



MyID

Version 10.8 Update 2

**Entrust Certificate Authority
Integration Guide**

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

Copyright

© 2001-2018 Intercede Limited. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished exclusively under a restricted license or non-disclosure agreement. Copies of software supplied by Intercede Limited may not be used resold or disclosed to third parties or used for any commercial purpose without written authorization from Intercede Limited and will perpetually remain the property of Intercede Limited. They may not be transferred to any computer without both a service contract for the use of the software on that computer being in existence and written authorization from Intercede Limited.

The software or web site referred to in this manual may utilize or contain material that is © 1994-2000 DUNDAS SOFTWARE LTD., all rights reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Intercede Limited.

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

Licenses and Trademarks

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

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

Conventions Used in this Document

- Lists:
 - ♦ Numbered lists are used to show the steps involved in completing a task when the order is important
 - ♦ Bulleted lists are used when the order is unimportant or to show alternatives
- **Bold** is used for menu items and for labels.
For example:
 - ♦ “Record a valid email address in **‘From’ email address**”
 - ♦ Select **Save** from the **File** menu
- *Italic* is used for emphasis and to indicate references to other sections within the current document:
For example:
 - ♦ “Copy the file *before* starting the installation”
 - ♦ “See *Issuing a Card* for further information”
- ***Bold and italic*** are used to identify the titles of other documents.
For example: “See the ***Release Notes*** for further information.”
Unless otherwise explicitly stated, all referenced documentation is available on the installation CD.
- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.
For example:
Note: This issue only occurs if updating from a previous version.
- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.
For example:

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

Contents

Entrust Certificate Authority	1
1 Introduction.....	5
1.1 Using Entrust CA certificates	5
1.2 Prerequisites.....	5
1.2.1 Entrust ESSC.....	6
1.2.2 Before you install MyID	6
1.2.3 Java Environment	6
1.2.4 Change your existing Entrust configuration settings in MyID	7
1.2.5 Issuing Certificates to users that do not exist in the directory	7
1.2.6 Certificate lifetime	8
1.2.7 Certificate revocation list.....	8
1.2.8 Multiple Entrust digital identities with a single Luna SA HSM	8
2 Configuration	9
2.1 Create the MyID server profile	9
2.2 Set up the MyID Entrust administration link	9
2.3 Key archival and recovery.....	10
2.4 LDAP configuration	10
2.5 Set up the MyID Entrust Certificate Authority.....	10
2.5.1 Admin EPF.....	11
2.6 Editing the CA policy in MyID.....	12
2.7 Enabling certificate policies.....	12
2.8 Updating CA details	15
2.9 Attribute mapping for PIV systems.....	17
2.9.1 Example attribute mapping for PIV systems	17
2.9.2 Example attribute mapping for PIV-I systems	17
2.9.3 Editing the attribute mappings	17
3 Using Directory Services	18
3.1 Microsoft Active Directory	18
3.2 Tracking Entrust DN changes.....	18
4 Troubleshooting and Known Issues	19
4.1 Troubleshooting	19
4.2 Logging.....	19
4.2.1 Entrust JTK logging	19
4.2.2 Entrust Admin logging.....	20
4.2.3 Entrust JTK Connector logging	20

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®.

The instructions it contains are applicable to the following combination of Entrust EASM and Entrust Security Manager Administration:

Entrust EASM	Entrust Security Manager Administration
SM 8.1 SP1 Patch 207324	SMA 8.1 SP1 patch 204648

- **IKB-222 – Entrust integration not available on Windows Server 2016**

At the time of release, integration of MyID with Entrust PKI is not available for MyID application servers running on the Windows Server 2016 operating system, due to dependencies on required Entrust components. Contact customer support quoting reference IKB-222 for further details.

1.1 Using Entrust CA certificates

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 card profile or through card updates and edits.

1.2 Prerequisites

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

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

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

- Java Runtime Environment 8.0 (32-bit).
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8.

Note: The Java Cryptography Extension is now provided with the latest version of the Java Runtime Environment. To configure the extension, you must edit the `java.security` file and set the `crypto.policy` security property to `unlimited`.

By default the `java.security` file is in the following folder:

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

For example:

```
C:\Program Files (x86)\Java\jre1.8.0_161\lib\security
```

If you are using an older version of the Java Runtime Environment, you must download the Java Cryptography Extension separately. You are recommended to upgrade to the latest version of the Java Runtime Environment instead.

- The Entrust Admin Toolkit for C version 6.1 Patch 183731.
- Entrust Authority Security Toolkit version 8.0 Patch 206325 for the Java Platform.

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.

1.2.1 Entrust ESSC

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

1.2.2 Before you install MyID

Before you install MyID, you must copy the `etadmintk.dll` from the Entrust Admin Toolkit to the following folder on the MyID application server:

```
Windows\SysWOW64
```

1.2.3 Java Environment

To enable the Java Interface between MyID and the Entrust 8.1 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 Java Toolkit to the directory containing the MyID Java component. If you have installed MyID in the default location, this is:

```
C:\Program Files (x86)\Intercede\MyID\components\java
```

or

- Copy the MyID Java components to the directory containing the Entrust Java Toolkit `.JAR` files.

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

```
HKEY_LOCAL_MACHINE\SOFTWARE\wow6432Node\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 `SysWOW64` folder on the application server:

- ♦ `jnicapi_32.dll`
- ♦ `JNIPKCS11_32.dll`
- ♦ `UALJNI_32.dll`

Check the Path variable

The installer adds the location of the client `jvm.dll` file to the `Path` variable on the MyID application server. You can check that the `Path` variable contains the correct value.

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 (x86)\Java\jre1.8.0_161\bin\client
```

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

8. Add the path of the parent folder of the folder containing the client `jvm.dll` file.

For example:

```
C:\Program Files (x86)\Java\jre1.8.0_161\bin
```

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:

```
<Path entries>;C:\Program Files
(x86)\Java\jre1.8.0_161\bin\client;C:\Program Files
(x86)\Java\jre1.8.0_161\bin;<More path entries>
```

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.

1.2.4 Change your existing Entrust configuration settings in MyID

If you have an existing installation of MyID that has been configured to use Entrust, then you must change a configuration option before applying the upgrade.

1. Log in to MyID.
2. Select the **Configuration** category and then chose **Operation Settings** from the menu displayed.
3. On the **Entrust** page, set **Entrust Enabled** to **No**.
4. Save your changes.

1.2.5 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.

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

1.2.6 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.

1.2.7 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.

1.2.8 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 Configuration

2.1 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**.

2.2 Set up the MyID Entrust administration link

1. Check that the `etadmintk.dll` file is in the `SysWOW64` 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 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 using a 32-bit library on a 64-bit operating system, you must add the following to the `[Entrust Settings]` section:

```
CryptokiV2LibraryNT=c:\Program Files\SafeNet\LunaClient\win32\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 2.1, *Create the MyID server profile*, to the MyID server.

Note: Write permissions must be set on the `.epf` 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.

2.3 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.

2.4 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. 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.

2.5 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. Select the **Configuration** category. The **Configuration** menu is displayed.
2. Select **Certificate Authorities** from the **Configuration** menu.
3. 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**.
4. From the **CA Type** drop-down list, select **Entrust JTK**.

The screenshot shows a 'Certificate Authority' configuration form. The fields are as follows:

- CA Name:
- CA Description:
- CA Type:
- Retry Delays:
- CA DN:
- CA Host:
- CA Port:
- Entrust.ini:
- Directory:
- Admin EPF:
- Admin EPF Password:
- Confirm Password:
- Encryption PFX:
- Encryption PFX Password:
- Confirm Password:
- Enable CA:

At the bottom, there is a note: "The Certificates available to this Certificate Authority will be updated automatically when Save is clicked. Please re-enter the workflow if the certificates need altering/disabling." and two buttons: "Save" and "Cancel".

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

5. 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.

- ◆ **Entrust.ini** – Enter the fully qualified path to the `entrust.ini` file.
- ◆ **Directory** – Select the LDAP directory being used from the list available.
- ◆ **Admin EPF** – See section 2.5.1, *Admin EPF* for details.
- ◆ **Admin EPF Password** – Enter the password used to access the file specified in **Admin EPF**.
- ◆ **Encryption PFX** – Enter the fully qualified path to the encryption certificate file. This can be a PFX or P12 file.

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 `N/A` in this field and in the **Encryption PFX Password** field.

- ◆ **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.

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

2.5.1 Admin EPF

The **Admin EPF** can either be the full file path to the `epf` file created in section 2.1, *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/SysWow64/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/win32/cryptoki.dll/123456789|HSMOfficer.tkn
```

2.6 Editing the CA policy in MyID

For a PIV system, if you add a new CA or add a new policy to a CA, you must run the following stored procedure on the MyID database before you can edit the policy in MyID:

```
sp_setEntrustCertExtensions
```

2.7 Enabling certificate policies

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 [Administration Guide](#) for details.
 - ◆ **Reverse DN** – select this option if the certificate requires the Distinguished Name to be reversed.
 - ◆ **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.
 - ◆ **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.
 - **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.
 - **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 type. ECC types 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**.

Attribute	Type	Value
common name	Dynamic	Common Name
publish flag	Static	No
FASC-N	Dynamic	FASC-N (Hex)
UserPrincipalName	Dynamic	User Principal Name
Email	Not Required	Not Required
UUID	Dynamic	UUID (Hex)
NACI Check	Dynamic	NACI Status
Common Name (Searchable)	Not Required	Not Required
Email (Searchable)	Not Required	Not Required
Additional Field 4 (Non-searchable)	Not Required	Not Required
Additional Field 5 (Non-searchable)	Not Required	Not Required
Employee ID (Non-searchable)	Not Required	Not Required
Address (Non-searchable)	Not Required	Not Required
Two letter country code. For example, US, UK. (Non-searchable)	Not Required	Not Required
AddField6 (Non-searchable)	Not Required	Not Required
Job title (Non-searchable)	Not Required	Not Required
Locality (Non-searchable)	Not Required	Not Required
state (Non-searchable)	Not Required	Not Required

* = Mandatory attribute
= Recommended attribute

[Hide 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 2.9, [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 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.

Select a CA

CA Name: Test1 CA Description: Test1 Certificate Authority

CA Type: Entrust JTK

CA Enabled: ●

Name	Description	Allow Issuance	Reverse DN	Archive Keys	Superseded
ent_ad_dc : Dual Usage on cn=VINFENTRUSTCA01,ou=PKI,ou=CA,dc=domain06,dc=local		✗	✗	✗	✗
ent_admsrvcs_userreg : Encryption on cn=VINFENTRUSTCA01,ou=PKI,ou=CA,dc=domain06,dc=local		✗	✗	✓	✗
ent_admsrvcs_userreg : Verification on cn=VINFENTRUSTCA01,ou=PKI,ou=CA,dc=domain06,dc=local		✗	✗	✓	✗
ent_admsrvcs_usrmgmt : Encryption on cn=VINFENTRUSTCA01,ou=PKI,ou=CA,dc=domain06,dc=local		✗	✗	✓	✗
ent_admsrvcs_usrmgmt : Verification on cn=VINFENTRUSTCA01,ou=PKI,ou=CA,dc=domain06,dc=local		✗	✗	✓	✗
ent_default : Encryption on cn=VINFENTRUSTCA01,ou=PKI,ou=CA,dc=domain06,dc=local		✗	✗	✓	✗
ent_default : Verification on cn=VINFENTRUSTCA01,ou=PKI,ou=CA,dc=domain06,dc=local		✗	✗	✗	✗
ent_desktop : Encryption on cn=VINFENTRUSTCA01,ou=PKI,ou=CA,dc=domain06,dc=local		✗	✗	✓	✗
ent_desktop : Verification on cn=VINFENTRUSTCA01,ou=PKI,ou=CA,dc=domain06,dc=local		✗	✗	✗	✗

[New](#)
[Edit](#)

3. Click **Edit**.

4. Make sure **Enable CA** is selected.

5. You can edit the following:

- ◆ **Entrust.ini** – Enter the fully qualified path to the `entrust.ini` file.
- ◆ **Admin EPF** – See section 2.5.1, *Admin EPF* for details.

Note: If you change the **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**.

2.9 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.

2.9.1 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)

2.9.2 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)

2.9.3 Editing the attribute mappings

To edit the attribute mapping:

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

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.
3. Click **Save**.

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`.

In some installations it may be found that the LDAP directory server being used will not support the `objectClass` `entrustCA`. For example, it may be `CA` or something similar. See your *Security Manager Directory Configuration Guide* (provided by Entrust) for details.

To allow for this, the query that MyID uses to find this entity may be overridden by altering a value in the MyID database.

For assistance in modifying MyID to specify the query, contact customer support quoting reference SUP-221.

3.1 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
```

3.2 Tracking Entrust DN changes

You can use the **Track Entrust DN Changes** option on the **LDAP** tab of the **Operation Settings** workflow to control whether DN changes are sent to Entrust. This option is set to **No** by default; you must switch it to **Yes** if you want MyID to update Entrust with DN changes.

When you switch this option on, the following occur:

- Updating the user DN using the **Edit Person** workflow or through LDAP synchronization causes the DN in Entrust to be changed to the new value.
- Certificates remain associated with the MyID user account.
- Certificates issued to the previous DN can still be revoked, suspended, or unsuspended through MyID.
- Archived certificates issued to the previous DN can still be recovered through MyID.

4 Troubleshooting and Known Issues

4.1 Troubleshooting

- **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`.

4.2 Logging

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\wow6432Node\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\Wow6432Node\Intercede\Edefice\Connector\EntrustJTK]
"JavaLocation"="C:\\Program Files (x86)\\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\Wow6432Node\Intercede\Edefice\Connector\EntrustJTK]
"JavaLocation"="C:\\Program Files
(x86)\\Intercede\\MyID\\Components\\Java"
"LogFile"="c:\\logs\\jtklog.log"
"LogLevel"=dword:00000000
```

or:

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Intercede\Edefice\Connector\EntrustJTK]
"JavaLocation"="C:\\Program Files
(x86)\\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\Wow6432Node\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\Wow6432Node\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.