MyID Enterprise

Version 12.13

Implementation Guide

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

Document reference: IMP1940-12.13.0-Enterprise

December 2024

Copyright

"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

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

© You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. ---

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

MyID® is a flexible and configurable solution for issuing and managing secure credentials. It integrates a wide range of security products and device types to enable a centralized management of credentialing processes.

This document provides a starting point for learning more about the product and its main components.

It is important to note that MyID is available in 'Enterprise' or 'PIV' configurations (PIV is targeted at US Federal Government and associated industries). Intercede may also have provided customizations to suit your deployment requirements. Additional capabilities or configurations may be available that are not mentioned below – further information may be provided for your installation to describe specific features or customizations.

1.1 Learning more about devices and systems that can be integrated with MyID

MyID can be integrated with a range of devices and systems, to:

- Store, protect and manage secure credentials on:
  - Smart cards.
  - USB tokens.
  - Mobile devices.
  - SCEP-compliant hardware devices.
  - Computers protected by hardware security such as Trusted Platform Modules.
- Issue and manage digital certificates, issued by a Certificate Authority. MyID:
  - Supports a range of certificate authority types using a connector based architecture.
  - Enables certificate policy management, including replacing policies and dynamically altering certificate content at issuance.
  - Supports secure key recovery based on configurable policy.
- Provide smart card graphical personalization using smart card printers, or connectivity to a card manufacturing bureau.
- Enable secure cryptographic processing and protect data with a Hardware Security Module.
- Retrieve user information from a connected Active Directory or enable information transfer to and from your own systems through APIs.

1.2 Product documentation

Detailed documentation is available covering the installation and configuration of MyID and administration of the system; integration guides are available for each major product and API that is supported.

1.2.1 Learning about the current release

Every version of MyID is supplied with comprehensive ***Release Notes*** that cover the new and updated features in the release, any end-of-support features, and known issues.

1.2.2 Learning more about what MyID can do

The MyID ***Operator's Guide*** and ***Administration Guide*** describes the workflows and processes available in the product. You can use these to manage the process of issuing and maintaining secure credentials, and administering the solution.

1.3 Learning more about the components of MyID and planning your deployment

For a description of the main software components of MyID, and information on versions and where to locate each item, see section *3*, *MyID components*.

For detailed information about the hardware and software requirements, planning and preparing for deploying MyID, and installation instructions, see the ***Installation and Configuration Guide***.

It is important that you evaluate the security of the overall solution – see the ***System Security Checklist*** for details of the security considerations you must evaluate when planning your deployment.

2 Getting started

MyID provides a comprehensive management solution to the problems associated with the issuance and maintenance of credentials to smart cards and tokens as well as hardware devices such as tablets, computers, smart phones and other mobile devices. It can help you to retain full control over the content and lifecycle of these devices and credentials, while permitting day to day operation by non-expert staff.

This document explains the design processes and configuration steps that you need to undertake to deploy MyID in your organization in the most efficient manner.

2.1 Basic concepts

To work effectively with MyID, it is important to understand some of the basic concepts that are fundamental to the product. These are primarily concerned with personnel account management, device content control and issuance models.

2.1.1 Personnel account management

A User Account is created for each MyID user in the MyID database. These accounts hold information about the individuals, which includes their rights and privileges within MyID and the devices and credentials that are known to be issued to them.

In any IT system, there are often many sources of information relating to individuals – directories, HR systems, accounting packages, and so on. MyID can integrate with systems such as these to collect and share such information, and also record data that is specific to MyID (such as roles and issued credentials).

User information must be kept current and MyID acts as a 'cache' for data that has been read from other systems. This means that it can be configured to verify that the user details are still correct before the data is used.

MyID can also be used as the primary owner of this information – data can be entered about a person directly to the user interface, and also provide business processes to ensure that information is in the correct and approved state prior to credentials being issued.

2.1.2 Role separation

A fundamental concept in the design of a secure credential issuance system is that of 'Role Separation'. This describes the practice of ensuring that no individual is permitted both to enroll users and issue credentials, thus avoiding a single point of failure in the deployment.

To support this, MyID lets you define multiple named 'Roles', each of which is granted access to a chosen subset of the MyID management options. Some default roles are provided as standard, but you may prefer to design your own roles to suit your particular organization and expected issuance models.

2.1.3 Groups and Directory Organizational Units

MyID lets you organize personnel into 'Groups'. These form a strict hierarchy, with each person belonging exclusively to a single group. This structure should normally be used to represent the reporting structure within your organization, since it forms the basis for defining the security 'scope' of each person.

If you are integrating with a directory, groups are usually associated with a particular Organizational Unit. This is especially important if you have a Certification Authority using data from the same directory (for example, to support Windows smart card logon). MyID is able to record such relationships and provides synchronization, import, and export options to help maintain the integrity of the overall solution.

2.1.4 Scope and multiple roles

A common problem with strict role-based authorization systems is that they struggle to accommodate the real-world situations where most people have multiple roles within their job description. Typically this means that you have to define role content for every possible combination of actual roles. MyID avoids this problem by permitting the allocation of multiple roles to each individual. In this manner, a person may be both a Manager and a Help Desk Operator without needing to define a 'Manager and Help Desk Operator' composite role.

The MyID roles mechanism can combine the allocation of a role to a person with the concept of 'Scope'. This determines which user accounts the person is allowed to manage within the menu options associated with the role. For example, individuals can be managers for people in their own groups and help desk operators for everyone in the organization.

Under these circumstances, a person connecting to MyID will see the combined set of menu options that are available for each of the assigned roles. However, when they execute each option they will only see those user account that they are allowed to carry out the selected operation on, according to their roles and associated scope.

Also, Administrative Groups can be used to allow an operator to manage user accounts located in MyID groups anywhere within the group hierarchy, including groups that are not directly connected to the operator's home group. See the *Administrative groups* section in the ***Administration Guide*** for details.

2.1.5 Extended attributes

MyID can be customized by adding attributes to record further information for objects held in the MyID database – for example, you may want to record postal addresses for each person or an asset tag number for a stored device. These attributes can then be used in management and personalization processes. The definition and implementation of custom attributes generally requires advice and assistance from the Professional Services team.

2.1.6 Credential personalization

Smart cards and tokens can be personalized electronically with a wide range of credentials, applications and data. These can be applied to either the contact or contactless portions of suitable cards and tokens. In addition, cards can be physically printed using a mixture of static and dynamic data, such as logos, photographs, names, dates and serial numbers.

Many mobile and other computing devices incorporate secure elements such as UICC SIM cards, secure microSD cards and Trusted Platform Modules that can behave in a similar way to smart cards. There are a growing number of software based alternative solutions that may also offer secure storage of credentials.

With such a range of possibilities, it is important to define and control a finite number of valid combinations, so that you can be certain that all issued devices and credentials will behave correctly in the application environment for which they were created.

To manage this, MyID lets you create named credential profiles. A profile defines:

- what may be issued – the technology type, such as a smart card, printed identity badge, virtual smart card or mobile identity
- the policy to be used – what are the PIN requirements, how shall the device be personalized, is an authentication code or fingerprint match required before issuance can take place
- how the request process is controlled – is pre-enrollment required, should an administrator approve issuance of this profile to a user
- which certificates are to be issued by the CA

This logical definition can also be associated with one or more visual ID badge layouts, giving you the ability to include rapid visual identification of logically different card types should you wish.

Finally, each credential profile has an associated list of permitted recipient roles and issuers. This means that you can define card content for different levels of privilege and be certain that they can only be issued to and by people who have been assigned the appropriate roles within MyID.

2.1.7 Issuance models

MyID supports a wide range of issuance models. You should be able to find an appropriate combination to suit your particular business model, whether this is primarily face-to-face, self-service or centralized bulk issuance. MyID lets you implement multiple issuance models, since we recognize that the method used for initial deployment is likely to be different to that needed for 'steady state' post-issuance management.

The important thing to consider is how the different stages of card and credential lifecycle are to be managed. The primary phases are:

- Enrollment

  How will you get user details into MyID? This might be individual keyed entry, import from a directory, or import through a web service.
- Request

  Will a card be requested at enrollment time or as a separate operation? Can users request their own credentials or should this be done by their manager or an administrator?
- Request authorization

  Do you want to have an additional person to authorize requests for cards?
- Collection

  Are the credentials to be collected by the users or their managers? Will you use a bureau or desktop printing? Are credentials to be collected in person or distributed by mail?
- Unblocking

  When the credentials are protected by a PIN, it is common for the PIN to be forgotten or become locked after a number of authentication attempts with the wrong value. Do you want users to be able to unblock the PIN on their own or should this be done by a manager or via a telephone help desk?

- Canceling and suspension

  Will the credentials be canceled centrally or remotely? Is any smart card recycling expected? What 'Reasons for Replacement' are required and what should the corresponding action be?

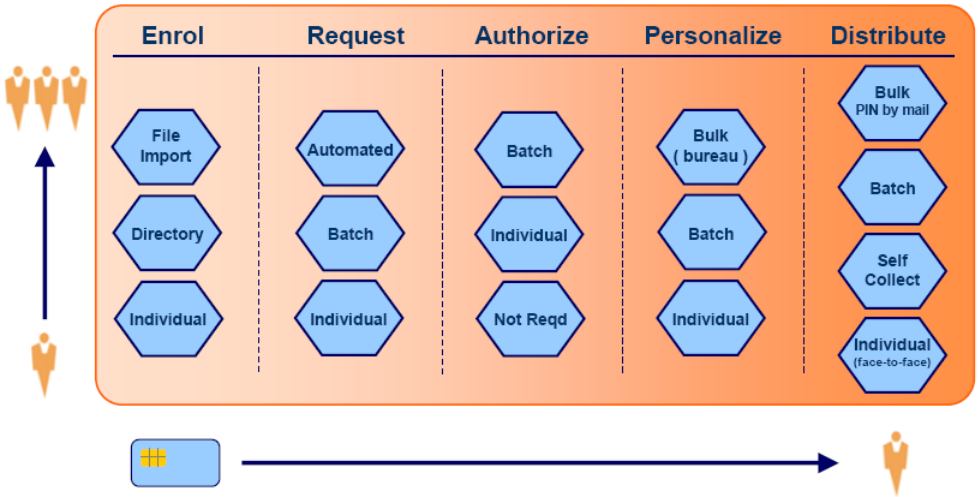
- Activation

  Are the credentials enabled immediately once created, or are they issued in a locked state, requiring an activation process either by the credential owner or with the help of an operator? How do you want to deal with this activation – do you want to use one-time authorization codes or pre-registered security questions to prove the identity of the owner?

2.2 Suggested configuration sequence

Before you start to install your production environment, it is essential that you design your implementation carefully. In many cases, this is best done through an iterative process, using a pilot or test installation to refine the model.

The first thing to consider is what issuance model(s) you want to implement, since this will directly affect the menu options and management roles that you will need. The simplest approach to this is to use the diagram below to decide which mechanism(s) you want to use for each stage in the card and credential's lifecycle.



This should enable you to decide whether you want to use one-pass face-to-face card issuance or a separate request-authorize-collect design, whether you are printing cards centrally or collecting remotely, and so on. It is important that this design stage is considered carefully, so that you have a consistent, efficient deployment model that meets your business objectives.

2.2.1 Roles

Use the issuance model requirements to define the roles that you will need to operate the system. Try to keep the roles 'atomic' in nature; that is, define discrete job functions rather than try to create a role for each combination of tasks that individuals may perform in your organization.

As an example, you might define a CardHolder role to contain those operations available to every cardholder (for example, Collect My Card). If you then define a 'Personnel' role, you should not repeat Collect My Card within that role, since you will expect every Personnel operator to also be a CardHolder. If you construct roles in this manner, it becomes much easier to change individual roles in one place.

2.2.2 Groups

Next, you should establish the organizational group structure that you will use to control the lines of authority within your MyID deployment. This may be by job function, geographically, based on LDAP Organizational Units and so on. It is important that this structure matches the 'Scope' of the roles that you have defined; usually this will reflect the reporting structure of your organization.

Many organizations will choose to use their LDAP Organizational Unit structure as the basis for their MyID group structure. In this case, we advise that before adding users to MyID, you should use the **Edit Groups** workflow to import the LDAP structure and thus create the MyID groups automatically. You may subsequently add to and modify your MyID groups if you wish.

Warning: If you are integrating with authentication services or disk encryption solutions, you should ensure that the connections to these external components are configured BEFORE creating MyID Groups or Users. This is because MyID group information must be 'pushed' to the external system as it is created.

2.2.3 Certificate templates

If you intend to use PKI certificates, you should now verify the connection to your certification authority (CA) and decide which certificate templates you will need to be issued through MyID. This will need someone with reasonable PKI knowledge and a good understanding of the applications and functions for which certificates are to be used. See your CA integration guide for details.

For each template (sometimes referred to as a 'policy') in each CA, you must decide whether it will be made available for MyID issuance, what friendly name and description you want it to have, plus settings such as key length, duration, hardware/software issuance, and so on.

When choosing friendly names for templates, you should consider that the person who will be using these names is the individual responsible for defining credential profiles. Their perspective is likely to be from a 'Business Services' viewpoint, so where appropriate, you should name templates to indicate the service(s) they are to be used for, rather than a description of their implementation and origin. As an example, you might rename 'Client signing 1024-RSA-365 on CA1' as 'Email Signature'.

2.2.4 Card layouts

If you are using smart cards that need to be printed to display details of your organization or the card holder, you should create a card layout using the Card Layout Editor. It is usually easiest to create composite images for the backgrounds using tools such as Photoshop or Paintshop Pro, and then store these as GIF or JPEG files. Typical card printers are capable of around 600dpi printing, so your images should be at least 2000x1275 pixels to take advantage of this.

Barcodes and magnetic stripe information are also configured through the Card Layout Editor. For information on 1D and 2D barcodes, see the *Adding barcodes* section in the ***Administration Guide***.

To add magnetic stripe information, use one of the three **Magnetic Stripe** fonts. You may position the magstripe text outside the displayed area of the card; it will be ignored by the 'Fit to Content' operation in the editor.

2.2.5 GlobalPlatform keys

If you are writing applets to Java cards, or you want to change the GlobalPlatform keys for cards at issuance, you should define the Factory and Customer keys at this point.

See the See the *GlobalPlatform keys* section in the ***Administration Guide*** and the ***System Security Checklist*** for details.

2.2.6 Applets

If you need to add applets to Java smart cards, you will need to prepare and install the applets. Contact Intercede for further details of this process, quoting reference SUP-295.

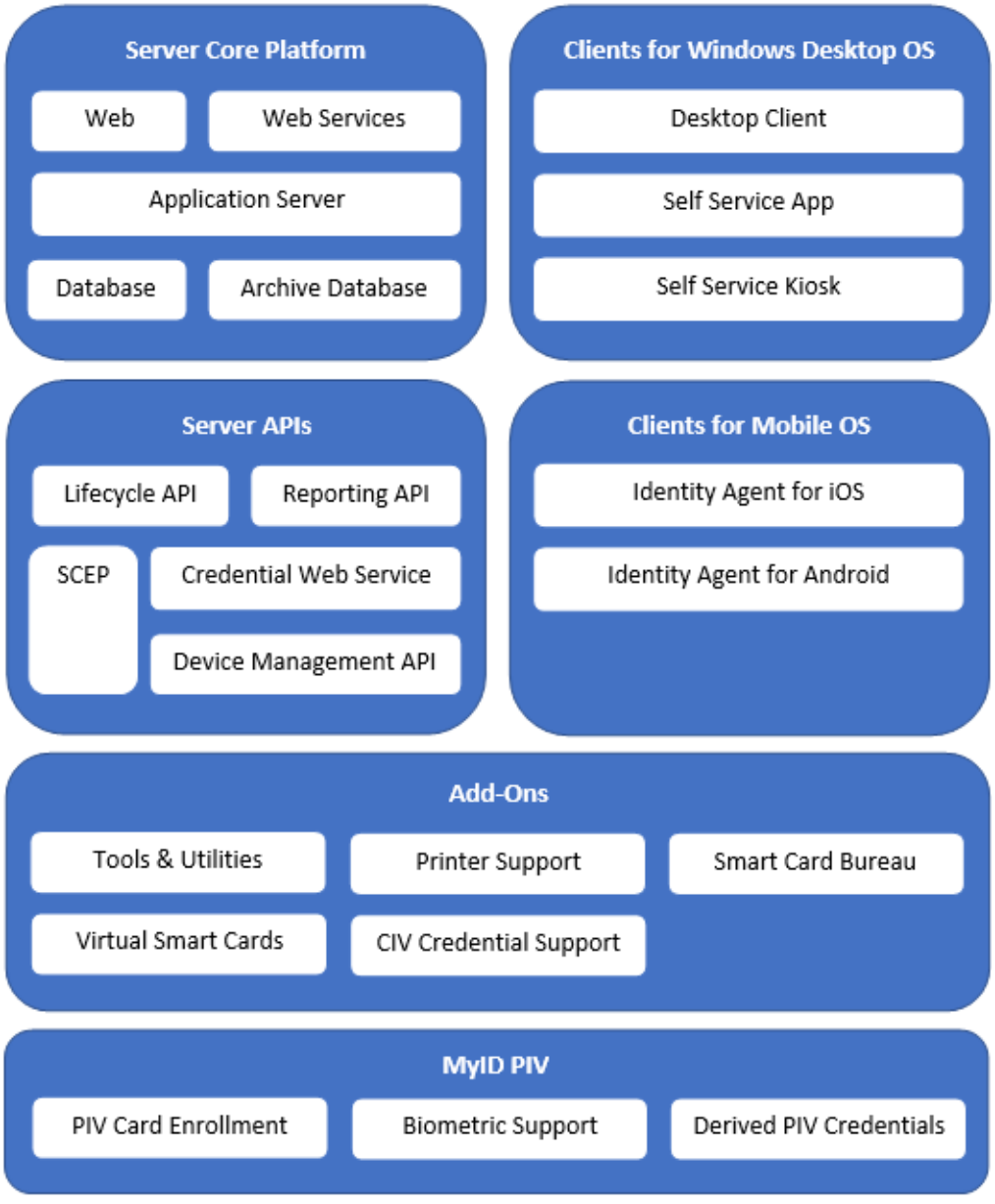
2.2.7 Licensing

MyID has a licensing mechanism that you must activate soon after installation. Without activation, MyID is restricted to a maximum of 250 user accounts for a maximum of 30 days. To request or install a license, from the **Configuration** category in MyID, select the **Licensing** workflow. The licensing process involves an email contact to customer support, so you should plan ahead to avoid delays in your implementation.

3 MyID components

The MyID Credential Management System is a highly flexible and configurable solution. This section provides an overview of the main components of MyID to help you plan your deployment and locate the necessary software.

A description of each component is provided in the subsequent sections of this document.



4 Server core platform

The Server Core Platform is the engine of MyID. The application and database servers provide the business logic, data access, and storage layers. The Web server (providing HTML based content) and Web Services server (providing client APIs) provide content to the MyID user interfaces.

4.1 Application Server

The MyID application server hosts the MyID components. These provide the business logic and access to the database servers.

See the *Additional hardware and software requirements* section in the ***Installation and Configuration Guide*** for details of requirements for this server.

4.2 Database Server

The MyID database server holds all the information about MyID; its features, configuration, user data, audit information, and so on.

See the *Setting up the database* section in the ***Installation and Configuration Guide*** for details of requirements for this server.

4.3 Archive Database Server

The MyID archive database server optionally contains an archive of audit or job information from the main MyID database, helping to keep the size of the main database down and therefore improve performance.

See the *Database configuration* section in the ***Advanced Configuration Guide*** for more information.

4.4 Web Server

The MyID web server contains web pages that are used for classic workflows with MyID Desktop.

See the *Additional hardware and software requirements* section in the ***Installation and Configuration Guide*** for details of requirements for this server.

4.5 Operator Client Web Services

The Operator Client Web Services (rest.core and web.oauth2) are used for the MyID Operator Client.

You can also use these web services to access the MyID Core API and for authentication; see the ***MyID Core API*** guide and the ***MyID Authentication Guide*** for details.

4.6 MyID Client Web Services

The MyID Client Web Services are used for the following client applications:

- MyID Desktop
- MyID Self-Service App
- MyID Self-Service Kiosk
- MyID Mobile Identity Management

See the ***Web Service Architecture*** guide for details.

4.7 Next steps

Next steps:

- Read the MyID ***Installation and Configuration Guide*** for detailed information on preparing your environment for installing or upgrading MyID.
- You can check your server is ready for installation using the System Interrogation Utility. See the ***System Interrogation Utility*** guide.
- You can connect the server core platform to Active Directory to allow import and synchronization of user information. For further information, see the *Using an LDAP directory* section in the ***Administration Guide***.
- Connectivity to a certificate authority is enabled from the server core platform. A range of certificate authorities can be supported. For more information, see the following documents:
  - ***DigiCert ONE Integration Guide***
  - ***Entrust CA Integration Guide***
  - ***Entrust CA Gateway Integration Guide***
  - ***Microsoft Windows CA Integration Guide***
  - ***PrimeKey EJBCA Integration Guide***
  - ***Symantec (Digicert) Managed PKI Integration Guide***
  - ***UniCERT Integration Guide***
- For production deployment, use of a Hardware Security Module is expected; this provides extra security for protecting secure information used by MyID. You can find information about supported HSMs and required configuration in the following documents:
  - ***Entrust nShield HSM Integration Guide***
  - ***Thales Luna HSM Integration Guide***
- In some circumstances, you may need to carry out a data preparation step before upgrading to the latest version of MyID. Scripts are located in the `\Support Tools\Upgrade\` folder. For details of the scripts, and when to use them, see the ***Installation and Configuration Guide***.

- You can install MyID onto servers hosted in Microsoft Azure and use the Microsoft SQL Azure database platform. For more details, see the ***Microsoft Azure Integration Guide***.
- You can install MyID onto servers hosted on AWS EC2 virtual machines and use an Amazon RDS for SQL Server database instance; see the ***Amazon Web Services Integration Guide***.

5 Clients for desktop operating systems

MyID clients provide a user interface for administrators and self-service users. These are provided for Windows and macOS operating systems.

Name	Operating system	Where is it?	Purpose	Additional information
MyID Desktop	Windows	`\MyID Clients\Desktop Client\`	Provides access to configuration operations, card issuance workflows, and advanced features.	The functionality available in this client is also accessible through the MyID Operator Client. The MyID Operator Client provides more comprehensive additional capabilities for person, device, and request management.
MyID Operator Client	Windows	`\MyID Clients\MCS\`	The primary user interface for MyID – provides access to all administration and management features.	The operator client web page is supported by the MyID Client Service, which is installed on the device being used. This acts as a communications layer between the web page and features that require interaction with connected devices, third-party software, or the other MyID clients.
Self Service App	Windows	`\MyID Clients\Self Service App\`	Simplified user interface for self service features; for example, credential collection, updates, and PIN management.	The Self-Service App will be superseded by the MyID Client for Mac and MyID Client for Windows.

Name	Operating system	Where is it?	Purpose	Additional information
Self Service Kiosk	Windows	`\MyID Clients\Self Service Kiosk\`	Designed to be used on shared computers – provides a kiosk-style user interface for smart card management collection, updates, and PIN resets.	
Unlock Credential Provider	Windows	`\MyID Clients\Unlock Credential Provider\`	Enables PIN reset for devices issued by MyID CMS that have a PIV Applet; for example, PIV cards and YubiKey devices. This feature is available from the Windows Logon screen.	This feature generates a challenge code for the connected device, which you can supply to a MyID operator. The operator can then generate an unlock code that you can provide to the credential provider. Once verified, you can then set a new PIN for the device.
MyID Client for Mac	macOS	`\MyID Clients\MyID Client for Mac\`	Provides self-service device collection, updates, and PIN management on macOS.	There are some differences in capabilities between the MyID Client for Mac and for Windows; this is due to operating system limitations. Refer to the installation guides for further details.

Name	Operating system	Where is it?	Purpose	Additional information
MyID Client for Windows	Windows	`\MyID Clients\MyID Client for Windows\`	Provides self-service device collection, updates, and PIN management on Windows.	There are some differences in capabilities between the MyID Client for Mac and for Windows; this is due to operating system limitations. Refer to the respective guides for further details. The MyID Client for Windows provides additional support for Microsoft VSC and Windows Hello for Business.

Next steps:

- See the *Installing MyID Desktop* section in the ***Installation and Configuration Guide*** for instructions on installing and configuring MyID Desktop.
- See the *Installing the MyID Client Service* section in the ***Installation and Configuration Guide*** for instructions on installing the MyID Client Service, which is required for the MyID Operator Client.

  See the ***MyID Operator Client*** guide for details of using the MyID Operator Client.
- See the *Installing the unlock credential provider* section in the ***Installation and Configuration Guide*** for instructions on installing and configuring the Unlock Credential Provider.
- The self-service apps have their own installation guides:
  - ***Self-Service App***
  - ***Self-Service Kiosk***
  - ***MyID Client for Mac***
  - ***MyID Client for Windows***
- Depending on the functionality required, you may require some add-ons on the client PC, such as components for:
  - Virtual Smart Cards – see section *8.18*, *Virtual Smart Cards*.
  - Printers – see section *8.14*, *Printer support*.

5.1 MSIX client installation programs

Intercede also 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.

See the ***MyID Client MSIX Installation Guide*** for details of working with these installation programs.

Name	Where is it?
MyID Client Suite	`\MyID Clients\MyID Client Suite\`
MyID Desktop	`\MyID Clients\MyID Client Suite\OptionalPackages\`
Self-Service App	`\MyID Clients\MyID Client Suite\OptionalPackages\`
MyID Client Service	`\MyID Clients\MyID Client Suite\OptionalPackages\`

6 Clients for mobile operating systems

Credentials such as digital certificates can be provided to mobile devices.

6.1 Mobile clients

Note: 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.

6.2 Mobile web services

For iOS OTA support, additional web services are required on the MyID server. You must select the **Mobile iOS OTA** option when installing MyID. For details, see the *Setting up iOS OTA provisioning* section in the ***Mobile Identity Management*** guide.

6.3 Next steps

Next steps:

- Further details about deploying mobile credentials are in the ***Mobile Identity Management*** guide.
- MyID can work with a range of Mobile Device Management and Enterprise Mobility Management systems, and may require special configuration for each.
- Software frameworks and SDKs are available to allow integration with your own mobile applications. For further details contact Intercede quoting reference SUP-294.

7 Server APIs

MyID has a range of APIs that enable other systems to integrate with MyID. This release provides a range of documentation for each API.

7.1 Credential Web Service

The Credential Web Service is an API that allows external sources to request the issuance of mobile devices and Microsoft Virtual Smart Cards (VSCs). The Credential Web Service can also be used to add and remove Additional Identities from MyID users.

To enable this API, select the **Credential Web Service** option when installing MyID.

For more information, see the ***Credential Web Service*** document.

7.2 Device Management API

The Device Management API is a mechanism that allows server-to-server management of devices from external sources within MyID. For example, this API allows an asset management system to register information about a computer or other hardware, enabling credential management for the device.

To enable this API, select the **Device Management API** option when installing MyID.

For more information, see the ***Device Management API*** guide.

7.3 Lifecycle API

The Lifecycle API provides an interface – the MyIDEnroll web service – to add, modify, or remove user records in MyID, create requests for credentials, and manage the status of issued credentials.

To enable this API, select the **Lifecycle API** option when installing MyID.

For more information, see the ***Lifecycle API*** guide.

Note: The Lifecycle API is no longer being developed, and customers are encouraged to move towards the REST API provided for the rest.core web service; see the ***MyID Core API*** guide

7.4 MyID Core API

The MyID Core API gives you access to the features used in the MyID Operator Client using a REST-based API, including:

- Adding, editing, and removing people.
- Requesting, canceling, and viewing devices.
- Approving, rejecting, and canceling device requests.

For more information, see the ***MyID Core API*** guide.

Note: You use the web.oauth2 web service for authentication to the MyID Core API; you can also use this web service for other systems. MyID provides a standalone version of this web service – web.oauth2.ext – that you can use for authentication without requiring access to the MyID application server. See the *Setting up the standalone authentication service* section in the ***MyID Authentication Guide*** for details.

7.5 Reporting Web Service API

The Reporting Web Service allows you to query details from the MyID database through a web service.

To enable this API, select the **Reporting Web Service API** option when installing MyID.

For more information, see the ***Reporting Web Service API*** document.

7.6 SCEP API

MyID supports the Simple Certificate Enrollment Protocol (SCEP) for issuing device identities. This allows you to issue device identities to devices that support SCEP; for example, you can issue a certificate to a router.

To enable this API, select the **SCEP API** option when installing MyID.

For more information, see the *Managing devices* chapter of the ***Administration Guide***.

7.7 REST API for credential provisioning

MyID provides a REST API for provisioning mobile credentials, soft certificates, and mobile identity documents (rest.provision). This API is currently used for:

- Soft certificate collection within the MyID Operator Client.
- 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.
- Mobile identity document provisioning.

For further information on mobile provisioning, see the *Setting up a signing certificate for iOS OTA* and *Setting up a custom PKCS #10 request* sections in the ***Mobile Identity Management*** guide.

For further information about soft certificates, see the *Working with soft certificates* section in the ***MyID Operator Client*** guide.

For information on setting up mobile identity documents, see the ***Mobile Identity Documents*** guide.

8 Add-ons

The add-ons listed in this section are available with the release, and on request.

8.1 Audit Verifier Tool

MyID maintains a signed audit record of events, but it can be difficult to verify that the audit records are valid and have not been tampered with.

The audit verifier tool is a simple utility that allows a customer to verify the integrity of MyID audit data.

See the readme in the utility folder for details of running the Audit Verifier Tool.

Name	Where is it?
Audit Verifier Tool	`\Support Tools\Audit Verifier Tool\`

8.2 Certificate Table User SID Utility

The Certificate Table User SID Utility allows you to extract the User SID from existing certificates and update the certificate's record in the MyID database.

See the *Using the Certificate Table User SID Utility* section in the ***Administration Guide*** for details.

Name	Where is it?
Certificate Table User SID Utility	`C:\Program Files\Intercede\MyID\Utilities\` on the MyID application server.

8.3 HSM Test Utility

The HSM Test utility carries out a series of cryptographic tests against either a Luna or nShield HSM. The results of these tests determine whether the HSM can be used with MyID. The utility generates temporary data on the HSM and deletes any objects it creates.

See the readme in the utility folder for details of running the HSM Test Utility.

Name	Where is it?
HSM Test Utility	`\Support Tools\HSM Integration\`

8.4 Key Migration Utility

The Key Migration Utility is a new utility that 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.

8.5 Password Change Tool

MyID uses Windows service accounts to provide security context between components and servers in a MyID installation. The Password Change Tool (PCT) is a support tool for automating the changing of passwords for the accounts used by MyID. You are recommended to use it if MyID is already installed and you are required to change passwords regularly by your security policy, or if a security breach has occurred.

See the ***Password Change Tool*** guide for details.

Name	Where is it?
Password Change Tool	`\Support Tools\Password Change Tool\`

8.6 Patch Removal Utility

Before upgrading MyID, in some cases, you may need to remove earlier patches from the installation. PowerShell scripts are provided to allow you to automate this step.

See the readme provided in the utility folder for details of running the PowerShell scripts.

Name	Where is it?
Patch Removal Utility	`\Support Tools\Upgrade\v10 Patch Removal\`

8.7 Server Diagnostic Report Utility

The Server Diagnostic Report (SDR) provides diagnostic information on the MyID server environment.

On a compatible server, it provides the following information:

- Intercede products installed.

  Lists the MyID server along with any installed add-ons, cumulative updates, and hotfixes.
- MyID server configuration.

  Provides a snapshot of the installation registry, the customization GUID, and non-sensitive data selected or input during installation.
- Features installed.

  Lists all MyID features, and marks each as "Local" (selected during installation) or "Absent" (not selected during installation).
- Licenses.
- Supported devices.

  Lists all devices supported in this version of MyID.
- Enabled certificate authorities.
- MyID server settings.
- Web applications.
- DLL files installed.
- COM interfaces.
- Shared reference counts.

  Indicates where installed products share files.

The Server Diagnostic Report is generated as part of the MyID Installation Assistant; see the *Server Diagnostic Report* section in the ***Installation and Configuration Guide*** for details.

You can also run the report standalone; see the readme provided in the utility folder for details of running the PowerShell script.

Name	Where is it?
Server Diagnostic Report	`\Support Tools\MyIDInstallationAssistant\SDR\`

8.8 System Interrogation Utility

The System Interrogation Utility (SIU) is a support tool for determining whether the prerequisites stated in the MyID ***Installation and Configuration Guide*** have been satisfied.

Note: Running the SIU does not eliminate the need to consult the core product documentation provided with MyID.

The SIU performs a series of automated tests on the hardware, software, and configuration of the computers of a MyID installation. You are recommended to run the utility both before and after the installation of MyID.

Important: You can run the SIU independently, but its tests are also incorporated into the MyID Installation Assistant, which runs the appropriate tests at the relevant points of the installation process. The MyID Installation Assistant provides a simpler and more user-friendly way to run the SIU tests. The ***System Interrogation Utility*** guide describes running the SIU independently; for information on running the tests as part of the MyID Installation Assistant, see the *MyID Installation Assistant* section in the ***Installation and Configuration Guide***.

Name	Where is it?
System Interrogation Utility	`\Support Tools\MyIDInstallationAssistant\SIU\`

8.9 TPM Interrogator

The TPM Interrogator is a utility that provides information about the status of a Trusted Platform Module (TPM) on a PC. Microsoft Virtual Smart Cards are stored on a TPM; for more information, see the ***Microsoft VSC Integration Guide***.

See the readme in the utility folder for details of running the TPM Interrogator.

Name	Where is it?
TPM Interrogator	`\Support Tools\TPM Utility\`

8.10 Recover Startup User

MyID provides a utility to re-create the startup user account if it does not exist; for example, you may have upgraded from an earlier version of MyID that did not use the startup user account, or removed the startup account as part of locking down the installation. You must use the GenMaster utility to set the password for this user once you have run the installation program.

Note: You need to use this utility only if you are using the legacy GenMaster utility. The updated GenMaster utility (incorporated into the MyID Installation Assistant or run as the standalone GenMasterEx utility) automatically creates the startup user if required.

See the readme in the utility folder for details of running the installer.

Name	Where is it?
Recover Startup User	`\Support Tools\Recover Startup User\`

8.11 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 readme and *Windows Logon Certificates* guide in the utility folder for details of running the Windows Logon Certificates utility.

Name	Where is it?
Windows Logon Certificates	`\Support Tools\Windows logon certificates utility\`

8.12 Authentication

MyID provides support for mobile AD FS authentication using the MyID Authenticator app and the AD FS Adapter Mobile, and FIDO AD FS authentication using the AD FS Adapter OAuth.

Both the AD FS Adapter Mobile and the AD FS Adapter OAuth are provided in the AD FS Adapter for MyID package.

For mobile authentication, the MyID Verification Service allows an external system to initiate a mobile authentication and a mobile device to return authentication data.. For details, see the *MyID Verification Service* section in the ***Mobile Authentication*** guide.

For more information on mobile authentication, see the ***Mobile Authentication*** guide.

For more information on FIDO authentication, see the ***MyID Authentication Guide***.

Name	Where is it?
MyID Authenticator for iOS	Apple App Store
MyID Authenticator for Android	Google Play store
AD FS Adapter for MyID	`\Authentication\AD FS Adapter for MyID\`

8.13 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. Contact your Intercede account manager for pricing details.

For more information, see the *MyID SecureVault* section in the ***Administration Guide***.

8.14 Printer support

MyID can work with a range of smart card printers. In some cases, you may need an additional SDK component to allow a MyID client to send commands to the printer.

For more information about supported smart card printers, see the ***Printer Integration Guide***.

Intercede provides packages containing the SDK for the following printers:

Name	Where is it?
Fargo Printer SDK	Available on request
Zebra Printer SDK	Available on request

8.15 Self-Service Request Portal

The Derived Credentials Self-Service Request Portal (SSRP) allows you to request a MyID derived credential for your smart card, USB token, smartphone, or Windows PC; this derived credential is based on a smart card that you already hold.

The SSRP is a website that does not require any additional software to be installed on the client PC. It works using Microsoft Edge and Google Chrome browsers, as well as Internet Explorer 11 in compatibility mode.

You can request derived credentials from existing credentials that were issued by the current MyID system, or from credentials that were issued by external systems.

For more information, see the ***Derived Credentials Self-Service Request Portal*** guide.

8.16 Smart card bureau

For large scale smart card deployments that include graphical personalization of the card, it is often more practical for the personalization to take place at the card vendor's manufacturing facility. This requires integration with the credential management system to transfer user information and track card delivery and data for lifecycle management of the personalized cards.

Typically, the integration requires specific configuration to match customer data requirements and data formats supported by the card vendor. If you intend to use smart card bureau integration, contact Intercede to discuss your requirements quoting reference SUP-293.

Name	Where is it?
Bureau Integration	Available on request

8.17 Translation

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.

For information about translating the MyID interface, contact customer support quoting reference SUP-138.

8.18 Virtual Smart Cards

MyID can create and manage Virtual Smart Cards (VSCs), which use device hardware capabilities to protect credentials assigned to a user.

Microsoft Virtual Smart Cards are protected by a Trusted Platform Module (TPM) in a computer. See the ***Microsoft VSC Integration Guide*** for details. A TPM Interrogator utility is also provided to allow you to check the detailed status of a TPM on a computer.

Name	Where is it?
Windows Integration Service	`\MyID Clients\Windows Integration Service\`
TPM Interrogator	`\Support Tools\TPM Utility\`