



**MyID**  
Version 11.4

# **Entrust Certificate Authority**

## **Integration Guide**

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

## Copyright

© 2001-2019 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 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

<b>Entrust Certificate Authority .....</b>	<b>1</b>
<b>1 Introduction.....</b>	<b>5</b>
1.1 ECC support .....	5
1.2 Using Entrust CA certificates .....	5
1.3 Prerequisites.....	5
1.3.1 Unlimited strength crypto policy .....	6
1.3.2 Entrust ESSC.....	6
1.3.3 Before you install MyID .....	6
1.3.4 Java Environment.....	7
1.3.5 Change your existing Entrust configuration settings in MyID.....	8
1.3.6 Issuing Certificates to users that do not exist in the directory .....	8
1.3.7 Certificate lifetime .....	8
1.3.8 Certificate revocation list.....	8
1.3.9 Multiple Entrust digital identities with a single Luna SA HSM .....	9
1.3.10 Certificate content.....	9
1.4 Change history.....	9
<b>2 Configuration .....</b>	<b>10</b>
2.1 Create the MyID server profile.....	10
2.2 Set up the MyID Entrust administration link .....	10
2.3 Key archival and recovery.....	11
2.4 LDAP configuration.....	11
2.5 Set up the MyID Entrust Certificate Authority.....	11
2.5.1 Admin EPF.....	13
2.6 Editing the CA policy in MyID.....	14
2.7 Enabling certificate policies.....	14
2.8 Updating CA details .....	17
2.9 Deleting a CA.....	18
2.10 Attribute mapping for PIV systems.....	19
2.10.1 Example attribute mapping for PIV systems .....	19
2.10.2 Example attribute mapping for PIV-I systems .....	19
2.10.3 Editing the attribute mappings .....	19
<b>3 Using Directory Services .....</b>	<b>20</b>
3.1 Setting the LDAP query string.....	20
3.2 Microsoft Active Directory .....	20
3.3 Tracking Entrust DN changes.....	21
3.3.1 Known issues.....	21
3.4 DN order .....	21
<b>4 Troubleshooting and Known Issues .....</b>	<b>22</b>
4.1 Troubleshooting .....	22
4.2 Logging.....	22
4.2.1 Entrust JTK logging .....	22
4.2.2 Entrust Admin logging.....	24
4.2.3 Entrust JTK Connector logging .....	24

# 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®.

## 1.1 ECC support

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

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

## 1.2 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 credential profile or through card updates and edits.

## 1.3 Prerequisites

The instructions in this document apply to the following combinations of Entrust EASM and Entrust Security Manager Administration:

Entrust EASM	Entrust Security Manager Administration
SM 8.1 SP1 Patch 207425	SMA 8.1 SP1 patch 204648
SM 8.2.40	SMA 8.2.40
SM 8.3.20	SMA 8.3.20

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

- **IKB-222 – Entrust integration not available on Windows Server 2016 or 2019**

At the time of release, integration of MyID with Entrust PKI is not available for MyID application servers running on the Windows Server 2016 or Windows Server 2019 operating systems, due to dependencies on required Entrust components. If you are integrating with Entrust, you are recommended to run MyID on Windows Server 2012 R2. Contact customer support quoting reference IKB-222 for further details.

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 Runtime Environment (JRE) 8.0 (32-bit).

**Note:** This release has been tested with JRE 8.0 update 231, and uses the following for example file paths:

`C:\Program Files (x86)\Java\jre1.8.0_231\`

Your Java file paths may be different if you are using a different update of the JRE.

- The Entrust Admin Toolkit for C version 6.1 Patch 207503.
- Entrust Authority Security Toolkit for the Java Platform version 8.0 Patch 206325.

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.

### 1.3.1 Unlimited strength crypto policy

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

To configure the extension, you must edit the `java.security` file and make sure that the `crypto.policy` security property is `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_231\lib\security
```

The 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 uncomment the line.

**Note:** If you are using an older version of the Java Runtime Environment, you must download the Java Cryptography Extension separately:

- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8.

However, you are recommended to upgrade to the latest version of the Java Runtime Environment instead, which includes the JCE.

### 1.3.2 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, please contact Intercede support for advice.

### 1.3.3 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
```

### 1.3.4 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 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 (x86)\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\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_231\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_231\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_231\bin\client;C:\Program Files  
(x86)\Java\jre1.8.0_231\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.

### 1.3.5 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.

### 1.3.6 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.

### 1.3.7 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.

### 1.3.8 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.



### 1.3.9 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".

### 1.3.10 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.

## 1.4 Change history

Version	Description
IMP1951-01	Released with MyID 11.0.
INT1951-02	Released with MyID 11.1.
INT1951-03	Released with MyID 11.2.
INT1951-04	Released with MyID 11.3.
INT1951-05	Released with MyID 11.4.

## 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 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 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 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`.

## 2.3 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; 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.

## 2.5 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 form is titled 'Certificate Authority' and contains several input fields. The 'CA Name' field is highlighted with an orange background. The 'CA Description' field is a text input. The 'CA Type' is a dropdown menu set to 'Entrust JTK'. The 'Retry Delays' field contains the value '15;60;60;60;60;120;180;360;3600;86'. The 'CA DN' field is a long text input. The 'CA Host' and 'CA Port' fields are text inputs. The 'LDAP Query' field is a text input. The 'Entrust.ini' field is a text input. The 'Directory' field is a dropdown menu set to 'Please select...'. The 'Admin EPF' field is a text input. The 'Admin EPF Password' and 'Confirm Password' fields are text inputs. The 'Encryption PFX' field is a text input. The 'Encryption PFX Password' and 'Confirm Password' fields are text inputs. The 'Enable CA' checkbox is checked. At the bottom of the form, 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.
  - ◆ **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.
  - ◆ **Directory** – Select the LDAP directory being used from the list available.
  - ◆ **Admin EPF** – See section 2.5.1, *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 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.  
**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.
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

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.

## 2.7 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.

The screenshot shows the 'Select a CA' configuration window. At the top, there is a dropdown menu for 'CA Name' set to 'Entrust ODSEE' and a 'CA Description' field containing 'Entrust ODSEE'. Below this, 'CA Type' is 'Entrust JTK' and 'CA Enabled' has a green checkmark. The main part of the window is a table with the following columns: Name, Description, Allow Issuance, Reverse DN, Archive Keys, and Superseded. The table lists various certificate policies with their corresponding status icons (green checkmarks for enabled, red X for disabled).

Name	Description	Allow Issuance	Reverse DN	Archive Keys	Superseded
ent_ad_dc : Dual Usage on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		X	X	X	X
ent_admsrvcs_ums_ea : Encryption on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		X	X	✓	X
ent_admsrvcs_ums_ea : Verification on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		X	X	X	X
ent_admsrvcs_userreg : Encryption on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		X	X	✓	X
ent_admsrvcs_userreg : Verification on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		X	X	X	X
ent_admsrvcs_usrmgmt : Encryption on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		X	X	✓	X
ent_admsrvcs_usrmgmt : Verification on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		X	X	X	X
ent_csres_approver : Encryption on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		X	X	X	X
ent_csres_approver : Verification on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		X	X	X	X
ent_csres_requestor : Encryption on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		X	X	✓	X
ent_csres_requestor : Verification on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		X	X	X	X
ent_default : Encryption on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		✓	X	✓	X
ent_default : Verification on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		X	X	X	X
ent_desktop : Encryption on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		✓	X	✓	X
ent_desktop : Verification on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		X	X	X	X
ent_eaccattached : Encryption on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		X	X	✓	X
ent_eaccattached : Verification on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		X	X	X	X
ent_eacon : Encryption on ou=Entrust ODSEE,ou=PKI,ou=CA,dc=domain15,dc=local		X	X	✓	X

At the bottom right of the table, there are three buttons: 'Delete', 'New', and 'Edit'.

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.

**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.

- **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.

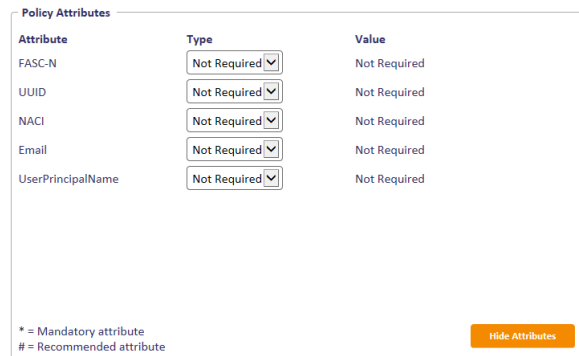
- ◆ **Key Purpose** – select one of the following:

- **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
FASC-N	Not Required	Not Required
UUID	Not Required	Not Required
NACI	Not Required	Not Required
Email	Not Required	Not Required
UserPrincipalName	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 [2.10, 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.

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 2.5.1, *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**.

## 2.9 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 [Administration Guide](#) for details.

## 2.10 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.

### 2.10.1 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)

### 2.10.2 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)

### 2.10.3 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`.

### 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

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.

#### 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.

### 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.

## 4 Troubleshooting and Known Issues

### 4.1 Troubleshooting

- **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 -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`.

- **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.

### 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.