



MyID

Version 10.8 Update 2

**UniCERT UPI 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

UniCERT UPI Certificate Authority	1
1 Introduction.....	5
1.1 Hardware and software requirements	5
2 Adding Support for the UniCERT UPI to MyID	6
2.1 Prerequisites.....	6
2.1.1 UniCERT CA.....	6
2.1.2 Java environment	7
2.2 UniCERT registration forms	8
3 After Installation	10
3.1 Setting up the CA.....	10
3.1.1 Configuring MyID to use a PKCS#11 device for the storage of the RAO/RRO Certificate.....	11
3.1.2 Certificate lifetime	11
3.2 Attribute mapping for PIV systems.....	12
3.2.1 Example attribute mapping for PIV systems	12
3.2.2 Example attribute mapping for PIV-I systems	12
3.3 Secure communications between MyID and UniCERT.....	13
4 Troubleshooting	14
5 Known Issues	15

1 Introduction

This document describes integrating the UniCERT CA (Certification Authority) with MyID® using the UniCERT UPI Java toolkit.

1.1 Hardware and software requirements

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

2 Adding Support for the UniCERT UPI to MyID

MyID integrates with the UniCERT CA through the UniCERT UPI.

Before installing the connector, please verify that the prerequisites are met.

2.1 Prerequisites

2.1.1 UniCERT CA

- Oracle
 - An installation of Oracle appropriate to the version of UniCERT being used.
- UniCERT 5.4.1.
 - UniCERT is a public-key certification platform providing online services for registration agents and remote users.
 - a) The following entities must be created and configured:
 - Certification Authority (CA).
 - CA Operator (CAO).
 - Registration Authority (RA).
 - Registration Authority Exchange (RAX).
 - Certificate Status Service (CSS).
 - Key Archival Server (KAS) – required if you intend to use key archival.
 - Note:** If you are using key archival, you must make sure that your certificate policies can be archived; make sure the policies are set up for data encipherment and/or key encipherment.
 - b) Start the CA, RA, RAX, CSS, and (optionally) KAS using the UniCERT Service Manager.
 - c) Create a policy for the Registration Authority Operator. This can be done via the WebRAO template.
 - d) Create an RAO entity. Export and save its PKCS#12 certificate or create the credential on your HSM.
 - If you are using KAS, create an RRO entity instead of an RAO entity.
 - e) Set up a group that will allow the RAO/RRO to authorize any policies you want to publish to MyID.
- UniCERT UPI 5.4.1.
 - Install and configure the UPI following the instructions provided on the UPI installation disk.

2.1.2 Java environment

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

- Java SE Runtime Environment 8 (32-bit).
This release has been tested with version 1.8+ only.
UniCERT 5.4.1 ships with 1.8u31.
The latest version is 1.8u161.
- 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.

You must copy the following `.JAR` files from UniCERT to the MyID application server:

- `KeyToolsPro.jar`
- `BRSP.jar`
- `commons-lang.jar`
- `commons-logging.jar`
- `ContainerLib.jar`
- `jcrypt.jar`
- `jdom.jar`
- `Shared.jar`
- `SharedClient.jar`
- `upiclient.jar`

These files are provided with your UniCERT installation material, and are not provided by Intercede.

To enable the Java Interface between MyID and the UniCERT server to function correctly, all the `.JAR` files must be in the same location on the MyID server. If you have installed MyID in the default location, this is:

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

This folder must contain the MyID UniCERT connector:

- `UPICconnector.jar`

Check the Path variable

The location of the client `jvm.dll` file must be included in the `Path` variable on the MyID application server.

To check the path variable:

1. Access **System Properties** on the MyID application server.
Select **System** from the **Control Panel**, then click **Advanced system settings**.

2. On the **Advanced** tab, click **Environment Variables**.
3. Find the `Path` variable in the list of **System variables** and select it.
4. Click **Edit**.
5. 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
```

Note: The path should be separated from any other paths in the variable with a semi-colon.

6. You must also make sure that the path of the parent folder of the folder containing the client `jvm.dll` file is included in the `Path` variable.

For example:

```
C:\Program Files (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.

7. Click **OK** to save any changes you have made to the path.
8. Click **OK** to close **Environment Variables**.
9. Click **OK** to close **System Properties**.

2.2 UniCERT registration forms

This solution uses UniCERT registration forms to make certificate requests to the CA. During this process, the DN supplied by the client is broken into its component parts and placed in the registration form.

Note: MyID requires the forms to have the **Archive Required** property set, and for the **Generation Site** property to be set to **Certificate Authority**.

By default the form fields are filled in the same order as the DN; for example, if your DN is in the following format:

```
cn=Joe Bloggs,ou=test,o=company,c=UK
```

The form elements would be filled like this:

```
CertificateTemplate[0]/Subject/RDN[0]/Value = Joe Bloggs
```

```
CertificateTemplate[0]/Subject/RDN[1]/Value = test
```

```
CertificateTemplate[0]/Subject/RDN[2]/Value = company
```

```
CertificateTemplate[0]/Subject/RDN[3]/Value = UK
```

Note: Any form fields that have default values in them will not be updated.

If your DN does not provide the elements in the appropriate order, you must override this mapping by setting values in the system registry:

1. Open the registry editor at the following location in:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Intercede\Edefice\Connector\Unicert\RDNMap
```

Note: You may have to create these keys if they do not already exist.

2. Add **DWORD** values to define the mapping; for example:

- ◆ Create a `DWORD` value named `RDN1` and set the value data to 3.

This would mean that the form field:

```
CertificateTemplate[0]/Subject/RDN[1]/Value
```

will be filled in with the fourth (zero based numbering) element of the DN as follows:

```
CertificateTemplate[0]/Subject/RDN[1]/Value = UK
```

3. Add entries for each RDN element on the certificate request form.

Note: If there is an element on the form that you do not want to fill in, you can set a value of `FFFFFFFF` (in Hexadecimal); for example:

```
RDN3 = FFFFFFFFFF
```

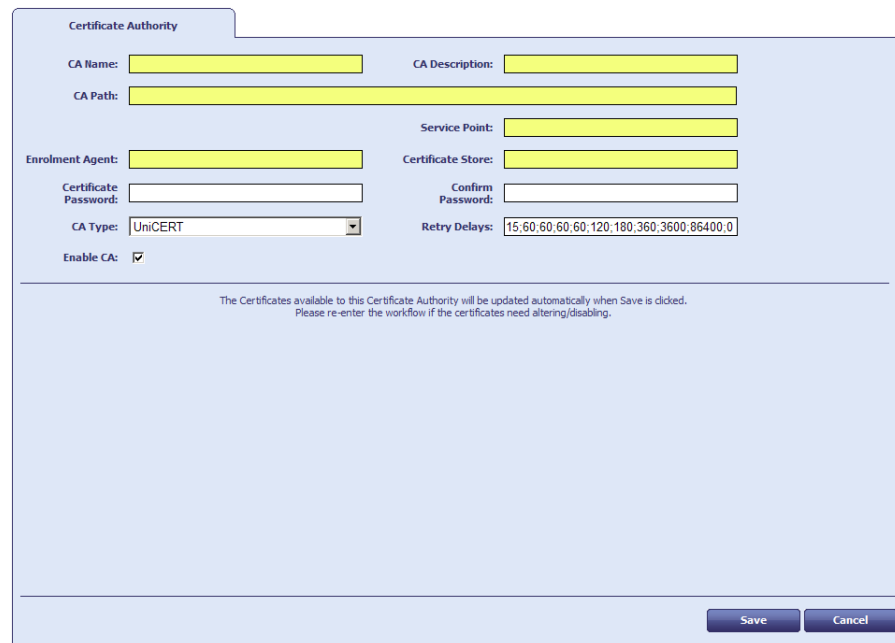
Note: These mappings are static and are only usable if the format of your DNs is also static. That is, if for instance the email is not always sent with the request you would not be able to use the RDN mapping feature.

3 After Installation

3.1 Setting up the CA

You must provide MyID with the certificate it needs to sign any requests it makes and make the policies published by the CA available for use.

1. Copy the PKCS#12 certificate generated by the Registration Authority Operator (RAO) to the MyID Application server.
2. Log on to MyID and click the **Configuration** category.
3. Select **Certificate Authorities** from the list of workflows displayed.
4. Click **New** at the bottom of the page.



5. Enter a name for the CA in **CA Name** and a short name in **CA Description**.
6. In **CA Type**, select **UniCERT**.
7. Enter the distinguished name (DN) for the CA in **CA Path**.
8. Enter the web address for contacting the UPI in **Service Point**.

For example:

`https://myserver.example.com/UPI`

9. Enter the DN for the RA in **Enrollment Agent**.
10. In **Certificate Store**, enter the location of the PKCS#12 certificate you copied to the application server – the RAO/RRO certificate.

For example:

`C:\unicert\myrro.p12`

11. Type the **Certificate Password** for the RAO/RRO certificate and confirm it in the **Confirm Password** box.
12. Set the **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.

The default is:

```
15;60;60;60;60;120;180;360;3600;86400;0
```

This retries after 15 seconds, then after a minute four times, then two minutes, three minutes, six minutes, an hour, 24 hours, then stops.

13. Click **Save**.

MyID automatically detects the policies published by the CA and these can immediately be enabled for use by card policies.

3.1.1 Configuring MyID to use a PKCS#11 device for the storage of the RAO/RRO Certificate

When configuring the CA in MyID, the Certificate Store entry may have two forms.

- Path to a PKCS#12 file on the application server
Points to a PKCS#12 file containing the RAO/RRO Certificate.
- Path to a PKCS#11 Device on the application server

To use a PKCS#11 device, create an entry like the following:

```
HSM://P11Driver/SlotName
```

Where:

- ◆ *P11Driver* is the filename of the PKCS#11 driver for your device. It may be the full path or just the name of the file if it is in the system path.
- ◆ *SlotName* is the name of the Slot on which the certificate resides.

To use a preferred signer from the slot, for example if you have a common partition shared by a number of CAs, the format instead is:

```
HSM://P11Driver/SlotName|PreferredSigner
```

For example:

```
HSM://cryptoki.dll/vinfunica01|MyID_HSM - DS, NR, KE
```

where the `PreferredSigner` name is how it is shown in the UniCERT TokenManager utility.

3.1.2 Certificate lifetime

If the expiry time for the certificate is later than the expiry date for the device, and the **Restrict certificate lifetimes to the card** option (on the **Certificates** page of the **Operation Settings** workflow within MyID) is set to *Yes*, the certificate lifetime is reduced to match the lifetime of the device.

MyID stores certificate lifetimes in days, while UniCERT may use other units; for example, years. MyID converts these units to the correct number of days, taking into account leap years, when displaying the lifetime of the certificate.

3.2 Attribute mapping for PIV systems

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

The attributes must be visible on the form in UniCERT; if the attributes are not visible, MyID will be unable to set any values. Not all attributes are required for all certificate profiles; you must make sure that these attributes are set to be optional in UniCERT. You are recommended to set the attributes to mandatory on the CA when MyID requires a value.

Note: The UUID mapping is required only for PIV Interoperable (PIV-I) devices, and is optional for standard PIV cards. 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.

3.2.1 Example attribute mapping for PIV systems

Certificate Policy	NACI Indicator	Subject Alt Federal Agency Smart Credential Number	Subject Alt Microsoft UPN	Subject Alt Email – RFC 822 Name
PIV Authentication	NACI Status	FASC-N (Hex)	User Principal Name	Not Required
PIV Card Authentication	NACI Status	FASC-N (Hex)	Not Required	Not Required
PIV Encryption	Not Required	Not Required	Not Required	Email
PIV Signing	Not Required	Not Required	Not Required	Email

3.2.2 Example attribute mapping for PIV-I systems

Certificate Policy	NACI Indicator	Subject Alt Uniform Resource Identifier	Subject Alt Microsoft UPN	Subject Alt Email – RFC 822 Name
PIV Authentication	Not Required	UUID (ASCII)	User Principal Name	Not Required
PIV Card Authentication	Not Required	UUID (ASCII)	Not Required	Not Required
PIV Encryption	Not Required	Not Required	Not Required	Email
PIV Signing	Not Required	Not Required	Not Required	Email

Note: The attribute names in the above tables are the defaults provided. These names are required for MyID to be able to find and set the attribute values.

3.3 Secure communications between MyID and UniCERT

To allow MyID to communicate with UniCERT over SSL, you must ensure that the Java environment on the MyID server trusts the SSL certificate that the UniCERT web server provides.

If the certificate is provided by a trusted root CA, such as the Thawte or VeriSign root CAs, there is no further configuration required. Otherwise, you must install the certificate in the Java environment's trusted certificate store.

Note: The SSL certificate must have a CN that is the fully qualified domain name (FQDN) for the Java environment. The **Service Point** as configured in MyID must also use the FQDN so that the Java environment matches the SSL certificate to the URL.

1. Export the SSL certificate.

One way to do this is to visit the UniCERT web site through https in a web browser, click on the certificate icon, then install the certificate. You can then copy the certificate to a file.

2. Locate the MyID server's Java home environment.

For example:

```
C:\Program Files\java\jre8
```

3. Import the SSL certificate into the MyID server's Java trusted certificate store.

```
<java_home>\bin\keytool -import -trustcacerts  
-alias <unicert_server_name>  
-keystore <java_home>\lib\security\cacerts  
-file \path\to\ssl_certificate.cer  
-storepass changeit
```

4 Troubleshooting

- **Invalid certificate policy for archival**

If you have not set up your certificate policies with data encipherment and/or key encipherment, and attempt to archive certificates, the MyID log events may contain an error similar to:

```
<Error>
  <Code>-2147195611</Code>
  <Function>DoCertRequest</Function>
  <Message>Failure in UPI during certificate request submission
Error generating the key pair for keyproperties with index
com.cybertrust.unicert.upi.client.UPIException: Error generating the
key pair for keyproperties with index:0 at
com.cybertrust.unicert.upi.client.SoftwareEEIdentity.generateKeyPair
(Unknown Source) at
com.intercede.cybertrust.CertRequester.DoCertRequest (CertRequester.j
ava:147) Caused by: java.lang.IllegalArgumentException: Policies
with archival required must specify an encipherment key usage. ...
2 more
  </Message>
  <StackTrace>com.cybertrust.unicert.upi.client.UPIException: Error
generating the key pair for keyproperties with index:0 at
com.cybertrust.unicert.upi.client.SoftwareEEIdentity.generateKeyPair
(Unknown Source) at
com.intercede.cybertrust.CertRequester.DoCertRequest (CertRequester.j
ava:147) Caused by: java.lang.IllegalArgumentException: Policies
with archival required must specify an encipherment key usage. ...
2 more
  </StackTrace>
</Error>
```

Make sure your certificate policies have been set up correctly.

- **KAS not available**

If you do not have the optional KAS UniCERT module, and attempt to issue archived certificates, an error similar to the following appears:

```
<Error>
  <Code>-2147195611</Code>
  <Function>DoCertRequest</Function>
  <Message>Failure in UPI during certificate request submission No
KAS certificate was found during the encryption/decryption
operation. com.cybertrust.unicert.upi.client.ConfigurationException:
upi.config.kascert.missing at
com.cybertrust.unicert.upi.client.CertificateRequestForm.addPrivateK
eyForArchive(Unknown Source) at
com.cybertrust.unicert.upi.client.SoftwareEEIdentity.generateKeyPair
(Unknown Source) at
com.intercede.cybertrust.CertRequester.DoCertRequest (CertRequester.j
ava:147)
  </Message>
  <StackTrace>com.cybertrust.unicert.upi.client.ConfigurationException
: upi.config.kascert.missing at
com.cybertrust.unicert.upi.client.CertificateRequestForm.addPrivateK
eyForArchive(Unknown Source) at
com.cybertrust.unicert.upi.client.SoftwareEEIdentity.generateKeyPair
(Unknown Source) at
com.intercede.cybertrust.CertRequester.DoCertRequest (CertRequester.j
ava:147)
  </StackTrace>
</Error>
```

5 Known Issues

- **IKB-234 – Key recovery from a UniCERT certificate authority as software certificates (PFX file) fails**

Attempts to recover a certificate with archived keys (for example, encryption certificates) to a software certificate file will fail due to an error in MyID. This affects new issuance of certificates using the **Collect My Certificates** workflow, and also recovering existing certificates using the **Recover Certificates** and **Recover My Certificates** workflows.