



MyID

CIV

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 product 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

1	Introduction.....	5
1.1	Change history.....	5
2	Installing and Configuring MyID for CIV	6
2.1	Locking down the server	6
2.2	Begin enrollment and card issuance	6
2.3	CIV card format.....	6
2.4	Card certificates	6
2.5	Controlling the content of subject alternative names	7
2.6	Configure server signing certificates	7
2.7	Configuring the PIV server hash algorithm	8
3	Accessing MyID for the First Time	9
3.1	PIV Card Application Administrator Key	9
3.1.1	Factory 9B keys	9
3.1.2	Customer 9B keys	10
3.2	Specify which certificates to use	11
3.3	Setting up the credential profile	12

1 Introduction

A Personal Identity Verification (PIV) card is a secure identity card issued by Federal agencies in accordance with the specifications laid out in FIPS 201. A PIV-interoperable (PIV-I) card is a non-Federal version of the same technology used by Federal contractors to access Federal buildings and networks.

CIV is *Commercial* Identity Verification – it is a method of using the PIV-I technology, specifications and data model without requiring cross-certification with Federal agencies. In short, it is a way of using PIV cards for your own organization.

Follow the instructions for installing MyID in the [Installation and Configuration Guide](#). This document provides instructions for additional configuration that you must carry out for CIV implementations.

1.1 Change history

Version	Description
INT1735-01	First release.
INT1735-02	Added information on CSP for SHA256.
INT1735-03	Content signing restrictions.
INT1735-04	Rebranding.
INT1735-05	Updated for MyID 10.6.
INT1735-06	Updated for MyID 10.7.
INT1735-07	Clarification about signing certificates. Must use RSA keys, not ECC.
INT1735-08	Documentation updated to use latest templates.

2 Installing and Configuring MyID for CIV

After you have installed MyID following the instructions in the [Installation and Configuration Guide](#), you must install the CIV module. See the readme provided with the CIV module for details.

2.1 Locking down the server

Most importantly, after you have your system configured, and before you start using it operationally, you must lock down your system. See the [System Security Checklist](#) document for more information.

2.2 Begin enrollment and card issuance

Once configuration of MyID has completed, enrollment of applicants for PIV cards can begin. Initially, you are recommended to focus on issuing cards to people who will fulfill the operator roles in MyID. This will then allow you to harden security of the system by cancelling any bootstrap cards and turning off Password Logon to MyID.

2.3 CIV card format

When you use the **Credential Profiles** workflow to set up the profile that you are going to use to issue cards, you must specify the **CivCertificatesCHUID.xml** as the **Card Format**.

This card format specifies the following PIV containers:

- Card Capability Container.
- Card Holder Unique Identifier (CHUID).
- Security Object.
- Certificates and KeyHistory.

2.4 Card certificates

There are four certificates expected on a PIV card, each in a named container on the card:

- PIV Authentication
- Digital Signature
- Key Management
- Card Authentication

The latest revision of the standard has also included the ability to store cryptographic key history, which allows recovery (onto cards that support the feature) of keys and certificates that are no longer active, following replacement or re-issuance of the PIV card.

2.5 Controlling the content of subject alternative names

By default, the content for subject alternative names is controlled by the CA, and content specified in a certificate request is not accepted. To specify content for subject alternative names, you may have to modify the configuration of the CA.

For details of any specific changes you need to make to the CA to allow the specification of content for subject alternative names, see the relevant CA implementation guide.

To control the content of subject alternative names in MyID, see section 3.2, [Specify which certificates to use](#).

2.6 Configure server signing certificates

To increase the level of security, MyID digitally signs some of the data objects that are written to the PIV card:

- CHUID (Card Holder Unique ID)
- Security Object

The server can either use a single certificate to sign the data objects or a separate certificate can be configured for each object.

Note: You must configure the server signing certificates on the server prior to issuing PIV cards.

Note: The signing certificate must use an RSA key – ECC is not supported.

The signing certificate must have an extended key usage attribute of:

```
id-PIV-content-signing (2.16.840.1.101.3.6.7)
```

The signing certificate must not require any user intervention when signing:

- Do not set the private key as User Protected; this requires a PIN entry dialog during signing.
- If the key is protected by an HSM, do not configure the key to launch a PIN entry dialog. For an nCipher HSM, the nCipher CSP must not be configured to protect the private key with an operator cardset that requires PIN entry. For nCipher HSMs, the content signer certificate can be protected either by the module, or by an operator cardset without PIN.

Refer to the FIPS 201 documentation for additional requirements relating to the PIV content signing certificate.

Before MyID can use a certificate to sign objects, the certificate must be available to the account used to run the MyID components.

Note: If you are using SHA256 (see section 2.7, [Configuring the PIV server hash algorithm](#)) you must use a CSP that supports SHA256; for example, you can use the Microsoft Enhanced RSA and AES Cryptographic Provider CSP.

1. On the MyID application server, log on using the account that you use to run the MyID components.
2. Request a certificate that will be protected either by CAPI (Cryptographic Service Provider) or by CNG (Key Storage Provider). You can issue a certificate from any certificate authority as long as it is available to CAPI or CNG.

Note: Do not enable strong private key protection on the certificate, as this will prevent processing of the request by the MyID account.

3. Once the certificate has been generated, install and save it as a .cer file (either Base64/PEM or binary format). You must save it in a location accessible to the MyID application, so save it to the `Components` folder within the MyID installation folder.

Note: You may need administrative privileges to save files to this area.

4. Enter the filename of the certificate in the system registry.
 - a) From the **Start** menu, click **Run** and type `regedit` in the dialog displayed. Click **OK**.
 - b) Navigate to:


```
HKEY_LOCAL_MACHINE\SOFTWARE\wow6432Node\Intercede\Edefice\PIV
```
 - c) Set the value of the following keys to the full path of the certificate:
 - CHUIDSigningCertificate
 - SecurityObjectSigningCertificate
5. If you are using multiple application servers, repeat this process on each application server.

Note: The server signing certificate will expire. Once the lifetime of issued cards goes beyond the expiration date of the server signing certificate, the issued card is no longer valid.

This means that the date at which the server signing certificate must be renewed depends not only on the expiration date of the server signing certificate, but also the intended card lifetime of the cards being issued.

To prevent a situation where the server signing certificate is not valid for the lifetime of the issued certificate, you must set up a procedure to ensure that the server signing certificate is manually renewed before issuing cards that have an expiration date that may exceed the expiration date of the server signing certificate.

2.7 Configuring the PIV server hash algorithm

You can specify the PIV server hash algorithm. Data can be hashed using SHA256 or SHA1. The default is SHA 256, and you are recommended to use this setting.

1. From the **Configuration** category, select **Security Settings**.
2. Click the **Server** tab.
3. Type a value for the **PIV Server hash algorithm** option.

You can type one of the following:

- ♦ SHA1
- ♦ SHA256

4. Click **Save changes**.

3 Accessing MyID for the First Time

3.1 PIV Card Application Administrator Key

You must enter the values of secret shared keys (9B keys) to enable the smart card management system to authenticate (and therefore manage) the smart cards. If you do not have this factory key, you cannot issue cards.

9B keys and related specifications are defined in *SP 800-73-1 – Interfaces for Personal Identity Verification* available at <http://csrc.nist.gov>.

3.1.1 Factory 9B keys

When cards are manufactured, they are provided with a factory key. You will have been given this factory 9B key by your smart card supplier; this is a string of characters in hexadecimal format.

1. From the **Configuration** category, select **Key Manager**.
2. From the **Select Key Type to Manage** list, select **PIV 9B Card Administration Key**, then click **Next**.
3. Click Add New Key.

The screenshot shows a web form titled "Add Key (PIV 9B Card Administration Key)". The form includes the following fields:

- Credential Type:** A dropdown menu with "A.E.T. Europe B.V." selected.
- Key Type:** A dropdown menu with "Factory" selected.
- Key Diversity:** A dropdown menu with "Static" selected.
- Encryption Type:** A dropdown menu with "2DES" selected.
- Description:** An empty text input field.
- Encryption Key:** A text input field with a yellow highlight.
- Save:** A button at the bottom right of the form.

4. Select the **Credential Type** from the drop-down list. This is the type of card you are using.
5. Select **Factory** from the **Key Type** drop-down list. This means that you are using the key provided by your supplier.
6. Select **Static** from the **Key Diversity** drop-down list. You can select only **Static** for factory keys.
7. Select the **Encryption Type** from the drop-down list.

Warning: Make sure you select the **Encryption Type** supported by the cards you are using. If you select the wrong length of key, you will not be able to issue cards.

8. Type a **Description** for the key.

9. Type the hexadecimal 9B key provided by your smart card supplier in the **Encryption Key** box.
10. Click **Save**.

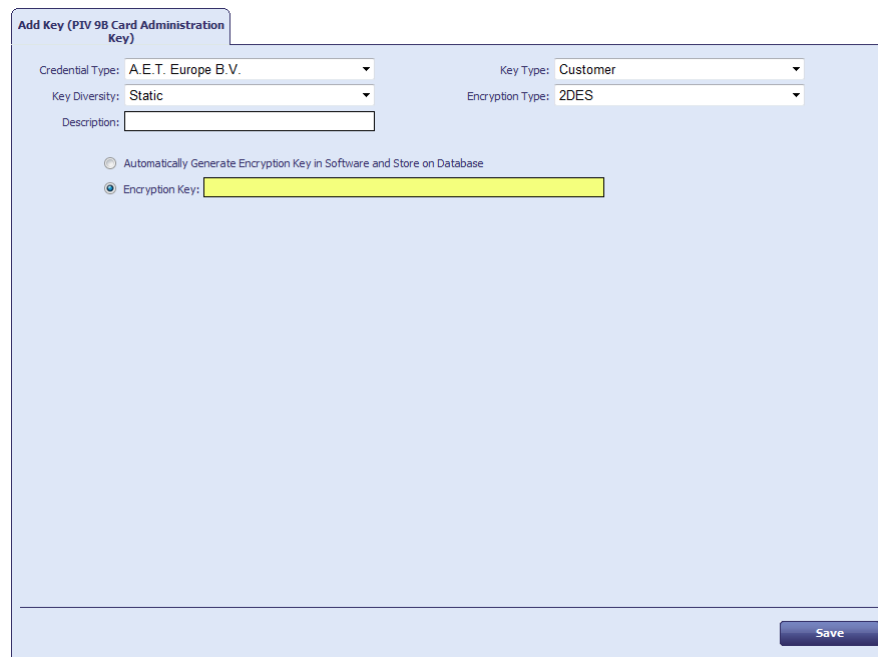
3.1.2 Customer 9B keys

For production systems, you *must* configure a customer 9B key for each card type. When issuing a card, MyID will change the factory 9B key to the customer 9B key.

This means that if you need to be able to reuse the card in different installations, you must cancel the card – canceling a card changes the customer 9B key back to the factory 9B key so the card can be reused.

Note: If you lose the key data held in the database or HSM, you will no longer be able to cancel or unlock the card.

1. From the **Configuration** category, select **Key Manager**.
2. From the **Select Key Type to Manage** list, select **PIV 9B Card Administration Key**, then click **Next**.
3. Click Add New Key.
4. Select the **Credential Type** from the drop-down list. This is the type of card you are using.
5. Select **Customer** from the **Key Type** drop-down list.



6. Select **Static** or **Diverse** from the **Key Diversity** drop-down list.
You are recommended to use diverse keys - diverse keys are more secure, as a new key is generated for each card.
7. Select the same **Encryption Type** as you specified for the factory key.
8. Type a **Description** for the key.
9. If you are storing the key in the database, choose one of the following options:
 - ♦ **Automatically Generated Encryption Key** – this option automatically creates an encryption key.
 - ♦ **Encryption Key** – type the hexadecimal key in the box. This is not recommended for production systems.

If you are storing the key on an HSM, choose one of the following options:

- ♦ **Automatically Generate Encryption Key on HSM** – this option generates a key on the HSM.
- ♦ **Existing HSM Key Label** – if you have an existing key on your HSM that you want to use, type its label.

10. Click **Save**.

GlobalPlatform keys for PIV cards

If you want to specify customer PIV keys for certain types of PIV cards, you must have a GlobalPlatform factory keyset defined for the cards – the GlobalPlatform key is used to authenticate any change to the PIV 9B key.

To create a GlobalPlatform key, click the **Applets** category and select the **Manage GlobalPlatform Keys** workflow from the list.

See the [System Security Checklist](#) for more information about GlobalPlatform keys.

Random SOPINs

For production systems, you are strongly recommended to set random SOPINs. See the [System Security Checklist](#) for more information.

3.2 Specify which certificates to use

You can specify which certificates to use for each type of cardholder – after you have set up the list of available certificates, you can assign these certificates to credential profiles that can be restricted to particular cardholder roles.

1. From the **Configuration** category, select **Certificate Authorities**.
2. Add or edit the CA that you want to use.

See the integration guide for your CA for any specific setup information.

- a) Enable the certificate policy you want to use.

Note: The selected policies must create certificates that are 2000 bytes or less in size to comply with the PIV specification.

- b) Click **Edit Attributes**.

Note: Make sure you have set up your CA to allow editing the policy. See your CA integration guide for details.

- c) Select the value you want to associate with the listed attributes.



Attribute	Type	Value
FASC-N	Not Required	Not Required
UUID	Not Required	Not Required
NACI	Not Required	Not Required
UserPrincipalName	Not Required	Not Required
Email	Not Required	Not Required

* = Mandatory attribute
= Recommended attribute

Hide Attributes

Note: Do not map the FASC-N or NACI attributes – these attributes are used for Federal PIV systems only. You are recommended to map UUID for the PIV Auth and Card Auth certificates.

- d) Click **Hide Attributes** to return to the **Certificate Authority** form.
Note: This does not complete the workflow. It is possible to edit attributes for more than one certificate policy.
- e) Set the **Archive Keys** option to **None** for the Authentication, Card Authentication and Digital Signature certificates.
- f) Set the **Archive Keys** option for the Key Management certificate – you are recommended to archive this certificate.
- g) Click **Save**.

3.3 Setting up the credential profile

1. From the **Configuration** category, select **Credential Profiles**.
2. Click **Create** to start a new profile.
Note: CIV systems do not support additional identities. Make sure you do not select the **Issue Additional Identities** option.
3. Click **PIN Settings**.
Note: You can modify the PIN policies for PIV cards in the **PIN Settings** section only within certain limits. This means if you make changes to the following settings outside the accepted parameters, they are ignored:
 - ♦ **Maximum PIN Length** – the maximum length of PIN for a PIV card is 8.
 - ♦ **Minimum PIN Length** – the minimum length of PIN for a PIV card is 6.
 - ♦ **Logon Attempts** – you cannot set this option for PIV cards.
 - ♦ **PIN Inactivity Timer** – you cannot set this option for PIV cards.
 - ♦ **PIN History** – you cannot set this option for PIV cards.
4. Click **PIN Characters**.
 It is possible to configure MyID to use non-numeric PIN characters for some PIV cards, although some cards will fail to issue.
 For PIV cards, set Numeric to be **Mandatory**, and uppercase letters, lowercase letters, and symbols to **Not Allowed**.
5. Click **Device Profiles**.
6. From the **Card Format** drop-down list, select one of the following:
 - ♦ **None** – select this for non-CIV cards.
 - ♦ **CivCertificatesCHUID.xml** – select this for CIV cards. This is the recommended option.
 - ♦ **CivCertificatesOnly.xml** – select this for cards onto which you want to write only the certificates, and none of the other CIV data.
 The card format uses data model files that determine the format of the content of the cards; that is, which data goes in which field.
7. Click **Next**.

Select Certificates

Please select the certificates that you wish this credential profile to have

		Use for MyID Signing	Use for MyID Encryption	Set Default Certificate	Use Named Container
<input type="checkbox"/> Unmanaged*	Unmanaged certificate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default
<input checked="" type="checkbox"/> PIVAuthentication on VINFHS2012DC01		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default
<input type="checkbox"/> PIVCardAuthentication on VINFHS2012DC01		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default
<input type="checkbox"/> PIVContentSigningCertificate on VINFHS2012DC01		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default
<input type="checkbox"/> PIVSigningCertificate on VINFHS2012DC01		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Default

* Certificate is set for key archival, these can only be issued if the credential profile supports encryption

Next >

8. For each certificate you want to use:
 - a) Select the certificate.
 - b) From the **Use Named Container** drop-down list, select the appropriate container.
 - c) If the card is to be used to log on to MyID, select **Use for MyID Signing** for one of the certificates.

You are advised to use the PIV Authentication Certificate for signing; you cannot use the Digital Signature Certificate.
9. Click **Next**.
10. Select the applets you want to copy onto the card.
11. Click **Next**.
12. In the **Can Be Issued** column, select the roles of the users to whom you want to be able to issue the cards.
13. In the **Can Issue** column, select the roles of the operators you want to be able to request cards using this profile.
14. Click **Next**.

Select the appropriate CIV card layout.

You can select several card layouts to be available in the profile. If so, the issuer selects the layout when printing the card.

You can customize and create new layouts using the **Card Layout Editor** in the **Configuration** category. See the [Administration Guide](#) for details.
15. Click **Next**, then complete the **Comments** box.
16. Click **Next** to complete the workflow.