MyID PIV

Version 12.11

Entrust CA Integration Guide

ENTRUST READY

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

Document reference: INT1951-12.11.0-PIV

June 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

This document provides a step-by-step guide to the installation and configuration requirements to integrate the Entrust CA (Certification Authority) with MyID®.

Entrust certificates can be used in exactly the same way as any other certificate within MyID. Certificates can be issued to cards or the local system, by specifying them in a credential profile or though card updates and edits.

Issuance or recovery of certificates with elliptic-curve cryptography (ECC) keys is not supported for the Entrust certificate authority.

RSA keys are supported. Note, however, that only 1024 and 2048 bit RSA keys are supported; 3072 and 4096 bit keys are not currently supported with this CA.

Important: MyID cannot work with an Entrust CA if it has been configured to support ECC keys and related signing algorithms.

1.1 Supported Entrust versions

MyID has been tested with the following CA versions:

- Entrust v10
- Entrust v8.x

For Entrust v10, MyID has no specific requirements for Entrust Authority Security Manager (EASM) or Entrust Security Manager Administration (SMA) – however, you must ensure that your Entrust system is installed and operational.

Intercede is currently providing support for the Entrust Administration Toolkit for C version 8.2 (64-bit only).

Intercede is continuing to investigate support for the Entrust Authority Security Toolkit for the Java Platform version 8.1 (64-bit only). A further statement will be provided when more information is available.

For Entrust v8.x, MyID has been tested with the following combinations of Entrust EASM and Entrust Security Manager Administration:

Entrust EASM	Entrust Security Manager Administration
SM 8.1 SP1 Patch 207533	SMA 8.1 SP1 patch 204648
SM 8.2.62	SMA 8.2.62
SM 8.3.61	SMA 8.3.61

Refer to your Entrust CA documentation for recommendations of the hardware and software needed for the Entrust CA.

1.1.1 Support for Entrust v10

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 the 64-bit Entrust Authority Security Toolkit for the Java Platform version 8.1, as a replacement for the 64-bit Entrust Administration Toolkit for C version 8.2. A further statement will be provided when more information is available.

For information about some issues that you may encounter when working with Entrust v10, see section *4.4*, *Entrust v10-specific behavior*.

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

1.1.2 Upgrading from MyID 11.4 or earlier

As of version 11.5 of MyID, only 64-bit versions of Entrust are supported. For continued operation, you must follow the setup instructions in this manual and switch to the 64-bit versions of the Entrust Administration Toolkit for C and the Entrust Authority Security Toolkit.

2 Configuration

This chapter contains instructions for configuring your Entrust system, including:

- Prerequisites for the Entrust system.
- Creating the MyID server profile.
- Setting up the MyID Entrust administration link.
- Key archival and recovery.
- LDAP configuration.
- Setting up the MyID Entrust Certificate Authority.
- Editing the CA policy in MyID.
- Enabling certificate policies.
- Updating the CA details.
- Deleting a CA.
- Attribute mapping for PIV systems.
- Ports required for Entrust.
- Mandatory NACI values for certificates.
- Configuring critical section protection.
- Deactivation of card authentication users.

2.1 Prerequisites

Before using the Entrust CA to issue certificates through MyID you must install and configure the following software components on the MyID application server:

- Java

  Entrust supports Java version 11 LTS; for example, Oracle Java SE Long Term Support (LTS) versions, or AdoptOpenJDK (LTS) version Hotspot. See the Entrust documentation for details.

  Note: This document uses the following for example file paths:

  ```
  C:\Program Files\Eclipse Adoptium\jdk-11.0.14.101-hotspot
  ```

  Your Java file paths may be different if you are using a different version of the JDK or the JRE. Use the appropriate paths based on your environment.
- The Entrust Administration Toolkit for C version 8.2 (64-bit only).
- Entrust Authority Security Toolkit for the Java Platform version 8.1 (64-bit only).

You will also need the following information and files in order to configure MyID to use the Entrust CA:

- Host address of the CA.
- Host port of the CA.
- DN of the CA (issuer of certificates).

- `Entrust.ini` file.
- Entrust Security officer profile file and password.
- An encryption certificate file and password.

  This is the certificate relating to the Encryption policy that is issued in Entrust to the security officer account. You may be able to convert the security officer's EPF profile file to a P12 file if you have an appropriate tool.

  This encryption certificate is required only if you are issuing archive certificates from your Entrust CA.

2.1.1 Unlimited strength crypto policy

The Java Cryptography Extension is provided with the latest version of the JDK and JRE.

To configure the extension, you must edit the `java.security` file and make sure that the `crypto.policy` security property to `unlimited`.

Depending on the version of Java you are using, the `java.security` file is in the following folder:

```
<java-home>\lib\security
```

or:

```
<java-home>\conf\security
```

For example:

```
C:\Program Files\Eclipse Adoptium\jdk-11.0.14.101-hotspot\conf\security
```

The `java.security` file should contain:

```
crypto.policy=unlimited
```

Depending on the version of Java, the file may already contain the following:

```
#crypto.policy=unlimited
```

In this case, remove the `#` to remove the comment from the line.

2.1.2 Entrust ESSC

Entrust ESSC connector has been superseded by the Entrust Authority Security Toolkit for the Java Platform. If you are upgrading an existing MyID installation that uses the old Entrust interface, contact Intercede support for advice.

2.1.3 Before you install MyID

Before you install MyID, you must copy the following files from the Entrust Admin Toolkit:

- `etadmintk.dll`
- `enterr.dll`
- `etkcore.dll`

Copy the files to the following folder on the MyID application server:

```
Windows\System32
```

2.1.4 Java Environment

To enable the Java Interface between MyID and the Entrust server to function correctly, all the `.JAR` files must be in the same location on the MyID application server. You have two options:

- Copy all the `.JAR` files provided with the Entrust Authority Security Toolkit for the Java Platform to the directory containing the MyID Java component. If you have installed MyID in the default location, this is:

  `C:\Program Files\Intercede\MyID\components\java`

  or

- Copy the MyID Java components to the directory containing the Entrust Authority Security Toolkit for the Java Platform `.JAR` files.

  Once this has been done, open regedit and browse to the registry node:

  `HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\Connector\EntrustJTK`

  If this registry entry does not exist, you must create it.

  Change the value of `JavaLocation` (which has type `String`) to the directory containing the `.JAR` files.

  Note: The default value is the `Components\java` folder used by MyID.

- If you are using HSM-based credentials, you must also copy the following files from the Entrust Java Toolkit to the `System32` folder on the application server:
  - `jnicapi_64.dll`
  - `JNIPKCS11_64.dll`
  - `UALJNI_64.dll`

2.1.4.1 Check the Path variable

You must check that the Path environment variable on the MyID application server contains both the location of the client `jvm.dll` file and its parent folder.

Important: If you update your version of Java, you must check the Path environment variable again, and update it if necessary.

1. Log on to the MyID application server as an account with administrative rights.
2. From the Windows Control panel, select **System**.
3. Click **Advanced system settings**.
4. Click **Environment Variables**.
5. From the list of **System variables**, select **Path**.
6. Click **Edit**.
7. Check that the full path of the folder containing the client `jvm.dll` file is included in the Path variable.

   For example:

   `C:\Program Files\Eclipse Adoptium\jdk-11.0.14.101-hotspot\bin\client`

   If this folder is not present in the path, add it.

8. Check that the path of the parent folder of the folder containing the client `jvm.dll` file is included in the Path variable.

   For example:

   ```
   C:\Program Files\Eclipse Adoptium\jdk-11.0.14.101-hotspot\bin
   ```

   If this folder is not present in the path, add it.

   Note: Make sure the paths are correct. If the paths are entered incorrectly, or are missing, you may experience errors, or you may experience a loss of functionality as the failure to find the `jvm.dll` file causes a silent failure.

   You must make sure that there are no spaces after the semicolons that delimit the entries in the path variable.

   For example:

   ```
   <Paths>;C:\Program Files\Eclipse Adoptium\jdk-11.0.14.101-hotspot\bin\client;C:\Program Files\Eclipse Adoptium\jdk-11.0.14.101-hotspot\bin;<More paths>
   ```

9. Click **OK** to save any changes you have made to the path.
10. Click **OK** to close **Environment Variables**.
11. Click **OK** to close **System Properties**.
12. Restart the server.

2.1.5 Issuing Certificates to users that do not exist in the directory

If you want to issue certificates to users that do not exist in the directory, make sure you have set the `noUserInDirectory=1` setting for the certificate policies you want to issue.

If you do not set this, and attempt to issue a certificate to a user who does not exist in the directory, Entrust displays an error with the code `-2976`.

This setting can be found in the `master.certspec` file on the CA. See your CA documentation for the procedure for updating this file.

2.1.6 Certificate lifetime

Previously, when requesting a certificate from Entrust, if the lifetime associated with the original (not the new) request had expired or was less than the minimum time the CA will allow (12 hours), Entrust reported an error that the signing/encryption date was not long enough. The MyID Entrust connector now resets the insufficient date (while still remaining within the card lifetime), allowing MyID to request the new certificates.

The Entrust errors reported by this issue were `-2768` or `-2767`. These errors should now occur only in the correct situations, where you are attempting to request a certificate with a lifetime less than the minimum allowed. This situation may occur, for example, if you are requesting a certificate that is constrained to the lifetime of a card that has less than 12 hours left on its lifetime.

2.1.7 Certificate revocation list

The MyID application server must be able to communicate with the Certificate Revocation List (CRL) location. The CRL is checked for validity whenever MyID connects to the CA.

2.1.8 Multiple Entrust digital identities with a single Luna SA HSM

It is possible for a toolkit application to support multiple Entrust digital identities concurrently with a single Luna SA HSM.

For more information, see the Entrust note reference TN7074.

One example could be two servers, Server1 and Server2 that require separate identities on the same Luna SA. In this case two partitions could be created on the Luna SA: PartitionA and PartitionB. PartitionA would then be assigned to Server1 and PartitionB would be assigned to Server2. When Server1 contacts the Luna SA through PKCS #11, PartitionA will be exposed as a single slot visible on the Luna SA. Similarly Server2 will see one slot, as PartitionB will be exposed to it. Each server based application can then create and log in to separate identities hosted on different partitions on the Luna SA.

In the case of multiple partitions assigned to a single client, for example if Server1 has both PartitionA and PartitionB assigned to it:

The clients will see multiple slots. The ckdemo tool can be used to verify how many slots are exposed.

The Java based clients would just pick the desired slot and attempt to log in to the identity on that particular slot.

The Administration Toolkit for C would take the profile name that is specified and cycle through the slots until it finds the correct identity. The profile name (`.tkn` entry) should be the concatenation of the "Entrust Path" and "Entrust User" data blobs from the LunaSA with "`.tkn`" appended. A Windows based example could be something like "`d:\\test\\admintk\\luna_officer_wf.tkn`".

2.1.9 Certificate content

In some circumstances, it is possible that, for a given user, the contents of certificates will be controlled by the Entrust policy; attributes may appear in certificates that you are not expecting. To prevent this, make sure that any unwanted extensions are explicitly blocked in the certificate policy configuration on the CA; use the SMA UI or another Entrust tool to enforce the Subject Alternative Name content.

2.1.10 Entrust user DN ordering

Entrust user DN ordering and MyID DN ordering should where possible be aligned through the use of the **Reverse DN** setting for each Entrust certificate policy in the CA workflow. A typical user's ordering reflects the CA's own DN ordering.

For example, for a CA whose DN is in the form:

```
ou=MyEntrustCA,ou=PKI,ou=CA,dc=mydomain,dc=local
```

Users (known to the CA) would be in the form:

```
cn=Arthur Alpha,ou=MyEntrustCA,ou=PKI,ou=CA,dc=mydomain,dc=local
```

However, for PIV issuance, where the form is:

```
dc=local, dc=mydomain, ou=CA, ou=PKI, ou=MyEntrustCA, cn=Arthur Alpha
```

Or in the alternative `noUserInDirectory` case:

```
C=US, o=U.S. Government, ou=Department of Administration, cn=Arthur Alpha
```

That means setting the **Reverse DN** flag to true.

Note: MyID does not recognize this option when using the **Issue Card** workflow to issue a card.

2.2 Create the MyID server profile

MyID requires a Security Officer level profile for administration of the Entrust system.

1. Within Entrust/RA, create a security officer and create a profile.
2. Right-click on the DN of the security officer and select **Add to Entrust** from the menu displayed.
3. The **User Properties** dialog box is displayed.
   a. On the **General** page check that:
      - **User role** is set to `Security Officer`
      - The **All groups** checkbox is selected
   b. Click **OK**
4. The **Create profile** dialog box is displayed.
   a. Enter a **Name** and a **Location** for the profile.
   b. Click **OK**.

2.3 Set up the MyID Entrust administration link

1. Check that the `etadmintk.dll` file is in the `System32` directory on the MyID application server.

   This file is supplied by Entrust as part of the Entrust Toolkit, or may be available separately from Entrust.
2. Copy the `entrust.ini` file from your Entrust server to the MyID application server. This file will need to be configured for the type of smart card you are using.

   The file must also be configured for the HSM you are using, if appropriate. For example, for a Luna HSM, you must add the following to the `[Entrust Settings]` section:

   ```
   CryptokiV2LibraryNT=c:\Program Files\SafeNet\LunaClient\cryptoki.dll
   ```

   See your Entrust documentation for further information.

   Note: You must make sure that the FIPS value in the `entrust.ini` file is set to `0`. Failure to do this will usually result in an Entrust `error = -162` being reported when you try to test the connection.

   You must make sure the copy of the `entrust.ini` file on the MyID application server reflects your existing Entrust configuration. If the file changes on the Entrust server, you must copy it to the MyID server.
3. Copy the `.epf` or `.apf` file for the profile you created in section *2.2, Create the MyID server profile*, to the MyID application server.

   Note: You must set write permissions for the MyID COM+ user for the profile file and its location, because it must be possible for Entrust to open this file with read/write access. Entrust profiles are managed by the CA and when a key or certificate expires, they are automatically updated. Errors will be encountered if this file is set to read only; for example, `-01055`.

2.4 Key archival and recovery

MyID can archive keys on the Entrust server or locally within MyID – within the Certificate Authorities workflow, you can set the **Archive Keys** drop-down list to **None**, **Internal**, or **Entrust**.

Within Entrust, the client generation value may be true, false, or missing – you are advised not to leave the value as missing, but to set the value to true if you want to archive the keys within MyID, and false if you want to archive the keys within Entrust.

Note: If you recover a revoked archive certificate, and the certificate is configured in the credential profile for **Historic Only**, a new archive certificate is created on the CA; this is expected Entrust behavior, and MyID correctly ignores this certificate and recovers the old revoked archive certificate. This does not happen if the certificate is live, or if the certificate is configured in the credential profile to **Use existing**.

2.5 LDAP configuration

You must use the **Directory Management** workflow to configure a directory entry for the LDAP directory connected to the Entrust CA. Do not use anonymous access; you must provide the user DN and password for the directory.

Note: MyID is configured for Active Directory by default; see section *3.2*, *Microsoft Active Directory*. If you want to use a different directory, or if MyID is using a different directory to the directory that Entrust is using, contact customer support, quoting reference SUP-195.

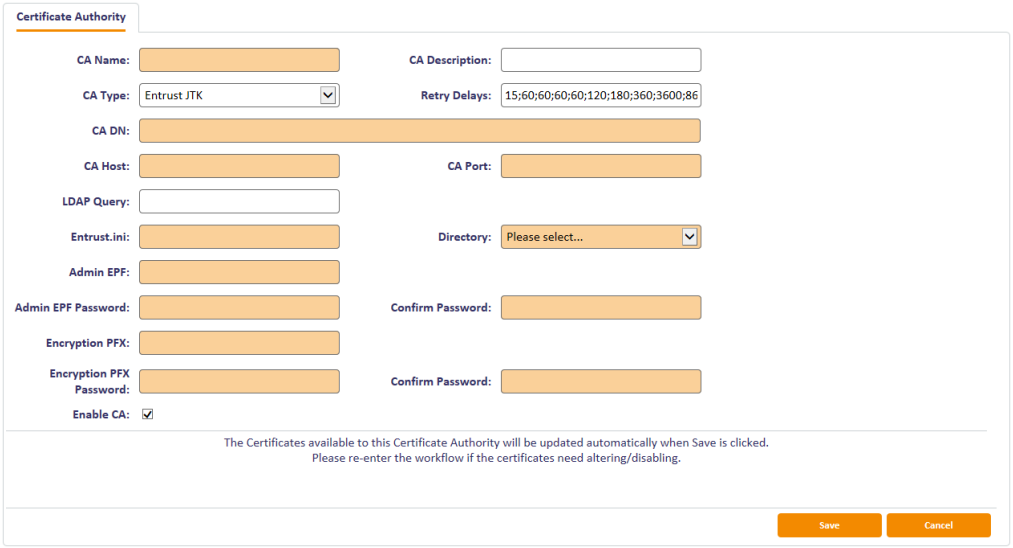
2.6 Set up the MyID Entrust Certificate Authority

Note: If you want to set up more than one Entrust CA within MyID, you may experience problems. For more information, contact customer support, quoting reference SUP-171.

To edit a Certificate Authority (CA):

1. From the **Configuration** category, select **Certificate Authorities**.
2. The **Certificate Authorities** workflow is displayed, with the **Select a CA** stage highlighted.
   - If an Entrust CA already exists, select it from the list and click **Edit**.
   - If an Entrust CA does not already exist, click **New**.

3. From the **CA Type** drop-down list, select **Entrust JTK**.



Note: All of the fields with a colored background in the example are mandatory.

4. Set the following fields:

- **CA Name** – Enter the name that you will use to identify the CA.
- **CA Description** – Enter a description for the CA.
- **CA Type** – Select **Entrust JTK**.
- **Retry Delays** – A semi-colon separated list of elapsed times, in seconds.

  For example, `5;10;20` means:

  - If the first attempt to retrieve details from the CA fails, a second attempt will be made after a `5` second delay.
  - If this second attempt fails, the CA will be contacted again after `10` seconds.
  - Subsequent attempts will be made to retrieve information every `20` seconds, until a response is received.

  If you want to limit the number of retry attempts, enter `0` as the last number in the sequence.
- **CA DN** – Enter the DN (distinguished name) of the CA.

  You can obtain this value from the `CA Distinguished Name` item in the `[Entrust Settings]` section of the `entrust.ini` file.
- **CA Host** – Enter the DNS name or IP address of the Entrust ESAM server.
- **CA Port** – Enter the IP Port of the Entrust ESAM server. The default port number is `829`.

  You can confirm the port number from the `CMPListen` item in the `[Comms]` section of the `entmgr.ini` file.
- **LDAP Query** – Enter the query that MyID uses to find the Entrust LDAP entity.

  See section *3.1*, *Setting the LDAP query string* for details.
- **Entrust.ini** – Enter the fully qualified path to the `entrust.ini` file.

Important: Do not use Windows-style back slashes (\) in the path. Use UNIX-style forward slashes (/).

- **Directory** – Select the LDAP directory being used from the list available.
- **Admin EPF** – See section *2.6.1*, *Admin EPF* for details.

  Important: Do not use Windows-style back slashes (\) in the path. Use UNIX-style forward slashes (/).
- **Admin EPF Password** – Enter the password for the Admin EPF file.
- **Encryption PFX** – Enter the fully qualified path to the encryption certificate file. This can be a PFX or P12 file.

  important: Do not use Windows-style back slashes (\) in the path. Use UNIX-style forward slashes (/).

  Note: This encryption certificate is required only if you are going to be issuing archive certificates from your Entrust CA. If you do not want to issue archive certificates, type a dummy value in this field and in the **Encryption PFX Password** field. The **Encryption PFX** field format is validated, so the dummy value must be in the correct format for a file path, but the file does not need to exist.
- **Encryption PFX Password** – Enter the password used in conjunction with the encryption certificate file.

  The password is the same as the password associated with the EPF profile file that you used to generate the certificate file.
- Select **Enable CA** to make the policies available for issue.

5. Click **Save** to save these setting to the database. MyID is now ready to issue certificates.

2.6.1 Admin EPF

The **Admin EPF** can either be the full file path to the epf file created in section *2.2*, *Create the MyID server profile*, or a compound value representing the P11 library for your HSM, the slot serial number where the hardware based credential was created, and the name of that profile.

Depending on what tools were used to create the hardware based credential, one or more files will have been created. You must copy those files to the MyID application server to a location with the same path as they were original generated.

Note: Contact Entrust for guidance on the appropriate tools for creating the hardware based credential; currently, Entrust suggest the PCU administration services utility.

An epf file can be copied anywhere – when it is a hardware based credential the copies of the files on the application server must match the location on the CA where they were created.

For example:

A hardware based credential was created into `c:\authdata\manager\epf` for a user HSM Officer. The profile for 'HSM Officer' was created (without a space) as HSMOfficer.

The files created, which will include one of more of `.apf/.arl/.cch/.crl/.pch/.xcc` must be copied to:

`C:\authdata\manager\epf`

on the MyID application server.

Within MyID, assuming your P11 DLL from your provider is `cryptoki.dll`, the Admin EPF value recorded in MyID would be:

```
<path to p11 dll>/SerialNumber|<ProfileName>.tkn
```

Note: There is no actual .tkn file at the location – the .tkn suffix is used to specify the name of the profile, not a filename.

Important: Do not use Windows-style back slashes (\) in the path. Use UNIX-style forward slashes (/).

```
C:/Windows/System32/cryptoki.dll/123456789|HSMOfficer.tkn
```

Or if it is on the system path:

```
cryptoki.dll/123456789|HSMOfficer.tkn
```

Or if at the point of installation:

```
C:/Program Files/SafeNet/LunaClient/cryptoki.dll/123456789|HSMOfficer.tkn
```

2.7 Editing the CA policy in MyID

If you add a new CA or add a new policy to a CA, and want to enable the mapping of extended attributes, you must run the following stored procedure on the MyID database before you can edit the policy in MyID:

```
sp_setEntrustCertExtensions
```

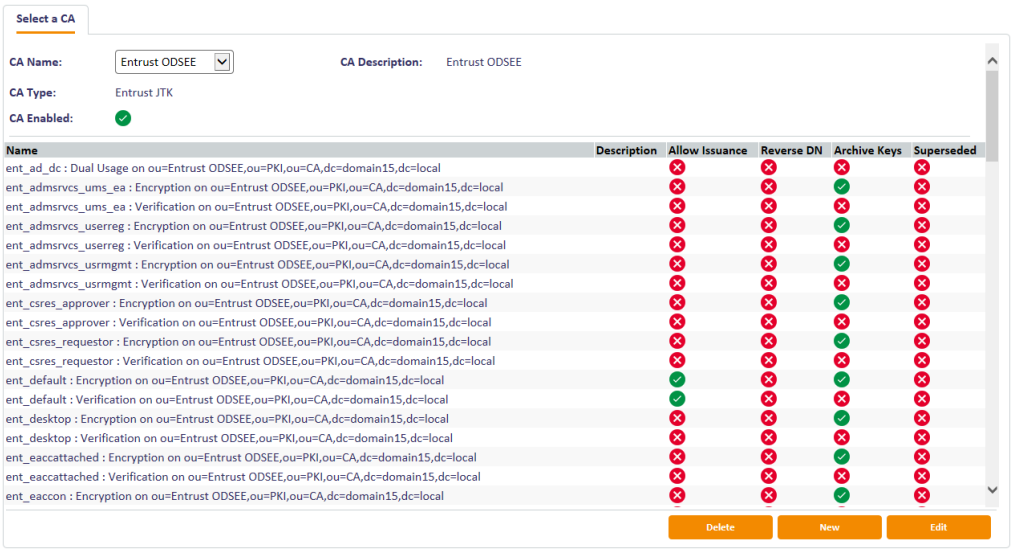
Note: This is mandatory when setting up certificate policies on PIV systems – PIV requires the use of attribute mapping – but you can also use attribute mapping on non-PIV systems.

2.8 Enabling certificate policies

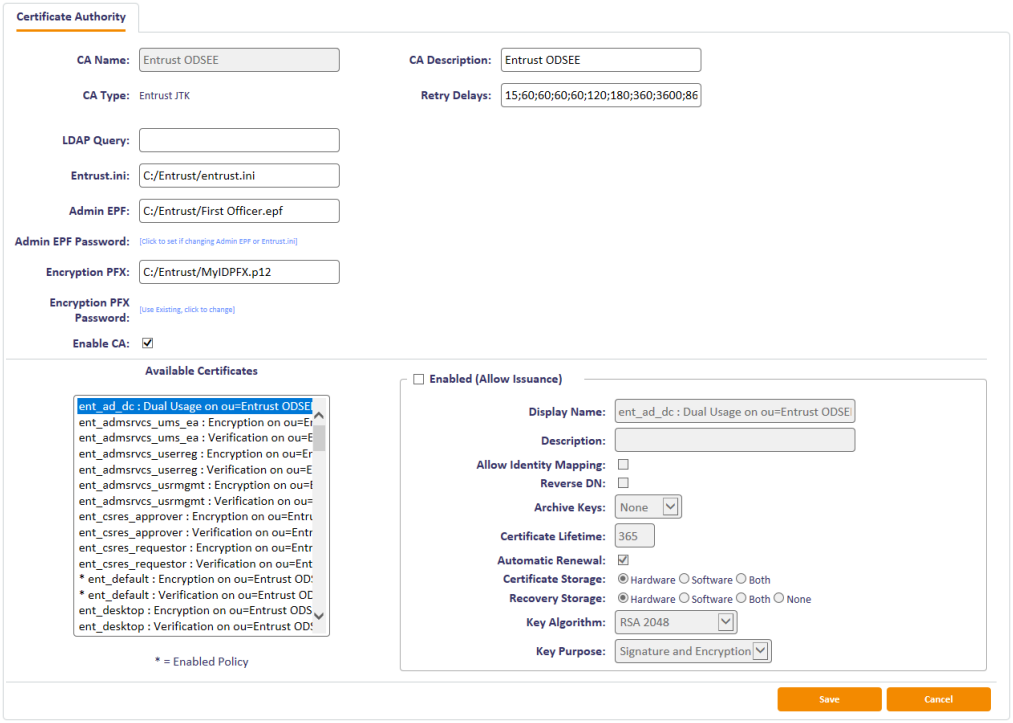
Note: You are recommended to set up your Entrust certificate policies to have a single key size and type.

Although all certificate policies are detected when you add the CA to MyID, they are all initially disabled. To enable them:

1. From the **Configuration** category, select **Certificate Authorities**.
2. From the **CA Name** drop-down list, select the certificate authority you want to work with.



3. Click **Edit**.



4. Make sure **Enable CA** is selected.
5. select a certificate template you want to enable for issuance within MyID in the **Available Certificates** list.
6. Click the **Enabled (Allow Issuance)** checkbox.
7. Set the options for the policy:
   - **Display Name** – the name used to refer to the policy.
   - **Description** – a description of the policy.
   - **Allow Identity Mapping** – used for additional identities. See the *Additional identities* section in the ***Administration Guide*** for details.
   - **Reverse DN** – select this option if the certificate requires the Distinguished Name to be reversed.

     Note: MyID does not recognize this option when using the **Issue Card** workflow to issue a card.
   - **Archive Keys** – select whether the keys should be archived.
   - **Certificate Lifetime** – the life in days of the certificate. You can request a certificate from one day up to the maximum imposed by the CA. For example, type `365` to request one-year certificates.

     Note: The default certificate lifetime value in MyID is 365 days. The default in Entrust is 36 months; if you want to configure MyID to match the Entrust default, enter 1095 days.

- **Automatic Renewal** – select this option if the certificate is automatically renewed when it expires.
- **Certificate Storage** – select one of the following:
  - **Hardware** – the certificate can be issued to cards.
  - **Software** – the certificate can be issued as a soft certificate.
  - **Both** – the certificate can be issued either to a card to as a soft certificate.
- **Recovery Storage** – select one of the following:
  - **Hardware** – the certificate can be recovered to cards.
  - **Software** – the certificate can be recovered as a soft certificate.
  - **Both** – the certificate can be recovered either to cards or to a soft certificate.
  - **None** – allows you to prevent a certificate from being issued as a historic certificate, even if the **Archive Keys** option is set. If the **Certificate Storage** option is set to **Both**, the certificate can be issued to multiple credentials as a shared live certificate, but cannot be recovered as a historic certificate.
- Additional options for storage:

  If you select **Software** or **Both** for the **Certificate Storage**, or **Software**, **Both**, or **None** for the **Recovery Storage**, set the following options:

  - **CSP Name** – select the name of the cryptographic service provider for the certificate. This option affects software certificates issued or recovered to local store for Windows PCs.

    The CSP you select determines what type of certificate templates you can use. For example, if you want to use a 2048-bit key algorithm, you cannot select the Microsoft Base Cryptographic Provider; you must select the Microsoft Enhanced Cryptographic Provider. See your Microsoft documentation for details.
  - **Requires Validation** – select this option if the certificate requires validation.
  - **Private Key Exportable** – when a software certificate is issued to local store, create the private key as exportable. This allows the user to export the private key as a PFX at any point after issuance.

    It is recommended that private keys are set as non-exportable for maximum security.

    Note: This setting affects only private keys for software certificates – private keys for smart cards are never exportable.

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

      Changes were introduced to the method MyID uses to generate software certificates in MyID 12.7.

      When MyID issues software certificates, it encrypts the passwords protecting the PFX files using AES256/SHA2.

This is a modern security standard, but it creates a problem when importing the certificates on devices that do not support this security standard; 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 are affected by this issue, contact Intercede customer support for further assistance, quoting reference IKB-392.

- **User Protected** – allows a user to set a password to protect the certificate when they issue or recover it to their local store.

  This means that whenever they want to make use of the soft certificate, they will be prompted for a password before they are allowed to use it. This is a CSP feature that is enabled when you set this option, and affects only software certificates that are issued or recovered to local store for Windows PCs.

- **Key Algorithm** – select the type and length of the key-pairs used for certificate generation. A longer key length is more secure but certain manufacturers' CSPs do not support longer lengths. Select the appropriate key length from the list. This must match the key type and length set up in your CA.

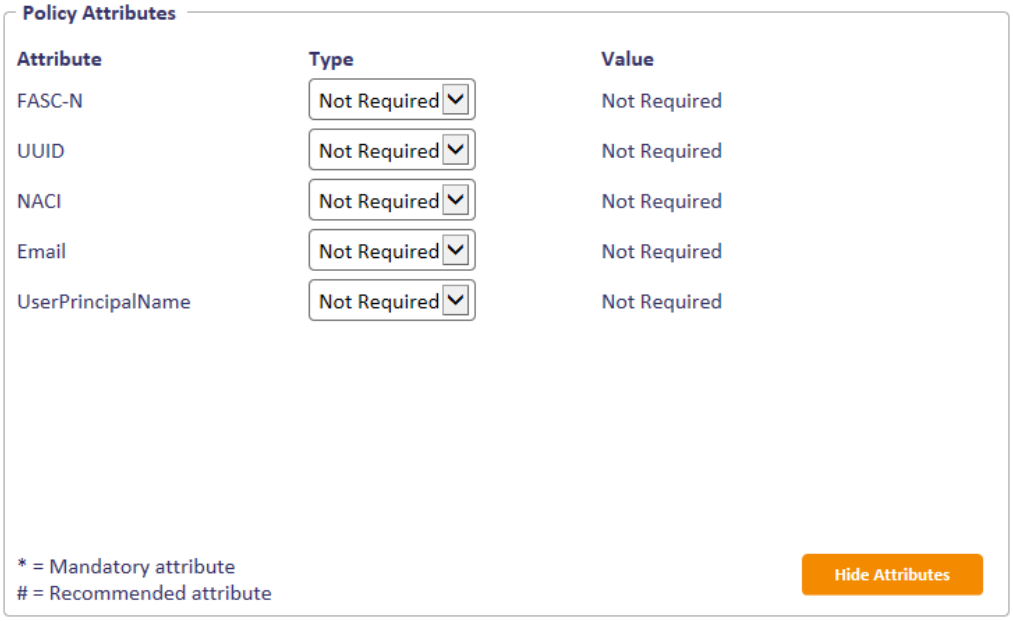
  Select an RSA 2048 type. Other types, including ECC, are not supported with Entrust CA in this version of MyID.

- **Key Purpose** – select one of the following:

  - **Signature** – the key can be used for signing only.
  - **Signature and Encryption** – the key can be used for either signing or encryption.

  Note: The **Key Purpose** option has an effect only where the device being issued supports the feature. PIV cards do not support this feature, while smart cards issued with minidrivers and software certificates issued to local store for Windows PCs do support this feature.

8. If you need to edit the policy attributes, click **Edit Attributes**.



   a. For each attribute, select one of the following options from the **Type** list:
      - **Not Required** – the attribute is not needed.
      - **Dynamic** – select a mapping from the **Value** list to match to this attribute.
      - **Static** – type a value in the **Value** box.
   b. Click **Hide Attributes**.

   For information on mapping attributes for PIV systems, see section *2.11*, *Attribute mapping for PIV systems*.

   Note: MyID may not override the settings of the CA. You need to obtain the correct settings from the administrator of your CA.

9. Click **Save**.

Note: Changes made to certificate profiles do not take effect immediately, as the normal interval for MyID to poll for updates is 50 minutes. To force MyID to poll for changes immediately, you must manually restart the **eKeyServer** service, then restart the **eCertificate** service.

2.8.1 Controlling certificate lifetimes

For PIV compliance and the desire to enable finer control over the issuance of certificates, MyID provides a certificate-based operation setting to constrain certificate lifetimes to the lifetime of the credential. That setting means certificate requests potentially, and by default are, restricted to lifetimes with their associated credential.

You can configure MyID to use the CA default lifetimes instead; typically, this is 36 months. MyID stores a representative value in the `EnProfileTemplates` table in the MyID database; however, individual CA instances may vary. When you enable this option, MyID is given whatever that particular instance is using for its 'user default key update policy'.

To set up MyID to use the CA default lifetimes:

1. From the **Configuration** category, select **Operation Settings**.
2. Click the **Certificates** tab.
3. Set the following option:
   - **Use Entrust default key update policy**

     Set this value to `Yes` to use the CA's default lifetimes.

     Set this value to `No` to constrain certificate lifetimes to the lifetime of the credential.
4. Click **Save changes**.

Entrust maintains a single value for all users however on a user by user basis, and therefore their certificate requests can have a specific or the default policy in place.

2.8.1.1 Effect on escrowed encryption certificates of allowing the CA to control lifetimes

If you have set the **Use Entrust default key update policy** option to `Yes`, and the CA is in control of certificate lifetimes, the behavior of Entrust when issuing encryption certificates is different. When MyID controls the lifetimes, when you issue an encryption certificate, Entrust always issues a new certificate. However, when Entrust controls the lifetimes, it issues a new encryption certificate only if there is not an existing escrowed encryption certificate; if there is an existing escrowed active encryption certificate, Entrust issues a copy instead.

Note, however, that if the existing certificate is expiring, Entrust issues a new certificate rather than recovering a copy.

2.8.2 Forcing the issuance of new escrow certificates

To force Entrust to issue new escrow certificates:

1. From the **Configuration** category, select **Operation Settings**.
2. Click the **Certificates** tab.
3. Set the following option:
   - **Entrust force new escrow**

     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.

     The default is `No`.
4. Click **Save changes**.

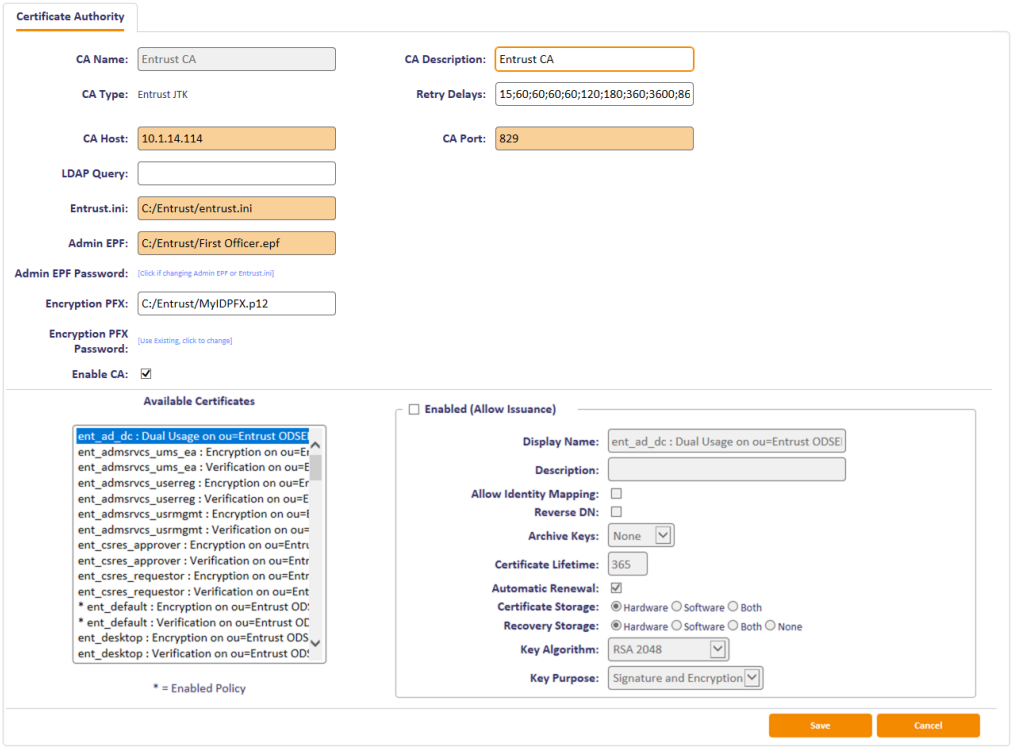
Note: Setting this option returns MyID to its previous behavior; you are recommended to keep this option at the default `No` for most systems, and set this option to `Yes` only if directed to by Intercede.

2.9 Updating CA details

You can edit the values for the **Entrust.ini**, the **Admin EPF**, and the **Encryption PFX**.

1. From the **Configuration** category, select **Certificate Authorities**.
2. From the **CA Name** drop-down list, select the certificate authority you want to work with.

3. Click **Edit**.



4. Make sure **Enable CA** is selected.
5. You can edit the following:
   - **CA Host** – Enter the DNS name or IP address of the Entrust ESAM server.
   - **CA Port** – Enter the IP Port of the Entrust ESAM server. The default port number is `829`.

     You can confirm the port number from the `CMPListen` item in the `[Comms]` section of the `entmgr.ini` file.
   - **LDAP Query** – Enter the query that MyID uses to find the Entrust LDAP entity.

     See section *3.1*, *Setting the LDAP query string* for details.
   - **Entrust.ini** – Enter the fully qualified path to the `entrust.ini` file.
   - **Admin EPF** – See section *2.6.1*, *Admin EPF* for details.

     Note: If you change the **LDAP Query**, **Entrust.ini**, or **Admin EPF**, you must re-enter the **Admin EPF Password**. Click the link to display the password fields.
   - **Encryption PFX** – Enter the fully qualified path to the signing PFX file.

     Note: If the **Encryption PFX Password** has not changed, you do not need to re-enter it. If the password has changed, click the link to display the password fields.
6. Click **Save**.

2.10 Deleting a CA

You can delete a CA from the list of available CAs if you no longer need to be able to work with it, or if you created it in error.

See the *Deleting a CA* section in the ***Administration Guide*** for details.

2.11 Attribute mapping for PIV systems

For PIV systems, you must set up the attributes of the PIV certificate policies to have specific dynamic mappings.

Note: The FASC-N mapping is required for standard PIV cards, but is not permitted for PIV-I cards. The PIV Card Authentication certificate policy *must not* contain a mapping for Email.

2.11.1 Example attribute mapping for PIV systems

Certificate Policy	FASC-N	UUID	NACI	User Principal Name	Email
PIV Authentication	FASC-N (Hex)	UUID (ASCII)	NACI Status	User Principal Name	Not Required
PIV Card Authentication	FASC-N (Hex)	UUID (ASCII)	NACI Status	Not Required	Not Required
PIV Encryption	Not Required	Not Required	Not Required	Not Required	Email (optional)
PIV Signing	Not Required	Not Required	Not Required	Not Required	Email (optional)

2.11.2 Example attribute mapping for PIV-I systems

Certificate Policy	FASC-N	UUID	NACI	User Principal Name	Email
PIV Authentication	Not Required	UUID (ASCII)	Not Required	User Principal Name	Not Required
PIV Card Authentication	Not Required	UUID (ASCII)	Not Required	Not Required	Not Required
PIV Encryption	Not Required	Not Required	Not Required	Not Required	Email (optional)
PIV Signing	Not Required	Not Required	Not Required	Not Required	Email (optional)

2.11.3 Editing the attribute mappings

To edit the attribute mapping:

1. Within the **Certificate Authorities** workflow, select an enabled certificate policy.
2. Click **Edit Attributes**.

3. For each attribute, select one of the following options from the **Type** list:
   - **Not Required** – the attribute is not needed.
   - **Dynamic** – select a mapping from the **Value** list to match to this attribute.
   - **Static** – type a value in the **Value** box.
4. Click **Save**.

2.12 Ports required for Entrust

You must configure your firewall so that the ports specified in the `entrust.ini` file are open between the client and the CA or LDAP.

The `entrust.ini` file refers to the following ports:

Entrust.ini reference	Port	Needed by the client?
Authority	829	Yes
Manager	709	No
Server	389†	Yes
ASHServer	710	Yes
XAP	443	No

†Where the LDAP port is variable between installations, 1389 and 389 are used locally depending on LDAP used – ODSEE or ADS.

2.13 Certificates with mandatory NACI values

On PIV systems, you can configure your certificate policies to make the NACI value mandatory (the `piv_interim` attribute, known as `interim_indicator` in Entrust). This is typically required for the PIV Authentication and PIV Card Authentication certificates. When MyID adds the user to Entrust, it includes the user's NACI value.

Note: This is relevant for PIV systems only. Users in MyID Enterprise systems do not have NACI values.

MyID makes sure to provide the user's captured NACI/`interim_indicator` value when it adds the user to Entrust.

Previously, you were recommended to use an optional setting, which means that while MyID would still encode the value for certificate submission, it did not need to provide it at the point of adding the user; typically the Card Authentication DN where MyID creates a new user for each issuance.

MyID now provides the captured value both as part of the user addition and the submission, whether its TRUE for incomplete or FALSE for NACI complete at both steps.

For most deployments that use the existing recommended optional `interim_indicator` value, this change makes no difference. For sites that want to use the now-deprecated NACI value in Card Authentication certificates, you can now use a mandatory `interim_indicator`.

If the MyID administrator does not configure a user attribute for use in NACI submissions, the certificate issuance will still fail and report error -8120; the change here is merely to provide it earlier in the Entrust user creation sequence, not create a value where none is present.

Note: If the CA being used has optional NACI configured, for a user without a NACI set and depending on the order that the certificates are issued, you may see the Card Authentication or PIV Authentication certificate be successfully issued before the issuance process fails and the certificates are then subsequently revoked.

2.14 Configuring critical section protection

The critical section protection for the Entrust Admin library ensures that only one process thread can use the library at a time.

This has been added because 'Remote Procedure call failed' errors have been seen when the library is used concurrently; however, if you want to disable this protection, you can do so by creating a DWORD registry value named `CriticalSections` in:

`HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\Connector\EntrustJTK`

and setting it to `0`.

If this is non-zero, or the registry value is not present, critical section protection is applied.

2.15 Deactivation of card authentication users

PIV Card Authentication certificates are usually issued to a different subject DN than other certificates, which is formed from the card FASC-N or GUID. As a result, the Entrust PKI creates an additional user account for this subject. The MyID Entrust PKI connector deactivates this additional account when card authentication certificates are revoked.

The account is deactivated if:

- The certificate being revoked was issued to the PIV Card Authentication container (5FC101).
- The certificate was issued to a subject that is not the user's main Distinguished Name – the value is normalized to take whitespace into account.

If you want to disable this functionality, you can do so by creating a DWORD registry value named `DeactivateCardAuthUser` in:

`HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\Connector\EntrustJTK`

and setting it to `0`.

If this is non-zero or the registry value is not present, then users are not deactivated.

To handle card reprovision events, if MyID attempts to issue a new certificate to an Entrust user who is deactivated, the user is reactivated.

3 Using directory services

The Entrust CA stores certificate policy information in the directory as an attribute of the CA entry. MyID has to be able to read this information to get the policy information and certificates that are available for issuance by MyID.

As the Entrust CA stores this information as an attribute of the CA object in the directory, MyID searches for the LDAP entity given the DN of the CA and the `objectClass` of `entrustCA`.

3.1 Setting the LDAP query string

In some installations it may be found that the LDAP directory server being used will not support the default query:

```
(objectClass=entrustCA)
```

For example, it may be `CA` or something similar; for Active Directory, the query should be:

```
(objectclass=certificationAuthority)
```

See your *Security Manager Directory Configuration Guide* (provided by Entrust) for details.

To allow for this, you can specify the query in the **LDAP Query** field of the **Certificate Authorities** workflow when you set up the CA in MyID.

3.2 Microsoft Active Directory

For a successful installation of the MyID system and the Entrust CA and Microsoft Active Directory Server there are some special requirements.

- The connection to the directory must be authenticated. When configuring the Directory connection within MyID, be sure to specify a username and password and the host and port information for the server. You cannot use an anonymous connection.
- The user specified for the directory configuration must be a member of the Entrust Security Administrators group on the Active Directory Server. You will need to have an administrator of the directory server do this.
- The LDAP root DN needs to be set as in the following format:

```
cn=AIA,cn=Public Key Services,cn=Services,cn=Configuration
```

followed by your particular domain information.

For example:

```
cn=AIA,cn=Public Key
Services,cn=Services,cn=Configuration,dc=mydomain,dc=co,dc=uk
```

3.3 Tracking Entrust DN changes

MyID can maintain a single Entrust entity/user after their (distinguished) name changes; for example, due to changes to marital status.

To trigger a change of DN, use the PIV applicant editing screens in the MyID Operator Client, click the **Position** tab, and edit the **PIV DN** field. Equally an update will result from a change to **First Name**, **Last Name**, **Employee ID** or the person's group's **Base DN**.

To complete a change of DN, the person must have at least one new certificate issued.

If a person changes DN multiple times without an new certificate actually being issued, only that last change will be reflected at the CA; for example, a person who changes from `Arthur Alpha` to `Arthur Beta` to `Arthur Gamma` is reflected at the Certificate Authority as `Arthur Alpha` becoming `Arthur Gamma`.

If a person changes DN multiple times and a new certificate has been issued, each change is reflected at the CA; for example, a person who changes from `Arthur Alpha` to `Arthur Beta` to `Arthur Gamma` is reflected at the Certificate Authority as individual approved DN changes.

Entrust refuses to process a change DN request in some circumstances because the user is not in appropriate state or only has revoked certificates. It does return specific errors in those cases but MyID cannot independently correct the situation.

If for any reason MyID is unable to complete a change of DN successfully, it continues to attempt to apply the change (unless undone) in future certificate requests.

Entrust refuses to allow a change of DN for a user if that user DN has ever existed in the lifetime of the Certificate Authority, even if that user has since been archived or removed. In such cases, you must use the Entrust Security Manager Administrator utility (other Entrust tools may be available) and change the 'Allow DN reuse' setting; the default is off/deselected.

Entrust allows a change of DN only if the user is using default key expiration settings; as such, as part of the processing, MyID reverts to defaults during the user change DN. However, as soon as a certificate is issued after the change of DN, the MyID configured settings are applied – they default to MyID being in control of lifetimes.

The DN change logic can track only one DN; this DN is the main DN that is used for certificate requests; for example, `Xu55`. If you need your DN to be in a particular order, make sure that your DN construction trigger and group Base DN values follow the pattern expected, and do not set `ReverseDN` against the policies.

Note: The **Track Entrust distinguished name changes** option on the **LDAP** tab of the **Operation Settings** workflow does not affect this functionality; this option was added for MyID Enterprise systems, not PIV systems.

3.3.1 Known issues

- **IKB-246 – Additional identities will not work when tracking Entrust DN changes**

  If you use MyID to issue additional identity certificates to a user, and have configured MyID to track Entrust DN changes, the additional identity certificates held in Entrust will not be affected when you update the DN. This is because the DN associated to the certificate is different to the primary DN of the user account in MyID.

- **IKB-352 – Change DN is sensitive to whitespace between DN elements**

  The Entrust Change DN feature may not identify the user to be updated in the Entrust certificate authority in some circumstances, leading to a new Entrust user account being created at next certificate issuance.

  This problem has been seen when the new Distinguished Name does not have spaces after the comma separators; for example:

  ```
  <DN>CN=Sam Jones,OU=Administrators,DC=mycorp,DC=local</DN>
  ```

  ```
  <AlternateDN>CN=Sam
  Jones,OU=Administrators,DC=mycorp,DC=local</AlternateDN>
  ```

  To work around this issue, ensure that PIV DN values imported to MyID, typed in, or created by customizations applied to MyID include spaces after the comma separators.

3.4 DN order

Entrust controls the order of the elements of the DN. Your Entrust system may have a different server-side configuration, but by default:

- When issuing a non-archived certificate, the DN is *always* reversed. Therefore you must always have the **Reverse DN** option selected if you want the DN to match the supplied DN.
- When issuing internally archived Entrust certificates, the DN is always CN first regardless of the source DN format or the state of the **Reverse DN** flag.

Note: MyID does not recognize this option when using the **Issue Card** workflow to issue a card.

4 Troubleshooting

This chapter contains information about:

- Troubleshooting errors produced by the CA.

  See section *4.1*, *Troubleshooting error messages*.
- Enabling logging for the Entrust components.

  See section *4.2*, *Logging*.
- Auditing details for Entrust operations.

  See section *4.3*, *Auditing*.
- Behavior specific to Entrust v10.

  See section *4.4*, *Entrust v10-specific behavior*.

4.1 Troubleshooting error messages

- **CA reporting error -142**

  This error, which presents as "INI file mismatch", may be caused by DNS lookup problems. Make sure that all servers have fully resolvable addresses and do not have DNS issues.
- **CA reporting error -162**

  You must make sure that the FIPS value in the `entrust.ini` file is set to `0`. Failure to do this will usually result in an `Entrust error = -162` being reported when you try to test the connection.
- **CA reporting error -2187**

  This error may be caused by incorrect mapping in the certificate attributes; for example, if you have mapped the **FASC-N** attribute to **FASC-N (ASCII)** instead of **FASC-N (Hex)**.
- **CA reporting error -2921**

  This CA error – `THE SIGNING/ENCRYPTION EXPIRATION DATE EXCEEDS THE LONGEST ALLOWED CERTIFICATE LIFETIME` – may occur if you have configured MyID to request a date that the CA cannot honor; that is, the CA's own certificate expires before the user certificate end date that you have requested.

  If you see an error with this code, you must reduce the credential profile or certificate lifetime to within a range that your CA can support. See your CA administrator for details of your CA's limits.
- **CA reporting error -8120**

  If you are working in a PIV environment, and your CA reports error `-8120`, you may need to update your `certspec` to remove the rule for `interim_indicator`.

  This error may also be caused (on a customized MyID system that passes Entrust user roles to the CA when requesting a certificate) by a mismatch between the user roles listed on the MyID system and in the Entrust CA. Make sure that the lists on the CA match the lists in MyID. Check the Entrust logs for more information on what might be causing this error.

- **CA reporting error -32712**

  This CA error – `GIVEN TIME VALUE IS NOT VALID` – relates to invalid time values that have previously occurred in situations relating to an overflow in the epoch calculation. If you see an error with this code, contact Intercede customer support, providing as much logging detail as possible.

- **CA reporting error -01055**

  This CA error – `UNABLE TO LOCK THE PROFILE FOR UPDATING` – relates to problems loading the Entrust EPF. If you see this error in your Entrust logs, try giving the MyID COM+ user local administrator privileges.

- **MyID reporting "Card Server Error During Process"**

  After upgrading MyID, if you see an error similar to:

  ```
  Card Server Error During Process
  ```

  when attempting to issue a certificate, with details similar to:

  ```
  BOL COM catch handler Function : ProcessAPDUCommand, catch handler.
  Error : Unspecified error An error occurred inside
  PivCardServer::ProcessCommand Error: 0x80004005 Unspecified error
  Unable to locate java method GetArchCert Unable to locate java method
  GetArchCert ------------------------ Exception raised in function:
  JavaEnvironment::GetMethodID In file JavaEnvironment.cpp at line 132 --
  ---------------------- Exception raised in function:
  JavaAccessor::getArchivedCertificate In file JavaAccessor.cpp at line
  67 In object EntrustJTKConnector.KeyStore.1
  ```

  this may have been caused by an issue during the upgrade installation process that prevented the `EntrustJTKConnector.jar` file from being replaced. As a workaround, you can copy the `EntrustJTKConnector.jar` file from another system, or you can raise a support case with Intercede to identify the cause – to do so, you must provide the `TestReports` folder from the MyID Installation Assistant and quote reference SUP-376.

4.2 Logging

This section contains information on enabling logging for the Entrust components.

Important: Disable the logging when you have completed diagnosing the issues, as the log files may become very large.

4.2.1 Entrust JTK logging

You can enable logging for the Entrust JTK component. On the application server, open regedit and browse to the registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\Connector\
EntrustJTK
```

This key contains the following values:

- `JavaLocation` – an existing value containing the path to the MyID Java components.
- `LogLevel` – a DWORD value containing the logging level to use.
- `LogFile` – a String value containing the path of the JTK log file.

If the `LogLevel` or `LogFile` entries do not exist, you can create them.

For example:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\Connector\EntrustJTK]
"JavaLocation"="C:\\Program Files\\Intercede\\MyID\\Components\\Java"
"LogFile"="c:\\logs\\jtklog.log"
"LogLevel"=dword:00000004
```

In this example, the `LogFile` has been set to the logs folder on drive C:, and in a file named `jtklog.log`.

The logging level is set to `4`. According to the Oracle documentation for logging, the available logging levels are:

- `0` – off
- `1` – basic
- `2` – network, cache, and basic
- `3` – security, network and basic
- `4` – extension, security, network and basic
- `5` – LiveConnect, extension, security, network, temp, basic, and Deployment Rule Set

The above example will log extension, security, network, and basic calls.

To disable logging, you can set the `LogLevel` to `0`, or remove the `LogFile` entry.

For example:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\Connector\EntrustJTK]
"JavaLocation"="C:\\Program Files\\Intercede\\MyID\\Components\\Java"
"LogFile"="c:\\logs\\jtklog.log"
"LogLevel"=dword:00000000
```

or:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\Connector\EntrustJTK]
"JavaLocation"="C:\\Program Files\\Intercede\\MyID\\Components\\Java"
```

Note: The difference between providing no values and a `LogLevel` setting of `0` is that the Java tracing will create or reset the existing log file to a file of length 0, and not produce any logging.

Note: Issuing a single certificate with a `LogLevel` of `4` produces a file over 500 KB; leaving the diagnostic running has implications for disk space.

4.2.2 Entrust Admin logging

You can also set up logging for the Entrust Admin component, which may provide additional information if the logging from the Entrust JTK component does not provide enough information to diagnose your issues.

To set up logging for the Entrust Admin component:

1. Set the following in the application server's registry:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\Trace`

If the `Trace` key does not exist, you must create it.

2. In the `Trace` key, create a DWORD value called `Entrust_Admin`. Set the value to `1` to enable logging, and `0` to disable logging.
3. In the `Trace` key, create a key called `Entrust_Admin`. Within this key, create a string value called `Location` and set this to the full path of the file to which you want to send the log information.

Note: You must ensure that the MyID named COM user has the necessary permissions to create and write to the log file. You can create a file then give the user write permissions if you prefer not to give the user create permissions.

Important: Disable the logging when you have completed diagnosing the issues, as the log file may become very large.

4.2.3 Entrust JTK Connector logging

You can also set up logging for the Entrust JTK Connector component, which may provide some additional information.

To set up logging for the Entrust JTK Connector component:

1. Set the following in the application server's registry:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Intercede\Edefice\Trace`

   If the `Trace` key does not exist, you must create it.
2. In the `Trace` key, create a DWORD value called `EntrustJTKConnector`. Set the value to `1` to enable logging, and `0` to disable logging.
3. In the `Trace` key, create a key called `EntrustJTKConnector`. Within this key, create a string value called `Location` and set this to the full path of the file to which you want to send the log information.

Note: You must ensure that the MyID named COM user has the necessary permissions to create and write to the log file. You can create a file then give the user write permissions if you prefer not to give the user create permissions.

You can set the log file to be the same as the file used by the Entrust Admin logging – the two components can share the file. Log entries include the name of the component; for example:

```
2017-03-29 12:30:04.032 [624.3548] Entrust_Admin CEntrustAdmin Destructor

2017-03-29 12:30:04.032 [6492.4824] EntrustJTKConnector
CConnector::CheckPolicy - CheckPolicy::_com_error IDispatch error #29440
0x80047500
```

Important: Disable the logging when you have completed diagnosing the issues, as the log file may become very large.

4.3 Auditing

The MyID audit report may contain useful information about certificate operations carried out with the Entrust server.

To run the audit report:

1. From the **Reporting** category, select **Audit Reporting**.
2. Select the search criteria; for example, from the **Operation** drop-down list, select **Certificate Requests**.
3. Click **Search**.

See the *Running the audit report* section in the ***Administration Guide*** for more information about the audit report.

Note: The order of the DN element displayed in the audit report may not match the order used for the actual certificate; internally, the DN may be stored in reverse. This does not affect the operation of the certificate.

4.4 Entrust v10-specific behavior

Entrust v10 behaves in a different way to Entrust 8.x, and you may encounter the following issues.

4.4.1 The size of server-generated encryption keys can be increased by the CA

The default key length for server-generated user encryption keys is configured when you first configure and initialize Security Manager.

For example, if you set the size of the server keys to 3K and then later request a 2K key, you receive a 3K key. This affects different key types; for example, if at install you chose ECC-384, then request an RSA 2048-bit key, Entrust returns an RSA 3072-bit key as the equivalent 3K size.

To prevent this from happening, set the policy `userEncryptionAlg` back down to RSA-2048 and you will get the expected key size.

4.4.2 Entrust v10 reports external user configuration failures differently

For usage of Entrust with non-co-located users, you must set a `noUserInDirectory` value for each policy; see section *2.1.5*, *Issuing Certificates to users that do not exist in the directory*.

If this is misconfigured, Entrust v8.x reports an unknown user error, which is easily interpreted.

However, Entrust v10 reports an error similar to the following:

```
-02989 LDAP protocol error
```