



**MyID PIV**  
Version 11.5

# **Derived Credentials**

## **Installation and Configuration 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

© 2001-2020 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.

### **Bouncy castle**

Copyright © 2000 – 2011 The Legion Of The Bouncy Castle  
(<http://www.bouncycastle.org>)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

### **KSoap2**

Copyright © 2003,2004 Stefan Haustein, Oberhausen, Rhld., Germany

Copyright © 2006, James Seigel, Calgary, AB., Canada

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

#### **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:

<b>Warning:</b> You must take a backup of your database before making any changes to it.
--

## Contents

<b>Derived Credentials.....</b>	<b>1</b>
<b>1 Introduction.....</b>	<b>6</b>
1.1 What are derived credentials? .....	6
1.2 Deriving credentials from other systems .....	6
1.3 Prerequisites and installation .....	7
1.4 Overview.....	8
1.5 Derived credentials for unknown users .....	9
1.6 FIPS 201-2 and derived credentials.....	9
1.7 Change history.....	10
<b>2 Configuring the System .....</b>	<b>11</b>
2.1 Recovering archived certificates .....	11
2.2 Setting the configuration options.....	11
2.2.1 Determining which cards are available for derived credentials .....	11
2.2.2 Setting the credential check period.....	12
2.2.3 Configuring certificate OIDs checked on PIV cards .....	12
2.2.4 Determining whether fingerprints are required for derived credentials.....	13
2.3 Granting access to the workflows .....	13
2.3.1 Role permissions .....	14
2.3.2 Scope .....	14
2.4 Configuring the Certificate Authority .....	15
2.4.1 Setting up the certificate attribute mappings .....	15
2.4.2 Setting up the certificate checks .....	15
2.5 Setting up the credential profiles for derived credentials .....	16
2.5.1 Creating an Identity Agent credential profile .....	16
2.5.2 Creating a VSC credential profile.....	17
2.5.3 Creating the imported credential profile .....	20
<b>3 Requesting Derived Credentials .....</b>	<b>21</b>
3.1 Requesting derived credentials.....	21
3.1.1 Setting the timeout for the PIN entry screen .....	21

# 1 Introduction

This document provides information on the support for MyID® Derived Credentials, including details on the following:

- Configuring the system to support the installation of derived credentials to mobile devices, Microsoft Virtual Smart Cards, and Intel Authenticate.
- Requesting derived credentials through the MyID Self-Service Kiosk.

In this document, the words *mobile device* may refer either to a smartphone or a tablet.

## 1.1 What are derived credentials?

Derived credentials are mobile- or VSC-based identities that are based on credentials already issued to a user. The derived credentials may include: a recovered archived encryption certificate, allowing the user access to their email and so on; a set of new certificates; and a badge layout that can be displayed on a mobile device.

You can use derived credentials for the following:

- Email signing
- Email encryption
- Authentication (for example, logon to Windows)

Because the credentials are *derived* from the original credentials, you do not need to go through an enrollment process for the user to issue the derived credentials.

## 1.2 Deriving credentials from other systems

MyID also allows you to create derived credentials from cards issued by systems other than the current MyID system. You cannot recover archived encryption certificates from these systems, but you can create a derived identity with a new set of certificates. You can integrate your MyID system with the external system by using the Derived Credentials Notification Listener; this web service allows you to inform the MyID system of the following events:

- `CessationOfTrust` – the cardholder is no longer eligible for a PIV credential.
- `TransferOfTrust` – the credential has been replaced by a newer credential.
- `ChangeOfDetails` – the cardholder's details have changed.

See the [\*Derived Credentials Notification Listener Application Interface\*](#) for details

## 1.3 Prerequisites and installation

For prerequisites and installation instructions, see the [readme.html](#) document provided with this release, which provides details of the MyID patches you need to have installed on your system.

- MyID Self-Service Kiosk

The Self-Service Kiosk allows you to request derived credentials.

See the [Self-Service Kiosk Installation and Configuration](#) document for details.

- MyID Identity Agent app

For mobile-based derived credentials, you must have the MyID Identity Agent app installed on your mobile device. You can configure the Self-Service Kiosk to allow you to download the Identity Agent onto your mobile device.

See the [Mobile Identity Management Installation and Configuration Guide](#) for system requirements and details of configuring your system for mobile identities.

- Trusted Platform Module

For Microsoft VSC-based derived credentials, you must have a PC with a Trusted Platform Module. See the [Microsoft Virtual Smart Card Integration Guide](#) for system requirements and details of configuring your system for Microsoft VSCs.

- Intel Authenticate

For Intel Authenticate-based derived credentials, your PC must support Intel Authenticate. See the [Intel Authenticate Integration Guide](#) for system requirements and details of configuring your system for Intel Authenticate VSCs.

## 1.4 Overview

The process is as follows:

1. You collect and activate a smart card from MyID.  
Alternatively, you obtain a smart card from another system.
2. At the Self-Service Kiosk, insert your issued smart card.
3. If required, validate your fingerprints.
4. Request a derived credential based on your original credential.
5. Follow the collection procedure for the type of derived credential you need.

For mobile identities:

- a) If you do not already have the MyID Identity Agent app, the Kiosk displays a QR code that allows you to download the app.

You must configure the appropriate URLs for each mobile platform you are using – see the [Administration Guide](#) for details of the **App Download URL** configuration options (on the **Issuance Processes** page of the **Operation Settings** workflow).

**Note:** You can configure MyID to display an alternative text-based URL that you can type in as an alternative to scanning the QR code. For details, contact customer support, quoting reference SUP-180.

- b) Open the MyID Identity Agent app and scan the displayed QR code.
- c) The MyID Identity Agent app downloads the certificates and badge layouts.
- d) Your device now contains a mobile identity derived from your original credentials.

For VSC-based derived credentials (Microsoft VSC or Intel Authenticate):

- a) If a one-time password is displayed on screen, take a note of this.

**Note:** To make use of a logon code, the user must have a SAM account name, otherwise the Self-Service App is unable to target the job when the user logs into their workstation. You must also make sure that the **Allow Logon Codes** configuration option (on the **Logon** page of the **Security Settings** workflow) is set to Yes.

- b) Check your email for instructions on installing the VSC on your PC.

**Note:** The user must have an email address registered within MyID. For imported users with cards issued by another system, they must have an email address attribute mapping in their signing and encryption certificates, as otherwise MyID cannot send an email notification to initiate collection of a VSC.

6. The derived credentials can be managed by MyID independently of the original credential – you can disable or cancel them.

**Note:** To renew or replace a derived credential, you must cancel the derived credential then repeat the original request process. This ensures all required derived credential verification steps take place.

7. After seven days, MyID performs a revocation check against the PIV Authentication certificate used during the request for derived credentials. If this certificate has been revoked, MyID revokes the derived credentials.



## 1.5 Derived credentials for unknown users

You can request derived credentials using cards that were not issued by the current MyID system, and that are held by users who are not in the MyID database.

When you request derived credentials using your card, if your DN does not match a user in the MyID database, a new user record is created within MyID with your details. The new user is created within the Derived Credentials top-level group, within a group with the name `Agency - XXXX`, where `XXXX` is your agency code. If possible, your photograph is extracted from the card and imported into the MyID user record.

Note, however, that facial biometrics and fingerprints are *not* extracted.

If it is not possible to extract the photograph from the card, the import continues, but the failure is noted in the MyID audit trail.

The smart card is also added to the MyID database and can be used to log on to MyID, once you have granted the appropriate permissions.

## 1.6 FIPS 201-2 and derived credentials

MyID derived credentials comply with the requirements of FIPS 201-2 in the following ways.

FIPS 201-2 Compliance	MyID Derived Credentials
Identity Level of Assurance 3 (LOA3) – Remote Identity Collection	The applicant approaches the Self-Service Kiosk and inserts their PIV card.
Applicant Must Demonstrate Possession and Control of the Related PIV Card	The PIV card is validated to ensure that it has not been tampered with.
Applicant Must Demonstrate Possession and Control of the Related PIV Card	The applicant enters their PIN for PIV card authentication.
The Applicant Shall Identify Himself/Herself Using a Biometric Sample That Can be Verified Against the Applicant's PIV Card	The applicant completes fingerprint verification.
Validate Identity Certificate to Federal Bridge	The PIV Auth Cert on the card is checked to ensure that it is valid and has not been revoked.
Key Generation on FIPS 140-2 level 1 Software Cryptographic Module (iOS)	Certificates/keys are provisioned to a FIPS 140-2 validated credentials store on the mobile device.
7 Day Revocation Check if Card is Revoked Within 7 Days After Issuance of Derived Credentials	The applicant's original PIV card is validated 7 days after initial issuance of derived credentials.
All Communications Shall be Authenticated and Protected from Modification	Communication is secured during the derived credentials process.
The Issuer of the Derived PIV Credential Shall Implement a Process that Maintains a Link Between the Subscriber's PIV Card and the Derived PIV Credential to Enable the Issuer of the Latter Credential to Track the Status of the PIV Card in Order to Perform Timely Maintenance and Termination Activities in Response to Changes in the Status of the PIV Card.	The applicant's PIV card and derived credentials are linked to ensure that credentials can be managed effectively.

## 1.7 Change history

Version	Description
IMP1947-01	Released with MyID 11.0.
IMP1947-02	Released with MyID 11.1.
IMP1947-03	Released with MyID 11.2.
IMP1947-04	Released with MyID 11.3.
IMP1947-05	Released with MyID 11.4.
IMP1947-06	Released with MyID 11.5.

## 2 Configuring the System

### 2.1 Recovering archived certificates

To recover a certificate from an existing card, the user must have a certificate that:

- has been issued by the current MyID system.
- is issued to a current device.
- has archived keys.
- is issuable and recoverable to software.
- has a policy that is available on at least one credential profile available to the user.

### 2.2 Setting the configuration options

#### 2.2.1 Determining which cards are available for derived credentials

You may want to configure your system to issue derived credentials only from cards that have been issued by specific federal agencies. To do this, you can match the agency code in the FASC-N.

To determine which cards you can use to request derived credentials:

1. From the **Configuration** category, select the **Operation Settings** workflow.
2. Click the **Certificates** tab.
3. Set the following option:

- ♦ **Cards allowed for derivation**

Set this option to a regular expression that will be matched against the ASCII version of the card's FASC-N to determine whether the card can be used to request derived credential. If the regular expression matches, the card can be used.

For example:

5400.+

This example allows any card from the agency with code 5400 to be used. The agency code appears at the start of the ASCII FASC-N.

**Note:** By default, this option is blank, which means that no cards can be used to request derived credentials. To allow *all* cards to be used, use the following regular expression:

.+

4. Click **Save changes**.

## 2.2.2 Setting the credential check period

By default, seven days after MyID issues derived credentials, it checks the original credentials that were used to request the derived credentials. If, during this period, the original credentials became no longer valid (for example, if the smart card was cancelled), MyID revokes the derived credentials.

You can adjust the time period for this check:

1. From the **Configuration** category, select **Operation Settings**.
2. On the **Certificates** tab, set the following:
  - ♦ **Derived credential revocation check offset** – set to the number of days after issuing derived credentials that you want MyID to check the original credentials.
3. Click **Save changes**.

## 2.2.3 Configuring certificate OIDs checked on PIV cards

When a PIV card is presented to the derived credential kiosk, MyID verifies that the cardholder can perform two factor authentication with the PIV card, performing the PKI-AUTH check to verify the PIV-Authentication certificate.

Additionally, MyID verifies the Digital Signature certificate.

These certificate checks ensure that the certificate is valid and was issued from a CA that chains up to a root certificate in the `DerivedCredentialTrustedRoot` store.

It also checks that the end-user certificate contains the correct OID to mark it as a PIV-Authentication or Digital Signature certificate.

By default, MyID is configured with the OIDs required by FIPS201-2; however, you can change the OIDs if required (for example, for a CIV certificate).

To configure the OIDs:

1. From the **Configuration** category, select **Operation Settings**.
2. On the **Certificates** tab, set the following:
  - ♦ **Derived credential certificate OID** – set this to the OID to be checked on the PIV Authentication certificate.  
 The default value is  
`2.16.840.1.101.3.2.1.3.13`
  - ♦ **Derived credential signing certificate OID** – set this to the a semicolon-delimited list of OIDs to be checked on the Digital Signature certificate.  
 The default value is  
`2.16.840.1.101.3.2.1.3.6;2.16.840.1.101.3.2.1.3.7;  
2.16.840.1.101.3.2.1.3.16`
3. Click **Save changes**.

## 2.2.4 Determining whether fingerprints are required for derived credentials

By default, MyID requires biometric verification to collect derived credentials. The user's fingerprints are checked against the sample stored on the card; the biometric sample is not imported into MyID.

If the smart cards onto which you want to collect derived credentials does not support biometric verification (for example, VSCs) you must set this option to No.

You can switch this option on or off:

1. From the **Configuration** category, select **Operation Settings**.
2. On the **Biometrics** tab, set the following:
  - ♦ **Require fingerprints for derived credentials** – set this to Yes to require fingerprint verification to collect derived credentials, or No to allow the collection of derived credentials without fingerprint verification.
3. Click **Save changes**.

## 2.3 Granting access to the workflows

The system makes use of the following workflows:

- **Request Derived Credentials** – used in the Self-Service Kiosk to allow a cardholder to request a derived credential.
- **Cancel Credential** – used within MyID to cancel a mobile ID and revoke its certificates.
- **Enable / Disable ID** – used within MyID to enable or disable a mobile ID, and suspend or enable its certificates.
- **Unlock Credential** – used within MyID to retrieve an unlock code for an issued mobile ID.
- **Collect My Updates** – used by the Identity Agent app to obtain a mobile ID.
- **Issue Device** – used by the Identity Agent app to obtain a mobile ID.

**Note:** The **Mobile Certificate Recovery**, **Collect My Updates**, and **Issue Device** workflows are not used within MyID or the Self-Service Kiosk; they are used to control access from a mobile device to the features of the web service.

- **Collect My Card** – used in the Self-Service App to collect VSCs.

Use the **Edit Roles** workflow to grant access for these workflows to the roles you want to be able to access them.

### 2.3.1 Role permissions

You must use the **Edit Roles** workflow to ensure that the roles used for derived credentials have the appropriate permissions.

The following roles are used for derived credentials:

- **Server Credentials**

Make sure this role has access to the following:

- ♦ **Request Derived Credentials (part 1)**
- ♦ **Collect My Updates**
- ♦ **Issue Device**

- **Derived Credential Owner**

This role is used for unknown users who are imported into MyID. Make sure this role has access to the following:

- ♦ **Request Derived Credentials (part 2)**
- ♦ **Collect My Updates.**
- ♦ **Issue Device**
- ♦ **Collect My Card** – used for VSC collection

- **PIV Applicant**

This role is used for existing MyID users. Make sure this role has access to the following:

- ♦ **Request Derived Credentials (part 2)**
- ♦ **Collect My Updates**
- ♦ **Collect My Card** – used for VSC collection

Alternatively, assign these permissions to a different role or roles – this allows you to lock down access to derived credentials to specific users.

**Note:** To access the Self-Service Kiosk, the PIV Applicant role must have **Smart Card** as a logon method; you can set this using the **Edit Roles** workflow.

**Note:** Any roles applied to user accounts by the derived credentials process override any role restrictions in MyID.

### 2.3.2 Scope

When a mobile device user, for example a guard, requests the details for another mobile device user, the guard must have the correct scope within MyID to view the details of the other user; for example, the user must be in the same group as the guard if the guard has Department scope.

## 2.4 Configuring the Certificate Authority

### 2.4.1 Setting up the certificate attribute mappings

PIV derived credentials must follow the PIV specifications for the certificate policies issued to the derived credential.

As described in NIST SP800-157, PIV derived credentials require the Derived PIV Authentication certificate. The details for this policy are described in the *Common Policy Certificate and CRL Profile* document published by FPKIPA.

You must set up the attribute mappings for this policy using the **Edit Attributes** button in the **Certificate Authorities** workflow; for more information, see the integration guide for your certificate authority. The following table displays the required mappings:

Certificate Policy	FASC-N	UUID	NACI	User Principal Name	Email
Derived PIV Authentication	Not required	UUID (ASCII)	NACI Status	Not required	Not required

Additionally, as described in NIST SP800-157, the PIV Signing and PIV Encryption certificates may also be issued to the derived credential.

If your installation allows, the PIV Encryption certificate can be recovered to the derived credential; that is, the same PIV Encryption certificates can be shared between the PIV card and the derived credential.

### 2.4.2 Setting up the certificate checks

For the derived credential certificate checks to work, you must export the certificate authority's root certificate, then install this on your MyID application server.

**Note:** The RootCA certificate (the certificate authority's root certificate) must be trusted by the MyID application server. If it is not already a trusted certificate, add it to the Trusted Root Certificate Authority store for the local machine.

1. In the **Issued Certificates** on the CA, open any issued certificate.
2. On the **Certification Path** tab, select the top-level certificate.
3. Click **View Certificate**.
4. On the **Details** tab, click **Copy to File**.
5. Use the Certificate Export Wizard to export the certificate.

Give the exported certificate the name `RootCA.cer`.

6. Copy the `RootCA.cer` file to the MyID application server.
7. Open a command prompt with Run as Administrator.
8. At the command line, type:

```
certutil -addstore -f -Enterprise DerivedCredentialTrustedRoots  
RootCA.cer
```

## 2.5 Setting up the credential profiles for derived credentials

You must create new credential profiles for the derived credentials.

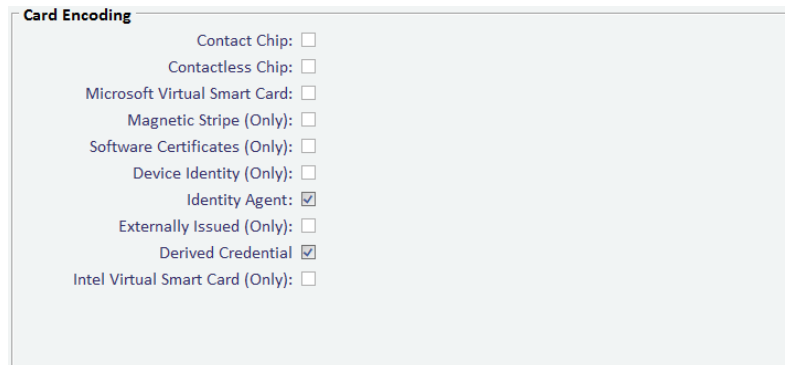
You must create at least one credential profile to contain the certificates that you want to issue to the derived credential. You may create as many of these credential profiles as you need; for example, you may want to create a credential profile for mobile devices, a credential profile for Microsoft VSCs, and a credential profile for Intel VSCs.

If you are creating derived credentials from cards that were not issued by the current MyID system, you must create an additional credential profile to be used for importing the original credential into the system.

### 2.5.1 Creating an Identity Agent credential profile

To create a credential profile for issuing derived credentials to mobile devices:

1. From the **Configuration** category, select **Credential profiles**.
2. Click **New**.
3. Type a **Name** for the credential profile.
4. In **Card Encoding**, select **Identity Agent** and **Derived Credential**.



5. In **Services**, make sure **MyID Logon** and **MyID Encryption** are selected.

**Note:** If you select the **Identity Agent** option *after* you select the **Derived Credential** option, you cannot select the **Services** option; however, **MyID Logon** and **MyID Encryption** are automatically selected.

6. In **Issuance Settings**, in the **Mobile Device Restrictions** drop-down list, select one of the following:
  - ♦ **Any** – The mobile identity can be loaded onto any mobile.
  - ♦ **Known Mobiles** – The mobile identity can be loaded onto any mobile that has already been registered with MyID. See the [Mobile Identity Management Installation and Configuration Guide](#) for details.
  - ♦ **My Mobiles Only** – The mobile identity can be loaded only onto mobiles associated with the user's account.
7. If you are issuing Identity Agent credentials for users associated with cards that were not issued by the current system, set the following option:
  - ♦ **Require Facial Biometrics** – Never Required.
8. In **Device Profiles**, from the **Card Format** drop-down list select **PIVDerivedCredential.xml**.  
 Select a different option *only* if you have a customized data model that you must use for your system.
9. Click **Next**.



10. Select the certificates you want to make available.
  - ♦ For credential profiles that use a PIV data model, select the PIV containers for the certificates. You must select a signing certificate. To allow online unlocking, you must include a certificate in the PIV Card Authentication Certificate container.
  - ♦ For credential profiles that do not use a PIV data model, do not select any containers.

All of the certificates you select here will be issued to your mobile device.

You can select the archived and historic certificate options on this screen. See the [Administration Guide](#) for details of the **Issue new**, **Use existing**, and **Historic Only** options.

11. Click **Next** and proceed to the Select Roles screen.
12. Select the roles you want to be able to issue this credential profile, and the roles you want to be able to be issued this credential profile.
 

**Note:** Any role to which you want to issue derived credentials must have the **Issue Device** option selected in the **Cards** category within the **Edit Roles** workflow.
13. Click **Next**.
14. Select the card layouts you want to make available to the mobile device.
 

Badges based on these layouts will be transferred to the mobile device as part of the mobile ID. Note, however, that the reverse sides of the selected layouts (the `_back` layouts) will not be available on the mobile device.

**Note:** You must select at least one card layout. If you do not want to display personalized badge information on the mobile device, create a card layout containing default artwork and no user information.
15. Select one of the layouts to be the default layout.
 

This layout will be displayed by default when using the Identity Agent app, and will be used for phone-to-phone identity verification.
16. Click **Next**.
17. Type your **Comments** and complete the workflow.

## 2.5.2 Creating a VSC credential profile

To create a credential profile for issuing derived credentials as Microsoft VSCs or Intel Authenticate:

1. From the **Configuration** category, select **Credential profiles**.
2. Click **New**.
3. Type a **Name** for the credential profile.
4. Select the **Card Encoding**:
  - ♦ For Microsoft VSCs, select **Microsoft Virtual Smart Card** and **Derived Credential**.
  - ♦ For Intel Authenticate, select **Intel Virtual Smart Card (Only)** and **Derived Credential**.
5. In **Services**, set the MyID Logon and MyID Encryption options:
  - ♦ For Microsoft VSCs, make sure **MyID Logon** and **MyID Encryption** are selected.
  - ♦ For Intel Authenticate, make sure **MyID Logon** is selected.

**Note:** You cannot use an Intel Authenticate VSC to log on to MyID, but setting this option allows you to select a certificate for signing.

6. In **Issuance Settings**, set the following options:

- ♦ **Generate Logon Code** - select one of the following:
  - **None** – no logon code is generated.
  - **Simple** – the logon code is generated using the complexity rules as defined by the **Simple Logon Code Complexity** configuration option.
  - **Complex** – the logon code is generated using the complexity rules as defined by the **Complex Logon Code Complexity** configuration option.

**Note:** To be FIPS 201-2 compliant, you must select **Simple** or **Complex**. See the [Administration Guide](#) for details of configuring the logon code complexity.

- ♦ **Credential Group** – if you want to restrict users to have a single derived credential VSC, type an identifier here; for example:

DC VSC

If you set the **Active credential profiles per person** configuration option (on the **Issuance Processes** page of the **Operation Settings** workflow) to **One per credential group**, MyID ensures that the user can have only one credential with the same **Credential Group** name.

**Important:** Do not issue more than one Intel Authenticate VSC to a user on a device. You *must* create a credential group and set the **Active credential profiles per person** configuration option to **One per credential group**; see the [Administration Guide](#) for details.

- ♦ **Cancel Previously Issued Device**

This option works in conjunction with the **Credential Group** setting. Select this option, and MyID cancels any previously-issued credentials instead of disabling them. When you collect the new VSC using the Self-Service App (and you have the **Erase Unused VSCs** permission for your role, as configured in the **Edit Roles** workflow) the Self-Service App will delete any of the cancelled VSCs on your device.

For more information on these options, see the [Administration Guide](#).

7. For Microsoft VSCs, set the PIN to 16 numeric digits.

This is required for FIPS 201-2 compliance.

- a) In **PIN Settings**, set the **Maximum PIN Length** and **Minimum PIN Length** options to 16.
- b) In **PIN Characters**, set **Numeric** to **Mandatory**, and **Lowercase**, **Uppercase**, and **Symbol** to **Not Allowed**.

**Note:** This step is not applicable for Intel Authenticate VSCs, as they do not allow you to change the PIN settings.

8. For Intel Authenticate VSCs, set the following PIN Settings:

- ♦ **PIN Algorithm** – EdeficePinGenerator.
- ♦ **Protected Key** – select the PIN generation key you created to protect the Intel Virtual Smart Card PINs. See the [Intel Authenticate Integration Guide](#) for details.

9. In **Device Profiles**, from the **Card Format** drop-down list select **PIVDerivedCredential.xml**.

Select a different option *only* if you have a customized data model that you must use for your system.

10. Set the **Requisite User Data** options.

**Note:** This section appears only if you have selected the **Requisite User Data** option on the **Issuance Processes** tab of the **Operation Settings** workflow.

This section contains a list of user attributes that must be present for this credential profile to be issued.

For example, if your VSC derived credential is to be used for email signing, you must select **Email** from the list, and provide an appropriate certificate for email signing – only users who have the Email attribute mapped in their user account will be able to receive a derived credential VSC based on this credential profile.

Similarly, if your VSC derived credential is to be used for Windows Logon, you must select **UPN** from this list, and provide an appropriate certificate for logging on to Windows.

11. Click **Next**.

12. Select the certificates you want to make available.

- ♦ For credential profiles that use a PIV data model, select the PIV containers for the certificates. To allow online unlocking, you must include a certificate in the PIV Card Authentication Certificate container.
- ♦ For credential profiles that do not use a PIV data model, do not select any containers.

All of the certificates you select here will be issued to your VSC.

You can select the archived and historic certificate options on this screen. See the [Administration Guide](#) for details of the **Issue new**, **Use existing**, and **Historic Only** options.

13. Click **Next** and proceed to the Select Roles screen.

14. Select the roles you want to be able to issue this credential profile, and the roles you want to be able to be issued this credential profile.

**Note:** Any role to which you want to issue derived credentials must have the following configured in the **Edit Roles** workflow:

- ♦ Select the **Issue Device** option in the list of workflows.
- ♦ Select the **Collect My Card** option in the list of workflows.
- ♦ Select the **Password** option in the **Logon Methods**.

15. Click **Next**.

16. Click **Next**.

17. Type your **Comments** and complete the workflow.

### 2.5.3 Creating the imported credential profile

If you are creating a derived credential from a card that was not issued by the current MyID system, MyID will import the deriving credential into the MyID database. You must create a credential profile to be used for this imported smart card.

1. From the **Configuration** category, select **Credential profiles**.
2. Click **New**.
3. Type a **Name** for the credential profile.

The screenshot shows a window titled "Card Encoding" with a list of card types and their corresponding checkboxes:

- Contact Chip: ☐
- Contactless Chip: ☐
- Microsoft Virtual Smart Card: ☐
- Magnetic Stripe (Only): ☐
- Software Certificates (Only): ☐
- Device Identity (Only): ☐
- Identity Agent (Only): ☐
- Externally Issued (Only): ☒
- Derived Credential: ☐
- Intel Virtual Smart Card (Only): ☐

4. In **Card Encoding**, select **Externally Issued (Only)**.
5. In **Services**, select **MyID Logon**.
6. Click **Next**.
7. On the Select Certificates screen, select an **Unmanaged** certificate profile.

This certificate profile is used to contain the authorization certificate imported from the original smart card from which the derived credential is created.

**Note:** You are strongly recommended to rename the Unmanaged policy to a name that indicates its use; for example, Imported PIV Card Authentication Certificate.

If the unmanaged policy is already in use, MyID provides a second unmanaged policy called **Unmanaged Imported**; this policy is disabled by default, which means that you must enable it using the **Certificate Authorities** workflow. If both unmanaged policies are already in use, and you need further unmanaged policies, contact customer support quoting reference SUP-229 for assistance.

8. Select the **Signing** option for the **Unmanaged** certificate profile.
- Note:** If the option to select the **Signing** box is not selectable, in the **Certificate Authorities** workflow, edit the **Unmanaged** CA, and set the **Archive Keys** option to **Internal**.
9. Click **Next**.
10. Select the roles you want to be able to issue and receive this credential profile.
11. Click **Next** and complete the workflow.

## 3 Requesting Derived Credentials

You can request derived credentials for your own mobile device or PC.

Collecting a mobile ID may take several minutes, depending on the complexity of the certificates and the speed of your network connection. If the collection fails due to network problems, you are recommended to use the **Cancel Credential** workflow to cancel the mobile ID, then request another mobile ID for the user.

**Note:** If you see any errors when requesting or collecting derived credentials, see the [Error Code Reference](#) document for possible explanations and solutions.

### 3.1 Requesting derived credentials

To request derived credentials for your own mobile device or PC, use the Self-Service Kiosk and follow the on-screen instructions.

You must run the Kiosk with the `/dc` command-line parameter. See the [Self-Service Kiosk Installation and Configuration](#) document for details.

To issue a derived credential, the PIV card that you present to the kiosk must contain both the PIV Authentication certificate and the Digital Signature certificate.

#### 3.1.1 Setting the timeout for the PIN entry screen

By default, the PIN entry screen for derived credentials on the Self-Service Kiosk will time out after 120 seconds. If you want to change this value, you can edit the configuration file.

To edit the configuration file:

1. On the client PC, back up the `MyIDKiosk.exe.config` file in the following folder:

```
C:\Program Files (x86)\Intercede\MyIDSelfServiceKiosk\
```

2. Using a text editor, open the `MyIDKiosk.exe.config` file.

**Note:** Make the changes to the config file exactly as shown. The case is important.

3. Edit the `value` parameter in the following line:

```
<add key="DerivedCredentialsPageTimeoutSeconds" value="120"/>
```

If this line does not exist, you can add it to the `<appSettings>` section.

For example:

```
<add key="DerivedCredentialsPageTimeoutSeconds" value="60"/>
```

This reduces the timeout to 60 seconds.

4. Save the configuration file.
5. Restart the Kiosk.