in the ***Derived Credentials Self-Service Request Portal*** guide.

10.5 Documentation updates in MyID 12.5.0

This section contains information on new and updated documentation in MyID 12.5.0.

10.5.1 Administration Guide

The *Administration Guide* has been updated with the following:

- Added a limitation to the **One Credential Profile Request Per Person** configuration option.

  See the *Devices page (Operation Settings)* section.

- Added the **Allow Self-Service at Logon** configuration option.

  See the *Logon page (Security Settings)* section.

- Added a note that the `Domain` must contain the NetBIOS domain name and not the DNS format when configuring Integrated Windows Logon.

  See the *Integrated Windows Logon* section.

- Added details of the **Limit derived credential lifetime to deriving credential** configuration option.

  See the *Certificates page (Operation Settings)* section.

- Added notes about the behavior of different CAs when requesting certificates using the **Expire Cards at End of Day** configuration option to specify expiry dates and times.

  See the *Issuance Processes page (Operation Settings)* section.

- Added a cross-reference to the information on viewing audit details in the MyID Operator Client.

  See the *Running the audit report* section.

- Updated the **Show Full Name at Logon** and **Show Photo at Logon** options which now affect the MyID Operator Client.

  See the *Logon page (Security Settings)* section.

- Updated the details of the **Device Friendly Name** credential profile option to indicate that it now also affects the MyID Operator Client.

  See the *Credential profile options* section.

- Added information about the notification schemes available in the **Credential Profiles** workflow for issuing mobile devices.

  See the *Issuance Settings* section.

- Updated the details of the **Certificate Recovery Password Complexity** option to cover its use in providing authentication codes for mobile device issuance.

  See the *Certificates page (Operation Settings)* section.

- Updated the details of the **App Download URL – ANDROID** and **App Download URL – iOS** options to detail their use on the provisioning page for mobile device issuance.

  See the *Issuance Processes page (Operation Settings)* section.

- Added a note to the Integrated Windows Logon section about restrictions relating to the Protected Users group in Active Directory.

  See the *Protected Users group in Active Directory* section.

10.5.2   Configuring Logging

The *Configuring Logging* guide has been updated with the following:

- Information on configuring a maximum file size and a backup location for registry-based logging.

  See the *Registry logging* section.

- Added details of configuring logging for the MyID Client WebSocket Service.

  See the *MyID Client WebSocket Service* section.

10.5.3   Derived Credentials Self-Service Request Portal

The *Derived Credentials Self-Service Request Portal* guide has been updated with the following:

- Details of the `ImportPIVDN` option in the configuration file.

  See the *Configuration file format* section.

- Added error `0009, CardProfileRequisiteDataCheckFailed`.

  See the *Error code reference* section.

- Added details of the **Limit derived credential lifetime to deriving credential** configuration option.

  See the *MyID configuration options* section.

10.5.4   Entrust CA Gateway

The *Entrust CA Gateway Integration Guide* has been updated with the following:

- Updated details on setting the **Certificate Lifetime** option in the **Certificate Authorities** workflow.

  See the *Enabling certificate policies* section.

- Added details of Entrust behavior when recovering a revoked archive certificate where the certificate is configured in the credential profile for **Historic Only**.

  See the *Key archival and recovery* section.

- Added extra details on obtaining the value for the **CA Path**.

  See the *Set up the MyID Entrust certificate authority* section.

- Listed the versions of the Entrust CA tested for the current release.

  See the *Supported Entrust CA Gateway versions* section.

10.5.5   Entrust CA Integration Guide

The *Entrust CA Integration Guide* has been updated with the following:

- Added details of Entrust behavior when recovering a revoked archive certificate where the certificate is configured in the credential profile for **Historic Only**.

  See the *Key archival and recovery* section.

10.5.6 Error Code Reference

The *Error Code Reference* has been updated with the following:

- Added the following MyID Operator Client error codes:
  - OA10060 – The credential profile to be collected requires user data approval, but the target user has no such approval.
  - OA10061 – The credential profile to be collected requires terms and conditions to be accepted, but assisted collection of updates does not support this.
  - OA10062 – MyID client service is not running.
  - OA10063 – You cannot retrieve security questions for this client.
  - OA10064 – The security questions logonmechanism is disabled for this client.
  - OA10065 – You cannot retrieve a challenge for this client.
  - OA10066 – The smartcard logon logonmechanism is disabled for this client.
  - OA10067 – Key-pair authentication failed, or you may not have permission to access this client.
  - OA10068 – Windows logon failed, your windows account is unknown or untrusted.
  - OA10069 – Windows logon failed, your user account is not permitted to logon.
  - OA10070 – Windows Authentication is disabled on the server.
  - OA10071 – Refresh Token failed to retrieve token.
  - OA10072 – Authorization failure, missing data for Token Refresh.
  - OC10015 – At least one record must be selected in order to perform this operation.
  - OC10016 – Your login has expired. Please re-authenticate to the MyID Operator Client.
  - OC10017 – You have re-authenticated to the MyID Operator Client with a different user. For security reasons, the operation has been canceled.
  - OC10018 – You have re-authenticated to the MyID Operator Client with a different logon mechanism. For security reasons, the operation has been canceled.
  - WS10005 – Unable to generate the requested EFT export file.
  - WS50058 – The selected user has no suitable biometric samples for EFT export.

  See the *MyID Operator Client error codes* section.

- Updated the details of the following errors:
  - WS50019 – Requests created using this API must include an appropriate encoding type.
  - WS50053 – The capabilities of the selected credential profile are not supported by this operation.

  See the *MyID Operator Client error codes* section.

- Added the following web service error code:
  - 9007151 – An existing request or device exists with a different exclusive group.

See the *Web Service error codes* section.

- Updated the description of the following errors:
  - 800551 – now includes the Protected Users group in Active Directory as a possible cause of the error.
  - 881044 – now includes the Protected Users group in Active Directory as a possible cause of the error.
  - 890588 – now specified the MyID Operator Client method for approving requests as well as the MyID Desktop method.
  - 9007098 – now includes Lost as a disposal status that prevents a device from being reissued.

See the *Web Service error codes* section.

- Updated the following MyID Client Service error:
  - 10000228 – This error has been updated to add a reference to the MyID Client WebSocket Service, misconfiguration of which may cause the error.

See the *MyID Client Service error codes* section.

- Added a workaround for the following error:
  - REST007 – Unrecoverable error has occurred.

See the *MyID Identity Agent error codes* section.

10.5.7 FIDO Authenticator Integration Guide

The ***FIDO Authenticator Integration Guide*** has been updated with the following:

- Updated instructions for obtaining the FIDO metadata.
  See the *Setting up the FIDO metadata* section.
- Updated configuration to include multiple origins.
  See the *Configuring the server settings* section.
- Updated troubleshooting information.
  See the *Troubleshooting* section.

10.5.8 Implementation Guide

The ***Implementation Guide*** has been updated with the following:

- Added information about the Windows Logon Certificates utility.
  See the *Windows Logon Certificates utility* section.
- Added information about the Key Migration Utility.
  See the *Key Migration Utility* section.

10.5.9 Installation and Configuration Guide

The *Installation and Configuration Guide* has been updated with the following:

- Updated the instructions for upgrading MyID from a pre-MyID 11 system.

  See the *Upgrading MyID from a 32-bit application to 64-bit* section.

- Updated the instruction for moving a database to a new server.

  See the *Upgrading to a new server* section.

- Added information about running the Installation Assistant from the PowerShell command line.

  See the *Running the Installation Assistant* section.

- Added a note about an expected delay between the installer window closing after completing the installation and the log results window appearing in the MyID Installation Assistant.

  See the *Starting the server installation* section.

- Updated the list of required features for the MyID database server to remove PowerShell 2.0 Engine.

  See the *Setting up Windows server roles and features* section.

- Made clearer that you must log on as the MyID COM+ user to run the SetHSMPIN utility.

  See the *Setting the HSM PIN* section.

- Corrected instructions for providing non-default ports for SQL Server. This information is provided on the Port Selection screen, not the database screen.

  See the *Configuring the databases* section.

- Added a new section on installing and configuring the MyID Client WebSocket Service.

  See the *Installing the MyID Client WebSocket Service* and *Installing the MyID Client Service* sections.

- Added a new section on the tests that the MyID Installation Assistant carries out to ensure that the web services have been installed and are running.

  See the *Checking the web services* section.

- Added information on updating the installation folder before carrying out an upgrade or update.

  See the *Upgrading or updating the MyID Installation Assistant* section.

10.5.10 Lifecycle API

The *Lifecycle API* guide has been updated with the following:

- Added notes about the behavior of different CAs when requesting certificates using the **Expire Cards at End of Day** configuration option to specify expiry dates and times.

10.5.11 Microsoft Windows CA Integration Guide

The ***Microsoft Windows CA Integration Guide*** has been updated with the following:

- Details of running a PowerShell script to populate the list of available websites before installing the web service for the Remote Microsoft Certificate Authority.

  See the *Installing the web service* section.

- Updated the name of the application pool used by the Remote Microsoft Certificate Authority.

  See the *Installing the web service* section.

10.5.12 Mobile Identity Management

The ***Mobile Identity Management*** guide has been updated with the following:

- Added instructions for setting up an external system for VMWare Workspace ONE.

  See the *Setting up an external system for Workspace ONE* section.

- Added a step for restarting the Edefice_BOL component after making changes to an MDM connector.

  See the *Setting up your MDM system* section.

- Updated throughout to cover configuring, requesting, canceling, enabling, disabling, unlocking, updating and renewing mobile devices through the MyID Operator Client.

  See the *Configuring SMS and email notifications for the MyID Operator Client*, *Creating the Identity Agent credential profile*, *Requesting a mobile ID for another user*, *Requesting replacement mobile IDs*, *Canceling mobile IDs*, *Enabling and disabling mobile IDs*, *Unlocking mobile IDs*, *Updating mobile IDs*, and *Renewing mobile IDs* sections.

- Updated the list of supported mobile operating systems

  See the *Supported devices* section.

10.5.13 MyID Authentication Guide

The **_MyID Authentication Guide_** has been updated with the following:

- Added `EnablePassphraseLogin` and `EnableCardLogin` to the list of logon mechanisms you can disable on a client type basis using the appsettings file.

  See the _Editing the configuration file_ section.

- Added information on using the `acr_values` and `login_hint` parameters when requesting an authorization code.

  See the _Requesting an authorization code_ section.

- Added the `EnableSelfService` option for clients that determines whether the **Manage My Credentials** option appears on the MyID Authentication screen.

  See the _Editing the configuration file_ and _Requesting an authorization code_ sections.

- Added the `EnableWindowsLogin` option for clients that determines whether operators can log in using their Windows credentials.

- See the _Editing the configuration file_ and _Requesting an authorization code_ sections.

- Added the `EnableHeadlessCardLogin` and `EnableHeadlessPassphraseLogin` options for key pair authentication for mobile identities.

  See the _Editing the configuration file_ section.

- Added details of the `AlwaysIncludeUserClaimsInIdToken` option that allows claims other than `sub` to be returned in the identity token.

  See the _Editing the configuration file_ section.

10.5.14 MyID Core API

The **_MyID Core API_** guide has been updated with the following:

- Information about using refresh tokens to extend authentication to the server.

  See the _Using refresh tokens_ section.

intercede

MyiD CMS

10.5.15   MyID Operator Client

The ***MyID Operator Client*** guide has been updated with the following:

- Added information on using the Self-Service App to manage your credentials from the MyID Authentication screen.

  See the *Managing your credentials from the MyID Authentication screen* section.

- Added details of customizing the number of buttons displayed in the button bar.

  See the *Using the button bar* and *Changing the number of buttons displayed in the button bar* sections.

- Adding information on canceling multiple requests.

  See the *Canceling multiple requests* section.

- Added details of configuring the MyID Operator Client to allow logon using Windows authentication.

  See the *Signing in using Windows authentication* section.

- Added a new section on working with the audit trail in the MyID Operator Client, including viewing stored binary objects.

  See the *Working with the audit trail* and *Viewing audit details* sections.

- Updated the instructions for the existing audit functionality to include viewing audit details.

  See the *Viewing a person's history* and *Unrestricted Audit Report* sections.

- Added details of timeouts and re-authentication.

  See the *Timeouts and re-authentication*, *Configuring re-authentication timeout periods*, and *Enabling or disabling re-authentication* sections.

- Added a reference to the MyID Client WebSocket Service.

  See the *Changing the port* section.

- Added details of the additional fields available on the Person search form.

  See the *People report* section.

- Added details of the **Enable Device** and **Disable Device** operations.

  See the *Enabling and disabling devices* section.

- Added details of launching the **Identify Device (Administrator)** workflow in MyID Desktop from the MyID Operator Client.

  See the *Viewing extended information about a device* section.

- Added details of configuring the Select Security Device screen in the MyID Operator Client to display the associated user image and full name of the cardholder.

  See the *Signing in to MyID* section.

- Added details of using the MyID Operator Client to request mobile devices.

  See the *Requesting a mobile device for a person* and *Requesting a replacement mobile device* sections.

- Updated the details of date entry.

  See the *Entering dates and times* section.

Release Notes   Page 161 of 283

10.5.16 Operator's Guide

The *Operator's Guide* has been updated with the following:

- A disposal status of Lose prevents the card from being reissued.

  See the *Disposing of cards* section.

10.5.17 Self-Service App

The *Self-Service App* guide has been updated with the following:

- Added a note that the `Domain` must contain the NetBIOS domain name and not the DNS format when configuring Integrated Windows Logon.

  See the *Integrated Windows Logon* section.

10.5.18 Smart Card Integration Guide

The *Smart Card Integration Guide* has been updated with the following:

- Information about SafeNet eToken 5110+ FIPS Level 2 tokens has been added.

  See the *Thales authentication devices* section.

- Deprecated the following devices:

  - SafeNet eToken 5110 FIPS

  - SafeNet eToken 5110+

  See the *Thales authentication devices* section.

- Updated information on enabling and disabling capabilities for YubiKey devices to include both NFC and USB interfaces.

  See the *Enabling and disabling device capabilities* section.

- Added information about configuring MyID to save data written to smart card containers to the database.

  See the *Saving container data* section.

- Clarified the meaning of the options for the Per Container PIN Policy for Yubico devices.

  See the *PIN policy settings* section.

- Clarified the effects of disabling the PIV capability for the USB interface.

  See the *Enabling and disabling device capabilities* section.

10.5.19 System Interrogation Utility

The *System Interrogation Utility* guide has been updated with the following:

- Test SIU-123 has been removed, as the MyID database server does not require the PowerShell 2.0 Engine feature.

  See the *Description of derived tests* section.

- Added tests SIU-323 to SIU-330 to cover checking that the web services have been installed and are running.

  See the *Description of derived tests* section.

10.5.20   System Security Checklist

The *System Security Checklist* has been updated with the following:

- Clarification on the **Show Full Name at Logon** and **Show Photo at Logon** configuration options, which now affect the MyID Operator Client.

  See the *Visibility of user data* section.

10.6   End of support features in MyID 12.5.0

There were no end of support features in MyID 12.5.0.

10.7   Known issues resolved in MyID 12.5.0

This section lists the known issues that were resolved in MyID 12.5.0. These are issues that were found across both editions of MyID – Enterprise and PIV – and may not all be relevant for your system.

- IKB-363 – Unable to install the MSCAWebService.

- IKB-364 – Encryption certificates will fail to be written when using the Identity Agent app and system key store on Apple iOS mobile devices.

11 Updates in MyID 12.4.1

This chapter provides details of the changes in MyID 12.4.1, including:

- New and updated features – new features in this version of MyID, and major improvements to existing features.

- Integration updates – updates to MyID's support for smart cards and other credentials, certificate authorities, printers, and HSMs.

- Improvements – minor updates to existing functionality.

Important: At MyID version 12.3, the version of .NET Core used was updated. This affects the MyID servers and all clients. See section *13.3.7*, *.NET Core versions* for details.

Important: Microsoft is making changes to DCOM security over the course of releases in 2021 to 2023 that may affect your system, depending on your configuration. See section *13.2.2*, *Microsoft Windows DCOM server security changes* for details.

11.1 New and updated features

This section contains information on the new and updated features in MyID 12.4.1.

11.1.1 Reprovisioning devices using self-service update

You can now configure the UserSync external system for the **Update My Device** feature in the Self-Service App to carry out a full reprovision of the device instead of an update to the latest version of the credential profile. This is a global option; the same setting is used for all devices.

See the *Self-service device update* section in the ***Self-Service App*** guide.

11.1.2 Restricting credential requests through exclusive groups

If you provide a value in the **Exclusive Group** field in the **Issuance Settings** section of a credential profile, MyID prevents you from requesting or collecting credentials if the cardholder already has an issued device or a request for a device that has a different value in its credential profile for its **Exclusive Group**.

You can request and collect as many credentials as you require that have the same **Exclusive Group** value. You can also request and issue as many credentials as you require that have no value in their **Exclusive Group**.

See the *Exclusive Group* section in the ***Administration Guide*** for details.

11.2 Integration updates

This section contains details of updates to MyID 12.4.1's support for integration with smart cards and other credentials, certificate authorities, printers, and HSMs.

This update does not contain any changes related to integration.

11.3 Improvements

This section provides details of minor improvements to existing functionality within MyID 12.4.1.

11.3.1 General bug fixes and improvements

This release contains general bug fixes and minor improvements as part of a program of continuous improvement.

This release incorporates the following hotfix:

- HOTFIX-12.4.0.1 – Updated MSCAWebService installer.

11.3.2 Forcing new Entrust escrow certificates

You can force Entrust to issue new certificates using the **Entrust force new escrow** configuration option (on the **Certificates** page of the **Operation Settings** workflow). When this option is set to `Yes`, if Entrust returns an existing escrow certificate in response to a request for a new certificate, MyID revokes the certificate and requests the new certificate again.

Setting this option returns MyID to its previous behavior; you are recommended to keep this option at the default `No` for most systems, and set this option to `Yes` only if directed to by Intercede.

See the *Forcing the issuance of new escrow certificates* section of the ***Entrust CA Integration Guide***.

Note: This option is not relevant for the Entrust CA Gateway.

11.4 Documentation updates in MyID 12.4.1

This section contains information on new and updated documentation in MyID 12.4.1.

11.4.1 Administration Guide

The ***Administration Guide*** has been updated with the following:

- Information about new **Exclusive Group** feature in the credential profile.

  See the *Exclusive Group* section.

- Added details of the **Entrust force new escrow** configuration option.

  See the *Certificates page (Operation Settings)* section.

11.4.2 Entrust CA Gateway

The ***Entrust CA Gateway Integration Guide*** has been updated with the following:

- Added information on issuing short-lifetime certificates.

  See the *Controlling certificate lifetimes* section.

11.4.3 Entrust CA Integration Guide

The ***Entrust CA Integration Guide*** has been updated with the following:

- Added details of the **Entrust force new escrow** configuration option.

  See the *Forcing the issuance of new certificates* section.

11.4.4 Entrust nShield HSM Integration Guide

The **_Entrust nShield HSM Integration Guide_** has been updated with the following:

- Clarified the instructions for setting the `CKNFAST_OVERRIDE_SECURITY_ASSURANCES` option to disable the Security Assurance Mechanism.

  See the *Security Assurance Mechanism* section.

11.4.5 Error Code Reference

The **_Error Code Reference_** has been updated with the following:

- Added the following error codes relating to exclusive groups:

  - WS50055 – The user has an existing request or device that exists with a different exclusive group, the request cannot be added.

  - WS50056 – The user has an existing request or device that exists with a different exclusive group, the request cannot be validated.

  See the *MyID Operator Client error codes* section.

11.4.6 Installation and Configuration Guide

The **_Installation and Configuration Guide_** has been updated with the following:

- Configuring Internet Options for the **Collect My Card** workflow.

  See the *Configuring Internet Options* section.

- The information on carrying out your initial server configuration has been moved to a new chapter to correspond with the initial server check stage of the MyID Installation Assistant.

  See the *Initial server configuration* section.

- The information on carrying out your pre-installation configuration has been moved to a new chapter to correspond with the pre-install check stage of the MyID Installation Assistant.

  See the *Pre-installation configuration* section.

- The information on post-installation configuration has been updated and reorganized to correspond better with the post-install check stage of the MyID Installation Assistant.

  See the *After installing MyID* section.

- Removed details of running the MyID Installation Assistant from the command line.

  See the *Running the Installation Assistant* section.

11.4.7 Self-Service App

The **_Self-Service App_** guide has been updated with the following:

- The external system configuration for the Update My Device feature now allows you to configure the feature to carry out a reprovision rather than an update of the device.

  See the *Self-service device update* section.

11.5 End of support features in MyID 12.4.1

There were no end of support features in MyID 12.4.1.

11.6   Known issues resolved in MyID 12.4.1

There were no known issues resolved in MyID 12.4.1.

12 Updates in MyID 12.4.0

This chapter provides details of the changes in MyID 12.4.0, including:

- New and updated features – new features in this version of MyID, and major improvements to existing features.

- Integration updates – updates to MyID's support for smart cards and other credentials, certificate authorities, printers, and HSMs.

- Improvements – minor updates to existing functionality.

Important: At MyID version 12.3, the version of .NET Core used was updated. This affects the MyID servers and all clients. See section *13.3.7*, *.NET Core versions* for details.

Important: Microsoft is making changes to DCOM security over the course of releases in 2021 to 2023 that may affect your system, depending on your configuration. See section *13.2.2*, *Microsoft Windows DCOM server security changes* for details.

12.1 New and updated features

This section contains information on the new and updated features in MyID 12.4.0.

12.1.1   The MyID Installation Assistant
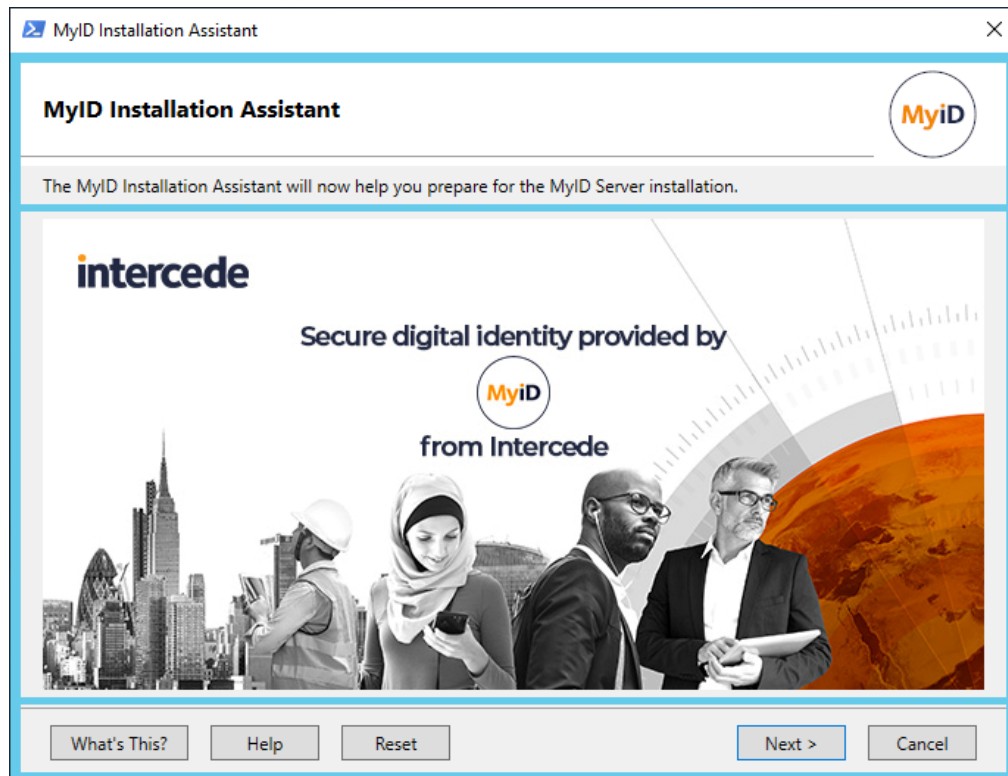
The MyID Installation Assistant is a major new feature of this release, and provides a new and comprehensive way of installing MyID. Combining the features of the installation program, a package manager, the System Interrogation Utility, and the Server Diagnostic Report, the MyID Installation Assistant guides you through the process of installing MyID.

The MyID Installation Assistant extends the capabilities of the System Interrogation Utility; if your system fails to pass a test, where possible the MyID Installation Assistant provides a signed PowerShell script to address the issue; for example, if your MyID COM+ user is not a member of the Distributed COM Users group, the script can add the user to the group; or if your web server does not have the IIS Management Console role, the script can add that role to your system. You can review these scripts before running them to ensure that you are in control of the changes to your system. You can run these tests before, during, and after installing MyID, or run them to check the configuration of an existing installation.

The MyID Installation Assistant also incorporates a package manager, which means it can install MyID (for example, MyID 12.4.0), install an update (for example, 12.4.2), install a server configuration package for custom functionality (for example, CONFIG-9999.1.1) and a hotfix (for example, HOTFIX-12.4.2.1) to install a system with the latest software without the need to run multiple installation packages manually in the correct order.

You can also use the MyID Installation Assistant to carry out upgrades from existing MyID 11 and MyID 12 systems. For upgrades from MyID 11 the Installation Assistant handles the changes from 32-bit to 64-bit software without the need to run the separate upgrade migration script.

For details, see the *MyID Installation Assistant* section in the ***Installation and Configuration Guide***.

Note: The System Interrogation Utility and the Server Diagnostic Report have been incorporated into the MyID Installation Assistant; however, you can still install and run these utilities separately if required. The location of the files for the utilities has changed; see the *System Interrogation Utility* and *Server Diagnostic Report Utility* sections of the ***Implementation Guide*** for details.

12.1.2   Launching administrative workflows in the MyID Operator Client

You can launch individual administrative workflows from the **More** category in the MyID Operator Client. The **More** category appears if you have access to one or more workflows in the category.
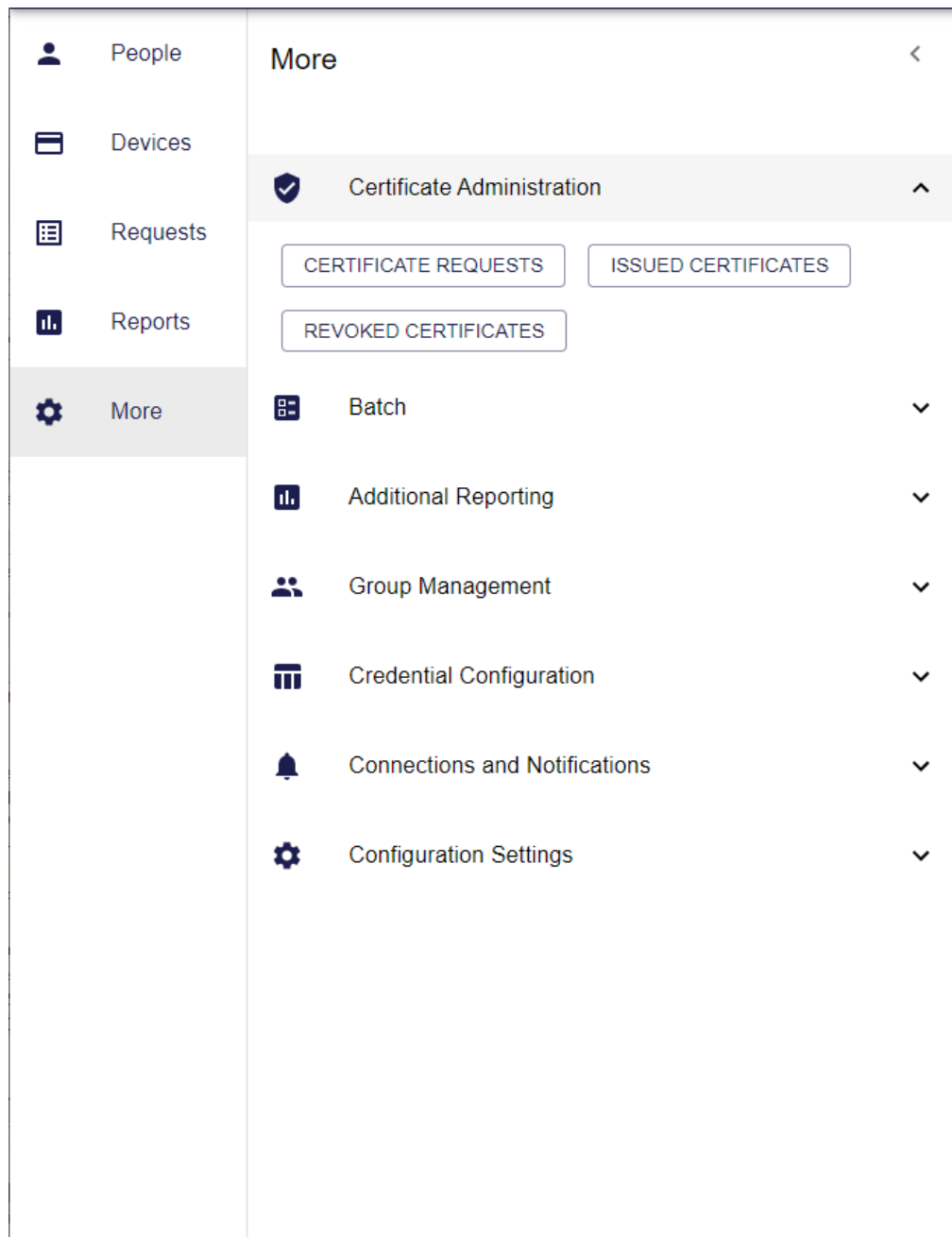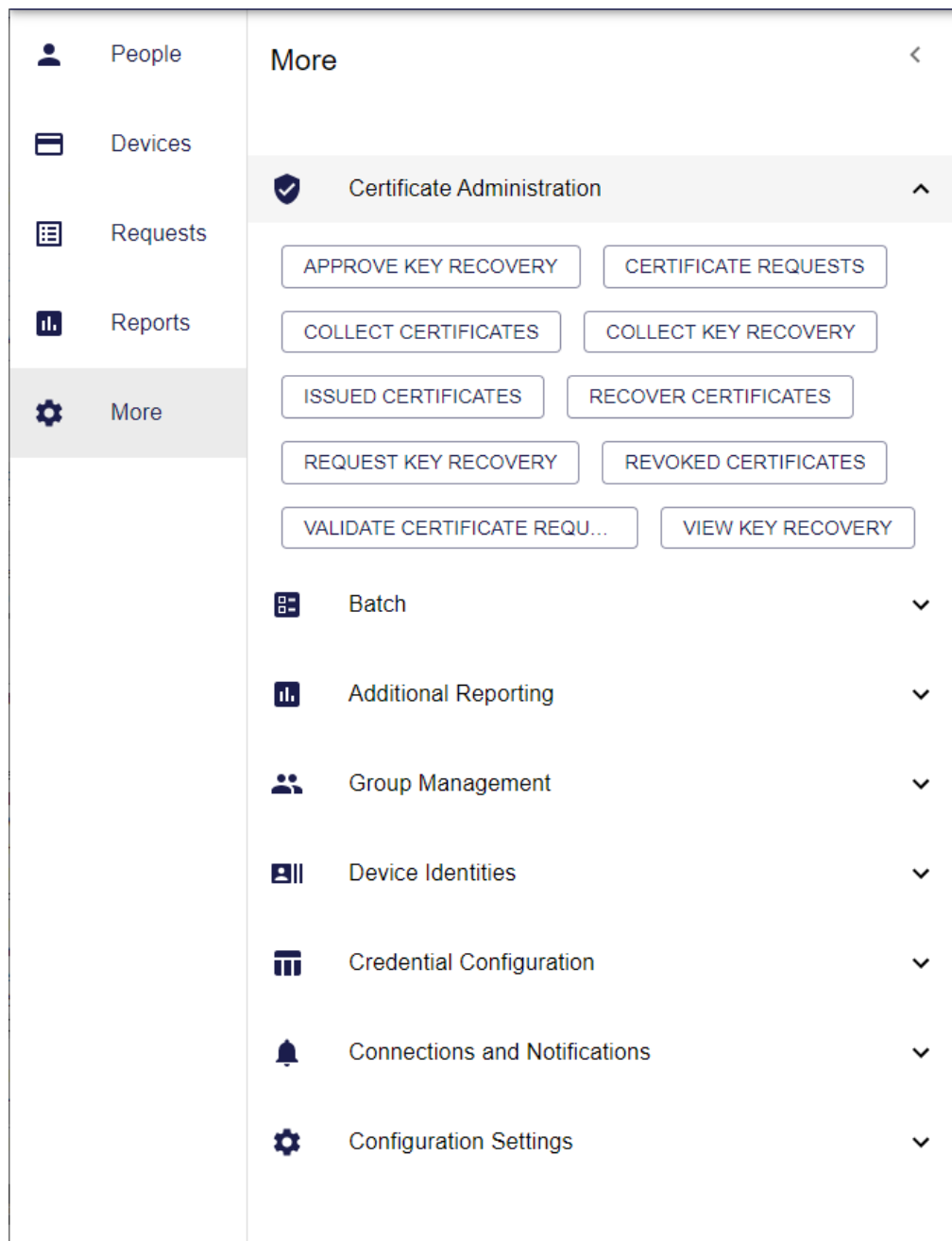
For example, you can launch the **Credential Profiles** workflow to add or update a credential profile, or launch the **System Events** workflow to view details of events that have occurred in the system log. Access to each workflow is controlled by your role, as in MyID Desktop.

You can launch the workflow from the MyID Operator Client, carry out the task you need to perform, then close the MyID Desktop window and carry on working in the MyID Operator Client. MyID handles all of the authentication for you, so you do not need to log in to MyID Desktop again – the process is seamless.

For details of which workflows you can use, see the *Launching administrative workflows* section in the **MyID Operator Client** guide.

12.1.3 Carrying out self-service operations in the MyID Operator Client

You can now click on the user icon in the top right of the MyID Operator Client screen to open the self-service menu.
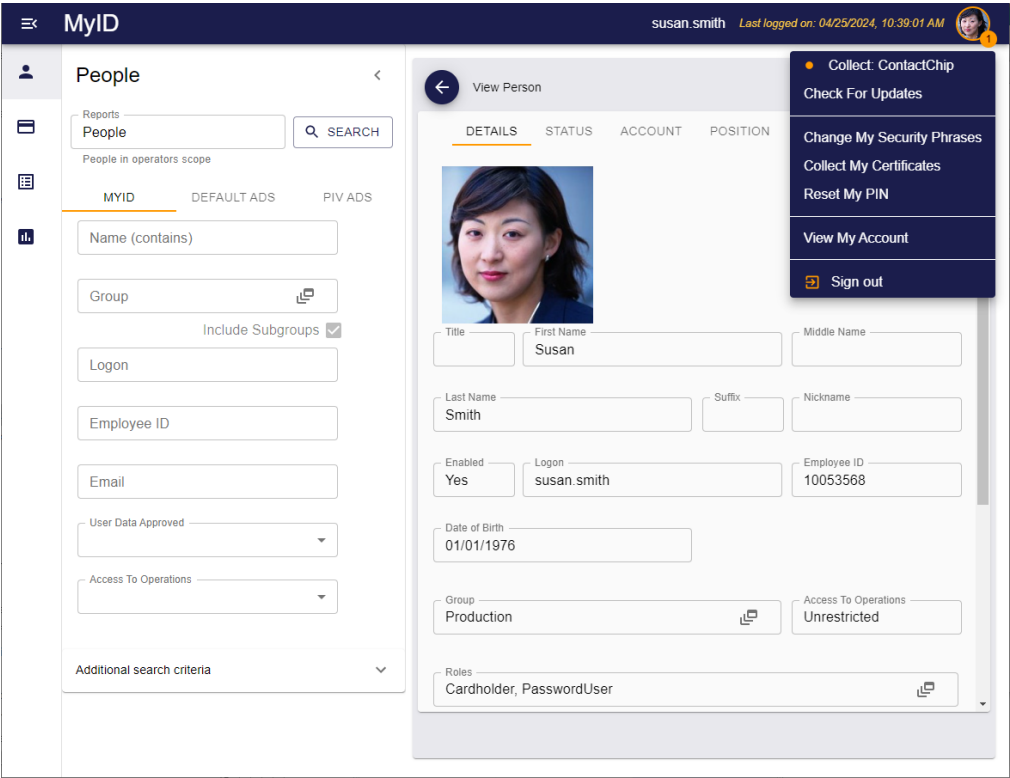
The user icon displays a badge with the number of requests available for you to collect; these requests are listed at the top of the menu.

You can also launch a variety of self-service operations in the Self-Service App or MyID Desktop from this menu.

For details, see the *Carrying out self-service operations* section in the ***MyID Operator Client*** guide.

12.1.4 Launching workflows from the View Device screen

You can now launch additional MyID Desktop workflows from the View Device screen. When you launch the workflow, the device you are viewing is automatically selected.

You can now launch the following workflows:

* **Manage VSC Access**

  See the *Requesting, updating, and canceling VSC locks* section in the ***MyID Operator Client*** guide.

* **Unlock VSC Temporary Access**

  See the *Providing time-limited VSC access* section in the ***MyID Operator Client*** guide.

* **Reinstate Card**

  See the *Reinstating a device* section in the ***MyID Operator Client*** guide.

* **Card Disposal**

  See the *Disposing of a device* section in the ***MyID Operator Client*** guide.

* **Print Mailing Document**

  See the *Printing a mailing document* section in the ***MyID Operator Client*** guide.

* **Change PIN**

  See the *Changing a device PIN* section in the ***MyID Operator Client*** guide.

12.1.5 Launching workflows from the View Person screen

You can now launch additional MyID Desktop workflows from the View Person screen. When you launch the workflow, the person you are viewing is automatically selected.

You can now launch the following workflows:

* **Authenticate Person**

  See the *Authenticating a person using MyID Desktop* section in the ***MyID Operator Client*** guide.

* **Change Security Phrases**

  See the *Changing a person's security phrases* section in the ***MyID Operator Client*** guide.

* **Unlock Security Phrases**

  See the *Unlocking a person's security phrases* section in the ***MyID Operator Client*** guide.

* **Manage Additional Identities**

  Note: This feature was replaced by the MyID Operator Client features for managing additional identities in MyID 12.7. See the *Working with additional identities* section in the ***MyID Operator Client*** guide.

* **Print Badge**

  See the *Printing a badge* section in the ***MyID Operator Client*** guide.

12.1.6 Launching workflows from the View Request screen

You can now launch an additional MyID Desktop workflow from the View Request screen. When you launch the workflow, the request you are viewing is automatically selected.

You can now launch the following workflow:

- **Deliver Card**

Note: This feature was superseded in MyID 12.7 by the **Accept Delivery** features. See the *Accepting delivery for a device* section in the *__MyID Operator Client__* guide.

12.1.7 Auditing the client IP address and identifier

MyID now captures the IP address and the client identifier of the workstation used to carry out the audited operation, and stores this information in the audit trail.

You can configure whether to capture this information using the following new configuration options on the **Server** page of the **Security Settings** workflow:

- **Capture Client Identifier** – Set this option to Yes to capture the client identifier

- **Capture IP Address** – Set this option to Yes to capture the client IP address.

By default, the client identifier is the fully-qualified domain name of the client PC; for example, `myworkstation.mydomain.local`. You can customize the client identifier by setting an option in the application's configuration file or the workstation's registry.

See the *Logging the client IP address and identifier* and *Specifying a custom client identifier* sections in the *__Administration Guide__* for details.

12.1.8 Collect Updates workflow

The new **Collect Updates** workflow allows you to collect updates that have been requested for another person, including credential profile updates, certificate renewals, and reprovision requests.

You can launch this workflow from MyID Desktop, or from the View Device screen of the MyID Operator Client.

For more information, see the *Collect Updates workflow* section in the *__Operator's Guide__* and the *Collecting updates for another person's device* section in the *__MyID Operator Client__* guide.

12.1.9 Email notifications for derived credential requests

You can now configure MyID to send an email notification to the owner of the deriving credential when a derived credential is requested through the Self-Service Request Portal.

MyID can obtain the email address from a certificate on the deriving credential and use this for the notification; it may also use the email address from the user account in MyID or the directory, depending on how you have configured it.

See the *Configuring email notifications* section in the *__Derived Credentials Self-Service Request Portal__* guide for details.

12.1.10 Global PIN

PIV cards support only numeric PINs for their user PINs. If you want to use alphanumeric PINs, your smart card must support Global PINs; this is an alternative PIN that can allow a wider range of characters, if the smart card has been manufactured to a custom specification that allows this. When you issue a smart card with its Global PIN enabled, the user PIN and the user PUK (Personal Unblocking Key) are disabled, and the Global PIN and Global PUK are used instead.

To issue a smart card with a Global PIN, you must enable the **Use Global PIN** option in the **PIN Settings** section of the **Credential Profiles** workflow. See the *PIN Settings* section of the ***Administration Guide*** for details.

If you are using server-generated PINs, you must use a PIN generator that supports alphanumeric characters. This release of MyID contains an enhancement to PIN generation to support this feature; see section *12.1.13*, *PIN generation and PIN policies*.

The Global PIN feature is supported within MyID only on IDEMIA smart cards that have this capability. Currently, this includes the following:

- IDEMIA ID-One PIV 2.4.2 on Cosmo V8.2 smart cards, manufactured to *BAP#087583 – ID-One PIV 2.4 on Cosmo v8.2 Global PIN*. This specification of card has been manufactured to require alphanumeric PINs. Within MyID this type of card is displayed with a device type of "IDEMIA ID-One PIV 2.4 on Cosmo v8.2 GT (GovTech)".

  See the *Global PIN support* section of the ***Smart Card Integration Guide***.

The MyID Card Utility has also been updated to support Global PINs for devices that support this feature.

12.1.11 Enhanced integration with Mobile Device Management systems

MyID now provides the following features for integration with Mobile Device Management (MDM) systems:

- Connection to a Microsoft Intune MDM.

  You can set up an external system to authenticate to a Microsoft Intune MDM.

  See the *Setting up an external system for Intune* section in the ***Mobile Identity Management*** guide for details.

- Setting up a credential profile for MDM restrictions.

  You can configure a credential profile to issue only to devices registered with the MDM, and you can require particular attributes of registered devices as stored in the MDM.

  See the *Configuring credential profiles for MDM restrictions* section in the ***Mobile Identity Management*** guide for details.

Note: These features require a compatible version of the MDM. Contact Intercede quoting SUP-367 for more information.

12.1.12   MSIX client installation programs

Intercede now provides MSIX versions of the installation programs for MyID Desktop, the Self-Service App, and the MyID Client Service. These are intended for an administrator to create an installation package that combines all of the necessary client software and administrator-controlled configuration.

MSIX is a Microsoft technology for packaging your apps. It supports the following features:

- Combining all of your client software in a single installation package.

  The MyID Operator Client requires the MyID Client Service, and makes use of MyID Desktop (for administrative operations) and the Self-Service App (for self-service operations). You are recommended to combine all of these applications into a single package for distribution to your MyID Operator Client users.

- Distributing a configuration package containing all required client configuration and customization.

  For example, the location of the MyID server, or files for rebranding.

- Configuring automatic updates.

The installation structure comprises an MSIX installer for the MyID Client Suite, which contains all of the common files for the MyID client software, and MSIX installers for the following client applications:

- MyID Desktop

- Self-Service App

- MyID Client Service

The installers are provided in the following folder in the MyID release image:

`\MyID Clients\MyID Client Suite`

Intercede also provides MSIX versions of the following additional software:

- Fargo Printer Support

These additional installers are distributed separately, but you can combine them into a package for distribution and installation with the rest of the client software.

For more information, see the ***MyID Client MSIX Installation Guide*** in the MyID Client Suite folder.

12.1.13 PIN generation and PIN policies

MyID allows you to generate PINs for your devices, either through using a random PIN generator (MyID generates a random PIN, then emails the cardholder with the PIN) or a server PIN generator (MyID uses a known algorithm and a secure key to generate a PIN based on the device serial number, which you can regenerate on another system if you know the algorithm and the secure key).

Previously, these PIN generation options did not take into account the PIN character settings configured in the credential profile (for example, a PIN that may contain lower alpha and upper alpha characters, and must contain at least one numeric character).

The random PIN generator has been enhanced to allow you to configure MyID to respect the PIN character settings on the credential profile when generating random PINs, using the **Use PIN policy settings in random server PIN generation** configuration option (on the **PINs** page of the **Security Settings** workflow).

Because the EdeficePinGenerator uses a publicly-published algorithm, this PIN generator has *not* been changed.

Instead, an additional server PIN generator is provided – EdeficePolicyPinGenerator – that uses a new algorithm that takes into account the PIN character settings configured on the credential profile. Unlike the previously-provided EdeficePinGenerator, this PIN generator can generate PINs that contain more than just numeric characters.

Note: If you configure the PIN character settings in the credential profile to specify only numeric characters in the PIN, the EdeficePolicyPinGenerator and EdeficePinGenerator produce the same PINs based on the same device serial number and secure key.

For information on using these PIN generators, see the *PIN generation* section in the *Administration Guide*.

12.1.14 Requesting updates for a device from the MyID Operator Client

You can use the **Request Update** option on the View Device screen in the MyID Operator Client to request an update for a device, either to update the device to the latest version of the credential profile used to issue it, or to reprovision it completely, using either the same credential profile or a different credential profile.

See the *Requesting an update for a device* section in the *MyID Operator Client* guide.

You can also carry out this operation from the MyID Core API using the following method:

```
POST /api/Devices/{id}/update
```

12.1.15 Setting up a custom PKCS #10 request

For requests made using the REST API for mobile credentials (rest.provision) you can customize the PKCS #10 certificate signing request where the subject name is provided in the request; you can create a DN from the information stored in the `vPeopleUserAccounts` view in the MyID database for the person for whom the request was made.

See the *Setting up a custom PKCS #10 request* section in the *Mobile Identity Management* guide for details.

12.2   Integration updates

This section contains details of updates to MyID 12.4.0's support for integration with smart cards and other credentials, certificate authorities, printers, and HSMs.

12.2.1   Additional identities

If you want to issue additional identities to devices with PIV applets, you must have a Windows minidriver installed to make the certificates available for uses such as Windows logon. MyID has now been tested issuing additional identities with the following:

- Yubikey devices in conjunction with the Yubikey minidriver.
- IDEMIA PIV cards using the IDEMIA minidriver.

For more information, see the *Additional identities on devices with PIV applets* section in the *Administration Guide*.

12.2.2   Entrust nShield HSMs

The HSMs previously known as nCipher nShield are now Entrust nShield HSMs. The documentation throughout has been updated to reflect this.

The *Entrust nShield HSM Integration Guide* is the new name for the *nCipher nShield HSM Integration Guide*.

12.2.3   IDEMIA devices

MyID now supports the IDEMIA ID-One PIV 2.4.2 on Cosmo V8.2 smart card in the following additional configuration:

- BAP#087583 – ID-One PIV 2.4 on Cosmo v8.2 Global PIN

See the *IDEMIA smart cards* section of the *Smart Card Integration Guide*.

12.2.4   Remote Microsoft CA

Problems have been identified with the ability to integrate with a Microsoft Certificate Authority on a remote domain (Remote Microsoft Certificate Authority).

Note: If you are using Microsoft Certificate Authority and it is hosted on the same domain as MyID, you will not be affected by this issue.

See the *Remote Microsoft Certificate Authority* section in the *Microsoft Windows CA Integration Guide*.

12.2.5   Thales authentication devices

MyID now supports the following Thales authentication device:

- IDPrime MD830nc

See the *Thales authentication devices* section of the *Smart Card Integration Guide*.

12.2.6   Yubico devices

The *Yubico smart cards* chapter of the **Smart Card Integration Guide** has been updated to cover enhancements to support for YubiKey devices:

- You can now use PIV PUK and Configuration Lock Code keys to secure your devices; see the *Setting up the PIV PUK key* and *Setting up the Configuration Lock Code* sections.

- The recommended cryptographic keys for YubiKey SC and YubiKey SC FIPS have been updated; see the *Cryptographic keys for Yubico cards* section.

- You can enable or disable device capabilities; see the *Enabling and disabling device capabilities* section.

12.3   Improvements

This section provides details of minor improvements to existing functionality within MyID 12.4.0.

12.3.1   General bug fixes and improvements

This release contains general bug fixes and minor improvements as part of a program of continuous improvement.

12.3.2   Cancel Card email notification

MyID now sends a notification to a cardholder when their device has been canceled, providing information about the serial number and device type.

The email template name is **Cancel Card** and has an ID of 219.

See the *Email notification* section in the **Administration Guide** for details of working with email notifications and email templates.

This notification is useful when working with derived credentials; see the *Editing the cancellation email template* section in the **Derived Credentials Self-Service Request Portal** guide.

12.3.3   Issue over Existing Credential option

For mobile derived credentials issued through an MDM, you can set the **Issue over Existing Credential** option in the **Issuance Settings** section of the **Credential Profiles** workflow.

When this option is set, if the device is already issued to the target user, it is automatically canceled and then the new device issued.

See the *Creating an Identity Agent credential profile* section of the **Derived Credentials Self-Service Request Portal** guide for details.

12.3.4   Logging for Windows clients

The Windows clients (MyID Desktop, Self-Service App, Self-Service Kiosk, and MyID Client Service) now use the same simplified method to enable logging.

See the *Windows clients* section in the **Configuring Logging** guide for details.

12.3.5 Mobile Devices report

You can now provide access to an additional report in the Devices category in the MyID Operator Client that provides details on the mobile devices in your system.

See the *Mobile Devices report* section in the **MyID Operator Client** guide for details.

12.3.6 Permissions for MyID Core API calls

You can now configure the documentation for the MyID Core API to display a list of the permissions that provide access to each API call.

See the *Accessing the API documentation* and *Accessing the API features* sections in the **MyID Core API** guide for details.

12.3.7 SSRP role configuration

The Derived Credentials Self-Service Request Portal has been updated to allow you to control whether a role specified in the configuration file is added to the list of roles for an existing user account, or is used only to filter the available credential profiles.

See the details about the `doNotUpdateUser` attribute in the *Configuration file format* section of the **Derived Credentials Self-Service Request Portal** guide.

12.4 Documentation updates in MyID 12.4.0

This section contains information on new and updated documentation in MyID 12.4.0.

12.4.1 Administration Guide

The *Administration Guide* has been updated with the following:

- Information about new PIN generation features.

  See the *PIN generation* section.

- Added the new **Use PIN policy settings in random server PIN generation** configuration option.

  See the *PINs page (Security Settings)* section.

- Added the new **Use Global PIN** credential profile option.

  See the *PIN Settings* section.

- Added the new **Verify Fingerprints During Card Update** and **Verify Fingerprints During Reset PIN** credential profile options.

  See the *Issuance Settings* section.

- Added information on capturing client IP address and identifier in the audit trail.

  See the *Logging the client IP address and identifier* section.

- Added configuration options for the client IP address and identifier.

  See the *Server page (Security Settings)* section.

- Added the new **Update email address from derivation** configuration option.

  See the *Certificates page (Operation Settings)* section.

- Updated the details of support for additional identities on PIV devices.

  See the *Additional identities on devices with PIV applets* section.

- Added details of the **Issue over Existing Credential** credential profile option.

  See the *Issue over Existing Credential* section.

- Added a note that the **Use Entrust default key update policy** configuration option is not relevant for the Entrust CA Gateway.

  See the *Certificates page (Operation Settings)* section.

- Clarified which operations are permitted with key recovery cards.

  See the *Key recovery* section.

12.4.2 Advanced Configuration Guide

The *Advanced Configuration Guide* has been updated with the following:

- Updated schedules for expiring items warnings.

  See the *Monitoring the expiry of system credentials* section.

intercede

12.4.3 Configuring Logging

The **_Configuring Logging_** document has been updated with the following:

- Combined the sections on logging the Windows clients (MyID Desktop, Self-Service App, Self-Service Kiosk, and MyID Client Service) into a single section as they now use the same configuration to set up logging.

  See the *Windows clients* section.

12.4.4 Derived Credentials Self-Service Request Portal

The **_Derived Credentials Self-Service Request Portal_** guide has been updated with the following:

- Details of the `doNotUpdateUser` attribute, which allows you to control whether a specified role is added to an existing user or is used only for filtering credential profiles.

  See the *Configuration file format* section.

- Added the new **Update email address from derivation** configuration option.

  See the *MyID configuration options* section.

- Added information about configuring email notifications.

  See the *Configuring email notifications* section.

- Added details of the **Issue over Existing Credential** credential profile option.

  See the *Creating an Identity Agent credential profile* section.

12.4.5 Entrust CA Gateway

The **_Entrust CA Gateway Integration Guide_** has been updated with the following:

- Note on not passing subject DN components through policy attributes.

  See the *Enabling certificate policies* section.

- Additional information about using the **Reverse DN** option.

  See the *Enabling certificate policies* section.

- Added `utf8` as an encoding option for policy extended attributes, and updated the example for User Principal Name to use this encoding.

  See the *Adding policy extended attributes* section.

- Added information on controlling certificate lifetimes, including the limitation that the minimum lifetime is seven days.

  See the *Controlling certificate lifetimes* and *Limitations* sections.

- The **Key Algorithm** and **Key Purpose** fields are now read-only, and obtain their value from the options configured for the policy on the CA.

  See the *Enabling certificate policies* section.

12.4.6 Entrust CA Integration Guide

The **_Entrust CA Integration Guide_** has been updated with the following:

- Updated the supported version numbers.

  See the *Supported Entrust versions* section.

12.4.7 Entrust nShield HSM Integration Guide

The ***Entrust nShield HSM Integration Guide*** is the new name for the *nCipher nShield HSM Integration Guide*.

12.4.8 Error Code Reference

The ***Error Code Reference*** has been updated with the following:

- Updated MyID Operator Client error wording and possible solutions.

  See the *MyID Operator Client error codes* section.

- Added new error codes related to requesting device updates:

  - WS40044 – There are no status mappings available for the selected operation.

  - WS40045 – The device cannot be updated because it has already expired.

  - WS40046 – The device cannot be updated because the issuance process has not been completed.

  - WS40047 – The device cannot be updated because it does not have a credential profile.

  - WS50052 – The device owner has a maximum expiry date that is earlier than the expiry date of the device. The update cannot be requested because the credential profile does not have Ignore User Expiry Date set.

  - WS50053 – The capabilities of the selected credential profile are not supported by this operation.

  - WS50054 – The selected credential profile has different capabilities to the current device credential profile.

  See the *MyID Operator Client error codes* section.

- Added a new error code related to biometric authentication:

  - 800630 – Biometrics are required.

  See the *Web Service error codes* section.

12.4.9 Implementation Guide

The ***Implementation Guide*** has been updated with the following:

- Updated the locations of the System Interrogation Utility (SIU) and Server Diagnostic Report (SDR), as they have been incorporated into the MyID Installation Assistant.

  See the *System Interrogation Utility* and *Server Diagnostic Report Utility* sections.

12.4.10   Installation and Configuration Guide

The ***Installation and Configuration Guide*** has been updated with the following:

- Added information on using the MyID Installation Assistant.

  See the *MyID Installation Assistant*, *Running the installation program*, *Running the update installation program*, and *Upgrading MyID* sections.

- The installation user must have a default schema of `dbo` in SQL Server if you are installing to an existing database.

  See the *Installation account* section.

- Recommendation to keep .NET Core updated with security releases from Microsoft, and a known issue where the .NET Core Desktop Runtime versions 6.0.1 and 6.0.2 cause a problem with the MyID Client Service.

  See the *Prerequisites* section.

- Removed the following entry from the list of required Windows features for the web server:

  - Web Server (IIS)\Management Tools\Management Service

  See the *Setting up server roles* section.

- Updated the list of supported client operating systems.

  See the *Operating systems* section.

- Added a new requirement to install the .NET Runtime package on the MyID application server.

  See the *Prerequisites* section.

- Updated the tested version of the Microsoft OLE DB Driver to 18.6.3.

  See the *Installing the database software* section.

- Added instructions on upgrading to a new server.

  See the *Upgrading to a new server* section.

12.4.11   Mobile Identity Management

The ***Mobile Identity Management*** guide has been updated with the following:

- Added information on creating a custom PKCS #10 request.

  See the *Setting up a custom PKCS #10 request* section.

- Updated the list of supported MDMs.

  See the *Supported Mobile Device Management integration* section.

- Added information about integration with MDMs.

  See the *Setting up your MDM system* section.

12.4.12   MyID Core API

The ***MyID Core API*** guide has been updated with the following:

- Information about providing a client identifier in the http header.

  See the *Providing a client identifier* section.

- Added information on configuring the API documentation to display the permissions that provide access to each API call.

  See the *Accessing the API documentation* and *Accessing the API features* sections.

12.4.13   MyID Operator Client

The *MyID Operator Client* guide has been updated with the following:

- Information about collecting updates for another person's device.

  See the *Collecting updates for another person's device* section.

- Added details of the MyID Desktop administrative workflows you can launch from the new **More** category within the MyID Operator Client.

  See the *Launching administrative workflows* section.

- Added details of the Request Update option on the View Device screen.

  See the *Requesting an update for a device* section.

- Added a known issue where the .NET Core Desktop Runtime versions 6.0.1 and 6.0.2 cause a problem with the MyID Client Service.

  See the *.NET Core Desktop Runtime versions* section.

- Added details of launching the **Authenticate Person** workflow from the View Person screen.

  See the *Authenticating a person* section.

- Added details of launching the **Change Security Phrases** and **Unlock Security Phrases** workflows from the View Person screen.

  See the *Working with security phrases* section.

- Added details of launching the **Manage Additional Identities** workflow from the View Person screen.

  Note: This feature has been superseded in MyID 12.7 by the additional identities features added to the MyID Operator Client; see the *Working with additional identities* section.

- Added details of launching the **Print Badge** workflow from the View Person screen.

  See the *Printing a badge* section.

- Added details of launching the **Deliver Card** workflow from the View Request screen.

  Note: This feature has been superseded in MyID 12.7 by the **Accept Delivery** feature; see the *Accepting delivery for a device* section.

- Added details of launching the **Manage VSC Access** and **Unlock VSC Temporary Access** workflows from the View Device screen.

  See the *Managing VSCs* section.

- Added details of launching the **Reinstate Card** workflow from the View Device screen.

  See the *Reinstating a device* section.

- Added details of launching the **Card Disposal** workflow from the View Device screen.

  See the *Disposing of a device* section.

- Added details of launching the **Print Mailing Document** workflow from the View Device screen.

  See the *Printing a mailing document* section.

- Added details of launching the **Change PIN** workflow from the View Device screen.

See the *Changing a device PIN* section.

- Added troubleshooting information for issues relating to launching MyID Desktop or the Self-Service App.

  See the *Troubleshooting MyID Client Service connection issues* section.

- Added information on using the self-service menu.

  See the *Carrying out self-service operations* section.

- Added information on the Mobile Devices report.

  See the *Mobile Devices report* section.

- Updated the table of **Edit Roles** options mapping to MyID Operator Client features.

  See the *Roles and groups* section.

12.4.14   Operator's Guide

The *Operator's Guide* has been updated with the following:

- Information about using the Collect Updates workflow to collect updates for another person's device.

  See the *Collect Updates workflow* section.

- Added a note about the behavior of the Card PIN authentication method in the **Reset Card PIN** workflow in relation to server-generated PINs.

  See the *Resetting a card's PIN* section.

12.4.15   Printer Integration Guide

The *Printer Integration Guide* has been updated with the following:

- Added a note that you must not connect the printer before being prompted when installing the Entrust Datacard printer driver.

  See the *Entrust Datacard printers* section.

12.4.16   PrimeKey EJBCA Integration Guide

The *PrimeKey EJBCA Integration Guide* has been updated with the following:

- Removed requirement to set the **Batch Generation** option.

  See the *Configuring end entity profiles* and *Key escrow policy configuration overview* sections.

- Generating subject DNs for EJBCA certificate requests.

  See the *Configuring end entity profiles* and *Key escrow policy configuration overview* sections.

- Added further details of the behavior of the **Reverse DN** option.

  See the *Enabling certificates policies on a CA* section.

12.4.17   Reporting Web Service API

The *Reporting Web Service API* guide has been updated with the following:

- Updated instructions on client certificate mapping for 2-way SSL.

  See the *Enabling 2-way SSL* section.

12.4.18 Securing Websites and Web Services

The *Securing Websites and Web Services* guide has been updated with the following:

- Updated instructions on client certificate mapping for 2-way SSL.

  See the *Configuring IIS client certificates* section.

12.4.19 Smart Card Integration Guide

The *Smart Card Integration Guide* has been updated with the following:

- Support for the IDEMIA ID-One PIV 2.4.2 on Cosmo V8.2 smart card has been extended to include the BAP#087583 configuration, which provides support for Global PIN.

  See the *IDEMIA smart cards* and *Global PIN support* sections.

- Support for YubiKey devices has been enhanced to provide support for PIV PUK and Configuration Lock Code keys, updated key settings for YubiKey SC and YubiKey SC FIPS devices, and configuring device capabilities.

  See the *Setting up the PIV PUK key*, *Setting up the Configuration Lock Code*, *Cryptographic keys for Yubico cards*, and *Enabling and disabling device capabilities* sections.

- Support for IDPrime MD830nc smart cards has been added.

  See the *Thales authentication devices* section.

- Updated the details of support for additional identities on IDEMIA PIV cards.

  See the *Additional identities for IDEMIA PIV cards* section.

12.4.20 System Interrogation Utility

The *System Interrogation Utility* guide has been updated with the following:

- Added new test SIU-321, which checks that .NET Core has been installed after IIS.

  See the *Description of derived tests* section.

- Added new test SIU-322, which provides a warning if CRL checks are required but there is no Internet access.

  See the *Description of derived tests* section.

12.5 End of support features in MyID 12.4.0

There were no end of support features in MyID 12.4.0.

12.6 Known issues resolved in MyID 12.4.0

This section lists the known issues that were resolved in MyID 12.4.0. These are issues that were found across both editions of MyID – Enterprise and PIV – and may not all be relevant for your system.

- IKB-356 – The Read Card operation returns error WS50040 for Key Recovery cards.

- IKB-357 – "Credential Profile is incompatible with this request" error returned incorrectly for some issued devices.

13 Updates in MyID 12.3.0

This chapter provides details of the changes in MyID 12.3.0, including:

- New and updated features – new features in this version of MyID, and major improvements to existing features.

- Integration updates – updates to MyID's support for smart cards and other credentials, certificate authorities, printers, and HSMs.

- Improvements – minor updates to existing functionality.

Important: The version of .NET Core used in this version of MyID has been updated. This affects the MyID servers and all clients. See section *13.3.7*, *.NET Core versions* for details.

Important: Microsoft is making changes to DCOM security over the course of releases in 2021 to 2023 that may affect your system, depending on your configuration. See section *13.2.2*, *Microsoft Windows DCOM server security changes* for details.

13.1 New and updated features

This section contains information on the new and updated features in MyID 12.3.0.

13.1.1 Assigning devices to requests

You can assign a specific device to an issuance or replacement issuance request in the MyID Operator Client. This ensures that the request can be collected using the specified device only.

You can insert the device to assign it to the request, or you can search for the device from the list of devices already known to MyID.

If you no longer want to associate a specific device with a request, you can unassign it.

See the *Assigning a device to a request* section in the **MyID Operator Client** guide for details.

13.1.2   Collecting your own device in the MyID Operator Client

Previously, the MyID Operator Client added the ability to collect devices for other users within the MyID Operator Client by launching the **Collect Card** workflow in a MyID Desktop window, allowing for seamless operation from a single logon.

This feature has now been enhanced to support collecting a device for a request for yourself; when you click the **Collect** option in the button bar at the bottom of the View Request screen, the behavior depends on the target of the request.

- If the request is for another person:

  The **Collect Card** workflow appears in a MyID Desktop window with the request already selected.

- If the request is for yourself:

  The **Collect My Card** feature appears in a Self-Service App window with the request already selected.

See the *Collecting a device request* section in the ***MyID Operator Client*** guide for details.

This feature requires the installation and configuration of the Self-Service App on the operator's workstation. See the *Launching MyID Desktop or Self-Service App workflows* section in the ***MyID Operator Client*** guide for details.

Important: To use this feature, you must upgrade your MyID Client Service and Self-Service App software to the latest versions.

13.1.3   Collecting device updates in the MyID Operator Client

You can now collect updates for your own device. When you click the **Collect Updates** option in the button bar at the bottom of the View Device screen, the MyID Operator Client checks whether there are any update jobs available, and if required the **Collect My Updates** feature appears in a Self-Service App window with the device update task already selected.

See the *Updating a device* section in the ***MyID Operator Client*** guide for details.

This feature requires the installation and configuration of the Self-Service App on the operator's workstation. See the *Launching MyID Desktop or Self-Service App workflows* section in the ***MyID Operator Client*** guide for details.

Important: To use this feature, you must upgrade your MyID Client Service and Self-Service App software to the latest versions.

13.1.4 Configuring authentication code complexity

This release contains several enhancements relating to the complexity of authentication codes.

13.1.4.1 Auth Code page

The **Security Settings** workflow has a new page called **Auth Code**. This page gathers configuration options relating to authentication codes in one place for ease of access.

This page contains the following options:

- **Auth Code Complexity** – new for MyID 12.3.
- **Auth Code Lifetime** – previously on the **PINs** tab.
- **Auth Code Lifetime for Immediate Use** – previously on the **PINs** tab.
- **Complex Logon Code Complexity** – previously on the **Logon** tab.
- **Logon Code Lifetime** – previously on the **PINs** tab.
- **Simple Logon Code Complexity** – previously on the **Logon** tab.

The documentation has been updated throughout to reflect the location of these configuration options.

See the *Auth Code page (Security Settings)* section in the ***Administration Guide*** for details.

13.1.4.2 Generate Logon Code option renamed Generate Code on Request

The **Generate Logon Code** option in the credential profile has been renamed **Generate Code on Request**. In addition, previously the available options were:

- **None**
- **Simple**
- **Complex**

The available options are now:

- **None**
- **Complex Logon Code**
- **Simple Logon Code**

See the *Logon using codes* section in the ***Administration Guide*** for details.

13.1.4.3 Specifying code complexity in email templates

You can now specify the complexity of auth codes in email templates.

In the **Email Templates** workflow, the following email templates have an additional **Complexity** option:

- Self Requested Authentication Code Email
- Self Requested Authentication Code SMS
- Activation Code Email
- Activation Code SMS
- Authentication Code Email
- Authentication Code SMS
- Unlock Credential Code Email
- Unlock Credential Code SMS

Select the **Complexity** you want to use for the codes included in messages generated using this template:

- **Simple** – the code is generated using the complexity rules as defined by the **Simple Logon Code Complexity** configuration option.
- **Complex** – the code is generated using the complexity rules as defined by the **Complex Logon Code Complexity** configuration option.

This complexity setting takes priority over any other complexity settings; for example, credential profile **Generate Code on Request** settings or the **Auth Code Complexity** configuration option.

Note: This option is not available for templates used to send job collection codes. For job collection codes, the complexity is determined by the credential profile, or if the credential profile does not contain a complexity setting, by the **Auth Code Complexity** configuration option.

See the *Changing email messages* section in the *Administration Guide* for details.

13.1.4.4 Auth Code Complexity

You can use the new **Auth Code Complexity** configuration option (on the **Auth Code** page of the **Security Settings** workflow) to determine the format of the auth code, if the complexity was not determined by the email template or the credential profile; for example, when sending a job collection code for a device based on a credential profile that did not have the **Generate Code on Request** option set, or when viewing an unlock code on screen.

Can be one of the following options:

- **Complex** – uses the complexity determined by the **Complex Logon Code Complexity** configuration option. This is the default.
- **Simple** – uses the complexity determined by the **Simple Logon Code Complexity** configuration option.

See the *Auth Code page (Security Settings)* section in the *Administration Guide* for details.

13.1.4.5 Excluding characters from generated codes

The **Complex Logon Code Complexity** and **Simple Logon Code Complexity** configuration options (on the **Auth Code** page of the **Security Settings** workflow) have been extended to allow you to exclude characters from the generated codes; this allows you to avoid ambiguity when sending codes in an email or SMS message where the font may make it difficult to differentiate, for example, between the number 0 and the letter O.

The default **Complex Logon Code Complexity** setting for new installations is now `12-12ULSN[BGI1OQDSZ]`, which means a 12-character code containing upper case, lower case, special characters, and numbers, with a set of commonly-confused letters excluded.

The default **Simple Logon Code Complexity** setting does not include any excluded characters.

See the *Auth Code page (Security Settings)* section in the ***Administration Guide*** for details.

13.1.5   MyID Integration Toolkit

The MyID Integration Toolkit is now available online, and provides information about integrating your systems with MyID. In this release, the content includes:

- **MyID Core API**

  You can use this API to integrate user and credential management from your own systems using REST APIs.

  The functionality currently available includes:

  - User enrollment and lifecycle management, including directory integration.

  - Creating and managing credential requests.

  - Device lifecycle activities such as revoking or replacing credentials.

  - Search, report, and retrieve information about people, credentials, devices, requests, and audit data.

- **MyID Client Services API**

  You can use this API to launch MyID Client apps programmatically, enabling you to integrate then with your own web pages for:

  - Smart card authentication to MyID.

  - Personalizing, unlocking, and erasing physical and virtual smart cards and tokens.

  - Scanning documents.

  - Modifying images using the MyID image editor.

- **Self-Service Kiosk API**

  You can use this API to add your own web content to the Self-Service Kiosk.

For further details, see the MyID Integration Toolkit on the Intercede customer portal (***forums.intercede.com/documentation***).

13.1.6 Reprovisioning devices in the MyID Operator Client

From the View Device screen in the MyID Operator Client, you can launch the **Reprovision Card** workflow in MyID Desktop to re-encode a another person's device completely, based on the data in the MyID database, using the latest version of the credential profile used during issuance.

See the *Reprovisioning a device* section in the ***MyID Operator Client*** guide for details.

13.1.7 Sending and viewing authentication codes for another person

Previous versions of MyID allowed you to request an authentication code at the login screen to allow you to log in to MyID; this feature has been expanded to allow an operator to request authentication codes on behalf of another person. The operator can request the code to be sent to the person by email or as an SMS to their mobile phone, or can display the code on screen so that the operator can read out the code over the phone or otherwise provide the code; for example, by copying and pasting the code into a secure chat channel.

This feature is available in the MyID Operator Client, and also through the MyID Authentication Server for third-party systems.

See:

- The *Configuring authentication codes for the MyID authentication server* section in the ***Administration Guide*** for details of configuring MyID to allow logon using authentication codes.

- The *Signing in using single-use authentication codes* and *Signing in to MyID* sections in the ***MyID Operator Client*** guide for details of using authentication codes to log in to MyID.

- The *Sending an authentication code to a person* section in the ***MyID Operator Client*** guide for details of sending authentication codes to another person using email or SMS.

- The *Viewing an authentication code for a person* section in the ***MyID Operator Client*** guide for details of viewing authentication codes for another person on screen.

- The *Authenticating using OpenID Connect* section in the ***MyID Authentication Guide*** for details of using the MyID Authentication Server.

13.1.8 Viewing authentication codes

In addition to sending authentication codes by email or SMS, you can now view authentication codes on screen, so that the operator can read out the code over the phone or otherwise provide the code; for example, by copying and pasting the code into a secure chat channel.

See:

- The *Setting up logon codes* section in the ***Administration Guide*** for details of configuring MyID to use job collection codes.

- The *Viewing a collection code on screen* section in the ***MyID Operator Client*** guide for details of viewing job collection codes on screen.

- The *Viewing an unlock code* section in the ***MyID Operator Client*** guide for details of viewing device unlock codes on screen.

- The *Viewing an authentication code for activation* section in the ***MyID Operator Client*** guide for details of viewing device activation codes on screen.

- The *Viewing an authentication code for a person* section in the ***MyID Operator Client*** guide for details of viewing authentication codes for another person on screen.

13.2 Integration updates

This section contains details of updates to MyID 12.3.0's support for integration with smart cards and other credentials, certificate authorities, printers, and HSMs.

13.2.1 DigiCert ONE certificate authority

MyID now supports integration with the DigiCert ONE certificate authority.

Note: Integration with DigiCert ONE currently does not support PIV or escrowed certificates.

See the ***DigiCert ONE Integration Guide*** for details.

13.2.2 Microsoft Windows DCOM server security changes

Microsoft is making changes to DCOM security over the course of releases in 2021 to 2023. See article ***KB5004442*** on the Microsoft support site (***support.microsoft.com***) for details. These changes affect your Windows DCOM Server Security configuration, including future updates.

There is no overall change to recommended MyID configuration required, but some customers have been affected where alternative configurations have been used. You are recommended to follow the instructions in the *MSDTC security configuration* section of the ***Installation and Configuration Guide*** carefully, and to use the System Interrogation Utility to check that your system is configured correctly (SIU tests SIU-083, SIU-084, and SIU-218).

If you experience any problems after installing Windows updates that relate to DCOM server security, contact Intercede customer support, quoting reference SUP-354.

13.2.3 MPKI 7

The **SymantecMPKI** option in the **Certificate Authorities** workflow, which was previously used to add a new MPKI 7 CA, is no longer available. Digicert have now ended support for MPKI 7, and MyID ended support for MPKI 7 at version 12.2. If you have an existing MPKI 7 CA you can still edit the details within MyID, but you cannot add a new MPKI 7 CA.

13.2.4   SQL Server versions

The versions of SQL Server with which MyID has been tested have been updated. MyID has now been tested with the following SQL Server versions:

- SQL Server 2019 – CU15 (15.0.4198.2 – January 2022)
- SQL Server 2017 – CU27 (14.0.3421.10 – October 2021)

See the *Database versions* section of the ***Installation and Configuration Guide*** for details.

13.2.5   Thales authentication devices

MyID now supports the following devices:

- IDPrime MD930nc
- IDPrime 940B T1 CC

See the *Thales authentication devices* section in the ***Smart Card Integration Guide***.

13.2.6   Thales Luna HSM Universal Client version

The version of the Thales Luna HSM Universal Client software tested with MyID has been updated to v10.4.

See the *Supported Thales Luna HSM models* section in the ***Thales Luna HSM Integration Guide*** for details.

13.2.7   Windows 11

MyID now supports Windows 11 as a client operating system.

Note, however, that at the time of release of this version of MyID, many third party device and peripheral vendors have not yet updated their drivers or software to be validated for use on Windows 11.

See the *Operating systems* section in the ***Installation and Configuration Guide*** for details of supported client operating systems.

13.3   Improvements

This section provides details of minor improvements to existing functionality within MyID 12.3.0.

13.3.1   General bug fixes and improvements

This release contains general bug fixes and minor improvements as part of a program of continuous improvement.

13.3.2 Additional identity improvements

MyID has been updated to allow you to renew certificates issued as additional identities. Previously, it was not possible to renew additional identity certificates.

Note: This applies only to additional identity certificates issued from MyID 12.3 onwards. If you have additional identity certificates issued in previous versions of MyID, see the *Renewing additional identities* section in the ***Administration Guide***.

MyID has also been updated to allow you to select certificate policies marked as additional identity policies in the credential profile. Previously, certificate policies with the **Allow Identity Mapping** option in the **Certificate Authorities** workflow were excluded from the list of certificates you could add to a credential profile.

For information on additional identities, see the *Additional identities* section in the ***Administration Guide***.

13.3.3 Configuring the timeout for launching external applications

The MyID Client Service can launch other applications (for example, MyID Desktop or the Self-Service App). You can configure the length of time the MyID Client Service waits before returning an error. By default, this is 60 seconds.

You can change the timeout by editing the MyID Client Service configuration file.

See the *Configuring the timeout for launching external applications* section in the ***MyID Operator Client*** guide.

13.3.4 EJBCA updates

The support for the EJBCA has been updated with the following improvements:

* If the EJBCA policy is configured to require multiple static OU values in the Subject DN, the Certificate Authorities workflow will now allow these to be set and saved correctly.

  Previously, only one OU value was saved, even though multiple values were displayed.

* You can now carry out a Key Recovery of an archived EJBCA certificate, including the recovery of expired certificates.

This improvement was originally provided in MyID 11.5.5.

13.3.5 Installing certificates on iOS 15

There has been an update to the requirements for installing certificates on iOS 15, where Apple now requires a unique identifier for each item in the profile. This release provides an update for the iOS OTA web service that provides this information.

This improvement was originally provided in MyID 11.5.5.

13.3.6 Logging configuration changes

The configuration required to set up logging for MyID Desktop, the Self-Service Kiosk, and the Self-Service App has changed.

The following line in the configuration file:

```
<layout type="log4net.Layout.XmlLayoutSchemaLog4j">
```

must now be:

```
<layout type="MyIDApp.Utility.XmlLayoutSchemaLog4j">
```

See the following sections in the ***Configuring Logging*** guide:

* *Windows clients*

Update: The configuration required to set up logging for the Windows clients (MyID Desktop, the Self-Service Kiosk, and the Self-Service App) changed at MyID 12.4. See the *Windows clients* section of the ***Configuring Logging*** guide for details.

13.3.7 .NET Core versions

MyID has been updated to use newer versions of .NET Core. Previous versions used .NET Core 3.1, while the current version requires the ASP.NET Core Runtime 6.0 Hosting Bundle on the server and the .NET Desktop Runtime 6.0 on the client. You must update the installations of .NET Core on each server and each client.

See the *Installing .NET Framework and .NET Core* section in the ***Installation and Configuration Guide***.

13.3.8 Page Timeout for Windows Clients configuration option

The default timeout for MyID Windows clients (MyID Desktop, the MyID Self-Service Kiosk, and the MyID Self-Service App) is controlled by the **Page Timeout for Windows Clients** configuration option (on the **General** page of the **Operation Settings** workflow).

If you want to change the timeout for a particular installation of MyID Desktop, the MyID Self-Service Kiosk, or the MyID Self-Service App you can edit the configuration file. This overrides the configuration option in **Operation Settings**.

See:

* The *General page (Operation Settings)* sections in the ***Administration Guide***.

* The *Configuring timeouts* section in the ***Installation and Configuration Guide*** for MyID Desktop.

* The *Kiosk page timeout* section in the ***Self-Service Kiosk*** guide.

* The *Timeout* section in the ***Self-Service App*** guide.

13.3.9 Resizing columns

In the MyID Operator Client, you can now resize the columns displayed in the lists of results.

Click the sizing handle:

And drag the column to the required size.

13.3.10 SOPIN handling for mobile devices

In some circumstances when working with mobile devices, the SOPIN becomes out of sync, and the mobile device becomes locked, requiring a factory reset of the phone. The MyID Identity Agent Framework SDKs have been updated to reset SOPINs where appropriate, and this MyID Server update provides support for this feature for the MyID components and web services.

This improvement was originally provided in MyID 11.5.5.

13.3.11 Using UPN with the AD FS Adapter Mobile

The AD FS Adapter Mobile has been enhanced to allow you to configure it to use UPN as the method of identifying the person who wants to authenticate, instead of the person's email address. This is controlled by the `userlookup` option in the configuration file.

See the *Overview* and *Configuration file* sections in the ***Mobile Authentication*** guide for details.

13.4 Documentation updates in MyID 12.3.0

This section contains information on new and updated documentation in MyID 12.3.0.

13.4.1 Administration Guide

The *Administration Guide* has been updated with the following:

- Updated the instructions for selecting a card format when creating a key recovery credential profile.

  See the *Setting up the credential profile* section.

- Added **Complexity** option for email templates that are used for generated auth codes.

  See the *Changing email messages* section.

- Updated instructions for logon codes to cover new complexity settings, requesting a code for another person, and viewing codes on screen.

  See the *Logon using codes* section.

- Updated the **Logon** and **PINs** pages of the **Security Settings** workflow to remove configuration options that are now on the new **Auth Code** page.

  See the *Logon page (Security Settings)* and *PINs page (Security Settings)* sections.

- Added the new **Auth Code** page on the **Security Settings** workflow.

  See the *Auth Code page (Security Settings)* section.

- Added the new **Auth Code Complexity** configuration option.

  See the *Auth Code page (Security Settings)* section.

- The list of standard email templates has been updated.

  See the *Standard templates* section.

- Added information on viewing audited terms and conditions

  See the *Viewing audited terms and conditions* section.

- The **Generate Logon Code** option in the credential profile has been renamed **Generate Code on Request**.

  See the *Credential profile options*, *Logon using codes*, and *Auth Code page (Security Settings)* sections.

- Added the new **Page Timeout for Windows Clients** configuration option.

  See the *General page (Operation Settings)* section.

- Updated instructions for additional identities to remove restrictions on using the additional identity certificate policies in the credential profile and provide instructions on renewing additional identity certificates issued in previous versions of MyID.

  See the *Setting up additional identities* and *Renewing additional identities* sections.

13.4.2   Configuring Logging

The ***Configuring Logging*** document has been updated with the following:

- Expanded on situations when you might want to enable extended logging for the Microsoft components for the REST and authentication web service.

  See the *Logging Microsoft components* section.

- Updated content of the configuration file for MyID Desktop, the Self-Service Kiosk, and the Self-Service App logging.

  See the *Windows clients* section.

- Added the DigiCert ONE component to the list of components logged using Log4Net.

  See the *Log4Net* section.

13.4.3   Derived Credentials Self-Service Request Portal

The ***Derived Credentials Self-Service Request Portal*** guide has been updated with the following:

- The **Generate Logon Code** option in the credential profile has been renamed **Generate Code on Request**.

  See the *Setting up the credential profiles for derived credentials* section.

13.4.4   DigiCert ONE Integration Guide

The ***DigiCert ONE Integration Guide*** is new for this release.

13.4.5   Entrust CA Integration Guide

The ***Entrust CA Integration Guide*** has been updated with the following:

- The example version of the Java has been updated, and a note added that you must check the Path variable if you update the version of Java. Also the note about downloading the Java Cryptography Extension has been removed, as it refers to an older version of Java.

  See the *Prerequisites* section.

13.4.6 Error Code Reference

The *Error Code Reference* has been updated with the following:

- Updated MyID Operator Client error details:
  - Error OC10013 updated to include the Self-Service App in addition to MyID Desktop, and to provide a cross-reference to the instructions for providing the location of the client software to the MyID Client Service.

  See the *MyID Operator Client error codes* section.

- The following new MyID Operator Client error code has been added:
  - OA10059 – There are no update jobs to collect for this device.

  See the *MyID Operator Client error codes* section.

- Updated web service error details:
  - Error 890543 updated to include an additional possible cause of entering an incorrect auth code.

  See the *Web Service error codes* section.

- New error codes relating to assigning devices:
  - WS40031 – This device is already assigned, and must be canceled before it can be reassigned to a different person. The system is not configured to allow unrestricted cancellation.
  - WS40032 – This device has a disposal status that prevents it being issued again.
  - WS40033 – This device cannot be issued or updated by MyID.
  - WS40034 – The request already has an assigned device.
  - WS40035 – The request type does not permit device assignment.
  - WS40036 – The request is not awaiting issuance or awaiting validation.
  - WS40037 – The request is for a person that is not within the authenticated operators scope
  - WS40038 – This device is not known to MyID and the credential profile can only be used with known serial numbers.
  - WS40039 – This device does not meet the requirements of the credential profile.
  - WS40040 – The request does not have an assigned device.
  - WS40041 – This device is already assigned, and must be canceled before it can be reassigned to a different person.
  - WS40042 – This device is assigned to the current operator.
  - WS50051 – There are no available reports to perform a secondary search.
  - OC10014 – This action cannot be performed. Please check the installed version of MyID Client Service, and try again.

  See the *MyID Operator Client error codes* section.

- New MyID Windows client error codes added:

- -99900028 – There has been an error accessing the Biometric device. Please contact your administrator.
- -99900009 – An error occurred attempting to retrieve data from the MyID Server.

See the *MyID Windows client error codes* section.

13.4.7 FIDO Authenticator Integration Guide

The *FIDO Authenticator Integration Guide* has been updated with the following:

- The **Generate Logon Code** option in the credential profile has been renamed **Generate Code on Request**.

See the *Setting up credential profiles for FIDO authenticators* section.

13.4.8 Installation and Configuration Guide

The *Installation and Configuration Guide* has been updated with the following:

- Clarified support for SQL Server

See the *Database versions* section.

- Updated the .NET Core prerequisites.

See the *Prerequisites* section.

- Updated to add Windows 11 as a platform.

See the *Operating systems* section.

- Added information on the new **Page Timeout for Windows Clients** configuration option.

See the *Configuring timeouts* section.

- Added information about Microsoft DCOM security changes.

See the *MSDTC security configuration* section.

- Updated the versions of SQL Server that have been tested.

See the *Database versions* section.

13.4.9 Lifecycle API

The *Lifecycle API* guide has been updated with the following:

- The `RolledPrint` element visible in the schema is no longer supported.

See the *PivCardRequest/Agency/Applicant/Biometry/BioSample* section.

- The `RevocationDelay` element description has been corrected to state hours rather than days.

See the *CMSCardRequest/Group/User/Actions/RevocationDelay* section.

13.4.10 Mobile Authentication

The *Mobile Authentication* guide has been updated with the following:

- Information about using the UPN instead of the email address to identify the person who wants to authenticate.

See the *Overview* and *Configuration file* sections.

13.4.11   MyID Operator Client

The *MyID Operator Client* guide has been updated with the following:

- Configuration required when using a load balancer.

  See the *Setting the issuer for load-balanced systems* section.

- You must remove the device from the reader after performing an assisted activation before you can use it.

  See the *Activating a device* section.

- The MyID Operator Client now supports launching Self-Service App features as well as MyID Desktop workflows.

  See the *Launching MyID Desktop or Self-Service App workflows* and *Setting the location of MyID Desktop or the Self-Service App* sections.

- You can now collect your own card by launching the Self-Service App from the MyID Operator Client.

  See the *Collecting a device request* section.

- You can now update your own device by launching the Self-Service App from the MyID Operator Client.

  See the *Updating a device* section.

- Updated the unlock codes section to cover the new complexity options.

  See the *Unlocking a device* section.

- Updated the activation codes section to cover the new complexity options.

  See the *Sending an authentication code to activate a device* section.

- Updated the job collection codes section to cover the new complexity options.

  See the *Sending a collection code* section.

- Updated the instructions for logging in with an auth code to cover the new complexity options and requesting a code for another person.

  See the *Signing in to MyID* section.

- Added sections on sending and viewing authentication codes for another person.

  See the *Sending an authentication code to a person* and *Viewing an authentication code for a person* sections.

- Updated the section on sending activation codes to include the new View Auth Code feature.

  See the *Sending an authentication code to activate a device* section.

- Updated the section on sending unlock codes to include the new View Auth Code feature.

  See the *Sending a code to unlock a device* section.

- Updated the section on sending job collection codes to include the new View Auth Code feature.

  See the *Sending a collection code* section.

- The **Generate Logon Code** option in the credential profile has been renamed **Generate Code on Request**.

  See the *Sending a collection code* section.

- Added information on the new feature for assigning devices to requests.

  See the *Assigning a device to a request* and *Assign Device Search report* sections.

- Updated the list of options in the **Edit Roles** workflow and how they map to MyID Operator Client features.

  See the *Roles and groups* section.

- Added information on the `ExternalClientConnectionTimeoutSeconds` configuration option for the MyID Client Service.

  See the *Configuring the timeout for launching external applications* section.

- Added instructions on reprovisioning a card from the View Device screen of the MyID Operator Client.

  See the *Reprovisioning a device* section.

- Added details of resizing columns in the list of results.

  See the *MyID Operator Client user interface* section.

13.4.12   Operator's Guide

The ***Operator's Guide*** has been updated with the following:

- Added information on removing a device assignment from a request.

  See the *Assigning a card* section.

- Updated the **Reprovision Card** workflow procedure to cover launching the workflow from the MyID Operator Client.

  See the *Reprovisioning cards* section.

13.4.13   Printer Integration Guide

The ***Printer Integration Guide*** has been updated with the following:

- Additional troubleshooting for Datacard printers regarding permissions and offset printing layouts.

  See the *Troubleshooting Datacard printers* section.

13.4.14   Self-Service App

The ***Self-Service App*** guide has been updated with the following:

- Added information on the new **Page Timeout for Windows Clients** configuration option.

  See the *Timeout* section.

13.4.15 Self-Service Kiosk

The *Self-Service Kiosk* guide has been updated with the following:

- Added information on the new **Page Timeout for Windows Clients** configuration option.

  See the *Kiosk page timeout* section.

13.4.16 Smart Card Integration Guide

The *Smart Card Integration Guide* has been updated with the following:

- Clarifications regarding software required for Thales authentication devices, and support for 5300 devices with Touch Sensor.

  See the *Thales authentication devices* section.

- Updated throughout to indicate the level of support for Windows 11 as a platform.

- Added the IDPrime MD930nc and IDPrime 940B T1 CC devices.

  See the *Thales authentication devices* section.

- Added a note that omitting a certificate from the Card Authentication (9E) container means that you cannot carry out self-service unlocking.

  See the *Issuing smart cards that have PIV applets* section.

13.4.17 Symantec MPKI Integration Guide

The *Symantec MPKI Integration Guide* has been updated with the following:

- The **SymantecMPKI** option, which was previously used to add a new MPKI 7 CA, is no longer available.

  See the *Configuring MyID* section.

13.4.18 System Interrogation Utility

The *System Interrogation Utility* guide has been updated with the following:

- Added information about the **Authentication WS User** and **Auth DB** fields.

  See the *Running the SIU* section.

13.4.19 System Security Checklist

The *System Security Checklist* has been updated with the following:

- For secure session cookies, you are recommended to configure the MyIDProcessDriver and MyIDDataSource web applications in addition to the MyID web application.

  See the *Secure session cookie* section.

13.4.20 Thales Luna HSM Integration Guide

The *Thales Luna HSM Integration Guide* has been updated with the following:

- Updated version of the Universal Client software.

  See the *Supported Thales Luna HSM models* section.

13.4.21 Windows Hello for Business

The ***Windows Hello for Business*** guide has been updated with the following:

- Updated information about using additional identities with Windows Hello.

  See the *Additional identities* section.

13.4.22 Updates for Windows 11

The documentation throughout has been updated for Windows 11 support, where appropriate.

See section *13.2.7*, *Windows 11* for details.

13.5 End of support features in MyID 12.3.0

There were no end of support features in MyID 12.3.0.

13.6 Known issues resolved in MyID 12.3.0

This section lists the known issues that were resolved in MyID 12.3.0. These are issues that were found across both editions of MyID – Enterprise and PIV – and may not all be relevant for your system.

- IKB-71 – Cannot renew an additional identity certificate.

- IKB-306 – Extra email notification sent when renewing encryption certificates.

- IKB-353 – Additional configuration required for logging on with authentication codes.

14 Updates in MyID 12.2.0

This chapter provides details of the changes in MyID 12.2.0, including:

- New and updated features – new features in this version of MyID, and major improvements to existing features.

- Integration updates – updates to MyID's support for smart cards and other credentials, certificate authorities, printers, and HSMs.

- Improvements – minor updates to existing functionality.

14.1 New and updated features

This section contains information on the new and updated features in MyID 12.2.0.

14.1.1 Authentication codes

Authentication code generation and management has been updated and extended in this release of MyID.

You can now use authentication codes for the following:

- Logging on to the MyID Operator Client.

  You can configure MyID to allow you to request a single-use authentication code that is sent to your email address or as an SMS message to your cell phone.

  Once you have received an authentication code, you can use it to authenticate to the MyID authentication server, and therefore access either your own external system or the MyID Operator Client.

  See the *Configuring authentication codes for the MyID authentication server* section in the ***Administration Guide*** for details of configuring MyID to use authentication codes.

  See the *Signing in using single-use authentication codes* section in the ***MyID Operator Client*** guide for details of requesting and using authentication codes.

  For information on using this authentication mechanism to carry out end-user authentication for your own external systems; see the *Configuring the web service for OpenID Connect* section in the ***MyID Authentication Guide***.

- Sending authentication codes for device activation.

  If the credential profile for a device has been configured to use authentication codes for activation, once the device is ready for activation, you can send an authentication code to the person so they can activate their device from the View Device screen in the MyID Operator Client.

  You can send an authentication code to the person through email, or as an SMS message to their cell phone. You can also choose whether to send a short use authentication code for immediate use (which is valid for two minutes by default) or a long use authentication code (which is valid for 30 days by default).

  See the *Sending an authentication code to activate a device* section in the ***MyID Operator Client*** guide for details.

- Sending authentication codes for device unlocking

  If a cardholder has locked their device, you can send an authentication code from the View Device screen of the MyID Operator Client that can be used for unlocking the device and resetting the PIN.

  The cardholder can provide the authentication code when using the **Reset PIN** option in the Self-Service App or the **I want to reset my PIN** option in the Self-Service Kiosk, or an operator can unlock the device using the **Authentication Code** tab of the **Reset Card PIN** or **Unlock Credential** workflows.

  See the *Sending a code to unlock a device* section in the ***MyID Operator Client*** guide for details.

- Sending authentication codes for device collection.

If the credential profile for a device has been set up to generate codes on request using the **Generate Code on Request** option, when the device is requested, MyID sends an email message with a single-use code that the person can use to log on to MyID for the single purpose of collecting their device.

If necessary (for example, if the original code has expired) you can now use the **Send Auth Code** feature on the View Request screen of the MyID Operator Client to send another code to the person; you can choose to send the code in an email or in an SMS text message to their cell phone.

You can send a code even if the credential profile has not been set up to send a code automatically on issuance; for example, you can create a request for a device, then when the cardholder contacts the helpline to indicate they are ready to collect their device, you can issue a short lifetime code for immediate use.

For information about configuring MyID, see the *Setting up logon codes* section of the ***Administration Guide***. For information about sending codes from the MyID Operator Client, see the *Sending collection codes* section in the ***MyID Operator Client*** guide for details.

In addition to making these features available in MyID Operator Client, the MyID Core API has been extended to allow integrated systems to request that authentication codes are sent for a range of credential lifecycle operations. The use of authentication codes has also been added to the MyID authentication server, enabling use with your integrated systems and for logging on to the MyID Operator Client.

14.1.2   Automatic job cancellation

In large deployments of MyID, it is not unusual for some credential requests to remain uncollected. MyID can now automatically cancel these requests if they have not been processed within a configurable number of days after the date the request was created. The feature will look for any requests that are in an active state and may also be filtered by the credential profile of the request. Optionally, email notifications to the target of the request can also be sent to inform them of the cancellation.

See the *Automatic job cancellation* section in the ***Administration Guide*** for details.

14.1.3   Collecting a device from the MyID Operator Client

You can now launch the **Collect Card** workflow from the View Request screen in the MyID Operator Client to collect a requested device.

For more information, see the *Launching MyID Desktop workflows* and *Collecting a device request* sections in the ***MyID Operator Client*** guide.

14.1.4   Erasing a device from the MyID Operator Client

You can now launch the **Erase Card** workflow from the View Device screen in the MyID Operator Client to erase a device.

For more information, see the *Launching MyID Desktop workflows* and *Erasing a device* sections in the ***MyID Operator Client*** guide.

14.1.5 Unlocking a device from the MyID Operator Client

You can now launch the **Unlock Credential** workflow from the View Device screen in the MyID Operator Client to obtain a code that can be used to unlock a device PIN. This uses a challenge-response process available to many device types, such as smart cards, USB tokens, virtual smart cards and mobile credentials issued by MyID.

For more information, see the *Launching MyID Desktop workflows* and *Unlocking a device* sections in the *MyID Operator Client* guide.

14.1.6 Managing soft certificates in the MyID Operator Client

The MyID Operator Client has been extended to allow management of software certificate packages. You can request a set of software certificates using the Request Device option, and view and manage these requests. You can find issued software certificate packages in device searches, and view their details, including information about individual certificates that are included. You can also create and manage cancellations and requests for renewal.

These features are also available in the MyID Core API.

See the *Issuing soft certificates using a credential profile* section in the *Operator's Guide* for details.

14.2 Integration updates

This section contains details of updates to MyID 12..2.0's support for integration with smart cards and other credentials, certificate authorities, printers, and HSMs.

14.2.1 Android versions supported

MyID now supports Android version 12.

Android version 8 is no longer supported.

See the *Supported devices* section in the *Mobile Identity Management* guide for details.

14.2.2 Epson Workforce DS-1630 scanner

MyID has now been tested with the Epson Workforce DS-1630 scanner.

See the *Tested scanners* section in the *Installation and Configuration Guide* for details.

14.2.3 IDEMIA devices

MyID now supports the following:

- IDEMIA ID-One PIV 2.4.2 on Cosmo V8.2 smart cards (including the SPE version)

See the *IDEMIA smart cards* section in the *Smart Card Integration Guide*.

14.2.4 iOS versions supported

MyID now supports iOS version 15.

iOS version 12 is no longer supported.

See the *Supported devices* section in the *Mobile Identity Management* guide for details.

14.2.5 Thales authentication devices

MyID now supports the following:

- IDPrime MD930 FIPS Level 3
- SafeNet eToken 5300 (USB-C)

The version of the SafeNet Authentication Client and SafeNet Minidriver has been updated to 10.8 R6.

See the *Thales authentication devices* section in the ***Smart Card Integration Guide***.

14.2.6 Windows 10 Version 21H2

MyID now supports Windows 10 November 2021 Update (32-bit and 64-bit) – Version 21H2.

See the *Operating systems* section in the ***Installation and Configuration Guide*** for details of supported client operating systems.

14.2.7 YubiKey devices

Integration with YubiKey 5 FIPS devices (firmware v5.3 onwards) has been updated to allow better recording of this device type in MyID. MyID records these devices as having a device type of YubiKey SC FIPS; see the *Identification of YubiKey 5, YubiKey SC, and YubiKey 5.7 devices* section in the ***Smart Card Integration Guide*** for details of how MyID determines the device type.

You can also configure a credential profile to require this device type by selecting the `YubiKeyFIPS.xml` data model. If you attempt to issue the credential profile, the attempt will be rejected unless the device is recognized as a YubiKey SC FIPS device. This allows a mix of YubiKey devices to be used with your MyID installation, but ensures sensitive credentials can be issued only to the required device type.

See the *Yubico smart cards* section in the ***Smart Card Integration Guide***.

14.3 Improvements

This section provides details of minor improvements to existing functionality within MyID 12.2.0.

14.3.1 General bug fixes and improvements

This release contains general bug fixes and minor improvements as part of a program of continuous improvement.

14.3.2 CreateUnknownGroups option in the Lifecycle API

You can now use the `CreateUnknownGroups` option, which determines whether MyID creates groups that do not already exist.

See the *Advanced settings* section in the ***Lifecycle API*** guide for details.

14.3.3 Hiding the category list and search form

You can now use the tray button to toggle the display of the category list and the search form:

Button	Action
☰◁	Hide the category list and search form.
☰	Display the category list and search form.

When you open a screen in a new tab or new window, the category list and search form are automatically hidden. To toggle the display of the category list (and search form, if appropriate), click the tray button.

If you want to open the screen with the category list and search form hidden, for example if you are embedding the MyID Operator Client screen in an iframe on your intranet page, you can add `/embedded` after the `#` in the URL; for example:

```
https://servername/MyID/OperatorClient/#/embedded/people/0F3E10FE-8B80-
4FA4-BF21-556A4E370C6F
```

See the *MyID Operator Client user interface*, *Opening a new tab or window* and *Using the browser location bar* sections in the ***MyID Operator Client*** guide for details.

Note: Each embedded MyID Operator Client screen requires authentication. If you want to avoid having to authenticate each time, you can configure the MyID authentication server to allow you to request an access token, then pass that to the embedded Operator Client screen; see the *Authenticating for embedded Operator Client screens* section in the ***MyID Authentication Guide*** for details.

14.3.4 Lifetime for auth codes

You can now configure the lifetime of auth codes using the **Auth Code Lifetime** option on the **Auth Code** tab of the **Security Settings** workflow. By default, the timeout is set for 720 hours.

See the *Requesting an authentication code* section in the ***Operator's Guide*** for details.

(**Note:** This has been updated to match the location of these settings at MyID version 12.3.)

14.3.5 Lifetime for logon codes

You can now configure the lifetime of logon codes using the **Logon Code Lifetime** option on the **Auth Code** tab of the **Security Settings** workflow. By default, the timeout is set for 720 hours.

See the *Logon using codes* section in the ***Administration Guide*** for details.

(**Note:** This has been updated to match the location of these settings at MyID version 12.3.)

14.3.6 Password Change Tool enhancements

You can now use the Password Change Tool to change the SQL account password for the web.oauth2, web.oauth2.ext, InternalWS, and ExternalWS web services.

See the *Working with SQL accounts*, *Usage*, and *Command-line arguments* sections in the ***Password Change Tool*** guide.

14.3.7 Report enhancements

Reports in the MyiD Operator Client have been enhanced:

- Data limits for reports have been removed. You can now page through reports without restriction.

  Note, however, that LDAP reports still have a limit of 1000 results, and downloaded reports now contain a maximum of 20,000 results.

- You can control access to the download results feature using the **Download Reports** option in the **Reports** section of the **Edit Roles** workflow. An operator whose role does not have access to this option cannot download reports.

See the *Running reports*, *Paging of results*, and *Granting access to reports* sections in the ***MyiD Operator Client*** guide.

14.3.8 Retirement of Internet Explorer

Microsoft have announced that Internet Explorer is being retired and will not be available on future Windows versions, including updates to Windows 10. MyiD no longer has dependencies on Internet Explorer; however, there are still some circumstances where Windows Internet Options configuration is still required for some parts of the product.

See the *Configuring Internet Options* section in the ***Installation and Configuration Guide*** for details.

See also section *18.1.12*, *Internet Explorer as a user interface* for more information.

14.3.9 Setting the timeout for FIDO registration in SSRP

You can now configure the timeout period for immediate registration of FIDO devices through the Self-Service Request Portal using the **FIDO Immediate Collect Timeout** option on the **PINs** tab of the **Security Settings** workflow. By default, the timeout is set for 120 seconds.

See the *Registering FIDO authenticators using the Self-Service Request Portal* section in the ***FIDO Authenticator Integration Guide***.

14.4 Documentation updates in MyiD 12.2.0

This section contains information on new and updated documentation in MyiD 12.2.0.

14.4.1   Administration Guide

The ***Administration Guide*** has been updated with the following:

- Information about new automatic job cancellation processor.

  See the *Automatic job cancellation* section.

- Added the following new configuration option to the **PINs** page of the **Security Settings** workflow:

  - **FIDO Immediate Collect Timeout**

  See the *PINs page (Security Settings)* section.

- Added the following new configuration options to the **Auth Code** page of the **Security Settings** workflow:

  - **Auth Code Lifetime**

  - **Auth Code Lifetime for Immediate Use**

  - **Logon Code Lifetime**

  See the *Auth Code page (Security Settings)* section.

  (**Note:** This has been updated to match the location of these settings at MyID version 12.3.)

- Added information about using the **Logon Code Lifetime** configuration option.

  See the *Logon using codes* section.

- Information about configuring MyID for single-use authentication codes for logon.

  See the *Configuring authentication codes for the MyID authentication server* section.

- Added information about the **Authentication Code** logon mechanism.

  See the *Logon Mechanisms page (Security Settings)* section.

- Added information about directory sort order in the MyID Operator Client, and a suggestion for naming a configuration-only directory to appear at the bottom of the list.

  See the *Setting up a configuration-only directory* section.

- Added a reference to the alternative method of sending an authentication code for activation using the MyID Operator Client.

  See the *Additional authentication* section.

- Added information on configuring MyID for single-use logon codes for device collection.

  See the *Setting up logon codes* section.

- Updated the description of the **Enable Facial Capture** configuration option. The option requires additional customization.

  See the *Identity Checks page (Operation Settings)* section.

- Removed the External Logon Providers section, as this functionality is no longer available.

14.4.2 Configuring Logging

The ***Configuring Logging*** document has been updated with the following:

- Updated procedure for setting up logging for the MyID Windows Integration Service.

  See the *MyID Windows Integration Service* section.

14.4.3   Error Code Reference

The *Error Code Reference* has been updated with the following:

- Addition of the following error code relating to expired authentication codes:

  - 881068 – Your authentication code has expired.

  See the *Web Service error codes* section.

- Extended the description of error 800551 to include expired logon codes as a possible cause.

  See the *Web Service error codes* section.

- Extended the description of error 30021 to include a configuration setting as a possible cause.

  See the *Web Service error codes* section.

- Added the following authentication errors:

  - OA10000 – Server Error.

  - OA10020 – FIDO basic and FIDO high logonmechanisms are disabled for this client.

  - OA10046 – The OTP has expired.

  - OA10047 – This item does not meet the requirements to perform this operation.

  - OA10048 – The user does not have the required contact details for this delivery mechanism.

  See the *MyID Operator Client error codes* section.

- Updated the information relating to possible causes for the following error:

  - -99900041 – Failed to communicate with MyID server. The application will now exit.

  See the *MyID Windows client error codes* section.

- Added the following web service errors:

  - WS10004 – Unable to generate the requested report file.

  - WS40017 – You must provide at least one resource name.

  - WS40018 – You must provide a language.

  - WS40019 – The specified language has not been configured for use.

  - WS40020 – No languages have been configured for use.

  - WS40021 – The specified entity does not exist.

  - WS40022 – The specified operation id is not a valid search operation.

  - WS40023 – The specified search operation id cannot be used for this endpoint.

  - WS40024 – The delivery mechanism specified does not exist or is not allowed for this operation.

  - WS40025 – The user does not have the required contact details for this delivery mechanism.

  - WS40026 – The specified delivery mechanism is not enabled for this operation.

- WS40027 – An auth code action must be supplied.

- WS40028 – The specified auth code action: {0}, is not supported.

- WS40029 – The specified auth code action: {0}, is not supported for this item.

- WS40030 – Email notifications have not been configured. Please contact your administrator.

- WS50046 – The specified resource is not accessible, or does not exist.

- WS50047 – Requests for Software Certificate Packages are not permitted for this operation.

- WS50048 – You do not have permission to download reports.

- WS50049 – Additional authorization is required to perform this operation.

See the *MyID Operator Client error codes* section.

14.4.4   Entrust CA Integration Guide

The ***Entrust CA Integration Guide*** has been updated with the following:

- The example version of the JDK has been updated.

See the *Prerequisites* section.

14.4.5   FIDO Authenticator Integration Guide

The ***FIDO Authenticator Integration Guide*** has been updated with the following:

- New configuration option to configure the timeout period for immediate registration of FIDO devices through the Self-Service Request Portal.

See the *Registering FIDO authenticators using the Self-Service Request Portal* section.

14.4.6 Installation and Configuration Guide

The *Installation and Configuration Guide* has been updated with the following:

- Updated driver version for Canon CanoScan LiDE 220.

  See the *Tested scanners* section.

- Added new Epson Workforce DS-1630 scanner.

  See the *Tested scanners* section.

- Updated the documentation for the retirement of Internet Explorer.

  See the *Client workstation* and *Configuring Internet Options* sections.

- Removed the requirement to add the "impersonate a client after authentication" permission for the installation user.

  See the *Installation account* section.

- Added notes that both the MyID web service account and MyID IIS account require the **Log on as a batch job** privilege, and you must make sure that your group policy does not remove this privilege – this is the same requirement as for the MyID COM+ user.

  See the *IIS user account* and *Web service user account* sections.

- Removed SQL Server 2014 from the list of supported databases.

  See the *Database versions* section.

- Updated the instructions for trusting the code signing certificates to use DigiCert instead of Thawte certificates.

  See the *Running the installation program* section.

- Updated the upgrading instructions to say that upgrading client software is recommended rather than mandatory.

  See the *Upgrading MyID from a 32-bit application to 64-bit* and *Upgrading from MyID 12.0 or 12.1* sections.

14.4.7 Lifecycle API

The *Lifecycle API* guide has been updated with the following:

- Updated information about the `CreateUnknownGroups` option, which determines whether MyID creates groups that do not already exist.

  See the *Advanced settings* section.

14.4.8 Microsoft Windows CA Integration Guide

The *Microsoft Windows CA Integration Guide* has been updated with the following:

- Moved the information for setting the application policy attribute to the same section as setting the user permissions and subject name options.

  See the *Published certificates* section.

14.4.9 Microsoft VSC Integration Guide

The *Microsoft VSC Integration Guide* has been updated with the following:

- Emphasis added on running the WSVC installation program as an administrator.

  See the *Installing the Windows Integration Service interactively* and *Installing the Windows Integration Service silently* sections.

14.4.10 Mobile Authentication

The *Mobile Authentication* guide has been updated with the following:

- You can use the Password Change Tool to change the SQL account password for the InternalWS and ExternalWS web services.

  See the *Encrypted database passwords* section.

- Updated the list of Android and iOS versions supported.

  See the *MyID Authenticator* section.

14.4.11 Mobile Identity Management

The *Mobile Identity Management* guide has been updated with the following:

- Updated the list of Android and iOS versions supported.

  See the *Supported devices* section.

14.4.12 MyID Authentication Guide

The *MyID Authentication Guide* has been updated with the following:

- You can use the Password Change Tool to change the SQL account password for the web.oauth2 and web.oauth2.ext web services.

  See the *Configuring the standalone authentication service* section.

- To avoid having to authenticate each time to embedded Operator Client screens, you can configure the MyID authentication server to allow you to request an access token, then pass that to the embedded Operator Client screen.

  See the *Authenticating for embedded Operator Client screens* section.

- Added information about using single-use authentication codes with the MyID authentication server.

  See the *Configuring the web service for OpenID Connect* section.

- Updated the text to use OpenID Connect throughout rather than abbreviating to OpenID, to avoid confusion with the obsolete OpenID technology.

  See the *Configuring the web service for OpenID Connect* section.

- Removed the section containing instructions to update the web.config file for the ADFS Auth web service, as the installation program now carries out this step.

  See the *Setting up the ADFS Auth web service* section.

14.4.13 MyID Core API

The *MyID Core API.pdf* has been updated with the following:

- Updated the list of Edit Roles options mapping to API endpoints.

  See the *Accessing the API features* section.

14.4.14   MyID Operator Client

The ***MyID Operator Client*** guide has been updated with the following:

- Launching the **Collect Card** workflow in a MyID Desktop window from View Request screen of the MyID Operator Client to collect a requested device.

  See the *Collecting a device request* section.

- Launching the **Erase Card** workflow in a MyID Desktop window from View Device screen of the MyID Operator Client to erase the content of a device.

  See the *Erasing a device* section.

- Launching the **Unlock Credential** workflow in a MyID Desktop window from the View Device screen of the MyID Operator Client to obtain a code that the cardholder can use to unlock the card in the MyID Card Utility.

  See the *Unlocking a device* section.

- Added details of the tray button that now hides the category list and search form, related display behavior when opening in a new tab or window, and using `/embedded` in the URL to produce the same result.

  See the *MyID Operator Client user interface*, *Opening a new tab or window* and *Using the browser location bar* sections.

- Added information on logging in to the MyID Operator Client using single-use authentication codes.

  See the *Signing in using single-use authentication codes* section.

- Added soft certificate to the list of device types you can request.

  See the *Requesting a device for a person* section.

- Updated the list of search criteria available for reports.

  See the *Working with reports* section.

- Added information on sending an authentication code to allow a person to activate their device.

  See the *Sending an authentication code to activate a device* section.

- Updated the information on reports to remove the data limit for paged reports, add a limit of 20,000 results for downloaded reports, and add control over access to downloaded reports through edit roles.

  See the *Running reports*, *Paging of results*, and *Granting access to reports* sections.

- Added information on sending an authentication code to allow a person to log on and collect their device.

  See the *Sending a collection code* section.

- Added information on sending an authentication code to allow a person to unlock their device and reset the PIN.

  See the *Sending a code to unlock a device* section.

- Updated the list of Edit Roles options that map to MyID Operator Client features.

  See the *Roles and groups* section.

14.4.15 Operator's Guide

The **Operator's Guide** has been updated with the following:

- Added information about using the **Auth Code Lifetime** configuration option.

  See the *Requesting an authentication code* section.

- Added information about using the MyID Operator client to request, renew, and cancel soft certificates.

  See the *Issuing soft certificates using a credential profile* section.

- Added clarification about how the credential profile options for archived certificates affect the certificates added to temporary replacement cards.

  See the *Temporary card replacement example* section.

- Added a reference to the alternative method of sending an authentication code for activation using the MyID Operator Client.

  See the *Requesting an authentication code* section.

14.4.16 Password Change Tool

The **Password Change Tool** guide has been updated with the following:

- You can now change the SQL account password for the web.oauth2, web.oauth2.ext, InternalWS, and ExternalWS web services.

  See the *Working with SQL accounts*, *Usage*, and *Command-line arguments* sections.

14.4.17 PrimeKey EJBCA Integration Guide

The **PrimeKey EJBCA Integration Guide** has been updated with the following:

- Added information about the DN components in a key escrow certificate.

  See the *Configuring end entity profiles* and *Key escrow policy configuration overview* sections.

- Updated information on setting the **Key recoverable** option.

  See the *Configuring end entity profiles* and *Key escrow policy configuration overview* sections.

- Updated information on attribute mapping for repeated components.

  See the *Enabling certificates policies on a CA* section.

14.4.18 Printer Integration Guide

The **Printer Integration Guide** has been updated with the following:

- Updated card reader driver version for the Fargo DTC4500e printer.

  See the *Fargo printers* section.

- Updated printer driver version for Entrust Datacard printers.

  See the *Supported printers* and *Entrust Datacard printers* sections.

14.4.19   Self-Service Kiosk

The **Self-Service Kiosk** guide has been updated with the following:

- Additional troubleshooting information relating to the WebView2 component cache.

  See the *WebView2 cache location* section.

- Updated the sample screenshot to show the new color scheme.

  See the *Self-Service Kiosk* section.

14.4.20   Smart Card Integration Guide

The *Smart Card Integration Guide* has been updated with the following:

- Information about the IDPrime MD930 FIPS Level 3 and SafeNet eToken 5300 (USB-C) devices has been added.

  See the *Thales authentication devices* section.

- Updated the driver version required for Windows logon for IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1 cards.

  See the *Windows logon using Oberthur ID-One PIV (v2.4.0) or IDEMIA ID-One PIV 2.4.1 on Cosmo V8.1 cards* section.

- Clarified that the maximum number of smart cards is a Windows limitation on the maximum number of smart card *readers* (including virtual readers for VSCs).

  See the *Limit on number of smart cards* section.

- Corrected the listings for SafeNet eToken 5300 devices, which use the SafeNet minidriver, not the SafeNet Authentication Client.

  See the *Thales authentication devices* section.

- Updated the supported features tables to indicate that PIV cards do not support the "Enumerate certificates on the card" feature.

  See the *Supported features for Giesecke+Devrient smart cards* and *Supported features for IDEMIA smart cards* sections.

- Updated the list of SafeNet eToken devices with Touch Sensor issues to include the SafeNet eToken 5300 (USB-C).

  See the *SafeNet eToken 5300 tokens with Touch Sensor* section.

- Updated the feature lists for SafeNet eToken 5300 FIPS (Mini), SafeNet eToken 5300 (Micro), and SafeNet eToken 5300 (USB-C) devices, which now have confirmed support for ECC NIST P521 Curve.

  See the *Supported features for Thales authentication devices* section.

- Added information about IDEMIA ID-One PIV 2.4.2 on Cosmo V8.2 smart cards (including the SPE version).

  See the *IDEMIA smart cards* section.

- Added information about YubiKey SC FIPS devices.

  See the *Yubico smart cards* section.

- Updated the version of the SafeNet Authentication Client and SafeNet Minidriver to 10.8 R6.

  See the *Thales authentication devices* and *SafeNet Authentication Client 10.8 R6* sections.

14.4.21   Symantec MPKI Integration Guide

The *Symantec MPKI Integration Guide* has been updated with the following:

- Removed MPKI 7 as a supported CA.

  See the *Symantec MPKI Integration Guide* throughout.

14.4.22 System Interrogation Utility

The *System Interrogation Utility* guide has been updated with the following:

- Updated the description of remote mode installation to provide more information about potential vulnerabilities.

  See the *Description of the installation and uninstallation process* section.

- Updated the description of tests SIU-009 and SIU-101 to remove SQL Server 2014, as it is no longer supported.

  See the *Description of derived tests* section.

14.4.23 Thales Luna HSM Integration Guide

The *Thales Luna HSM Integration Guide* has been updated with the following:

- Removal of the troubleshooting step relating to an issue where the key server failed to start in HA mode when the password was not cached; this issue was addressed in a previous release.

  See the *Troubleshooting* section.

14.4.24 UniCERT Integration Guide

The *UniCERT Integration Guide* has been updated with the following:

- The example version of the JDK has been updated.

  See the *Java environment* section.

14.5 End of support features in MyID 12.2.0

This section contains information about features that are no longer supported in MyID as of MyID 12.2.0.

See:

- section *14.5.1*, *MPKI 7*.

- section *14.5.2*, *SQL Server 2014*.

14.5.1 MPKI 7

Digicert have now ended support for MPKI 7, therefore support for this certificate authority version has also ended with MyID. You can continue to use Digicert MPKI 8 with MyID; see the *Symantec MPKI Integration Guide* for details.

If you require support to transition to a new certificate authority, contact your Intercede account manager to discuss your requirements.

14.5.2 SQL Server 2014

SQL Server 2014 is no longer supported as a database platform for MyID.

See the *Database versions* section of the *Installation and Configuration Guide* for details of supported databases.

14.6 Known issues resolved in MyID 12.2.0

This section lists the known issues that were resolved in MyID 12.2.0. These are issues that were found across both editions of MyID – Enterprise and PIV – and may not all be relevant for your system.

- IKB-345 – Certificate revocations failing when no user DN is present in a certificate.

- IKB-350 – Special characters in the common name not supported for key archival certificates.

- IKB-351 – 7 day revocation check does not cancel the FIDO credential.

15 Updates in MyID 12.1.0

This chapter provides details of the changes in MyID 12.1.0, including:

- New and updated features – new features in this version of MyID, and major improvements to existing features.
- Integration updates – updates to MyID's support for smart cards and other credentials, certificate authorities, printers, and HSMs.
- Improvements – minor updates to existing functionality.

15.1 New and updated features

This section contains information on the new and updated features in MyID 12.1.0.

15.1.1 Archiving jobs

The `Jobs` table in the MyID database is used for managing active issuance jobs as well as retaining a history of completed jobs. Over time, the information on completed jobs can build up and ultimately reduce performance due to the size of the data. As a solution to this, you can archive the completed, failed, and canceled jobs over a certain age.

Reports are available in the MyID Operator Client that allow you to view archived jobs.

For information, see the *Archiving jobs* section in the ***Advanced Configuration Guide***.

15.1.2 Browser location bar enhancements

The location bar of your browser now updates with the current location within the MyID Operator Client website. You can bookmark these links, or send them to other operators; when you click on these links, you authenticate to the MyID Operator Client website if necessary, then open the page at the correct location.

This allows you to bookmark frequently-used search screens, or send a link to another operator; for example, you can send a link to a device request that needs to be validated by another operator.

This feature also allows you to open links in new tabs or windows by right-clicking a button or search result item, then selecting either **Open in a new tab** or **Open in a new window** from the pop-up menu.

See the *Using the browser location bar* section in the ***MyID Operator Client*** guide.

15.1.3 Delayed cancellation and revocation

If the **Delayed Cancellation Period** configuration option (on the **Devices** page of the **Operation Settings** workflow) is set to a value greater than `0`, there is an additional reason available when you request the replacement of a device: **Device Replacement (Delayed Cancellation)**. If you select this option, the device and its certificates are not canceled immediately, but are canceled after the number of hours specified in the configuration option.

For more information, see:

- The *Requesting a replacement card* and *Certificate reasons* sections in the ***Operator's Guide***.

- The *Requesting a replacement device* section in the ***MyID Operator Client*** guide.

- The *Devices page (Operation Settings)* section in the ***Administration Guide***.

15.1.4 Device Keys report

The new Device Keys management information report lists all issued devices that are not expired and that use GlobalPlatform or PIV 9B keys. For each set of keys in use by the device, the report shows both the current and latest key sets, and uses this information to supplement an overall Key Status for the device.

The possible Key Status values are:

- All keys are up to date

- GP key is out of date

- 9B key is out of date

- GP and 9B keys are out of date

You can filter this report by Key Status as well as by device serial number, device type name, and device owner (`LogonName`).

For information on running MI reports, see the *Working with reports* section in the ***Operator's Guide***.

See also section *15.1.11*, *Rotating customer keys*.

Note: This feature was first included in MyID 11.4.2 in April 2021.

15.1.5 Launching MyID Desktop workflows from the MyID Operator Client

Some operations listed on the button bar (for example **Reset Card PIN**) are carried out by launching a MyID Desktop workflow; this allows you to perform activities in MyID Operator Client (such as interacting with smartcards) that are implemented in a native client rather than the browser. To use these features, you must have both the MyID Client Service and MyID Desktop installed.

Currently, you can use the following from the MyID Operator Client:

- Reset Card PIN – available on the View Device screen.
- Assisted Activation – available on the View Device screen.

Important: To use this feature, you must upgrade your MyID Client Service and MyID Desktop software to the latest versions.

For more information, see the *Launching MyID Desktop workflows*, *Searching for a device*, and *Setting the location of MyID Desktop* sections in the ***MyID Operator Client*** guide.

15.1.6 Logging on with FIDO without usernames

You can now configure MyID to obtain the username from the FIDO authenticator device. This means that you do not need to type the username manually when logging on the MyID using your FIDO authenticator.

See the *Logging on to MyID with FIDO authenticators* section in the ***FIDO Authenticator Integration Guide***.

15.1.7 Reissuing cards

Reissuance is a type of card update job that you can request the Lifecycle API; when collected, the job carries out the following:

- Revokes existing certificates present on the device.
- Re-applies data model electronic personalization.
- Issues and writes a new set of certificates onto the device (according to the credential profile).
- If the **Rotate Keys On Card Update** configuration option is set (on the **Issuance Processes** page of the **Operation Settings** workflow) applies the latest customer GlobalPlatform and PIV 9B keys.

For Enterprise, use the following in the CMSCardRequest or CMSUserUpdate schema:

- `Group/User/Card/Update/ParametersXML/ReIssue`

For PIV, use the following in the PivCardRequest or PivApplicantUpdate schema:

- `Agency/Applicant/Card/Update/ParametersXML/ReIssue`

See the ***Lifecycle API*** guide for details.

Important: Currently, you must request reissuance card update jobs through the Lifecycle API, and collect these jobs using the MyID Self-Service App. You cannot collect reissuance jobs using MyID Desktop.

Note: This feature was first included in MyID 11.4.2 in April 2021.

15.1.8 Reports in the MyID Operator Client

The MyID Operator Client provides a series of reports that you can use to interrogate the data held in your MyID system. Some reports act as search options for the main categories; for example, the Devices, Assigned Devices, and Unassigned Devices reports each provide a different way of searching for a device in the Devices category; you can click on the report to open the View Device screen for that device. Other reports are simple lists of information from the MyID database; for example, the Unrestricted Audit Report provides a list of audit entries.

You can download the results of a report as a CSV (comma separated value) file that you can import into a spreadsheet for further sorting and analysis.

Access to these reports is restricted by the operator's role.

See the *Working with reports* section in the *MyID Operator Client* guide.

15.1.9 Requesting FIDO authenticators through the Self-Service Request Portal

You can now use the Self-Service Request Portal to request, and optionally register, a FIDO authenticator. You can configure MyID to use the standard registration process (using a registration email and registration code) or you can configure MyID to allow the cardholder to register their FIDO authenticator immediately in the Self-Service Request Portal. Using the Self-Service Request Portal to register your FIDO authenticator requires no additional software, just a browser with access to the Self-Service Request Portal site, an already-issued smart card, and a FIDO authenticator device you can register.

For more information, see:

- The *Creating a FIDO authenticator credential profile* section in the *Derived Credentials Self-Service Request Portal* guide

- The *Configuring roles for registering FIDO authenticators*, *Setting up a FIDO credential profile for the Self-Service Request Portal*, *Requesting FIDO authenticators using the Self-Service Request Portal*, and *Registering FIDO authenticators using the Self-Service Request Portal* sections in the *FIDO Authenticator Integration Guide*.

15.1.10 REST API for mobile credentials

This release includes a new REST API for provisioning mobile credentials. The new API is currently used only for Mobile Identity Management integration projects where a mobile application written by third party vendors is using the Identity Agent Framework version 3.2 and above for iOS or Android. Where other mobile apps are used, for example apps built with earlier versions of the Identity Agent Framework, or the Intercede Identity Agent or MyID Authenticator apps available from the iOS or Android app store, the existing APIs remain in place and continue to operate as before.

For further information on configuring the signing certificate for the new API, see the *Setting up a signing certificate for iOS OTA* section in the *Mobile Identity Management* guide.

15.1.11   Rotating customer keys

You can use the **Rotate Keys On Card Update** configuration option (on the **Issuance Processes** tab of the **Operation Settings** workflow) to configure MyID to carry out additional processing whenever a card update (including certificate renewals) is collected to determine whether the GlobalPlatform or PIV 9B keys that are used by the device need to be updated. If either set of keys is out of date, during the collection of the update job MyID applies the latest sets of keys that are applicable to the device.

New issuance, reprovision, and replacement jobs continue to behave as before, swapping out factory keys for customer keys if appropriate customer keys have been configured for the type of device being issued.

See the *Rotating customer keys* section in the ***Administration Guide*** for details.

See also section *15.1.4*, *Device Keys report*.

Note: This feature was first included in MyID 11.4.2 in April 2021.

15.1.12   RSA transport keys

You can now use RSA 2048-bit keys to secure the transport of keys between systems. You can create the transport key in your database or HSM (if available), then export the public key, which you can provide to the system that has the key you want to transfer. You can use this public key to export and encrypt a key, then transfer it to the original system, and use a key ceremony to import the key using the stored RSA key.

For more information, see the *Using RSA transport keys* section in the ***Administration Guide***.

15.1.13   Server customization

MyID provides post-install PowerShell scripts as part of its server installation package. These scripts can be used to deliver server customizations, including the following:

- Provide updated versions of MyID files for the application server.

- Provide new components to be registered alongside the MyID core components.

- Provide updated website files.

- Register new and existing components on the application server.

- Update the Windows registry.

- Update the dictionary resource files for the MyID Operator Client and other systems that use the rest.core and related authentication web services.

- Set permissions on Windows folders.

- Start Windows services.

- Update the appsettings.json files for the web services.

- Update IIS to add web service and application pools.

See the *Running post-install PowerShell scripts* section in the ***Installation and Configuration Guide*** for details.

If you want to provide your own custom MyID configuration components, files, and database scripts, contact customer support quoting reference SUP-351.

15.1.14 Translating MyID

MyID provides mechanisms for translating the user interface to allow you to run MyID in multiple languages, or to customize the terminology used on screen. This now includes the MyID Operator Client.

For information about translating the MyID interface, contact customer support quoting reference SUP-138.

15.2 Integration updates

This section contains details of updates to MyID 12.1.0's support for integration with smart cards and other credentials, certificate authorities, printers, and HSMs.

15.2.1 Entrust CA Gateway

MyID now supports Entrust CAs where there is an Entrust CA Gateway configured for redirecting API calls between the client and the Entrust CA.

See the *Entrust CA Gateway Integration Guide* for details.

15.2.2 PrimeKey EJBCA versions

The current version of MyID has been tested with:

* PrimeKey EJBCA Enterprise PKI version 7.5.

See the *Supported PrimeKey EJBCA versions* section of the *PrimeKey EJBCA Integration Guide*.

15.2.3 Thales Luna HSM firmware and software

MyID now supports Thales Luna HSM firmware version 7.11.1 and client software version 7.11.0-25.

Note: Luna HSMs in FIPS mode no longer support key ceremonies where a symmetric key is ECB wrapped with another symmetric key. Instead you must use an RSA public key to secure the key for transport and import into the HSM. See the *Using RSA transport keys* section in the *Administration Guide* for details.

See the *What is needed?* section in the *Thales Luna HSM Integration Guide* for details of supported Thales Luna HSMs.

15.2.4 YubiKey devices

MyID now supports the latest generation of YubiKey 5 using firmware 5.4. This introduces a major change to how MyID communicates with YubiKey devices by adding support for Secure Channel Protocol 03 (SCP03), which is part of the GlobalPlatform standard.

To issue one of the new YubiKey devices, you must register the factory global platform key with MyID; this allows communication over the secure channel to the device. You must also set up the PIV 9B management key.

When MyID personalizes the token, you can change both key types along with the administrator SOPIN (PUK) to unique values known only to MyID, allowing the token to be locked to your installation for management purposes.

YubiKey FIPS and YubiKey 5 devices with firmware versions later than v5.3 are identified as Yubikey SC (representing "Secure Channel"). Older firmware versions of YubiKey devices continue to be supported, without any of the additional key requirements.

For a full list of the capabilities that MyID has with YubiKey devices, see the *Yubico smart cards* section in the ***Smart Card Integration Guide***. Note that in this release, you cannot use YubiKey devices where a "Batch Management Key" (a diversified global platform or PIV 9B key) has been created on the device by Yubico before delivery to the customer.

MyID can also issue additional identity certificates to these YubiKey devices – see the *Additional identities for YubiKey tokens* section in the ***Smart Card Integration Guide***.

Additionally, MyID can continue to issue YubiKey devices as FIDO tokens; however, this remains a separate process to issuing certificates to the PIV (smart card) interface of the device. For further information on using MyID to issue FIDO credentials, see the ***FIDO Authenticator Integration Guide***.

15.3 Improvements

This section provides details of minor improvements to existing functionality within MyID 12.1.0.

15.3.1 General bug fixes and improvements

This release contains general bug fixes and minor improvements as part of a program of continuous improvement.

15.3.2 Case sensitivity in username matching

There are updates to the case sensitivity of matching user names against the Windows logon name; all matches are now case-insensitive.

See the *Case sensitivity* section of the ***Web Service Architecture*** guide for details.

15.3.3 Filtering out jobs for absent devices

You can use the new `FilterJobsForAbsentVirtualDevices` configuration option for the Self-Service App to filter out jobs for virtual devices (for example, VSCs, Windows Hello) that are not present on the current PC.

See the *Filtering jobs for absent virtual devices* section of the ***Self-Service App*** guide for details.

15.3.4   Clearing the stored PIN using the SetHSMPIN utility

You can now use the /ClearPIN command-line option of the SetHSMPIN utility to remove a PIN that has previously been stored in the registry.

See the *Setting the HSM PIN* section of the ***Installation and Configuration Guide***.

15.3.5   Location of the installation program

The MyID server installation program is now located in a folder called Installer in the MyID release image.

This folder now contains all of the files and folders needed to install the MyID server components. The other folders in the release image contain other files, such as documentation, client installation programs, and support tools.

See the *The Installation Package Manager* section in the ***Installation and Configuration Guide*** for details.

15.3.6   New CivCertificatesOnlyCompressed.xml card format

You can now use the CivCertificatesOnlyCompressed.xml card format; you can use this for CIV cards that do not require CHUID and applet customization, using compressed data.

See the *Issuing smart cards that have PIV applets* and *Installation and configuration for Yubico smart cards* sections in the ***Smart Card Integration Guide*** for more information.

15.3.7   Processing a range of entries in the Batch LDAP Synchronization Tool

Where multiple application servers are available, you can configure the Batch LDAP Synchronization Tool to spread processing load over these servers.

Where load sharing is required, the records processed by each application server are specified by providing the range of records to be processed using the **Start range** and **End range** options.

See the *Running the tool by specifying a processing range* section in the ***Administration Guide***.

15.3.8   Requesting replacement VSCs

Previously if you attempted to collect a replacement VSC on the same device that already held a VSC for the same user, you would see an error. You can now use the use the **Erase Unused VSC** option first to allow you to collect the VSC.

See the *Permanently replacing the VSC on a new device* section in the ***Microsoft VSC Integration Guide***.

15.3.9 Support for fast user switching

The MyID Client Service must bind to a WebSocket port that the MyID Operator Client is aware of, but only one instance can be bound to a port at a time.

Previously, if you used the Fast User Switching feature in Windows to switch to another user account while the MyID Client Service was already running, the second login could not launch the MyID Client Service because the port had already been consumed.

Now, if the MyID Client Service detects that the current user's session is being locked, it shuts down any running MyID Client Service applets (for example, the Select Security Device pop-up window, or the MyID Document Scanner) and unbinds from the WebSocket port to allow it to be consumed in another session.

If you do not want your applet windows to close when your workstation is locked, and do not need to support fast user switching, you can disable this behavior.

See the *Fast user switching* section in the **MyID Operator Client** guide.

15.3.10 YubiKey additional identity issue addressed

Previously, there was an issue where the first additional identity on a YubiKey device would be removed when subsequent additional identities were added. This has been addressed in the current version.

For more information about additional identities on YubiKey devices, see the *Additional identities for YubiKey tokens* section in the **Smart Card Integration Guide**.

15.4 Documentation updates in MyID 12.1.0

This section contains information on new and updated documentation in MyID 12.1.0.

15.4.1 Administration Guide

The ***Administration Guide*** has been updated with the following:

- Information about the **Start range** and **End range** options for load sharing in the Batch LDAP Synchronization Tool.

  See the *Running the tool by specifying a processing range* section.

- Information about using abbreviated command-line options for the Batch LDAP Synchronization Tool.

  See the *Running the tool from the command line* section.

- Clarified the situation around additional identities and PIV cards.

  See the *Additional identities* section.

- Updated to remove references to Intel Authenticate.

  See the *Working with credential profiles* section.

- Updated to add information about configuring logon code attempts.

  See the *Logon using codes* section.

- Information about the **Delayed Cancellation Period** configuration option.

  See the *Devices page (Operation Settings)* section.

- Updated to add information about RSA transport keys.

  See the *Using RSA transport keys*, *The Key Manager workflow*, and *Managing GlobalPlatform keys* sections.

- Added information on rotating customer keys.

  See the *Rotating customer keys* section.

15.4.2 Advanced Configuration Guide

The ***Advanced Configuration Guide*** has been updated with the following:

- Added information about archiving job data.

  See the *Archiving jobs* section.

15.4.3 Derived Credentials Self-Service Request Portal

The ***Derived Credentials Self-Service Request Portal*** guide has been updated with the following:

- Details of setting up a credential profile for FIDO derived credentials.

  See the *Creating a FIDO authenticator credential profile* section.

15.4.4 Derived Credentials Self-Service Request Portal

The ***Derived Credentials Self-Service Request Portal*** guide has been updated with the following:

- Removal of references to Intel Authenticate.

  See the *Introduction* section.

15.4.5 Entrust CA Gateway

The ***Entrust CA Gateway Integration Guide*** is new for this release.

15.4.6   Entrust CA Integration Guide

The **_Entrust CA Integration Guide_** has been updated with the following:

- A list of ports for which you must configure your firewall.

  See the *Ports required for Entrust* section.

- Added information about tracking DN changes in Entrust in relation to PIV DNs.

  See the *Tracking Entrust DN changes* section.

15.4.7 Error Code Reference

The **_Error Code Reference_** has been updated with the following:

- Removal of references to Intel Authenticate.

  See the *MyID Windows client error codes* section.

- Added the following error codes relating to the Identity Agent when operating through the REST API:

  - REST001 – The network has failed, please check connectivity.

  - REST002 – The user aborted the operation.

  - REST003 – Failed to get authorization.

  - REST004 – The MyID Server is busy. Please try again later.

  - REST005 – The information provided in the provisioning link is not valid.

  - REST006 – The URL is malformed.

  - REST007 – Unrecoverable error has occurred.

  - REST008 – Unrecoverable error has occurred.

  See the *MyID Identity Agent error codes* section.

- Added the following error codes relating to launching MyID Desktop and the Self-Service App from the MyID Operator Client:

  - OC10008 – Unable to launch the Desktop Application. Please check configuration and try again.

  - OC10009 – Unable to connect to the Desktop Application. Please try again.

  - OC10010 – Unable to launch the Desktop Application. Please try again.

  - OA10018 – You do not have any FIDO tokens registered.

  - OA10037 – You do not have permission to perform this operation. Your permissions could not be verified.

  - OA10038 – You do not have permission to perform this operation.

  - OA10039 – You do not have permission to perform this operation on the identified object or the identified object does not exist.

  - OA10040 – Your assigned roles do not have permission to collect this request's credential profile.

  - OA10041 – Authorization failure, missing data.

  - OA10042 – This item is not in the correct state to perform this operation.

  - OA10043 – Your assigned roles do not have permission to unlock this device.

  - OA10044 – You cannot perform this operation on yourself.

  - OA10045 – You cannot perform this operation on others.

  See the *MyID Operator Client error codes* section.

- Added the following error codes relating to authentication:
  - OA10019 – Username should not be null or empty.
  - OA10020 – Invalid return URL.
  - OA10030 – MyID:Database:ConnectionStringCore is not configured.
  - OA10031 – MyID:Database:ConnectionStringAuth is not configured.
  - OA10032 – Unable to find configured JWT signing certificate.
  - OA10033 – No JWT signing certificate configured and no RSA signing key containername configured.
  - OA10034 – JWT signing key is configured, but has an incorrect algorithm or key size.
  - OA10035 – Generated JWT signer certificate, but unable to load it.
  - OA10036 – No JWT signing certificate configured and no RSA signing key containername configured, and not configured to generate a JWT signing key.

  See the *MyID Operator Client error codes* section.

- Added the following error codes relating to URL navigation:
  - OC10011 – The item is not available. Check the link is valid and you have permission to access this information.
  - OC10012 – The item is not available. Check the link is valid and you have permission to access this information.

  See the *MyID Operator Client error codes* section.

- Added the following error code relating to an incorrect version of MyID Desktop:
  - OC10013 – Unable to launch the Desktop Application. Please try again.

  See the *MyID Operator Client error codes* section.

- Added the following error codes relating to authentication and card issuance:
  - 85188 – Unable to connect to the authentication server.
  - 890483 – There are no jobs for this device.
  - 9001005 – The terms and conditions certificate could not be validated.
  - 9007124 – Card type must match the card stock.

  See the *Web Service error codes* section.

15.4.8   FIDO Authenticator Integration Guide

The *FIDO Authenticator Integration Guide* has been updated with the following:

- Details of configuring roles to allow cardholders to use the Self-Service Request Portal to request FIDO authenticators.

  See the *Configuring roles for registering FIDO authenticators* section.

- Details of configuring a credential profile to use the Self-Service Request Portal to request and register FIDO authenticators.

  See the *Setting up a FIDO credential profile for the Self-Service Request Portal* section.

- Details of requesting a FIDO authenticator through the Self-Service Request Portal.

  See the *Requesting FID authenticators using the Self-Service Request Portal* section.

- Details of registering a FIDO authenticator through the Self-Service Request Portal.

  See the *Registering FIDO authenticators using the Self-Service Request Portal* section.

- Details of logging on to MyID without providing a username.

  See the *Logging on to MyID with FIDO authenticators* section.

15.4.9   Implementation Guide

The *Implementation Guide* has been updated with the following:

- Added a section on obtaining information from Intercede customer support about translating the MyID user interface.

  See the *Translation* section.

- Removal of references to Intel Authenticate.

  See the *Virtual Smart Cards* section.

15.4.10 Installation and Configuration Guide

The *Installation and Configuration Guide* has been updated with the following:

- Removal of references to Intel Authenticate.

  See the *Virtual Smart Cards* section.

- Information added about the limitations of the installation program's Modify feature.

  See the *Modifying the installation* section.

- Added information about upgrading terms and conditions.

  See the *Upgrading credential profiles* section.

- Updated the launch permissions instructions for the case where the web server on the same machine as the application server to use the Distributed COM users group.

  See the *Web server on the same machine as the application server* section.

- Added details of the new `/ClearPIN` command-line option for the SetHSMPIN utility.

  See the *Setting the HSM PIN* section.

- Added a note about upgrading systems with customized services.

  See the *Upgrading systems with customized services* section.

- Updated information on the location of the MyID server installation program, which is now in the `Installer` folder.

  See the *Running the installation program* and *Running post-install PowerShell scripts* sections.

- Added information on upgrading from MyID 12.0.

  See the *Upgrading from MyID 12.0* section.

- Added a SUP reference for server customization.

  See the *Running post-install PowerShell scripts* section.

15.4.11 Intel Authenticate Integration Guide

The Intel Authenticate Integration Guide has been removed from the documentation set. References to Intel Authenticate in other documents have also been removed.

MyID support for Intel Authenticate Virtual Smart Cards has now been deprecated. If you are currently using this solution or have further questions about it, contact Intercede for further details quoting SUP-349.

15.4.12 Lifecycle API

The ***Lifecycle API*** guide has been updated with the following:

- Updated the `GenerateUserDn` examples to use `0`.

  See the *CMS Sample* and *PIV Sample* sections.

- Updated the details of the `CardExpiryDate` node; specifying a `CardExpiryDate` later than the person's configured **Maximum Expiry Date** no longer produces an error, but uses the earlier date instead.

  See the *CMSCardRequest/Group/User/Card/CardExpiryDate* and *PivCardRequest/Agency/Applicant/Card/CardExpiryDate* sections.

- Added information on the `ReIssue` node.

  See the *CMSCardRequest/Group/User/Card/Update/ParametersXML/ReIssue* and *PivCardRequest/Agency/Applicant/Card/Update/ParametersXML/ReIssue* sections.

15.4.13 Microsoft Azure Integration Guide

The ***Microsoft Azure Integration Guide*** has been updated with the following:

- Information about installing the authentication database.

  See the *Installing the database* section.

15.4.14 Microsoft VSC Integration Guide

The ***Microsoft VSC Integration Guide*** has been updated with the following:

- Details on requesting a replacement VSC on the same device that already holds a VSC for the same user.

  See the *Permanently replacing the VSC on a new device* section.

15.4.15 Microsoft Windows CA Integration Guide

The ***Microsoft Windows CA Integration Guide*** has been updated with the following:

- Removal of references to Intel Authenticate.

  See the *ECC support* section.

15.4.16 Mobile Identity Management

The ***Mobile Identity Management*** guide has been updated with the following:

- Instructions for adding the signing certificate thumbprint to the configuration file for the rest.provision web service.

  See the *Setting up a signing certificate for iOS OTA* section.

15.4.17 MyID Core API

The **MyID Core API** guide has been updated with the following:

- Information about obtaining an operation extension token that allows you to call the MyID Client Service to carry out operations in MyID Desktop that are not currently supported by the MyID Core API such as resetting PINs.

  See the *Operation extension* section.

  Note: This feature is reserved for future use. The MyID Client Service web sockets API is not currently available.

15.4.18 MyID Operator Client

The **MyID Operator Client** guide has been updated with the following:

- Information on launching MyID Desktop workflows from the MyID Operator Client.

  See the *Launching MyID Desktop workflows*, *Searching for a device*, and *Setting the location of MyID Desktop* sections.

- Information about configuring delayed cancellation and revocation using the **Delayed Cancellation Period** configuration option.

  See the *Requesting a replacement device* section.

- Updated information on display of date formats.

  See the *Displaying dates and times* section.

- Added information about using the browser location bar for bookmarking, sending links, and working in multiple tabs or windows.

  See the *Using the browser location bar* section.

- Added information about configuring support for fast user switching in Windows.

  See the *Fast user switching* section.

- Added information about using reports in the MyID Operator Client.

  See the *Working with reports* section.

- Added information about errors that appear if you are using an older version of the MyID Client Service.

  See the *MyID Operator Client error messages* section.

15.4.19 Operator's Guide

The **Operator's Guide** has been updated with the following:

- Information about configuring delayed cancellation and revocation using the **Delayed Cancellation Period** configuration option.

  See the *Requesting a replacement card* section.

- Information about the new **Device Replacement (Delayed Cancellation)** certificate reason.

  See the *Certificate reasons* section.

- Added Device Keys to the list of available reports.

  See the *Working with reports* section.

15.4.20 Password Change Tool

The *Password Change Tool* guide has been updated with the following:

- Information on updating the MyID IIS user account password for IIS client certificate configuration.

  See the *Working with Active Directory accounts* section.

15.4.21 PrimeKey EJBCA Integration Guide

The *PrimeKey EJBCA Integration Guide* has been updated with the following:

- Removal of references to Intel Authenticate.

  See the *ECC support* section.

- Updated the listed version of EJBCA to 7.5.

  See the *Supported PrimeKey EJBCA versions* section.

- Added known issue relating to special characters and key archival certificates.

15.4.22 Printer Integration Guide

The *Printer Integration Guide* has been updated with the following:

- Updated list of printers supported by the EDI Secure software, and updated details of installing this software for XID printers.

  See the *Supported printers* and *XID printers* sections.

15.4.23 Securing Websites and Web Services

The *Securing Websites and Web Services* guide has been updated with the following:

- Information on updating the MyID IIS user account password for IIS client certificate configuration.

  See the *Configuring IIS client certificates* section.

15.4.24 Smart Card Integration Guide

The *Smart Card Integration Guide* has been updated with the following:

- Requirement to use the Yubico Minidriver if you want to use YubiKey devices for additional identities.

  See the *Additional identities for YubiKey tokens* section.

- Addition of the **CivCertificatesOnlyCompressed.xml** card format.

  See the *Issuing smart cards that have PIV applets* and *Installation and configuration for Yubico smart cards* sections.

- Removal of references to Intel Authenticate.

  See the *Introduction* section.

- Added references to the FIDO guide.

  See the *FIDO for Thales authentication devices* and *FIDO for Yubico devices* sections.

15.4.25 Self-Service App

The ***Self-Service App*** guide has been updated with the following:

- Removal of references to Intel Authenticate.

  See the *Command line reference* section.

- New `FilterJobsForAbsentVirtualDevices` configuration option that allows you to filter out jobs for virtual devices (for example, VSCs, Windows Hello) that are not present on the current PC.

  See the *Filtering jobs for absent virtual devices* section

15.4.26 Symantec (DigiCert) Managed PKI Integration Guide

The ***Symantec MPKI Integration Guide*** has been updated with the following:

- Removal of references to Intel Authenticate.

  See the *ECC support* section.

- Added a known issue relating to duplicate certificate records.

  See the *Troubleshooting* section.

15.4.27 System Interrogation Utility

The ***System Interrogation Utility*** has been updated with the following:

- New SIU tests SIU-310 to SIU-320.

  See the *Description of derived tests* section.

- Added the `AuthWSUser` to the list of users in the configuration file.

  See the *Users section* section.

- Added `AuthDB` to the list of databases in the configuration file.

  See the *SQLSettings section* section.

15.4.28 System Security Checklist

The ***System Security Checklist*** has been updated with the following:

- Updates to the instructions for setting secure session cookies.

  See the *Secure session cookie* section.

15.4.29 Thales Luna HSM Integration Guide

The ***Thales Luna HSM Integration Guide*** has been updated with the following:

- Information on an issue recovering end-user archived certificates that were issued and archived by the Microsoft CA where the KRA certificate uses the SafeNet CSP when a LUNA T-Series HSM with firmware v7.11 is running in FIPS mode.

  See the *Troubleshooting* section.

- Added details of Luna HSM firmware version 7.11.1 and client software version 7.11.1, along with details of support for RSA public key ceremonies.

  See the *What is needed?* section.

15.4.30 Web Service Architecture

The **Web Service Architecture** guide has been updated with the following:

- Updates to case sensitivity of target username matches.

  See the *Case sensitivity* section.

15.5 End of support features in MyID 12.1.0

This section contains information about features that are no longer supported in MyID as of MyID 12.1.0.

See:

- section *15.5.1*, *XID printers*.

15.5.1 XID printers

The following printers have been discontinued:

- XID 560ie, 570ie, 580ie, 590ie

- XID 9300, 9330

- DCP 360

See the *Supported printers* section in the **Printer Integration Guide** for details of which XID printers are supported.

15.6 Known issues resolved in MyID 12.1.0

This section lists the known issues that were resolved in MyID 12.1.0. These are issues that were found across both editions of MyID – Enterprise and PIV – and may not all be relevant for your system.

- IKB-76 – Additional identities not supported on PIV or CIV systems, or non-PIV systems using cards with PIV applets.

- IKB-222 – Entrust integration not available on Windows Server 2019.

- IKB-269 – Self-Service App notifications not fully compatible with Windows 10 notification system.

- IKB-325 – Problem when specifying non-standard ports.

- IKB-328 – Temporary credential profiles are included in the Select Profile drop-down list.

- IKB-329 – Credential profiles created as a result of superseded certificates may lose information.

- IKB-338 – Unrestricted execution policy for PowerShell scripts required.

- IKB-343 – Issues for monitored SSL certificates.

- IKB-346 – Image not saved if captured using Edit Person (Directory) screen.

16 Updates in MyID 12.0.1

This chapter provides details of the changes in MyID 12.0.1, including:

- New and updated features – new features in this version of MyID, and major improvements to existing features.
- Integration updates – updates to MyID's support for smart cards and other credentials, certificate authorities, printers, and HSMs.
- Improvements – minor updates to existing functionality.

16.1 New and updated features

There are no new or updated features in this release. This release contains improvements only.

16.2 Integration updates

There are no integration updates in this release.

16.3 Improvements

This section provides details of minor improvements to existing functionality within MyID 12.0.1.

16.3.1 General bug fixes and improvements

This release contains general bug fixes and minor improvements as part of a program of continuous improvement.

16.3.2 Default vetting dates

There has been a change of behavior in the Lifecycle API when importing users with the User Data Approved flag set.

When you set the following options:

- `CMSCardRequest/Group/User/Account/UserDataApproved` *or*
- `PivCardRequest/Agency/Applicant/NACI/CardIssuanceApproved`

to `YES` or `1`, and do not set an explicit `VettingDate` in the request, the `VettingDate` is now set to the current date.

See the *Lifecycle API* guide for details.

16.3.3 New version of the Self-Service Kiosk

This release provides an updated version of the Self-Service Kiosk, providing an additional command-line parameter:

- `/showcursor` – shows the mouse cursor instead of hiding it.

See the *Command-line parameters* section in the *Self-Service Kiosk* guide for details.

16.4 Documentation updates in MyID 12.0.1

This section contains information on new and updated documentation in MyID 12.0.1.

16.4.1 Administration Guide

The *Administration Guide* has been updated with the following:

- Information about the permissions required to create a trace file in the Batch LDAP Synchronization Tool.

  See the *Running the tool from the command line* section.

16.4.2 FIDO Authenticator Integration Guide

The *FIDO Authenticator Integration Guide* has been updated with the following:

- Updated the troubleshooting information for JSON configuration file format issues.

  See the *Troubleshooting* section.

- Updated information on editing the JSON configuration file for the FIDO access token.

  See the *Setting up the FIDO access token* section.

- Added a new section on amending the `Origin` and `ServerDomain` configuration settings, with additional information about the priority of the settings specified in the installation program, `appsettings.json`, and `appsettings.Production.json` files; previously, information about these options was included in the FIDO access token section.

  See the *Configuring the server settings* section.

16.4.3 Installation and Configuration Guide

The *Installation and Configuration Guide* has been updated with the following:

- Clarification on the user account to use when running the upgrade migration script to restore your backed-up configuration.

  See the *Upgrading MyID from a 32-bit application to 64-bit* section.

16.4.4 Lifecycle API

The *Lifecycle API* guide has been updated with the following:

- Updated the `CMSCardRequest/Group/User/Account/UserDataApproved` and `PivCardRequest/Agency/Applicant/NACI/CardIssuanceApproved` nodes to state that the `VettingDate` is set to the current date if these fields are set to `YES` or `1` and an explicit `VettingDate` is not set in the request.

16.4.5 MyID Authentication Guide

The *MyID Authentication Guide* has been updated with the following:

- Updated the troubleshooting information for ADFS JSON configuration file format issues.

  See the *Troubleshooting* section in the *MyID AD FS Adapter OAuth* chapter.

- Updated the troubleshooting information for OpenID JSON configuration file format issues.

  See the *Troubleshooting* section in the *Authenticating using OpenID* chapter.

16.4.6 MyID Core API

The *MyID Core API* guide has been updated with the following:

- Updated the troubleshooting information for JSON configuration file format issues.

  See the *Troubleshooting* section.

16.4.7 Self-Service Kiosk

The *Self-Service Kiosk* guide has been updated with the following:

- New `/showcursor` command-line parameter to show the mouse cursor instead of hiding it.

  See the *Command-line parameters* section.

16.4.8 System Interrogation Utility

The *System Interrogation Utility* guide has been updated with the following:

- Updated the description for test SIU-217 to clarify the affected user account.

  See the *Description of derived tests* section.

16.5 End of support features in MyID 12.0.1

There were no new end of support features in MyID 12.0.1.

16.6 Known issues resolved in MyID 12.0.1

There were no known issues resolved in MyID 12.0.1.

17 Updates in MyID 12.0.0

This chapter provides details of the changes in MyID 12.0.0, including:

- New and updated features – new features in this version of MyID, and major improvements to existing features.

- Integration updates – updates to MyID's support for smart cards and other credentials, certificate authorities, printers, and HSMs.

- Improvements – minor updates to existing functionality.

17.1 New and updated features

This section contains information on the new and updated features in MyID 12.0.0.

17.1.1 64-bit MyID server

The MyID server components are now provided as 64-bit applications.

This affects the installation location, registry settings, and use of the Windows `System32` folder. The documentation has been updated throughout with the 64-bit information.

This also affects integration with third-party components; for example, you must set up your HSMs to use 64-bit software.

Note: MyID clients continue to be supplied as 32-bit applications, so paths and registry settings relating to clients have not changed.

You cannot upgrade MyID from an earlier version to a 64-bit version by installing over the previous version; the file paths and registry settings have changed. You must back up your configuration, uninstall your previous version of MyID, retaining the database, install the 64-bit version, then restore your configuration to the 64-bit locations on the file system and in the registry.

Intercede has provided a utility that automates this process for you; see the *Upgrading MyID from a 32-bit application to 64-bit* section in the ***Installation and Configuration Guide***.

17.1.2 Authentication database and authentication user

As part of the suite of new and enhanced authentication features for this release, MyID now has an additional SQL Server database that is used to store authentication information, including details of audited authentication attempts. You can use this database for reporting; see the *Reporting on the authentication database* section in the ***MyID Authentication Guide*** for details.

If you are using SQL Authentication, you must create an additional login for this database; see the *Configuring SQL Server for SQL Authentication* section in the ***Installation and Configuration Guide*** for details.

You must also create a new authentication user service account, in addition to the COM+ account, the IIS account, and the web service account; see the *MyID Authentication account* section in the ***Installation and Configuration Guide*** for details.

17.1.3 Canceling a device using the MyID Operator Client

You can now cancel devices using the MyID Operator Client.

See the *Canceling a device* section in the ***MyID Operator Client*** guide for details.

17.1.4 Capturing images in the MyID Operator Client

You can now capture user images for a person in the MyID Operator Client using an attached webcam, or by uploading an existing photograph. This feature is available in the Edit Person and Add Person screens.

Important: This functionality requires the latest version of the MyID Client Service. Make sure you install the version of the MyID Client Service provided with MyID 12.0 on all client PCs.

See the *Capturing images* section in the ***MyID Operator Client*** guide for details.

17.1.5 Enhanced Requisite User Data feature

The Requisite User Data feature in credential profiles has been enhanced. You can now choose whether to enforce the user data requirements at request, validation, and collection, or just at validation and collection, allowing you to create requests for users who do not yet have all their information captured, but will have that information captured before the device is validated or collected.

You can also optionally provide a list of accepted values for the user data.

A new configuration option, **Show Disqualified Credential Profiles**, allows you to hide credential profiles that do not meet the Requisite User Data requirements in the MyID Operator Client.

For more information see the *Requisite User Data* section in the ***Administration Guide***.

17.1.6 FIDO support

MyID now supports management of FIDO2 devices. Once registered, you can use FIDO devices to authenticate to the MyID authentication server, which you can use for authentication to MyID, AD FS, or OpenID Connect supported systems.

MyID offers policy control over the registration of FIDO devices; you can use credential profiles to set this control for registration. The options include:

- User Verification required
- Authenticator type
- FIDO credential lifetime

You can revoke FIDO devices using the Cancel Device option in the MyID Operator Client.

For information about configuring your system for FIDO, and requesting, registering, and canceling FIDO authenticators, see the ***FIDO Authenticator Integration Guide***.

For information about using the MyID AD FS adapter for FIDO, see the *MyID AD FS Adapter OAuth* section in the ***MyID Authentication Guide***.

For information about using the authentication server for OpenID Connect supported systems, see the *Authenticating using OpenID* section in the ***MyID Authentication Guide***.

17.1.7 Identify Device (Administrator) workflow

MyID now provides the **Identify Device (Administrator)** workflow, which allows an administrator to view the details of a smart card or other issued device, including sensitive details such as the initial server-generated PIN, if available. This workflow is separate to the existing **Identify Card** workflow, which allows you to configure your system so that only trusted high-level operators are allowed to access this additional sensitive information.

For more information, see the *Using the Identify Device (Administrator) workflow* in the ***Operator's Guide***.

17.1.8 Logging on with security phrases in the MyID Operator Client

You can now configure MyID to allow people to log on to the MyID Operator Client using security phrases (passwords) instead of, for example, a smart card.

For more information, see the *Signing in using security phrases* section in the ***MyID Operator Client*** guide.

For additional information on configuring MyID to allow logon with security phrases, see the *Logon using security phrases* section in the ***Administration Guide***.

17.1.9 MyID authentication service

The MyID authentication service (web.oauth2) provides authentication services for the MyID Operator Client and the MyID Core API.

With this release, the authentication service has been extended to support:

- An Active Directory Federation Services (AD FS) adapter for FIDO authenticators to provide authentication to AD FS.

  See the *MyID FIDO ADFS Adapter* section in the ***MyID Authentication Guide***.

- Using OpenID to provide authentication for an external system that supports OpenID Connect.

  See the *Authenticating using OpenID* section in the ***MyID Authentication Guide***.

- A standalone version of the authentication service (web.oauth2.ext) for high availability operations, recommended for supporting authentication to third-party systems.

  See the *Setting up the standalone authentication service* section in the ***MyID Authentication Guide***.

- Reporting on the authentication database.

  See the *Reporting on the authentication database* section in the ***MyID Authentication Guide***.

As part of this updated feature, you must set up an additional user account for MyID before you install; see the *MyID Authentication account* section in the ***Installation and Configuration Guide***.

17.1.10 MyID Authenticator for Android

The MyID Authenticator app is now available for Android devices.

See the *MyID Authenticator* section in the ***Mobile Authentication*** guide.

17.1.11 MyID Core API

The MyID Core API was first added in MyID 11.6, initially to provide connectivity and functionality between the MyID Operator Client and the MyID application server. The API is used to facilitate the migration away from older user interface technologies such as ActiveX and Internet Explorer.

This API is now available for use directly; for example, you can use it to integrate into other business systems that provide information to MyID or to trigger credential lifecycle events.

The MyID Core API is based on REST architectural principles, and allows you to access a wide range of MyID features directly.

The API is secure by default, requiring authentication of the calling system in order to use the API and restricting access to available features and data using MyID role-based access and scope control.

You can use the API for such actions as:

- Searching and retrieving information about a person, device or request.

- Adding or updating a person's information in MyID.

- Managing the lifecycle of people, devices, and requests.

Comprehensive API documentation is provided, including schema information to simplify integration development.

For more information on accessing the API and configuring its authentication, see the *MyID Core API* document.

17.1.12 Removing a person using the MyID Operator Client

You can now remove people using the MyID Operator Client.

See the *Removing a person* section in the *MyID Operator Client* guide for details.

17.1.13 Server-generated PINs for PIN reset

You can now configure a credential profile to generate PINs on the server when using the **Reset Card PIN** workflow. The operator who is resetting the card's PIN does not then have to provide a new PIN manually, and can print out a mailing document to send to the cardholder containing their new PIN.

See the *Credential profile setup for PIN generation* section in the *Administration Guide* and the *Resetting a card's PIN* section in the *Operator's Guide*.

17.2 Integration updates

This section contains details of updates to MyID 12.0.0's support for integration with smart cards and other credentials, certificate authorities, printers, and HSMs.

17.2.1 10-slap fingerprint reader integration

The range of 10-Slap fingerprint readers that you can use with MyID has been extended to cover a broader range of device vendors and models:

- HID Guardian
- HID Guardian 100
- HID Guardian 200
- HID Guardian 300
- HID Patrol
- Thales Greenbit DactyScan84c
- Integrated Biometrics Kojak
- Integrated Biometrics Five-O
- Jenetric LiveTouch Quattro

Support for 10-Slap fingerprint enrollment requires additional software to be installed onto your MyID environment. If you would like access to this feature, or want to discuss use of an alternative fingerprint reader, contact your Intercede account manager for further details.

17.2.2 Additional identities on YubiKey tokens

You can now store additional identity certificates on YubiKey 4 and 5 tokens using the Retired Key Management container slots.

See the *Additional identities for YubiKey tokens* section in the ***Smart Card Integration Guide***.

17.2.3 Browser support for the MyID Operator Client

The list of browsers recommended for use with the MyID Operator Client has been extended to include Edge and Firefox. The full list of recommended browsers is now:

- Google Chrome
- Microsoft Edge (Chromium version)
- Mozilla Firefox.

See the *Supported browsers* section in the ***MyID Operator Client*** guide for details.

17.2.4 Entrust Datacard printers

MyID has been tested with Datacard XPS Card Printer Driver Version 8.0 for Microsoft Windows, enabling use of a range of current and new smart card printer models from Entrust Datacard.

See the *Supported printers* section in the ***Printer Integration Guide*** for details.

17.2.5 FIDO authenticators

MyID now supports issuing FIDO authenticators. You can also configure MyID to allow logon using an issued FIDO authenticator.

For more information, see the ***FIDO Authenticator Integration Guide***.

17.2.6   SafeNet eToken 5300 devices

MyID now supports the following devices:

- SafeNet eToken 5300 FIPS (Mini)
- SafeNet eToken 5300 (Micro)

See the *Thales authentication devices* section in the ***Smart Card Integration Guide***.

Note: Due to issues relating to signing operations with SafeNet eToken 5300 devices with a Touch Sensor, these versions of the token are not currently supported with MyID. For more information, see the *SafeNet eToken 5300 tokens with Touch Sensor* section in the ***Smart Card Integration Guide***

17.2.7   Thales Luna HSMs

Support for Thales Luna HSMs has been updated to include the use of the Universal Client software, and also cloud-based HSMs through the Thales Data Protection on Demand (DPoD) service.

See the ***Thales Luna HSM Integration Guide*** for details.

17.2.8   Egofy v3.0 with FIDO devices

MyID now supports Egofy v3.0 with FIDO devices.

See the *Egofy smart cards* section in the ***Smart Card Integration Guide***.

17.2.9   Windows 10 Version 20H2

MyID now supports Windows 10 October 2020 Update (32-bit and 64-bit) – Version 20H2.

See the *Operating systems* section in the ***Installation and Configuration Guide*** for details of supported client operating systems.

17.3   Improvements

This section provides details of minor improvements to existing functionality within MyID 12.0.0.

17.3.1   General bug fixes and improvements

This release contains general bug fixes and minor improvements as part of a program of continuous improvement.

17.3.2   Alternative authentication for the mobile verification service

By default, the mobile verification service is configured to require 2-way TLS.

If you want to configure your system to use an alternative authentication system in IIS, you can now disable TLS in the `MobileAuthInternal` service configuration file.

See the *Disabling 2-way TLS for the internal authentication service* section in the ***Mobile Authentication*** guide.

intercede

MyiD CMS

17.3.3 Entering dates in the MyID Operator Client

The date fields in the MyID Operator Client have been enhanced to allow date entry either through verified text entry or through a date picker dialog.

See the *Entering dates and times* section in the **MyID Operator Client** guide.

17.3.4 Installation changes for mobile authentication

The MyID Verification Service now uses the main MyID installation program instead of the MMVS installer.

See the *Installing the verification service* section in the **Mobile Authentication** guide.

The AD FS Adapter for MyID is now called the AD FS Adapter Mobile, and shares an installation program with the AD FS Adapter OAuth.

See the *Installing the AD FS Adapter Mobile* section in the **Mobile Authentication** guide.

17.3.5 Requesting and canceling Windows Hello using the MyID Operator Client

You can now use the MyID Operator Client to request or cancel a Windows Hello credential.

See the *Requesting a Windows Hello credential* and *Canceling a Windows Hello credential* sections in the **Windows Hello for Business** guide.

17.4 Documentation updates in MyID 12.0.0

This section contains information on new and updated documentation in MyID 12.0.0.

17.4.1 Administration Guide

The *Administration Guide* has been updated with the following:

- Added information on the new feature that allows you to configure a credential profile to use server-generated PINs when resetting a card's PIN.

  See the *Credential profile setup for PIN generation* and *PIN Settings* sections.

- Added information on the updated Requisite User Data feature, including the new **Show Disqualified Credential Profiles** configuration option.

  See the *Requisite User Data* and *Issuance Processes page (Operation Settings)* sections.

- Added clarifications regarding the credential expiry date functionality.

  See the **Set expiry date at request** and **Expire Cards at End of Day** options in the *Issuance Processes page (Operation Settings)* section.

- Updated the configuration options on the **Video** page of the **Operation Settings** workflow to cover the use of these options for image capture in the MyID Operator Client.

  See the *Video page (Operation Settings)* section.

- Clarified the behavior of the **Case sensitive security questions** configuration option in relation to logon codes.

  See the *Setting up logon codes* and *PINs page (Security Settings)* sections.

- Updated the information on using security phrases to log on to incorporate details of using the MyID Operator Client, and added clarifications surrounding the configuration options used to set up security phrase logon.

  See the *Logon using security phrases* and *Logon page (Security Settings)* sections.

17.4.2 Configuring Logging

The *Configuring Logging* document has been updated with the following:

- Changes for using 64-bit server components, including file paths and registry settings.

  Note that the client components have not changed, and still use 32-bit file paths and registry settings.

17.4.3 Derived Credentials Notifications Listener API

The *Derived Credentials Notifications Listener API* guide has been updated with the following:

- Updated the details of the `CessationOfTrustOfCertificate` method section to contain the correct information.

  See the *CessationOfTrustOfCertificate* section.

- Updated the details of the `CessationOfTrust` and `CessationOfTrustOfCertificate` methods to include the limitation that where an applicant has multiple derived credentials on the same device, only the first derived credential is canceled.

  See the *CessationOfTrust* and *CessationOfTrustOfCertificate* sections.

17.4.4 Entrust CA Integration Guide

The ***Entrust CA Integration Guide*** has been updated with the following:

- Added troubleshooting information about CA error -2187.

  See the *Troubleshooting error messages* section.

- Added clarification on the behavior of CA-controlled encryption certificate issuance when the certificate already exists but is approaching expiry.

  See the *Effect on escrowed encryption certificates of allowing the CA to control lifetimes* section.

17.4.5 Entrust nShield HSM Integration Guide

The ***Entrust nShield HSM Integration Guide*** has been updated with the following:

- Updated information on disabling the Security Assurance Mechanism.

  See the *Security Assurance Mechanism* section.

- Minor updates on the recommended support software version.

  See the *Hardware and software requirements* section.

- Changes for 64-bit operation throughout the document.

17.4.6 Error Code Reference

The ***Error Code Reference*** document has been updated with the following new error codes:

- 85080 – Open Platform Keys are not defined for this device.

- 3102130 – Provided image path does not exist or is inaccessible.

- 3102131 – Failed to load image. This is usually because it is in an unsupported format.

- OA10003 – You do not have sufficient security questions configured.

- OA10004 – Your username or security response is incorrect, please try again.

- OA10005 – The registration link is invalid.

- OA10006 – Logoncode OTPs are disabled on the server.

- OA10007 – Your OTP has been entered incorrectly, is locked or you do not have permission to perform this operation. Please try again.

- OA10008 – Your session has timed out or is invalid, please try again.

- OA10009 – Error registering FIDO in browser.

- OA10010 – Error authenticating FIDO in browser.

- OA10011 – FIDO authentication failed, please try again. You may not have permission to access this client.

- OA10012 – FIDO registration failed, the FIDO token used to register was not trusted. Try a different FIDO token if you have one. <details>

- OA10013 – FIDO registration failed, user mismatch.

- OA10014 – FIDO registration failed, the credential profile is invalid.

- OA10015 – FIDO registration failed, this token is already registered.

- OA10016 – FIDO registration failed, the credential profile is set to Enforce Authenticator Attestation Check, but the token registered does not have metadata available on the server. Try registering a different token.

- OA10017 – FIDO registration failed, there was a problem accessing the FIDO Metadata Server.

- OA10018 – You do not have any FIDO tokens registered.

- OC10005 – The file you have uploaded is not an image. Please upload an image.

- OC10006 – MyID Client Service error.

- OC10007 – A problem has occurred when connecting to the camera.

- WS10002 – Unable to retrieve the values for the specified selection box.

- WS10003 – Unable to retrieve the requested session information.

- WS30021 – Biometric samples of the required type cannot be found for the user.

- WS30022 – must be a date in the future.

- WS30023 – must be a date in the past.

- WS50038 – The selected credential profile is not allowed because the person that requested the job was not allowed to request this credential profile.

- WS50039 – You cannot action your own adjudications.

- WS50041 – This action cannot be performed because the user has outstanding adjudications.

- WS50042 – The request task type is not supported by the credential profile.

- WS50043 – This credential profile can only be requested from Request Device

- WS50044 – This device requires secondary authorization to cancel it. Please use the MyID Desktop Cancel Credentials workflow.

- WS50045 – The device selected cannot be canceled. Please refer to product documentation for further guidance.

17.4.7 FIDO Authenticator Integration Guide

The *FIDO Authenticator Integration Guide* is new for this release.

See section *17.2.5*, *FIDO authenticators* for details of this new feature.

17.4.8　Installation and Configuration Guide

The *Installation and Configuration Guide* has been updated with the following:

- Clarification on the procedure to set up the registry for the unlock credential provider.

  See the *Customizing the unlock credential provider* section.

- Updated the instructions for running GenMaster and the SetHSMPIN utility; you may be prompted for administration credentials.

  See the *Using GenMaster* and *Setting the HSM PIN* sections.

- Note on using the Windows Control Panel Programs and Features option to uninstall MyID, and *not* the Windows Apps & Features screen.

  See the *Uninstalling MyID* section.

- The list of supported client operating systems has been extended to include Windows 10 Version 20H2.

  See the *Operating systems* section.

- Updated the instructions for installing MyID to take account of the Scripts folder.

  See the *Running the installation program* and *Uninstalling MyID* sections.

- Added instructions for upgrading from older versions of MyID to 64-bit MyID 12.

  See the *Upgrading MyID from a 32-bit application to 64-bit* section.

- Added details of the versions of the .NET Core Desktop Runtime required on client PCs.

  See the *Prerequisites* section.

- Added information about signed PowerShell scripts.

  See the *Running the installation program* section.

- Added information on requirements for the new Authentication user account.

  See the *MyID Authentication account* section.

- Updated the installation procedure to include the authentication database, the authentication user, and the new features available in the Server Roles and Features screen.

  See the *Running the installation program* section.

17.4.9　Lifecycle API

The *Lifecycle API* guide has been updated with the following:

- Added a note to the sections on importing answers to security phrases – do not include leading or trailing spaces.

- Added clarifications regarding the credential expiry date functionality; see the `CardExpiryDate` and `MaxRequestExpiryDate` sections.

- The `CMSCardRequest/Group/User/CardUpdate/ParametersXML/UnlockPIN` option is not supported.

Note: The Lifecycle API is now deprecated. For information about the status of this feature, see section *18.1.14*, *Lifecycle API support*.

17.4.10 Microsoft Azure Integration Guide

The *Microsoft Azure Integration Guide* has been updated with the following:

*   Information about requirements for the new authentication database.

    See the *Prerequisites* section.

17.4.11 Mobile Authentication

The *Mobile Authentication* guide has been updated with the following:

*   Added information about configuring the verification service to use an alternative authentication method to 2-way TLS.

    See the *Disabling 2-way TLS for the internal authentication service* section.

*   Added information about the local log on privilege requirements for the MyID web service user.

    See the *Installing the verification service* section.

*   The MyID Authenticator app is now available for Android devices.

    See the *MyID Authenticator* section.

*   Updated the installation process for the MyID Verification Service – now uses the main MyID installation program.

    See the *Installing the verification service* section.

*   Updated the AD FS Adapter for MyID instructions. This is now called the AD FS Adapter Mobile, and shares an installation program with the AD FS Adapter OAuth.

    See the *AD FS Adapter Mobile* section.

17.4.12 Mobile Identity Management

The *Mobile Identity Management* guide has been updated with the following:

*   Supported iOS and Android operating systems.

    See the *Supported devices* section.

*   Added VMWare Workspace ONE to the list of supported Mobile Device Management (MDM) systems.

    See the *Supported Mobile Device Management integration* section

17.4.13 MyID Authentication Guide

The *MyID Authentication Guide* is new for this release.

See section *17.1.9*, *MyID authentication service* for details of this new feature.

17.4.14 MyID Core API

The *MyID Core API* document is new for this release.

See section *17.1.11*, *MyID Core API* for details of this new feature.

17.4.15   MyID Operator Client

The **MyID Operator Client** guide has been updated with the following:

- Added Request Device Renewal to the list of features controlled by the **Request Replacement Card** entry in **Edit Roles**.

  See the *Roles and groups* section.

- Added details of the new date fields.

  See the *Entering dates and times* section.

- Added information about capturing user images.

  See the *Capturing images* section.

- The list of recommended browsers has been updated.

  See the *Supported browsers* section.

- Clarifications regarding the credential expiry date functionality.

  See the *Approving requests* section.

- Added information on using security phrases to log on to the MyID Operator Client.

  See the *Signing in using security phrases* section.

- Added information on configuration changes that require the web server to be refreshed.

  See the *Setting configuration options* section.

- Added information on canceling a device.

  See the *Canceling a device* section.

- Adding information on removing a person.

  See the *Removing a person* section.

- Added Windows Hello to the list of device types you can request.

  See the *Requesting a device for a person* section.

- Added clarification on the use of the button bar.

  See the *Using the button bar* section.

17.4.16　Operator's Guide

The ***Operator's Guide*** has been updated with the following:

- Added information on using the new **Identify Device (Administrator)** workflow.

  See the *Using the Identify Device (Administrator) workflow*.

- Added information on the server-generated PINs option for the **Reset Card PIN** workflow.

  See the *Resetting a card's PIN* section.

- Clarifications regarding the credential expiry date functionality.

  See the *Setting expiry dates for a card* section.

- Added information on the legacy **Change PIN** workflow.

  See the *Changing a card's PIN* section.

- Added information on not configuring your system to upload images to the web server instead of the database if you are using the MyID Operator Client.

  See the *Storing images on the web server* section.

17.4.17　PrimeKey EJBCA Integration Guide

The ***PrimeKey EJBCA Integration Guide*** has been updated with the following:

- Clarifications regarding using an HSM-backed RA certificate.

  See the *Configuring the MyID RA user* and *Configuring the CA within MyID* sections.

17.4.18　Printer Integration Guide

The ***Printer Integration Guide*** has been updated with the following:

- Support for Zebra printers has been deprecated.

  See the *Supported printers* section.

- The Datacard section has been renamed Entrust Datacard, and the details of supported Datacard driver version and printer models have been updated.

  See the *Supported printers* and *Entrust Datacard printers* sections.

- The XID section has been updated with details of the supported printer software, and a note about the incompatibility of the standalone XID printer driver with the EDISecure Connect software.

  See the *XID printers* and *Installing the printer software for XID printers* sections.

17.4.19　Self-Service App

The ***Self-Service App*** guide has been updated with the following:

- Clarification on the procedure to hide which actions are available.

  See the *Controlling which actions are available using the registry* section.

17.4.20 Smart Card Integration Guide

The *Smart Card Integration Guide* has been updated with the following:

- Information about SafeNet eToken 5300 FIPS (Mini) and SafeNet eToken 5300 (Micro) USB tokens has been added.

  See the *Thales authentication devices* and *SafeNet eToken 5300 tokens with Touch Sensor* sections.

- Updated the interoperability information to state that you can use YubiKey tokens to store additional identities.

  See the *Additional identities for YubiKey tokens* section.

- Information about Egofy v3.0 with FIDO devices has been added.

  See the *Egofy smart cards* section.

17.4.21 Symantec MPKI Integration Guide

The *Symantec MPKI Integration Guide* has been updated with the following:

- Updated example CA URL for MPKI 8.

  See the *Configuring the CA in the Certificate Authorities workflow* section.

17.4.22 System Interrogation Utility

The *System Interrogation Utility* guide has been updated with the following:

- Information about the requirement for port 5985 when running the SIU remotely has been added.

  See the *Running the SIU* section.

17.4.23 System Security Checklist

The *System Security Checklist* has been updated with the following:

- Clarification on the **Show Full Name at Logon** and **Show Photo at Logon** configuration options.

  See the *Visibility of user data* section.

17.4.24 Thales Luna HSM Integration Guide

The *Thales Luna HSM Integration Guide* has been updated with the following:

- Information about the Universal Client software and Thales Data Protection on Demand (DPoD).

  See the *Supported Thales Luna HSM models* section.

- Changes for 64-bit operation throughout the document.

17.4.25 Web Service Architecture

The *Web Service Architecture* guide has been updated with the following:

- Information on configuring the web services to handle reverse proxies.

  See the *Reverse proxies and load balancing* section.

17.4.26 Windows Hello for Business

The *Windows Hello for Business* guide has been updated with the following:

- You can now use the MyID Operator Client to request or cancel a Windows Hello credential.

  See the *Requesting a Windows Hello credential* and *Canceling a Windows Hello credential* sections.

17.4.27 Updates for 64-bit MyID

The documentation throughout has been updated for 64-bit operation. Primarily the changes are:

- The default installation location for MyID server has changed from:

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

  to:

  `C:\Program Files\Intercede\`

- Registry locations on the MyID server no longer use the `WoW6432Node`.

- MyID now uses the Windows `System32` folder instead of the Windows `SysWOW64` folder.

Note: MyID clients continue to be supplied as 32-bit applications, so paths and registry settings relating to clients have not changed.

17.4.28 Supported operating systems and databases

The documentation throughout has been updated to remove support for the following:

- Windows 8.1

- Windows Server 2012 R2

- SQL Server 2012 SP4

See section *17.5.4*, *Windows 8.1 end of support*, section *17.5.5*, *Windows Server 2012 R2 end of support*, and section *17.5.3*, *SQL Server 2012 SP4 end of support* for details of the end-of-support features.

17.4.29 Additional Windows installer requirements

The documentation throughout has been updated to remove the additional requirements for Windows installer versions. All versions of Windows supported by MyID have a suitable version of Windows installer included as standard.

17.4.30 Document conversions

The following documents are now available in HTML, allowing for full text search across the documentation set:

- *Reporting Web Service API*

- *Credential Web Service*

Only the *Lifecycle API* document is now available only in PDF format; for information about the status of this document see section *18.1.14*, *Lifecycle API support*.

17.5   End of support features in MyID 12.0.0

This section contains information about features that are no longer supported in MyID as of MyID 12.0.0.

See:

- section *17.5.1*, *Android 7 end of support*.
- section *17.5.2*, *iOS 11 end of support*.
- section *17.5.3*, *SQL Server 2012 SP4 end of support*.
- section *17.5.4*, *Windows 8.1 end of support*.
- section *17.5.5*, *Windows Server 2012 R2 end of support*.

17.5.1   Android 7 end of support

Android 7 OS version is now End of Support.

For information on supported mobile OS versions, see the *Supported devices* section in the *Mobile Identity Management* guide.

17.5.2   iOS 11 end of support

iOS 11 is now End of Support.

For information on supported mobile OS versions, see the *Supported devices* section in the *Mobile Identity Management* guide.

17.5.3   SQL Server 2012 SP4 end of support

Support for SQL Server 2012 SP4 for all Intercede-provided software has now ended.

See the *Database versions* section in the *Installation and Configuration Guide* for details of the databases that are currently supported.

17.5.4   Windows 8.1 end of support

Support for Windows 8.1 for all Intercede-provided software has now ended.

See the *Operating systems* section in the *Installation and Configuration Guide* for details of the client operating systems that are currently supported.

17.5.5   Windows Server 2012 R2 end of support

Support for Windows Server 2012 R2 for all Intercede-provided software has now ended.

See the *Operating systems* section in the *Installation and Configuration Guide* for details of the server operating systems that are currently supported.

17.6   Known issues resolved in MyID 12.0.0

This section lists the known issues that were resolved in MyID 12.0.0. These are issues that were found across both editions of MyID – Enterprise and PIV – and may not all be relevant for your system.

- IKB-334 – Problems when setting the User Data Approved field.
- IKB-335 – Incorrect storage of dates.

- IKB-336 – Error recorded in the audit when setting the User Data Approved field.
- IKB-337 – Incorrect date displayed for Maximum Expiry Date in the MyID Operator Client.

18   Feature lifecycle

This section contains details of the lifecycle of supported features.

See section *18.1*, *Deprecated features* for details of features that are no longer being actively developed and are expected to become End of Support in the near future.

Once a feature has become End of Support, it is listed in the Release Notes for that release; see:

- section *6.4*, *End of support features in MyID 12.9.0*
- section *7.5*, *End of support features in MyID 12.8.0*.
- section *8.5*, *End of support features in MyID 12.7.0*.
- section *9.5*, *End of support features in MyID 12.6.0*.
- section *10.6*, *End of support features in MyID 12.5.0*.
- section *11.5*, *End of support features in MyID 12.4.1*.
- section *12.5*, *End of support features in MyID 12.4.0*.
- section *13.5*, *End of support features in MyID 12.3.0*.
- section *14.5*, *End of support features in MyID 12.2.0*.
- section *15.5*, *End of support features in MyID 12.1.0*.
- section *16.5*, *End of support features in MyID 12.0.1*.
- section *17.5*, *End of support features in MyID 12.0.0*.

18.1   Deprecated features

This section contains information about features that are deprecated in MyID.

A feature listed as deprecated indicates that it is no longer being actively developed and is expected to become End of Support in the near future. This means:

- Deprecated features are still supported in the current release of software.
- Intercede will provide only critical bug fixes on a deprecated feature.
- Customers currently using deprecated features should plan to transition to a replacement feature or alternative solutions.

18.1.1   MyID Desktop workflows

As MyID moves towards greater use of the MyID Operator Client, some workflows within MyID Desktop are either duplicated in the MyID Operator Client or relate to features that are no longer being developed. This list of deprecated MyID workflows is added to over time.

The following workflows in MyID Desktop are now deprecated, and you are recommended to start using the alternative functionality provided by the MyID Operator Client or the Self-Service App where appropriate.

18.1.1.1 MyID Desktop workflows deprecated at MyID 12.12.0

The following MyID Desktop workflows are deprecated:

Category	Workflow	Alternative
Cards	Print Badge	You can create a credential profile that allows you to issue cards that comprise only a printable surface (with or without a magnetic stripe). These cards are added to the MyID database, allowing you to manage the cards; for example, you can renew, replace, disable, or cancel them. See the *Setting up a credential profile for physical printed cards* section in the ***Administration Guide*** for more information.

18.1.1.2 MyID Desktop workflows deprecated at MyID 12.8.0

The following MyID Desktop workflows are deprecated:

Category	Workflow	Alternative
Cards	Identify Device (Administrator)	You can view the device history and its initial PIN from the View Device screen in the MyID Operator Client. See the *Viewing a device's history* and *Viewing the initial PIN for a device* sections in the ***MyID Operator Client*** guide for details.
Cards	Reinstate Card	Use the Reinstate option for a device in the MyID Operator Client. See the *Reinstating a device* section in the ***MyID Operator Client*** guide for details.
Certificates	Certificate Requests	Use the Certificates feature in the MyID Operator Client. See the *Working with certificates* section in the ***MyID Operator Client*** guide for details.
Certificates	Issued Certificates	Use the Certificates feature in the MyID Operator Client. See the *Working with certificates* section in the ***MyID Operator Client*** guide for details.
Certificates	Revoked Certificates	Use the Certificates feature in the MyID Operator Client. See the *Working with certificates* section in the ***MyID Operator Client*** guide for details.
Configuration	Audited Items	You can make modifications to audited items as part of project configuration. Contact your Intercede account manager for further details.

18.1.1.3 MyID Desktop workflows deprecated at MyID 12.7.0

The following MyID Desktop workflows are deprecated:

Category	Workflow	Alternative
People	Manage Additional Identities	Use the additional identities features in the MyID Operator Client. See the *Working with additional identities* section in the ***MyID Operator Client*** guide for details.
People	Manage My Additional Identities	Use the additional identities features in the MyID Operator Client. See the *Working with additional identities* section in the ***MyID Operator Client*** guide for details.
Cards	Batch Request Card	This is replaced by new batch capabilities in the MyID Operator Client. See the *Adding multiple people from a directory* and *Requesting devices for multiple people* sections in the ***MyID Operator Client*** guide for details.
Cards	Card Disposal	Use the Change Disposal Status screen in the MyID Operator Client. See the *Disposing of a device* section in the ***MyID Operator Client*** guide for details.
Cards	Deliver Card	Use the Accept Delivery option in the MyID Operator Client. See the *Accepting delivery for a device* section in the ***MyID Operator Client*** guide for details.

18.1.1.4 MyID Desktop workflows deprecated at MyID 12.6.0

The following MyID Desktop workflows are deprecated:

Category	Workflow	Alternative
People	Add Person	Use the Add Person screen in the MyID Operator Client. See the *Adding a person* section in the ***MyID Operator Client*** guide for details.
People	Authenticate Person	This comprised the following features: • Identity Documents – will not be replaced. • Operator Approval – will not be replaced. • Security Phrases – Security Phrase authentication is available to access self service operations, as well as the MyID authentication server for integration into other processes.
People	Edit Person	Use the Edit Person screen in the MyID Operator Client. See the *Editing a person* section in the ***MyID Operator Client*** guide for details.
People	Remove Person	Use the Remove Person screen in the MyID Operator Client. See the *Removing a person* section in the ***MyID Operator Client*** guide for details.

Category	Workflow	Alternative
People	View Person	Use the View Person screen in the MyID Operator Client. See the *Searching for a person* section in the **MyID Operator Client** guide for details.
Cards	Assign Card	Use the Assign Device feature in the MyID Operator Client. See the *Assigning a device to a request* section in the **MyID Operator Client** guide for details.
Cards	Cancel Credential	Use the Cancel Device screen in the MyID Operator Client. See the *Canceling a device* section in the **MyID Operator Client** guide for details.
Cards	Collect My Card	Use the card collection feature in the Self-Service App. See the *Self-Service App features* section in the **Self-Service App** guide for details.
Cards	Collect My Updates	Use the card update feature in the Self-Service App. See the *Self-Service App features* section in the **Self-Service App** guide for details.
Cards	Enable/Disable Card	Use the Enable Device and Disable Device screens in the MyID Operator Client. See the *Enabling and disabling devices* section in the **MyID Operator Client** guide for details.
Cards	Identify Card	Use the View Device screen in the MyID Operator Client; you can search for a device, or insert the device. See the *Searching for a device* and *Reading a device* sections in the **MyID Operator Client** guide for details.
Cards	Issue Card	Use the Request Device Issuance screen followed by the Collect option on the View Request screen in the MyID Operator Client. See the *Requesting a device for a person* and *Collecting a device request* sections in the **MyID Operator Client** guide for details.
Cards	Issue Temporary Card	Use the Request Device Issuance screen followed by the Collect option on the View Request screen in the MyID Operator Client. See the *Requesting a device for a person* and *Collecting a device request* sections in the **MyID Operator Client** guide for details.
Cards	Manage VSC Access	The feature for managing access to VSCs will not be replaced.

Category	Workflow	Alternative
Cards	Reprovision Card	Use the Request Update screen followed by the Collect Updates option on the View Device screen in the MyID Operator Client. See the *Requesting an update for a device* and *Updating a device* sections in the **MyID Operator Client** guide for details.
Cards	Reprovision My Card	Use the Request Update screen in the MyID Operator Client, followed by the card update feature in the Self-Service App. See the *Requesting an update for a device* section in the **MyID Operator Client** guide and the *Self-Service App features* section in the **Self-Service App** guide for details. Alternatively, you can configure MyID for self-service updates using the Self-Service App; see the *Configuring MyID to allow self-service device updates* section in the **Self-Service App** guide for details.
Cards	Request Auth Code	Use the Send Activation Code or Send Unlock Code screen in the MyID Operator Client. See the *Sending an authentication code to activate a device* and *Sending a code to unlock a device* sections in the **MyID Operator Client** guide for details.
Cards	Request Card	Use the Request Device Issuance screen in the MyID Operator Client. See the *Requesting a device for a person* section in the **MyID Operator Client** guide for details.
Cards	Request Card Update	Use the Request Update screen in the MyID Operator Client. See the *Requesting an update for a device* section in the **MyID Operator Client** guide for details.
Cards	Request Replacement Card	Use the Request Replacement Device screen in the MyID Operator Client. See the *Requesting a replacement device* section in the **MyID Operator Client** guide for details.
Cards	Unlock Temporary VSC Access	The feature for managing access to VSCs will not be replaced.
Cards	Update Card	Use the Request Update screen followed by the Collect Updates option on the View Device screen in the MyID Operator Client. See the *Requesting an update for a device* and *Updating a device* sections in the **MyID Operator Client** guide for details.

Category	Workflow	Alternative
Cards	Validate Request	Use the Approve Request screen in the MyID Operator Client. See the *Approving, rejecting, and canceling requests* section in the **MyID Operator Client** guide for details.
Mobile	Enable/Disable ID	Use the Enable Device and Disable Device screens in the MyID Operator Client. See the *Enabling and disabling devices* section in the **MyID Operator Client** guide for details.
Mobile	Request ID	Use the Request Mobile Issuance screen in the MyID Operator Client. See the *Requesting a mobile device for a person* section in the **MyID Operator Client** guide for details.
Mobile	Request Replacement ID	Use the Request Replacement Device screen in the MyID Operator Client. See the *Requesting a replacement device* section in the **MyID Operator Client** guide for details.

18.1.2   Entrust Administration Toolkit for C

MyID's integration with Entrust using the Entrust Administration Toolkit for C, as documented in the **Entrust CA Integration Guide**, is now deprecated, and has been superseded by support for the Entrust Authority Security Administration Toolkit for the Java Platform (JASTK).

For information about the differences between MyID's integration with Entrust through JASTK as opposed to through the Entrust Administration Toolkit for C, see the *Differences with JASTK* section of the **Entrust JASTK CA Integration Guide**.

For assistance with migrating from the Entrust Administration Toolkit for C to the Entrust Authority Security Administration Toolkit for the Java Platform (JASTK), contact Intercede customer support quoting reference SUP-389.

Note: This feature was first announced as deprecated at MyID 12.12.0.

18.1.3   Athena smart cards

This section lists Athena devices that are currently deprecated.

Customers already using these devices should plan to migrate to alternative devices.

See the *Athena smart cards* section in the **Smart Card Integration Guide** for details.

18.1.3.1 Athena smart cards deprecated at MyID 12.12.0

The following Athena devices are deprecated:

- Athena IDProtect

  As an alternative, you are recommended to migrate to Egofy smart cards.

  See the *Egofy smart cards* section in the **Smart Card Integration Guide** for details.

18.1.4   Giesecke+Devrient smart cards

This section lists Giesecke+Devrient devices that are currently deprecated.

Customers already using these devices should plan to migrate to alternative devices.

See the *Giesecke+Devrient smart cards* section in the **Smart Card Integration Guide** for details.

18.1.4.1 Giesecke+Devrient smart cards deprecated at MyID 12.12.0

The following Giesecke+Devrient devices are deprecated:

- Sm@rt Café® Expert 6.0

  As an alternative, you are recommended to migrate to SCE v7.0 devices.

18.1.5   IDEMIA smart cards

This section lists IDEMIA devices that are currently deprecated.

Customers already using these devices should plan to migrate to alternative devices.

See the *IDEMIA smart cards* section in the **Smart Card Integration Guide** for details.

18.1.5.1 IDEMIA smart cards deprecated at MyID 12.12.0

The following IDEMIA devices are deprecated:

- Oberthur ID-One Cosmo v7.0.1 with IAS Standard applet

  As an alternative, you are recommended to migrate to IDEMIA ID-One PIV 2.4.2 on Cosmo V8.2 smart cards.

18.1.6   GenMaster

The GenMaster utility is now deprecated, and has been replaced by incorporating its features into the MyID Installation Assistant process.

See the *Using GenMaster* section in the **Installation and Configuration Guide** for details.

Note: This feature was first announced as deprecated at MyID 12.12.0.

18.1.7   MyID CMS Authenticator App

The MyID CMS Authenticator app, and accompanying ADFS integration feature, are now deprecated.

Similar capabilities based on FIDO Passkeys are available with MyID MFA; see:

www.intercede.com/myid-product-suite/myid-mfa/

For further guidance, contact Intercede quoting reference SUP-392.

Note: This feature was first announced as deprecated at MyID 12.12.0.

18.1.8   MyID Identity Agent app

The MyID Identity Agent app provided the ability to issue certificates to the iOS and Android system key chains or an Identity Agent key store that could be accessed by third-party apps built for the purpose.

Following a review of use in customer deployments, these apps are now deprecated in favor of integrations with Mobile Device Management systems and third-party apps built using the MyID Identity Agent Framework.

For further information on integration with these solutions, see the *Mobile Identity Management* guide.

Note: This feature was first announced as deprecated at MyID 12.12.0.

18.1.9   Thales authentication devices

This section lists Thales authentication devices that are currently deprecated.

Customers already using these authentication devices should plan to migrate to alternative devices.

See the *Thales authentication devices* section in the *Smart Card Integration Guide* for details.

18.1.9.1 Thales authentication devices deprecated at MyID 12.8.0

The following Thales authentication devices are deprecated:

- IDPrime MD3810
- IDPrime MD830
- IDPrime MD830 Rev B FIPS Level 2
- IDPrime MD830 Rev B FIPS Level 3
- IDPrime MD831

18.1.9.2 Thales authentication devices deprecated at MyID 12.5.0

The following Thales authentication devices are deprecated:

- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110+

18.1.9.3 Thales authentication devices deprecated at MyID 11.8.0

The following Thales authentication devices deprecated:

- IDPrime MD3840
- IDPrime MD840 Rev A
- IDPrime PIV Card v2.0
- SafeNet eToken 4100
- SafeNet eToken 5100
- SafeNet eToken 5110
- SafeNet eToken 5110 CC

18.1.10 Self-Service App automation mode

The Self-Service App automation mode is designed to run on the user's own PC and to carry out VSC lock operations without user interaction. This feature is now deprecated, and will not be replaced by equivalent functionality.

Note: This feature was first announced as deprecated at MyID 12.6.0.

18.1.11 Save to Excel

The Save to Excel feature of Management Information Reports is now deprecated.

As an alternative, you can save reports from the MyID Operator Client in CSV format, which you can open in Excel; see the *Working with reports* section in the ***MyID Operator Client*** guide.

Note: This feature was first announced as deprecated at MyID 12.2.0.

18.1.12 Internet Explorer as a user interface

Customers upgrading from earlier versions of MyID may have continued to use Internet Explorer to access the MyID user interface, including the use of direct links to operations using Portal Integration API. Following Microsoft's announcement of the retirement of Internet Explorer, this method of accessing MyID is now deprecated.

Customers should plan migration to the MyID Operator Client instead. During this transition period, customers affected by the retirement of Internet Explorer should follow guidance from Microsoft on using Microsoft Edge in Internet Explorer Mode; see the following page for details:

docs.microsoft.com/en-us/deployedge/edge-ie-mode-policies#configure-sites-on-the-enterprise-site-list

Note: This feature was first announced as deprecated at MyID 12.2.0.

18.1.13 Intel Authenticate Virtual Smart Card support

MyID support for Intel Authenticate Virtual Smart Cards has now been deprecated. If you are currently using this solution or have further questions about it, contact Intercede for further details quoting SUP-349.

Note: This feature was first announced as deprecated at MyID 12.1.0.

18.1.14 Lifecycle API support

The MyID Lifecycle API is now deprecated, and is in the process of being replaced by the MyID Core API. Full replacement will take place over a number of product releases.

The Lifecycle API will continue to be maintained, but in the longer term, it will no longer be available for use, and will eventually be fully removed from MyID.

Intercede recommends that you incorporate migration away from the Lifecycle API into your future planning, and would be happy to assist you with this process. For further details, contact your Intercede account manager.

For more information about the MyID Core API, see the ***MyID Core API*** guide.

Note: This feature was first announced as deprecated at MyID 12.0.0.

18.1.15   Zebra printer support

Support for Zebra smart card printers is now deprecated. Customers using these printers should plan to migrate to alternative devices.

See the *Supported printers* section in the *Printer Integration Guide* for more information.

Note: These printers were first announced as deprecated at MyID 12.0.0.

19   Known issues

This section contains known issues with MyID. These are issues that have been found across both editions of MyID – Enterprise and PIV – and may not all be relevant for your system.

- **IKB-15 – 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.

- **IKB-16 – Pressing back shortcut key causes blank screen**

  As many MyID workflows are based on web pages, and MyID Desktop embeds a browser control to display these workflows, you may experience problems if you attempt to use the browser's controls to go back; for example, pressing ALT + left arrow or pressing Backspace when not editing a field. These browser controls cannot be overridden.

  Typically, the problem presents itself as a blank screen.

  If this happens, click the Home button and restart the workflow.

- **IKB-20 – Pressing refresh (F5) causes blank screen**

  As many MyID workflows are based on web pages, and MyID Desktop embeds a browser control to display these workflows, you may experience problems if you attempt to use the browser's controls to refresh the screen using the F5 key.

  Typically, the problem presents itself as a blank screen.

  If this happens, click the Home button and restart the workflow, or close MyID Desktop and restart.

- **IKB-27 – Cannot click on links in email notifications**

  There is an issue with links being removed from email messages. This may occur with emails received through Outlook Web Access or on some mobile mail clients. In some cases, Microsoft Exchange may remove hyperlinks from messages.

  For more information, contact Intercede customer support quoting reference SUP-176.

- **IKB-35 – OTP fails to validate if security phrases are locked**

  If you attempt to validate a job OTP (for example, a logon code, or a challenge code for SCEP issuance) but the user's security phrases are locked, the validation will fail.

  As a workaround, unlock the user's security phrases using the Unlock Security Phrases workflow before attempting to validate the OTP.

- **IKB-80 – Cannot activate a card that has been reinstated when it was issued using 1-Step pre-encoding**

  If you have issued a card using the 1-Step option for **Pre-encode Card** in the credential profile, then use **Reinstate Card**, you cannot proceed to activate the card; the card is not recognized as being ready for activation.

  As a workaround, you must cancel and re-issue the card.

- **IKB-81 – Cannot click on links in email notifications**

  You can configure MyID to notify users by email that a mobile identity is available for them to collect. There is an issue with some email servers where they remove links from email messages before sending the message to mobile clients, which stops the email notification link from being used to start Identity Agent to collect the mobile identity. Additionally some email clients can also remove the link even if it has been provided in the email from the server. For more information, contact Intercede customer support quoting reference SUP-176.

- **IKB-84 – Cannot use the Request Replacement ID workflow with Identity Agent-based credential profiles**

  The **Request Replacement ID** workflow allows you to request a replacement ID for a user where the mobile device may have been lost or stolen. If the credential profile used to issue the mobile ID had the **Identity Agent (Only)** option selected, you cannot use this workflow; an error appears in MyID when you attempt to request a replacement ID.

  As a workaround, you can cancel the mobile credential using the **Cancel Credential** workflow, then request a new mobile identity for the user.

- **IKB-88 – Existing mobile credentials overwritten**

  When using Identity Agent-based credential profiles, if you request a mobile identity for a user, the new identity overwrites the existing identity; the original identity is canceled in MyID, but the certificates remain issued.

- **IKB-118 – Issue when using MyID Desktop with JAWS**

  You may experience an intermittent problem when using the JAWS screen-reading software (version 12 and later): MyID Desktop may become unresponsive when you open the New Action dialog, depending on the number of available workflows.

- **IKB-182 – Mobile devices with multiple keystores show one entry, but cancel all**

  When canceling credentials on a mobile device, the search results display a single entry that represents the primary keystore on the device. Where the device has been issued with multiple keystores, all the associated certificates will be canceled.

- **IKB-215 – Software certificate renewals use the original credential profile settings**

  The content of software certificate packages is determined by a credential profile. When renewing software certificates, changes to the certificate policies assigned to the credential profile will not be picked up – the policies defined in the original version of the credential profile will be used. If a certificate policy has been superseded, the replacement policy will be used automatically.

- **IKB-219 – Contactless card detection**

  There are some differences between the **Issue Card** workflow and the updated **Collect Card** and **Batch Collect Card** workflows.

  With **Issue Card**, you cannot issue a dual-interface (contact chip and contactless) smart card unless it has been previously imported to the system using the **Import Serial Numbers** workflow, or it has been previously issued as a dual-interface smart card using **Collect Card**. Unknown dual-interface cards are not supported. Contactless-only cards require the credential profile to be set as **Must be a Proximity Card** when used with **Issue Card**.

  If you require Contactless-only card issuance to be restricted to known devices only (to enforce the credential profile setting **Must be a known Proximity Card**), or require information to be sent to a PACS, the card details must be imported separately. Contact customer support quoting reference IKB-219 for assistance.

- **IKB-236 – Differences in PIN policy between Change PIN and Reset PIN workflows**

  You can set the PIN Policy for smart cards within the credential profile. If you change the PIN policy in the credential profile after issuing a card, the **Change PIN** workflow, and older web-based workflows (**Unlock Card**, **Auto Unlock Card**) will continue to use the PIN policy set at the time the card was issued.

  The Self-Service Kiosk, the **Reset Card PIN** workflow, and self-service **Reset PIN** feature in MyID Desktop will use the PIN policy from the latest version of the credential profile, allowing PIN policy to be changed at any time. During any issuance process, the PIN policy is always taken from the latest version of the credential profile.

  If you need to modify your PIN policy and are affected by this issue, contact customer support quoting reference SUP-284.

- **IKB-247 – Problem with transaction locking smart cards**

  When MyID clients interact with smart cards or tokens that present a smart card interface, a transaction lock to the card takes place to prevent other software from interrupting any processing that MyID is carrying out.

  Some actions in Windows, typically involving authentication (for example, locking the Windows logon session using CTRL-ALT-DELETE, or starting an application such as Task Manager that requires administrator authentication with a smart card) that take place while a MyID client is accessing the smart card may result in Windows being unable to access the card.

  This could cause issues such as preventing the user from unlocking the computer again. Removing the smart card from the reader or waiting for the Windows operation to time out will overcome the problem.

- **IKB-251 – Revoking certificates outside MyID may cause errors**

  MyID provides a management interface to certificate authorities and controls the issuance and revocation process of certificates. If the status of a certificate issued by MyID is changed on the certificate authority (for example a certificate is revoked) MyID will not be aware of the status change of the certificate, so subsequent attempts to revoke

the certificate may fail. Depending on the type of certificate authority, the nature of the failure may be different. Failures to revoke certificates will be reported in the **System Events** and **Audit Reports** workflow.

- **IKB-268 – Automatic Update Collection configuration option is amended on upgraded systems**

  If you have upgraded an existing system, check the value of the **Automatic Update Collection** configuration option on the **Issuance Processes** page of the **Operation Settings** workflow. This option controls which workflows run automatically at logon if the user has a pending job. The upgrade process changes this value to `2,245;2,255` – you must check that this is appropriate and revert it to its previous value if necessary.

- **IKB-291 – Cannot use smart card after updating to Elliptic Curve (ECC) certificates**

  If you attempt to update a smart card to change from using certificates with RSA Key Pairs to Elliptic Curve certificates, the card will not be usable after the update process has completed.

  This will occur if you use the **Update Card** or **Collect My Updates** workflows, or collect the update using the Self-Service App.

  An alternative method to replace all certificates is to use the **Reprovision Card** or **Reprovision My Card** workflow, or request a card update using the following reason:

  - **New credential profile needs to be applied**

  which creates a reprovision request to be collected using the Self-Service App.